CompTIA Security+ 2021

1. An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE).

A. TFTP, FTP

B. TLS, SSL

C. Login, rlogin

D. SNMPW1, SNMPv2

E. POP, IMAP

F. SNMPv2, SNMPv3

G. Telnet, SSH

H. SFTP, FTPS

I. HTTP, HTTPS

Answer(s): B,D,H

---

2. The concept of connecting a user account across the systems of multiple enterprises is best known as:

A. federation

B. a remote access policy.

C. multifactor authentication

D. single sign-on.

Answer(s): D

---

3. A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?

A. NIC Teaming

B. Port mirroring

C. Defense in depth

D. High availability

E. Geographic dispersal

Answer(s): C

---

4. Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories

B. State actors

C. Threat feeds

D. Dark web

E. Vulnerability databases

Answer(s): A

---

5. A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal dat a. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

A. Enable the remote-wiping option in the MDM software in case the phone is stolen.

B. Configure the MDM software to enforce the use of PINs to access the phone.

C. Configure MDM for FDE without enabling the lock screen.

D. Perform a factory reset on the phone before installing the company's applications.

Answer(s): C

---

6. An IT security team is concerned about the confidentiality of documents left unattended in MFPs. Which of the following should the security team do to mitigate the situation?

A. Install a software client in every computer authorized to use the MFPs.

B. Update the management software to utilize encryption.

C. Educate users about the importance of paper shredder devices.

D. Deploy an authentication factor that requires in-person action before printing.

Answer(s): D

---

7. A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

A. Incremental backups followed by differential backups

B. Full backups followed by incremental backups

C. Delta backups followed by differential backups

D. Incremental backups followed by delta backups

E. Full backup followed by different backups

Answer(s): B

---

8. A security analyst is reviewing SIEM logs during an ongoing attack and notices the following:

A. SQLi

B. CSRF

C. API attacks

D. Directory traversal

Answer(s): D

---

9. An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

A. HSM

B. CASB

C. TPM

D. DLP

Answer(s): A

---

10. While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps

B. A Telnet session

C. An SSH connection

D. SFTP traffic

Answer(s): B

---

11. A company recently experienced an attack during which its main website was Directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers, Which of the following should the company implement to prevent this type of attack from occurring In the future?

A. IPsec

B. SSL/TLS

C. ONSSEC

D. SMIME

Answer(s): B

---

12. Which of the following can reduce vulnerabilities by avoiding code reuse?

A. Memory management

B. Stored procedures

C. Normalization

D. Code obfuscation

Answer(s): A

---

13. Which of the following measures the average time that equipment will operate before it breaks?

A. SLE

B. MTBF

C. RTO

D. ARO

Answer(s): C

---

14. A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A split-tunnel VPN

D. Load-balanced servers

Answer(s): B

---

15. The CIRT is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company dat a. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?

A. SD-WAN utilizing IPSec

B. NGFW utilizing application inspection

C. WAP utilizing SSL decryption

D. UTM utilizing a threat feed

Answer(s): B

---

16. A security engineer is working to address the growing risks that shadow IT services are introducing to the organization. The organization has taken a cloud-first approach and does not have an on-premises IT infrastructure. Which of the following would best secure the organization'?

A. Upgrading to a next-generation firewall

B. Deploying an appropriate in-line CASB solution

C. Conducting user training on software policies

D. Configuring double key encryption in SaaS platforms

Answer(s): B

---

17. A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

A. MFA

B. Lockout

C. Time-based logins

D. Password history

Answer(s): A

---

18. Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area?

A. Barricades

B. Thermal sensors

C. Drones

D. Signage

E. Motion sensors

F. Guards

G. Bollards

Answer(s): A,D

---

19. A systems administrator is working on a solution with the following requirements:

A. AAA

B. Non-repudiation

C. CIA

D. Zero Trust

Answer(s): D

---

20. experienced railed log-in attempts when authenticating from the same IP address:

A. Spraying

B. Rainbow table

C. Brute-force

D. Dictionary

Answer(s): C
