CHAMELEON

FOR OUR SMARTER WORLD

CLI Attack Tools – Cheat Sheet

Introduction:

This is a cheat sheet written to be ran on Kali Linux for exploitation testing. As it comes with a plethora of preinstalled hacking tools. By using VirtualBox and installing Kali Linux. I was able to test and run the preinstalled programs using Linux's CLI. Below is the list of CLI attack tools we can use for testing.

Programs mentioned:

- Nmap

  Nmap is a useful tool for network scanning, we can discover hosts and services on a network.

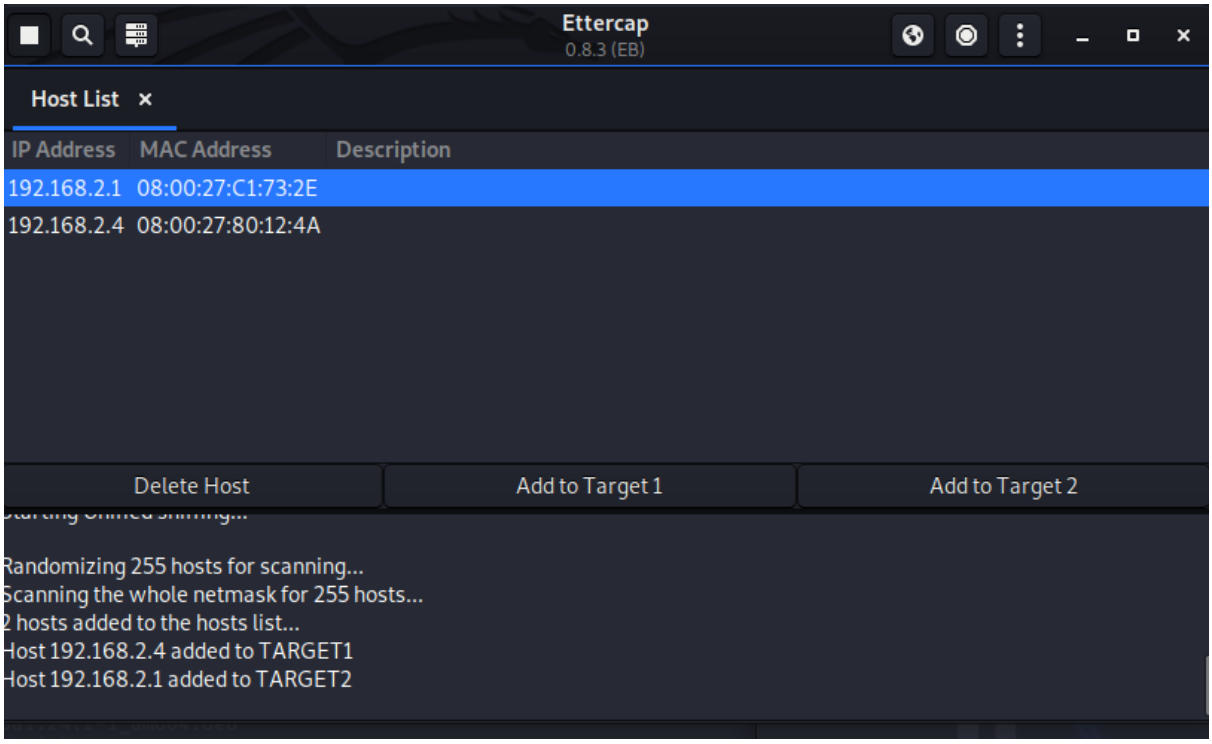
  - Basic Scan: **nmap <target>**
  - OS Detection: **nmap -0 <target>**
  - UDP Scan: **namp -sU <target>**
  - Service version detection: **namp -sV <target>**

