CEH

(CEH v12/13)

BY

Jawad Noonari

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

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:

CEH Questions	Possible Answer
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 nonrepudiation 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 Zacmen 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.

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

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 websites that are similar to a specified target URL?	Related:

'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.eccouncil.org.

So, the search query is looking for results that include the keyword "fees" from the domain eccouncil.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 networkrelated 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 highlevel 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 realtime. 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: ● Tool supports to present data using graphs. ● Tool supports to examine the links between different data.	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.

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."