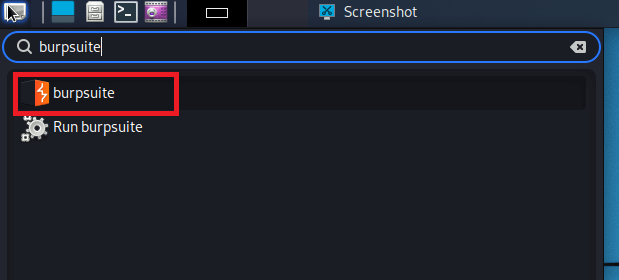
Jeeshu Das 21BPS1477

Assessment 2

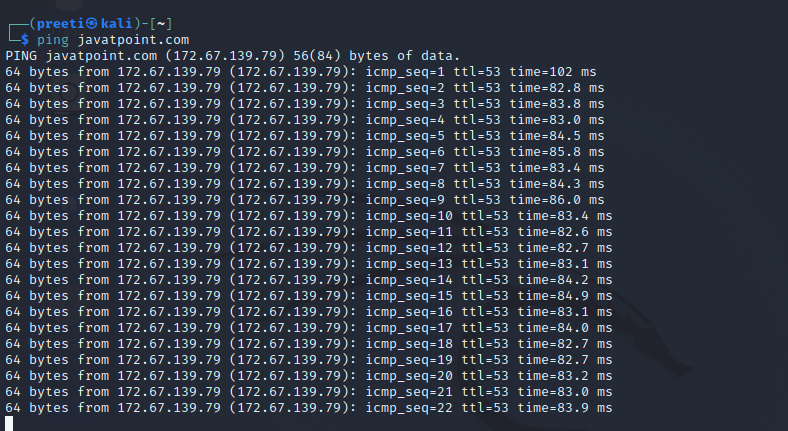
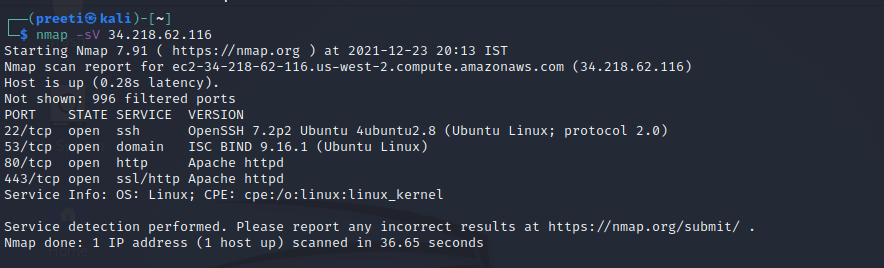
Top 10 Kali Linux tools for hacking

1. Burp Suite: One of the most widely used web application security testing tools is **Burp Suite**. It is utilized as a **proxy**, which means all requests from the proxy's browser pass via it. And, because the request runs through the **burp suite**, we can make changes to it as needed, which is useful for **testing vulnerabilities** such as **XSS** and **SQLi**, and other web-related issues.

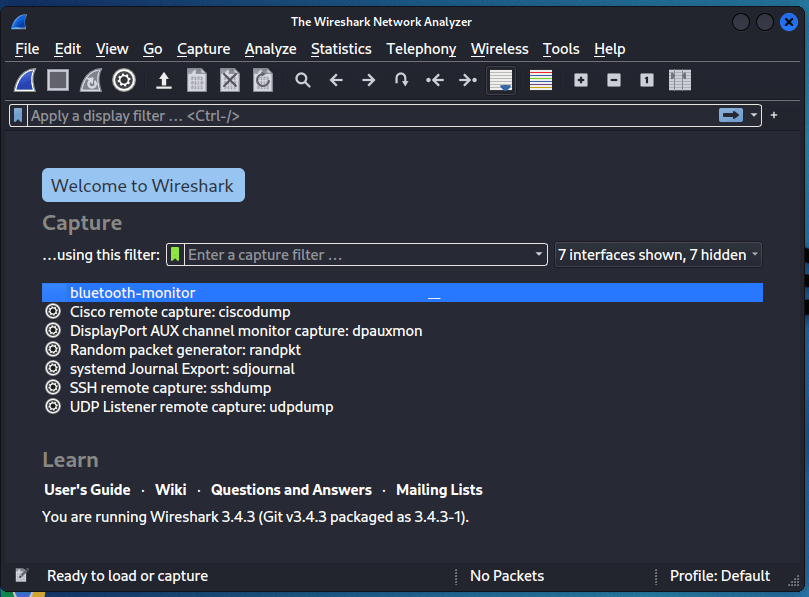


Burp suite community edition is free with Kali Linux, but there is a premium version called **burp suite professional** that has many more features than the free version.

