**LAB 1**

**REPORT**

* ***Kali Linux*:**Kali Linuxis a Linux distro containing

comprehensive set of tools designed for penetesting, vulnerability analysis, and reverse engineering.

Kali Linux has approximately 600 penetration-testing programs (tools), including Armitage (a graphical cyber attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), metasploit (penetration testing framework), John the Ripper (a password cracker), sqlmap (automatic SQL injection and database takeover tool), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp Suite, Nikto, and OWASP ZAP web application security scanners.  
It is often used for learning ethical hacking and doing CTFs.

* ***Metasploit*:** The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities.

Metasploit allows users to check if a target system is vulnerable, choose and configure exploits, and execute them to gain access.

It supports various platforms and includes over 2074 exploits and 592 payloads, making it a robust tool for ethical hacking and security testing.

* ***Burp Suite*:** Burp Suite is apentesting software used for web applications. It’s also used for their security assessment.

Some of the features of Burp Suite include in this suite include features to proxy web-crawls (Burp Proxy), log HTTP requests/responses (Burp Logger and HTTP History), capture/intercept in-motion HTTP requests (Burp Intercept), and aggregate reports which indicate weaknesses (Burp Scanner). This software uses a built-in database containing known-unsafe syntax patterns and keywords to search within captured HTTP requests/responses.

Burp Suite possesses several penetration-type functionalities. A few built-in PoC services include tests for HTTP downgrade, interaction with tool-hosted external sandbox servers (Burp Collaborator), and analysis for pseudorandomization strength (Burp Sequencer). This tool permits integration of user-defined functionalities through download of open-source plugins (such as Java Deserialization Scanner and Autorize).

* ***OWASP*:** OWASP aka **Open Worldwide Application Security Project** is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the fields of IoT, system software and web application. The OWASP provides free and open resources.

One of OWASP's most well-known contributions is the OWASP Top Ten, a regularly updated list of the most critical web application security risks. This list serves as a reference for developers and security professionals to prioritize and address the most prevalent vulnerabilities, such as injection flaws, broken authentication, and insecure design.

In addition to the Top Ten, OWASP offers several other valuable resources, including:

* **OWASP Application Security Verification Standard (ASVS)**: A framework that defines security requirements and verification methods for web applications.
* **OWASP Testing Guide**: A comprehensive guide for conducting web application security testing.
* **OWASP Zed Attack Proxy (ZAP)**: An open-source tool used for automated and manual detection of security vulnerabilities in web applications
* ***OWASP ZAP*:** OWASP Zed Attack Proxy is a free, open-source penetration testing tool designed for testing web applications. It acts as a man-in-the-middle proxy, intercepting and inspecting messages between the browser and the web application, allowing testers to modify and forward packets as needed.

ZAP is widely used for identifying security vulnerabilities during development and testing, offering both passive and active scanning capabilities.

Passive scanning examines all proxy requests and responses without altering them, making it safe to use, while active scanning attempts to find vulnerabilities using known attack vectors, which requires explicit permission from the target application's owner. ZAP also includes features like fuzzing, AJAX spidering, and an API for integration with other tools, making it a versatile choice for security professionals

* ***Ettercap*:** Ettercap is a FOSS network security tool for man-in-the-middle attacks on a LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows.

It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols

Ettercap works by putting the network interface into promiscuous mode and by ARP poisoning the target machines. Thereby it can act as a *man in the middle* and unleash various attacks on the victims. Ettercap has plugin support so that the features can be extended by adding new plugins.

* ***Hydra*:** Hydra is a parallelized network login cracker built into various operating systems like Kali Linux, Parrot and other major penetration testing environments. It was created as a POC tool, for security researchers to demonstrate how easy it can be to crack logins.

Hydra works by using different approaches, such as *brute-force attacks* and *dictionary attacks*, in order to guess the right username and password combination. Hydra is commonly used by penetration testers together with a set of programmes like crunch, cupp etc, which are used to generate wordlists based on user-defined patterns.

Hydra can launch attacks on multiple targets at once using threads, called *hydra heads*. The tool keeps track of the threads using another structure, the *hydra brain*. Each target is attacked using a module that corresponds to a protocol.

