QUESTION 82
A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

A. Man-in- the middle
B. Spear-phishing
C. Evil twin
D. DNS poising

Correct Answer: D
Explanation:
DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).
https://en.wikipedia.org/wiki/DNS_spoofing

QUESTION 83
Which of the following describes the ability of code to target a hypervisor from inside

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Correct Answer: B
Explanation:
Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor.

https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs)%20running%20on%20that%20host.

QUESTION 84
A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

- www.company.com (main website)
- contactus.company.com (for locating a nearby location)
- quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

A. SAN
B. Wildcard
C. Extended validation
D. Self-signed

Correct Answer: B

QUESTION 85
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

Correct Answer: DF

QUESTION 86
A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time In the event of a failure, which being maindful of the limited available storage space?

A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
B. Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
C. Implement nightly full backups every Sunday at 8:00 p.m
D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00

Correct Answer: B

QUESTION 87
A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth
B. SSO
C. SAML
D. PAP

Correct Answer: C

QUESTION 88
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

Correct Answer: C

QUESTION 89
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system
D. An OpenID Connect authentication system

Correct Answer: D

QUESTION 90
Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team
B. While team
C. Blue team
D. Purple team

Correct Answer: A
Explanation:
Red team-performs the offensive role to try to infiltrate the target.

QUESTION 91
A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

A. Unsecme protocols
B. Default settings
C. Open permissions
D. Weak encryption

Correct Answer: D

QUESTION 92
Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

Correct Answer: B
Explanation:
"Blockchain technology has a variety of potential applications. It can ensure the integrity and transparency of financial transactions, online voting systems, identity management systems, notarization, data storage, and more."

QUESTION 93
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Correct Answer: BD

QUESTION 94
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us

Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Correct Answer: D

QUESTION 95
A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

A. DNS sinkholding
B. DLP rules on the terminal
C. An IP blacklist

D. Application whitelisting

Correct Answer: D

QUESTION 96
A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

Correct Answer: D

QUESTION 97
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

A. A firewall
B. A device pin
C. A USB data blocker
D. Biometrics

Correct Answer: C

QUESTION 98
HOTSPOT
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS
Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.