FINAL REPORT

Cyber Security Tools (MP-11)

Submitted By:

Anirudh Kumar Kushwaha
181500093
B. Tech CSE – 3K

Submitted To:

Mr. Piyush Vashishth

Problem Statement

Over the years, the term Cyber Security has gained much importance and become a common part of each one's life who is associated with a computer or a smartphone device.
When people submit their data online, it becomes vulnerable to cyber-attacks or cyber-crimes. Moreover, cyber-attacks can happen over an external facing DNS server or an internal firewall, which in turn effects the data and infrastructure within the enterprise that inherently causes significant damage to the business of the associated organization.

Cyber Security involves protecting key information and devices from cyber threats. Lot of money are invested in protecting all this information in an online platform. With the number of people accessing the information online increasing each day, threats to the information are also increasing, with the cost of online crimes estimated in billions.

Objective of this Project

This project will be combination of various tools such as: -

- MAC Changer
- Network Scanner
- ARP Spoofer
- Web Crawler
- Web Spider

Tools mentioned are fully interactive

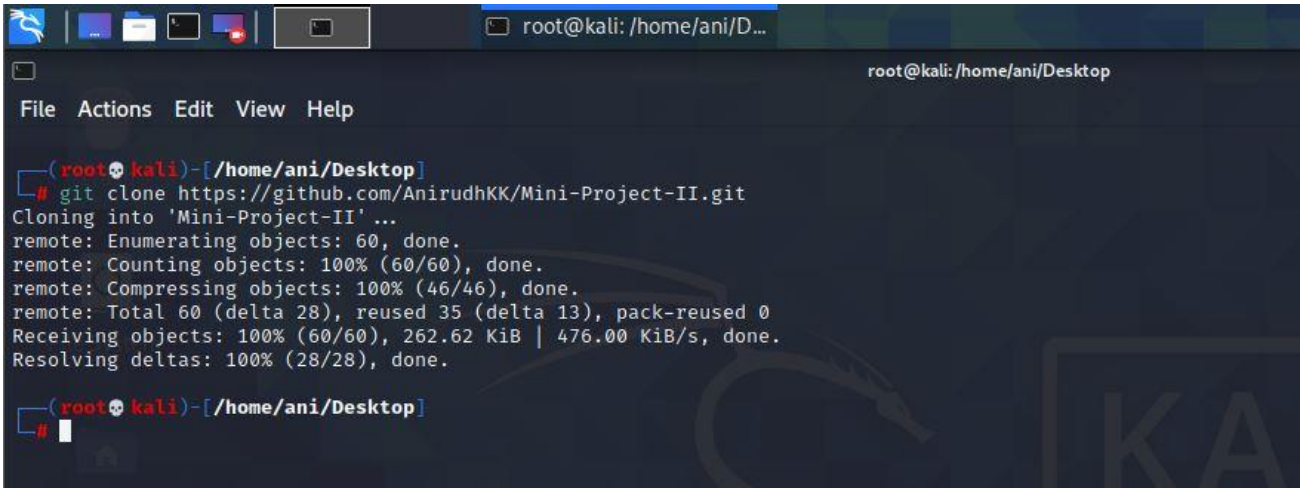
Methodology

Each tool will have their own independent implementation

- MAC Changer – ifconfig
- Network Scanner – Pinging all IPs
- ARP Spoofer – Spoofed Packets
- Web Crawler – GET requests on a list of sub-domains
- Web Spider – Extracting links for Pages and further traversing.

