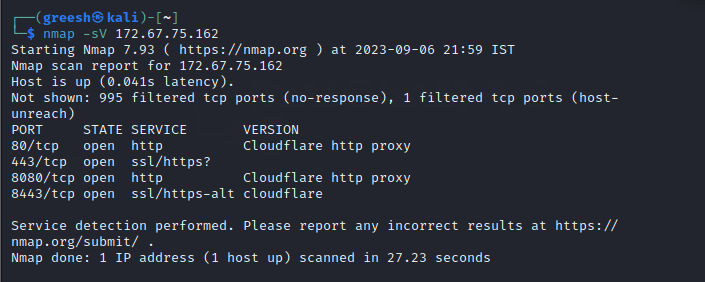
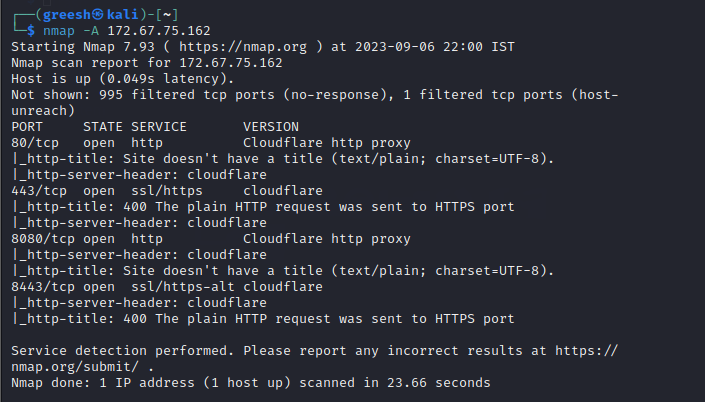
Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts and penetration testers, or in simple words, it is for those who work under the umbrella of cybersecurity and analysis.

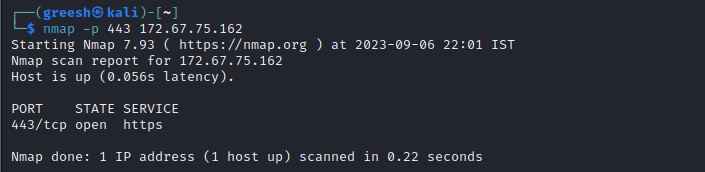
Linux tools that could save a lot of your time and effort.

1. **Nmap:**

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It is one of the most popular reconnaissance tools.

