Silo,Oracle套件放棄

```
└─# nmap -sCV -
p80,135,139,445,1521,5985,8080,47001,49152,49153,49154,49155,49159,49160,49161,49162,6
1080 -A 10.10.10.82
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 02:42 EDT
Nmap scan report for 10.10.10.82
Host is up (0.28s latency).

PORT      STATE  SERVICE      VERSION
80/tcp    open   http         Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
| http-methods: 
|_  Potentially risky methods: TRACE
135/tcp   open   msrpc        Microsoft Windows RPC
139/tcp   open   netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open   microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1521/tcp  open   oracle-tns   Oracle TNS listener 11.2.0.2.0 (unauthorized)
5985/tcp  open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open   http         Oracle XML DB Enterprise Edition httpd
| http-auth: 
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=XDB
|_http-title: 401 Unauthorized
|_http-server-header: Oracle XML DB/Oracle Database
47001/tcp open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open   msrpc        Microsoft Windows RPC
49153/tcp open   msrpc        Microsoft Windows RPC
49154/tcp open   msrpc        Microsoft Windows RPC
49155/tcp open   msrpc        Microsoft Windows RPC
49159/tcp open   oracle-tns   Oracle TNS listener (requires service name)
49160/tcp open   msrpc        Microsoft Windows RPC
49161/tcp open   msrpc        Microsoft Windows RPC
49162/tcp open   msrpc        Microsoft Windows RPC
61080/tcp closed unknown
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=7/20%OT=80%CT=61080%CU=44445%PV=Y%DS=2%DC=T%G=Y%TM=
OS:669B5D08%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=107%TI=I%CI=I%II=I%S
OS:S=S%TS=7)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST1
OS:1%O5=M53CNW8ST11%O6=M53CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000
OS:%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%
OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=
OS:Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R
OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0
OS:%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: supported
| smb2-security-mode:
|   3:0:2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-07-20T06:45:19
|_  start_date: 2024-07-20T06:35:35

TRACEROUTE (using port 61080/tcp)
HOP RTT       ADDRESS
1   316.75 ms 10.10.14.1
2   318.55 ms 10.10.10.82

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 154.44 seconds
```

SMB失敗
80進行目錄爆破有資料，有都顯示server error，
都看到`aspnet_Client`，網路上找到`aspnet_client/system_web/`是敏感目錄，但無法使用。
8080需帳密

1521 Oracle疑似資料庫，有漏洞。但有套件要弄

參考：https://github.com/quentinhardy/odat