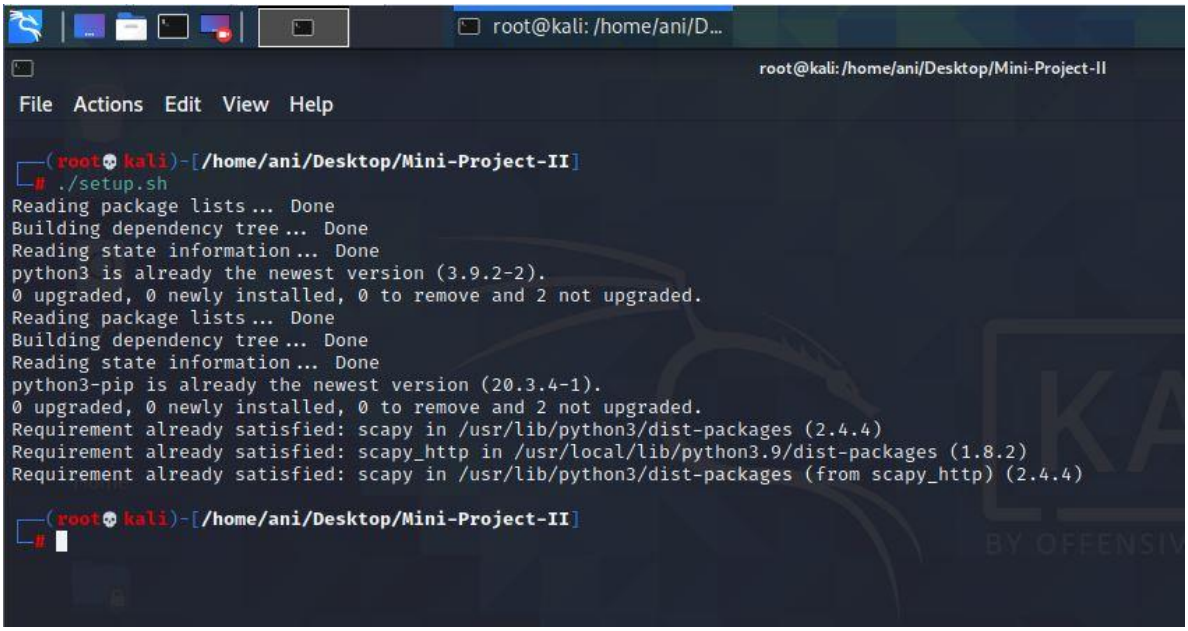
Getting Started

1. Cloning the repo



2. Giving ‘executable’ permission to the setup.sh script

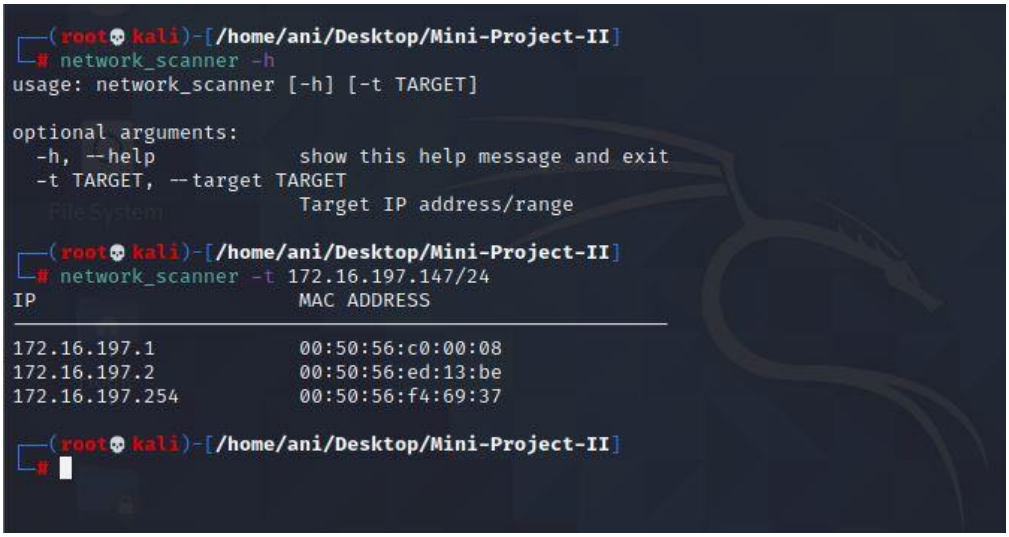
3. Letting the script install the required dependencies



