1.

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

Which of the following tools is employed by Clark to create the spoofed email?

PyLoris

PLCinject

Slowloris

Evilginx

2.

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-4: Orchestrators

Tier-1: Developer machines

Tier-3: Registries

Tier-2: Testing and accreditation systems

3.

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

An intruder’s malware is installed on a target’s machine.

An intruder creates malware to be used as a malicious attachment to an email.

An intruder’s malware is triggered when a target opens a malicious email attachment.

An intruder sends a malicious attachment via email to a target.

4.

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.

128

255

64

138

5.

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?

TCP Maimon scan

UDP scan

ACK flag probe scan

ARP ping scan

6.

What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

The internal command RCPT provides a list of ports open to message traffic.

The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.

A list of all mail proxy server addresses used by the targeted host

Reveals the daily outgoing message limits before mailboxes are locked

7.

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

Which of the following attack techniques is used by Stella to compromise the web services?

SOAPAction spoofing

XML injection

WS-Address spoofing

Web services parsing attacks

8.

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 × 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key (Km1) and a rotation key (Kr1) for performing its functions.

What is the algorithm employed by Harper to secure the email messages?

GOST block cipher

AES

DES

CAST-128

9.

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization’s web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks.

Which of the following security scanners will help John perform the above task?

Cisco ASA

AlienVault® OSSIM™

Syhunt Hybrid

Saleae Logic Analyzer

10.

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

Cloud cryptojacking

Metadata spoofing attack

Cloudborne attack

Man-in-the-cloud (MITC) attack

11.

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

Key derivation function

Key stretching

Public key infrastructure

Key reinstallation

12.

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

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

Denial-of-service attack

Buffer overflow attack

Side-channel attack

HMI-based attack

13.

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes.

Which type of attack can she implement in order to continue?

Pass the hash

Pass the ticket

LLMNR/NBT-NS poisoning

Internal monologue attack

14.

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?

ARP spoofing attack

VLAN hopping attack

DNS poisoning attack

STP attack

15.

Mirai malware targets IoT devices. After infiltration, it uses them to propagate and create botnets that are then used to launch which types of attack?

DDoS attack

Password attack

MITM attack

Birthday attack

16.

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

Permutation scanning technique

Topological scanning technique

Subnet scanning technique

17.

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

nmap -sT -O -T0

nmap -sP -p-65535 -T5

nmap -A --host-timeout 99 -T1

nmap -A – Pn

18.

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

Evil-twin attack

War driving attack

Phishing attack

MAC spoofing attack

19.

Kate dropped her phone and subsequently encountered an issue with the phone’s internal speaker. Thus, she is using the phone’s loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate’s phone so that he can monitor the loudspeaker’s output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy.

What is the type of attack Bob performed on Kate in the above scenario?

aLTEr attack

Spearphone attack

Man-in-the-disk attack

SIM card attack

20.

Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim’s system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components.

What is the attack technique used by Stephen to damage the industrial systems?

Reconnaissance attack

HMI-based attack

Spear-phishing attack

SMishing attack

21.

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

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

Operational threat intelligence

Tactical threat intelligence

Strategic threat intelligence

Technical threat intelligence

22.

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

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

SMTP

GPG

S/MIME

PGP

23.

Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

Rootkit

Worm

Trojan

Adware

24.

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

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

Virtual machine

Serverless computing

Zero trust network

Docker

25.

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

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

Azure IoT Central

IoTSeeker

IoT Inspector

AT&T IoT Platform

26.

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

Which of the following tools is used by Jack to perform vulnerability scanning?

Infoga

NCollector Studio

Netsparker

WebCopier Pro

27.

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?

Maintaining access

Scanning

Gaining acces

Reconnaissance

28.

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

Evil twin attack

MAC flooding

DNS cache flooding

DDoS attack

29.

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

keylogrecorder

getsystem

autoroute

getuid

30.

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.

Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

net view

macof

wash

ntptrace

31.

Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files.

What is the type of injection attack Calvin’s web application is susceptible to?

