Name:_____ Class:_____ Date:_____

Mod 02: Threat Management and Cybersecurity Resources

1. What is the primary goal of penetration testing?

a. Attempt to uncover deep vulnerabilities and then manually exploit them
b. Scan a network for open FTP ports
c. Perform SYN DOS attack towards a server in a network
d. Attempt to perform an automated scan to discover vulnerabilities

ANSWER: a

FEEDBACK:

a. Correct. The primary goal of penetration testing is to uncover deep vulnerabilities and then manually exploit them.
b. Incorrect. Scanning a network for open FTP ports is one of the various ways of performing active reconnaissance on a network.
c. Incorrect. A TCP SYN DOS (SYN flood) is a type of distributed denial of service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.
d. Incorrect. Attempting to perform an automated scan to discover vulnerabilities is known as vulnerability scanning.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

2. There is often confusion between vulnerability scanning and penetration testing. What is the best explanation of the difference between vulnerability scanning and penetration testing?

a. Vulnerability scanning is performed using an automated tool to scan a network for known vulnerability signatures. Penetration testing involves attempting to manually uncover deep vulnerabilities just as a threat actor would, and then exploiting them.
b. Vulnerability scanning checks a network for outdated versions of services. Penetration testing is attempting to manually uncover deep vulnerabilities just as a threat actor would, and then exploiting them.
c. Vulnerability scanning is performed by manually scanning a network for known vulnerabilities. Penetration testing is attempting to manually scan a network for known vulnerability signatures using an advanced scanning tool.
d. Vulnerability scanning checks a network for open ports and services. Penetration testing is attempting to manually scan a network for known vulnerability signatures using an advanced scanning tool.

ANSWER: a

FEEDBACK:

a. Correct. This is the correct difference between vulnerability scanning and penetration testing.

b. Incorrect. Vulnerability scanning is not checking a network for outdated versions of services.
c. Incorrect. Penetration testing is not attempting to manually scan a network for known vulnerability signatures using an advanced scanning tool.
d. Incorrect. Checking a network for open ports and services is not vulnerability scanning. Penetration testing is not attempting to manually scan a network for known vulnerability signatures using an advanced scanning tool.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

3. Khalid joins a security team where he is assigned an SOC developer role and has to build different teams under SOC. Which of the following teams should he build to deal with providing real-time feedback related to security incidents and threat detections, which can then be utilized to facilitate better prioritization of threats and a mature way of detecting threats?

a. Red team
b. Blue team
c. Purple team
d. White team

ANSWER: c
FEEDBACK:
a. Incorrect. The red team scans for vulnerabilities and then exploits them.
b. Incorrect. The blue team monitors for red team attacks and shores up defenses as necessary.
c. Correct. The purple team provides real-time feedback between the red and blue teams to enhance the testing.
d. Incorrect. The white team enforces the rules for penetration testing.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

4. Kile is assigned a role as a grey box penetration tester in the financial sector. He has to conduct a pen testing

attack on all the application servers in the network. Which of the following tasks should he perform first while conducting a penetration testing attack on a network?

a. Tailgating
b. Phishing
c. Vishing
d. Footprinting

ANSWER: d

FEEDBACK:

a. Incorrect. A tailgating attack, also known as "piggybacking," involves an attacker who lacks proper authentication seeking entry to a restricted area.
b. Incorrect. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
c. Incorrect. Vishing is a social engineering attack that attempts to trick victims into giving up sensitive information over the phone. In most cases, the attacker strategically manipulates human emotions, such as fear, sympathy, and greed, to accomplish their goals
d. Correct. Footprinting is the process of collecting as much information about the target system as possible to find ways to penetrate the system. Information such as IP address, whois records, DNS information, operating system, employee email id, phone numbers, etc., comes under this.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

5. Which of the following tools can be used to scan 16 IP addresses for vulnerabilities?

a. Nessus Essentials
b. Nessus
c. QualysGuard
d. App Scan

ANSWER: a

FEEDBACK:

a. Correct. Nessus has a free version called Nessus Essentials that scans 16 IP addresses.
b. Incorrect. Nessus is perhaps the best-known and most widely used vulnerability scanner. It is a product of Tenable and contains a wide array of prebuilt templates
c. Incorrect. QualysGuard is the Qualys Cloud Platform. Qualys IT, Security,

and Compliance apps are natively integrated, each sharing the same scan data for a single source of truth.

