**Forest walkthrough**

# **Index**

[Index 1](#_Toc193824078)

[List of pictures 1](#_Toc193824079)

[Disclaimer 2](#_Toc193824080)

[Reconnaissance 2](#_Toc193824081)

[Initial foothold 3](#_Toc193824082)

[User flag 3](#_Toc193824083)

[Privilege escalation 4](#_Toc193824084)

[Personal comments 5](#_Toc193824085)

[References 5](#_Toc193824086)

# **List of pictures**

[Figure 1 - nMap scan results (part 1) 2](#_Toc193824053)

[Figure 2 - nMap scan results (part 2) 2](#_Toc193824054)

[Figure 3 - Users retrieved using Enum4Linux 3](#_Toc193824055)

[Figure 4 - svc.alfresco Kerberos ticket 3](#_Toc193824056)

[Figure 5 - Ticket cracked 4](#_Toc193824057)

[Figure 6 - BloodHound suggested exploitation 4](#_Toc193824058)

[Figure 7 - Hacker account created 4](#_Toc193824059)

[Figure 8 - Hacker account added to "Exchange Windows Permission" group 4](#_Toc193824060)

[Figure 9 - Hacker account added to "Remote Management Users" group 4](#_Toc193824061)

[Figure 10 - Administrator NTLM credentials found 5](#_Toc193824062)

[Figure 11 - Root flag 5](#_Toc193824063)

# **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:

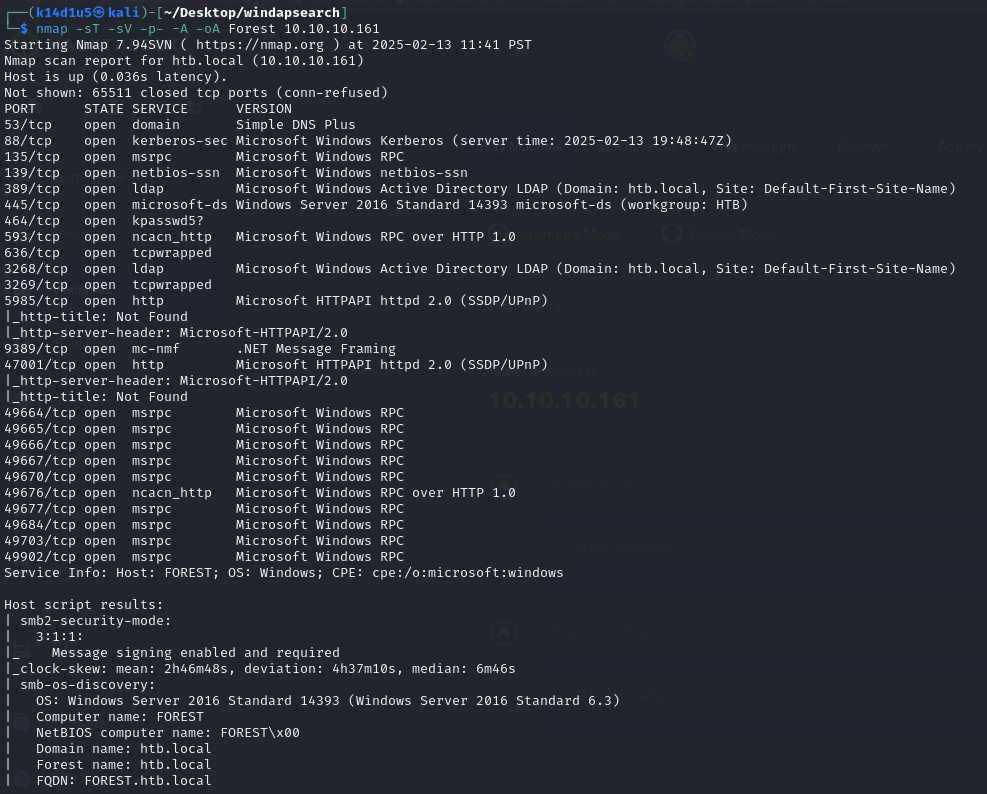


Figure 1 - nMap scan results (part 1)

