Dropzone(AD),tftp(AD訊息收集)

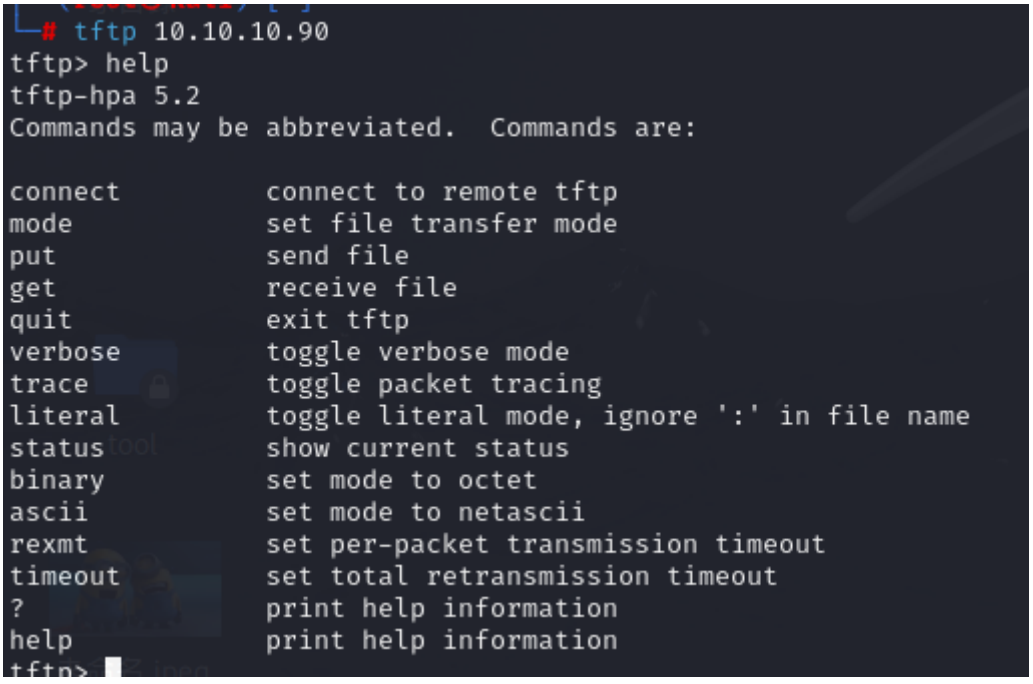
```
—# nmap -sCV -p69 -A 10.10.10.90
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 06:56 EDT
Nmap scan report for 10.10.10.90
Host is up (0.27s latency).

PORT   STATE    SERVICE VERSION
69/tcp filtered tftp
Device type: specialized|general purpose
Running: AKCP embedded, General Dynamics embedded, Microsoft Windows 2000|2003|XP
OS CPE: cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2003
cpe:/o:microsoft:windows_xp::sp2
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   274.69 ms 10.10.14.1
2   275.04 ms 10.10.10.90

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 13.00 seconds
```

測試都只有tftp Port



測試上傳一個文件(成功)，但不能讀取到(但沒報錯)。。

顯示`C:\`看起來像windows

```
tftp> get test.txt
Error code 1: Could not find file 'C:\test.txt'.
tftp> put test.txt
tftp> get test.txt
tftp> ?
tftp-hpa 5.2
```

SAM設定取得密碼?(無法)

```
tftp> get /etc/passwd
Transfer timed out.

tftp> get Windows\System32\config\sam
Transfer timed out.

tftp> get \Windows\System32\config\sam
Error code 1: The process cannot access the file 'C:\Windows\System32\config\sam' because it is being used by another process.
tftp> get \windows\system32\config\sam
Error code 5: Connection isn't established.
```

下載`\windows\system32\license.rtf`或`\windows\system32\eula.txt`這兩個檔案將協助確定Windows 作業系統的版本。

在`\windows\system32\eula.txt`找到是XP版本

```
tftp> get \windows\system32\eula.txt
tftp>


┌──(root㉿kali)-[~]
└─# head \\windows\\system32\\eula.txt
END-USER LICENSE AGREEMENT FOR MICROSOFT
SOFTWARE

MICROSOFT WINDOWS XP PROFESSIONAL EDITION
SERVICE PACK 3

IMPORTANT-READ CAREFULLY: This End-User
License Agreement ('EULA') is a legal
agreement between you (either an individual
or a single entity) and Microsoft Corporation
```