d. Incorrect. AppScan is intended to test web applications for security vulnerabilities during the development process, when it is least expensive to fix such problems.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

6. Which of the following penetration testing consultants have limited knowledge of the network and some elevated privileges?

a. Gray box
b. White box
c. Black box
d. Bug bounty

ANSWER: a
FEEDBACK:

a. Correct. Gray box testers have limited knowledge of the network and some elevated privileges.
b. Incorrect. White box testers are given full knowledge of the network and the source code of applications.
c. Incorrect. Black box testers have no knowledge of the network and no special privileges.
d. Incorrect. A bug bounty is a monetary reward given for uncovering a software vulnerability. Most software developers offer some type of bug bounty, ranging from several thousands of dollars to millions of dollars.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

7. Which of the following is the most efficient means of discovering wireless signals?

a. War flying

b. War chalking
c. War cycling
d. Wardriving

ANSWER: a

FEEDBACK:

a. Correct. War flying is the most efficient means of discovering a Wi-Fi signal. War flying uses drones, which are officially known as unmanned aerial vehicles. Because they can quickly cover a wider area, are not limited to streets and sidewalks, and can easily fly over security perimeters such as fences, drones are the preferred means of finding Wi-Fi signals.
b. Incorrect. War chalking is the act of using specific chalk markings, usually on a sidewalk, to identify Wi-Fi hotspots.
c. Incorrect. No such attack exists in information security.
d. Incorrect. Wardriving is searching for wireless signals from an automobile or on foot
while using a portable computing device. Several tools are necessary to maximize wireless signal detection, but war flying is more efficient than wardriving.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

8. Which of the following techniques is a method of passive reconnaissance?

a. War driving
b. War flying
c. Open Source Intelligence (OSINT)
d. Port scanning

ANSWER: c

FEEDBACK:

a. Incorrect. Wardriving is searching for wireless signals from an automobile or on foot
while using a portable computing device, making it a type of active reconnaissance.
b. Incorrect. War flying uses drones, which are officially known as unmanned aerial vehicles, making it a method of active reconnaissance.
c. Correct. OSINT is used to search online for publicly accessible information. It is a method of passive reconnaissance.
d. Incorrect. Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is a method of performing active reconnaissance.

POINTS: 1

Mod 02: Threat Management and Cybersecurity Resources

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

9. What is the primary difference between credentialed and non-credentialed scans?

a. Credentialed scans use valid authentication credentials to mimic threat actors, while non-credentialed scans do not provide authentication credentials.
b. Credentialed scans are performed by pen testers, while non-credentialed scans are performed by authorized officers.
c. Credentialed scans use advanced scanning tools, while non-credentialed scans do not use tools.
d. Credentialed scans are legal, while non-credentialed scans are illegal.

ANSWER: a
FEEDBACK:
a. Correct. Credentialed scans are the process where valid authentication credentials are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials. A non-credentialed scan provides no such authentication information.
b. Incorrect. Credentialed scans can be performed by pen testers or authorized officers and also by advanced automated vulnerability scanning tools like Qualysguard, Nessus, or AppScan, while non-credentialed scans can be performed only by vulnerability assessment engineers using any basic automated vulnerability scanning tools like OpenVAS (open source tool).
c. Incorrect. The difference between credentialed and non-credentialed scans cannot be determined by their usage of scanning tools.
d. Incorrect. Credentialed and non-credentialed scans are both authorized and legal.
POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

10. Alice, a vulnerability assessment engineer at a bank, is told to find all the vulnerabilities on an internet-facing web application server running on port HTTPS. When she finishes the vulnerability scan, she finds several different vulnerabilities at different levels. How should she proceed?

a. Only look at the highest priority vulnerability

b. Look at the priority and the accuracy of the vulnerability
c. Only look at the accuracy of the vulnerability
d. Escalate the situation to a higher analyst

ANSWER: b

FEEDBACK:

a. Incorrect. A vulnerability with high priority but low accuracy is not significant.
b. Correct. Looking at the priority and the accuracy of the vulnerability is the most appropriate approach for Alice.
c. Incorrect. Accuracy alone is not a measured parameter in judging the severity/significance of a vulnerability.
d. Incorrect. This is not the right approach in this scenario, as it will waste time during the escalation process.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

11. Which of the following is a characteristic of a vulnerability scan that is not a characteristic of a penetration test?

a. A vulnerability scan identifies deep vulnerabilities.
b. A vulnerability scan is usually automated.
c. A vulnerability scan is usually a manual process.
d. A vulnerability scan can be done when a regulatory body requires it or on a pre-determined schedule.

