



MID-TERM 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

Tools mentioned above will be 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

Progress

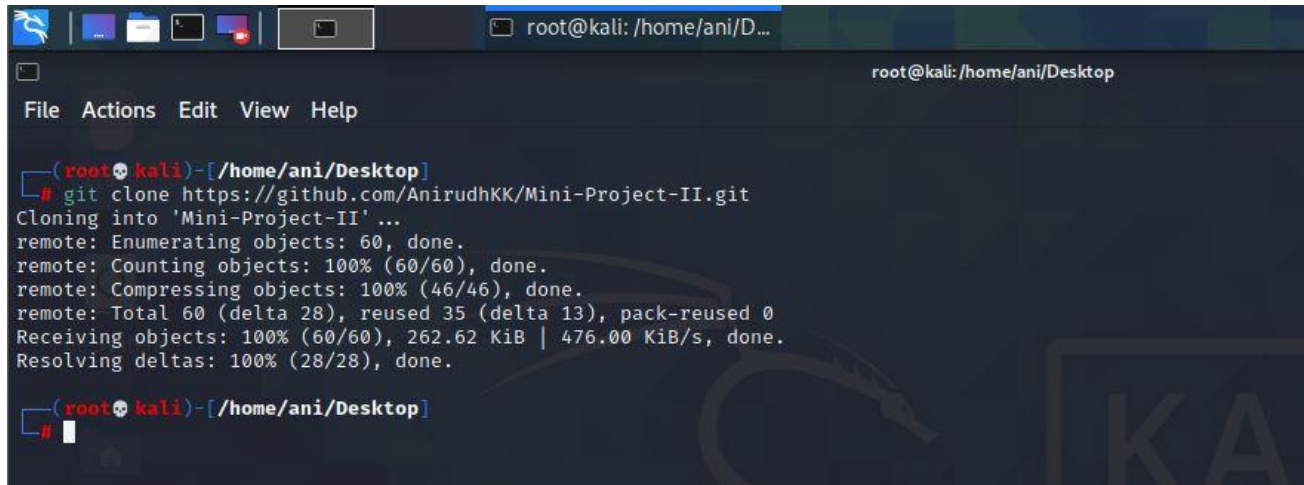
Three out four scripts have been completed so far including MAC Changer, Network Scanner and ARP Spoofer.

A setup shell script is also provided to make the installation easier. The script automatically installs all the dependencies and allows the user to directly run the tool without using the “python3” prefix.

Tools themselves are well elaborated and have a “-h” option available that gives more information about the tool and even tells about the options a user can enter.

Getting Started


1. Cloning the repo

A terminal window on a Kali Linux system. The prompt is root@kali: /home/ani/Desktop. The user runs the command 'git clone https://github.com/AnirudhKK/Mini-Project-II.git'. The output shows the cloning process: 'Cloning into 'Mini-Project-II' ...', 'remote: Enumerating objects: 60, done.', 'remote: Counting objects: 100% (60/60), done.', 'remote: Compressing objects: 100% (46/46), done.', 'remote: Total 60 (delta 28), reused 35 (delta 13), pack-reused 0', 'Receiving objects: 100% (60/60), 262.62 KiB | 476.00 KiB/s, done.', and 'Resolving deltas: 100% (28/28), done.' The prompt returns to root@kali: /home/ani/Desktop.

```
(root@kali)-[/home/ani/Desktop]
# git clone https://github.com/AnirudhKK/Mini-Project-II.git
Cloning into 'Mini-Project-II' ...
remote: Enumerating objects: 60, done.
remote: Counting objects: 100% (60/60), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 60 (delta 28), reused 35 (delta 13), pack-reused 0
Receiving objects: 100% (60/60), 262.62 KiB | 476.00 KiB/s, done.
Resolving deltas: 100% (28/28), done.

(root@kali)-[/home/ani/Desktop]
```

