Experiment No. 14

Title: **MITM Attack**

Roll No.: 16010420075 **Experiments No.: 14**

Aim: Perform MITM using Xerosploit

\

Resources: virtual box

Theory

Xerosploit is a penetration testing toolkit whose goal is to perform man-in-themiddle attacks for penetration testing purposes. It brings various modules together that will help you perform very efficient attacks.

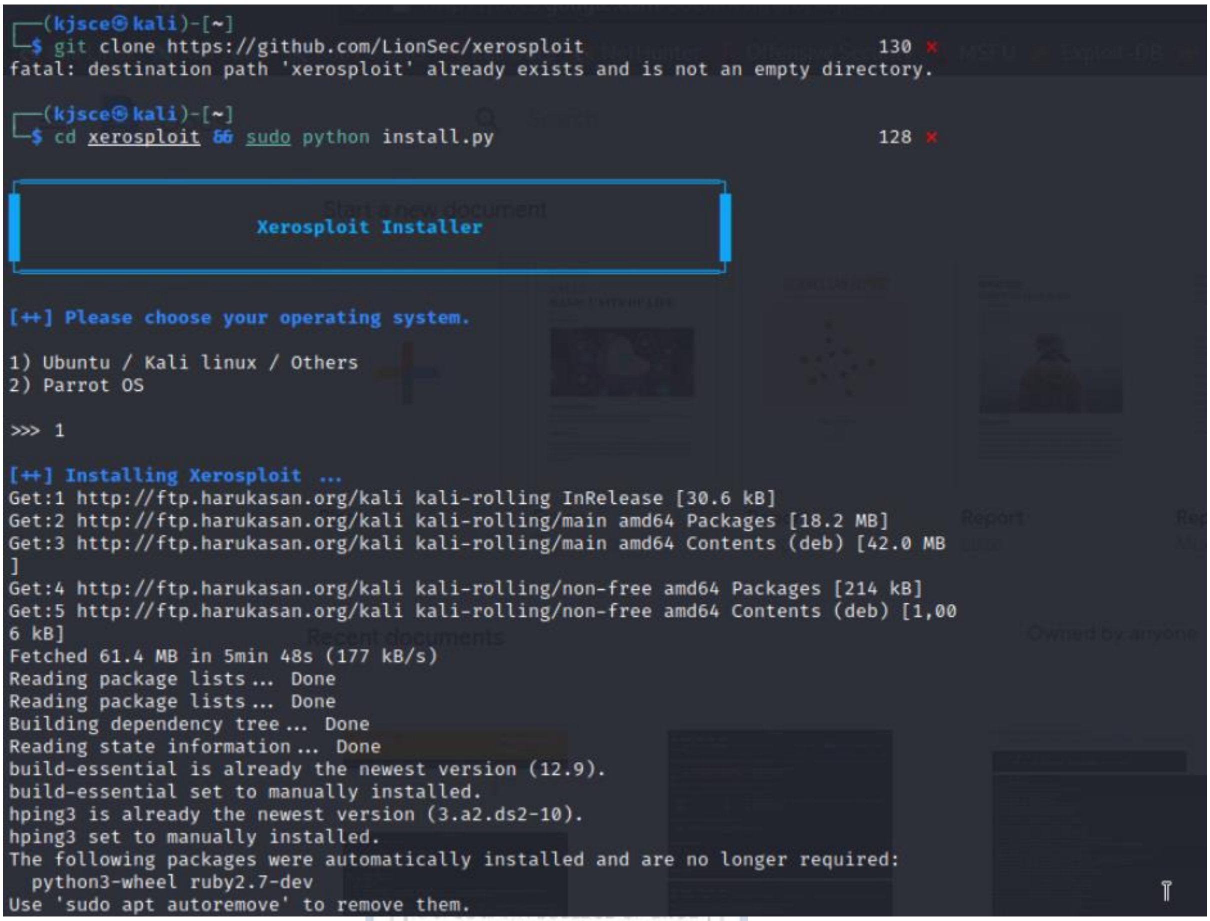
It can perform Port Scanning, Network Mapping, DOS Attack, HTML Code Injection, JavaScript Code Injection, Sniffing, DNS Spoofing, Image replacement, Driftnet and Web Page Defacement. We will be trying to emulate an attack of MITM using Xerosploit.
A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application, with intention of either eavesdropping or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, businesses, e-commerce sites and other websites where logging in is required.
In order to install Xerosploit , we will use git to clone it into our machine . The files downloaded will have xerosploit in them and we will need python on the system to install xerosploit. Supposing we have python, we will run the following command and allow the installation to proceed by itself.

IMPLEMENTATION AND RESULTS:

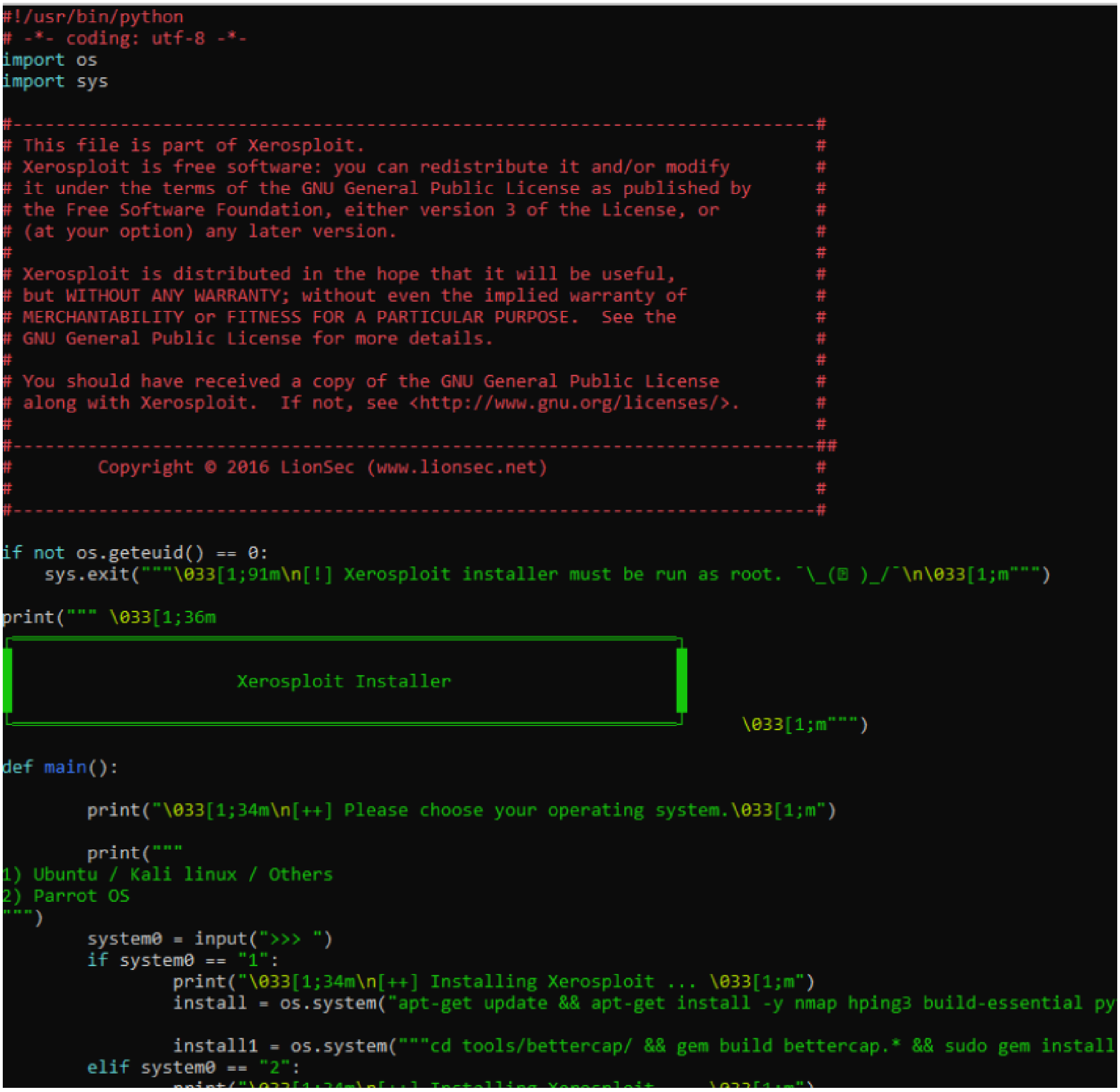
We will be using another kali machine connected to the same network as the victim machine.
In this, we will conduct an ethical hacking project of doing a MITM attack by using the replace command in Xerosploit running inside the Kali Linux machine.

1) git clone https://github.com/LionSec/xerosploit.git
2) Go to the xerosploit folder and run sudo python3 install.py