ANSWER: b

FEEDBACK:

a. Incorrect. A vulnerability scan does not identify deep vulnerabilities.
b. Correct. A vulnerability scan is automated, while a penetration test is performed manually.
c. Incorrect. A vulnerability scan is not a manual process.
d. Incorrect. Both vulnerability scans and penetration tests can be done when a regulatory body requires it or on a pre-determined schedule

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/17/2021 6:16 PM

Mod 02: Threat Management and Cybersecurity Resources

DATE MODIFIED: 2/17/2021 6:16 PM

12. A cyber analyst needs to quickly do a vulnerability scan on an enterprise network with many devices. Which approach should the analyst take?

a. Scan all devices, each for a very short time
b. Scan the most important devices for as long as it takes for each device
c. Scan only infrastructure devices for a very short time
d. Scan all endpoint devices

ANSWER: b

FEEDBACK:

a. Incorrect. All devices cannot be scanned quickly.
b. Correct. When there is limited time to scan a network and provide efficient and effective results, it's best to scan the most important devices, like internet-facing web, app, and DB servers, for as long as it takes for each device
c. Incorrect. All infrastructure devices cannot be scanned within a short time, and not all of them are important enough to need scanning.
d. Incorrect. Vulnerabilities on endpoint devices are not important, as they are not internet facing.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

13. A vulnerability assessment engineer performed vulnerability scanning on active directory servers and discovered that the active directory server is using a lower version of Kerberos. To alert management to the risk behind using a lower version of Kerberos, he needs to explain what an attacker can do to leverage the vulnerabilities in it. Which of the following actions can the attacker perform after exploiting vulnerabilities in Kerberos?

a. Use DLL injection
b. Use privilege escalation
c. Use a lateral movement
d. Use a vertical movement

ANSWER: b

FEEDBACK:

a. Incorrect. DLL injection is used to manipulate the execution of a running process. DLL injection primarily tricks an application into calling a malicious DLL file, which then gets executed as part of the target process. It could be used to load an advanced malware as a service.
b. Correct. After compromising a low-level user account, privilege escalation is

the only possible way to gain access to a highly privileged user, such as a domain admin or enterprise admin, so that the red teamer can do more damage to the network.

c. Incorrect. Lateral movement can be a paradigm inside privilege escalation. Red teamers can move laterally to a more important server, like the AD server, with an elevated level of access.

d. Incorrect. Vertical movement means the attack is maneuvering between different roles (client to server to a domain controller). Although privilege escalation and vertical movement sound similar, privilege escalation is a more appropriate technical approach for this.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

14. Which of the following is NOT an automated vulnerability scanning tool?

a. Nikto
b. OpenVAS
c. W3AF
d. ELK Stack

ANSWER: d
FEEDBACK:

a. Incorrect. Nikto is an open-source vulnerability scanning software that focuses on web application security. Nikto can find around 6,700 harmful files causing issues to web servers and report outdated servers-based versions.

b. Incorrect. OpenVAS is a powerful vulnerability scanning tool that supports large-scale scans. This tool finds vulnerabilities in web applications or web servers and in databases, operating systems, networks, and virtual machines.

c. Incorrect. Web application attack and framework (W3AF) is a free and open-source tool. This tool is an open-source vulnerability scanning tool for web applications.

d. Correct. ELK Stack is a data monitoring tool used as an SIEM and threat hunting solution.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM

Mod 02: Threat Management and Cybersecurity Resources

DATE MODIFIED: 2/17/2021 6:16 PM

15. What are the primary features of a security information event management (SIEM) tool?

a. Aggregation, correlation, event deduplication, time synchronization, and alerting
b. Filtering, alerting, packet dropping, packet capturing, and traffic analyzing
c. Bandwidth monitoring, alerting, and volume measuring
d. Aggregation, deep packet investigation, and policy creation

