Nest(放棄),有VB

```
└──# nmap -sCV -A -p 445,4386 10.10.10.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 22:21 PDT
Nmap scan report for 10.10.10.178
Host is up (0.24s latency).

PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
4386/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LANDesk-RC, LDAPBindReq,
LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq,
TerminalServer, TerminalServerCookie, X11Probe:
|     Reporting Service V1.2
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOptions:
|     Reporting Service V1.2
|     Unrecognised command
|   Help:
|     Reporting Service V1.2
|     This service allows users to run queries against databases using the legacy HQK
format
|     AVAILABLE COMMANDS ---
|     LIST
|     SETDIR <Directory_Name>
|     RUNQUERY <Query_ID>
|     DEBUG <Password>
|_    HELP <Command>
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4386-TCP:V=7.94SVN%I=7%D=4/23%Time=662896DA%P=aarch64-unknown-linux
SF:-gnu%r(NULL,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(G
SF:enericLines,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUn
SF:recognised\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20S
SF:ervice\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOption
SF:s,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised
SF:\x20command\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x2
SF:0V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQ
SF:K\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSVersionBindReqTCP,21
SF:,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSStatusReques
SF:tTCP,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Help,F2,
```

```
SF:"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nThis\x20service\x
SF:20allows\x20users\x20to\x20run\x20queries\x20against\x20databases\x20us
SF:ing\x20the\x20legacy\x20HQK\x20format\r\n\r\n---\x20AVAILABLE\x20COMMAN
SF:DS\x20---\r\n\r\nLIST\r\nSETDIR\x20<Directory_Name>\r\nRUNQUERY\x20<Que
SF:ry_ID>\r\nDEBUG\x20<Password>\r\nHELP\x20<Command>\r\n>")%r(SSLSessionR
SF:eq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalSe
SF:rverCookie,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TL
SF:SSessionReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(K
SF:erberos,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(SMBPr
SF:ogNeg,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(X11Prob
SF:e,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(FourOhFourR
SF:equest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecog
SF:nised\x20command\r\n>")%r(LPDString,21,"\r\nHQK\x20Reporting\x20Service
SF:\x20V1\.2\r\n\r\n>")%r(LDAPSearchReq,21,"\r\nHQK\x20Reporting\x20Servic
SF:e\x20V1\.2\r\n\r\n>")%r(LDAPBindReq,21,"\r\nHQK\x20Reporting\x20Service
SF:\x20V1\.2\r\n\r\n>")%r(SIPOptions,3A,"\r\nHQK\x20Reporting\x20Service\x
SF:20V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(LANDesk-RC,21,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServer,21,"\
SF:r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>");
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone
7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows 7 or
Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft
Windows Server 2008 R2 or Windows 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or
Windows 8 (89%), Microsoft Windows 7 (89%), Microsoft Windows 7 Professional or
Windows 8 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Host script results:
|_clock-skew: -1s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-24T05:24:21
|_  start_date: 2024-04-23T11:33:17
```

```
TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   264.04 ms 10.10.14.1
2   264.02 ms 10.10.10.178

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 213.66 seconds
```

SMB

```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.178
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.178 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

找到文件

```
smb: \Shared\Templates\> cd HR
lsmb: \Shared\Templates\HR\> ls
  .                                   D        0  Wed Aug  7 12:08:01 2019
  ..                                  D        0  Wed Aug  7 12:08:01 2019
  Welcome Email.txt                   A      425  Wed Aug  7 15:55:36 2019

└─# cat 'Welcome Email.txt'
We would like to extend a warm welcome to our newest member of staff, <FIRST
NAME> <SURNAME>

You will find your home folder in the following location:
\\HTB-NEST\Users\<USERNAME>

If you have any issues accessing specific services or workstations, please i
nform the
IT department and use the credentials below until all systems have been set
up for you.

