CYBER SECURITY LABORATORY

EXPLORING TOOLS IN KALI LINUX

Objective: In this assignment, you are required to explore 2-3 tools available in Kali Linux. For each tool, provide a brief explanation (2-3 lines) detailing what the tool is and its primary use case. Additionally, include a screenshot of the tool's home page or interface.

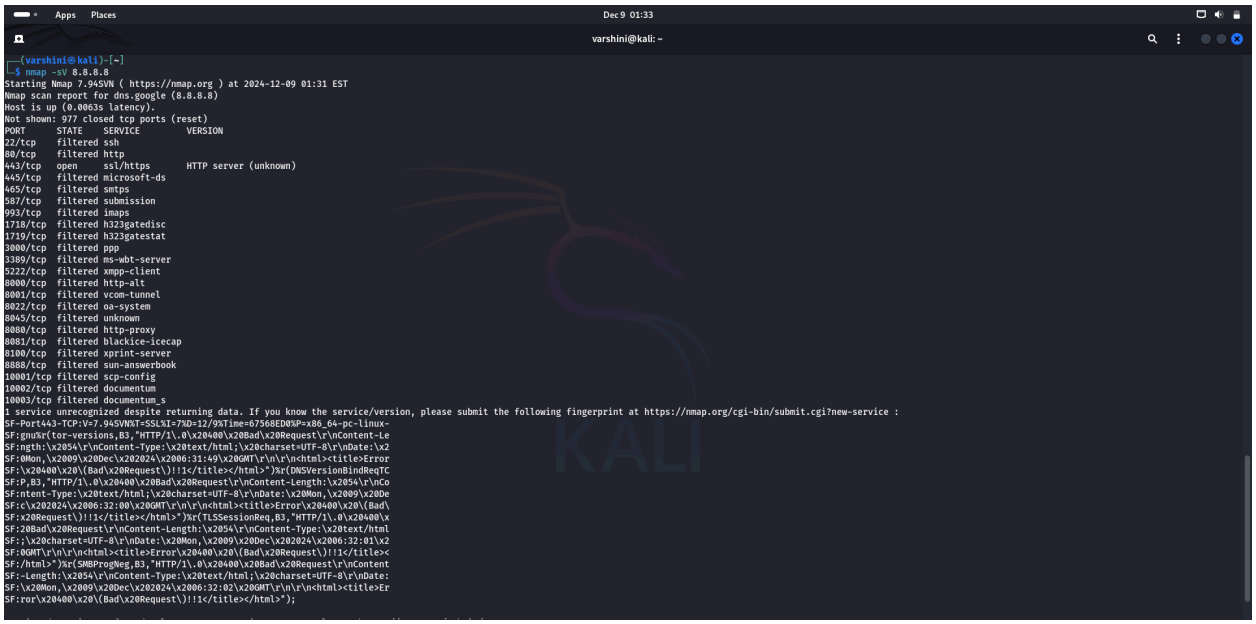
Information Gathering:

Nmap: *(Network mapper)*

- Nmap is a powerful open-source tool used for network discovery and security auditing.
- It can scan large networks quickly, identifying live hosts, open ports, services, and operating systems.
- Nmap is widely used by network administrators and security professionals to perform reconnaissance and vulnerability assessments.

Primary Use Cases:

- Scanning networks to discover hosts and services.
- Identifying open ports and running services on target machines.
- Detecting vulnerabilities and misconfigurations.



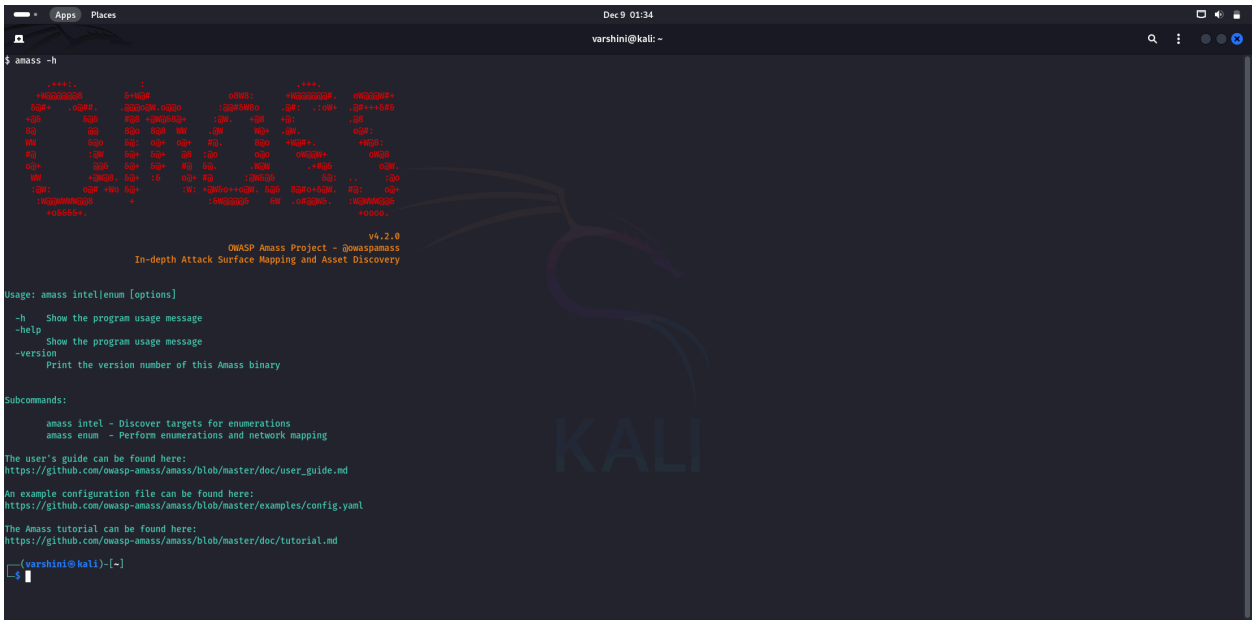
Amass

- Amass is an open-source tool developed by the OWASP Foundation for performing advanced network mapping and asset discovery.
- It is primarily used for subdomain enumeration, discovering external assets, and mapping attack surfaces by gathering

information from public sources and active reconnaissance techniques.

Primary Use Cases:

- Discovering subdomains associated with a target domain.
- Mapping an organization's external infrastructure.
- Performing reconnaissance to identify potential attack vectors.



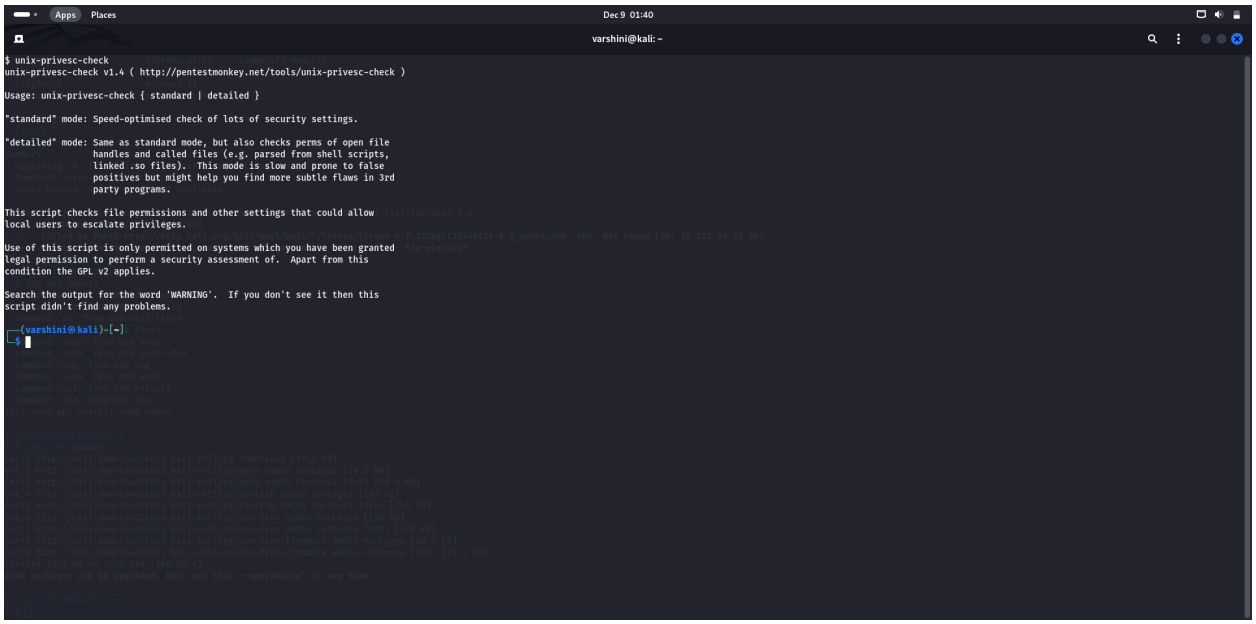
Vulnerability Analysis:

unix-privesc-check

- unix-privesc-check is a command-line tool designed to identify potential privilege escalation paths on Unix-based systems.
- It scans the system for misconfigurations, improper file permissions, and other vulnerabilities that can allow an attacker to elevate privileges from a standard user to root.
- It is particularly useful for post-exploitation analysis.

