**WRITE-UPS FOR Manager –** *solve on 02/08/2024*

1. **Get the access**

First, we do some nmap to find out more about the machine. These are what I could find:

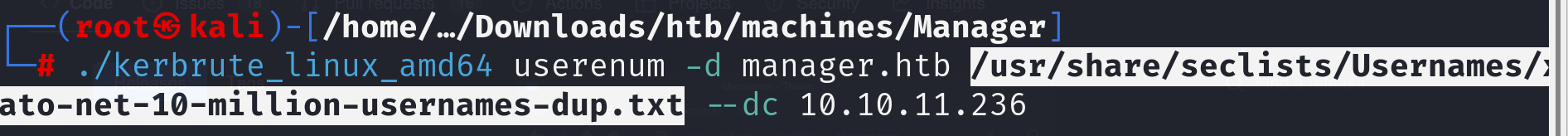
* Microsoft Windows Active Directory LDAP
* Microsoft Windows Kerberos
* Microsoft Windows RPC / over HTTP 1.0
* 445/tcp open microsoft-ds?
* 464/tcp open kpasswd5?
* Microsoft SQL Server 2019

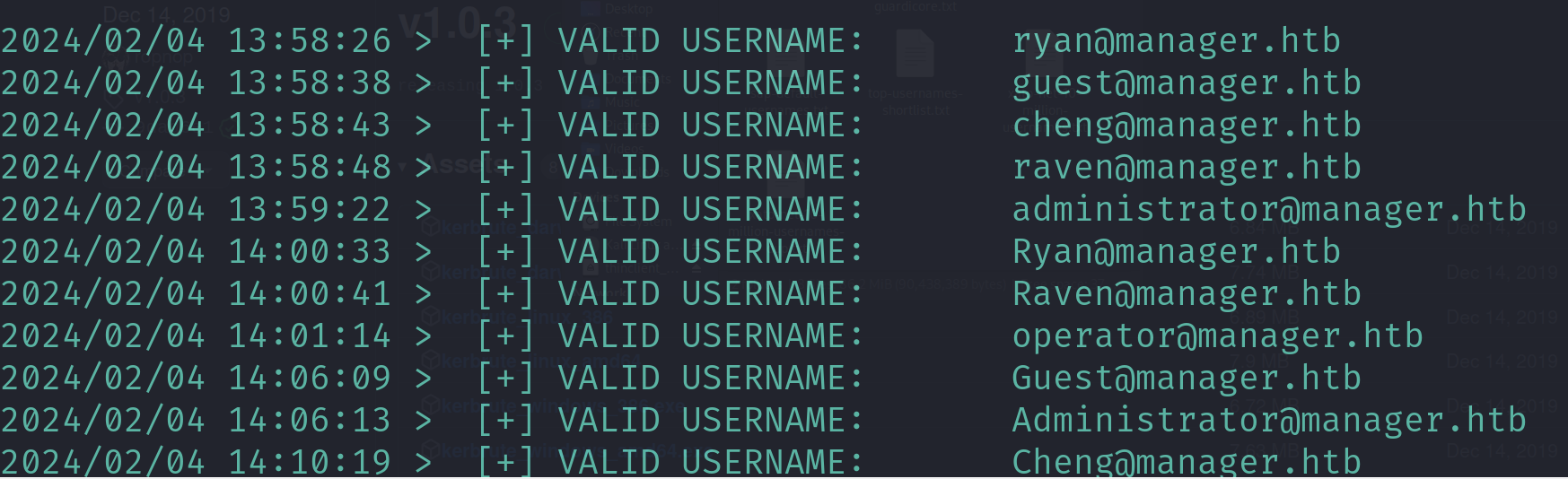
By *Microsoft Windows Kerberos*, I looking for

*Kerberos* Exploitation:

<https://book.hacktricks.xyz/network-services-pentesting/pentesting-kerberos-88>

* <https://github.com/ropnop/kerbrute/releases>





For *Microsoft Windows Active Directory LDAP*

*LDAP Exploitation*:

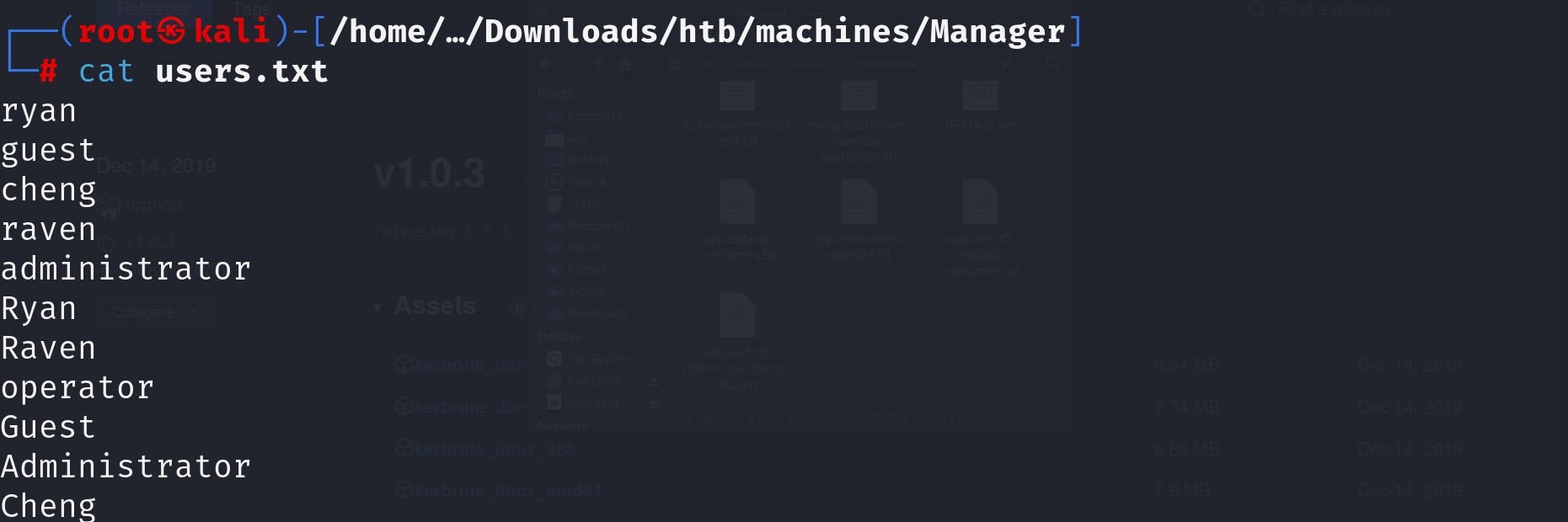
<https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb>

After readding the docs, I found out that we have to use *crackmapexec*, then I start looking how to use it

How to use *crackmapexec*:

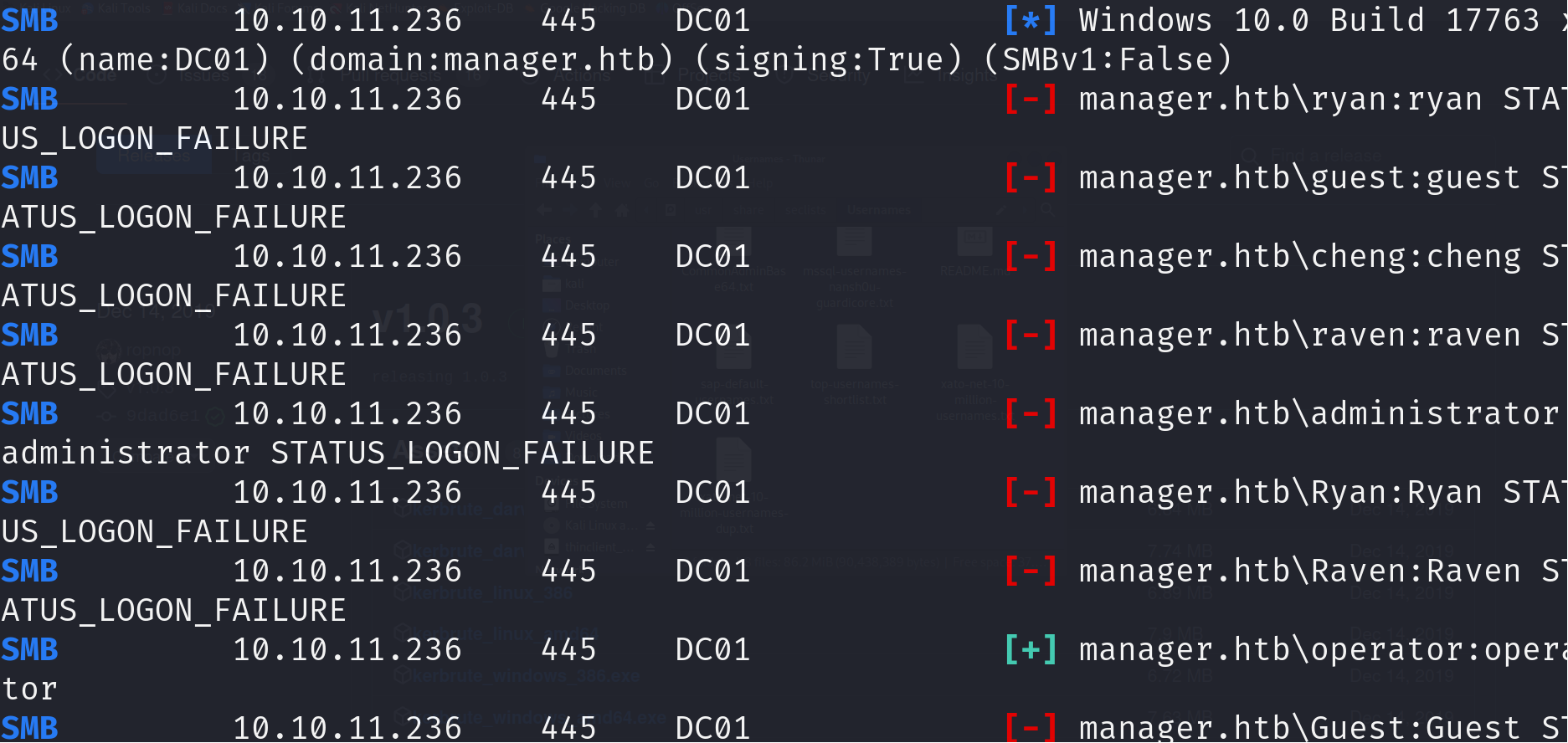
<https://www.poplabsec.com/kerberoasting-with-crackmapexec/>