Username: TempUser
Password: welcome2019
```

username : TempUser

paswd : welcome2019

進行smb user帳戶搜尋資料並下載到本地

查詢該使用者可讀文件

```
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
```

在data找到一堆文件，但都在IT資料夾，開始整理

```
┌──(root㉿kali)-[~]
└─# smbclient -U TempUser //10.10.10.178/Data
Password for [WORKGROUP\TempUser]:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Shared
/Maintenance/Maintenance Alerts.txt (0.0 KiloBytes/sec) (average 0.0 KiloByt
es/sec)
getting file \IT\Configs\Adobe\editing.xml of size 246 as IT/Configs/Adobe/e
diting.xml (0.2 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\Options.txt of size 0 as IT/Configs/Adobe/Opt
ions.txt (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\projects.xml of size 258 as IT/Configs/Adobe/
projects.xml (0.2 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\settings.xml of size 1274 as IT/Configs/Adobe
/settings.xml (1.0 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \IT\Configs\Atlas\Temp.XML of size 1369 as IT/Configs/Atlas/Tem
p.XML (1.1 KiloBytes/sec) (average 0.4 KiloBytes/sec)
getting file \IT\Configs\Microsoft\Options.xml of size 4598 as IT/Configs/Mi
crosoft/Options.xml (4.5 KiloBytes/sec) (average 1.0 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as IT/Confi
gs/NotepadPlusPlus/config.xml (5.6 KiloBytes/sec) (average 1.5 KiloBytes/sec
)
getting file \IT\Configs\NotepadPlusPlus\shortcuts.xml of size 2108 as IT/Co
nfigs/NotepadPlusPlus/shortcuts.xml (1.7 KiloBytes/sec) (average 1.5 KiloByt
es/sec)
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as IT/Configs/
RU Scanner/RU_config.xml (0.2 KiloBytes/sec) (average 1.4 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Shared/Te
mplates/HR/Welcome Email.txt (0.3 KiloBytes/sec) (average 1.3 KiloBytes/sec)
smb: \> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disco
nnected now
```

整理完畢

```
┌──(root㉿kali)-[~]
└─# find IT -type f -ls
3598436      4 -rw-r--r--   1 root     root         1369  4月 23 23:14 IT/Configs/Atlas/Temp.XML
3598438      8 -rw-r--r--   1 root     root         6451  4月 23 23:14 IT/Configs/NotepadPlusPlus/config.xml
3598439      4 -rw-r--r--   1 root     root         2108  4月 23 23:14 IT/Configs/NotepadPlusPlus/shortcuts.xml
3598437      8 -rw-r--r--   1 root     root         4598  4月 23 23:14 IT/Configs/Microsoft/Options.xml
3598434      4 -rw-r--r--   1 root     root          258  4月 23 23:14 IT/Configs/Adobe/projects.xml
3598433      0 -rw-r--r--   1 root     root            0  4月 23 23:14 IT/Configs/Adobe/Options.txt
3598435      4 -rw-r--r--   1 root     root         1274  4月 23 23:14 IT/Configs/Adobe/settings.xml
3598432      4 -rw-r--r--   1 root     root          246  4月 23 23:14 IT/Configs/Adobe/editing.xml
3598440      4 -rw-r--r--   1 root     root          270  4月 23 23:14 IT/Configs/RU\ Scanner/RU_config.xml
```

又找到帳密

```
└─# cat IT/Configs/RU\ Scanner/RU_config.xml
<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

```
<Port>389
<Username>c.smith
<Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=
```

密碼解不出來

```
└─# cat passwd|base64 -d |xxd
00000000: 7d31 3301 f603 a33d 58ce 4aa1 4241 fa19  }13....=X.J.BA..
00000010: 0158 2a9d 5763 9866 edb8 ce3f ceb2 6311  .X*.Wc.f...?..c.
```