Primary Use Cases:

- Identifying potential privilege escalation vulnerabilities.
- Auditing system configurations for insecure settings.
- Assisting penetration testers in finding paths to root access.



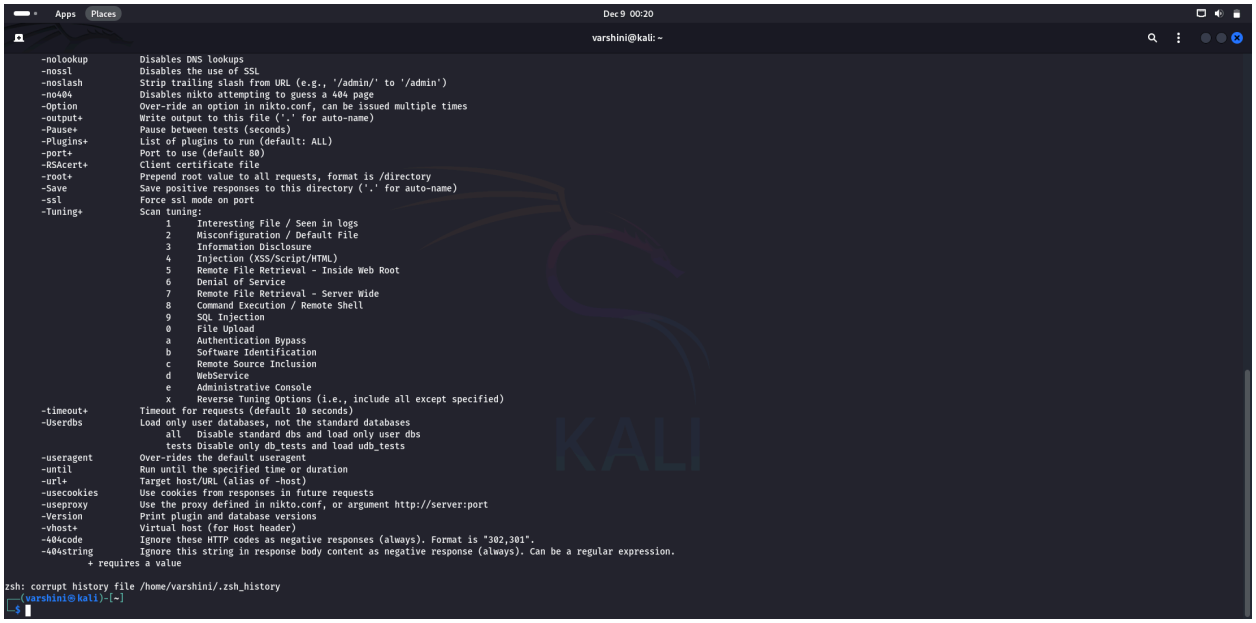
Nikto:

- Nikto is an open-source web server scanner that performs comprehensive tests to detect vulnerabilities, misconfigurations, and outdated software on web servers.
- Developed in Perl, Nikto quickly scans for over 6,700 potentially dangerous files or programs, checks for outdated versions of server software, and identifies common security issues.

Primary Use Cases:

- Identifying vulnerabilities in web servers.

- Checking for misconfigurations and outdated software.
- Performing security assessments on web applications.



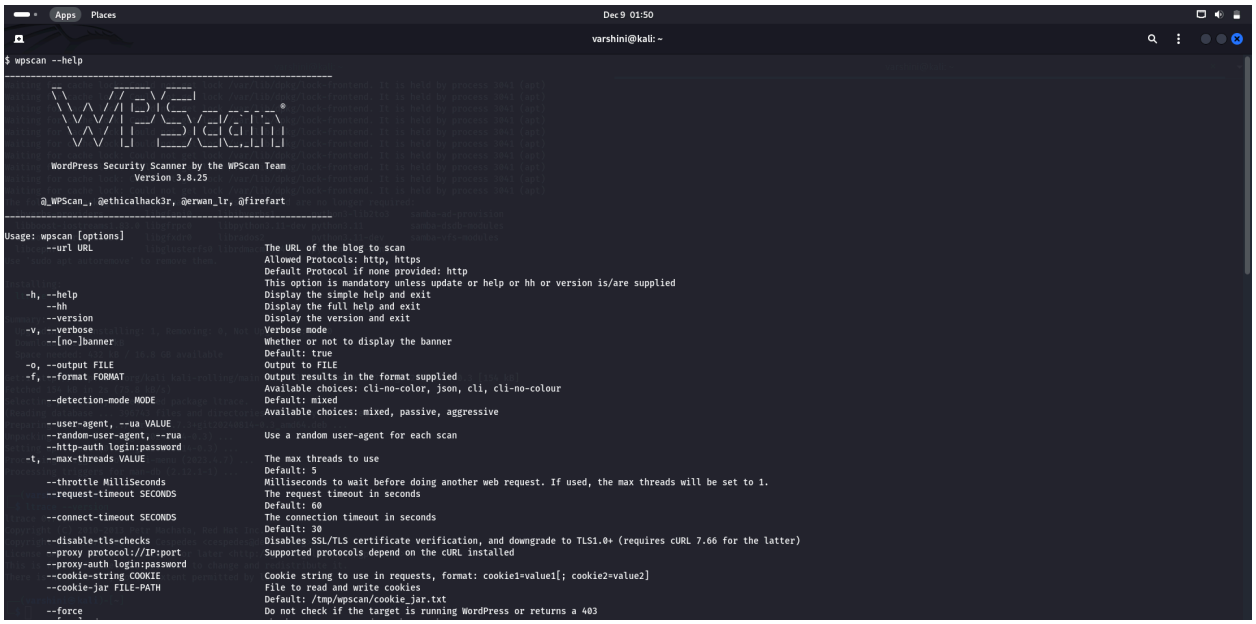
Web Application Analysis:

WPScan

- WPScan is a specialized WordPress vulnerability scanner designed to detect security issues within WordPress installations.
- It helps security professionals, penetration testers, and website administrators identify vulnerabilities in WordPress core files, plugins, themes, and configurations.
- WPScan is effective in detecting outdated versions, misconfigurations, and potential attack vectors on WordPress websites.

Primary Use Cases:

- Scanning WordPress websites for vulnerabilities.
- Identifying outdated plugins and themes with known security issues.
- Detecting weak user passwords and security misconfigurations.

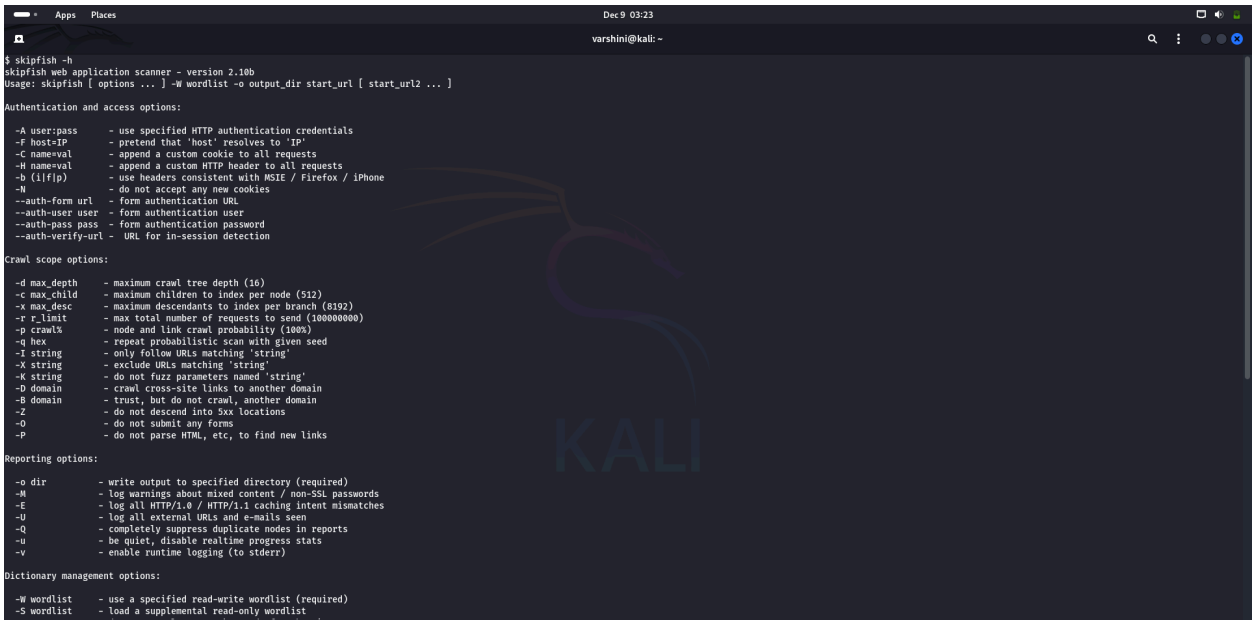


Skipfish

- Skipfish is an open-source web application security scanner designed for fast and efficient vulnerability scanning.
- It is written in C and focuses on scanning websites for common web security flaws such as cross-site scripting (XSS), SQL injection, and other critical issues.
- Skipfish generates detailed reports and provides an interactive interface for analyzing the results.

