



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.

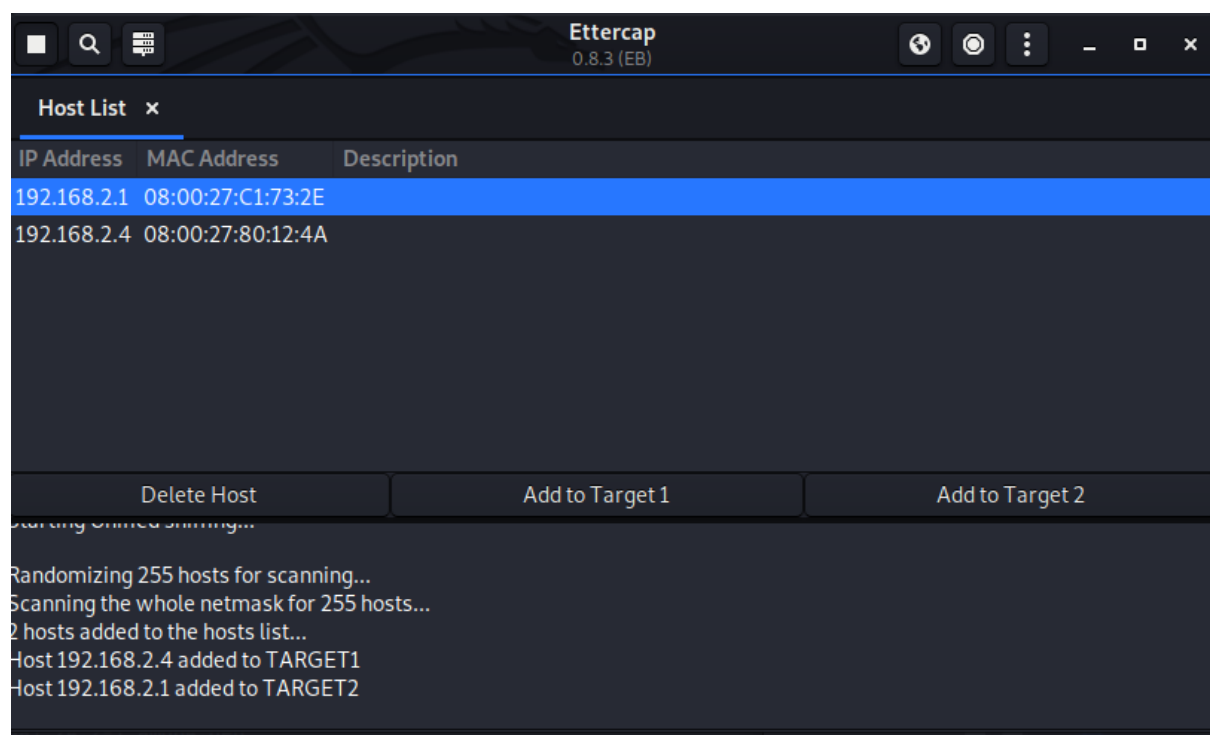
- Basic Scan: **nmap <target>**
- OS Detection: **nmap -O <target>**
- UDP Scan: **nmap -sU <target>**
- Service version detection: **nmap -sV <target>**

