

# PROOF OF CONCEPT

By V.R.Devanand 181MC117

**Xerosploit** : xerosploit is a pentesting toolkit which is mainly used to perform Man In The Middle attack (MITM) attack. It also contains various modules such as

- Port scanning
- Network mapping
- Denial of service (DOS) attack
- Sniffing etc..

## Installation:

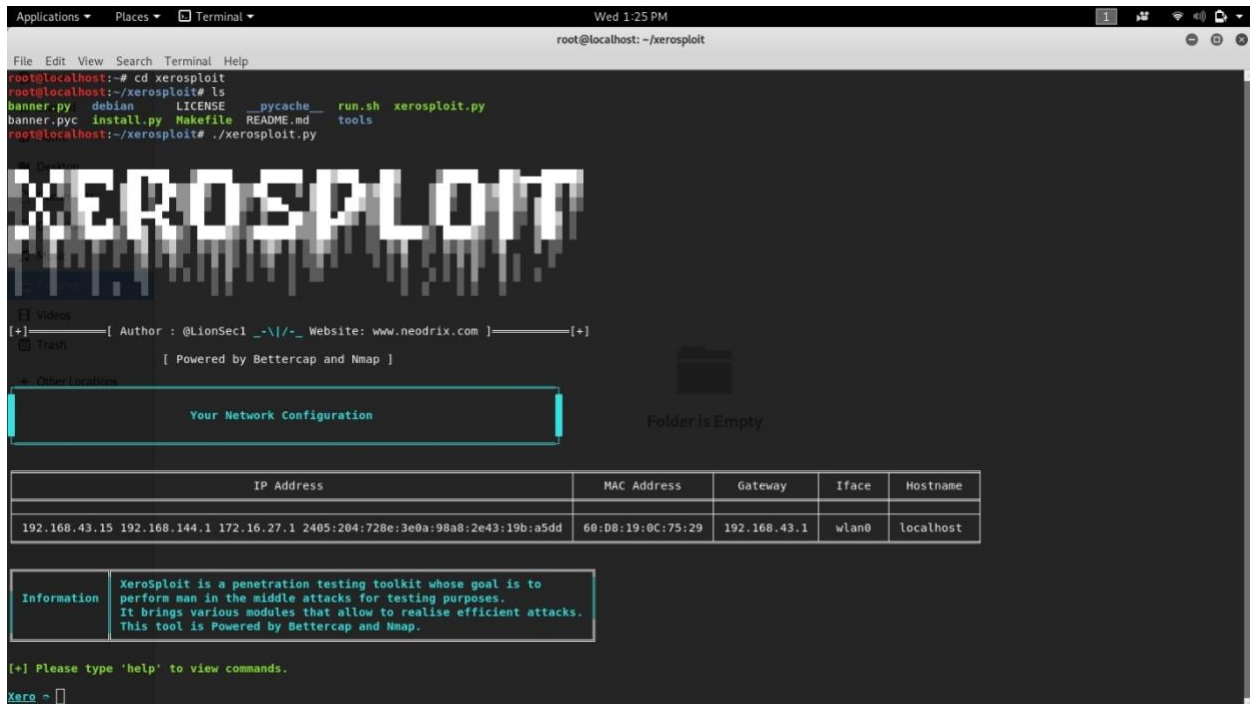
1. `git clone https://github.com/LionSec/xerosploit` //cloning or downloading package from GitHub
2. `cd xerosploit` //change directory to xerosploit
3. `sudo python install.py`
4. `Pip2 install terminal tables` //dependencies for xerosploit
5. `Pip2 install tabulates` //dependencies for xerosploit

## To launch xerosploit:

1. `cd xerosploit` //change directory to xerosploit
2. `./xerosploit.py` //to launch xerosploit.