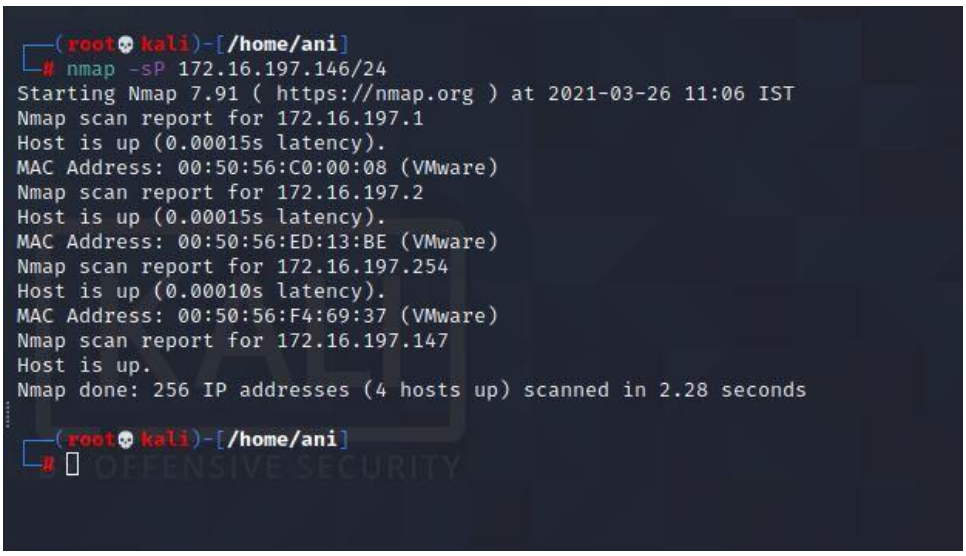
After it has completed you are ready to run your tools.

Tools

1. Network Scanner :



It takes an IP range and pings them all for active hosts. Results were crossed checked with Nmap.



2. MAC Changer :

```
┌──(root💀kali)-[/home/ani/Desktop/Mini-Project-II]
└─# mac_changer -h
Usage: mac_changer [options]

Options:
  -h, --help            show this help message and exit
  -i INTERFACE, --interface=INTERFACE
                        Interface name to change MAC Address for
  -m NEW_MAC_ADDRESS, --mac=NEW_MAC_ADDRESS
                        New MAC address you want

┌──(root💀kali)-[/home/ani/Desktop/Mini-Project-II]
└─#
```

Changes MAC address for specified network interface.

