Pivoting (Metasploit)

- *Anurag Srivastava*

Email - *theanuragsrivastava@gmail.com*

Linkedin - *https://in.linkedin.com/in/hexachordanu*

Exploit-db Author page – *https://www.exploit-db.com/author/?a=9053*

Greetz : Offsec team,Nipun Jaswal,Deepankar Arora ,Kishan Sharma,Nitin Pandey,Faisal Shadab Yazdani ,Spririted wolf, Manish Kishan Tanwar,Raghav Bisht,Vivek Chauhan,Shah Rukh ,Shrey, Akash Shukla,S@mur@!,D3 and Vardan .

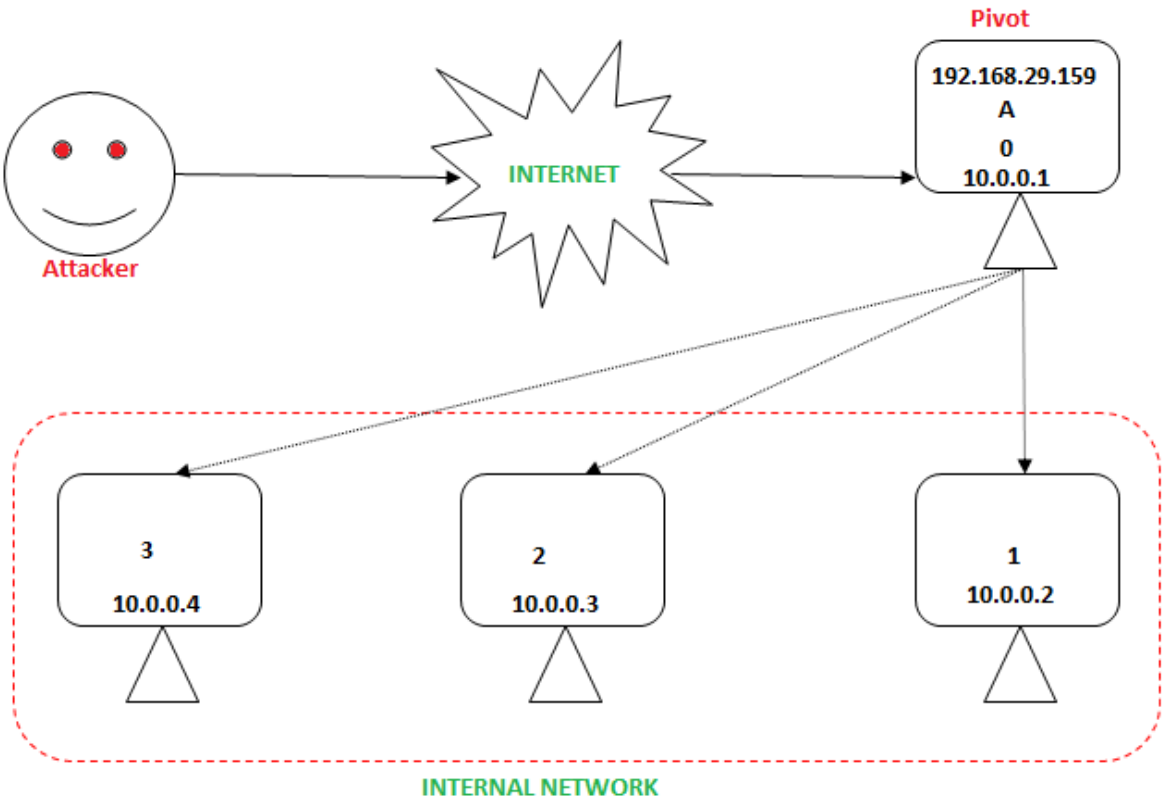
Table of Contents

1. Pivoting :

It is a technique of using a compromised system to attack other systems on the same network.

Consider a scenario where there is some juicy information hosted inside a local network and there is only one system which is connected to internet. In this scenario, an attacker can compromise the system which is connected to internet and then use that particular compromised system in-order to test or attack other systems in the same network which are only accessible via local network.

These kind of multilayer attack allows you to scan other systems in the same network , compromising domain controller etc .