## Performing scan in our network:

1. Launch xerosploit using ./xerosploit.py command in terminal in xerosploit directory



```
root@localhost:~# cd xerosploit
root@localhost:~/xerosploit# ls
banner.py  debian  LICENSE  __pycache__  run.sh  xerosploit.py
banner.pyc  install.py  Makefile  README.md  tools
root@localhost:~/xerosploit# ./xerosploit.py
```

**XEROSPL0IT**

[+] Author : @LionSec1 \_-\\/\_- Website: www.neodrix.com [ + ]

[ Powered by Bettercap and Nmap ]

Other Locations

Your Network Configuration

Folder is Empty

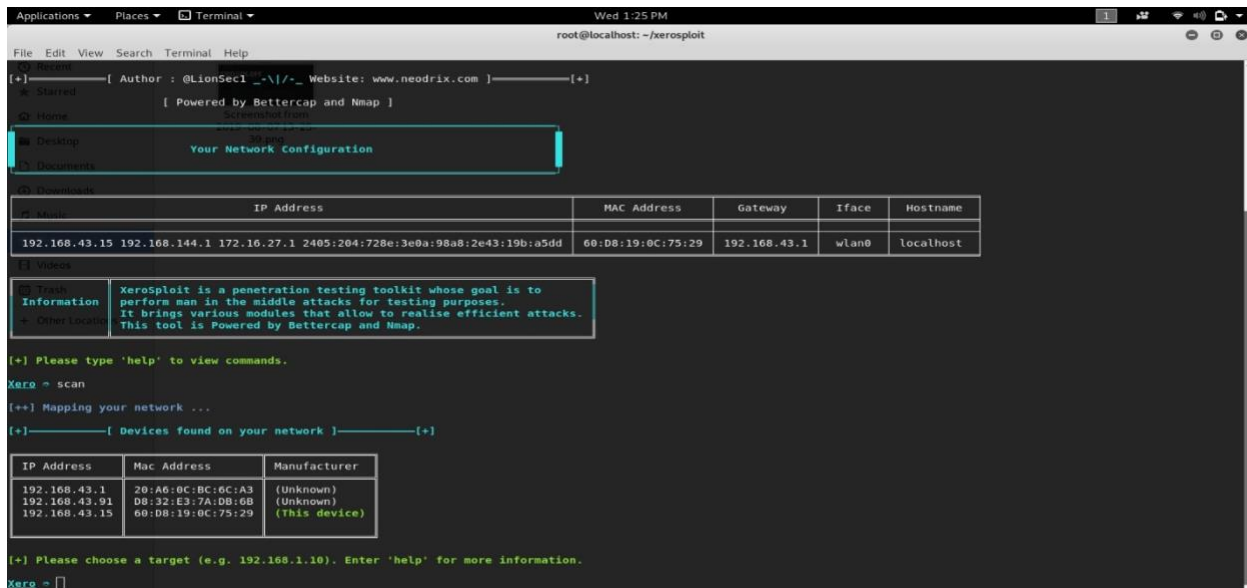
IP Address	MAC Address	Gateway	Iface	Hostname
192.168.43.15 192.168.144.1 172.16.27.1 2405:204:728e:3e0a:98a8:2e43:19b:a5dd	60:D8:19:0C:75:29	192.168.43.1	wlan0	localhost

Information XeroSploit is a penetration testing toolkit whose goal is to perform man in the middle attacks for testing purposes. It brings various modules that allow to realise efficient attacks. This tool is Powered by Bettercap and Nmap.

[+] Please type 'help' to view commands.