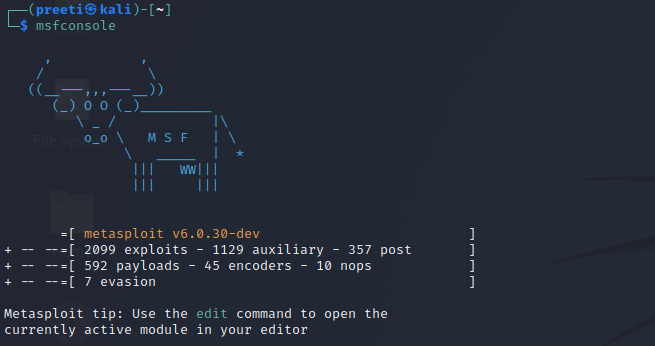
1. Nmap: Nmap is an open-source network scanner for **reconfiguring** and **scanning networks**. It is used to find ports, hosts, and services along with their versions over a network. It sends packets to the host and then examines the responses to get the intended outcomes. It might also be used to **discover hosts, detect operating systems**, and **scan for open ports**. It is one of the most widely used reconnaissance tools.

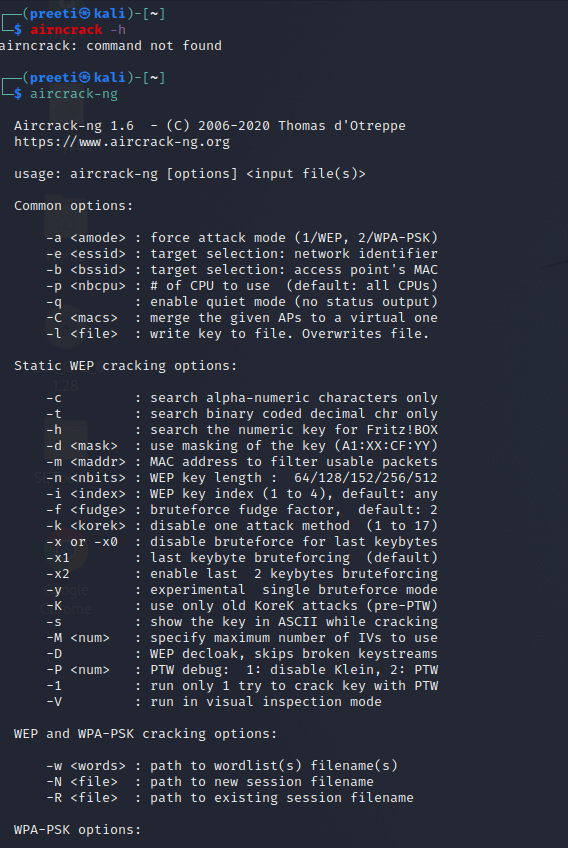
1. Wireshark: Wireshark is a network security tool that analyses and manipulates data transferred across a network. It is used to examine packets sent across a network. The source and destination IP addresses, the protocol used, the data, and the various headers may all be included in these packets. The packets usually have a ".pcap" extension and can be read using the Wireshark tool.



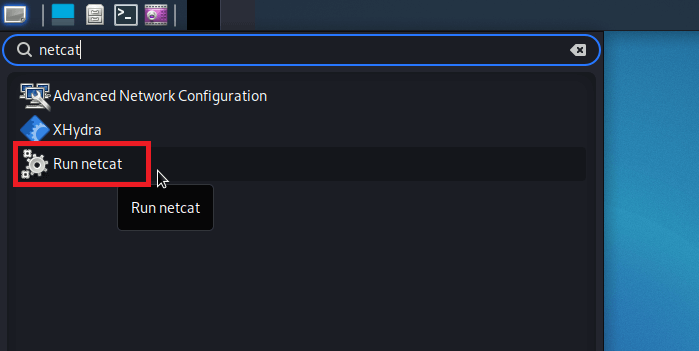
1. Metasploit Framework: Metasploit is an open-source tool that was developed by Rapid7 technologies. It is one of the most widely used penetration testing frameworks globally. It includes a large number of exploits for exploiting the vulnerabilities over a network or operating system. Metasploit is often used on local networks; however, we may utilize Metasploit for hosts over the internet using "port forwarding". Metasploit is primarily a command-line tool, but it also includes a graphical user interface (GUI) package called "Armitage" that makes using the Metasploit more convenient and feasible.