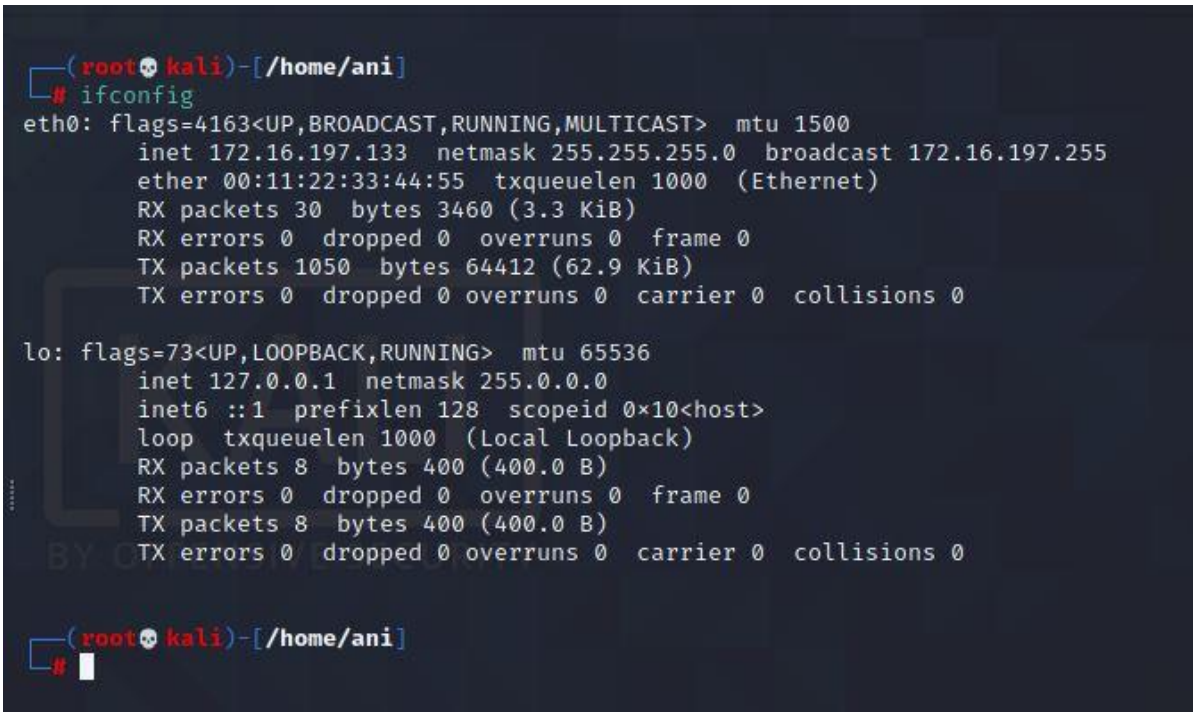
```
┌──(root💀kali)-[/home/ani]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.197.147  netmask 255.255.255.0  broadcast 172.16.197.255
        inet6 fe80::20c:29ff:fed7:efcd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d7:ef:cd  txqueuelen 1000  (Ethernet)
        RX packets 21  bytes 2070 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1043  bytes 63172 (61.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

(before)

Changing MAC for “eth0” to “00:11:22:33:44:55”

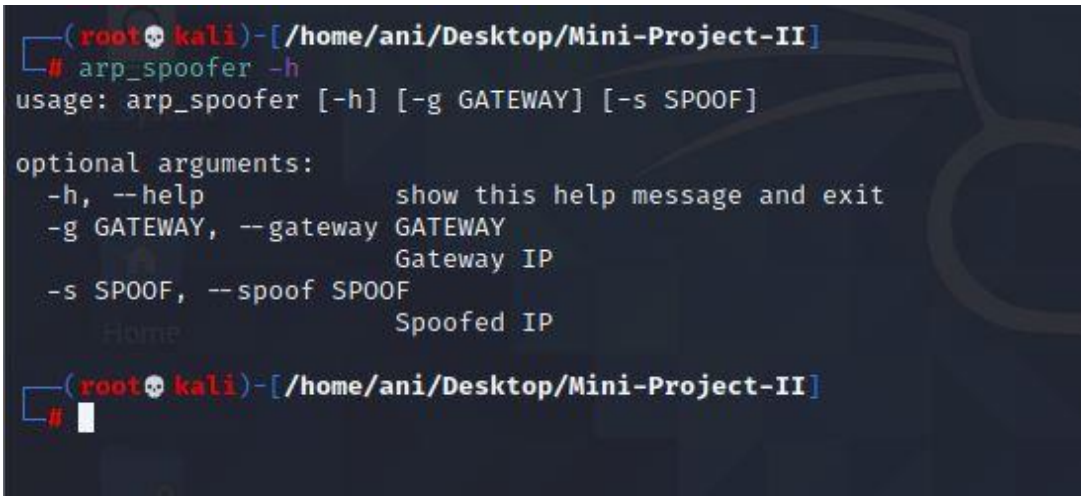
```
┌──(root💀kali)-[/home/ani/Desktop/Mini-Project-II]
└─# mac_changer -i eth0 -m 00:11:22:33:44:55
[+] Changing MAC address for eth0 to 00:11:22:33:44:55
[+] MAC address changed to 00:11:22:33:44:55

┌──(root💀kali)-[/home/ani/Desktop/Mini-Project-II]
└─#
```

Checking MAC now



As we can see, the MAC address has been successfully changed.

3. ARP Spoofer :



Arp spoofer continuously sends spoofed packets to the gateway IP and the victim IP (spoofed IP)

After receiving Keyboard Interrupt, it restores the ARP tables automatically.

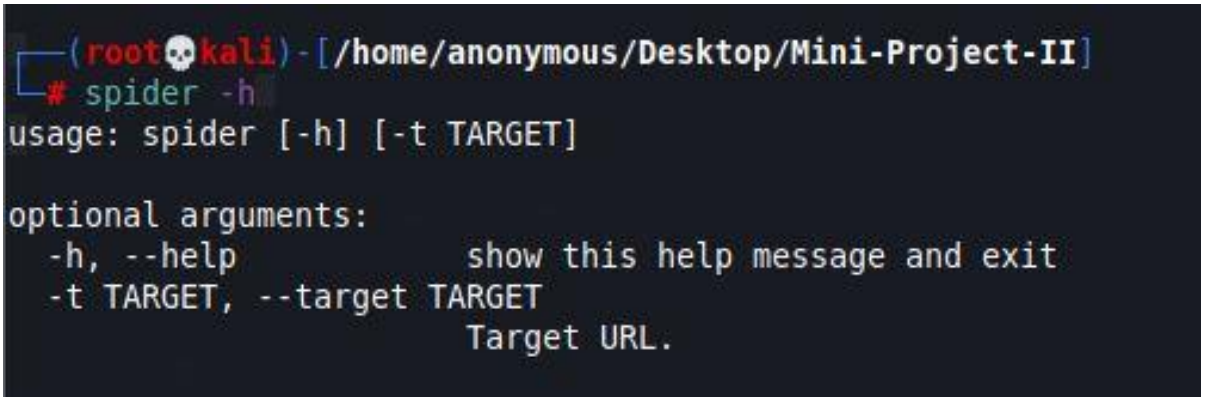
4. Web Crawler :

