UNIT 4

Sniffers

1. What is a Sniffer?

- A sniffer is a tool used to capture and analyze network traffic.
- It monitors the data packets flowing through a network.
- **Example**: Wireshark is a popular sniffing tool.

---

2. Using a Sniffer

- A sniffer works by setting a network card into **promiscuous mode**, allowing it to capture all traffic on the network.
- **Example**: Capturing login credentials sent over an unsecured HTTP connection.

---

3. Switched Network Sniffing

- On a switched network, data packets are sent directly to their destination rather than broadcasted.
- Sniffing on such networks requires specific techniques, like:
  - **ARP Poisoning**
  - **MAC Flooding**

---

4. MAC Flooding

- The attacker overwhelms the switch by sending a large number of fake MAC addresses.
- This forces the switch into "hub mode," broadcasting traffic to all devices, allowing sniffing.

---

5. ARP Poisoning

- Attacker sends fake ARP messages to trick devices into thinking their MAC address corresponds to another device's IP address.
- This lets the attacker intercept traffic between devices.

---

6. MAC Spoofing

- Changing your device's MAC address to mimic another device.
- **Use**: Bypass access control or impersonate a trusted device.

---

7. Port Mirroring (SPAN Port)

- A network switch duplicates the traffic from one port to another for monitoring.

- Often used by administrators for legitimate purposes, but can be exploited for sniffing.

---

8. Detecting Sniffing Attacks

- Look for abnormal network behavior, like unexpected traffic spikes.
- Use tools like **arpwatch** to detect ARP poisoning.
- Use secure protocols like HTTPS or VPNs to encrypt traffic.

Social Engineering

1. What is Social Engineering?

- Manipulating people to give confidential information.
- It exploits human psychology rather than technical vulnerabilities.

---

2. Social Engineering Phases

1. **Research**: Gathering information about the target (e.g., through social media).
2. **Hook**: Establishing trust and initiating contact.
3. **Play**: Exploiting the trust to extract sensitive information.
4. **Exit**: Leaving without arousing suspicion.

---

3. Commonly Employed Threats

- **Phishing**: Fake emails or websites to steal login credentials.
- **Pretexting**: Pretending to be someone else, like a bank employee.
- **Baiting**: Offering something tempting (e.g., a free USB drive) to get access.

---

4. Identity Theft

- Stealing someone’s personal details to impersonate them.
- **Example**: Using stolen credit card details to make purchases.
- **Countermeasures**:
  - Be cautious about sharing sensitive information.
  - Use strong, unique passwords.

Denial of Service (DoS)

1. Understanding DoS

- Overloading a system with requests so it becomes unavailable to legitimate users.
- **Example**: Sending thousands of requests to a web server until it crashes.

2. Understanding DDoS

- Distributed Denial of Service (DDoS) uses multiple devices (often botnets) to launch a coordinated attack.
- **Example**: Using infected IoT devices to flood a website with traffic.

3. DoS Tools

- Tools used to generate massive amounts of traffic:
    - **LOIC (Low Orbit Ion Cannon)**: A basic tool for launching DoS attacks.
    - **HOIC (High Orbit Ion Cannon)**: More advanced and customizable.

4. DDoS Tools

- Tools for large-scale attacks:
    - **Mirai Botnet**: A famous botnet that targeted IoT devices.
    - **Stresser Services**: Paid services offering DDoS capabilities.

5. DoS Pen Testing Considerations

- **Goal**: Test the robustness of a system against DoS attacks.
- **Challenges**: Penetration testing for DoS should avoid actual system downtime. Simulations or small-scale tests are recommended.

Defensive Measures Against DoS/DDoS

- Use firewalls and intrusion detection systems (IDS).
- Employ **rate limiting** to control incoming traffic.
- Use content delivery networks (CDNs) to distribute traffic.