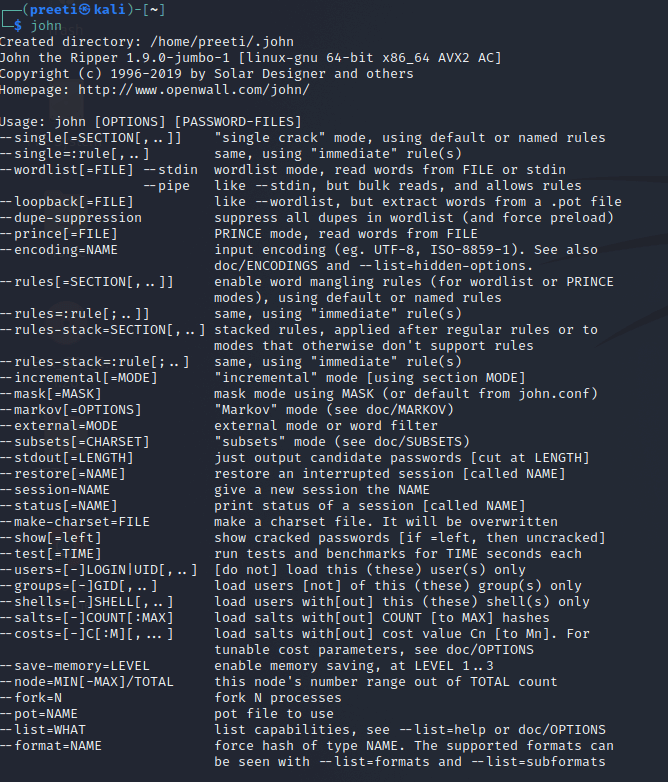
1. Air-crack: is an all-in-one packet sniffer, WEP, and WPA/WPA cracker, analysing tool and a hash capturing tool. It is a tool that is mainly used to hack WIFI. Using this, we can capture the package, and read the hashes out of them as well as the cracking of those hashes by various attacks such as dictionary attacks. It supports almost all modern wireless interfaces.



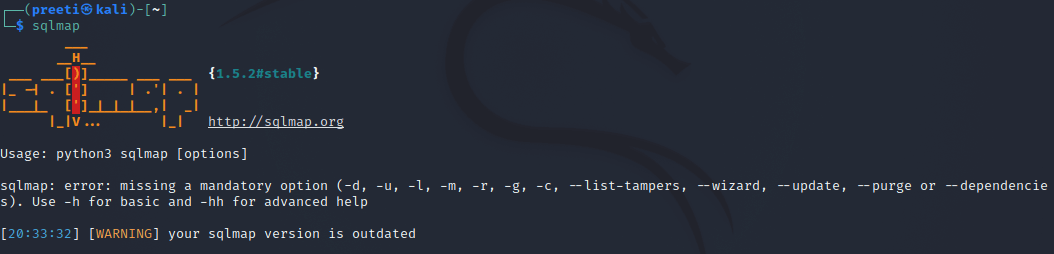
1. Netcat: Netcat is a network tool for working with ports and performs tasks such as port scanning, listening, and redirection. This command is useful for debugging and testing network daemons. This tool is known as the Swiss army knife of networking tools. It could also be used to perform TCP, UDP, or UNIX-domain sockets or to open remote connections, and much more.



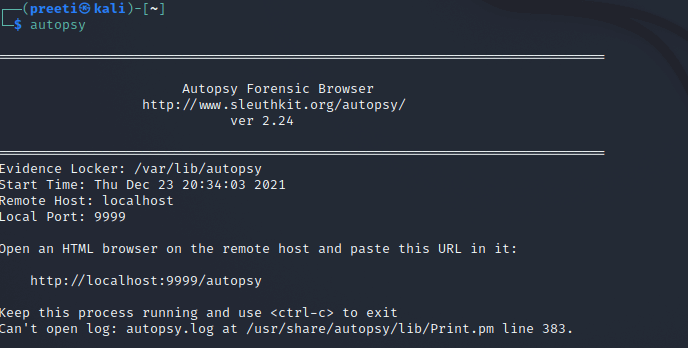
1. John the Ripper: John the Ripper is a fantastic tool for cracking passwords utilizing well-known brute-force attacks such as dictionary attacks, or custom wordlist attacks, etc. It can also be used to crack hashes or passwords for zipped or compressed files and locked files. It includes a lot of options for cracking hashes and passwords.



1. Sqlmap: One of the greatest tools for performing SQL injection attacks is sqlmap. It simply automates the process of testing a parameter for SQL injection, as well as the process of exploiting the vulnerable parameter.



1. Autopsy: An autopsy is a digital forensics tool that collects data from forensics. Or in other words, we used this tool to investigate files or logs to see what exactly was done with the system. It may also be used to recover files from a memory card or a pen drive.



1. Social Engineering Toolkit: The Social Engineering Toolkit is a set of tools which we can use to perform social engineering attacks. These tools gather information by exploiting and manipulating human behavior. It is also a fantastic tool for phishing websites. It is an open-source penetration testing framework designed for social engineering. SET includes a number of unique attack vectors that permit us to launch a convincing attack in a matter of seconds