2. Giving 'executable' permission to the setup.sh script

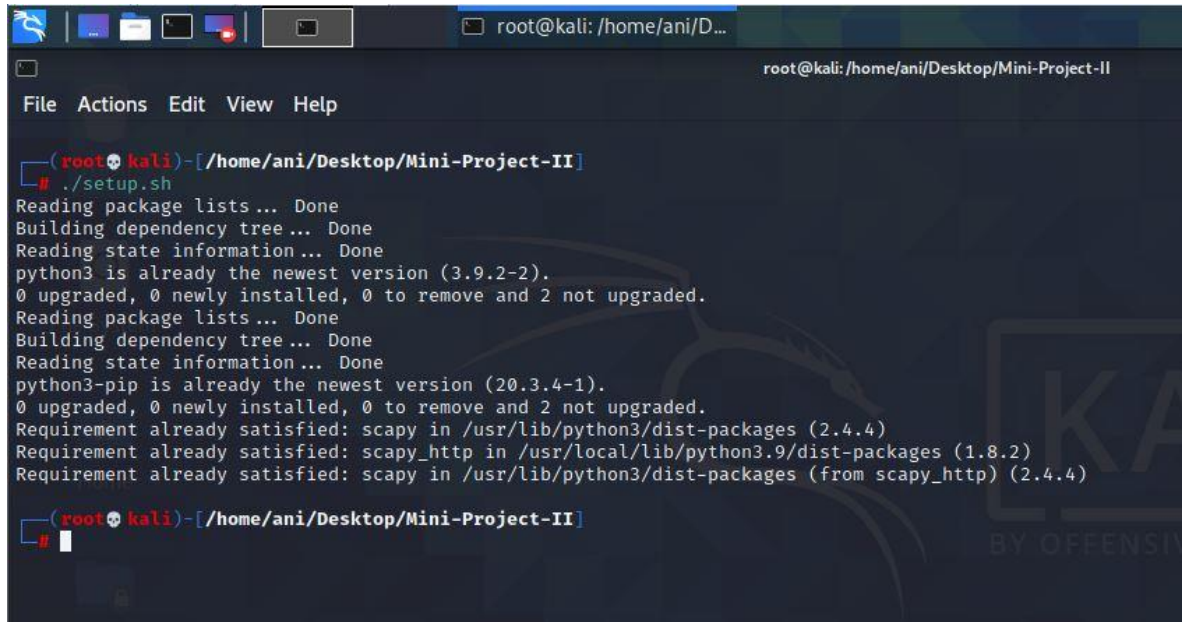
A terminal window on a Kali Linux system. The prompt is root@kali: /home/ani/Desktop. The user runs the command 'cd Mini-Project-II'. The prompt changes to root@kali: /home/ani/Desktop/Mini-Project-II. The user then runs the command 'chmod +x setup.sh'. The prompt returns to root@kali: /home/ani/Desktop/Mini-Project-II.

```
(root@kali)-[/home/ani/Desktop]
# cd Mini-Project-II

(root@kali)-[/home/ani/Desktop/Mini-Project-II]
# chmod +x setup.sh

(root@kali)-[/home/ani/Desktop/Mini-Project-II]
```

3. Letting the script install the required dependencies

A terminal window on a Kali Linux system. The window title is 'root@kali: /home/ani/Desktop/Mini-Project-II'. The terminal shows the execution of a script './setup.sh'. The output indicates that python3 and python3-pip are already at their latest versions. It also shows that the requirements for 'scapy' and 'scapy_http' are already satisfied in the system's package lists. The prompt returns to the user after the script finishes.

```
(root@kali)-[/home/ani/Desktop/Mini-Project-II]
# ./setup.sh
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.9.2-2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-pip is already the newest version (20.3.4-1).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Requirement already satisfied: scapy in /usr/lib/python3/dist-packages (2.4.4)
Requirement already satisfied: scapy_http in /usr/local/lib/python3.9/dist-packages (1.8.2)
Requirement already satisfied: scapy in /usr/lib/python3/dist-packages (from scapy_http) (2.4.4)

(root@kali)-[/home/ani/Desktop/Mini-Project-II]
#
```

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

Tools

1. Network Scanner :

```
(root@kali)~[/home/ani/Desktop/Mini-Project-II]
# network_scanner -h
usage: network_scanner [-h] [-t TARGET]

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        Target IP address/range
                        File System

(root@kali)~[/home/ani/Desktop/Mini-Project-II]
# network_scanner -t 172.16.197.147/24
IP                MAC ADDRESS
-----
172.16.197.1      00:50:56:c0:00:08
172.16.197.2      00:50:56:ed:13:be
172.16.197.254    00:50:56:f4:69:37

(root@kali)~[/home/ani/Desktop/Mini-Project-II]
#
```

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

```
(root@kali)~[/home/ani]
# nmap -sP 172.16.197.146/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-26 11:06 IST
Nmap scan report for 172.16.197.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 172.16.197.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:ED:13:BE (VMware)
Nmap scan report for 172.16.197.254
Host is up (0.00010s latency).
MAC Address: 00:50:56:F4:69:37 (VMware)
Nmap scan report for 172.16.197.147
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.28 seconds

(root@kali)~[/home/ani]
#
```


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

```
(root@kali)-[/home/ani]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.197.133 netmask 255.255.255.0 broadcast 172.16.197.255
    ether 00:11:22:33:44:55 txqueuelen 1000 (Ethernet)
    RX packets 30 bytes 3460 (3.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1050 bytes 64412 (62.9 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 0<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

(root@kali)-[/home/ani]
#
```

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

3. ARP Spoofer :

```
(root@kali)-[/home/ani/Desktop/Mini-Project-II]
# arp_spoof -h
usage: arp_spoof [-h] [-g GATEWAY] [-s SPOOF]

optional arguments:
  -h, --help            show this help message and exit
  -g GATEWAY, --gateway GATEWAY
                        Gateway IP
  -s SPOOF, --spoof SPOOF
                        Spoofed IP

Home
```

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

```
(root@kali)-[/home/ani/Desktop/Mini-Project-II]
# arp_spoof -g 172.16.197.1 -s 172.16.197.254
[+] Sent packets: 8
```

```
(root@kali)-[/home/ani/Desktop/Mini-Project-II]
# arp_spoof -g 172.16.197.1 -s 172.16.197.254
[+] Sent packets: 16
```

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

```
(root@kali)-[/home/ani/Desktop/Mini-Project-II]
# arp_spoofers -g 172.16.197.1 -s 172.16.197.254
[+] Sent packets: 24^C
[+] Resetting ARP tables ...

(root@kali)-[/home/ani/Desktop/Mini-Project-II]
#
```