Do as the instruction, after that, I write users that I found into a file call *users.txt* (Do not confuse with the user flag ^^)



Use *crackmapexec* to find if any user is vulnerable and hurray, the *operator* one

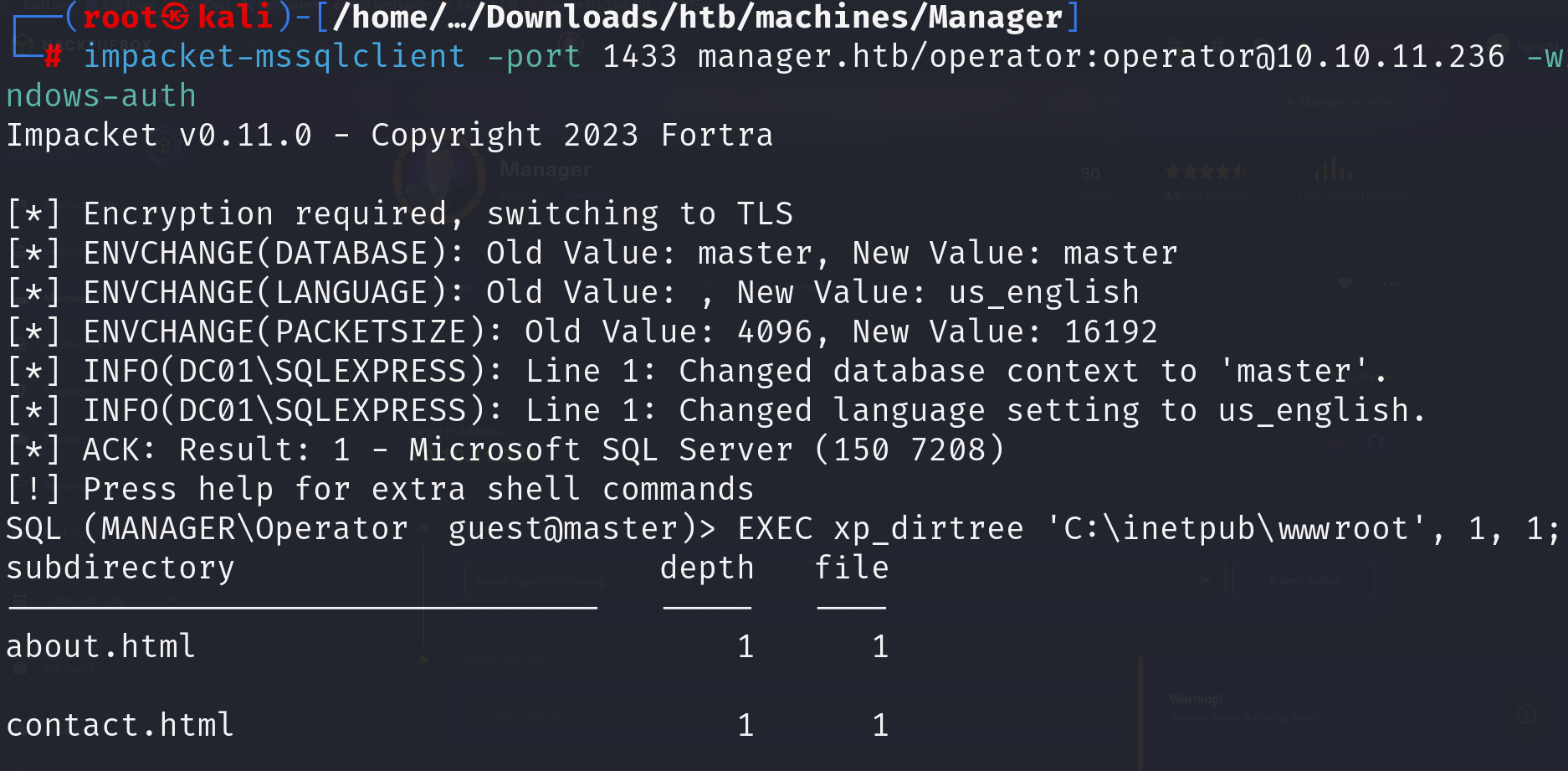




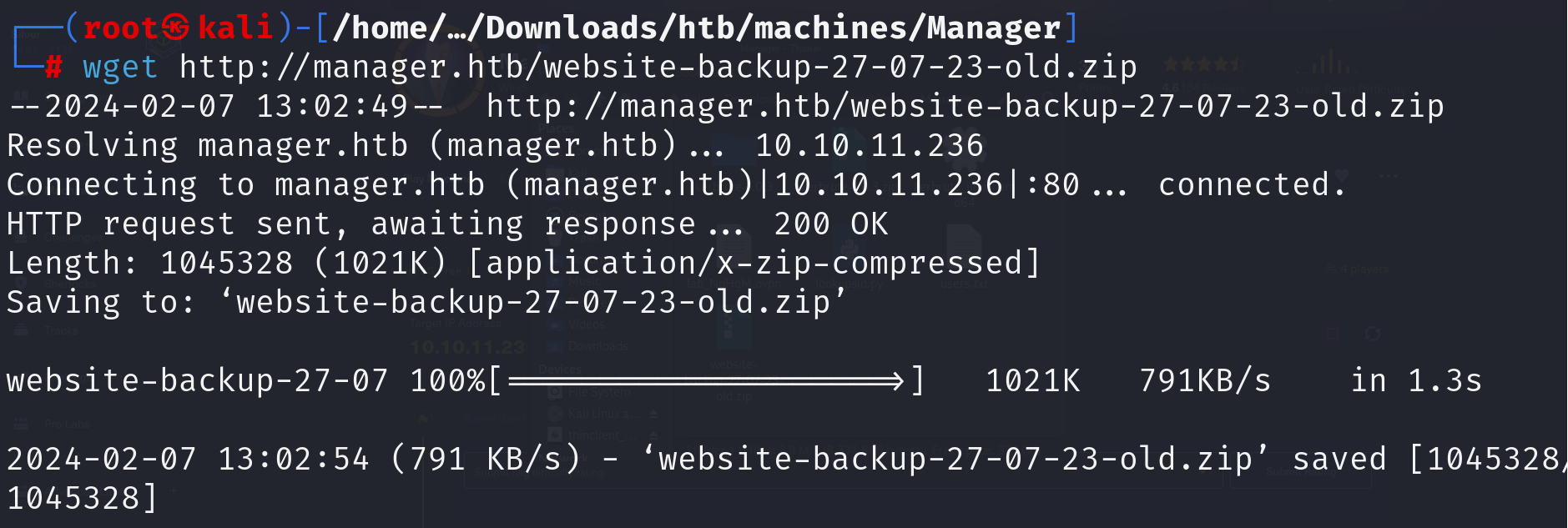
Continue with out *nmap* result, I try to exploit *Microsoft SQL Server on port 1433*. So I looked up the Internet and found this link useful.