Important MCQ of UNIT 4

Sniffers (15 Questions)

1. What is the primary function of a sniffer?
   a) Encrypt network traffic
   b) Capture and analyse network traffic
   c) Block unauthorized users
   d) Perform vulnerability scanning
   Answer: b

2. Which of the following tools can be used for sniffing?
   a) Wireshark
   b) Metasploit
   c) Nmap
   d) Nessus
   Answer: a

3. What mode must a network interface card (NIC) be in for sniffing?
   a) Managed mode
   b) Promiscuous mode
   c) Monitor mode
   d) Normal mode
   Answer: b

4. In switched network sniffing, what is the purpose of ARP poisoning?
   a) Encrypt traffic
   b) Redirect traffic to the attacker's device
   c) Disable the switch
   d) Clone MAC addresses
   Answer: b

5. What is the result of MAC flooding on a network switch?
   a) Switch operates in promiscuous mode
   b) Switch behaves like a hub
   c) Switch disables all ports
   d) Switch redirects traffic to the router
   Answer: b

6. Which of the following is NOT a sniffing method?
   a) Port mirroring
   b) SPAN port
   c) Social engineering
   d) ARP poisoning
   Answer: c

7. What is a SPAN port used for?
   a) Encrypting network traffic
   b) Mirroring network traffic for monitoring
   c) Assigning IP addresses
   d) Spoofing MAC addresses
   Answer: b

8. Which technique is used to detect sniffing attacks?
   a) Using encrypted protocols
   b) Checking ARP tables for anomalies
   c) Monitoring excessive traffic
   d) All of the above
   Answer: d

9. What protocol is commonly vulnerable to sniffing attacks?
   a) HTTP
   b) HTTPS
   c) SSH
   d) SFTP
   Answer: a

10. What is the primary purpose of MAC spoofing?
    a) Mask the attacker's identity
    b) Encrypt traffic
    c) Deny service to the network
    d) Overload the network switch
    Answer: a

11. Which tool is effective for switched network sniffing?
    a) Ettercap
    b) Nmap
    c) Nikto
    d) Burp Suite
    Answer: a

12. What is ARP in the context of ARP poisoning?
    a) Address Resource Protocol
    b) Address Resolution Protocol
    c) Advanced Routing Protocol
    d) Access Recovery Protocol
    Answer: b

13. Which attack manipulates a switch to behave like a hub?
    a) DNS spoofing
    b) MAC flooding
    c) Packet injection
    d) Ping of death
    Answer: b

14. Which countermeasure prevents sniffing on a network?
    a) Using VLANs
    b) Enabling SSL/TLS
    c) Monitoring ARP tables
    d) All of the above
    Answer: d

15. What type of traffic can sniffers capture on an unencrypted network?
    a) HTTP
    b) FTP
    c) Telnet
    d) All of the above
    Answer: d

Social Engineering (15 Questions)

16. What is social engineering?
    a) Hacking software vulnerabilities
    b) Manipulating people to divulge confidential information
    c) Sniffing network traffic
    d) Performing cryptographic attacks
    Answer: b

17. Which of the following is an example of social engineering?
    a) Phishing
    b) SQL injection
    c) ARP poisoning
    d) Port scanning
    Answer: a

18. What phase involves gathering information about the target in social engineering?
    a) Play
    b) Exit
    c) Research
    d) Hook
    Answer: c

19. A fake email designed to steal login credentials is an example of:
    a) Pretexting
    b) Baiting
    c) Phishing
    d) Identity theft
    Answer: c

20. Offering a free USB drive loaded with malware is an example of:
    a) Pretexting
    b) Baiting
    c) Phishing
    d) Shoulder surfing
    Answer: b

21. What is the final phase of a social engineering attack?
    a) Hook
    b) Research
    c) Play
    d) Exit
    Answer: d

22. Pretexting involves:
    a) Sending fake emails
    b) Impersonating someone to gain information
    c) Distributing malware
    d) Installing sniffers
    Answer: b

23. Identity theft is often a result of:
    a) ARP poisoning
    b) Weak encryption
    c) Social engineering attacks
    d) Denial-of-service attacks
    Answer: c

24. What is shoulder surfing?
    a) Observing someone entering their credentials
    b) Installing malware on a device
    c) Spoofing an email
    d) Using a sniffer to capture data
    Answer: a

25. Which is a countermeasure to social engineering attacks?
    a) Employee training
    b) Multi-factor authentication
    c) Monitoring unusual requests
    d) All of the above
    Answer: d

26. Which type of social engineering attack exploits social networks?
    a) Dumpster diving
    b) Spear phishing
    c) Vishing
    d) Baiting
    Answer: b

27. What is vishing?
    a) Voice phishing
    b) Email phishing
    c) Visual phishing
    d) Video manipulation
    Answer: a

28. Which is NOT a social engineering tactic?
    a) Baiting
    b) Pretexting
    c) ARP spoofing
    d) Phishing
    Answer: c