Primary Use Cases:

- Scanning web applications for vulnerabilities.
- Identifying common web security flaws such as XSS, SQL injection, and information leakage.
- Quickly assessing the security of websites and web applications.



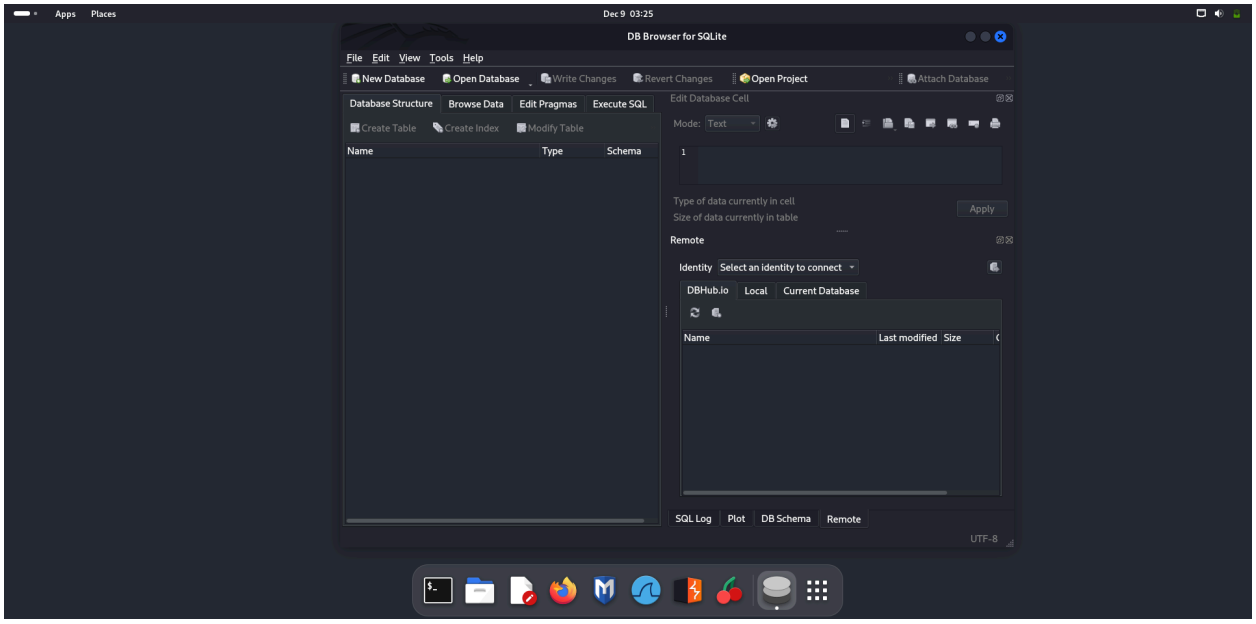
Database Assessment:

SQLite Database Browser

- SQLite Database Browser (also known as DB Browser for SQLite) is a free, open-source tool that provides an intuitive interface for managing SQLite databases.
- It allows users to create, design, and edit SQLite database files, perform queries, and browse through stored data.
- It is especially useful for developers, testers, and security professionals working with SQLite-based applications.

Primary Use Cases:

- Viewing, editing, and managing SQLite databases.
- Running SQL queries directly on the database.
- Analyzing and manipulating data within SQLite databases.
- Extracting information from SQLite databases during penetration testing and forensic investigations.



SQLmap

- SQLmap is an open-source penetration testing tool used for automating the process of detecting and exploiting SQL injection vulnerabilities in web applications.
- It is highly effective at identifying and exploiting SQL injection flaws and gaining access to underlying databases.
- SQLmap supports a wide range of database management systems (DBMS) such as MySQL, PostgreSQL, MSSQL, Oracle, and others.

Primary Use Cases:

- Detecting SQL injection vulnerabilities in web applications.
- Exploiting vulnerabilities to extract data from databases.
- Bypassing web application firewalls (WAFs) and other protective mechanisms.
- Performing database fingerprinting to identify the type and version of the underlying DBMS.
- Dumping data (such as user credentials and other sensitive information) from vulnerable databases.

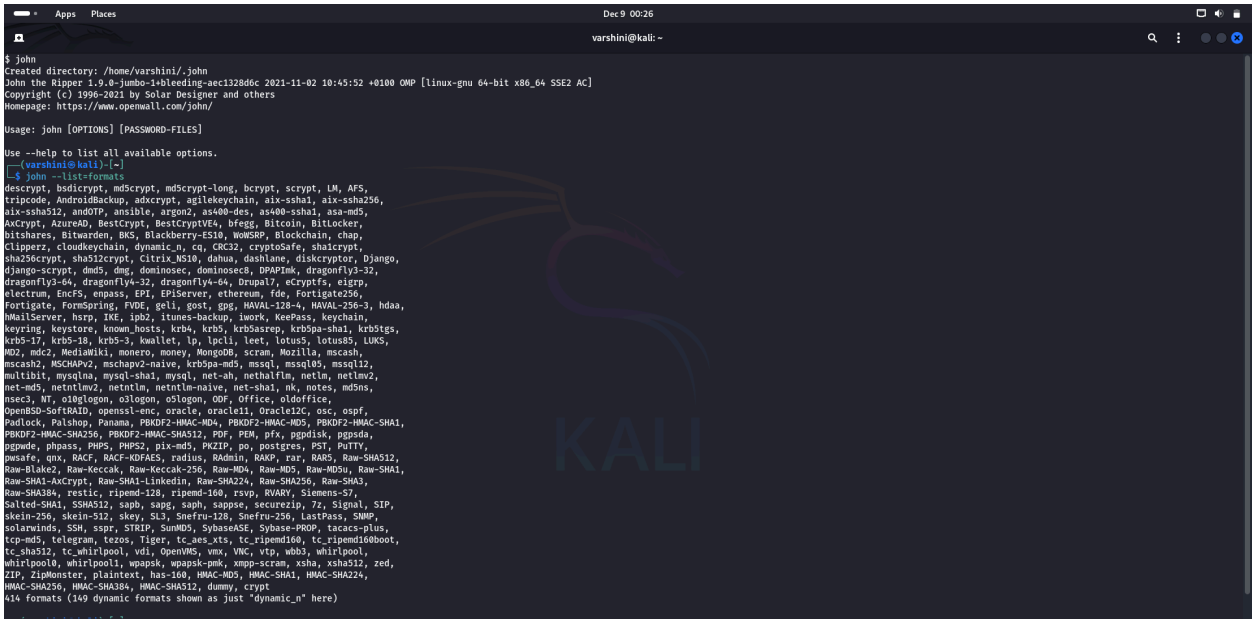
Password Attacks:

John the Ripper

- John the Ripper is a fast, open-source password-cracking tool designed to detect weak passwords and recover lost passwords.
- It supports various encryption algorithms and password hash types, making it a popular tool among penetration testers and security professionals.
- John the Ripper can perform dictionary-based attacks, brute-force attacks, and rainbow table attacks.

Primary Use Cases:

- Cracking passwords to test the strength of user credentials.
- Recovering lost passwords for system and file access.
- Auditing password security in systems.
- John the Ripper is highly effective for auditing password security and identifying weak passwords.



Hashcat:

- Hashcat is a powerful, open-source password cracking tool designed to crack various hash types using a wide range of attack methods, such as brute-force, dictionary, and rule-based attacks.
- It is widely regarded as one of the fastest password recovery tools and supports GPU acceleration, making it significantly faster than CPU-based cracking tools.
- Hashcat is used by security professionals and penetration testers to audit password security.

