Version: 8.4

Question: 1

The configuration allows a wired or wireless network interface controller to pass all trafice 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. WEM
B. Multi-cast mode
C. Promiscuous mode
D. Port forwarding

Answer: B

Question: 2

In Risk Management, how is the term “likelihood” related to the concept of “threat?”

A. Likelihood is the probability that a vulnerability is a threat-source.
B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.
D. Likelihood is the probability that a threat-source will exploit a vulnerability.

Answer: D

Question: 3

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. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Web form input validation
D. Clickjacking

Answer: A

Question: 4

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

A. Verity access right before allowing access to protected information and UI controls
B. Use security policies and procedures to define and implement proper security settings

C. Validate and escape all information sent over to a server
D. Use digital certificates to authenticate a server prior to sending data

Answer: A

Question: 5

An incident investigator asks to receive a copy of the event from all firewalls, prosy 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. The security breach was a false positive.
C. The attack altered or erased events from the logs.
D. Proper chain of custody was not observed while collecting the logs.

Answer: C

Question: 6

This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. Wificracker
B. WLAN-crack
C. Airguard
D. Aircrack-ng

Answer: D

Question: 7

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. Nessus
B. Tcptraceroute
C. Tcptrace
D. OpenVAS

Answer: C

Question: 8

You have compromised a server on a network and successfully open a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the 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 xxxxxxxxxx.
QUITTING!
```

What seems to be wrong?

A. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
B. This is a common behavior for a corrupted nmap application.
C. OS Scan requires root privileged.
D. The nmap syntax is wrong.

Answer: D

Question: 9

Which of the following is the greatest threat posed by backups?

A. An un-encrypted backup can be misplaced or stolen
B. A back is incomplete because no verification was performed.
C. A backup is the source of Malware or illicit information.
D. A backup is unavailable during disaster recovery.

Answer: A

Question: 10

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, that the user is directed to a phishing site.
Which file does the attacker need to modify?

A. Hosts
B. Networks
C. Boot.ini
D. Sudoers

Answer: A