Open book Chapter review (17 questions) - Quiz One

1. A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

A. Domain reputation

B. Domain hijacking

C. Disassociation

D. DNS poisoning

2. A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

Click here to unsubscribe

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection

B. Broken authentication

C. XSS

D. XSRF

3. A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

   A. Hoaxes

   B. SPIMs

   C. Identity fraud

   D. Credential harvesting

4. A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded. However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

   A. DNS poisoning

   B. MAC flooding

   C. DDoS attack

   D. ARP poisoning

5. Which of the following is the MOST effective control against zero-day vulnerabilities?

   A. Network segmentation

   B. Patch management

   C. Intrusion prevention system

   D. Multiple vulnerability scanners

6. An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup, but every time the Chief Financial Officer logs in to the file server, the same files are deleted again. No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

   A. Logic bomb

   B. Cryptomalware

   C. Spyware

   D. Remote access Trojan

7. Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:

☞ All users share workstations throughout the day.

☞ Endpoint protection was disabled on several workstations throughout the network.

☞ Travel times on logins from the affected users are impossible.

☞ Sensitive data is being uploaded to external sites.

All user account passwords were forced to be reset and the issue continued. Which of the following attacks is being used to compromise the user accounts?

A. Brute-force

B. Keylogger

C. Dictionary

D. Rainbow

8. A security analyst is designing the appropriate controls to limit unauthorized access to a physical site. The analyst has a directive to utilize the lowest possible budget. Which of the following would BEST meet the requirements?

A. Preventive controls

B. Compensating controls

C. Deterrent controls

D. Detective controls

9. A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

A. XSS attack

B. SQLi attack

C. Replay attack

D. XSRF attack

10. A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A

security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data loss?

A. Logic bomb

B. Ransomware

C. Fileless virus

D. Remote access Trojans

E. Rootkit

11. A technician enables full disk encryption on a laptop that will be taken on a business trip. Which of the following does this process BEST protect?

A. Data in transit

B. Data in processing

C. Data at rest

D. Data tokenization

Answer questions from 12 to 14 based on the following scenario.

instruction: label uppercase letters in ascending order for attack identified column and assign: lower case letters in ascending order for Best preventive column so your answer should something like (A:c, B: a etc.

12. Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

Hot Area:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

13. Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

14. Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

15. A user's account is constantly being locked out. Upon further review, a security analyst found the following in the SIEM:

Time	Log Message	
9:00:00 AM	login: user	password: aBG23TMV
9:00:01 AM	login: user	password: aBG33TMV
9:00:02 AM	login: user	password: aBG43TMV
9:00:03 AM	login: user	password: aBG53TMV

Which of the following describes what is occurring?

A. An attacker is utilizing a password-spraying attack against the account.

B. An attacker is utilizing a dictionary attack against the account.

C. An attacker is utilizing a brute-force attack against the account.

D. An attacker is utilizing a rainbow table attack against the account.

16. An analyst receives multiple alerts for beaconing activity for a host on the network. After analyzing the activity, the analyst observes the following activity:

* A user enters hilcoe.net into a web browser.

* The website that appears is not the hilcoe.net site.

* The website is a malicious site from the attacker.

* Users in a different office are not having this issue.

Which of the following types of attacks was observed?

A. On-path attack

B. DNS poisoning

C. Locator (URL) redirection

D. Domain hijacking

17. A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?

A. On-path

B. Evil twin

C. Jamming

D. Rogue access point

E. Disassociation