Primary Use Cases:

- Cracking hashed passwords to recover lost passwords or test password strength.
- Auditing password databases to identify weak passwords.
- Performing dictionary, brute-force, and hybrid attacks on password hashes.
- Testing password security in various cryptographic hash algorithms.

Wireless Attacks:

Wifite

- Wifite is an open-source. It is specifically designed for ease of use, automating the process of capturing handshakes and performing attacks on wireless networks.
- Wifite can conduct a variety of attacks, including dictionary-based and brute-force attacks on WPA/WPA2 networks, making it a valuable tool for penetration testers and security researchers.

Primary Use Cases:

- Cracking WEP and WPA/WPA2 encryption on wireless networks.
- Capturing handshakes to attempt offline password cracking.
- Automating attacks on weak or poorly configured wireless networks.
- Penetration testing and security assessments of wireless networks.

Kismet:

- Kismet is an advanced, open-source wireless network detector, sniffer, and intrusion detection system (IDS).
- It is designed to work with a wide variety of wireless network interfaces and provides detailed information about Wi-Fi networks, including their signal strength, encryption type, and potential vulnerabilities.

Primary Use Cases:

- Detecting and monitoring Wi-Fi networks in the vicinity.
- Detecting hidden networks (i.e., networks that do not broadcast their SSID).
- Intrusion detection in wireless environments by identifying rogue access points and unauthorized clients.

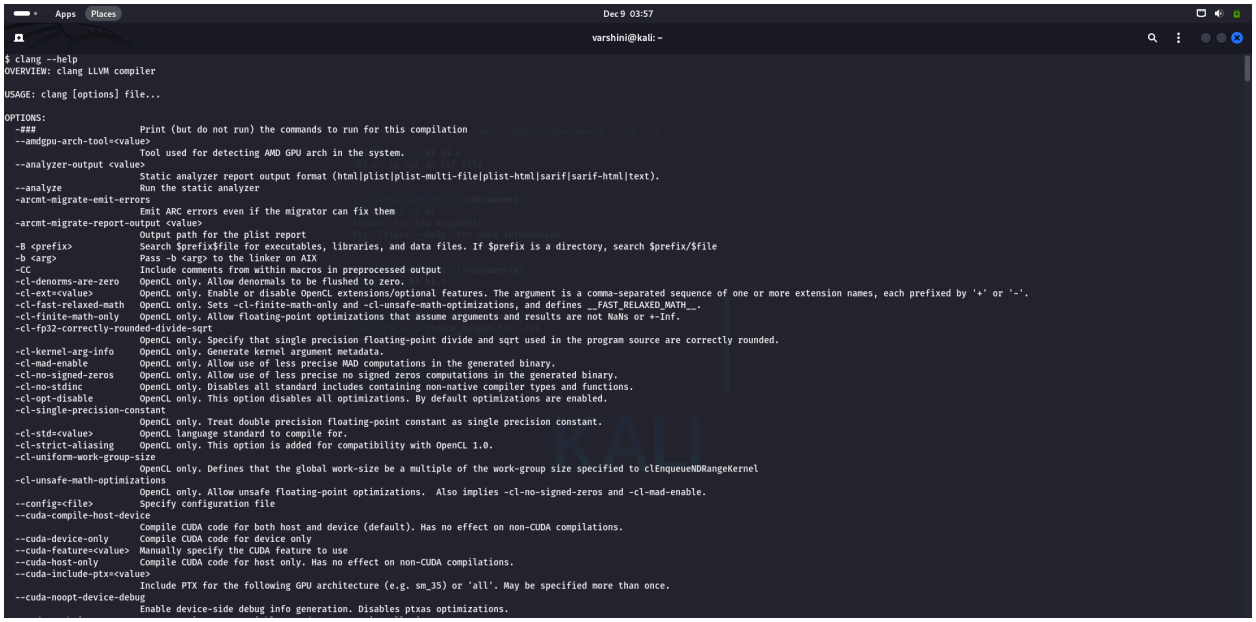
Reverse Engineering:

Clang

- Clang is part of the LLVM (Low Level Virtual Machine) project and provides an alternative to the GCC (GNU Compiler Collection).
- Clang is designed to be highly efficient, fast, and feature-rich, providing better diagnostics (error and warning messages), and producing optimized, high-performance executables.

Primary Use Cases:

- Compiling C, C++, and Objective-C code for various platforms.
- Static analysis and code diagnostics to identify bugs and security vulnerabilities.
- Debugging and profiling using integration with tools like gdb or lldb.



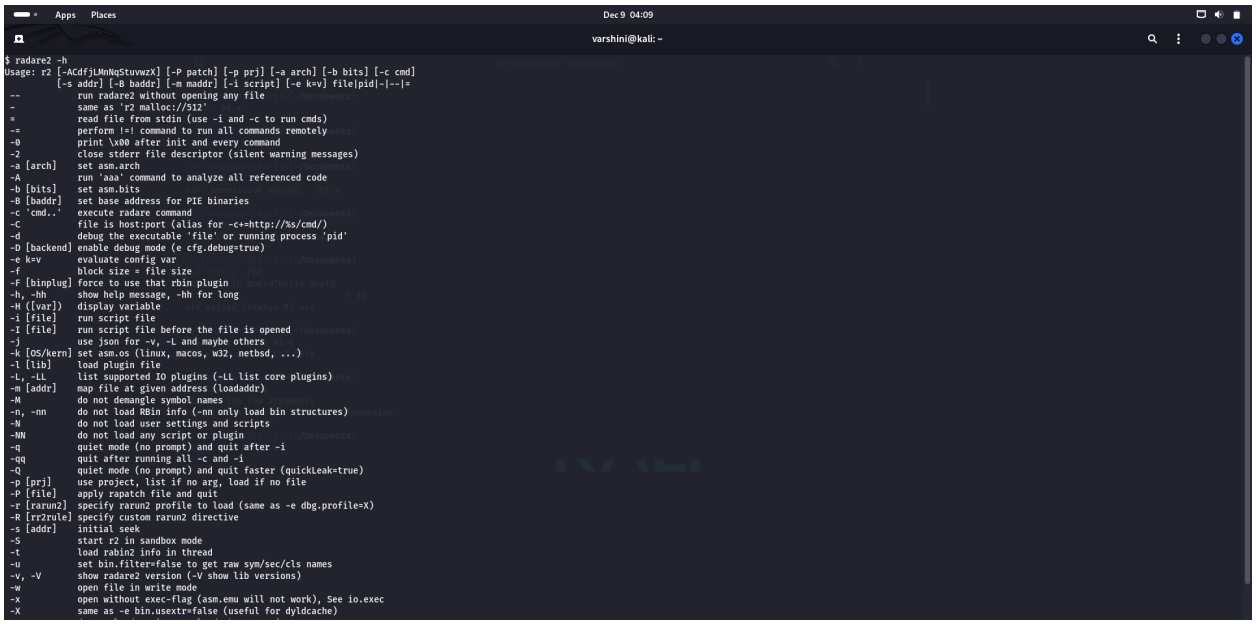
Radare2

- Radare2 is an open-source, reverse engineering framework that provides a comprehensive set of tools for analyzing and disassembling binaries, debugging, and performing low-level analysis on executable files.
- Radare2 is highly flexible and can be used for a wide range of tasks, from simple file inspection to complex vulnerability research.

Primary Use Cases:

- Disassembly and decompilation of machine code into human-readable formats.
- Malware analysis to understand the functionality and behavior of potentially malicious software.
- Binary patching to modify executable files for testing and debugging.

- Security auditing and vulnerability research to identify weaknesses in compiled code.



