# Support - Copy

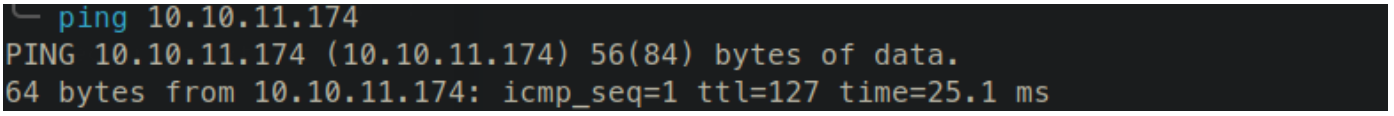
## Support

- 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
```



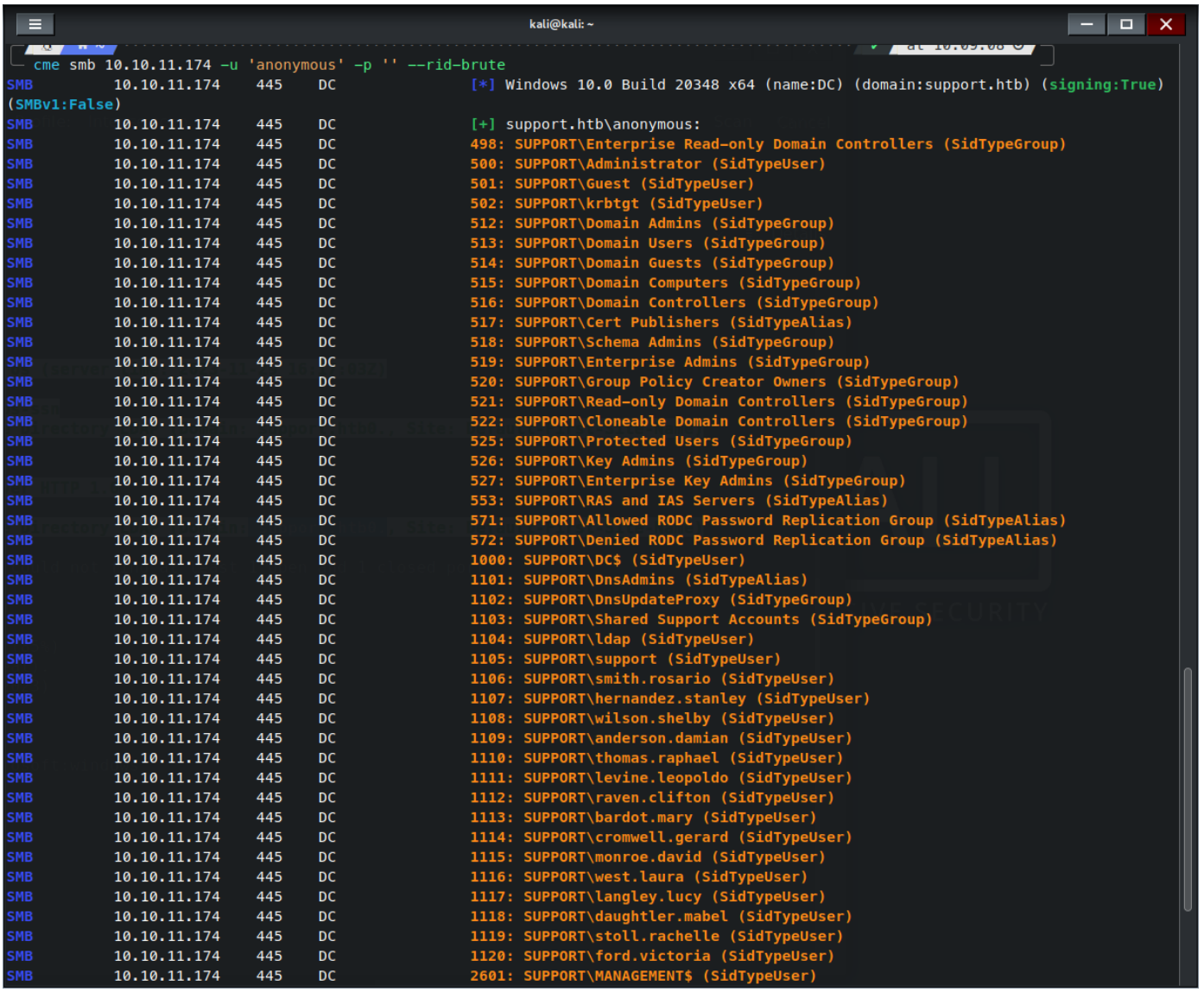

### Nmap

```
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
```




```
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
```

Result:

```
└─ cat users.txt
ldap
support
smith.rosario
hernandez.stanley
wilson.shelby
anderson.damian
thomas.raphael
levine.leopoldo
raven.clifton
bardot.mary
cromwell.gerard
monroe.david
west.laura
langley.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) (si
gning: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         10.10.11.174    445    DC              -----           -----------     ------
SMB         10.10.11.174    445    DC              ADMIN$                          Remote Admin
SMB         10.10.11.174    445    DC              C$                              Default share
SMB         10.10.11.174    445    DC              IPC$            READ            Remote IPC
SMB         10.10.11.174    445    DC              NETLOGON                        Logon server share
SMB         10.10.11.174    445    DC              support-tools   READ            support staff tools
SMB         10.10.11.174    445    DC              SYSVOL                          Logon server share
```

```
~/ctf/support/userinfo
└─ file UserInfo.exe
UserInfo.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```