29. Dumpster diving refers to:
    a) Gaining information from discarded items like documents or devices
    b) Flooding a network with traffic
    c) Monitoring a victim's online activity
    d) Cracking passwords
    Answer: a

30. What is the main goal of social engineering?
    a) Overload systems
    b) Gain unauthorized access to information
    c) Monitor network traffic
    d) Encrypt data
    Answer: b

Denial of Service (DoS) (20 Questions)

31. What is the primary objective of a DoS attack?
    a) Capture user credentials
    b) Overwhelm a system to make it unavailable
    c) Encrypt network data
    d) Redirect network traffic
    Answer: b

32. A DDoS attack uses:
    a) Multiple systems to flood a target
    b) A single system to overwhelm a target
    c) Only encrypted traffic
    d) SQL injection
    Answer: a

33. Which of the following is a DoS tool?
    a) LOIC
    b) Nmap
    c) Wireshark
    d) Metasploit
    Answer: a

34. A botnet is used in:
    a) ARP spoofing
    b) DDoS attacks
    c) SQL injection
    d) Session hijacking
    Answer: b

35. What is a countermeasure to DoS attacks?
    a) Rate limiting
    b) Using firewalls
    c) Load balancing
    d) All of the above
    Answer: d

36. What does LOIC stand for?
    a) Low Orbit Ion Cannon
    b) Light Operating Internet Controller
    c) Limited Object Interaction Component
    d) Loss of Internet Connection
    Answer: a

37. Which layer of the OSI model is commonly targeted by DoS attacks?
    a) Transport
    b) Application
    c) Network
    d) All of the above
    Answer: d

38. Ping of death involves:
    a) Sending oversized packets to crash a system
    b) Manipulating ARP tables
    c) Cracking passwords

d) Using botnets for attacks
Answer: a

39. Which is a common effect of a DDoS attack?
a) Website downtime
b) Unauthorized data access
c) Traffic encryption
d) Malware installation
Answer: a

40. What is the purpose of rate limiting in DoS protection?
a) Restrict the number of requests a system can handle in a given time
b) Block all incoming traffic
c) Detect vulnerabilities
d) Encrypt data packets
Answer: a

Additional 10 MCQs

---

1. What is the main difference between a DoS and a DDoS attack?
a) DoS uses multiple systems, DDoS uses a single system
b) DoS uses a single system, DDoS uses multiple systems
c) DoS targets servers, DDoS targets networks
d) DoS attacks require physical access, DDoS does not
Answer: b

---

2. What is the goal of ARP poisoning in sniffing?
a) Encrypt traffic between devices
b) Redirect traffic to the attacker's device
c) Disable network devices
d) Increase network speed
Answer: b

---

3. Which is a common vulnerability exploited by sniffing tools?
a) Encrypted protocols
b) Unsecured HTTP connections
c) VPN-protected networks
d) TLS connections
Answer: b

---

4. What is spear phishing?
a) Sending generic emails to a large audience
b) Targeting specific individuals or organizations with phishing attempts
c) Scanning for vulnerabilities in networks
d) Using brute force to crack passwords
Answer: b

---

5. Which of the following is an example of baiting?

a) Impersonating a company representative

b) Leaving a malware-infected USB drive in a public place

c) Sending fake invoices to users

d) Using spoofed emails to gather credentials

Answer: b

---

6. Which tool is commonly used to mitigate DDoS attacks?

a) Load balancer

b) Wireshark

c) Port scanner

d) SQL injector

Answer: a

---

7. What is the purpose of a botnet in DDoS attacks?

a) Spread malware

b) Monitor network activity

c) Flood the target with traffic from multiple devices

d) Encrypt data on the target server

Answer: c

---

8. What is an effective way to prevent sniffing on a network?

a) Using ARP poisoning

b) Enabling strong encryption like SSL/TLS

c) Disabling firewalls

d) Using unsecured HTTP connections

Answer: b

---

9. What is the main purpose of social engineering?

a) To gain unauthorized access through human manipulation

b) To encrypt data on servers

c) To scan open network ports

d) To flood a network with traffic

Answer: a

---

10. Which of the following best describes a denial-of-service (DoS) attack?

a) Gaining administrative access to a network

b) Stealing confidential information from a user

c) Overloading a system to render it unusable

d) Scanning for open ports on a network

Answer: c