ANSWER: a

FEEDBACK:

a. Correct. Aggregation, correlation, event deduplication, time synchronization, and alerting are the important features of a SIEM tool.
b. Incorrect. Filtering, alerting, packet dropping, packet capturing, and traffic analyzing are the primary features of an IPS tool.
c. Incorrect. Bandwidth monitoring, alerting, and volume measuring are some features of a layer-3 DDOS management tool.
d. Incorrect. Aggregation, deep packet investigation, and policy creation are some features of a next-generation firewall/IPS and a web application firewall.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.4 - Describe different cybersecurity resources
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

16. What is the most accurate explanation of sentiment analysis, and what kind of a tool or product can be utilized to perform this operation?

a. Using text analysis techniques and IBM QRadar to interpret and classify emotions (positive, negative, and neutral) within text data
b. Using Cisco Firepower for computationally identifying and categorizing opinions, usually expressed in response to textual data, to determine the writer's attitude toward a particular topic
c. Using SIEM for combining many logs into one record based on IP addresses, usernames, and port numbers
d. Using Wireshark for detecting hidden and persistent threats from a network

ANSWER: a

FEEDBACK:

a. Correct. Sentiment analysis is the interpretation and classification of emotions (positive, negative, and neutral) within text data using text analysis techniques. Sentiment analysis has been used when tracking threat actor posts in discussion forums with other attackers to better determine threat actors' behaviors and mindsets. SIEM tool is used to perform this analysis.
b. Incorrect. CISCO Firepower is an IPS tool which cannot be used to perform sentiment analysis.

c. Incorrect. Combining many logs into one record based on IP addresses, usernames, and port numbers is known as "event coalescing" or "aggregation" and is used in SIEM.

d. Incorrect. Detecting hidden and persistent threats from a network is possible through "threat hunting" operations. Wireshark is a packet capture or packet forensics tool that can be used as a complementary solution while performing threat hunting.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.4 - Describe different cybersecurity resources
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

17. Which operation is carried out by proactively searching security logs for cyber threats that have thus far gone undetected.

a. Threat hunting
b. Vulnerability hunting
c. Vulnerability scanning
d. Data hunting

ANSWER: a
FEEDBACK:

a. Correct. Threat hunting is proactively searching for cyber threats that have thus far gone undetected in a network. Threat hunting begins with a critical, central premise: threat actors have already infiltrated our network.

b. Incorrect. No such term exists in information security

c. Incorrect. Vulnerability assessment/scanning is a cyclical process of ongoing scans of weaknesses/flaws in applications, services, software, frameworks, and servers, and continuously monitoring them to reduce the attack surface.

d. Incorrect. No such term exists in information security.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.4 - Describe different cybersecurity resources
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

18. Which of the following technologies can be used together for data management in security infrastructure and collecting and analyzing data.

a. SIEM and IPS
b. Firewall and IDS
c. SIEM and SOAR
d. SOAR and packet sniffer

ANSWER: c

FEEDBACK:

a. Incorrect. IPS is an active security tool that performs deep packet inspection and will drop/block and packets if they contain malicious content and then alert us.
b. Incorrect. IDS can perform deep packet inspection to detect packets with malicious contents but cannot drop/block the packet.
c. Correct. SIEM and SOAR together can be used for data management in security infrastructure and collecting and analyzing data.
d. Incorrect. A packet sniffer is used to capture network packets and perform packet forensics.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.4 - Describe different cybersecurity resources
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

19. Which of the following compliance standards was introduced to provide a minimum degree of security to organizations who handle customer information such as debit card and credit card details daily?

a. PCIDSS
b. SOX
c. FISMA
d. GLB

ANSWER: a

FEEDBACK:

a. Correct. PCIDSS was introduced to provide a minimum degree of security to organizations that handle customer information such as debit cards and credit card details daily.
b. Incorrect. The Sarbanes-Oxley Act of 2002, often simply called SOX, is a US law meant to protect investors from fraudulent accounting activities by corporations.
c. Incorrect. FISMA stands for the Federal Information Security Management Act; it requires federal agencies to implement information security plans to protect sensitive data.
d. Incorrect. The Gramm-Leach-Bliley Act requires financial institutions-companies that offer consumers financial products or services like loans, financial or investment advice, or insurance-to explain their information-sharing practices to their customers and safeguard sensitive data.

