NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

Exploring tools in Kali Linux

Nmap (Network Mapper):

Nmap is a versatile network scanning tool. It can discover hosts, open ports, and services running on a network.

It supports various scanning techniques, including TCP, UDP, and OS fingerprinting.

Nmap can be used for network reconnaissance and vulnerability assessment.

Burp Suite:

Burp Suite is a powerful web application security testing tool used for both manual and automated testing.

It includes features like proxying, scanning, crawling, and various tools for identifying and exploiting web vulnerabilities like SQL injection and XSS.

Burp Suite is widely used by web application security professionals.

Metasploit Framework:

Metasploit is a penetration testing and exploitation framework that helps identify and exploit vulnerabilities in systems.

It provides a vast collection of pre-built exploits, payloads, and auxiliary modules.

Metasploit is a go-to tool for both security professionals and attackers to test and secure systems.

Wireshark:

Wireshark is a network protocol analyzer used for capturing and analyzing network traffic in real-time.

It allows you to inspect packets, dissect protocols, and troubleshoot network issues.

Wireshark is valuable for diagnosing network problems and understanding network behavior.

John the Ripper:

John the Ripper is a popular password cracking tool used to crack password hashes.

It supports various hash algorithms and attack methods, including dictionary attacks and brute force attacks.

Security professionals use it to test the strength of passwords in their environments.

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

Ghidra:

Ghidra is a powerful open-source software reverse engineering tool developed by the NSA.

It helps analyze and decompile binary executables to understand their functionality and vulnerabilities.

Ghidra is commonly used for malware analysis and vulnerability research.

Autopsy:

Autopsy is a graphical interface for The Sleuth Kit, a popular open-source digital forensic toolkit.

It is used for analyzing disk images, file systems, and recovering data from storage media.

Autopsy is valuable in digital forensics investigations.

Volatility:

Volatility is a memory forensics framework used to analyze system memory dumps.

It can extract information about running processes, open network connections, and identify rootkits or malware in memory.

Volatility is crucial for memory analysis in incident response and forensics.

Social Engineer Toolkit (SET):

SET is a toolkit for conducting social engineering attacks, such as spear-phishing and credential harvesting.

It includes various attack vectors like email spoofing, website cloning, and credential capture.

SET is for ethical use and security awareness training.

MagicTree:

MagicTree is a reporting tool designed for penetration testers to create and manage penetration test reports.

It provides a structured way to document findings, vulnerabilities, and recommendations.

MagicTree helps testers deliver clear and comprehensive reports to clients.