Wireshark

hash ntlmv2(smb2)

SMB es un protocolo cuyo principal cometido es el compartir ficheros en la red con otros equipos.

```
Formato de hash nltm:
[user Name]::[domain name]:[NTLM server challenge]:[NtproofStr]:[Rest
of NTLMv2 Response]
```

Paquete donde se localiza el NTLM server challenge

filtrar por smb2

```
SMB2 359 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
```

Paquete donde se localiza el resto de elementos

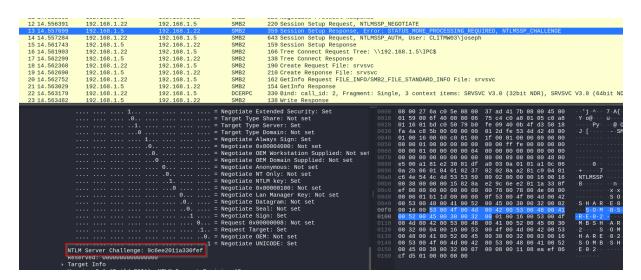
en este paquete se realiza la autenticación

13 14.557099	192.168.1.5	192.168.1.22	SMB2	359 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRE
14 14.557284	192.168.1.22	192.168.1.5	SMB2	643 Session Setup Request, NTLMSSP_AUTH, User: CLITMW03\joseph
15 14 561742	102 160 1 5	102 160 1 22	CMD2	150 Cassian Catum Despansa

User name and Domain name

```
220 Session Setup Request, NILMSSP_NEGUIIATE
359 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NT
12 14.556391
                                                192.168.1.22
                                                                                                           192.168.1.5
                                                                                                                                                                        SMB2
 13 14.557099
                                                192.168.1.5
                                                                                                            192.168.1.22
                                                                                                                                                                        SMB2
                                                                                                                                                                                                    643 Session Setup Request, NTLMSSP_AUTH, User: CLITMW03\joseph
159 Session Setup Response
166 Tree Connect Request Tree: \\192.168.1.5\IPC$
138 Tree Connect Response
190 Create Request File: srvsvc
210 Create Response File: srvsvc
162 GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: srvsvc
15 14.561743
16 14.561903
                                                192.168.1.22
                                                                                                            192.168.1.5
                                                                                                                                                                        SMB2
17 14.562299
                                                192.168.1.5
                                                                                                            192.168.1.22
                                                                                                                                                                        SMB2
18 14.562368
19 14.562690
                                                192.168.1.22
192.168.1.5
                                                                                                            192.168.1.5
192.168.1.22
                                                                                                                                                                        SMB2
SMB2
20 14.562752
                                                192.168.1.22
                                                                                                            192.168.1.5
                                                                                                                                                                        SMB2
                                                192.168.1.5
192.168.1.22
192.168.1.5
                                                                                                                                                                                                     134 GetInfo Response
330 Bind: call_id: 2, Fragment: Single, 3 context items: SRVSVC V3.0 (:
138 Write Response
21 14.563029
                                                                                                            192.168.1.22
                                                                                                                                                                        SMB2
22 14.563179
23 14.563482
                                                                                                                                                                        DCERPC
                                                                                                                                                                         SMB2
                              Attribute: DNS computer name: SOMBSHARE02
Attribute: Timestamp
Attribute: Flags
Attribute: Flags
Attribute: Restrictions
Attribute: Channel Bindings
Attribute: Target Name: cifs/192.168.1.5
Attribute: End of list
padding: 00000000
Domain name: CLITMW03
User name: joseph
Host name: CLITMW03
Session Key: 29140a119e3d9f192df6c8be4441af3b
                                                                                                                                                                                                                                                                                                              00 4c 00 49 00
00 6f 00 73 00
00 54 00 4d 00
00 00 00 00 00
00 00 00 10 d6
62 1f 88 01 01
0f 45 01 98 9f
00 16 00 53 00
00 52 00 45 00
00 44 00 42 00
00 48 00 41 00
00 58 00 41 00
00 48 00 41 00
00 58 00 41 00
00 59 00 60 00
                                                                                                                                                                                                                                                                                                                                                         54 00 4d
65 00 70
57 00 30
00 00 00
5b 74 62
00 00 00
f1 0d ae
4f 00 4d
33 00 45
53 00 45
52 00 45
4d 00 42
32 00 07
00 00 00
                                                                                                                                                                                                                                                                                                                                                                                      00 57
00 68
00 33
00 00
55b 53
00 00
e2 22
00 42
00 01
00 45
00 33
00 08
                                User name: Joseph
Host name: CLITMW08
Session Key: 29f4da1f9e3d9f192df6c8be4441af3b
Negotiate Flags: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negot
1...... = Negotiate 56: Set
..... = Negotiate Key Exchange: Set
```

