D. Technical

Correct Answer: A

QUESTION 47
A company uses wireless tor all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard
B. WPA-EAP
C. IP filtering
D. A WIDS

Correct Answer: B
Explanation:
"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism." https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010.

https://jaimelightfoot.com/blog/comptia-security-wireless-security/ "EAP has been expanded into multiple versions."

- "The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3."
- "The Wi-Fi Alliance added EAP-FAST to its list of supported protocols for WPA/WPA2/WPA3."
- "The Wi-Fi Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3."

QUESTION 48
An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering it the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

A. Disallow new hires from using mobile devices for six months
B. Select four devices for the sales department to use in a CYOD model
C. Implement BYOD for the sates department while leveraging the MDM
D. Deploy mobile devices using the COPE methodology

Correct Answer: C

QUESTION 49
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

Correct Answer: AC
Explanation:
heat map and site survey will provide the wifi strength and identify the weakness areas..this will give the opportunity if we need to increase WiFI strength or give suggestion to the forklift drivers about the movement

QUESTION 50
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

Correct Answer: C

QUESTION 51
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A. http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
B. http://sample.url.com/someotherpageonsite/../../../etc/shadow
C. http://sample.url.com/select-from-database-where-password-null
D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect

Correct Answer: B

QUESTION 52
A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

A. Due to foreign travel, the user's laptop was isolated from the network.
B. The user's laptop was quarantined because it missed the latest path update.
C. The VPN client was blacklisted.
D. The user's account was put on a legal hold.

Correct Answer: A

QUESTION 53
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

Correct Answer: A

QUESTION 54
An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

A. NGFW
B. Pagefile
C. NetFlow
D. RAM

Correct Answer: B

QUESTION 55
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

Correct Answer: A

QUESTION 56
During an incident response, a security analyst observes the following log entry on the web server. Which of the following BEST describes the type of attack the analyst is experience?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

Correct Answer: D

QUESTION 57
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement
B. Least privilege
C. An acceptable use policy
D. Ofboarding

Correct Answer: D

QUESTION 58
A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting
B. Keylogger
C. Brute-force
D. Spraying

Correct Answer: D
Explanation:
If a user tries to authenticate with a wrong password, the domain controller who handles the authentication request will increment an attribute called badPwdCount. As you can see in the image, the badpwdcount attribute for the user states that many passwords were used to try to log in without success. Password spraying is an attack that attempts to access a large number of accounts (usernames) with a few commonly used passwords.
https://www.coalfire.com/the-coalfire-blog/march-2019/password-spraying-what-to-do-and-how-to-avoid-it

https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

QUESTION 59
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. IaaS
D. DaaS

Correct Answer: C

QUESTION 60
A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboars are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Loss of proprietary information
B. Damage to the company's reputation
C. Social engineering
D. Credential exposure

Correct Answer: A
Explanation:
In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

QUESTION 61
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Correct Answer: C

QUESTION 62
In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Correct Answer: E