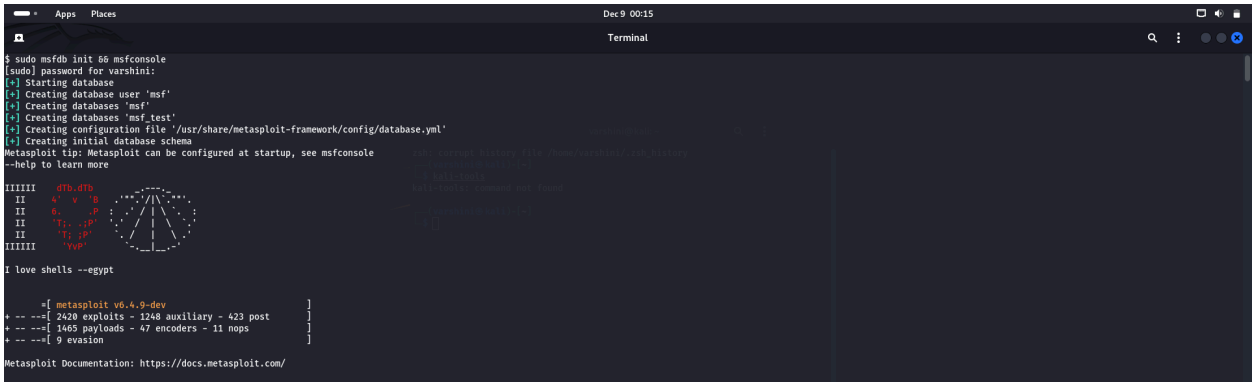
Exploitation Tools:

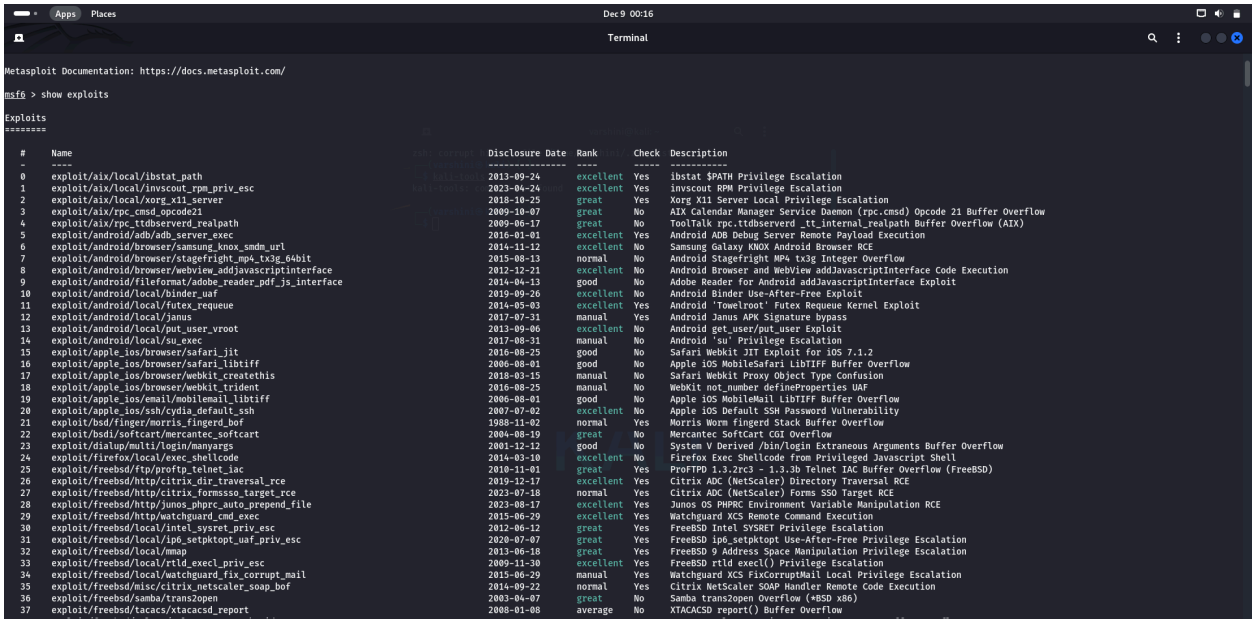
Metasploit Framework

- Metasploit is an open-source penetration testing framework.
- It is widely used by ethical hackers and security professionals to identify, exploit, and validate vulnerabilities in networks, systems, and applications.

Primary Use Cases:

- Identifying vulnerabilities in systems and networks.
- Developing and testing exploits.
- Conducting penetration tests.
- Metasploit supports both command-line and GUI-based interfaces (such as Armitage).



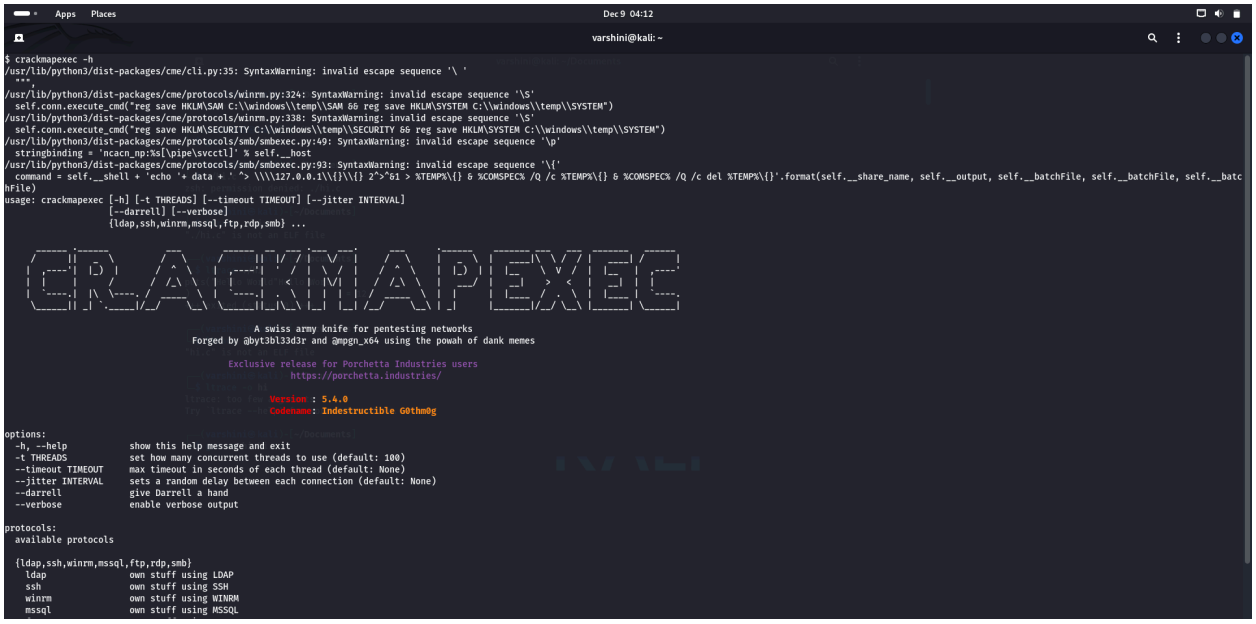


CrackMapExec *(CME)*

- CrackMapExec (CME) is an open-source, post-exploitation tool primarily used for network penetration testing and Windows environment assessments.
- It automates the assessment of large Active Directory (AD) networks by providing a simple and effective way to perform tasks like SMB enumeration, credential validation, command execution, and more.

Primary Use Cases:

- Network enumeration (SMB, RDP, and other services).
- Credential validation across multiple machines in a Windows domain.
- Dumping password hashes and performing Pass-the-Hash (PTH) attacks.
- Reconnaissance and exploitation in Active Directory (AD) environments.



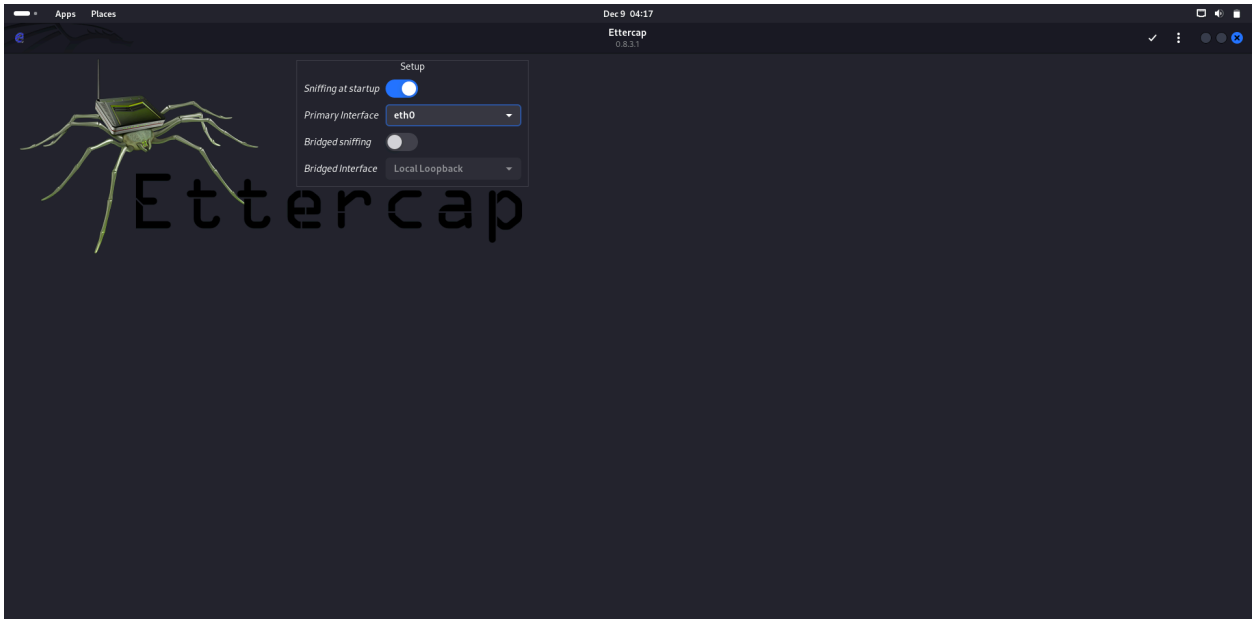
Sniffing & Spoofing:

Ethercap-Graphical

- Ethercap-Graphical is the graphical user interface (GUI) version of Ettercap, a well-known network sniffing and man-in-the-middle (MITM) attack tool.
- Ettercap is widely used for packet sniffing, network traffic analysis, and performing MITM attacks on local area networks (LANs).

Primary Use Cases:

- Man-in-the-Middle (MITM) attacks, including ARP poisoning and DNS spoofing.
- Packet sniffing and analysis on local networks to monitor traffic.
- Intercepting and modifying network traffic in real-time (e.g., injecting custom responses or altering data in transit).
- Session hijacking to take control of active user sessions.



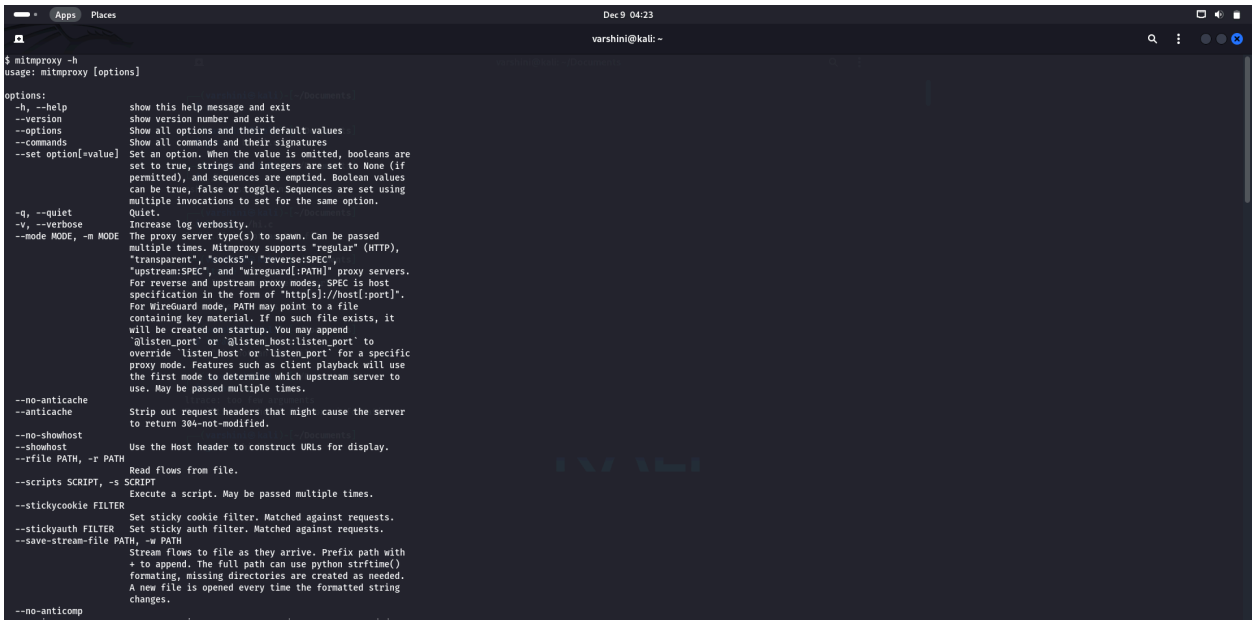
---

mitmproxy

- mitmproxy is an open-source, interactive proxy tool used for intercepting, inspecting, modifying, and debugging HTTP and HTTPS traffic in real-time.
- It supports both HTTP/1.x and HTTP/2 protocols, and provides a console-based interface (mitmproxy), a web-based interface (mitmweb), and an API for automated scripting.

Primary Use Cases:

- Intercepting and modifying HTTP/HTTPS traffic between clients and servers.
- Capturing and analyzing web traffic for sensitive data like login credentials, tokens, etc.
- Testing web applications for vulnerabilities such as cross-site scripting (XSS), SQL injection, and other web security issues.
- Debugging and analyzing web services by inspecting headers, cookies, and response data.



Post Exploitation:

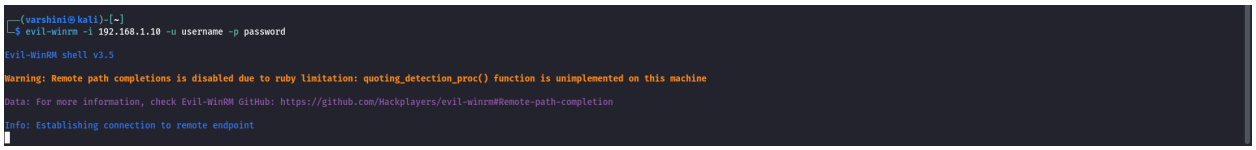
Evil-WinRM

- Evil-WinRM is a powerful open-source tool used for Windows Remote Management (WinRM) exploitation and post-exploitation in penetration testing and red team operations.

- Evil-WinRM is often employed in lateral movement across networks and post-exploitation activities, as it enables attackers to gain command-line access to Windows machines, bypassing traditional remote access tools like RDP.

Primary Use Cases:

- Remote command execution on Windows systems over WinRM, particularly in Active Directory (AD) environments.
- Remote administration and troubleshooting for legitimate penetration testing scenarios (with permission).
- Pivoting and lateral movement in a network to gain access to other machines and sensitive data.



Netcat *(nc)*

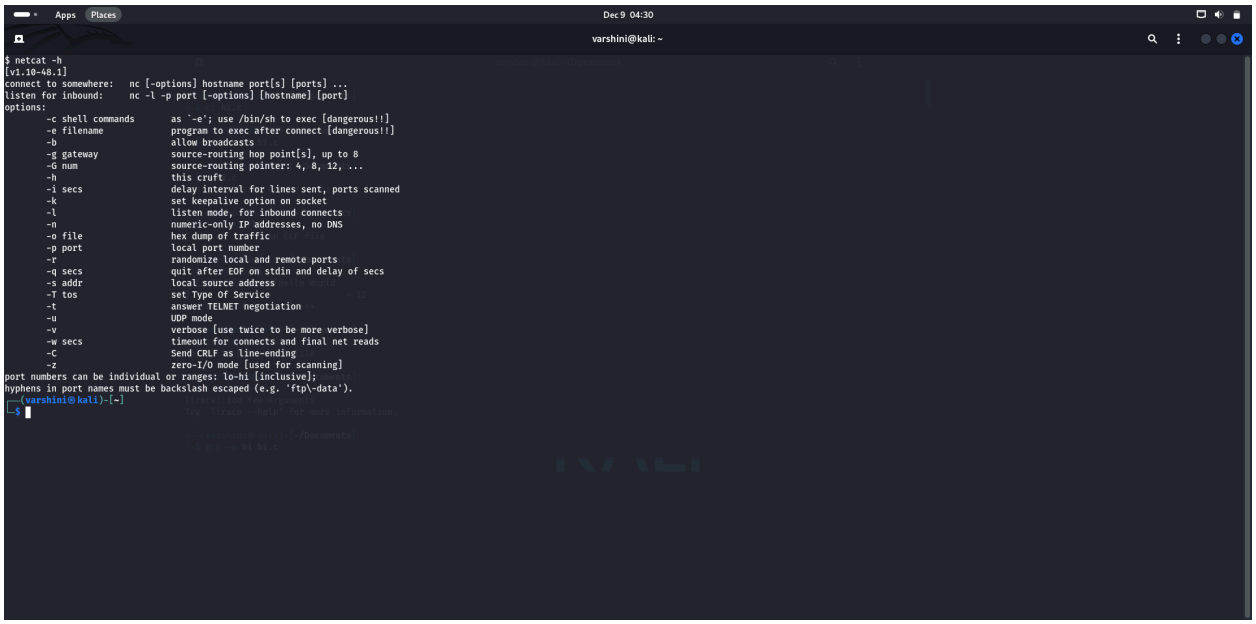
- Netcat (nc) is a versatile and widely used networking utility that can create both TCP and UDP connections between two machines.
- Often referred to as the "Swiss army knife" of networking tools, Netcat can be used for a wide range of tasks, such as

port scanning, banner grabbing, file transfers, remote access, and network debugging.