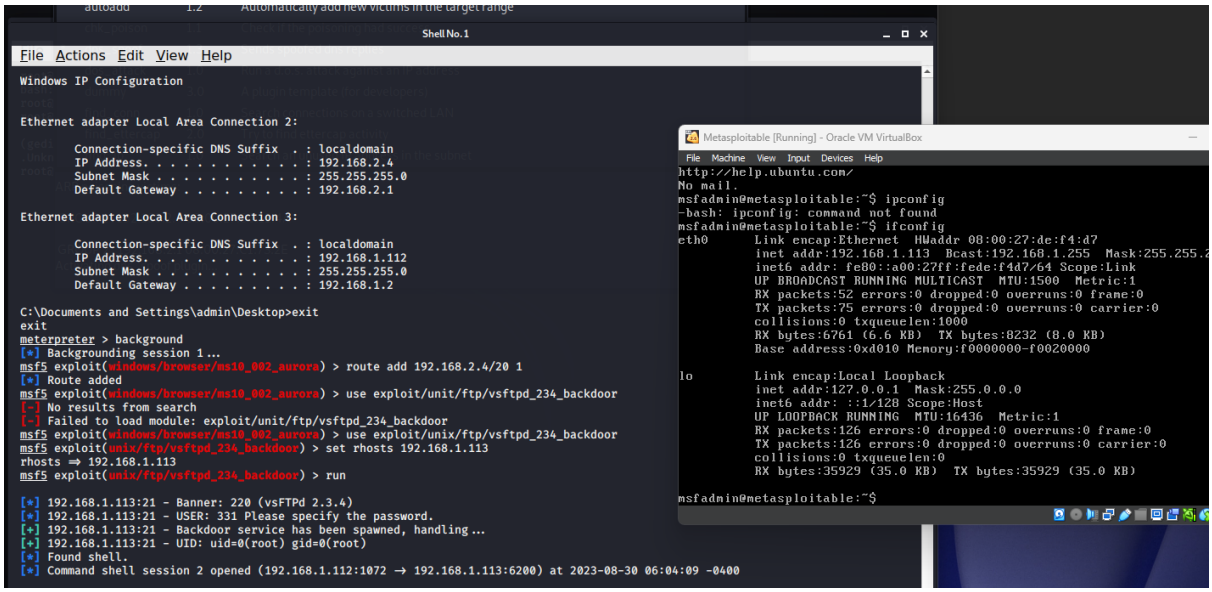
- Metasploit

  Metasploit is a powerful penetration testing framework. It allows us to test exploit and vulnerabilities in Chameleon.

  - Launch Metasploit: **msfconsole**
  - Search exploits: **search**
  - Display User ID: **getuid**
  - Access Content of password file: **hashdump**
  - Display all privileges: **getprivs**
  - Set payload: **set PLAYLOAD <playload>**