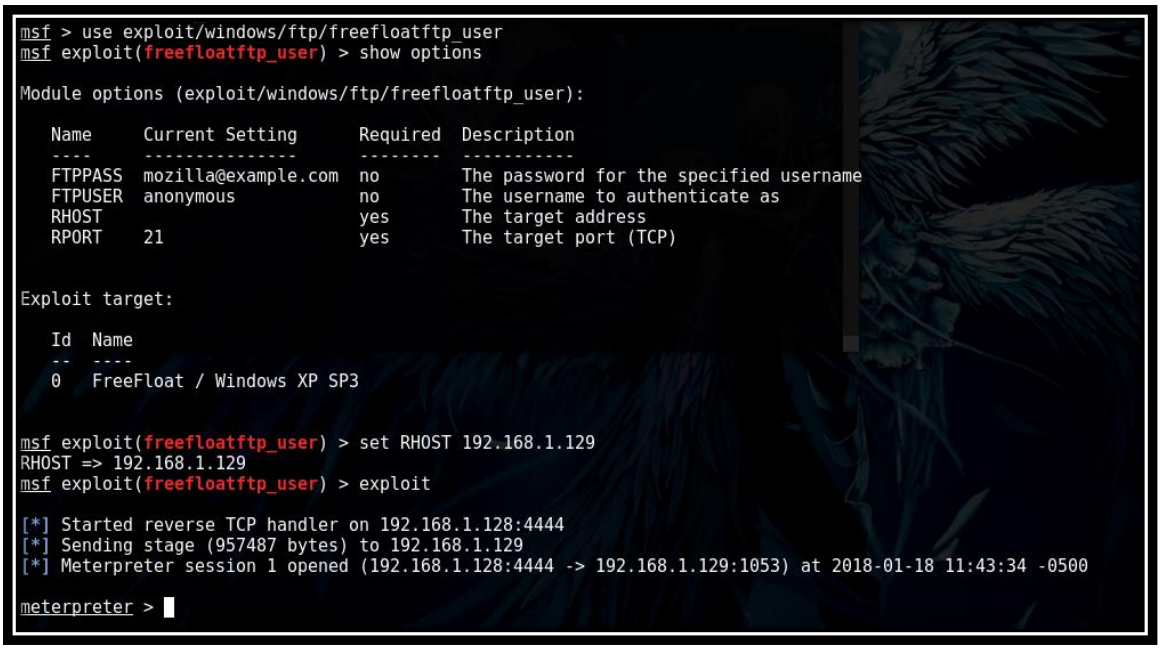
The above diagram shows a rough outline of pivoting however there are more things involved in between (eg. Firewalls,routers etc) which I have skipped for simplicity .

Let’s understand the above diagram:

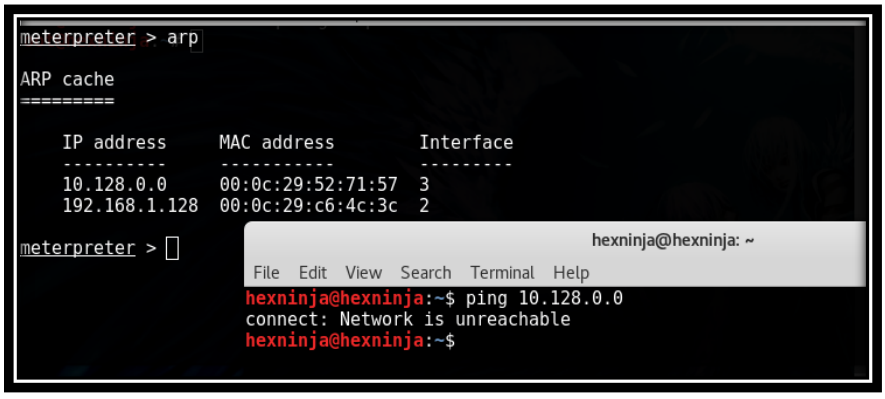
- A smart admin is running confidential internal server inside his local network containing sensitive data. Since he is smart☺ , no one else from outside the network is allowed to access that server.
- The admin has setup four servers/system and one system in that is connected to internet having no important/sensitive data.
- An attacker having bad intention wants to hack the server which is visible to him having some clue about local network data or no clue about location of sensitive data.
- The attacker, somehow try to compromise the target system which is visible to him.
- After getting access to the compromised target data , he may come across two situation –
    - He got some data from that server and still looking for more.
    - He didn’t get any sensitive or important data and therefore he need to find a way to get it.
- In both the situation, attacker is seeking for more sensitive data in-order to accomplish his goals.
- The attacker is aware about the concept of pivoting , and he attempt to do that .
- Attacker finds other network interface through arp scan and try to add route to access other systems in the network via compromised system as pivot point.
- Since now the attacker has added a route , he try to start a socks server through msf auxiliary .
- The attacker is now able to access all the internal system and try to find some vulnerability by scanning/testing.
- Once he find out the other vulnerable system, he get access to many information and compromise many system.