有發現檔案路徑`cat IT/Configs/NotepadPlusPlus/config.xml`

```
        <File filename="C:\windows\System32\drivers\etc\hosts" />
        <File filename="\\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
        <File filename="C:\Users\C.Smith\Desktop\todo.txt" />
```

有一組security$

沒辦法從外部下載，但能讀取並從內部下載

```
NT_STATUS_NO_SUCH_FILE listing \IT\Carl\*
smb: \IT\Carl\> ls
  .                                   D        0  Wed Aug  7 12:42:14 2
019
  ..                                  D        0  Wed Aug  7 12:42:14 2
019
  Docs                                D        0  Wed Aug  7 12:44:00 2
019
  Reports                             D        0  Tue Aug  6 06:45:40 2
019
  VB Projects                         D        0  Tue Aug  6 07:41:55 2
019

                5242623 blocks of size 4096. 1839374 blocks available
smb: \IT\Carl\> recurse on
smb: \IT\Carl\> prompt off
smb: \IT\Carl\> mget *
getting file \IT\Carl\Docs\ip.txt of size 56 as Docs/ip.txt (0.1 KiloBy
tes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Carl\Docs\mmc.txt of size 73 as Docs/mmc.txt (0.1 Kilo
Bytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner.sln of size 871 as V
```

資訊整理

```
└─# find . -type f -ls
3598454      4 -rw-r--r--   1 root     root          871  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner.sln
3598456      4 -rw-r--r--   1 root     root          772  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/ConfigFile.vb
3598463      8 -rw-r--r--   1 root     root         4888  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/Utils.vb
3598462      4 -rw-r--r--   1 root     root          133  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/SsoIntegration.vb
3598460      8 -rw-r--r--   1 root     root         4828  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/RU\ Scanner.vbproj
3598457      4 -rw-r--r--   1 root     root          279  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/Module1.vb
3598468      4 -rw-r--r--   1 root     root         1163  4月 23 23:52 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/AssemblyInfo.vb
3598466      4 -rw-r--r--   1 root     root          441  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/Application.Designer.vb
3598469      4 -rw-r--r--   1 root     root         2776  4月 23 23:52 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/Resources.Designer.vb
3598470      8 -rw-r--r--   1 root     root         5612  4月 23 23:52 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/Resources.resx
3598472      4 -rw-r--r--   1 root     root          279  4月 23 23:52 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/Settings.settings
3598467      4 -rw-r--r--   1 root     root          481  4月 23 23:52 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/Application.myapp
3598471      4 -rw-r--r--   1 root     root         2989  4月 23 23:52 ./VB\ Projects/WIP/RU/RUScanner/My\ Project/Settings.Designer.vb
3598461      4 -rw-r--r--   1 root     root          143  4月 23 23:51 ./VB\ Projects/WIP/RU/RUScanner/RU\ Scanner.vbproj.user
3598448      4 -rw-r--r--   1 root     root           56  4月 23 23:51 ./Docs/ip.txt
3598449      4 -rw-r--r--   1 root     root           73  4月 23 23:51 ./Docs/mmc.txt
```

卡點有vb看不懂

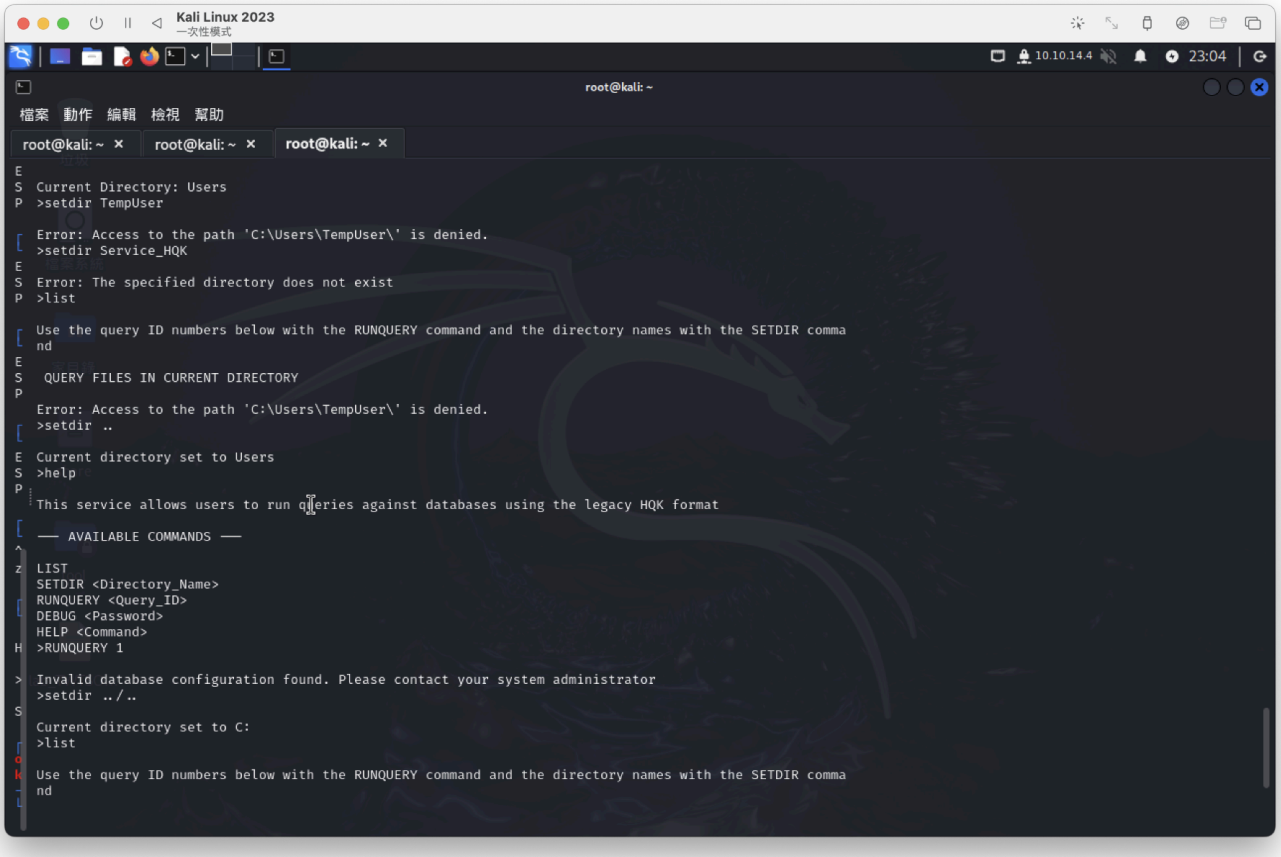
4386 port

nc測試失敗，只用telnet

`HQK Reporting Service V1.2 => 無漏洞`

```
└─# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQK Reporting Service V1.2

>help

This service allows users to run queries against databases using the legacy
HQK format

-- AVAILABLE COMMANDS --

LIST
SETDIR <Directory_Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
>
```

都被deny


Kali Linux 2023
一次性模式
10.10.14.4
23:04
root@kali: ~
檔案 動作 編輯 檢視 幫助
root@kali: ~
root@kali: ~
root@kali: ~
Current Directory: Users
>setdir TempUser
Error: Access to the path 'C:\Users\TempUser\' is denied.
>setdir Service_HQK
Error: The specified directory does not exist
>list
Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR comma
nd
QUERY FILES IN CURRENT DIRECTORY
Error: Access to the path 'C:\Users\TempUser\' is denied.
>setdir ..
Current directory set to Users
>help
This service allows users to run queries against databases using the legacy HQK format
—— AVAILABLE COMMANDS ——
LIST
SETDIR <Directory_Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
>RUNQUERY 1
Invalid database configuration found. Please contact your system administrator
>setdir ../..
Current directory set to C:
>list
Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR comma
nd