Example of Metasploit



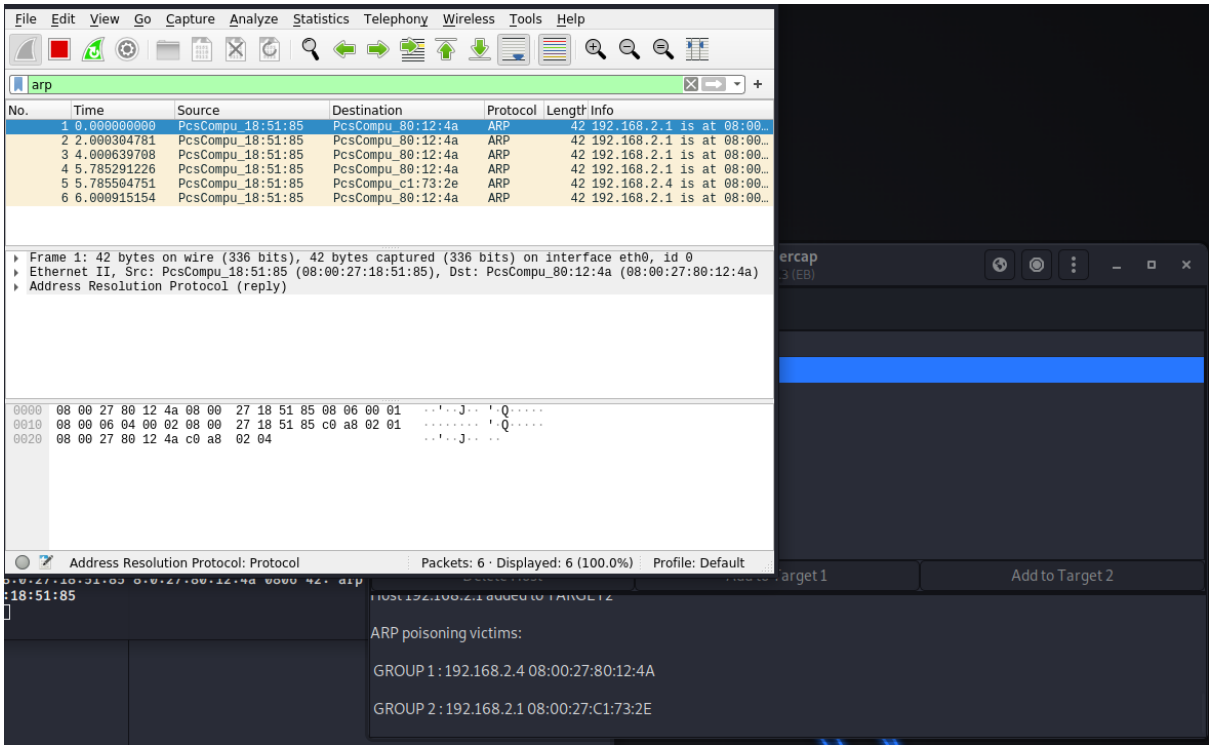


This shows how the attack is managed to attack a different computer finding their IP address then setting a Playload to their PC. Then it ran a loopback script.

