Vendor: CompTIA

Exam Code:CS0-001

Exam Name: CompTIA Cybersecurity Analyst

Version: Demo

QUESTION 1

Which of the following describes why it is important for an organization\\'s incident response team and legal department to meet and discuss communication processes during the incident response process?

A. To comply with existing organization policies and procedures on interacting with internal and external parties

B. To ensure all parties know their roles and effective lines of communication are established

C. To identify which group will communicate details to law enforcement in the event of a security incident

D. To predetermine what details should or should not be shared with internal or external parties in the event of an incident

Correct Answer: A

QUESTION 2

A vulnerability scan came back with critical findings for a Microsoft SharePoint server:

```
Vulnerable Software installed: Office 2007
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-S-18\Products\000021096F0100000100000000F01FEC\InstallProperties - key
exists The Office component Microsoft Office Excel Services Web Front End
Components is running an affected version - 12.0.6612.1000
```

Which of the following actions should be taken?

A. Remove Microsoft Office from the server.

B. Document the finding as an exception.

C. Install a newer version of Microsoft Office on the server.

D. Patch Microsoft Office on the server.

Correct Answer: D

QUESTION 3

A threat intelligence analyst who works for a financial services firm received this report:

"There has been an effective waterhole campaign residing at www.bankfinancecompsoftware.com. This domain is delivering ransomware. This ransomware variant has been called "LockMaster" by researchers due to its ability to overwrite the MBR, but this term is not a malware signature. Please execute a defensive operation regarding this attack vector."

The analyst ran a query and has assessed that this traffic has been seen on the network. Which of the following actions

should the analyst do NEXT? (Select TWO).

A. Advise the firewall engineer to implement a block on the domain

B. Visit the domain and begin a threat assessment

C. Produce a threat intelligence message to be disseminated to the company

D. Advise the security architects to enable full-disk encryption to protect the MBR

E. Advise the security analysts to add an alert in the SIEM on the string "LockMaster"

F. Format the MBR as a precaution

Correct Answer: BD

QUESTION 4

A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.

B. The corporate network should have a wireless infrastructure that uses open authentication standards.

C. Guests using the wireless network should provide valid identification when registering their wireless devices.

D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

Correct Answer: C

QUESTION 5

A Chief Information Security Officer (CISO) needs to ensure that a laptop image remains unchanged and can be verified before authorizing the deployment of the image to 4000 laptops. Which of the following tools would be appropriate to use in this case?

A. MSBA

B. SHA1sum

C. FIM

D. DLP

Correct Answer: B

QUESTION 6

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.

During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access

B. Spoofing

C. Man-in-the-middle

D. Replay

Correct Answer: C

QUESTION 7

Company A suspects an employee has been exfiltrating PII via a USB thumb drive. An analyst is tasked with attempting to locate the information on the drive. The PII in question includes the following:

comp@mail.com	564-23-4765
tia@mail.com	754-09-3276
puter@mail.com	143-32-2323
sam@mail.com	545-11-0192
jim@mail.com	093-45-3748

Which of the following would BEST accomplish the task assigned to the analyst?

A. 3 [0-9]\d-2[0-9]\d-4[0-9]\d

B. \d(3)-d(2)-\d(4)

C. ?[3]-?[2]-?[3]

D. \d[9] `XXX-XX-XX\\'

Correct Answer: B

QUESTION 8

The Chief Security Officer (CSO) has requested a vulnerability report of systems on the domain, identifying those running outdated OSs. The automated scan reports are not displaying OS version details, so the CSO cannot determine risk exposure levels from vulnerable systems. Which of the following should the cybersecurity analyst do to enumerate OS information as part of the vulnerability scanning process in the MOST efficient manner?

A. Execute the ver command

B. Execute the nmap -p command

C. Use Wireshark to export a list

D. Use credentialed configuration

Correct Answer: A

QUESTION 9

A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

A. The security analyst should recommend this device be placed behind a WAF.

B. The security analyst should recommend an IDS be placed on the network segment.

C. The security analyst should recommend this device regularly export the web logs to a SIEM system.

D. The security analyst should recommend this device be included in regular vulnerability scans.

Correct Answer: A

QUESTION 10

Weeks before a proposed merger is scheduled for completion, a security analyst has noticed unusual traffic patterns on a file server that contains financial information. Routine scans are not detecting the signature of any known exploits or malware. The following entry is seen in the ftp server logs:

tftp –I 10.1.1.1 GET fourthquarterreport.xls

Which of the following is the BEST course of action?

A. Continue to monitor the situation using tools to scan for known exploits.

B. Implement an ACL on the perimeter firewall to prevent data exfiltration.

C. Follow the incident response procedure associate with the loss of business critical data.

D. Determine if any credit card information is contained on the server containing the financials.

Correct Answer: C

QUESTION 11

A security analyst has been asked to scan a subnet. During the scan, the following output was generated:

```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT        STATE              SERVICE
22/tcp      open               ssh
53/tcp      open               domain
111/tcp     open               rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT        STATE              SERVICE
22/tcp      open               ssh
80/tcp      open               http
111/tcp     open               rpcbind
443/tcp     open               ssl/http

Nmap finished: 256 IP addresses (2 hosts up) scanned in 7.223 seconds
```


Based on the output above, which of the following is MOST likely?

A. 192.168.100.214 is a secure FTP server

B. 192.168.100.214 is a web server

C. Both hosts are mail servers

D. 192.168.100.145 is a DNS server

Correct Answer: B

QUESTION 12

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client\\'s company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

A. Enumeration and OS fingerprinting

B. Email harvesting and host scanning

C. Social media profiling and phishing

D. Network and host scanning

Correct Answer: C

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: