

Forum:[Hack Forums](#)

Thread: [Kali Linux Guide: PT 2 \(Common Tools\)](#)

463n7 - August 25, 2023, 8:01 pm

Here is PT 2, which outlines and details some common tools used within Kali Linux. These are only just a few, as there are many tools available to use. So take the time and at the minimum, go into your OS, and glance over all of them just to see what is there.

1. Nmap:

Nmap is a powerful network scanning tool used for discovering hosts and services on a network. It helps identify open ports, detect vulnerabilities, and map network layouts.

2. Wireshark:

Wireshark is a popular packet analysis tool used for capturing and analyzing network traffic. It allows you to examine packets, filter data, and gain insights into network protocols and behavior.

3. Metasploit Framework:

Metasploit Framework is a comprehensive penetration testing tool that helps assess vulnerabilities in systems. It provides a wide range of exploits, payloads, and auxiliary modules to test network security.

4. Aircrack-ng:

Aircrack-ng is a suite of wireless network auditing tools. It helps assess the security of Wi-Fi networks by capturing packets, cracking encryption keys, conducting replay attacks, and performing various other wireless security tests.

5. John the Ripper:

John the Ripper is a powerful password cracking tool. It uses various techniques like dictionary attacks, brute force attacks, and rainbow tables to crack passwords and hashes.

6. Hydra:

Hydra is a popular password cracking tool for online services. It automates the process of trying different username and password combinations against various login pages, making it useful for testing the strength of passwords or conducting brute force attacks.

7. Burp Suite:

Burp Suite is a web application security testing tool. It helps in identifying vulnerabilities, intercepting and modifying web traffic, and performing various security tests on web applications.

8. Maltego:

Maltego is a data mining and information gathering tool. It allows you to visualize relationships and connections between people, organizations, and other entities by analyzing and mapping data from various sources.

9. WiFite:

WiFite is a wireless network auditing tool specifically designed for automated attacks against Wi-Fi networks. It simplifies the process of capturing handshakes, cracking passwords, and performing other wireless security assessments.

This is for educational purposes only, I'm not responsible for your house getting raided for the misuse of these tools.