Mod 02: Threat Management and Cybersecurity Resources

POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.2.2 - Identify the rules of engagement and how to perform a pen test
ACCREDITING STANDARDS:	SY0-601.5.2 - Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture
TOPICS:	Cybersecurity Resources
KEYWORDS:	Bloom's: Remember
DATE CREATED:	2/17/2021 6:16 PM
DATE MODIFIED:	2/17/2021 6:16 PM

20. Which of the following offensive tools can be used by penetration testers post-exploitation or successful compromise of a user account in a network that dumps passwords from memory and hashes, PINs, and Kerberos tickets, and thus are used for privilege escalation attacks?

a. Mimikatz and hashcat
b. Ophcrack and John-the-Ripper
c. Powershell and procdump
d. Tor and NMAP

ANSWER: a

FEEDBACK:

a. Correct. Mimikatz and hashcat dump passwords from memory, as well as hashes, PINs, and Kerberos tickets, and thus are used for privilege escalation attacks
b. Incorrect. Ophcrack is a Windows password cracker based on Rainbow Tables, and John the Ripper is an open-source password security auditing and password recovery tool.
c. Incorrect. PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting. ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps.
d. Incorrect. Tor is free and open-source software for enabling anonymous communication by directing internet traffic through a free, worldwide, volunteer overlay network. NMAP is an active reconnaissance tool used to perform port scanning, vulnerability scanning, service scanning, OS banner grabbing, etc.

POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS:	SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS:	Penetration Testing
KEYWORDS:	Bloom's: Apply
DATE CREATED:	2/17/2021 6:16 PM
DATE MODIFIED:	2/17/2021 6:16 PM

21. Which of the following is the advantage of penetration testing over vulnerability scanning?

a. Penetration testing uncovers and exploits deep vulnerabilities, while vulnerability scanning only discovers surface vulnerabilities.
b. Penetration testing scans a network for open FTP ports to prevent penetration, while vulnerability scanning only discovers versions of the running services.
c. Penetration testing performs SYN DOS attacks towards a server in a network, while vulnerability scanning only discovers versions of the running services.
d. Penetration testing performs automated scans to discover vulnerabilities and prevent penetration, while vulnerability scanning requires manually scanning for vulnerabilities.

ANSWER: a

FEEDBACK:

a. Correct. Penetration testing attempts to uncover deep vulnerabilities and exploit them manually with the mindset of a threat actor, while vulnerability scanning is able to discover surface vulnerabilities.
b. Incorrect. Scanning a network for open FTP ports is one of the many ways of performing active reconnaissance on a network. It is not the purpose of penetration testing.
c. Incorrect. A TCP SYN flood attack occurs when an attacker floods the system with SYN requests to overwhelm the target and make it unable to respond to legitimate requests. It is not the purpose of penetration testing.
d. Incorrect. Vulnerability scanning involves automated scans used to discover vulnerabilities.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

22. Which of the following is a primary difference between a red team and a white team?

a. The red team scans for vulnerabilities and exploits them manually, whereas the white team defines the rules of the penetration testing.
b. The red team uses an automated vulnerability scanning tool to find vulnerabilities, whereas the white team defines the rules of penetration testing.
c. The red team uses an automated vulnerability scanning tool to find vulnerabilities, whereas the white team decides which tool to use in automated vulnerability scanning.
d. The red team provides real-time feedback to enhance the threat detection capability, whereas the white team defines the rules of penetration testing.

ANSWER: a

FEEDBACK:

a. Correct. Red teams perform vulnerability scanning, and white teams set the rules for penetration testing.
b. Incorrect. While red teams perform vulnerability scanning, vulnerability

scanning does not scan a network for outdated versions of services.

c. Incorrect. Red teams do not perform vulnerability scans with automated tools, nor do white teams decide which tools should be used in automated vulnerability scanning.

d. Incorrect. Red teams don't provide feedback during scanning or testing.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

23. Dillip is assigned the role of a SOC developer who must build different teams under the SOC. He must build a new team that will put security defenses in place to prevent another team from penetrating the network. Which team should he build to monitor the other team's attacks and shore up security defenses as necessary?