* ***Mosquitto*:** Mosquitto is a lightweight, open-source message broker that follows the **MQTT protocol**, licensed under EPL/EDL. It's designed to run efficiently on a wide range of device - from resource-constrained single-board computers to fully powered servers.

The MQTT protocol enables streamlined messaging using a publish/subscribe architecture. This design makes Mosquitto ideal for IoT applications, such as communication between low-power sensors, mobile gadgets, embedded systems, and microcontrollers.

In addition to the broker, the Mosquitto project offers a robust **C client library** for building custom MQTT clients, along with two widely-used command-line tools: *mosquitto\_pub* for publishing messages and *mosquitto\_sub* for subscribing to topics.

* ***Nmap*:** Nmap (Network Mapper) is a network scanner used to discover host and services on a computer network by sending packets and analyzing the responses. It’s a powerful network exploration and security auditing tool used for tasks such as port scanning, service detection, and network discovery.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

For example, the command *nmap -p 135 192.168.5.102* can be used to check if port 135 is open on a specific IP address.

* ***Netcat*:** Netcat, often abbreviated as *nc*, is a computer networking utility for reading from and writing to network connections using TCP or UDP. It is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.

It is a feature-rich network debugging and investigation tool, since it can produce almost any kind of connection its user could need and has a number of built-in capabilities.

It is able to perform port scanning, file transferring and port listening.

*nc [options] [hostname] [port]* is the syntax to use the command.

Ex: *nc -l 1234* is used to listen on port 1234.

* ***SQLmap*:** SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
* ***SQLninja*:** SQLninja is an open-source penetration testing tool designed to exploit SQL injection vulnerabilities in web applications that use Microsoft SQL Server as their backend. Its primary goal is to help ethical hackers and security professionals gain remote OS-level access to vulnerable database servers—even in highly restricted environments.  
  The difference between SQLmap and SQLninja is we use SQLmap when you want a versatile, automated tool that can scan for and exploit SQL injection across many database types and use SQLninja when you're targeting a Microsoft SQL Server and need deep exploitation, especially for remote shell access or privilegeescalation.
* ***msfvenom*:** msfvenom is a tool used for generating and encoding payloads, combining the functionalities of msfpayload (Metasploit framework payload) and msfencode (Metasploit framework encode) into a single tool.

 It was introduced to standardize command line options, improve efficiency, and simplify payload generation. The tool allows users to select payloads, specify output formats, and apply encoders to avoid bad characters. It also supports various options for customizing the payload generation process, such as specifying the architecture, platform, and encoding iterations.

 msfvenom is widely used in penetration testing and security research for creating custom payloads.

* ***Microsoft Threat Model*:** The Microsoft Threat Modeling Tool is a powerful asset within the Security Development Lifecycle (SDL) that helps identify and mitigate security vulnerabilities during the design phase of software development.

It allows users to visually represent system architecture through data flow diagrams and analyze threats using the *STRIDE* framework, covering **Spoofing, Tampering, Repudiation, Information Disclosure,** **Denial of Service, and Elevation of Privilege**. By offering guided analysis, automated suggestions, and detailed reporting, the tool simplifies threat modeling even for non-security experts.

Its primary goal is to enable teams to proactively assess potential risks and apply effective mitigations, ensuring stronger, more secure software designs from the outset.

* ***PyCharm*:** PyCharm is an integrated development environment (IDE) used for programming in Python. PyCharm is developed by the Czech company JetBrains and built on their IntelliJ platform.

PyCharm offers a rich suite of features that make Python development smoother and more efficient. Its intelligent code editor provides smart suggestions, syntax highlighting, and real-time error checking, helping developers write cleaner code faster.

The integrated debugger allows for detailed inspection of code execution, while seamless support for version control systems like Git simplifies collaborative work.

PyCharm also supports popular web frameworks such as Django and Flask, and includes powerful refactoring tools for safely restructuring code. With built-in database tools, testing support, and performance profiling, PyCharm serves as a comprehensive development environment suitable for both beginners and professionals.