Cybersecurity

Cybersecurity

- Cybersecurity Quiz 1: Questions & Answers

Cybersecurity Quiz 1: Questions & Answers

1. **Question:** What is meant by IP spoofing in cybersecurity?
   Answer: Fabricating source IP addresses to disguise identity.
2. **Question:** Define session hijacking.
   Answer: Maliciously taking over an active, authenticated web session.
3. **Question:** How would you describe packet sniffing?
   Answer: Passively capturing and analysing network data packets.
4. **Question:** What is an example of an attack that exploits IP communication?
   Answer: The Smurf attack combining IP spoofing and ICMP.
5. **Question:** How does a Man-in-the-Middle (MITM) attack work?
   Answer: Intercepting and altering traffic between two communicating parties.
6. **Question:** What are the effects of a Man-in-the-Middle (MITM) attack?
   Answer: Information disclosure, identity theft, and financial fraud.
7. **Question:** How does IP spoofing work?
   Answer: Altering source IP fields to impersonate trusted hosts.
8. **Question:** Give an example of session hijacking.
   Answer: Injecting unauthorised shell commands into Telnet sessions.
9. **Question:** Name two tools used for packet sniffing.
   Answer: Wireshark and Tcpdump are popular sniffing tools.
10. **Question:** What is a countermeasure against IP spoofing and packet interception?
    Answer: Implementing IPsec for packet encryption and authentication.
11. **Question:** What is the purpose of network segmentation?
    Answer: Isolating critical networks to contain security compromises.
12. **Question:** How can firewalls and IDS help prevent spoofing and hijacking attacks?
    Answer: Rejecting forged packets and analysing traffic anomalies.
13. **Question:** What is a TCP SYN Flood attack?
    Answer: Overwhelming servers with spoofed connection-initiating SYN packets.
14. **Question:** What is the result of a TCP SYN Flood attack?
    Answer: Backlog queue exhaustion, blocking legitimate connection attempts.
15. **Question:** What is session hijacking in TCP?
    Answer: Desynchronising and forging packets within TCP data flows.
16. **Question:** What is a UDP flood attack?
    Answer: Flooding randomised destination ports with high-volume UDP packets.
17. **Question:** Why is UDP vulnerable to attacks?
    Answer: Statelessness and lack of native authentication mechanisms.
18. **Question:** What is the difference between TCP and UDP?
    Answer: TCP is connection-oriented; UDP is connectionless and stateless.
19. **Question:** What is a security risk of DNS over UDP?
    Answer: Vulnerability to IP spoofing and cache poisoning attacks.

20. **Question:** How can HTTP over TCP be attacked?
    Answer: Stealing session cookies or injecting malicious HTTP payloads.
21. **Question:** What is a TCP RESET attack?
    Answer: Sending spoofed RST packets to terminate connection states.
22. **Question:** What are examples of UDP-based attacks?
    Answer: UDP floods, Fraggle attacks, and DNS amplification exploits.
23. **Question:** How can a TCP SYN Flood attack be prevented?
    Answer: Deploying SYN cookies, CDNs, or increasing backlog limits.
24. **Question:** How can UDP-based attacks be prevented?
    Answer: Restricting ICMP responses, perimeter filtering, and BCP 38.
25. **Question:** How can protocol security flaws be mitigated?
    Answer: Deploying encryption, ingress filtering, and network microsegmentation.