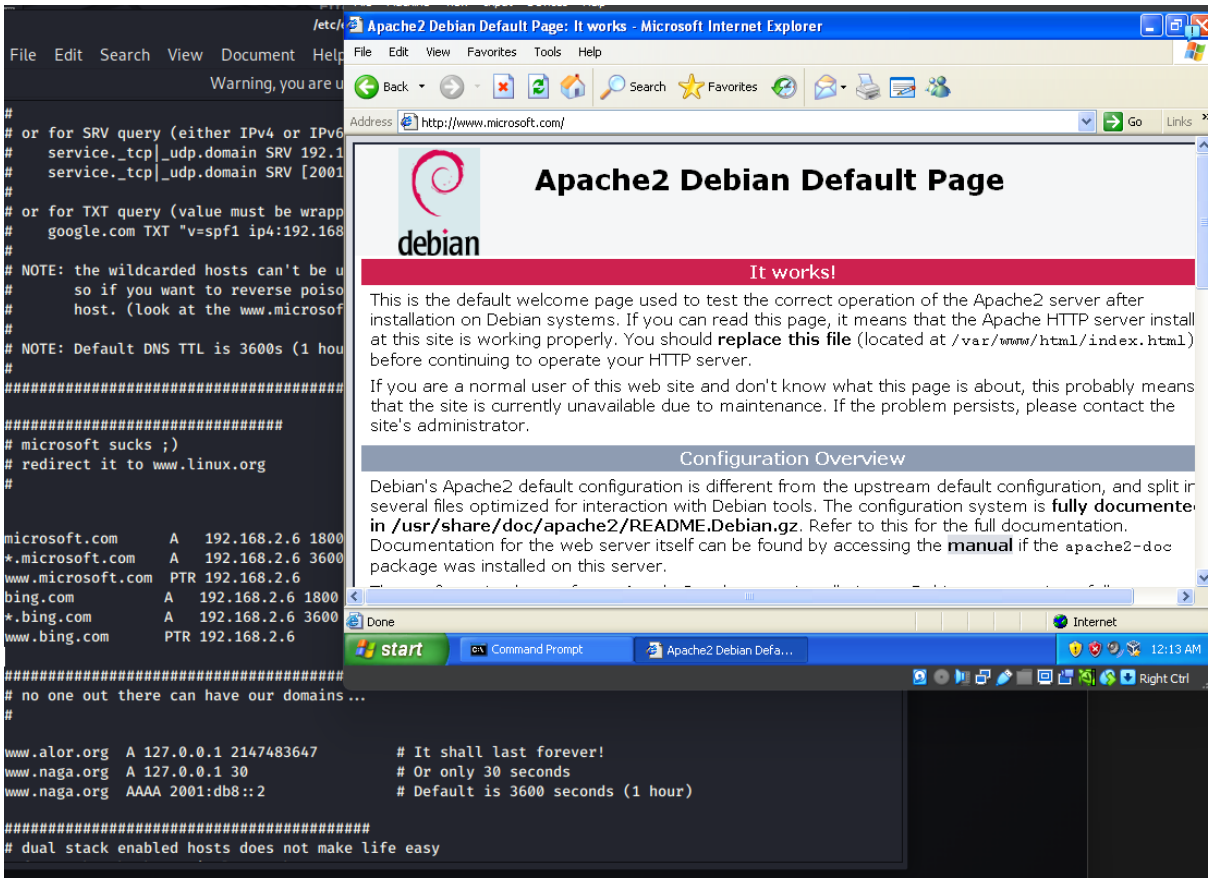
- Wireshark

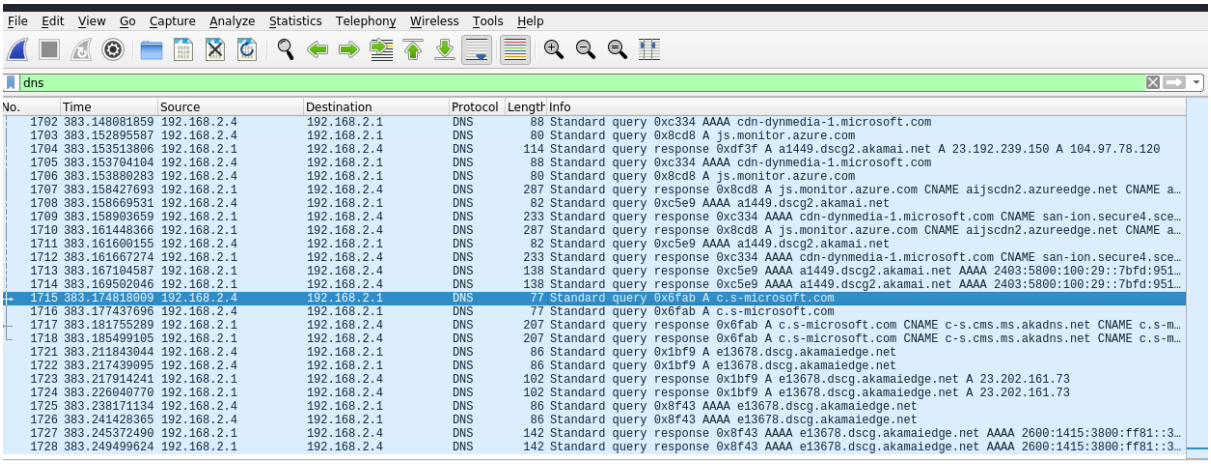
  Wireshark is a common network protocol analyser. It can be used for network troubleshooting, analysis, and protocol development.

  - Capturing Packets: **wireshark -i**
  - Filtering Packets: **wireshark -i <filter_expression> (eg. Tcp)**
  - Export capture session: **wireshark -r**



In this screenshot you can see how APR poisoning attack is active shown in Wireshark. It shows how DNS can be spoofed in the next two screenshots.





- John the Ripper

John the Ripper is a commonly used tool for password cracking. We can use this to test Chameleon password encryption algorithms

- Download John the Ripper: git clone https://github.com/magnumripper/JohnTheRippper - b bleeding - jumbo
- Wordlist cracking: ./john –worldlist=password.lst hasfile
- Brute force crack: ./john –incremental hasfile
- Loopback wordlist: ./john –loopback hasfile

Conclusion:

Listed are the most used tools for exploitation testing. There are more tools can be added if any team members specific new testing tools. All tools are testing on a VM running Kali Linux to ensure legal precautions and cyber security safety.