Server-side template injection

Server-side includes injection

CRLF injection

Server-side JS injection

32.

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

Wardriving

GPS mapping

Spectrum analysis

Wireless sniffing

33.

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?

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

Retain all unused modules and application extensions

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

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

34.

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory.

What is this mechanism called in cryptography?

Key escrow

Key archival

Certificate rollover

Key renewal

35.

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

Incident recording and assignment

Preparation

Eradication

36.

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

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

App sandboxing

Social engineering

Reverse engineering

Jailbreaking

37.

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

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

WPA3

WPA

WPA2

WEP

38.

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 daemon

Docker registries

Docker client

Docker objects

39.

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?

KRACK

Wardriving

Evil twin

Chop chop attack

40.

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?

Host-based assessment

Database assessment

Distributed assessment

Credentialed assessment

41.

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

What is the best example of a scareware attack?

A banner appears to a user stating, “Your account has been locked. Click here to reset your password and unlock your account.”

A pop-up appears to a user stating, “Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue.”

A pop-up appears to a user stating, “You have won a free cruise! Click here to claim your prize!”

A banner appears to a user stating, “Your Amazon order has been delayed. Click here to find out your new delivery date.”

42.

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company.

What is the API vulnerability revealed in the above scenario?

Improper use of CORS

No ABAC validation

Business logic flaws

Code injections

43.

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

What is the tool used by Hailey for gathering a list of words from the target website?

Shadowsocks

Psiphon

CeWL

Orbot

44.

What would be the purpose of running “wget 192.168.0.15 -q -S” against a web server?

Flooding the web server with requests to perform a DoS attack

Performing content enumeration on the web server to discover hidden folders

Downloading all the contents of the web page locally for further examination

Using wget to perform banner grabbing on the webserver

45.

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.

Which of the following techniques is employed by Dayn to detect honeypots?

Detecting the presence of Honeyd honeypots

Detecting the presence of Sebek-based honeypots

Detecting the presence of Snort\_inline honeypots

Detecting honeypots running on VMware

46.

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

Which service is this and how can you tackle the problem?

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

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

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

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

47.

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?

FTP

IP

FTPS

HTTPS

48.

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

Investigation

Exploration

Enumeration

Reconnaissance

49.

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

What is the technique used by Jack to launch the fileless malware on the target systems?

Phishing

Legitimate applications

In-memory exploits

Script-based injection

50.

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

What is the character?

Tilde (~)

Period (.)

Exclamation mark (!)

Underscore (\_)

51.

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

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

-PP

-Pn

–PY

-PU

52.

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

<!DOCTYPE blah [ < !ENTITY trustme SYSTEM "file:///etc/passwd" > ] >

SQLi

IDOR

XXS

XXE

53.

Which Nmap switch helps evade IDS or firewalls?

-oN/-oX/-oG

-T

-n/-R

-D

54.

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 the answers to his security questions when responding to the post.

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.

55.

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

Which of the following tools was employed by Lewis in the above scenario?

Wapiti

Censys

Lacework

NeuVector

56.

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

VoIP footprinting

Dark web footprinting

VPN footprinting

Website footprinting

57.

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

58.

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.

What is the framework used by James to conduct footprinting and reconnaissance activities?

Browser Exploitation Framework

OSINT framework

SpeedPhish Framework

WebSploit Framework

59.

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?

[allinurl:]

[link:]

[location:]

[site:]

60.

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?

Phlashing

Session splicing

Desynchronization

Slowloris attack

61.

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

Enumeration

Vulnerability analysis

Scanning networks

Malware analysis

62.

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?

Credentialed assessment

Internal assessment

Passive assessment

External assessment

63.

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

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

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

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

64.

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

What is the technique employed by Eric to secure cloud resources?

Zero trust network

Container technology

Demilitarized zone

Serverless computing

65.

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, a

lso causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

Frequency/voltage tampering

Power/clock/reset glitching

Temperature attack

Optical, electromagnetic fault injection (EMFI)

66.

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

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

Nmap

Wireshark

Burp Suite

CxSAST

67.