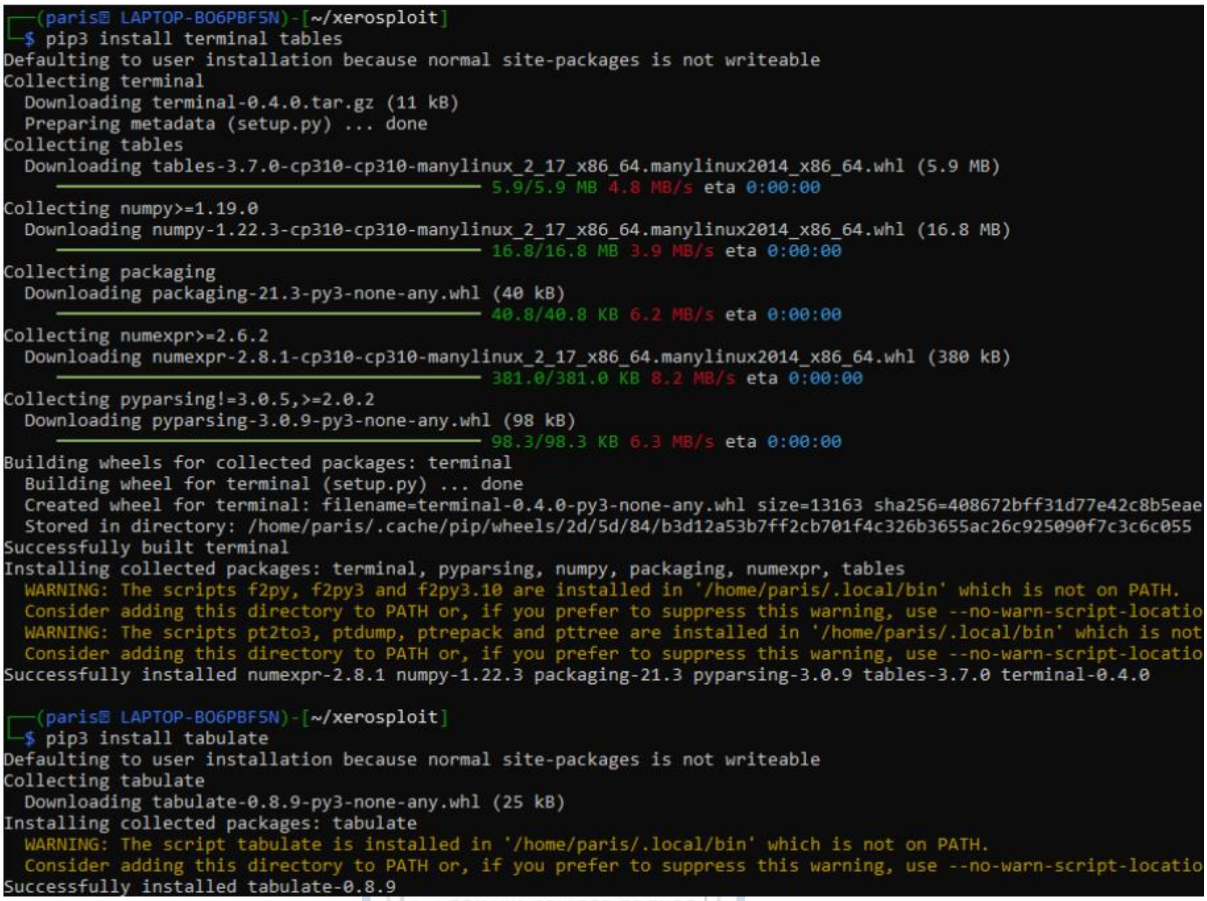
```
┌──(kjsce㉿kali)-[~]
└─$ git clone https://github.com/LionSec/xerosploit                  130 ✗
fatal: destination path 'xerosploit' already exists and is not an empty directory.

┌──(kjsce㉿kali)-[~]
└─$ cd xerosploit && sudo python install.py                          128 ✗

                    Xerosploit Installer

[++] Please choose your operating system.

1) Ubuntu / Kali linux / Others
2) Parrot OS

>>> 1

[++] Installing Xerosploit ...
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.6 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [18.2 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 Contents (deb) [42.0 MB
]
Get:4 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [214 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Contents (deb) [1,00
6 kB]
Fetched 61.4 MB in 5min 48s (177 kB/s)
Reading package lists ... Done
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
build-essential is already the newest version (12.9).
build-essential set to manually installed.
hping3 is already the newest version (3.a2.ds2-10).
hping3 set to manually installed.
The following packages were automatically installed and are no longer required:
  python3-wheel ruby2.7-dev
Use 'sudo apt autoremove' to remove them.
```

3) Change the contents of the install.py file; Replace all the raw_input occurrences by input using nano



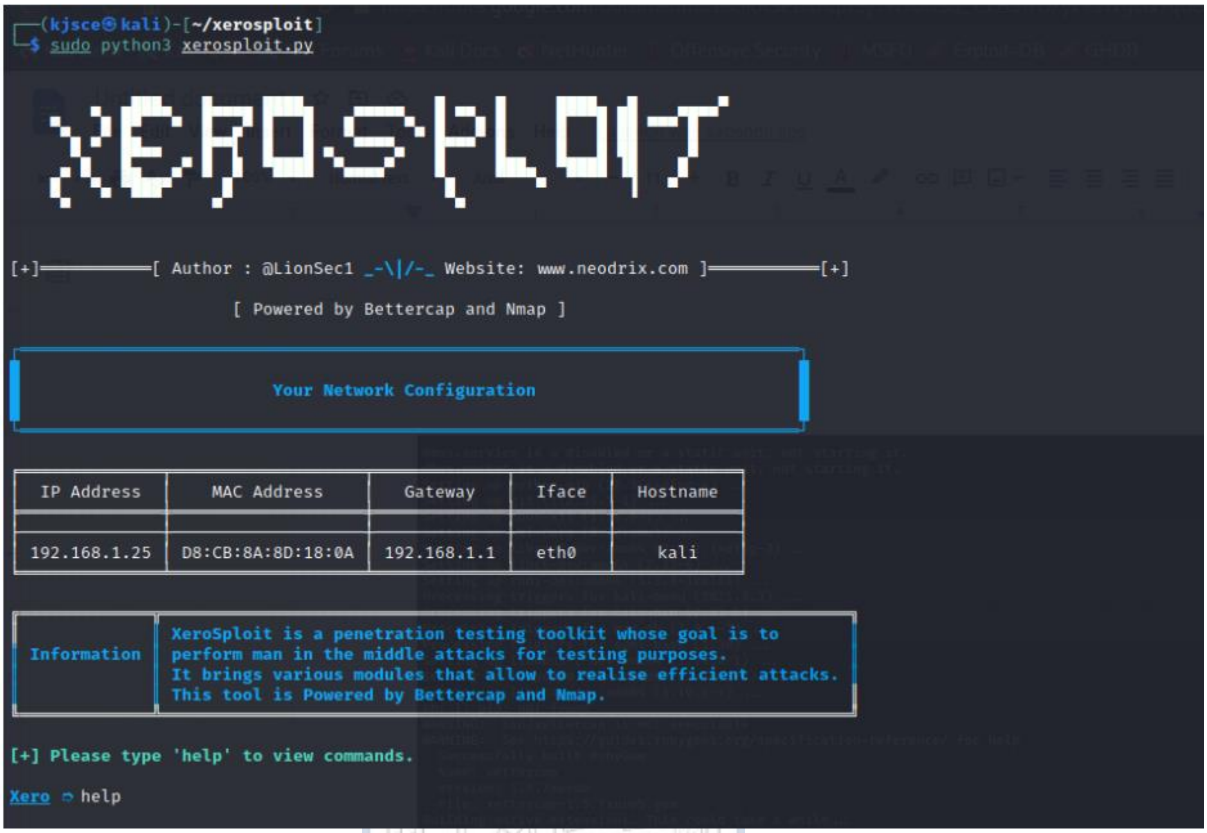
```
#!/usr/bin/python
# -*- coding: utf-8 -*-
import os
import sys

#---------------------------------------------------------------------------#
# This file is part of Xerosploit.                                          #
# Xerosploit is free software: you can redistribute it and/or modify        #
# it under the terms of the GNU General Public License as published by      #
# the Free Software Foundation, either version 3 of the License, or         #
# (at your option) any later version.                                       #
#                                                                           #
# Xerosploit is distributed in the hope that it will be useful,            #
# but WITHOUT ANY WARRANTY; without even the implied warranty of            #
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the             #
# GNU General Public License for more details.                              #
#                                                                           #
# You should have received a copy of the GNU General Public License         #
# along with Xerosploit.  If not, see <http://www.gnu.org/licenses/>.       #
#                                                                           #
#---------------------------------------------------------------------------##
#        Copyright © 2016 LionSec (www.lionsec.net)                         #
#                                                                           #
#---------------------------------------------------------------------------#

if not os.geteuid() == 0:
    sys.exit("""\033[1;91m\n[!] Xerosploit installer must be run as root. ¯\_(ツ )_/¯\n\033[1;m""")

print(""" \033[1;36m
┌──────────────────────────────────────────────────────────────┐
│                      Xerosploit Installer                    │
└──────────────────────────────────────────────────────────────┘
                                                                     \033[1;m""")

def main():

        print("\033[1;34m\n[++] Please choose your operating system.\033[1;m")

        print("""
1) Ubuntu / Kali linux / Others
2) Parrot OS
""")
        system0 = input(">>> ")
        if system0 == "1":
                print("\033[1;34m\n[++] Installing Xerosploit ... \033[1;m")
                install = os.system("apt-get update && apt-get install -y nmap hping3 build-essential py

                install1 = os.system("""cd tools/bettercap/ && gem build bettercap.* && sudo gem install
        elif system0 == "2":
                print("\033[1;34m\n[++] Installing Xerosploit ... \033[1;m")
```

4) If you face this error after running xerosploit.py



```
┌──(paris㉿ LAPTOP-BO6PBF5N)-[~/xerosploit]
└─$ pip3 install terminal tables
Defaulting to user installation because normal site-packages is not writeable
Collecting terminal
  Downloading terminal-0.4.0.tar.gz (11 kB)
  Preparing metadata (setup.py) ... done
Collecting tables
  Downloading tables-3.7.0-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (5.9 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 5.9/5.9 MB 4.8 MB/s eta 0:00:00
Collecting numpy>=1.19.0
  Downloading numpy-1.22.3-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (16.8 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 16.8/16.8 MB 3.9 MB/s eta 0:00:00
Collecting packaging
  Downloading packaging-21.3-py3-none-any.whl (40 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 40.8/40.8 KB 6.2 MB/s eta 0:00:00
Collecting numexpr>=2.6.2
  Downloading numexpr-2.8.1-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (380 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 381.0/381.0 KB 8.2 MB/s eta 0:00:00
Collecting pyparsing!=3.0.5,>=2.0.2
  Downloading pyparsing-3.0.9-py3-none-any.whl (98 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 98.3/98.3 KB 6.3 MB/s eta 0:00:00
Building wheels for collected packages: terminal
  Building wheel for terminal (setup.py) ... done
  Created wheel for terminal: filename=terminal-0.4.0-py3-none-any.whl size=13163 sha256=408672bff31d77e42c8b5eae
  Stored in directory: /home/paris/.cache/pip/wheels/2d/5d/84/b3d12a53b7ff2cb701f4c326b3655ac26c925090f7c3c6c055
Successfully built terminal
Installing collected packages: terminal, pyparsing, numpy, packaging, numexpr, tables
  WARNING: The scripts f2py, f2py3 and f2py3.10 are installed in '/home/paris/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-locatio
  WARNING: The scripts pt2to3, ptdump, ptrepack and pttree are installed in '/home/paris/.local/bin' which is not
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-locatio
Successfully installed numexpr-2.8.1 numpy-1.22.3 packaging-21.3 pyparsing-3.0.9 tables-3.7.0 terminal-0.4.0

┌──(paris㉿ LAPTOP-BO6PBF5N)-[~/xerosploit]
└─$ pip3 install tabulate
Defaulting to user installation because normal site-packages is not writeable
Collecting tabulate
  Downloading tabulate-0.8.9-py3-none-any.whl (25 kB)
Installing collected packages: tabulate
  WARNING: The script tabulate is installed in '/home/paris/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-locatio
Successfully installed tabulate-0.8.9
```

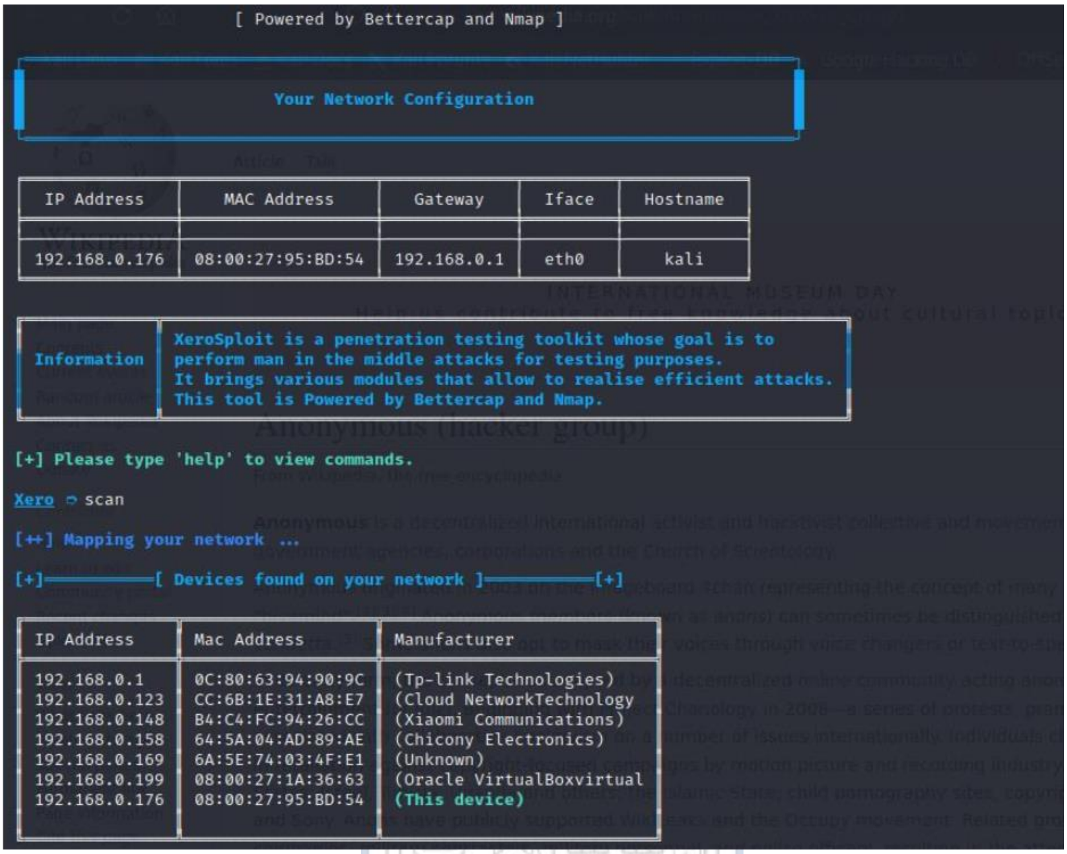
5) Then Run sudo python3 xerosploit



```
┌──(kjsce㉿kali)-[~/xerosploit]
└─$ sudo python3 xerosploit.py

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

                  [ Powered by Bettercap and Nmap ]

                     Your Network Configuration

┌──────────────┬───────────────────┬─────────────┬───────┬──────────┐
│  IP Address  │    MAC Address    │   Gateway   │ Iface │ Hostname │
├──────────────┼───────────────────┼─────────────┼───────┼──────────┤
│ 192.168.1.25 │ D8:CB:8A:8D:18:0A │ 192.168.1.1 │ eth0  │   kali   │
└──────────────┴───────────────────┴─────────────┴───────┴──────────┘

┌─────────────┬──────────────────────────────────────────────────────────┐
│             │ XeroSploit is a penetration testing toolkit whose goal is to │
│ Information │ 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 ➮ help
```

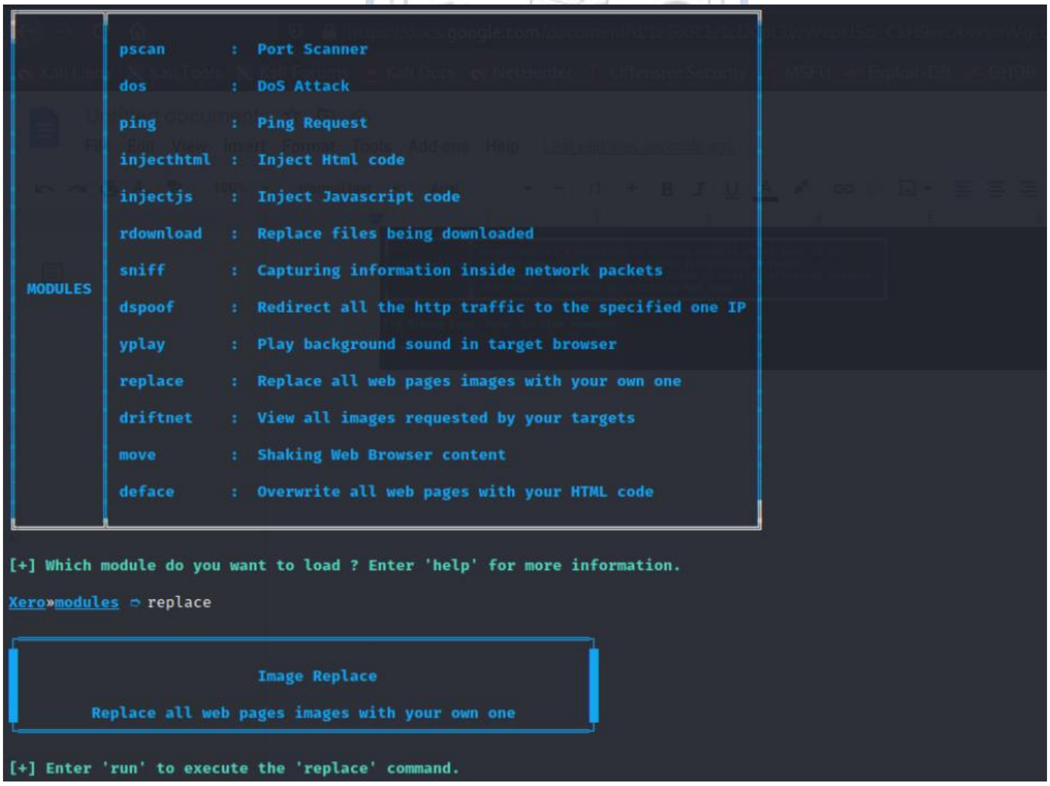
6) The following are some commands which will be used in this attack:
   a. **scan:** To scan your Local network.
   b. **run:** To execute the module
   c. **back:** To exit from a particular module
   d. **help:** To see all the available modules of this tool.

7) The scan command scans our local network for possible devices to target on the network



```
                [ Powered by Bettercap and Nmap ]

                    Your Network Configuration

 IP Address      MAC Address         Gateway       Iface    Hostname

 192.168.0.176   08:00:27:95:BD:54   192.168.0.1   eth0     kali

 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 ➲ scan

[++] Mapping your network ...

[+]────────[ Devices found on your network ]────────[+]

 IP Address      Mac Address         Manufacturer

 192.168.0.1     0C:80:63:94:90:9C   (Tp-link Technologies)
 192.168.0.123   CC:6B:1E:31:A8:E7   (Cloud NetworkTechnology
 192.168.0.148   B4:C4:FC:94:26:CC   (Xiaomi Communications)
 192.168.0.158   64:5A:04:AD:89:AE   (Chicony Electronics)
 192.168.0.169   6A:5E:74:03:4F:E1   (Unknown)
 192.168.0.199   08:00:27:1A:36:63   (Oracle VirtualBoxvirtual
 192.168.0.176   08:00:27:95:BD:54   (This device)
```

8) With help command you can view the actions which can be performed:



```
            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
 MODULES    dspoof       :  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 ➲ replace

                        Image Replace

            Replace all web pages images with your own one

[+] Enter 'run' to execute the 'replace' command.
```

9) Here is the explanation of all the modules of this tool.

pscan: It scans all the ports of the victim's machine, and shows you a list of all the open ports.

DOS: This module will make your victim's machine unresponsive. After this attack, the victim's machine hangs and doesn't give any response.

ping: To ensure that your victim is reachable or not.

injecthtml: This module injects HTML code in your victim's machine, and whenever your victim opens a website, your HTML code will be shown there.

injectjs: Similar to Injecthtml. Whenever your victim opens any website, your javascript also runs there.

sniff: It sniffs the packets of your victim's machine.

dspoof: It will redirect all HTTP traffic to a specific Website, which you gave in this module.