a. Red team
b. Blue team
c. Purple team
d. White team

ANSWER: b
FEEDBACK:

a. Incorrect. The red team scans for vulnerabilities and then exploits them.

b. Correct. The blue team monitors for red team attacks and shores up defenses as necessary.

c. Incorrect. The purple team provides real-time feedback between the red team and the blue team to enhance the testing.

d. Incorrect. The white team enforces the rules for penetration testing.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

24. Robert is a black box penetration tester who conducted pen testing attacks on all of the network's application servers. He was able to exploit a vulnerability and gain access to the system using a mimikatz tool. Which of the following activities did he perform using mimikatz, and which task should he perform next?

a. Robert used mimikatz for tailgating, and should perform phishing next.
b. Robert used mimikatz for phishing, and should perform lateral movement next.
c. Robert used mimikatz for footprinting, and should install a backdoor next.
d. Robert used mimikatz for credential harvesting, and should perform privilege escalation using a high-privileged account next.

ANSWER: d

FEEDBACK:

a. Incorrect. A tailgating attack, also known as "piggybacking," involves an attacker seeking entry to a restricted area that lacks proper authentication. Phishing is a social engineering attack that isn't used in pen testing.
b. Incorrect. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers, not access to privileges. Lateral movement can only happen when an attacker, or tester, has gained elevated privileges.
c. Incorrect. Footprinting collects as much information such as IP address, Whois records, DNS information, operating system used, employee email id, phone numbers, etc., about the target system. A backdoor cannot be installed until the attacker, or tester, has elevated privileges.
d. Correct. Mimikatz is used for credential harvesting, which will dump all the credentials stored in the OS's memory. If an account with higher privilege, such as a domain admin or an enterprise admin, is discovered, then privilege escalation is performed to gain access to the account with elevated privileges.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

25. How can a configuration review reduce the impact of a vulnerability scan on the network's overall performance?

a. It performs a fast initial scan that identifies open ports and responsive software.
b. It identifies configuration and security postures within the network.
c. It focuses the full scan by first comparing network configurations against known vulnerability databases.
d. It ensures the scan is designed to meet its intended goals by defining scope and sensitivity levels.

ANSWER: d

FEEDBACK:

a. Incorrect. Non-credentialed vulnerability scans look for open ports and software that is responsive to requests.
b. Incorrect. Credentialed vulnerability scans assess the configuration settings of installed software and the network's security posture.
c. Incorrect. Vulnerability scanning software checks known vulnerability databases, like the Mitre Common Vulnerabilities and Exposures (CVE), to

identify vulnerabilities in the network.

d. Correct. A configuration review can reduce the impact of a vulnerability scan on the network's overall performance in part because it defines a targeted group of devices to scan, ensures the scan is designed to meet its intended goals, determines the sensitivity level of the scan, and specifies the types of data that will be scanned.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

26. Which penetration testing consultants are not given any knowledge of the network nor any elevated privileges?

a. Gray box
b. White box
c. Black box
d. Bug bounty

ANSWER: c
FEEDBACK:

a. Incorrect. The gray box testers are given limited knowledge of the network and some elevated privileges.
b. Incorrect. The white box testers are given full knowledge of the network and the source code of applications.
c. Correct. The black box testers have no knowledge of the network and no special privileges.
d. Incorrect. A bug bounty is a monetary reward given for uncovering a software vulnerability. Most software developers offer some type of bug bounty, ranging from several thousands of dollars to millions of dollars.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.1 - Explain what a penetration test is
ACCREDITING STANDARDS: SY0-601.1.8 - Explain the techniques used in penetration testing.
TOPICS: Penetration Testing
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

27. Keily is a vulnerability assessment engineer. She is told to find surface vulnerabilities on all internet-facing web servers in the network. Which of the following are surface vulnerabilities that she should initially chase?

a. Missing patches, lack of OS hardening, network design flaw, lack of application hardening, weak passwords, and misconfigurations
b. Lack of OS hardening, network design flaw, lack of application hardening, weak passwords, misconfigurations, and SQL Injections
c. Lack of OS hardening, network design flaw, lack of application hardening, misconfigurations, and brute force
d. Lack of OS hardening, network design flaw, weak passwords, and misconfigurations