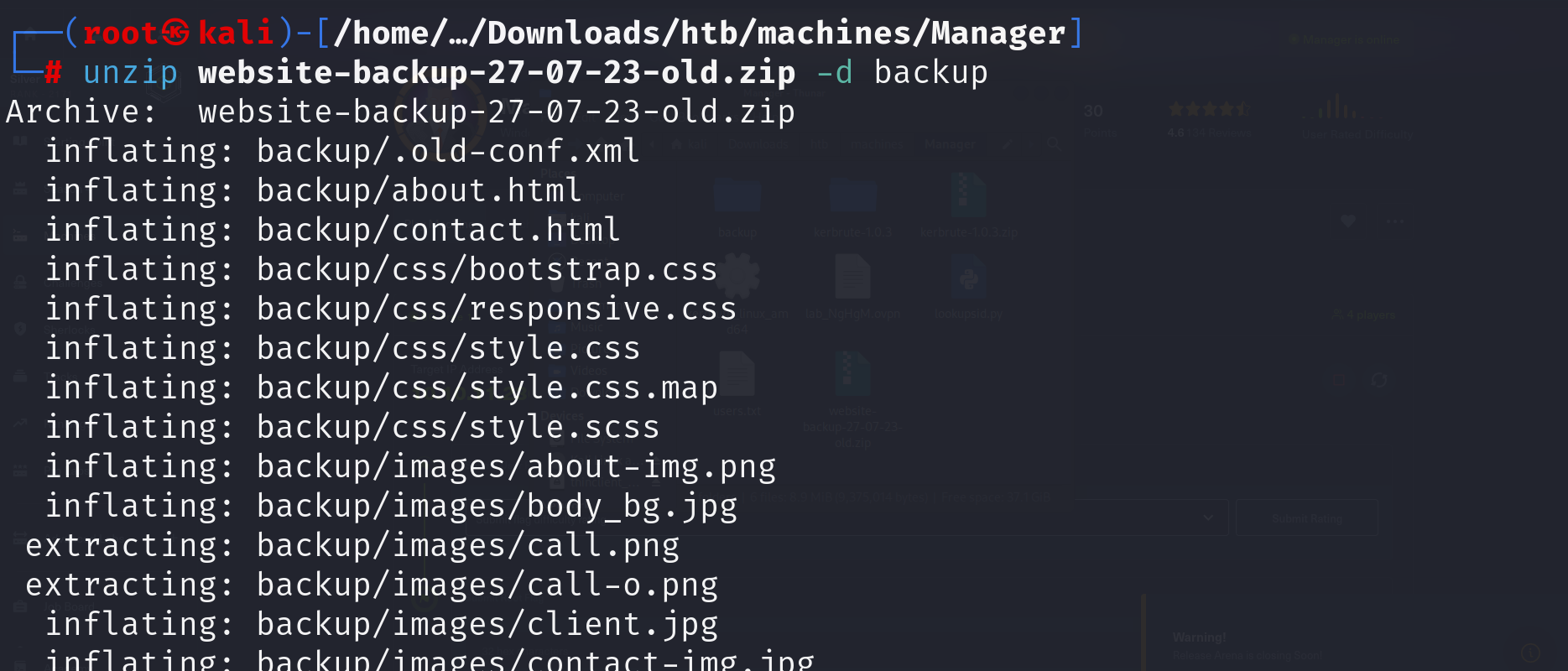
<https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server>

Continuing the docs, let’s use *mssqlclient* to exploit the vulnerability to get the reverse shell



