**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.

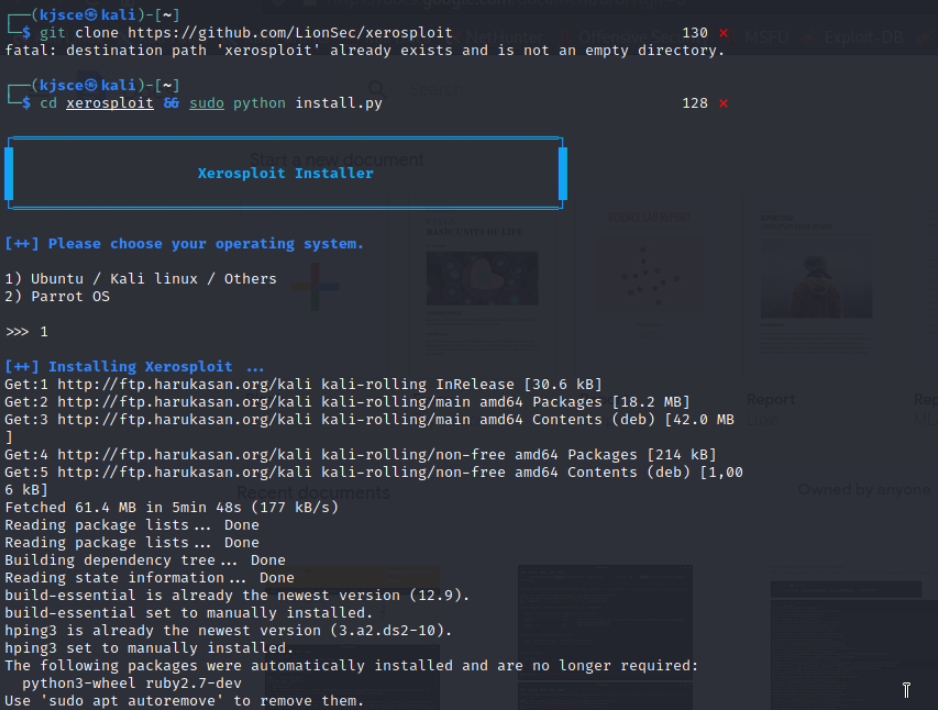
It can perform Port Scanning, Network Mapping, DOS Attack, HTML Code Injection, JavaScript Code Injection, Sniffing, DNS Spoofing, Image replacement, Driftnet and Web Page Defacement. We will be trying to emulate an attack of MITM using Xerosploit.  
A man in the middle (MITM) attack is a general term 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.  
 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

