UNIT 2

Enumeration

1. **What is Enumeration?**
   - Enumeration is the process of extracting detailed information about a target system, such as user names, group names, shares, and services. It's a step after footprinting and scanning in ethical hacking.
2. **Windows Enumeration:**
   - Windows enumeration involves gathering information from Windows-based systems, including usernames, network shares, and system configurations. Tools like **Netstat** and **Netcat** are commonly used for Windows enumeration.
3. **Enumeration with SNMP (Simple Network Management Protocol):**
   - SNMP enumeration is the process of gathering information from network devices such as routers and switches that use SNMP. Attackers exploit SNMP to gather system details, configurations, and passwords if default settings or weak credentials are used.
4. **LDAP and Directory Service Enumeration:**
   - **LDAP** (Lightweight Directory Access Protocol) enumeration allows attackers to query directory services like Active Directory for user account information, group memberships, and network resources.
5. **SMTP Enumeration:**
   - SMTP enumeration refers to extracting email addresses or user accounts from an SMTP (Simple Mail Transfer Protocol) server. By sending special requests to the server, attackers can find valid user accounts.

System Hacking

1. **What is System Hacking?**
   - System hacking is the process of exploiting system vulnerabilities to gain unauthorized access, manipulate system settings, or steal data. It includes activities like password cracking, privilege escalation, and executing malicious code.
2. **Password Cracking:**
   - Password cracking is the process of guessing or cracking passwords using methods like brute force, dictionary attacks, or rainbow tables. Tools like **John the Ripper** and **Hashcat** are used for this purpose.

3. **Authentication on Microsoft Platforms:**
    - Microsoft platforms use various authentication methods like NTLM (NT LAN Manager) and Kerberos. Attackers may attempt to bypass authentication using techniques like pass-the-hash or ticket-hopping.
4. **Executing Applications:**
    - After gaining unauthorized access, attackers may execute malicious applications or payloads to further compromise the system. This could include malware, remote access tools (RATs), or exploit kits.

Malware

1. **Malware and the Law:**
    - Malware creation, distribution, and use are illegal in many countries. Laws like the **Computer Fraud and Abuse Act** in the U.S. make it a crime to intentionally distribute malicious software. Legal consequences can include fines and imprisonment.
2. **Categories of Malware:**
    - **Viruses**: Malicious programs that replicate and spread to other files.
    - **Worms**: Self-replicating malware that spreads over networks without human intervention.
    - **Spyware**: Software that secretly monitors and gathers user information without consent.
    - **Adware**: Malware that displays unwanted advertisements to generate revenue for the attacker.
    - **Scareware**: Fake security alerts designed to scare users into paying for unnecessary software or services.
    - **Ransomware**: Malware that encrypts a victim's files and demands payment for decryption.
    - **Trojans**: Malware disguised as legitimate software, often used to gain unauthorized access.
3. **Overt and Covert Channels:**
    - **Overt Channels**: Legitimate communication channels (e.g., email, network protocols) used by malware for command and control.
    - **Covert Channels**: Hidden or unauthorized communication paths used to transmit malware data, often bypassing security systems (e.g., using steganography or unused protocol fields).

Important MCQ

Enumeration

1. **What is the primary goal of enumeration in ethical hacking?**
   - a) To delete system files
   - **b) To gather detailed information about a target system**
   - c) To disrupt network communication
   - d) To access protected files
2. **Which of the following is used for Windows enumeration?**
   - a) Ping
   - **b) Netstat**
   - c) Nmap
   - d) Wireshark
3. **What does SNMP enumeration help attackers gather?**
   - a) User passwords
   - **b) System configurations and network details**
   - c) Encrypted communication
   - d) Application logs
4. **Which protocol is used for LDAP enumeration?**
   - a) HTTP
   - b) FTP
   - **c) LDAP**
   - d) SNMP
5. **What is the main use of SMTP enumeration?**
   - a) To gather system files
   - **b) To discover valid email addresses**
   - c) To scan for open ports
   - d) To analyze encrypted data