NTLM server Challenge

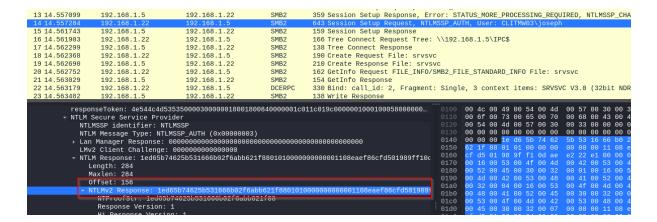


NTProofStr

```
13 14.557099
                   192.168.1.5
                                           192.168.1.22
                                                                    SMB2
                                                                                359 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIF
                                                                                159 Session Setup Response
                                                                                166 Tree Connect Request Tree: \\192.168.1.5\IPC$
138 Tree Connect Response
190 Create Request File: srvsvc
16 14.561903
                   192.168.1.22
                                           192.168.1.5
                                                                    SMB2
                                                                    SMB2
SMB2
17 14.562299
                   192.168.1.5
                                            192.168.1.22
                   192.168.1.22
18 14.562368
                                           192.168.1.5
                   192.168.1.5
192.168.1.22
                                           192.168.1.22
192.168.1.5
                                                                                210 Create Response File: srvsvc
162 GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: srvs
19 14.562690
                                                                    SMR2
20 14.562752
                                                                    SMB2
21 14.563029
                   192.168.1.5
                                           192.168.1.22
                                                                    SMB2
                                                                                154 GetInfo Response
22 14.563179
                   192.168.1.22
                                           192.168.1.5
                                                                    DCERPC
                                                                                330 Bind: call_id: 2, Fragment: Single, 3 context items: SRVSVC
23 14.563482
                    192.168.1
                                                168.1
                                                                                                                          responseToken: 4e544c4d535350000300000018001800840000001c011c019c0000001000100058000000.
        0b
00
                                                                                                                                                   00
04
00
             NTLM Response: 1ed65b74625b531666b02f6abb621f880101000000000001108eaef86cfd501989ff10c
Length: 284
               Maxlen: 284
Offset: 156
NTLMv2 Rosp
                                                                                                                                                   82
4e
84
                  TSEC. 100
LMV2 Response: 1cd65b74625b521666b92f6abb621f880101000000000001108eaef86cfd5019891
NTProofStr: 1ed65b74625b531666b92f6abb621f88
```

Resto del hash

Copiar valor desde wireshark haciendo clic derecho en el campo del hash, después borrar la parte de NTProofStr



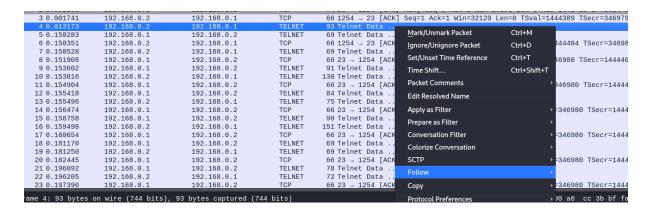
crackear hash

john --wordlist=/usr/share/wordlists/rockyou.txt hash

Telnet

Telnet es un protocolo por el que se puede realizar una conexión de forma remota entre dos equipos, es un protocolo inseguro ya que estas conexiones no van cifradas como en ssh.

hacer clic derecho en un paquete telnet y darle a follow>tcp, nos mostrara el intercambio de datos entre cliente servidor y podremos ver las credenciales.



FTP

Instalar librería descargándola del siguiente enlace:

https://pypi.org/project/pyftpdlib/#files

```
Distribución fuente

pyftpdlib-1.5.9.tar.gz (204.8 kB ver hashes)

Uploaded 25 oct 2023 Source
```

```
# en Downloads, descomprimimos
tar -xvf pyftpdlib-1.5.9.tar.gz

# entramos en el directorio generado
# instalamos
sudo python setup.py install

# levantamos servidor ftp
sudo python -m pyftpdlib -u user -P 123 -p 21

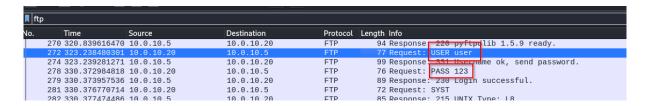
-u --> indicamos usuario del servidor ftp
-P --> indicamos una contraseña
-p --> indicamos el puerto
```

iniciamos wireshark para capturar los paquetes de conexión con el servidor ftp.

Desde ubuntu server nos conectamos al server ftp.

ftp IPKALI
usuario:user
password:123

En wireshark filtramos por ftp



HTTP

Con wireshark snifando accedemos al Login de la siguiente web.

http://testphp.vulnweb.com/login.php

introducimos unas credenciales cualquiera.

En wireshark filtramos por http.

Clic derecho en un paquete http y a continuación follow>tcp

```
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.0

Date: Sat. 27 Apr 2024 15:34:25 GMT
```

ICMP

Realizamos un ping a nuestra maquina o desde nuestra maquina y filtramos por icmp

