AI for Cyber Security with IBM Qradar

Name: Prince Levin Panditi Email: prince.21bce9648@vitapstudent.ac.in

KALI TOOLS:

1. Nmap (Network Mapper):

- Network Scanning: Nmap is primarily used for network scanning and discovery, allowing users to find hosts and services on a network.
- OS Detection: It can determine the operating system of a target system by analyzing network responses.
- Service Version Detection: Nmap can identify the version of services running on open ports, helping assess potential vulnerabilities.
- Scripting Engine: It has a built-in scripting engine (Nmap Scripting Engine or NSE) that allows users to create custom scripts for advanced network reconnaissance.
- Stealth Scanning: Nmap offers various scanning techniques, including stealth scans (e.g., SYN scan) to minimize the chances of detection.

2. Wireshark:

- Packet Analysis: Wireshark captures and analyzes network packets in real-time, providing insights into network traffic and protocols.
- Protocol Support: It supports a wide range of network protocols, making it a versatile tool for network troubleshooting and security analysis.
- Filtering: Users can apply filters to focus on specific types of traffic or packets, making it easier to isolate and analyze issues.
- Colorization: Wireshark colorizes packets based on protocol type, making it visually intuitive to identify potential anomalies.
- Exporting Data: Captured packet data can be exported to various formats for further analysis or reporting.

3. Metasploit Framework:

- Exploit Development: Metasploit is known for its extensive database of exploits, making it a valuable tool for developing and testing exploits.
- Payloads: It provides a wide range of payloads for taking control of compromised systems, including reverse shells and meterpreter sessions.
- Vulnerability Assessment: Security professionals can use Metasploit to assess the security of systems by simulating real-world attacks.
- Post-Exploitation: Metasploit offers post-exploitation modules to maintain access, gather information, and pivot within a compromised network.
- Community Contributions: It has an active community that continually contributes new exploits and modules, keeping it up-to-date.

4. Burp Suite:

- Web Application Testing: Burp Suite is designed for testing web applications, including scanning for vulnerabilities like SQL injection and cross-site scripting (XSS).
- Proxy Features: It acts as a proxy server, allowing users to intercept and modify web traffic, making it ideal for identifying and manipulating requests and responses.

- Spidering: Burp Suite can automatically crawl a web application, mapping out its structure and identifying potential entry points for testing.
- Scanner: It includes an automated scanner that can identify common web vulnerabilities and provide detailed reports.
- Repeater and Intruder: These features enable users to manually modify and replay requests (Repeater) and perform automated attacks (Intruder) for in-depth testing.

5. Hydra:

- Password Cracking: Hydra is a versatile tool for performing password attacks, including dictionary and brute-force attacks.
- Protocols Supported: It supports a wide range of network protocols, such as SSH, FTP, HTTP, and many others.
- Parallel Attacks: Hydra can execute multiple attack attempts simultaneously, speeding up the password-cracking process.
- Customization: Users can configure attack parameters, including usernames, passwords, and character sets, to suit their specific targets.
- Wordlist Support: It allows users to provide custom wordlists for dictionary-based attacks, increasing the chances of success.

6. Aircrack-ng:

- Wi-Fi Security: Aircrack-ng is a suite of tools focused on Wi-Fi network security assessment and penetration testing.
- Packet Capture: It can capture and analyze Wi-Fi data packets, enabling the identification of vulnerabilities in wireless networks.
- WEP/WPA Cracking: Aircrack-ng can be used to crack WEP and WPA/WPA2 encryption keys, provided certain conditions are met.
- Deauthentication Attacks: It supports deauthentication attacks, which can be used to disconnect devices from a Wi-Fi network.
- Packet Injection: Aircrack-ng can inject custom packets into Wi-Fi networks, allowing for various types of attacks and tests.

7. John the Ripper:

- Password Cracking: John the Ripper is a highly efficient password cracking tool known for its speed and support for various hashing algorithms.
- Multiple Platforms: It works on multiple platforms, including Unix, Windows, and macOS, making it versatile for password cracking tasks.
- Hash Support: John supports a wide range of password hash types, including crypt, MD5, SHA-1, and more.
- Wordlist and Rules: Users can use custom wordlists and rules to improve the effectiveness of password cracking.
- Community Contributions: Like Metasploit, John the Ripper benefits from an active user community that contributes to its development and maintains updated hash cracking rules.

8. Nikto:

- Web Server Scanner: Nikto is a web server scanner that identifies potential vulnerabilities in web servers and web applications.
- Database of Tests: It comes with an extensive database of tests for known security issues, outdated software, and misconfigurations.
- Plugin Support: Nikto supports the use of plugins, allowing users to extend its functionality and customize tests.

- Reporting: It generates detailed reports, making it easy to document and address discovered vulnerabilities.
- HTTP Method Testing: Nikto can test for issues related to various HTTP methods, such as PUT, DELETE, and TRACE.

9. SQLMap:

- SQL Injection Testing: SQLMap is a specialized tool for detecting and exploiting SQL injection vulnerabilities in web applications.
- Automatic Enumeration: It can automatically enumerate databases, tables, columns, and data within a vulnerable database.
- Database Takeover: SQLMap can be used to gain unauthorized access to a database, extract data, and even execute arbitrary SQL queries.
- Supported Databases: It supports various database management systems, including MySQL, PostgreSQL, Oracle, and Microsoft SQL Server.
- Custom Injection Techniques: Users can customize injection techniques and payloads for advanced testing.

10. Snort:

- Intrusion Detection: Snort is an open-source intrusion detection and prevention system (IDPS) designed to detect and respond to network-based threats.
- Rule-Based: It uses a rule-based system to identify known attack patterns and anomalies in network traffic.
- Packet Logging: Snort can log packets associated with detected threats, aiding in incident response and forensic analysis.
- Community Rules: Users can access a vast library of community-contributed Snort rules to enhance detection capabilities.
- Real-Time Alerts: It provides real-time alerts when suspicious or malicious network activity is detected, helping security teams respond promptly to threats.