- Netcat is commonly used in penetration testing and red teaming activities due to its ability to create backdoors and facilitate data exfiltration.

Primary Use Cases:

- Banner grabbing to identify services and versions running on remote systems.
- Port scanning to identify open ports on target systems.
- Data exfiltration by sending files over the network.
- Simple file transfer between systems.



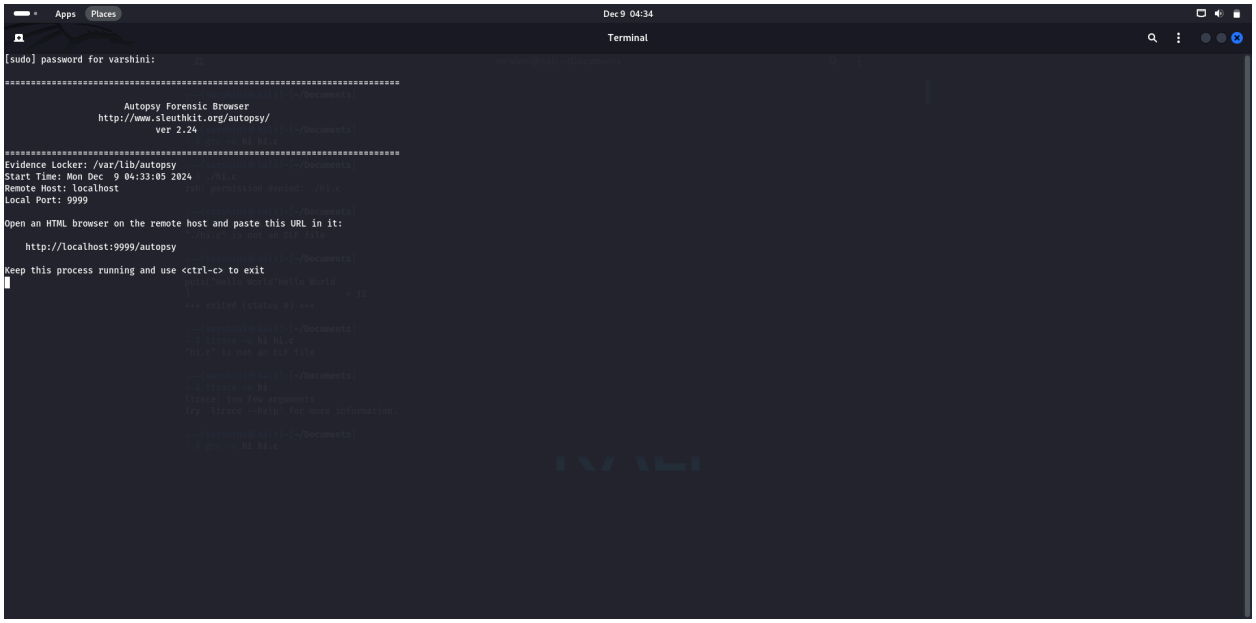
Forensics:

Autopsy

- Autopsy is an open-source, digital forensics platform used for investigating and analyzing data from computers, mobile devices, and storage media.
- Autopsy is commonly used by forensic professionals, law enforcement, and cybersecurity experts to recover, analyze, and report on data from various devices.
- It supports file analysis, metadata extraction, timeline analysis, and much more.

Primary Use Cases:

- Digital forensics investigations, particularly in law enforcement and incident response scenarios.
- File recovery and examination, including deleted files and hidden data.
- Evidence tracking for ensuring that all digital evidence is preserved and properly documented.
- Malware analysis by extracting and analyzing data from infected systems or drives.

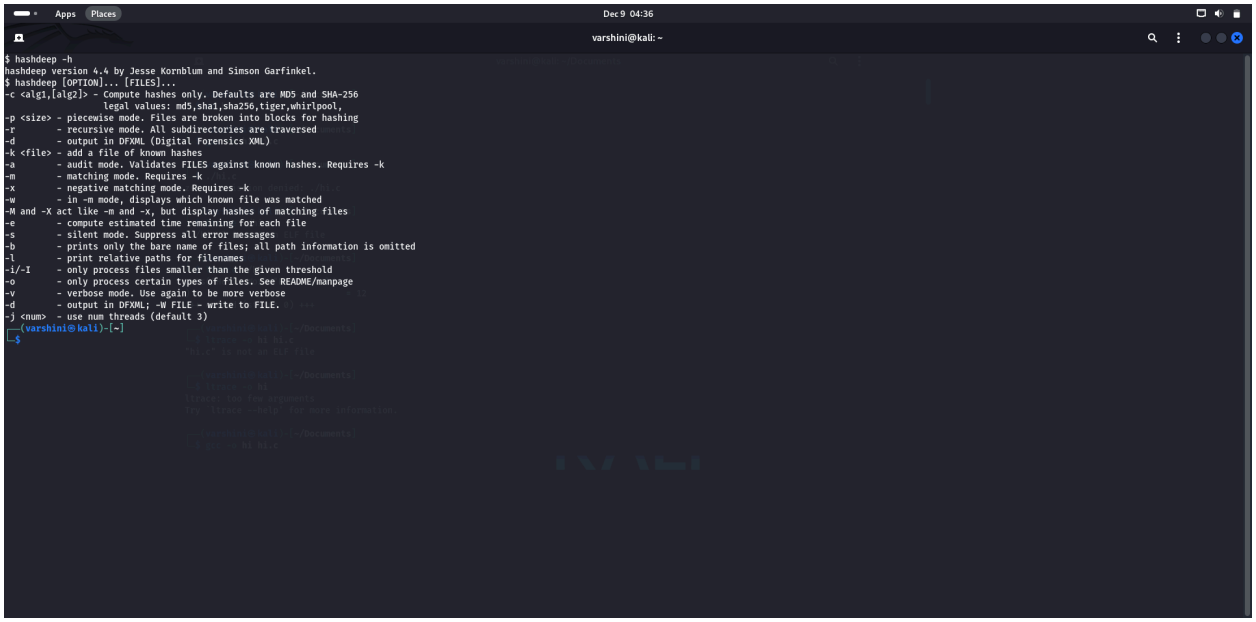


Hashdeep

- Hashdeep is an open-source command-line tool for computing and verifying hashes of files, and for deep hashing across directories.
- It supports a variety of hash algorithms, including MD5, SHA-1, SHA-256, and more.
- Hashdeep is primarily used in file integrity checking, data verification, and forensic investigations to ensure the authenticity and integrity of files, especially when comparing hashes between different systems or performing audits on large collections of files.

Primary Use Cases:

- File integrity checking: Ensuring that files have not been altered, especially in digital forensics and cybersecurity investigations.
- Data verification: Comparing file hashes across different systems or environments to verify consistency.
- Forensic investigations: Checking the integrity of evidence by comparing hashes to known values or a hash database.
- Bulk hashing: Calculating hashes for many files in a directory or filesystem for auditing or forensic analysis.



Reporting Tools:

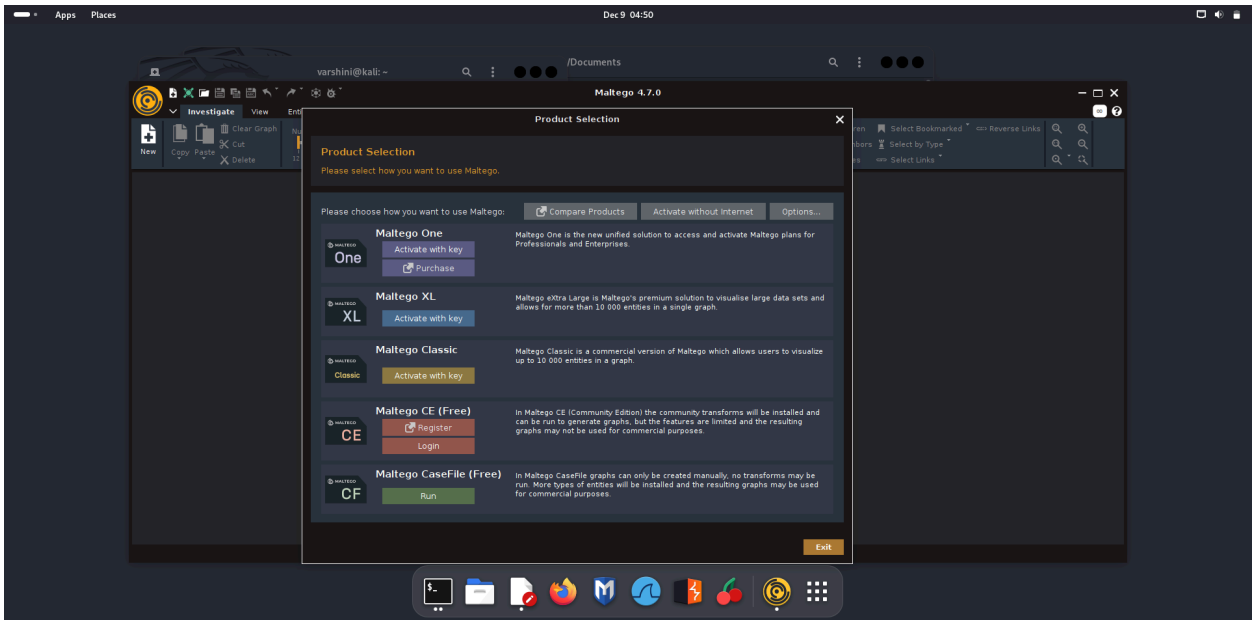
Maltego:

- Maltego is a powerful open-source intelligence (OSINT) and forensic investigation tool that focuses on mapping relationships between various entities such as people, organizations, domains, IP addresses, and more.
- It is used to conduct network analysis, data mining, and reconnaissance in cybersecurity and threat intelligence. Maltego excels at visualizing complex relationships and connections in a graph format, making it easier to identify patterns and understand the connections between different pieces of information.