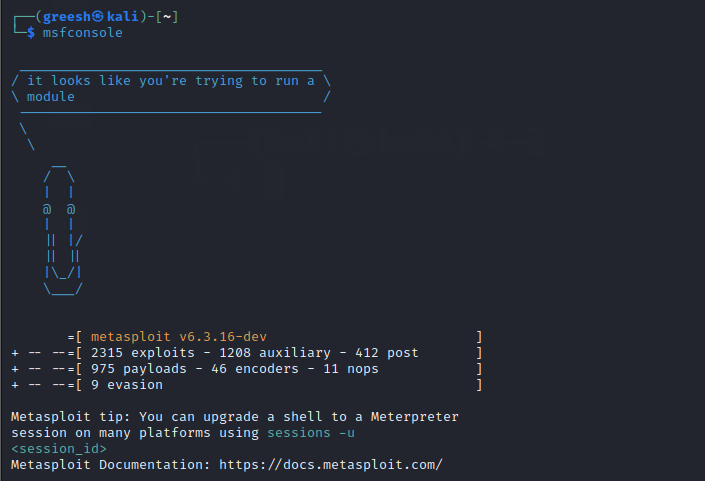


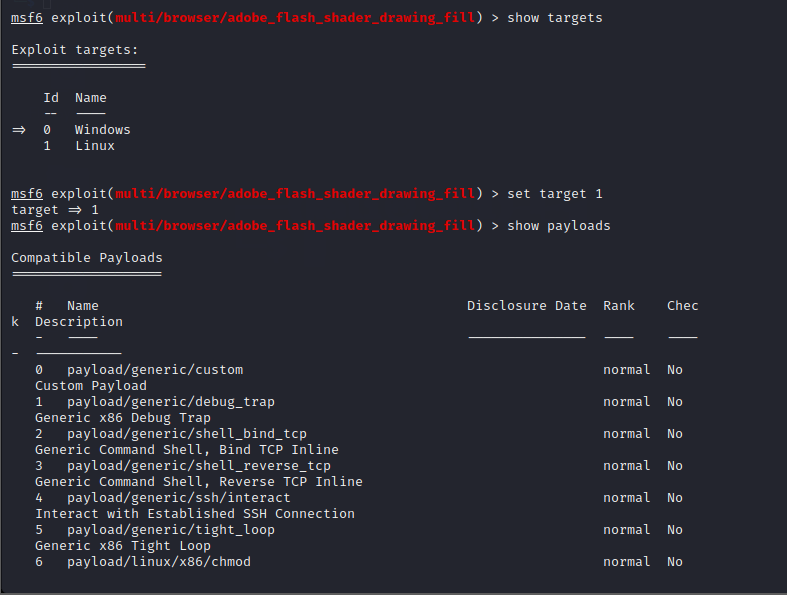
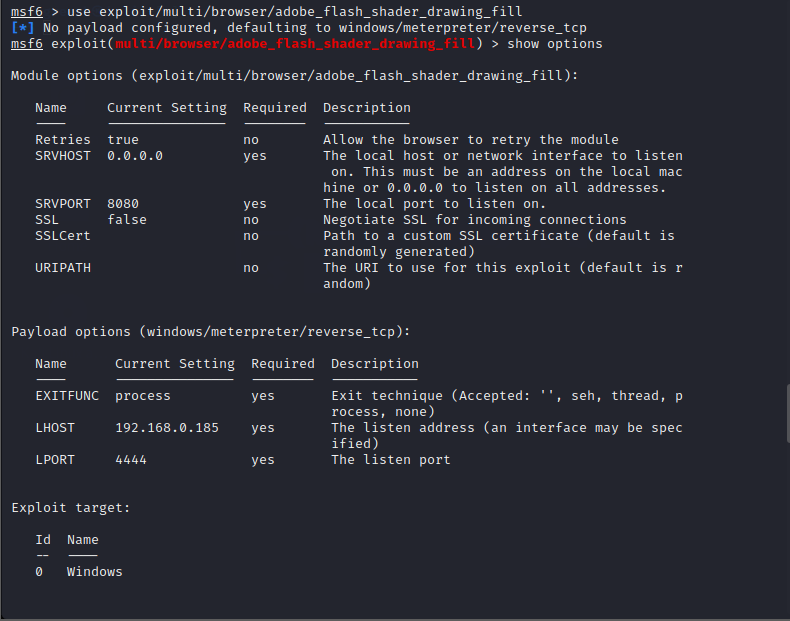




1. **Metasploit Framework:**

Metasploit is an open-source tool that was designed by Rapid7 technologies. It is one of the world’s most used penetration testing frameworks. It comes packed with a lot of exploits to exploit the vulnerabilities over a network or operating systems. Metasploit generally works over a local network but we can use Metasploit for hosts over the internet using “port forwarding “. Basically, Metasploit is a CLI-based tool but it even has a GUI package called “Armitage” which makes the use of Metasploit more convenient and feasible.

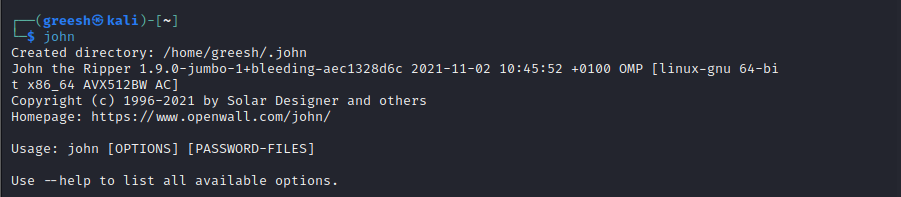




1. **John the Ripper:**

John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.

Besides several crypt (3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

****