Penetration Testing Tools and Shell Commands Recap – 07/05

Cybersecurity Tools and Concepts

1. **Metasploit Framework**:
   - **Use**: Development and execution of exploit code.
   - **Example**: Used to test the vulnerability of a system by simulating attacks.
   - **Key Command**: `msfconsole`
2. **Wireshark**:
   - **Use**: Network packet capture and analysis.
   - **Example**: Diagnosing network issues by analyzing packet data.
   - **Key Command**: Capture interfaces are selected from the Wireshark GUI.
3. **Burp Suite**:
   - **Use**: Interception and modification of HTTP traffic.
   - **Example**: Testing web applications for security vulnerabilities.
   - **Key Component**: Proxy, Scanner, Intruder.
4. **Sqlmap**:
   - **Use**: Automation of SQL injection detection and exploitation.
   - **Example**: Finding and exploiting SQL injection flaws in a web application.
   - **Key Command**: `sqlmap -u "http://target.com/vulnerable.php?id=1" --dbs`
5. **Hydra**:
   - **Use**: Brute-force and dictionary attacks on passwords.
   - **Example**: Testing the strength of passwords on network services like SSH or HTTP.
   - **Key Command**: `hydra -l user -P passwordlist.txt target.com ssh`
6. **Nmap**:
   - **Use**: Network scanning for open ports and services.
   - **Example**: Mapping the network and discovering which services are exposed.
   - **Key Command**: `nmap -sV target.com`
7. **John**:
   - **Use**: Password cracking.
   - **Example**: Recovering passwords by testing against a set of hash values.
   - **Key Command**: `john --wordlist=passwordlist.txt hashfile.txt`
8. **OWASP ZAP**:
   - **Use**: Web application vulnerability scanning.
   - **Example**: Identifying security flaws in web applications during development.
   - **Key Component**: Active Scan, Passive Scan.
9. **Nessus**:
   - **Use**: Automated vulnerability scanning.
   - **Example**: Assessing systems for known vulnerabilities and misconfigurations.
   - **Key Command**: Configured and run through the Nessus GUI.
10. **Aircrack-ng**:
    - **Use**: Wireless network security testing.
    - **Example**: Cracking WEP and WPA-PSK keys.
    - **Key Command**: `aircrack-ng -b BSSID capturefile.cap`
11. **Nikto**:
    - **Use**: Scanning web servers for vulnerabilities.

- **Example**: Checking for outdated server software or insecure server configurations.
- **Key Command**: `nikto -h http://target.com`

Linux Shell Commands

1. **grep**:
   - **Use**: Search for patterns within files.
   - **Example**: `grep "error" /var/log/syslog` (Search for "error" in the syslog file).
2. **chmod**:
   - **Use**: Change file permissions.
   - **Example**: `chmod 755 script.sh` (Sets read, write, execute for owner; read, execute for others).
3. **ifconfig**:
   - **Use**: Display or configure network interface parameters.
   - **Example**: `ifconfig eth0` (Shows details for the eth0 interface).
4. **tcpdump**:
   - **Use**: Capture and analyze network packets.
   - **Example**: `tcpdump -i eth0` (Captures packets on the eth0 interface).
5. **ps**:
   - **Use**: Display current running processes.
   - **Example**: `ps aux` (Shows all processes with details).
6. **less**:
   - **Use**: View file contents one page at a time.
   - **Example**: `less /etc/passwd` (Displays the contents of the passwd file page by page).
7. **route**:
   - **Use**: Display or modify the IP routing table.
   - **Example**: `route -n` (Displays the current routing table).
8. **scp**:
   - **Use**: Securely copy files between hosts.
   - **Example**: `scp file.txt user@remote:/path/to/destination` (Copies file.txt to a remote host).
9. **iptables**:
   - **Use**: Configure the Linux kernel firewall.
   - **Example**: `iptables -L` (Lists all current firewall rules).
10. **df**:
    - **Use**: Display disk space usage.
    - **Example**: `df -h` (Shows disk usage in a human-readable format).
11. **whois**:
    - **Use**: Lookup domain registration details.
    - **Example**: `whois example.com` (Shows registration details for example.com).
12. **awk**:
    - **Use**: Pattern scanning and processing language for text data.
    - **Example**: `awk '{print $1}' file.txt` (Prints the first column from file.txt).
13. **find**:
    - **Use**: Search for files and directories.