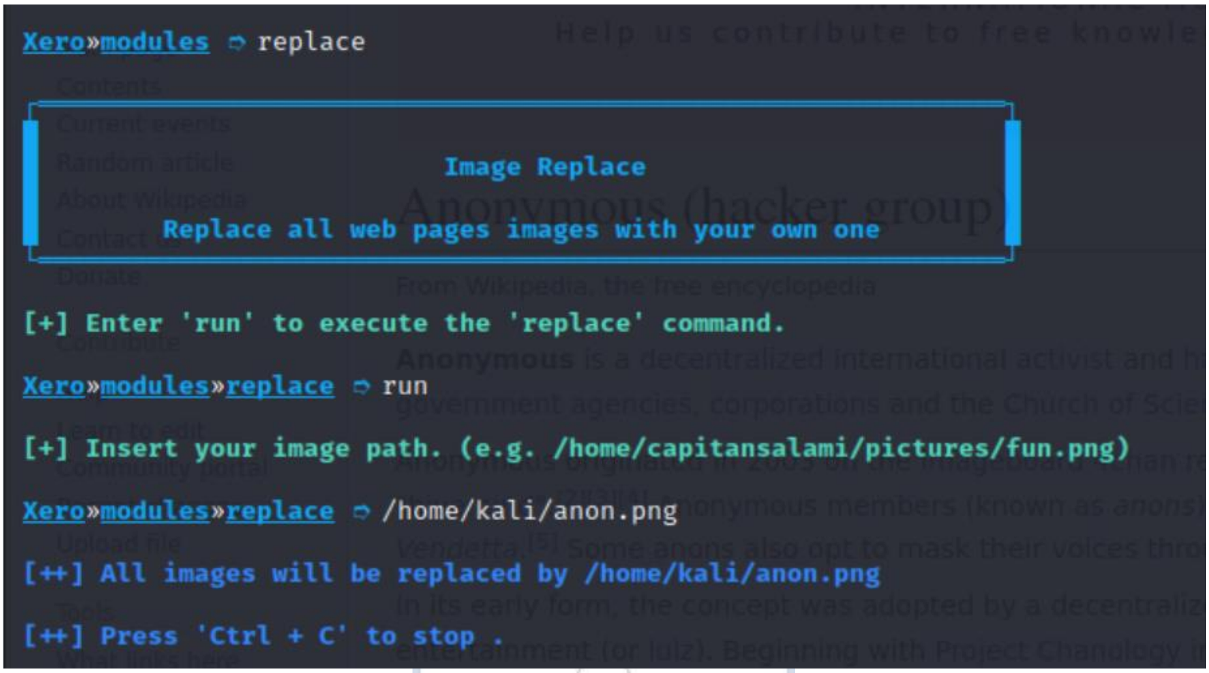
yplay: Whenever your victim opens any website, a sound, which is specified in this module, is played in the background.

replace: This is also interesting. It replaced all the images of the victim's browser with a specific image which you provided.

driftnet: This module captures every image seen by your victim.

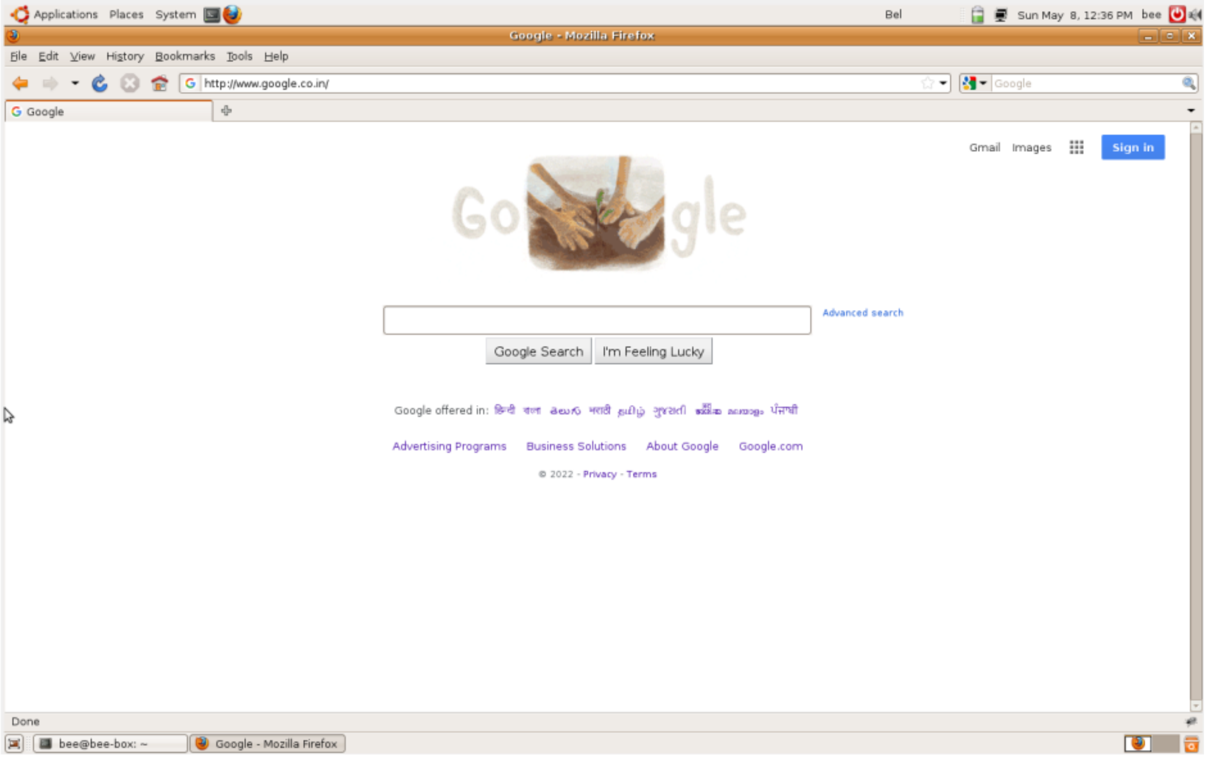
move: This module moves everything in the web browser of your victim's machine.

deface: This tool overwrites each web page with your particular HTML page.