ANSWER: a

FEEDBACK:

a. Correct. Missing patches, lack of OS hardening, network design flaw, lack of application hardening, weak passwords, and misconfigurations are the low hanging fruits (vulnerabilities, in context) that Keily should chase first.
b. Incorrect. SQL injection is not a low hanging fruit (vulnerabilities, in context) that Keily should chase first.
c. Incorrect. Brute force is not a low hanging fruit (vulnerabilities, in context) that Keily should chase first.
d. Incorrect. While these are all vulnerabilities that Keily should chase first, she should also look for missing patches.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

28. What is the fastest-running vulnerability scan, and why does this type of scan run so fast?

a. Intrusive scans can provide a deeper insight into the system by accessing the installed software by examining the software's configuration settings and current security posture.
b. Credentialed scans perform fundamental actions such as looking for open ports and finding software that will respond to requests.
c. Non-credentialed scans perform fundamental actions such as looking for open ports and finding software that will respond to requests.
d. Non-intrusive scans find deep vulnerabilities that would have otherwise gone unnoticed.

ANSWER: c

FEEDBACK:

a. Incorrect. An intrusive scan just like a threat actor will attempt to employ any vulnerabilities that it finds, and it is not related to the speed of scanning.
b. Incorrect. Credentialed scans are slower but can provide a deeper insight into the system by accessing a wider range of installed software and examine the software's configuration settings and current security posture.
c. Correct. Non-credentialed scans run faster because they perform fundamental actions such as looking for open ports and finding software that will respond to requests.

d. Incorrect. A non-intrusive scan does not attempt to exploit the vulnerability but only records that it was discovered. It is also not related to the speed of scanning.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.3 - Define Vulnerability Scanning
ACCREDITING STANDARDS: SY0-601.1.7 - Summarize the techniques used in security assessments.
TOPICS: Vulnerability Scanning
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

29. Which standardized framework was developed by NIST to be used as a guidance document designed to help organizations assess and manage risks to their information and systems, and are also used as a comprehensive roadmap that organizations can use to seamlessly integrate their cybersecurity?

a. Risk management framework (RMF)
b. Cybersecurity framework (CSF)
c. ISO 27001
d. CIS Controls

ANSWER: a
FEEDBACK:

a. Correct. NIST's risk management framework (RMF) is considered a guidance document designed to help organizations assess and manage risks to their information and systems. It is viewed as a comprehensive roadmap for organizations to seamlessly integrate their cybersecurity, privacy, and supply chain risk management processes.
b. Incorrect. NIST's cybersecurity framework (CSF) is used as a measuring stick for companies to use to compare their cybersecurity practices against the threats they face.
c. Incorrect. ISO 27001 provides requirements for an information security management system.
d. Incorrect. CIS Controls consist of more than 20 basic and advanced cybersecurity recommendations made by the Center for Internet Security (CIS).

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.4 - Describe different cybersecurity resources
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Cybersecurity Resources
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM

Mod 02: Threat Management and Cybersecurity Resources

30. Which of the following is considered an industry-specific cybersecurity regulation?

a. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
b. Sarbanes-Oxley Act of 2002 (SOX)
c. Personal Information Protection and Electronic Documents Act (PIPEDA)
d. Gramm-Leach-Bliley Act (GLB)

ANSWER: a

FEEDBACK:

a. Correct. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains regulations protecting the privacy and security of certain personal health information (PHI).
b. Incorrect. The Sarbanes-Oxley Act of 2002 (SOX) is a broadly applicable regulation that protects investors from fraudulent accounting activities by corporations.
c. Incorrect. The Personal Information Protection and Electronic Documents Act (PIPEDA) is an international regulation that protects the personal information of Canadian citizens.
d. Incorrect. The Gramm-Leach-Bliley Act (GLB) is a broadly applicable regulation that mandates that companies that offer consumers financial products or services, financial or investment advice, or insurance, explain their information-sharing practices to their customers and also ensure that sensitive data is safeguarded.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.2.2 - Identify the rules of engagement and how to perform a pen test
ACCREDITING STANDARDS: SY0-601.5.2 - Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture
TOPICS: Cybersecurity Resources
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/17/2021 6:16 PM
DATE MODIFIED: 2/17/2021 6:16 PM