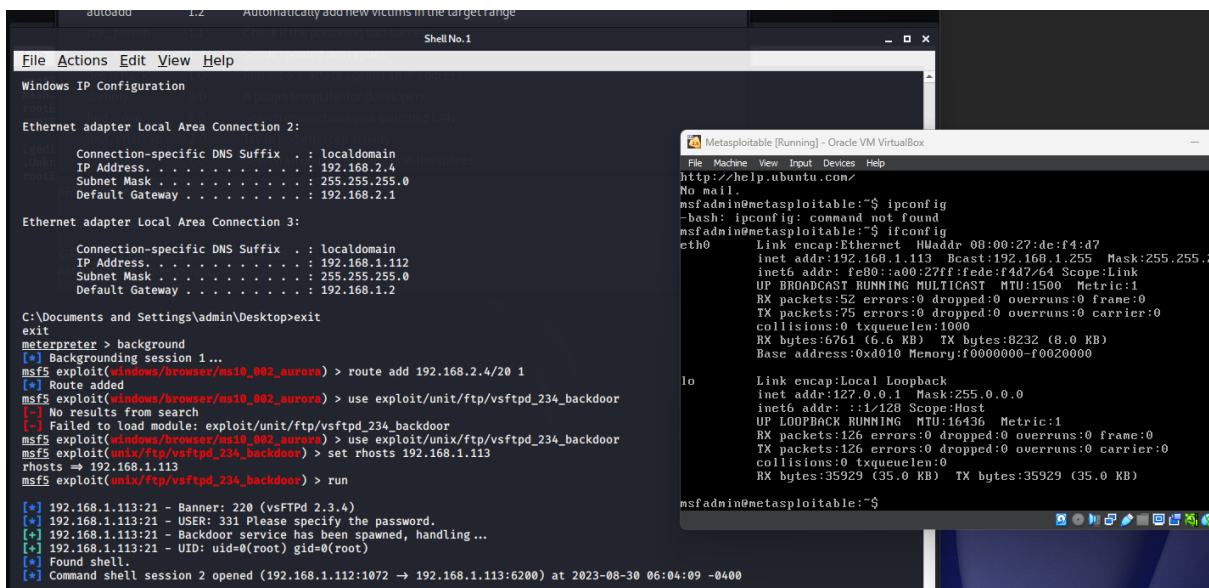
- Metasploit

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 PAYLOAD <payload>**

Example of Metasploit



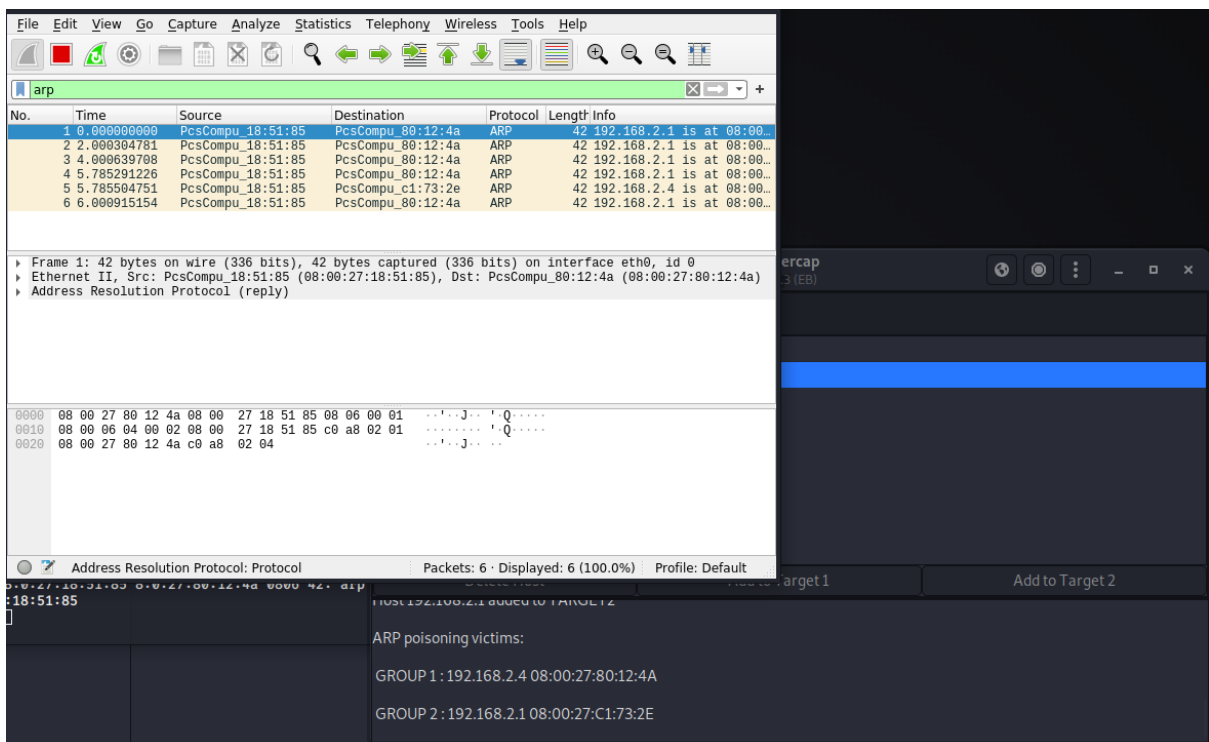


This shows how the attack is managed to attack a different computer finding their IP address then setting a Payload to their PC. Then it ran a loopback script.

