Kali Linux tool categories

Kali Linux contains a number of tools that can be used during the penetration testing process. The penetration testing tools included in Kali Linux can be categorized into the following categories:

- **Information gathering**: This category contains several tools that can be used to gather information about DNS, IDS/IPS, network scanning, operating systems, routing, SSL, SMB, VPN, voice over IP, SNMP, e-mail addresses, and VPN.
- **Vulnerability assessment**: In this category, you can find tools to scan vulnerabilities in general. It also contains tools to assess the Cisco network, and tools to assess vulnerability in several database servers. This category also includes several fuzzing tools.
- **Web applications**: This category contains tools related to web applications such as the content management system scanner, database exploitation, web application fuzzers, web application proxies, web crawlers, and web vulnerability scanners.
- **Password attacks**: In this category, you will find several tools that can be used to perform password attacks, online or offline.
- **Exploitation tools**: This category contains tools that can be used to exploit the vulnerabilities found in the target environment. You can find exploitation tools for the network, Web, and database. There are also tools to perform social engineering attacks and find out about the exploit information.
- **Sniffing and spoofing**: Tools in this category can be used to sniff the network and web traffic. This category also includes network spoofing tools such as Ettercap and Yersinia.
- **Maintaining access**: Tools in this category will be able to help you maintain access to the target machine. You might need to get the highest privilege level in the machine before you can install tools in this category. Here, you can find tools for backdooring the operating system and web application. You can also find tools for tunneling.
- **Reporting tools**: In this category, you will find tools that help you document the penetration-testing process and results.
- **System services**: This category contains several services that can be useful during the penetration testing task, such as the Apache service, MySQL service, SSH service, and Metasploit service.

To ease the life of a penetration tester, Kali Linux has provided us with a category called **Top 10 Security Tools**. Based on its name, these are the top 10 security tools commonly used by penetration testers. The tools included in this category are `aircrack-ng` , `burp-suite` , `hydra` , `john` , `maltego` , `metasploit` , `nmap` , `sqlmap` , `wireshark` , and `zaproxy` .

Besides containing tools that can be used for the penetration testing task, Kali Linux also comes with several tools that you can use for the following:

- **Wireless attacks**: This category includes tools to attack Bluetooth, RFID/NFC, and wireless devices.
- **Reverse engineering**: This category contains tools that can be used to debug a program or disassemble an executable file.
- **Stress testing**: This category contains tools that can be used to help you in stress testing your network, wireless, Web, and VOIP environment.
- **Hardware hacking**: Tools in this category can be used if you want to work with Android and Arduino applications.
- **Forensics**: In this category, you will find several tools that can be used for digital forensics, such as acquiring a hard disk image, carving files, and analyzing the hard disk image. To use the forensics capabilities in Kali Linux properly, you need to navigate to **Kali Linux Forensics** | **No Drives or Swap Mount** in the booting menu. With this option, Kali Linux will not mount the drives automatically, so it will preserve the drives' integrity.

In this book, we are focusing only on Kali Linux's penetration testing tools.