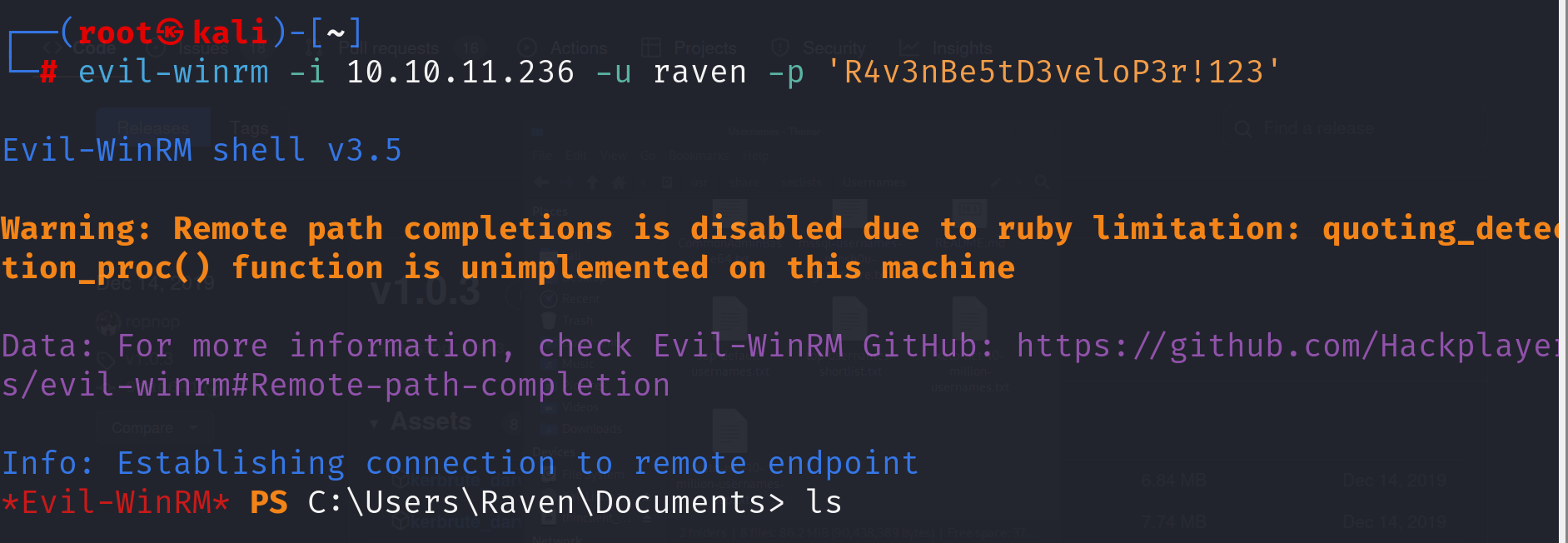
Found a *backup.zip* file seems intriguing, I got it, unzip it and found a credential.







Great, now we use *evil-winrm* to access the machine. And **USER FLAG** ‘ll be at our hand.



1. **Priviledge Escalation**

After looking around for a while, there’s nothing useful.

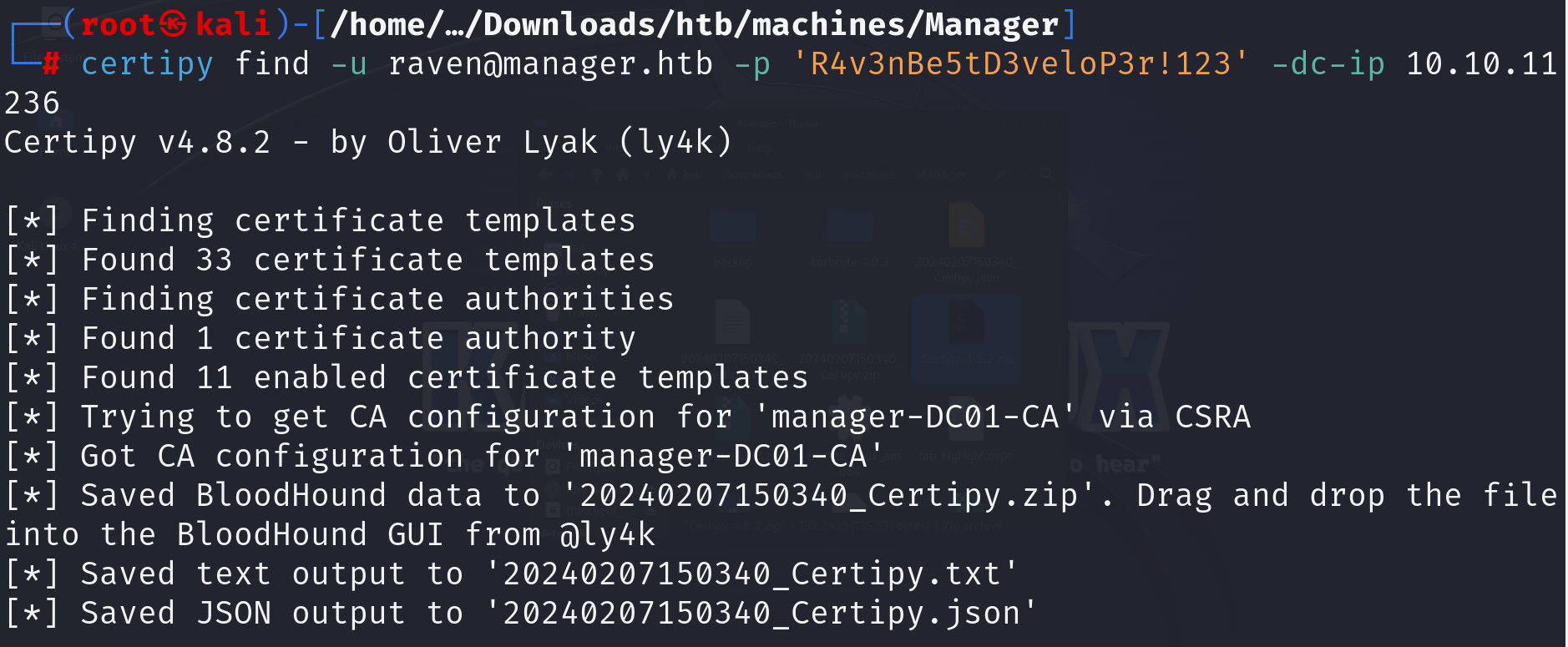
*SeMachineAccountPrivilege Add workstations to domain Enabled*