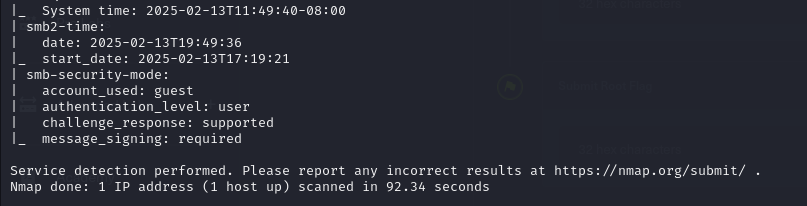


Figure 2 - nMap scan results (part 2)

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:

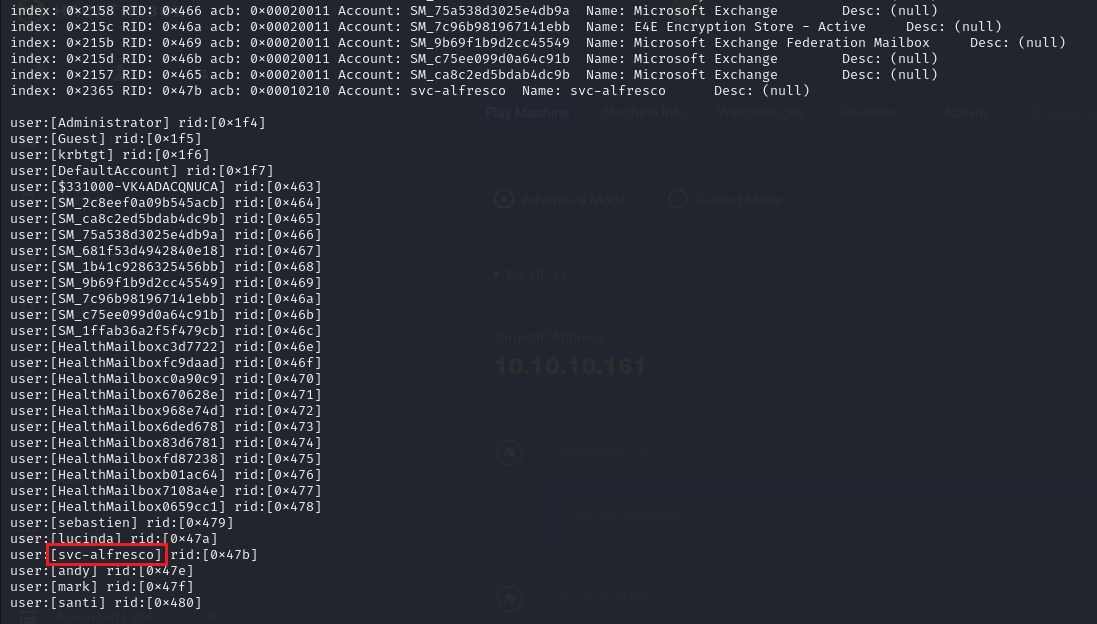


Figure 3 - Users retrieved using Enum4Linux

I checked on the Internet the user 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 user has not Kerberos pre-authentication, I was able to retrieve its Kerberos ticket:

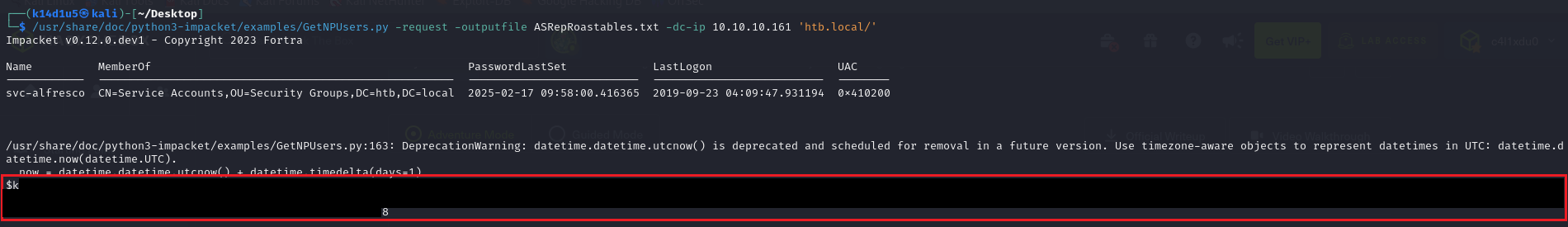


Figure 4 – svc-alfresco Kerberos ticket

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 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 and uploaded these information on BloodHound. I found out an interesting way to escalate my privileges:

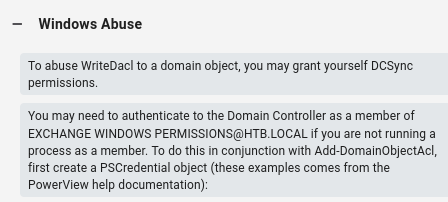


Figure 6 - BloodHound suggested exploitation

At this point, to not ruin my account, I created a new account:



Figure 7 - Hacker account created

This new account needed some privileges and groups:



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



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:

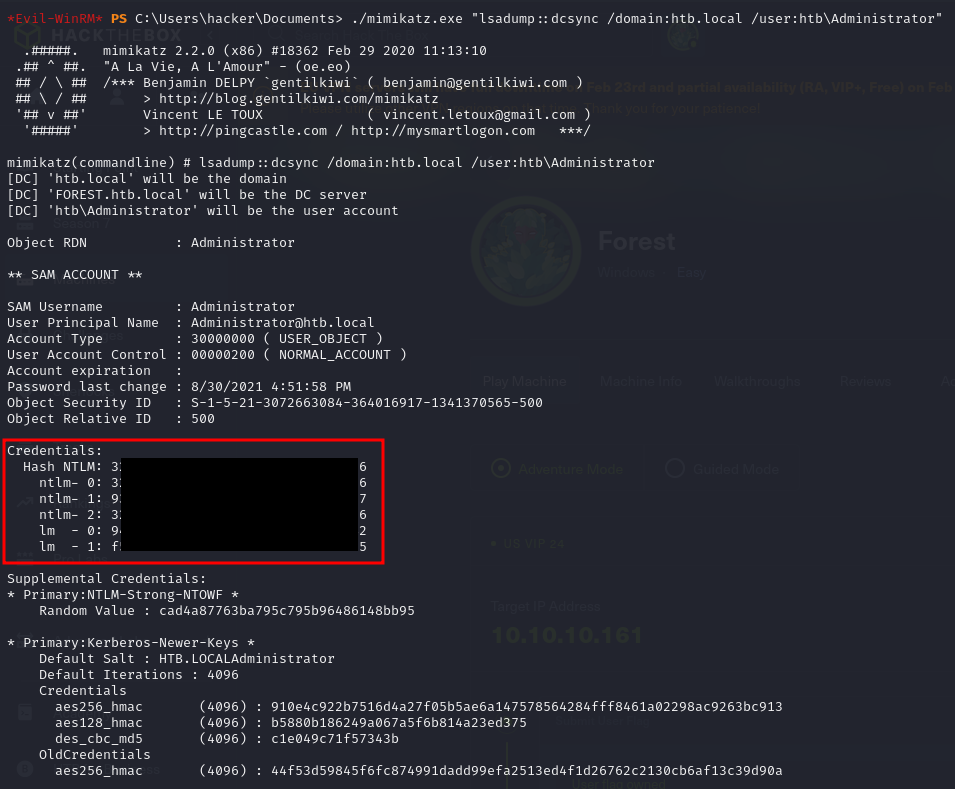


Figure 10 - Administrator NTLM credentials found

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

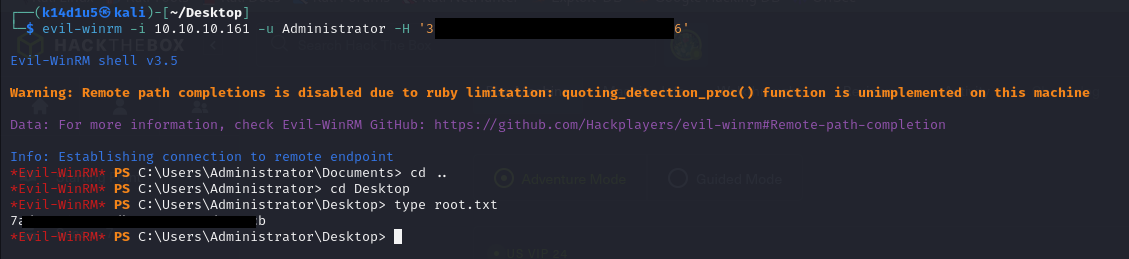


Figure 11 - Root flag

# **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/>.