```
┌──(root💀kali)-[/home/anonymous/Desktop/Mini-Project-II]
└─# crawler -h
usage: crawler [-h] [-t TARGET] [-w WORDLIST] [-s]

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        Target URL.
  -w WORDLIST, --wordlist WORDLIST
                        Full path to the wordlist to use.
  -s                    The site uses HTTPS rather than simple HTTP.
```

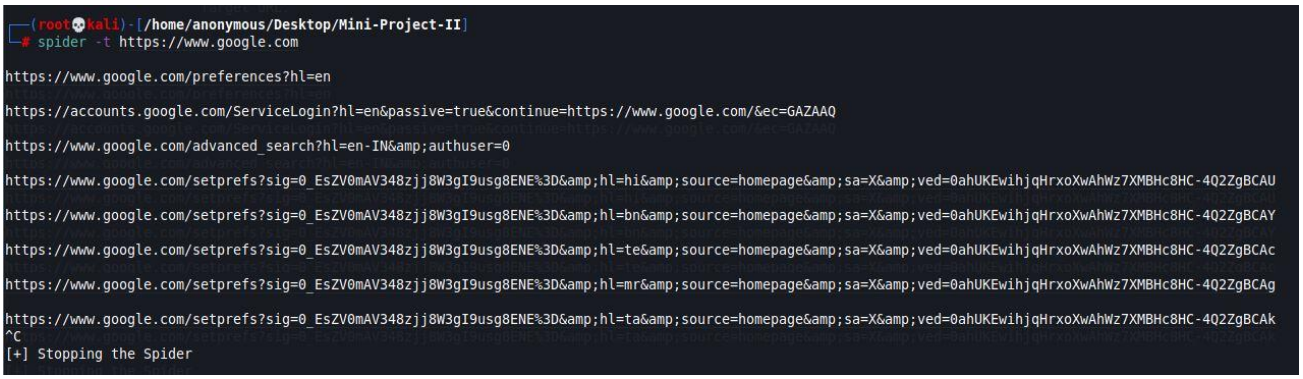
The script uses a subdomain wordlist and sends HTTP GET requests on the resultant URL. Furthermore, it extracts link from those working URLs.

```
┌──(root💀kali)-[/home/anonymous/Desktop/Mini-Project-II]
└─# crawler -t google.com -w ./subdomain.txt -s

----------------------LINKS FOR mail.google.com-------------------------
https://accounts.google.com/signin/usernamerecovery?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&amp;service=mail&amp;ss=1&amp;scc=1&amp;rm=false&amp;osid=1&amp;ltmpl=default&amp;hl=en-GB

https://accounts.google.com/AccountChooser?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&amp;service=mail&amp;rm=false&amp;ltmpl=default&amp;scc=1&amp;ss=1&amp;osid=1&amp;emr=1

https://accounts.google.com/SignUp?service=mail&amp;continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&amp;ltmpl=default

https://www.google.com/intl/en-GB/about

https://accounts.google.com/TOS?loc=IN&hl=en-GB&privacy=true

https://accounts.google.com/TOS?loc=IN&hl=en-GB

http://www.google.com/support/accounts?hl=en-GB

----------------------LINKS FOR www.google.com-------------------------
https://play.google.com/?hl=en&tab=w8
```

5. Web Spider :



It extracts links from a given target website and keeps traversing them and finding new and unique links.



Conclusion

Making this project was fun and learning. I came to know about various concepts of Networking as well as Ethical Hacking. Although, there are pre-built versions of these apps but making them from scratch gave me a chance to get to know these tools deeply.

I would also like to thank my mentor Mr. Piyush Vashishth for giving me this opportunity to work on such an amazing project.