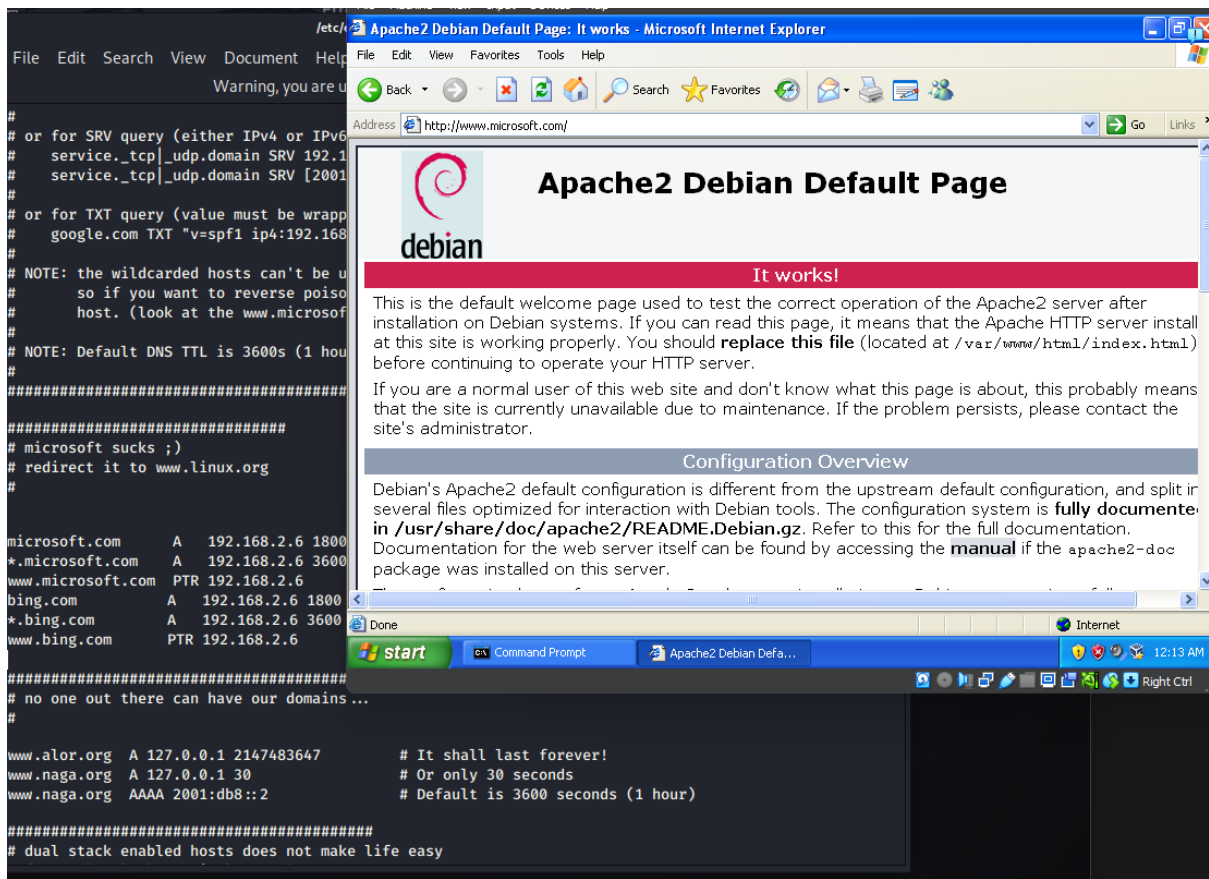
- Wireshark

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.