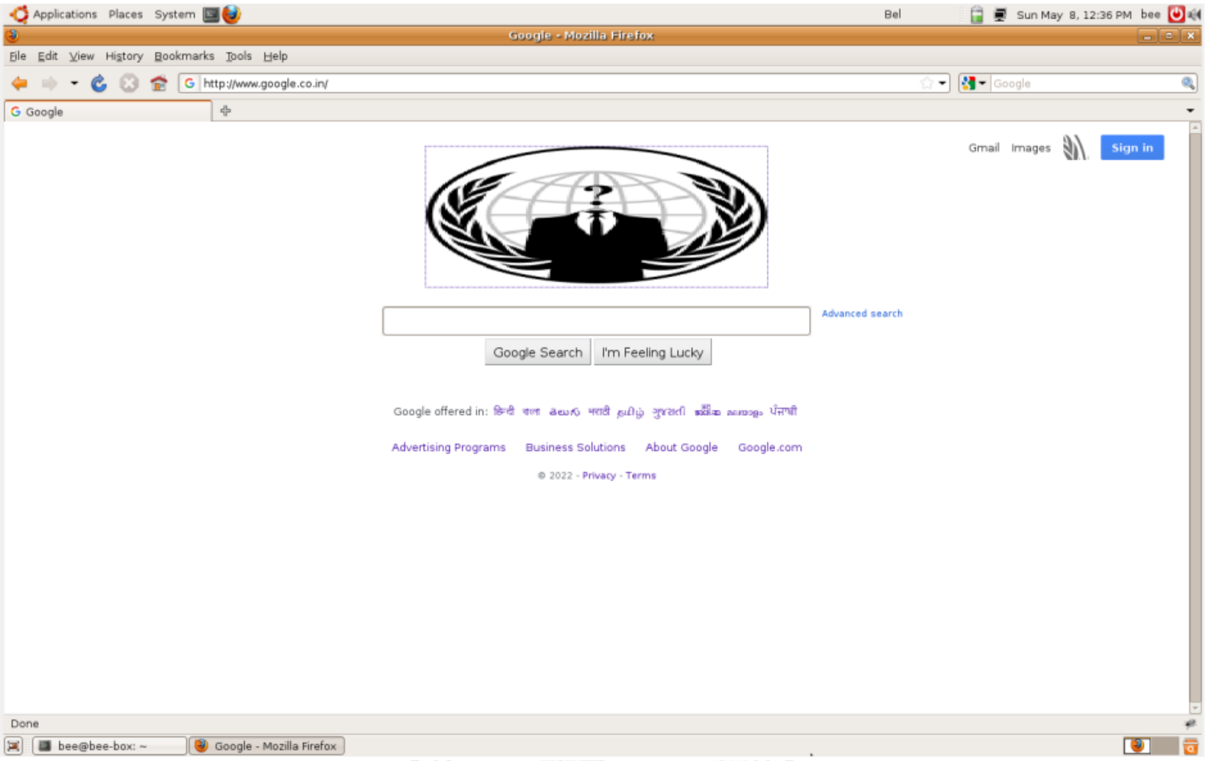


```
Xero»modules ➩ replace

                    Image Replace
   Replace all web pages images with your own one

[+] Enter 'run' to execute the 'replace' command.

Xero»modules»replace ➩ run

[+] Insert your image path. (e.g. /home/capitansalami/pictures/fun.png)

Xero»modules»replace ➩ /home/kali/anon.png

[++] All images will be replaced by /home/kali/anon.png

[++] Press 'Ctrl + C' to stop .
```

Before the MITM Attack :


Applications Places System
Sun May 8, 12:36 PM bee
Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.co.in/
Google
Gmail Images Sign in
Advanced search
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
Advertising Programs Business Solutions About Google Google.com
© 2022 - Privacy - Terms
Done
bee@bee-box: ~
Google - Mozilla Firefox

After the MITM Attack:


Applications Places System
Bel
Sun May 8, 12:36 PM bee
Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.co.in/
Google
Gmail Images
Sign in
Advanced search
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
Advertising Programs Business Solutions About Google Google.com
© 2022 - Privacy - Terms
Done
bee@bee-box: ~
Google - Mozilla Firefox

As we can see all the images on google's website changed to the image at /home/kali/anon.png

Outcomes:

CO2: Comprehend purpose of Anonymity and Foot printing.

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

We have successfully performed a MITM attack on machine by using Xerosploit.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org