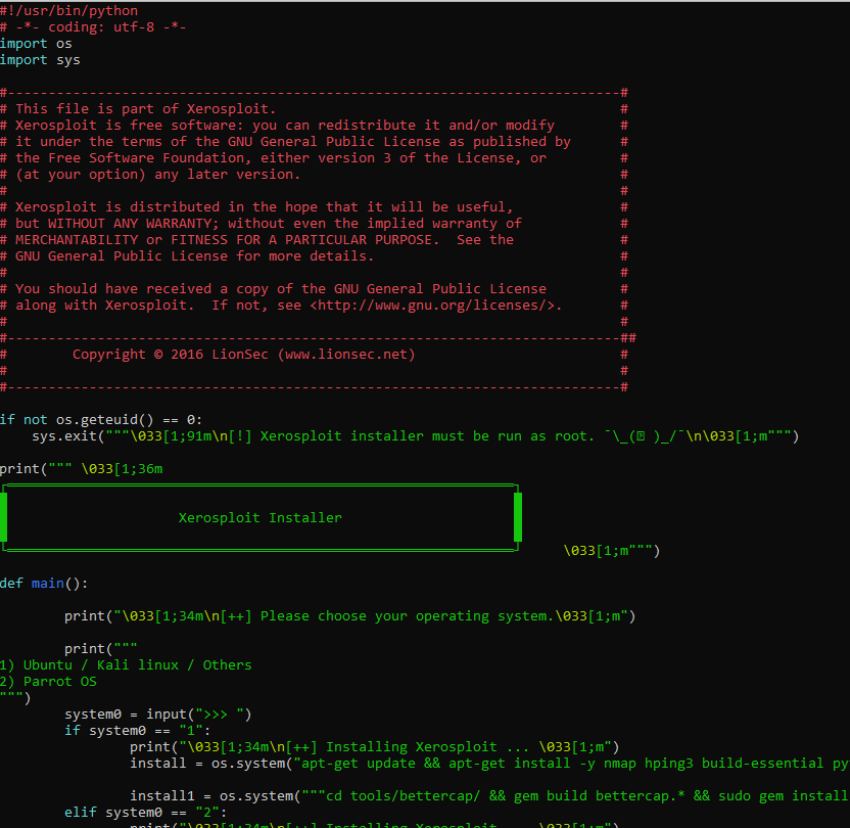
**IMPLEMENTATION AND RESULTS:**

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.

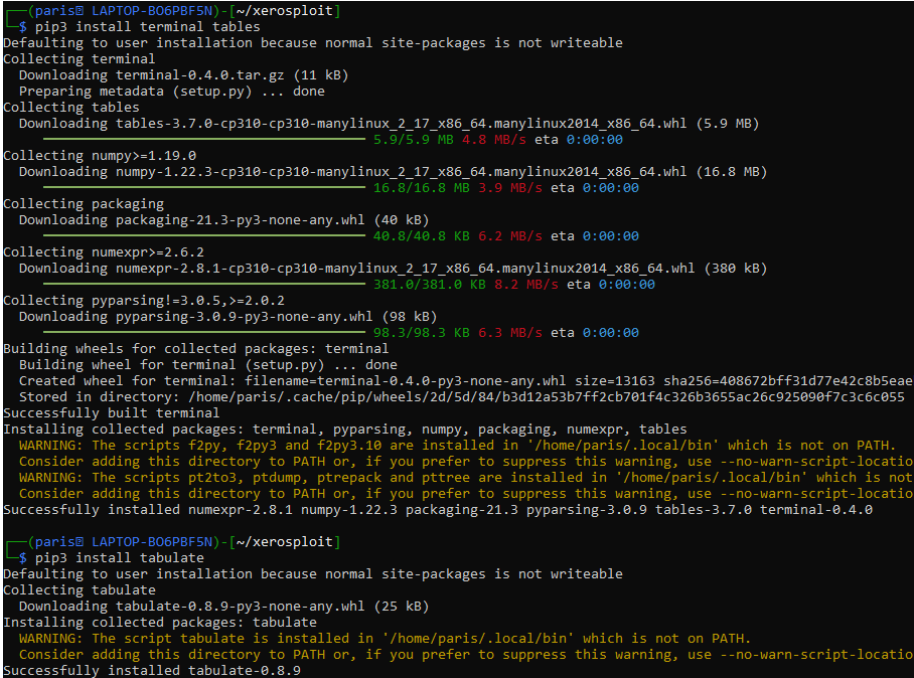
1. git clone <https://github.com/LionSec/xerosploit.git>
2. Go to the xerosploit folder and run sudo python3 install.py



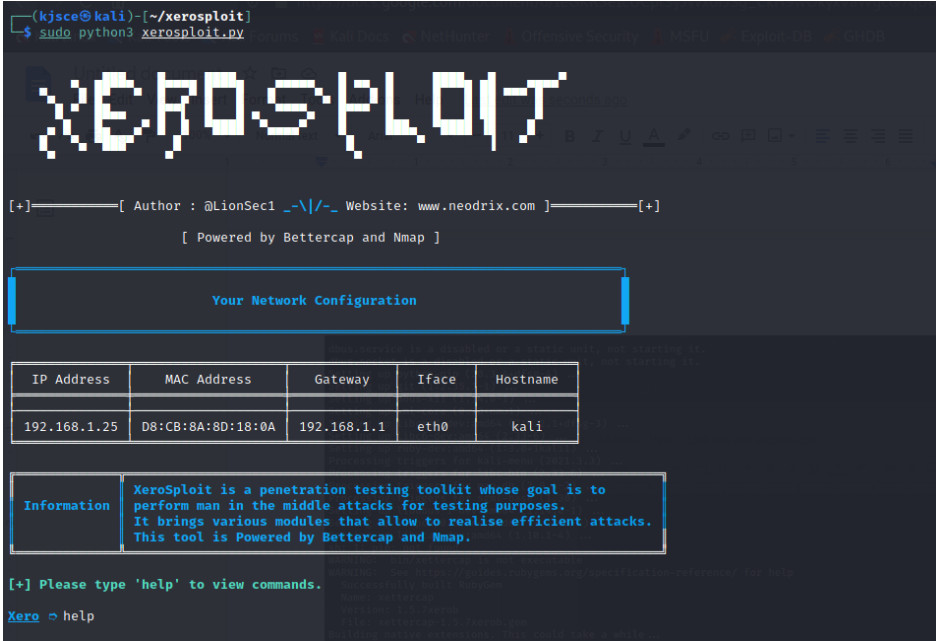
1. Change the contents of the install.py file; Replace all the raw\_input occurrences  
   by input using nano



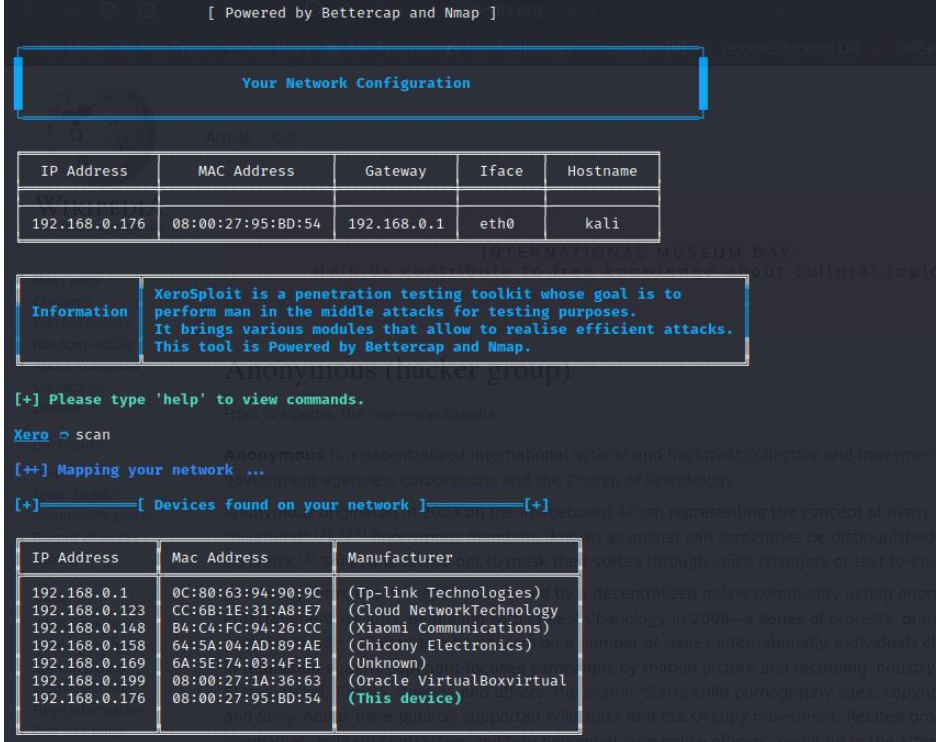
1. If you face this error after running xerosploit.py



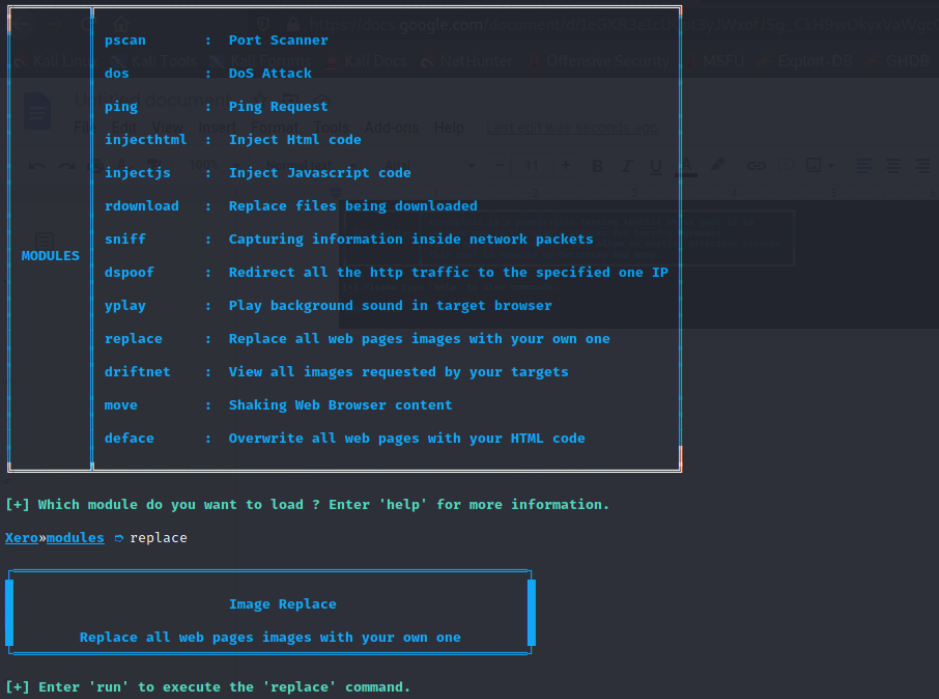
1. Then Run sudo python3 xerosploit



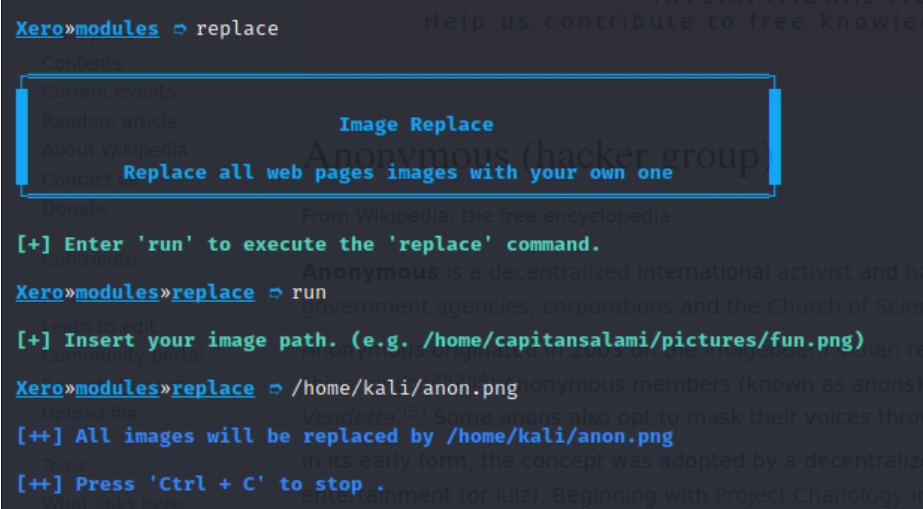
1. The following are some commands which will be used in this attack:  
   a. **scan:** To scan your Local network.  
   b. **run:** To execute the module  
   c. **back:** To exit from a particular module  
   d. **help:** To see all the available modules of this tool.
2. The scan command scans our local network for possible devices to target  
   on the network

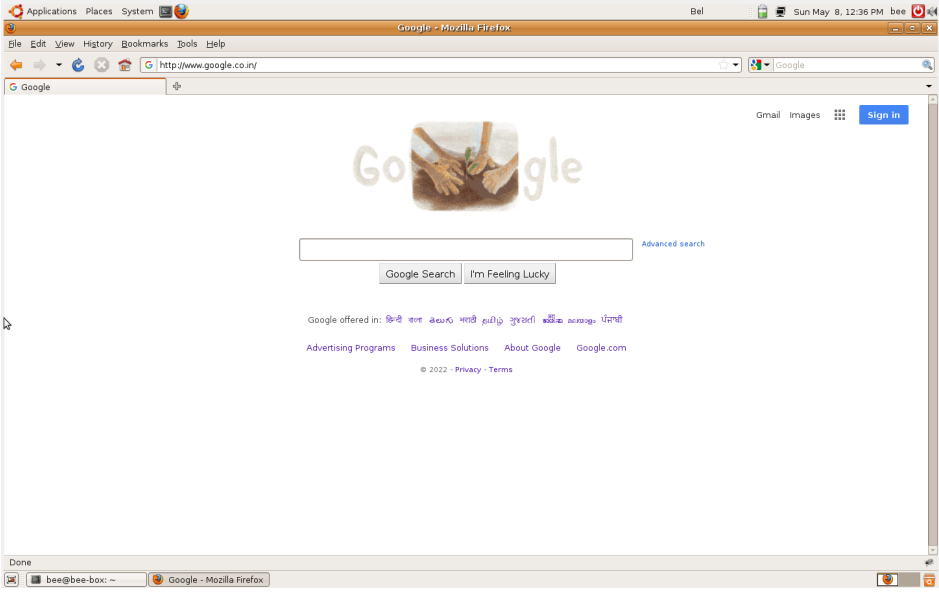


1. With help command you can view the actions which can be performed:

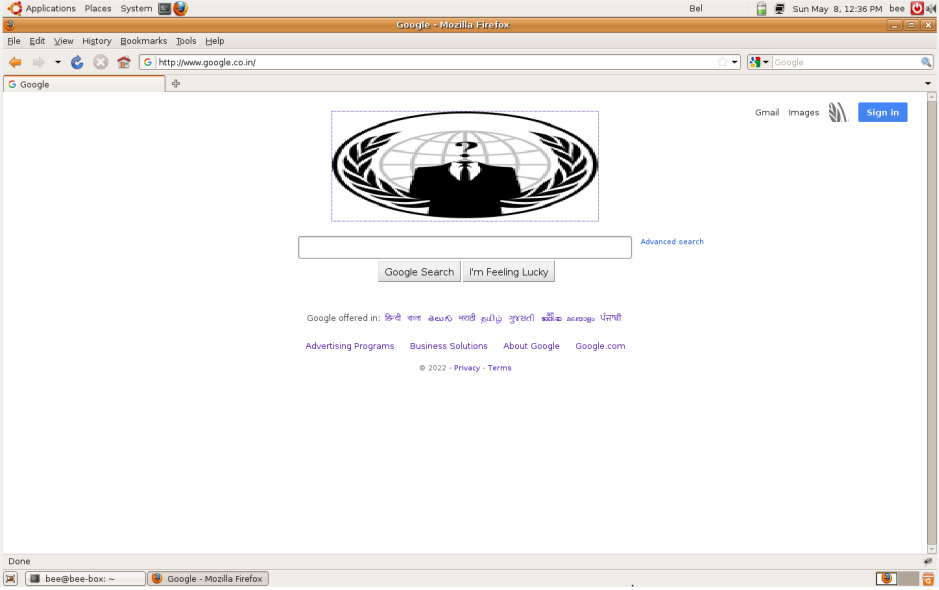


1. Here is the explanation of all the modules of this tool.  
   **pscan:** It scans all the ports of the victim’s machine, and shows you a list of all the open  
   ports.  
   **DOS:** This module will make your victim’s machine unresponsive. After this attack, the  
   victim’s machine hangs and doesn’t 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.



Before the MITM Attack :  


After the MITM Attack:



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](http://www.kali.org)