No.	Time	Source	Destination	Protocol	Length	Info
1702	383.148081859	192.168.2.4	192.168.2.1	DNS	88	Standard query 0xc334 AAAA cdn-dynmedia-1.microsoft.com
1703	383.152895587	192.168.2.4	192.168.2.1	DNS	88	Standard query 0x8cd8 A js.monitor.azure.com
1704	383.153513806	192.168.2.1	192.168.2.4	DNS	114	Standard query response 0xdf3f A a1449.dscg2.akamai.net A 23.192.239.150 A 104.97.78.120
1705	383.153704104	192.168.2.4	192.168.2.1	DNS	88	Standard query 0xc334 AAAA cdn-dynmedia-1.microsoft.com
1706	383.153880283	192.168.2.4	192.168.2.1	DNS	88	Standard query 0x8cd8 A js.monitor.azure.com
1707	383.158427693	192.168.2.1	192.168.2.4	DNS	287	Standard query response 0x8cd8 A js.monitor.azure.com CNAME aijscdn2.azureedge.net CNAME a...
1708	383.158669531	192.168.2.4	192.168.2.1	DNS	82	Standard query 0xc5e9 AAAA a1449.dscg2.akamai.net
1709	383.158903659	192.168.2.1	192.168.2.4	DNS	233	Standard query response 0xc334 AAAA cdn-dynmedia-1.microsoft.com CNAME san-ion.secure4.sce...
1710	383.161448366	192.168.2.1	192.168.2.4	DNS	287	Standard query response 0x8cd8 A js.monitor.azure.com CNAME aijscdn2.azureedge.net CNAME a...
1711	383.161600155	192.168.2.4	192.168.2.1	DNS	82	Standard query 0xc5e9 AAAA a1449.dscg2.akamai.net
1712	383.161667274	192.168.2.1	192.168.2.4	DNS	233	Standard query response 0xc334 AAAA cdn-dynmedia-1.microsoft.com CNAME san-ion.secure4.sce...
1713	383.167104587	192.168.2.1	192.168.2.4	DNS	138	Standard query response 0xc5e9 AAAA a1449.dscg2.akamai.net AAAA 2403:5800:100:29::7bfd:951...
1714	383.169502046	192.168.2.1	192.168.2.4	DNS	138	Standard query response 0xc5e9 AAAA a1449.dscg2.akamai.net AAAA 2403:5800:100:29::7bfd:951...
1715	383.174316069	192.168.2.4	192.168.2.1	DNS	77	Standard query 0x6fab A c.s-microsoft.com
1716	383.177431696	192.168.2.4	192.168.2.1	DNS	77	Standard query 0x6fab A c.s-microsoft.com
1717	383.181755289	192.168.2.1	192.168.2.4	DNS	207	Standard query response 0x6fab A c.s-microsoft.com CNAME c.s.cms.ms.akadns.net CNAME c.s-m...
1718	383.185499105	192.168.2.1	192.168.2.4	DNS	207	Standard query response 0x6fab A c.s-microsoft.com CNAME c.s.cms.ms.akadns.net CNAME c.s-m...
1721	383.211843044	192.168.2.4	192.168.2.1	DNS	86	Standard query 0x1bf9 A e13678.dscg.akamaiedge.net
1722	383.217439995	192.168.2.4	192.168.2.1	DNS	86	Standard query 0x1bf9 A e13678.dscg.akamaiedge.net
1723	383.217914241	192.168.2.1	192.168.2.4	DNS	102	Standard query response 0x1bf9 A e13678.dscg.akamaiedge.net A 23.202.161.73
1724	383.226040770	192.168.2.1	192.168.2.4	DNS	102	Standard query response 0x1bf9 A e13678.dscg.akamaiedge.net A 23.202.161.73
1725	383.238171134	192.168.2.4	192.168.2.1	DNS	86	Standard query 0x8f43 AAAA e13678.dscg.akamaiedge.net
1726	383.241428365	192.168.2.4	192.168.2.1	DNS	86	Standard query 0x8f43 AAAA e13678.dscg.akamaiedge.net
1727	383.245372490	192.168.2.1	192.168.2.4	DNS	142	Standard query response 0x8f43 AAAA e13678.dscg.akamaiedge.net AAAA 2600:1415:3800:ff81::3...
1728	383.249499624	192.168.2.1	192.168.2.4	DNS	142	Standard query response 0x8f43 AAAA e13678.dscg.akamaiedge.net AAAA 2600:1415:3800:ff81::3...

- 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/JohnTheRipper> - b bleeding - jumbo
- Wordlist cracking: ./john --wordlist=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.