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 –PS < target IP address >

nmap –sn –PO < target IP address >

nmap –sn –PA < target IP address >

nmap –sn –PP < target IP address >

68.

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

Which of the following techniques is used by Joel in the above scenario?

Clickjacking attack

Watering hole attack

DNS rebinding attack

MarioNet attack

69.

Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization’s network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.

Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

<00>

<20>

<03>

<1B>

70.

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

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

Reverse image search

Google advanced search

Meta search engines

Advanced image search

71.

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

Which of the following design flaws in the authentication mechanism is exploited by Calvin?

Insecure transmission of credentials

Password reset mechanism

User impersonation

Verbose failure messages

72.

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?

Cleanup

Initial intrusion

Persistence

Preparation

73.

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

Bug bounty program

White-hat hacking program

Ethical hacking program

Vulnerability hunting program

74.

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

Risk assessment

Remediation

Vulnerability scan

75.

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

Boolean-based blind SQL injection

Blind SQL injection

Union SQL injection

Error-based injection

76.

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64

Window Size: 5840

What is the OS running on the target machine?

Linux OS

Windows OS

Mac OS

Solaris OS

77.

Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company’s IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.

What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

Implement cognitive radios in the physical layer

Disable TCP SYN cookie protection

Allow the transmission of all types of addressed packets at the ISP level

Allow the usage of functions such as gets and strcpy

78.

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

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

Operational threat intelligence

Tactical threat intelligence

Technical threat intelligence

Strategic threat intelligence

79.

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

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

Serpent

RC5

TEA

CAST-128

80.

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?

DoS attack

DHCP spoofing

ARP cache poisoning

DNS hijacking

81.

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

What is the defensive technique employed by Bob in the above scenario?

Enforce least privileges

Output encoding

Whitelist validation

Blacklist validation

82.

What is the following command used for?

sqlmap.py -u "http://10.10.1.20/?p=1&forumaction=search" –dbs

Creating backdoors using SQL injection

Enumerating the databases in the DBMS for the URL

Searching database statements at the IP address given

Retrieving SQL statements being executed on the database

83.

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

You cannot identify such an attack and must use a VPN to protect your traffic.

You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.

You should check your ARP table and see if there is one IP address with two different MAC addresses.

You should use netstat to check for any suspicious connections with another IP address within the LAN.

84.

select

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?

-sS

-sV

-Pn

-V

85.

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

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

btlejack -f 0x129f3244 -j

btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

btlejack -f 0x9c68fd30 -t -m 0x1fffffffff

btlejack -c any

86.

Which of the following tactics uses malicious code to redirect users’ web traffic?

Phishing

Pharming

Spear-phishing

Spimming

87.

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system.

What is the first step that the bank should take before enabling the audit feature?

Perform a vulnerability scan of the system

Perform a cost/benefit analysis of the audit feature

Allocate funds for staffing of audit log review

Determine the impact of enabling the audit feature

88.

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

Unspecified proxy activities

Use of DNS tunneling

Use of command-line interface

Data staging

89.

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?

Service-based solutions

Product-based solutions

Inference-based assessment

Tree-based assessment

90.

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

[inurl:]

[site:]

[info:]

[related:]

91.

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

Which regional Internet registry should Becky go to for detailed information?

RIPE

APNIC

ARIN

LACNIC

92.

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

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

Zero trust network

Transport Layer Security (TLS)

Web of trust (WOT)

Secure Socket Layer (SSL)

93.

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

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

Outlook scraper

Credential enumerator

NetPass.exe

WebBrowserPassView

94.

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

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

WS-Security

WSDL

WS-Policy

WS-Work Processes

95.

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

What is the enumeration technique used by Henry on the organization?

DNSSEC zone walking

DNS zone walking

DNS cache poisoning

DNS cache snooping

96.

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

SSO

RADIUS

WPA

NTLM

97.

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

What type of attack is this?

Error-based SQL injection

Time-based SQL injection

Blind SQL injection

Union SQL injection

98.