2. Step-wise Demonstration :

Let's suppose the attacker got the access to vulnerable visible machine by exploiting a vulnerable free float ftp server running on the target system.

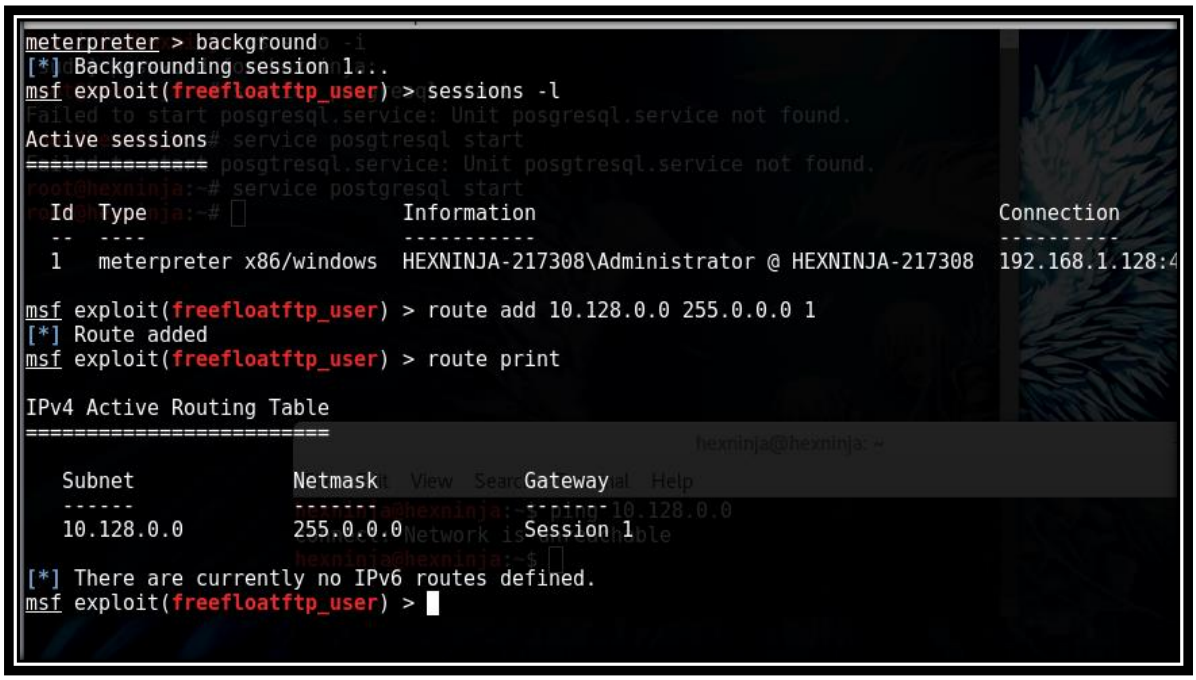


Now the attacker do an arp scan :