6. **Which type of information can be obtained through Windows enumeration?**
    - a) Password hashes
    - b) User names and group memberships
    - **c) All of the above**
    - d) Only system logs
7. **In SNMP enumeration, which device information can be extracted?**
    - a) Device configurations
    - b) Passwords
    - **c) Network details**
    - d) All of the above
8. **What is the common tool used for LDAP enumeration?**
    - **a) Nmap**
    - b) Netstat
    - c) Metasploit
    - d) Burp Suite
9. **Which of the following is NOT a typical use case for enumeration?**
    - a) Identifying user accounts
    - b) Mapping network shares
    - **c) Gaining unauthorized access**
    - d) Discovering services running on a system
10. **What is the result of performing SMTP enumeration on a mail server?**
    - a) Discovering open ports
    - **b) Identifying valid email addresses**
    - c) Accessing email content
    - d) Obtaining system information

System Hacking

11. **What is the primary objective of system hacking?**
    - a) To hack into social media accounts
    - b) To scan for open ports
    - **c) To exploit system vulnerabilities and gain unauthorized access**
    - d) To monitor network traffic
12. **Which of the following is NOT a common method for password cracking?**
    - a) Brute force attack
    - b) Dictionary attack
    - **c) Data encryption**
    - d) Rainbow table attack
13. **Which Microsoft authentication protocol is commonly targeted by attackers?**
    - a) Kerberos
    - **b) NTLM**
    - c) LDAP
    - d) RDP
14. **What is the first step in system hacking?**
    - a) Executing malicious code
    - **b) Gaining unauthorized access**
    - c) Escalating privileges
    - d) Scanning for open ports
15. **Which tool is commonly used for password cracking?**
    - a) Wireshark
    - b) **John the Ripper**
    - c) Nmap
    - d) Burp Suite
16. **What is the purpose of executing applications in system hacking?**
    - a) To disrupt system operations
    - b) To encrypt files
    - **c) To further compromise the system after gaining access**
    - d) To scan for vulnerabilities

17. **What is pass-the-hash in Microsoft platforms?**
    - a) A technique for cracking passwords
    - **b) A method for bypassing password authentication**
    - c) A vulnerability scanning method
    - d) A data encryption technique
18. **What is a key part of privilege escalation in system hacking?**
    - a) Cracking passwords
    - **b) Gaining higher-level permissions**
    - c) Exploiting vulnerabilities
    - d) Using social engineering
19. **Which tool is used for executing commands remotely on a compromised system?**
    - a) **Metasploit**
    - b) Netstat
    - c) Ping
    - d) Burp Suite
20. **Which of these techniques is used to hide malicious activities after system access?**
    - a) Brute force attack
    - b) **Rootkits**
    - c) Encryption
    - d) Social engineering

Malware

21. **Which of the following is NOT a category of malware?**
    - a) Viruses
    - b) Worms
    - **c) Antivirus**
    - d) Trojans

22. **What is the purpose of ransomware?**

    - ○ **a) To encrypt files and demand payment for decryption**
    - ○ b) To monitor user activities
    - ○ c) To display unwanted advertisements
    - ○ d) To replicate and spread across a network

23. **Which type of malware disguises itself as legitimate software?**

    - ○ a) Worm
    - ○ b) Virus
    - ○ **c) Trojan**
    - ○ d) Spyware

24. **What type of malware is designed to collect sensitive information, such as passwords and browsing habits?**

    - ○ a) Worm
    - ○ **b) Spyware**
    - ○ c) Adware
    - ○ d) Scareware

25. **Which of the following is considered a covert channel for malware communication?**

    - ○ a) Email attachment
    - ○ **b) Steganography**
    - ○ c) DNS lookup
    - ○ d) HTTP request

26. **What is the main goal of adware?**

    - ○ a) To monitor and steal data
    - ○ **b) To display unwanted advertisements**
    - ○ c) To encrypt files for ransom
    - ○ d) To replicate and spread across networks

27. **What type of malware often uses scare tactics to trick users into purchasing unnecessary software?**
    - a) Virus
    - b) **Scareware**
    - c) Trojan
    - d) Worm

28. **Which malware category is known for its self-replicating nature?**
    - a) Adware
    - b) **Worm**
    - c) Spyware
    - d) Trojan

29. **Which type of malware modifies files on a system and then spreads to other files or systems?**
    - a) Worm
    - **b) Virus**
    - c) Ransomware
    - d) Spyware

30. **Which of the following laws addresses malware distribution in the U.S.?**
    - a) HIPAA
    - b) **Computer Fraud and Abuse Act (CFAA)**
    - c) GDPR
    - d) DMCA