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

MIB\_II.MIB

WINS.MIB

DHCP.MIB

99.

Jude, a pen tester, examined a network from a hacker’s perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.

What is the type of vulnerability assessment that Jude performed on the organization?

Passive assessment

External assessment

Application assessment

Host-based assessment

100.

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

4.0–6.9

4.0–6.0

3.9–6.9

3.0–6.9

101.

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

Cloud carrier

Cloud broker

Cloud connector

Cloud provider

102.

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

Which information security standard is most applicable to his role?

Sarbanes–Oxley Act

FISMA

HITECH

PCI-DSS

103.

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?

Host-based assessment

Wireless network assessment

Distributed assessment

Application assessment

104.

Miley, a professional hacker, decided to attack a target organization’s network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system’s IP address. By performing this, Miley received messages directed to the victim’s MAC address and further used the tool to intercept, steal, modify, and block sensitive communication to the target system.

What is the tool employed by Miley to perform the above attack?

DerpNSpoof

BetterCAP

Gobbler

Wireshark

105.

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

1)    Remediation

2)    Identify assets and create a baseline

3)    Verification

4)    Monitor

5)    Vulnerability scan

6)    Risk assessment

Identify the correct sequence of steps involved in vulnerability management.

2-->5-->6-->1-->3-->4

1-->2-->3-->4-->5-->6

2-->1-->5-->6-->4-->3

2-->4-->5-->3-->6-->1

106.

George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities.

Which of the following anonymizers helps George hide his activities?

http://karmadecay.com

https://www.baidu.com

https://www.wolframalpha.com

http://www.guardster.com

107.

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

What is the type of attack performed by Simon?

Rainbow table attack

Internal monologue attack

Combinator attack

Dictionary attack

108.

Which is the first step followed by Vulnerability Scanners for scanning a network?

Firewall detection

Checking if the remote host is alive

TCP / UDP Port scanning

OS Detection

109.

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

ZigBee

WPA3-Personal

Bluetooth

WPA2-Enterprise

110.

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

PCI-DSS

ISO/IEC 27001:2013

SOX

FISMA

111.

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

What is the attack technique used by Jude for finding loopholes in the above scenario?

Spoofed session flood attack

UDP flood attack

Peer-to-peer attack

Ping-of-death attack

112.

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

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

Etcd cluster

Kube-scheduler

Kube-apiserver

Kube-controller-manager

113.

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

-sF

-sA

-sT

-sX

114.

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 hefound on the Internet. He

What type of attack is Ricardo performing?

Known plaintext

Dictionary

Brute force

Password spraying

115.

When considering how an attacker may exploit a web server, what is web server footprinting?

When an attacker creates a complete profile of the site’s external links and file structures

When an attacker uses a brute-force attack to crack a web-server password

When an attacker gathers system-level data, including account details and server names

When an attacker implements a vulnerability scanner to identify weaknesses

116.

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?

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

RPC and the best practice is to disable RPC completely

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

SNMP and he should change it to SNMP V3

117.

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

EXPN

CHK

RCPT

VRFY

118.

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?

Secure development lifecycle

Patch management

Security awareness training

Vendor risk management

119.

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

What is the attack performed in the above scenario?

Timing-based attack

Side-channel attack

Cache-based attack

Downgrade security attack

120.

Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.

Which of the following tools would not be useful for cracking the hashed passwords?

John the Ripper

Hashcat

THC-Hydra

netcat

121.

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user’s activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages.

What is the type of spyware that Jake used to infect the target device?

Androrat

Zscaler

DroidSheep

Trident

122.

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

Check MITRE.org for the latest list of CVE findings

Create a disk image of a clean Windows installation

Use the built-in Windows Update tool

Use a scan tool like Nessus

123.

A “Server-Side Includes” attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

.cms

.rss

.html

.stm

124.

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 private key; Alice’s public key

Bryan’s public key; Alice’s public key

Alice’s public key; Alice’s public key

Bryan’s public key; Bryan’s public key

125.

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?

ZoomInfo

Factiva

Netcraft

Infoga