CompTIA Security+ 2023

1. Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A. Hacktivist

B. Whistleblower

C. Organized crime

D. Unskilled attacker

Answer(s): C

---

2. Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching

B. Data masking

C. Steganography

D. Salting

Answer(s): D

---

3. An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation

B. Pretexting

C. Typosquatting

D. Phishing

Answer(s): D

---

4. An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25.
Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53

B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Answer(s): D

---

5. A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications.
Which of the following methods would allow this functionality?

A. SSO

B. LEAP

C. MFA

D. PEAP

Answer(s): A

---

6. Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.

B. Employees who open an email attachment receive messages demanding payment in order to access files.

C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.

D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Answer(s): A

---

7. A company prevented direct access from the database administrators' workstations to the network segment that contains database servers.
Which of the following should a database administrator use to access the database servers?

A. Jump server

B. RADIUS

C. HSM

D. Load balancer

Answer(s): A

---

8. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow.
Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW

B. WAF

C. TLS

D. SD-WAN

Answer(s): B

---

9. An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords.
Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication

B. Permissions assignment

C. Access management

D. Password complexity

Answer(s): A

---

10. An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification.
Which of the following social engineering techniques are being attempted? (Choose two.)

- [ ] A. Typosquatting
- [ ] B. Phishing
- [ ] C. Impersonation
- [ ] D. Vishing
- [ ] E. Smishing
- [ ] F. Misinformation

Answer(s): C E

---

11. Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:
"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."
Which of the following are the best responses to this situation? (Choose two).

- [ ] A. Cancel current employee recognition gift cards.
- [ ] B. Add a smishing exercise to the annual company training.
- [ ] C. Issue a general email warning to the company.
- [ ] D. Have the CEO change phone numbers.
- [ ] E. Conduct a forensic investigation on the CEO's phone.
- [ ] F. Implement mobile device management.

Answer(s): B C

---

12. A company is required to use certified hardware when building networks.
Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain

B. A legally enforceable corporate acquisition policy

C. A right to audit clause in vendor contracts and SOWs

D. An in-depth penetration test of all suppliers and vendors

Answer(s): A

---

13. Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement

B. Supply chain analysis

C. Right to audit clause

D. Due diligence

Answer(s): A

---

14. A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement.
Which of the following reconnaissance types is the tester performing?

A. Active

B. Passive

C. Defensive

D. Offensive

Answer(s): A

15. Which of the following is required for an organization to properly manage its restore process in the event of system failure?

A. IRP

B. DRP

C. RPO

D. SDLC

Answer(s): B

---

16. Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking

B. Memory injection

C. Resource reuse

D. Side loading

Answer(s): D

---

17. A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying

B. Account forgery

C. Pass-the-hash

D. Brute-force

Answer(s): A

---

18. An analyst is evaluating the implementation of Zero Trust principles within the data plane.
Which of the following would be most relevant for the analyst to evaluate?

A. Secured zones

B. Subject role

C. Adaptive identity

D. Threat scope reduction

Answer(s): A

---

19. An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources.
Which of the following would be the best solution?

A. RDP server

B. Jump server

C. Proxy server

D. Hypervisor

Answer(s): B

---

20. A company's web filter is configured to scan the URL for strings and deny access when matches are found.
Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A. encryption=off

B. http://

C. www.*.com

D. :443

Answer(s): B