    - **Example**: `find /home -name "*.txt"` (Finds all .txt files in the home directory).
14. **wget**:
    - **Use**: Download files from the internet.
    - **Example**: `wget http://example.com/file.zip` (Downloads file.zip from example.com).
15. **sed**:
    - **Use**: Stream editor for modifying text in files.
    - **Example**: `sed 's/old/new/g' file.txt` (Replaces all occurrences of "old" with "new" in file.txt).
16. **tar**:
    - **Use**: Create or extract archives.
    - **Example**: `tar -cvf archive.tar /path/to/files` (Creates an archive of specified files).
17. **touch**:
    - **Use**: Create an empty file or update the timestamp of an existing file.
    - **Example**: `touch newfile.txt` (Creates a new empty file named newfile.txt).
18. **kill**:
    - **Use**: Terminate a process.
    - **Example**: `kill 1234` (Terminates the process with PID 1234).
19. **gzip**:
    - **Use**: Compress files.
    - **Example**: `gzip file.txt` (Compresses file.txt into file.txt.gz).
20. **netstat**:
    - **Use**: Display network connections, routing tables, and interface statistics.
    - **Example**: `netstat -tuln` (Shows listening ports and services).

Questions:

1. **What is the primary function of the Metasploit Framework in penetration testing?**

   A. It acts as a firewall to block malicious traffic.

   B. It is used to scan networks for vulnerabilities.

   C. It provides a platform for developing and executing exploit code.

   D. It encrypts communication between users and servers.

2. **In the context of shell commands, what does the `grep` command do?**

   A. Searches for a pattern in files and displays matching lines.

   B. Changes the file permissions for a specified file.

   C. Lists all files and directories in the current directory.

   D. Moves or renames a file to a different location.

3. **Which tool is commonly used for network packet analysis and can capture and display data passing through a network interface?**

   A. Nmap

   B. Wireshark

   C. John the Ripper

   D. Hydra

4. **In Linux, what is the purpose of the `chmod` command?**

   A. It changes the ownership of a file.

   B. It changes the permissions of a file or directory.

   C. It compresses files into a single archive.

   D. It displays the disk usage of files and directories.

5. **What is a key characteristic of the tool Burp Suite in web application security testing?**

   A. It automates the process of SQL injection attacks.

   B. It is primarily used for password cracking.

   C. It provides a proxy for intercepting and modifying HTTP requests.

   D. It encrypts web traffic to prevent interception.

6. **Which command is used in Linux to find the IP address and network configuration of the system?**

   A. `ifconfig`

   B. `ps`

   C. `ls`

   D. `netstat`

7. **What is the main purpose of the `tcpdump` tool?**

   A. To capture and analyze network packets.

   B. To perform DNS lookups.

   C. To test the reachability of a host.

   D. To generate random passwords.

8. **In penetration testing, what is the function of the `sqlmap` tool?**

   A. It performs brute-force attacks on passwords.

   B. It scans for open ports and services.

   C. It automates the detection and exploitation of SQL injection vulnerabilities.

   D. It intercepts and modifies web traffic.

9. **Which Linux command is used to display the contents of a file, page by page?**

    A. `less`

    B. `cat`

    C. `echo`

    D. `touch`

10. **What is the primary use of the `nmap` tool in network security?**

    A. To encrypt network traffic.

    B. To scan for open ports and services on a network.

    C. To manage firewalls and security policies.

    D. To decrypt sensitive information.

11. **In shell scripting, what is the significance of `#!/bin/bash` at the beginning of a script?**

    A. It comments out the line in the script.

    B. It specifies the script is written in Python.

    C. It indicates which shell should execute the script.

    D. It runs the script with administrative privileges.

12. **Which command would you use to change the owner of a file in Linux?**

    A. `chmod`

    B. `chown`

    C. `chgrp`

    D. `cp`

13. **In web application security, what is the purpose of using OWASP ZAP?**

    A. To encrypt web traffic.

    B. To perform SQL injections.

    C. To scan web applications for vulnerabilities.

    D. To manage SSL/TLS certificates.

14. **What does the `ps` command do in a Unix/Linux system?**

    A. It displays the current directory.

    B. It lists the currently running processes.

    C. It prints the system's uptime.

    D. It shows the memory usage of files.

15. **Which command can be used to display a list of files in a directory, including hidden files, in Linux?**