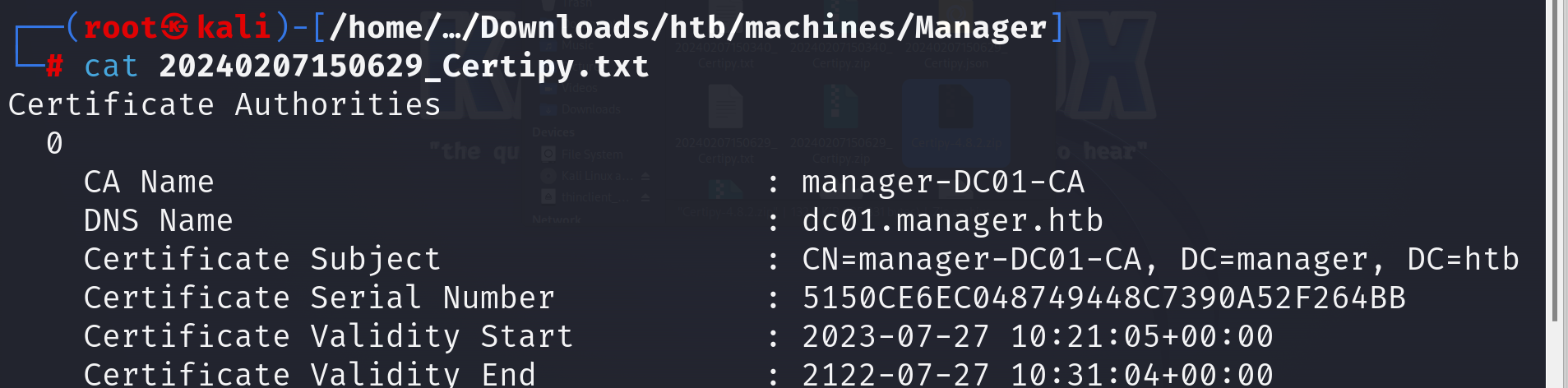
*SeChangeNotifyPrivilege Bypass traverse checking Enabled*

*SeIncreaseWorkingSetPrivilege Increase a process working set Enabled*

So I try to find if there is a vulnerable certificate I could exploit. I seems to be the *manager-DC01-CA*.

<https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation?source=post_page-----c56f238991c0-------------------------------->

