

Support - Copy

Support

- Target: 10.10.11.174
- HTB , Windows machine

Ping

- As we can see target is alive with "ttl=127" (probably a windows machine).

```
ping 10.10.11.174
```

```
└─ ping 10.10.11.174
PING 10.10.11.174 (10.10.11.174) 56(84) bytes of data.
64 bytes from 10.10.11.174: icmp_seq=1 ttl=127 time=25.1 ms
```

Nmap

```
nmap -T4 -A -v 10.10.11.174
```

```

Host is up (0.027s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2023-11-29 16:17:03Z)
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: support.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: support.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (85%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.018 days (since Wed Nov 29 15:52:36 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-11-29T16:17:10
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   30.51 ms  10.10.14.1
2   30.70 ms  10.10.11.174

NSE: Script Post-scanning.
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Initiating NSE at 16:17
Completed NSE at 16:17, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
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 57.45 seconds
Raw packets sent: 2077 (95.072KB) | Rcvd: 40 (2.448KB)

```

crackmapexec

```
cme smb 10.10.11.174 -u 'anonymous' -p '' --rid-brute
```

```
kali@kali: ~  
cme smb 10.10.11.174 -u 'anonymous' -p '' --rid-brute  
SMB 10.10.11.174 445 DC [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True)  
(SMBv1:False)  
SMB 10.10.11.174 445 DC [+] support.htb\anonymous:  
SMB 10.10.11.174 445 DC 498: SUPPORT\Enterprise Read-only Domain Controllers (SidTypeGroup)  
SMB 10.10.11.174 445 DC 500: SUPPORT\Administrator (SidTypeUser)  
SMB 10.10.11.174 445 DC 501: SUPPORT\Guest (SidTypeUser)  
SMB 10.10.11.174 445 DC 502: SUPPORT\krbtgt (SidTypeUser)  
SMB 10.10.11.174 445 DC 512: SUPPORT\Domain Admins (SidTypeGroup)  
SMB 10.10.11.174 445 DC 513: SUPPORT\Domain Users (SidTypeGroup)  
SMB 10.10.11.174 445 DC 514: SUPPORT\Domain Guests (SidTypeGroup)  
SMB 10.10.11.174 445 DC 515: SUPPORT\Domain Computers (SidTypeGroup)  
SMB 10.10.11.174 445 DC 516: SUPPORT\Domain Controllers (SidTypeGroup)  
SMB 10.10.11.174 445 DC 517: SUPPORT\Cert Publishers (SidTypeAlias)  
SMB 10.10.11.174 445 DC 518: SUPPORT\Schema Admins (SidTypeGroup)  
SMB 10.10.11.174 445 DC 519: SUPPORT\Enterprise Admins (SidTypeGroup)  
SMB 10.10.11.174 445 DC 520: SUPPORT\Group Policy Creator Owners (SidTypeGroup)  
SMB 10.10.11.174 445 DC 521: SUPPORT\Read-only Domain Controllers (SidTypeGroup)  
SMB 10.10.11.174 445 DC 522: SUPPORT\Cloneable Domain Controllers (SidTypeGroup)  
SMB 10.10.11.174 445 DC 525: SUPPORT\Protected Users (SidTypeGroup)  
SMB 10.10.11.174 445 DC 526: SUPPORT\Key Admins (SidTypeGroup)  
SMB 10.10.11.174 445 DC 527: SUPPORT\Enterprise Key Admins (SidTypeGroup)  
SMB 10.10.11.174 445 DC 553: SUPPORT\RAS and IAS Servers (SidTypeAlias)  
SMB 10.10.11.174 445 DC 571: SUPPORT\Allowed RODC Password Replication Group (SidTypeAlias)  
SMB 10.10.11.174 445 DC 572: SUPPORT\Denied RODC Password Replication Group (SidTypeAlias)  
SMB 10.10.11.174 445 DC 1000: SUPPORT\DC$ (SidTypeUser)  
SMB 10.10.11.174 445 DC 1101: SUPPORT\DnsAdmins (SidTypeAlias)  
SMB 10.10.11.174 445 DC 1102: SUPPORT\DnsUpdateProxy (SidTypeGroup)  
SMB 10.10.11.174 445 DC 1103: SUPPORT\Shared Support Accounts (SidTypeGroup)  
SMB 10.10.11.174 445 DC 1104: SUPPORT\ldap (SidTypeUser)  
SMB 10.10.11.174 445 DC 1105: SUPPORT\support (SidTypeUser)  
SMB 10.10.11.174 445 DC 1106: SUPPORT\smith.rosario (SidTypeUser)  
SMB 10.10.11.174 445 DC 1107: SUPPORT\hernandez.stanley (SidTypeUser)  
SMB 10.10.11.174 445 DC 1108: SUPPORT\wilson.shelby (SidTypeUser)  
SMB 10.10.11.174 445 DC 1109: SUPPORT\anderson.damian (SidTypeUser)  
SMB 10.10.11.174 445 DC 1110: SUPPORT\thomas.rafael (SidTypeUser)  
SMB 10.10.11.174 445 DC 1111: SUPPORT\levine.leopoldo (SidTypeUser)  
SMB 10.10.11.174 445 DC 1112: SUPPORT\raven.clifton (SidTypeUser)  
SMB 10.10.11.174 445 DC 1113: SUPPORT\bardot.mary (SidTypeUser)  
SMB 10.10.11.174 445 DC 1114: SUPPORT\cromwell.gerard (SidTypeUser)  
SMB 10.10.11.174 445 DC 1115: SUPPORT\monroe.david (SidTypeUser)  
SMB 10.10.11.174 445 DC 1116: SUPPORT\west.laura (SidTypeUser)  
SMB 10.10.11.174 445 DC 1117: SUPPORT\langley.lucy (SidTypeUser)  
SMB 10.10.11.174 445 DC 1118: SUPPORT\daughtler.mabel (SidTypeUser)  
SMB 10.10.11.174 445 DC 1119: SUPPORT\stoll.rachelle (SidTypeUser)  
SMB 10.10.11.174 445 DC 1120: SUPPORT\ford.victoria (SidTypeUser)  
SMB 10.10.11.174 445 DC 2601: SUPPORT\MANAGEMENT$ (SidTypeUser)
```

```
cat u.txt |grep -i user |rev |cut -f2 -d ' ' |rev |grep SUPPO |cut -f2 -d  
'\' |grep -Ev (DC|SVC) |tail -n +4 > users.txt
```

```
└─ cat users.txt
ldap
support
smith.rosario
hernandez.stanley
wilson.shelby
anderson.damian
thomas.rafael
levine.leopoldo
raven.clifton
bardot.mary
cromwell.gerard
monroe.david
west.laura
lingley.lucy
daughtler.mabel
stoll.rachelle
ford.victoria
MANAGEMENT$
```

```
cme smb 10.10.11.174 -u 'anonymous' -p '' --shares
SMB 10.10.11.174 445 DC [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.174 445 DC [+] support.htb\anonymous:
SMB 10.10.11.174 445 DC [*] Enumerated shares
SMB 10.10.11.174 445 DC
```

	Share	Permissions	Remark
SMB	-----	-----	-----
SMB	ADMIN\$		Remote Admin
SMB	C\$		Default share
SMB	IPC\$	READ	Remote IPC
SMB	NETLOGON		Login server share
SMB	support-tools	READ	support staff tools
SMB	SYSVOL		Login server share

```
file UserInfo.exe
UserInfo.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```