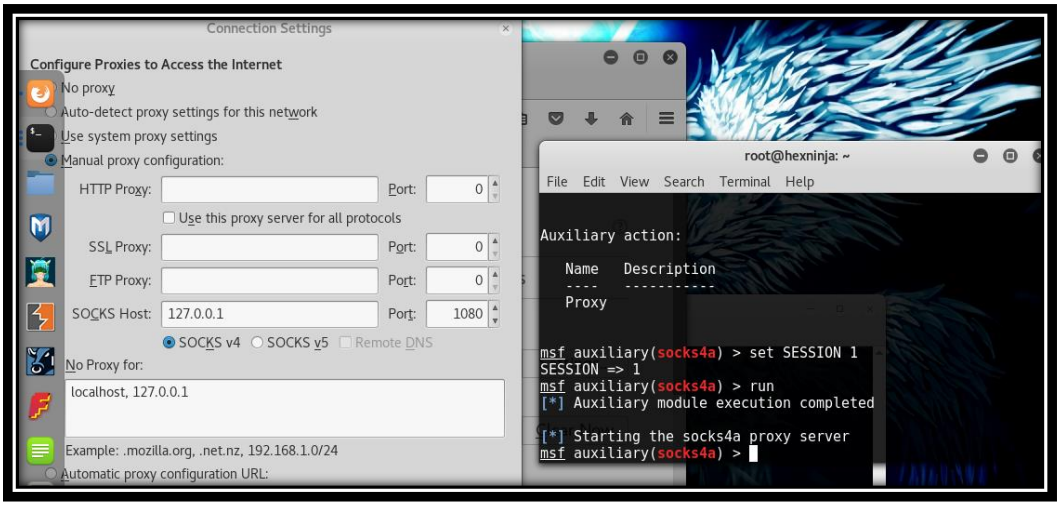


The attacker discovers another interface i.e Interface 3 .He then try to ping the system directly which is not possible, since it is in a local network having private ip as well .

The attacker adds a route in-order to route the traffic through th pivot point or compromised system.

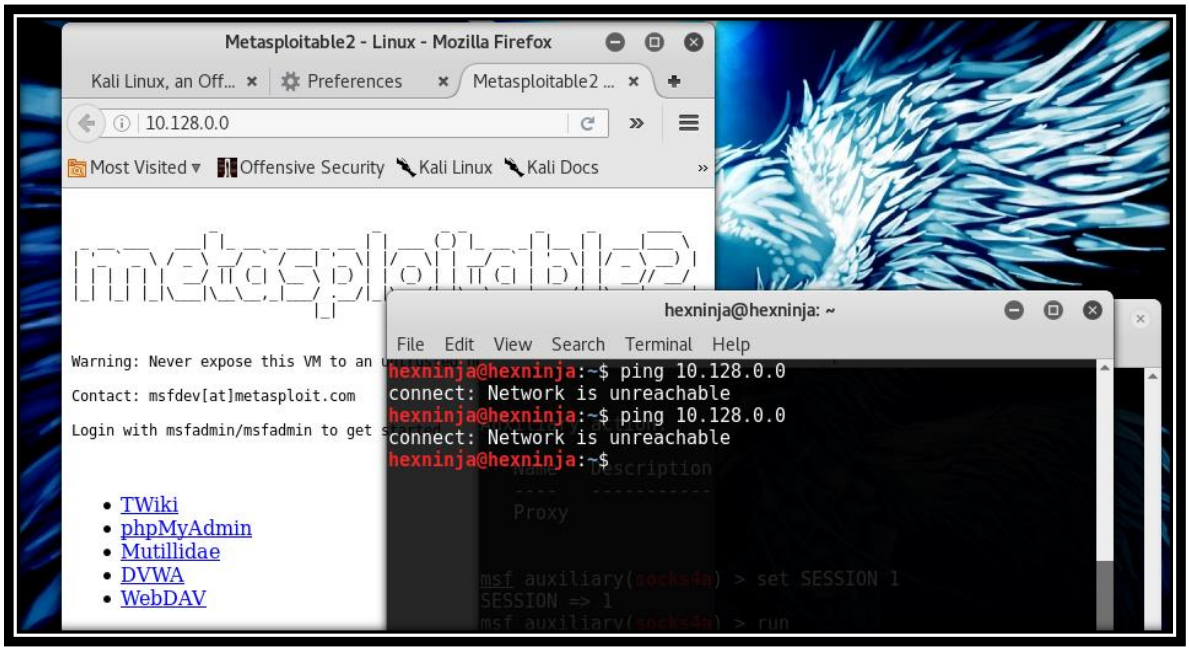


Running a socks auxiliary module of metasploit :



By Configuring the socks proxy in the browser, attacker is able to access other systems/server.

Attacker is able to access an internal server and now he can further test it to find other vulnerabilities and gain access to it.



3. References :

a. https://www.offensive-security.com/metasploit-unleashed/pivoting/

b. https://null-byte.wonderhowto.com/how-to/hack-like-pro-pivot-from-victim-system-own-every-computer-network-0149847/