    A. `ls -a`

    B. `ls -l`

    C. `ls -t`

    D. `ls -r`

16. **What is the main function of the `Hydra` tool in penetration testing?**

    A. To perform DNS analysis.

    B. To crack passwords using brute-force or dictionary attacks.

    C. To intercept and modify network traffic.

    D. To create encrypted tunnels for secure communication.

17. **In Linux, what does the `df` command display?**

    A. Disk usage of files and directories.

    B. Free and used space on mounted file systems.

    C. Detailed information about a specific file.

    D. File contents in hexadecimal format.

18. **What is the purpose of the `whois` command in network reconnaissance?**

    A. To list all open ports on a server.

    B. To gather registration details about a domain name.

    C. To monitor network traffic.

    D. To perform a trace route to a server.

19. **In the context of Linux file permissions, what does `chmod 755` do?**

    A. Sets read, write, and execute permissions for the owner; read and execute for others.

    B. Sets read and write permissions for the owner; read only for others.

    C. Removes all permissions from the file.

    D. Adds execute permissions for the owner, group, and others.

20. **Which penetration testing tool is best known for its capability to automate the discovery and exploitation of vulnerabilities in web applications?**

    A. Wireshark

    B. Nessus

    C. Acunetix

    D. Snort

21. **In the context of Linux, what is the function of the `scp` command?**

    A. To copy files securely between hosts on a network.

    B. To display system performance metrics.

    C. To manage software packages.

    D. To print the current working directory.

22. **What does the `iptables` command do in a Linux system?**

A. It manages the firewall rules.

B. It creates encrypted VPN connections.

C. It lists network interfaces and their configurations.

D. It scans for vulnerabilities on a network.

23. **Which command is used to display the routing table on a Unix/Linux system?**

A. `route`

B. `traceroute`

C. `ping`

D. `netstat`

24. **What is the main use of the tools like `medusa, hydra and John` in cybersecurity?**

A. To perform network scans.

B. To crack passwords using various algorithms.

C. To analyze malware behavior.

D. To intercept web traffic.

25. **In shell scripting, what does the `&&` operator do?**

A. Runs two commands in parallel.

B. Executes the second command only if the first command succeeds.

C. Executes the second command only if the first command fails.

D. Redirects the output of the first command to the input of the second command.

26. **Which tool is commonly used for automated vulnerability scanning and assessment in network security?**

A. Aircrack-ng

B. Burp Suite

C. Nessus

D. Ettercap

27. **In Linux, what is the purpose of the `kill` command?**

    A. To terminate a process by sending a signal.

    B. To close a network connection.

    C. To delete files securely.

    D. To stop network traffic analysis.

28. **What does the `awk` command do in Unix/Linux systems?**

    A. It processes and analyzes text data.

    B. It compresses files into archives.

    C. It lists open files and network connections.

    D. It manages user permissions.

29. **Which command would you use to download a file from the internet in a Unix/Linux terminal?**

    A. `wget`

    B. `mkdir`

    C. `grep`

    D. `echo`

30. **What is the primary function of the `Nikto` tool in web security testing?**

    A. To intercept and modify HTTP requests.

    B. To scan web servers for vulnerabilities.

    C. To brute-force web application passwords.

    D. To encrypt HTTP traffic.

31. **In Linux, which command would you use to view detailed information about a running process, including its memory and CPU usage?**

    A. `top`

    B. `ping`

    C. `ps`

    D. `ls`

32. **What does the `tar` command do in Unix/Linux systems?**

    A. Creates or extracts files from an archive.

    B. Displays the contents of a file.

    C. Transfers files between remote systems.

    D. Lists files in a directory.

33. **Which penetration testing tool is specifically designed for testing the security of wireless networks?**

    A. Aircrack-ng

    B. OpenVAS

    C. BeEF

    D. SQLmap

34. **In the context of shell commands, what does the `find` command do?**

    A. It searches for files and directories based on specified criteria.

    B. It displays the current system time and date.

    C. It compiles source code into executable programs.

    D. It lists all open network connections.

35. **What is the purpose of the `wget` command in a Linux environment?**

    A. To download files from the web.

    B. To monitor system performance.

    C. To display network configuration details.

    D. To change file ownership.

36. **Which tool is commonly used to intercept and modify requests and responses between a web browser and a web server?**

    A. Wireshark

    B. Burp Suite

    C. Nmap

    D. Metasploit

37. **In a Unix/Linux system, what does the `sed` command do?**

    A. It edits text in a file or stream based on specified patterns.

    B. It synchronizes files and directories between locations.

    C. It schedules tasks to run at specified times.

    D. It analyzes network traffic and logs.

38. **Which command is used to compress files using the gzip algorithm in Unix/Linux?**

    A. `gzip`

    B. `tar`

    C. `zip`

    D. `bzip2`

39. **In penetration testing, what is the main purpose of using the tool `Nikto`?**

    A. To perform SQL injections.

    B. To scan web servers for known vulnerabilities and misconfigurations.

    C. To capture and analyze network traffic.

    D. To brute-force web application passwords.

40. **Which Linux command is used to create an empty file or update the timestamp of an existing file?**

    A. `touch`

    B. `nano`

    C. `rm`

    D. `cp`