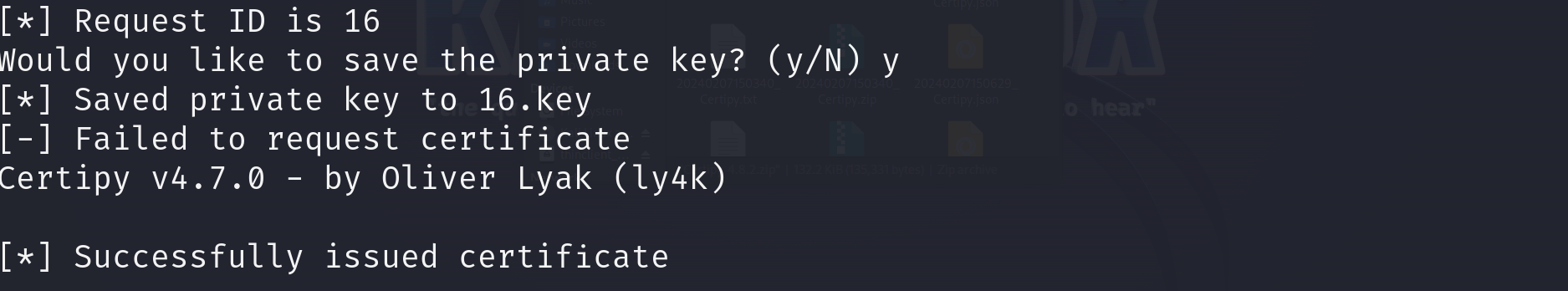




Using the command in the documents

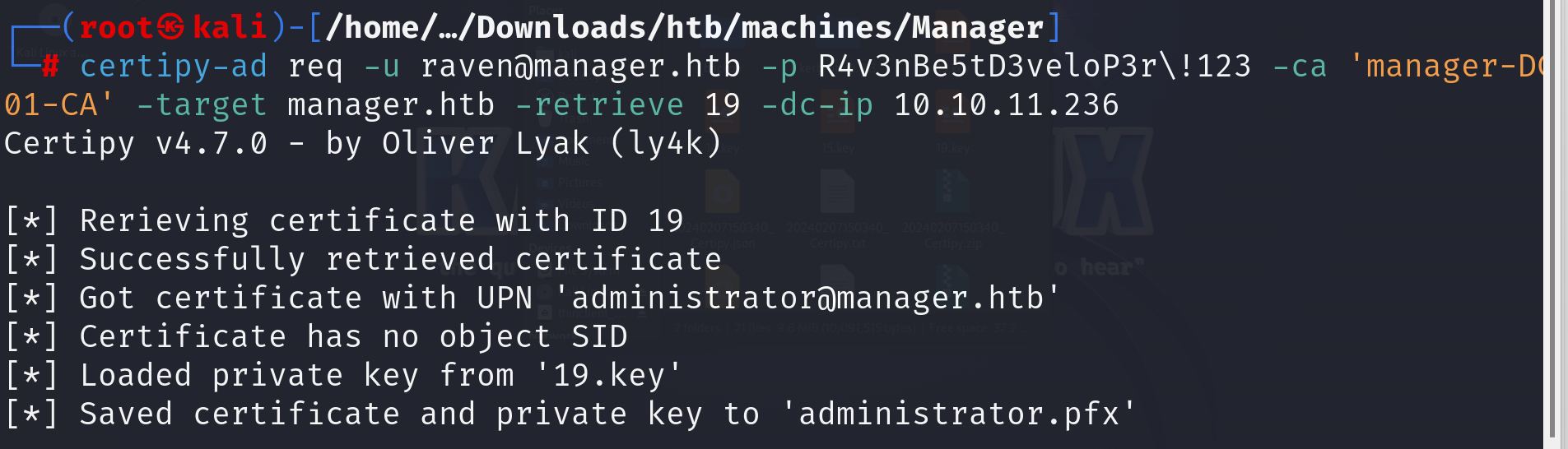
After unsuccessfully trying command separately, I decided to use them all.





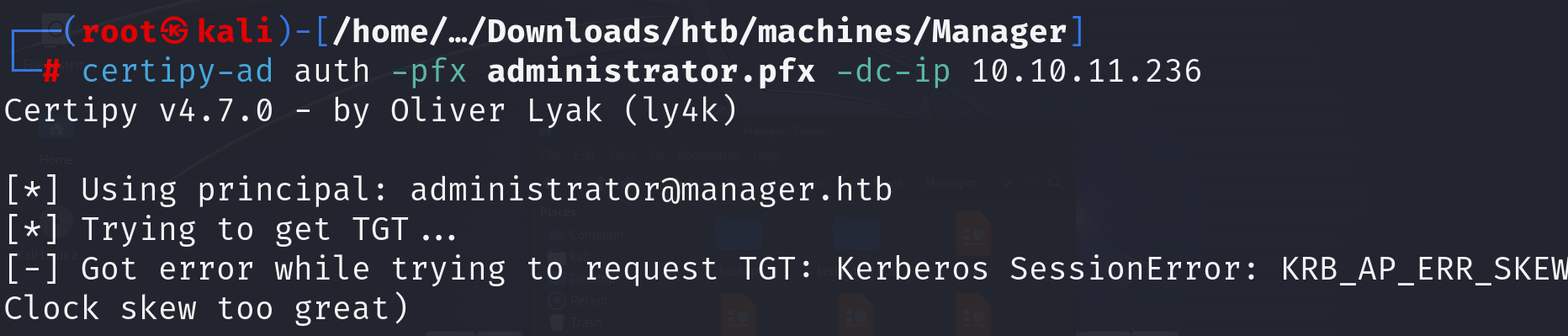
Hurray, now we successfully issued the certificate.

Next step, I save certificate and private key to *administrator.pfx*



We got trouble with time issue (demonstrated in the below PNG). So I search the internet, it’s because the time is not synchronize with the target.

I use this command that worked for me: *rdate -n manager.htb*



After all things work well, I have got the HASH. And the last thing is to connect to the victim using *evil-winrm*. ALL THINGS DONE.!!!