Xero ~

2. Now type **scan** to perform scan the ip address of devices in our network.

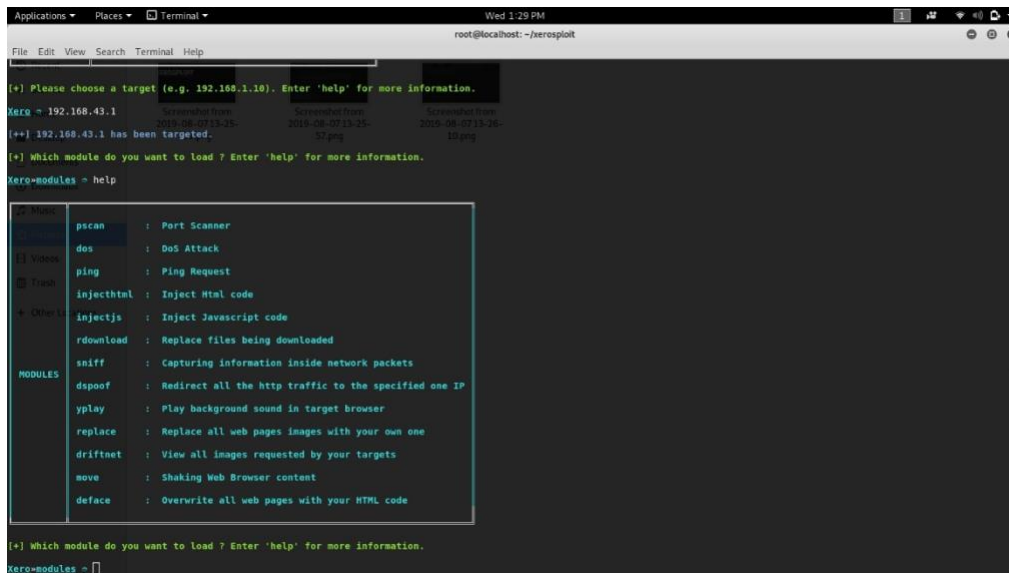


```
[+] Please type 'help' to view commands.
Xero ~ scan
[+] Mapping your network ...
[+] [ Devices found on your network ] [ + ]
```

IP Address	Mac Address	Manufacturer
192.168.43.1	20:A6:0C:BC:0C:A3	(Unknown)
192.168.43.31	08:32:E3:7A:00:60	(Unknown)
192.168.43.15	60:D8:19:0C:75:29	(This device)

```
[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more information.
Xero ~
```

3. Now choose the **target** by entering the **victims' ip** and type help for seeing various **modules**.



```
[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more information.
Xero ~ 192.168.43.1
[+] 192.168.43.1 has been targeted.
[+] Which module do you want to load ? Enter 'help' for more information.
Xero-modules ~ help
```

Module	Description
pscan	: Port Scanner
dos	: DoS Attack
ping	: Ping Request
injecthtml	: Inject Html code
injectjs	: Inject Javascript code
rdownload	: Replace files being downloaded
sniff	: Capturing information inside network packets
dspooof	: Redirect all the http traffic to the specified one IP
yplay	: Play background sound in target browser
replace	: Replace all web pages images with your own one
driftnet	: View all images requested by your targets
move	: Shaking Web Browser content
deface	: Overwrite all web pages with your HTML code

```
[+] Which module do you want to load ? Enter 'help' for more information.
Xero-modules ~
```

#### 4. Now for performing a port scan on victims' ip type **pscan**

The screenshot shows a terminal window titled 'root@localhost: ~/xerosploit'. The 'MODULES' menu is open, listing several modules: dsproof, yplay, replace, driftnet, move, and deface. The 'pscan' module is selected. The terminal then shows the command 'Xero-modules ~ pscan' and a prompt to enter 'run' to execute the module. The output shows the scan results for 192.168.43.1, indicating that port 53/TCP is open.

```
File Edit View Search Terminal Help
root@localhost: ~/xerosploit

MODULES
dsproof : Redirect all the http traffic to the specified one IP
yplay   : Play background sound in target browser
replace : Replace all web pages images with your own one
driftnet : View all images requested by your targets
move     : Shaking Web Browser content
deface   : Overwrite all web pages with your HTML code

[+] Which module do you want to load ? Enter 'help' for more information.
Xero-modules ~ pscan

Port Scanner
Find open ports on network computers and retrieve
versions of programs running on the detected ports

[+] Enter 'run' to execute the 'pscan' command.
Xero-modules-pscan ~ run

[++] Please wait ... Scanning ports on 192.168.43.1
[+] [ Port scan result for 192.168.43.1 ] [++]

SERVICE PORT STATE
DOMAIN 53/TCP OPEN

[+] Enter 'run' to execute the 'pscan' command.
Xero-modules-pscan ~
```

#### 5. The port scan is done and it lists the ports available and its state.