Primary Use Cases:

- Network mapping to identify how domains, subdomains, IP addresses, and services are connected.

- Cyber threat intelligence to analyze the connections between different threats, such as attackers, malware, and victims.
- Investigative forensics for examining the relationships between people, organizations, and online activities in criminal investigations.
- Social engineering attacks, mapping out key individuals or targets and their networks.
- Phishing and fraud detection by mapping the links between email addresses, domains, and IP addresses.



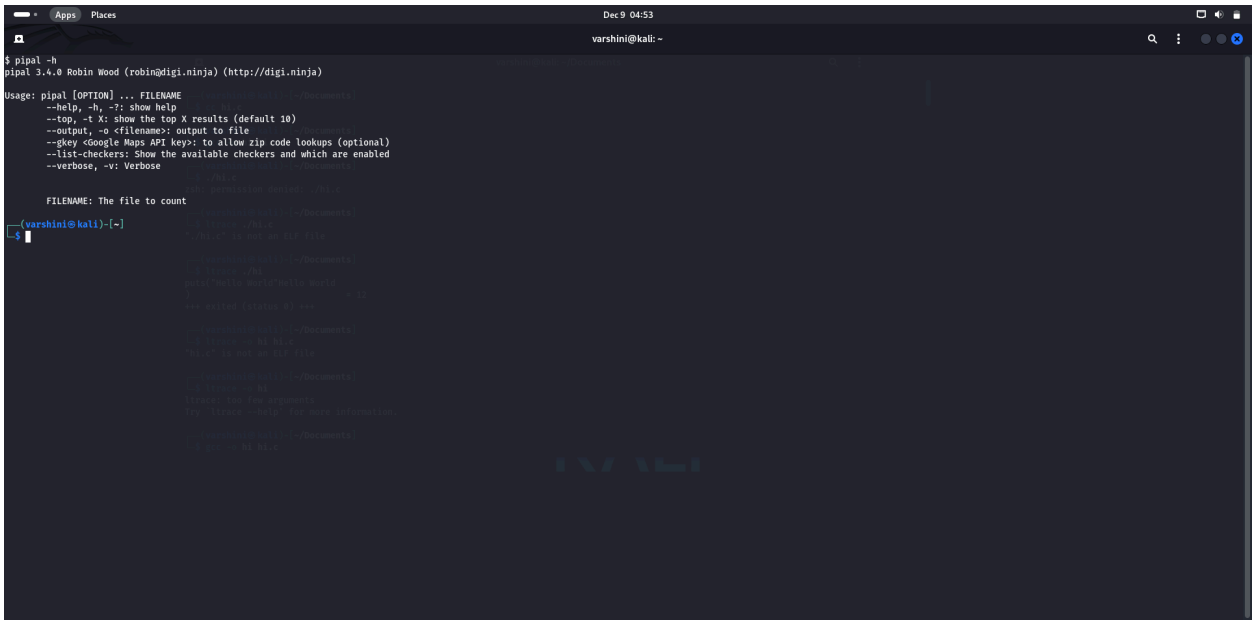
Pipal

- Pipal is a password analysis tool used for statistical analysis of password datasets.
- It is primarily designed to evaluate and report on the strength and security of passwords within a given dataset.
- Pipal analyzes large collections of passwords (typically password dumps) and generates statistical reports,

identifying common password patterns, character distributions, and password length.

Primary Use Cases:

- Password analysis: Analyzing large datasets of passwords to identify common patterns and weak passwords.
- Security audits: Evaluating the strength of passwords used within an organization by checking against common password lists and patterns.
- Cracking password hashes: Assisting in cracking hashed passwords by identifying commonly used passwords and generating wordlists for further attacks.



Social Engineering Tools

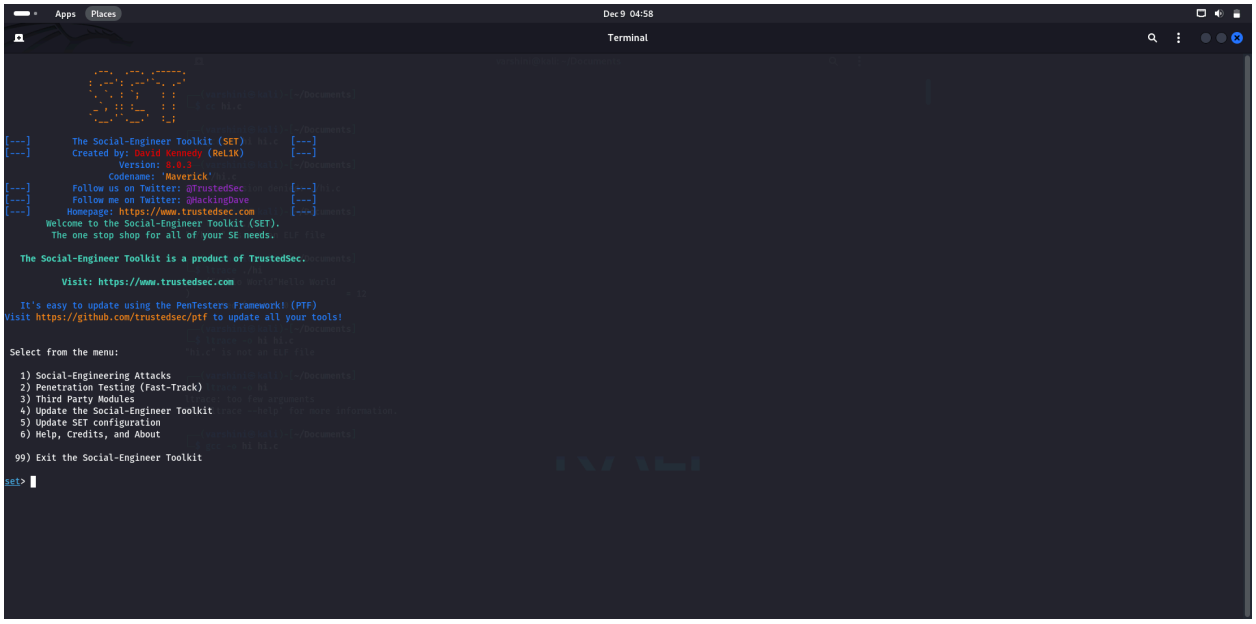
Social Engineering Toolkit:

- The Social Engineering Toolkit (SET) is an open-source penetration testing tool specifically designed for social engineering attacks.

- SET offers a wide range of attack vectors, including phishing, credential harvesting, and payload delivery mechanisms, making it a powerful tool for assessing and improving security awareness among employees.

Primary Use Cases:

- Phishing simulations: Crafting realistic phishing emails and fake websites to test if users will click on malicious links or provide credentials.
- Credential harvesting: Capturing user credentials by creating fake login pages that resemble legitimate ones.
- Penetration testing: Enhancing red team assessments by incorporating social engineering techniques.



MSF Payload Creator *(MSFvenom Payload Creator - MSFPC)*

- MSF Payload Creator (MSFPC) is a script-based tool designed to simplify the creation of Metasploit payloads.

- It acts as a wrapper for MSFvenom, making it easier to generate payloads for different platforms and attack scenarios.

Primary Use Cases:

- Generating payloads for use with the Metasploit Framework.
- Simplifying payload creation by offering an intuitive, menu-driven interface.
- Automating reverse shell and bind shell payload generation for various operating systems (Windows, Linux, macOS, Android).