Forest walkthrough

Index

List of pictures

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:

```
┌──(k14d1u5㉿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?
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:

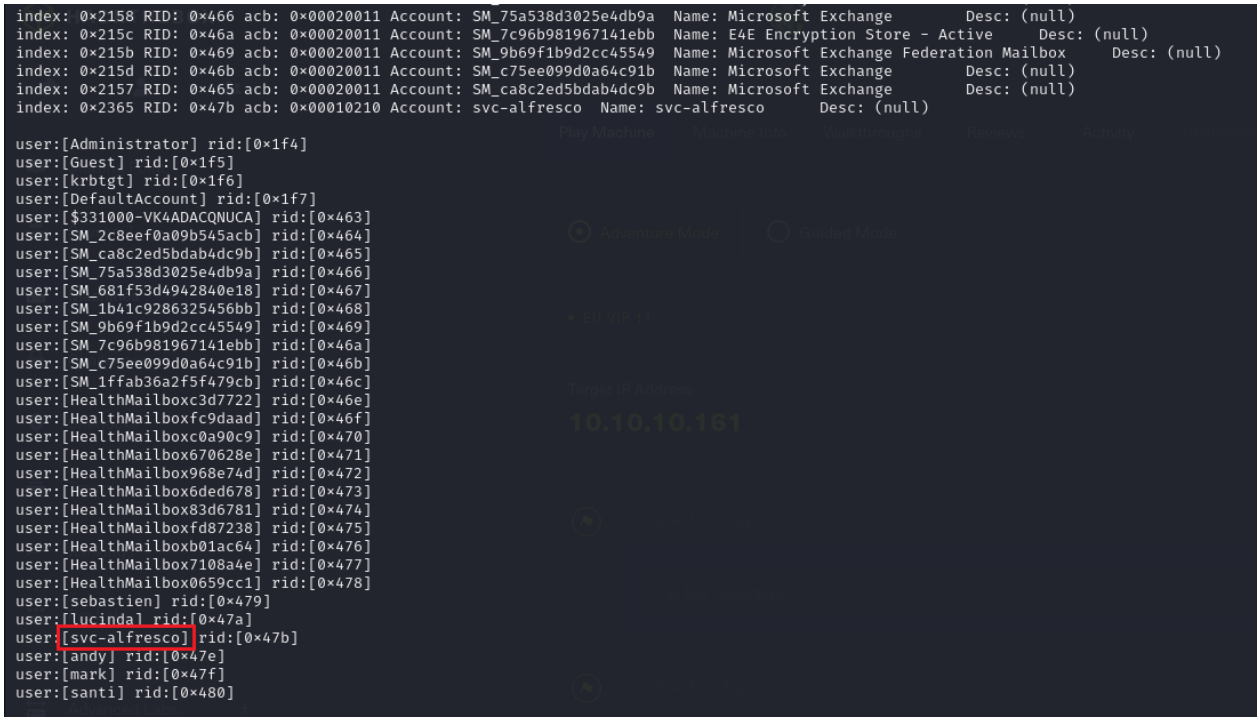

Figure 3 - Users retrieved using Enum4Linux

I checked on the Internet the user $svc - alfresco$ and I found out that it is a service account. Studying the alfresco 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:

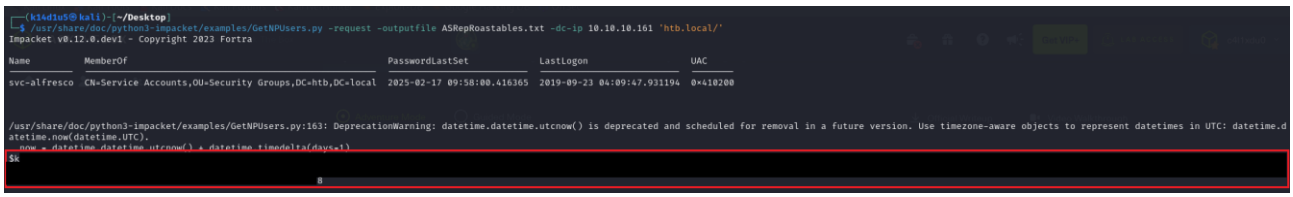

Figure 4 – svc-alfresco Kerberos ticket

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

Figure 5 - Ticket cracked

Luckly, 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:

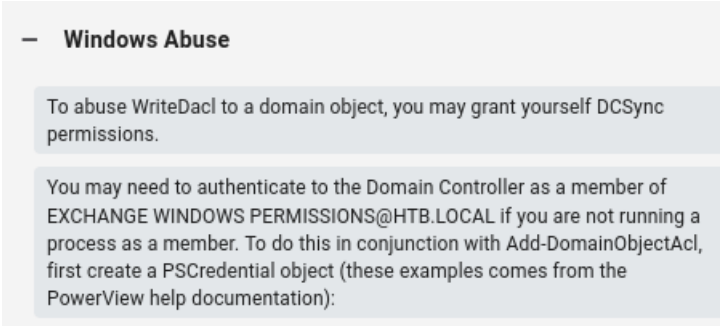

Figure 6 - BloodHound suggested exploitation

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:

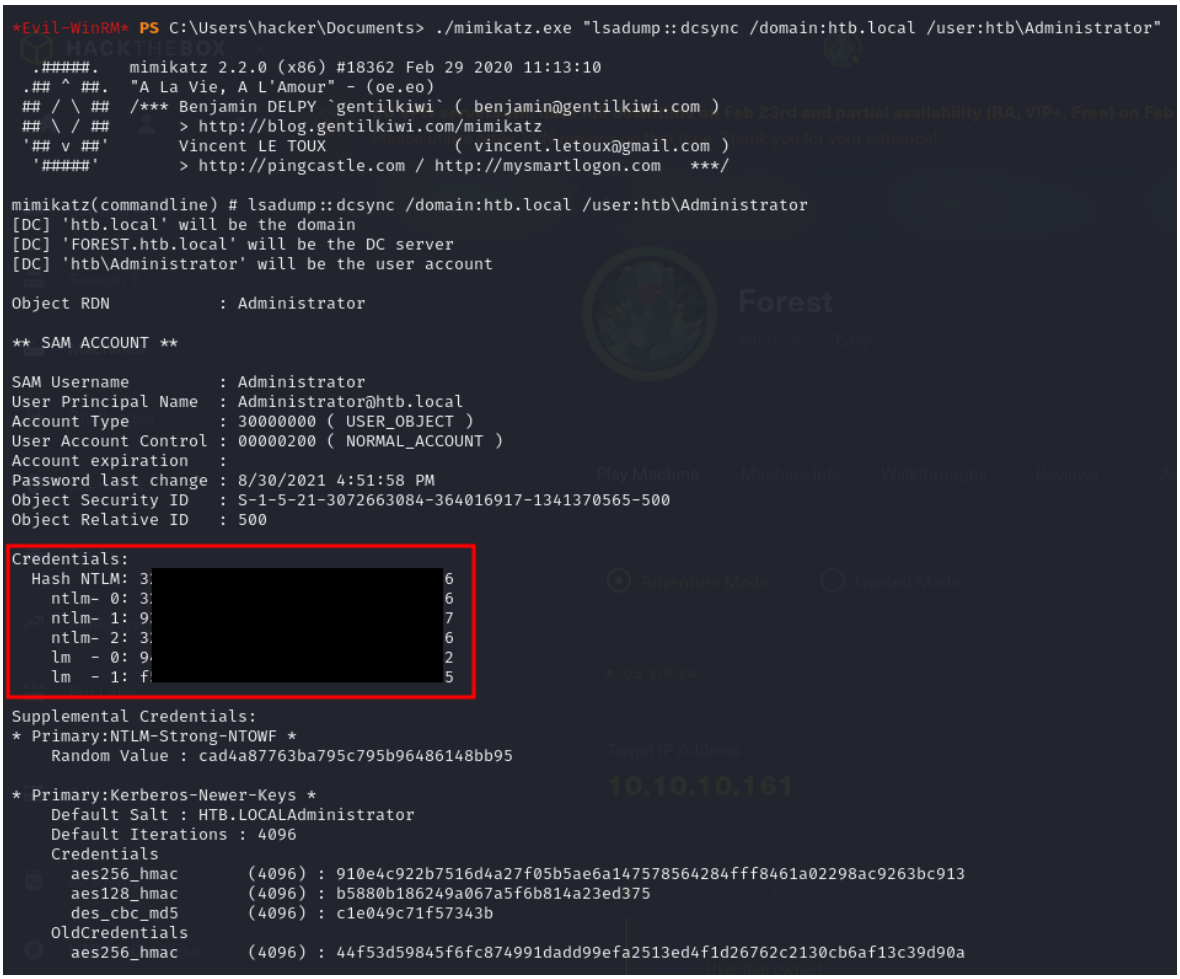

Figure 10 - Administrator NTLM credentials found

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

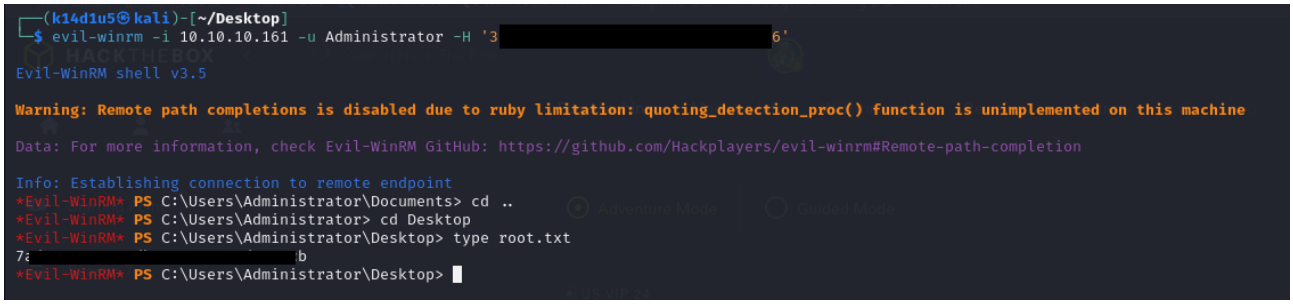

Figure 11 - Root flag

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/.