AI for Cyber Security

Assignment – 2

Name: Pabbisetty Pranavi

Reg No: 21BCE9459

Installation of Kali Linux:

Kali Linux is a powerful penetration testing and ethical hacking distribution that comes with a wide range of tools for cybersecurity professionals. It's important to note that using Kali Linux for ethical and legal purposes, such as learning about cybersecurity, conducting security assessments on your own systems, or for authorized penetration testing, is essential. Unauthorized hacking is illegal and unethical.

Installation:

1. Ensure you have a compatible computer or virtual machine to install Kali Linux.
2. Download the Kali Linux ISO image from the official website (https://www.kali.org/downloads/).
3. Create a bootable USB drive or set up a virtual machine using software like VirtualBox or VMware.

Basic Usage:

Once installed, log in using the default username kali and password kali.

After logging in, you'll have access to the Kali Linux desktop environment.

Update and Upgrade:

Open a terminal window and run the following commands to update and upgrade your system:

```
sudo apt update
sudo apt upgrade
```

Kali Linux comes with a plethora of tools categorized for different purposes such as information gathering, vulnerability analysis, exploitation, post-exploitation, and more.

You can access these tools from the Kali Linux menu. Navigate through the categories to explore various tools.

Since Kali Linux is built on Debian, it's essential to have a basic understanding of Linux commands and the command-line interface.

You can start with commands like **ls, cd, pwd, mkdir, touch, cp, mv,** and **rm** to navigate the file system and perform basic operations.

Documentation:

Refer to the Kali Linux documentation (https://docs.kali.org/) to learn more about the tools and their usage.

Each tool has its documentation and tutorials available online. Explore resources and blogs related to ethical hacking and penetration testing.

Exploring the tools of Kali Linux:

Kali Linux includes a vast array of tools for various cybersecurity and penetration testing purposes.

1. **Information Gathering:**

Nmap: A powerful network scanning tool for discovering open ports, services, and vulnerabilities.

Recon-ng: A reconnaissance framework for information gathering, including DNS, OSINT, and more.

theHarvester: Collects email addresses, subdomains, hosts, employee names, and more from public sources.

2. **Vulnerability Analysis:**

Nessus: A vulnerability scanner that identifies security issues in networks and systems.

OpenVAS: An open-source vulnerability scanner and manager with a continuously updated database.

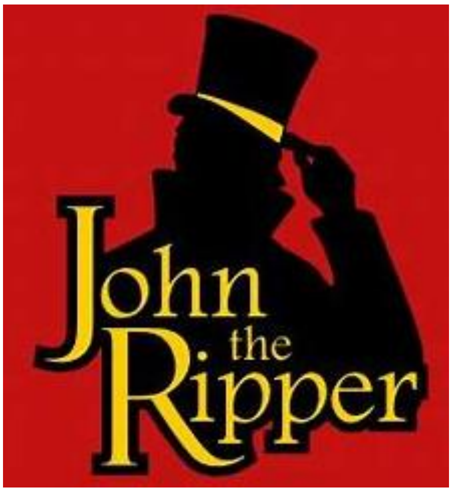
3. **Exploitation Tools:**

Metasploit Framework: A widely used penetration testing framework for developing and executing exploits.

Exploit-db: A database of exploits and vulnerabilities.

Searchsploit: A command-line search tool for finding exploits in the Exploit Database.

4. **Password Attacks:**



John the Ripper: A popular password cracking tool.

Hydra: A versatile password-cracking tool supporting various protocols like SSH, HTTP, FTP, and more.

5. **Wireless Attacks:**

Aircrack-ng: A suite of tools for testing and attacking wireless networks.

Wifite: An automated wireless attack tool for cracking WEP and WPA/WPA2-PSK networks.

6. **Web Application Testing:**

Burp Suite: A powerful web application security testing tool for scanning and intercepting web traffic.

OWASP ZAP: An open-source web application scanner for finding vulnerabilities in web applications.

7. **Forensics Tools:**

Autopsy: A graphical interface for digital forensics analysis.

Volatility: A memory forensics framework for analyzing RAM dumps.

8. Network Analysis Tools:

Wireshark: A popular network protocol analyzer for capturing and inspecting data on a network.

Tcpdump: A command-line network packet analyzer.

9. Stress Testing and DDoS:

Hping: A network tool for packet generation and testing.

LOIC (Low Orbit Ion Cannon): A network stress testing application.

10. Post-Exploitation Tools:

Meterpreter: A Metasploit payload for post-exploitation activities on compromised systems.

Empire: A post-exploitation framework.

11. Social Engineering Tools:

Setoolkit (Social-Engineer Toolkit): A framework for creating and executing social engineering attacks.

12.Reverse Engineering:

Ghidra: An open-source software reverse engineering tool.

Radare2: A framework for reverse engineering and analyzing binaries.

13.Sniffing and Spoofing:

Ettercap: A comprehensive suite for man-in-the-middle attacks.

Bettercap: A Swiss Army knife for network attacks and monitoring.

14.Hardware Hacking:

Bus Pirate: A universal bus interface that can be used to interact with and hack hardware.

Shikra: A USB-controlled logic analyzer and digital signal generator.

15.Reporting Tools:

Dradis: An open-source framework for effective information sharing and reporting in penetration testing.