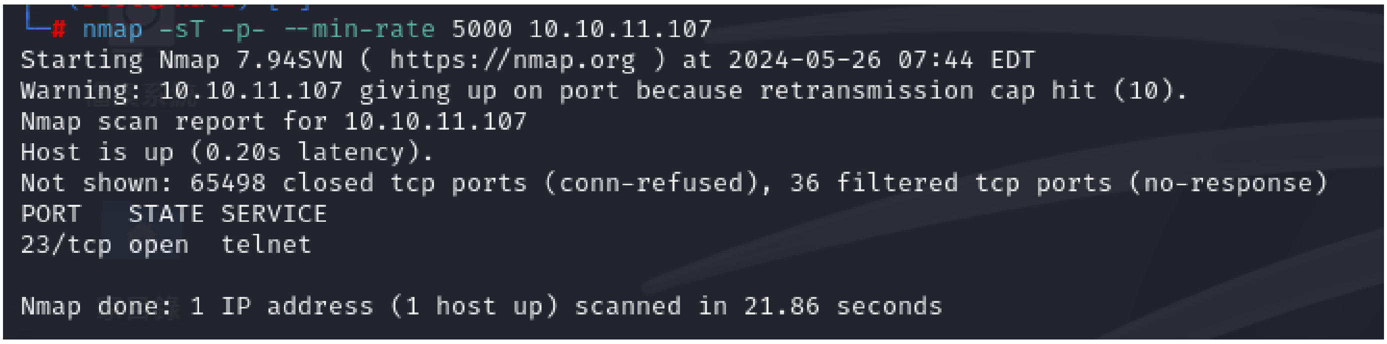
Antique(),snmp

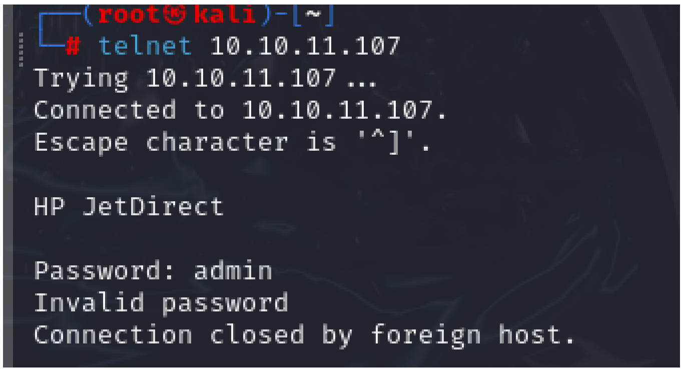
指有單一Port23 ??!
掃了兩次解果一樣



```
└─# nmap -sT -p- --min-rate 5000 10.10.11.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 07:44 EDT
Warning: 10.10.11.107 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.107
Host is up (0.20s latency).
Not shown: 65498 closed tcp ports (conn-refused), 36 filtered tcp ports (no-response)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 21.86 seconds
```

看起來是印表機但無密碼

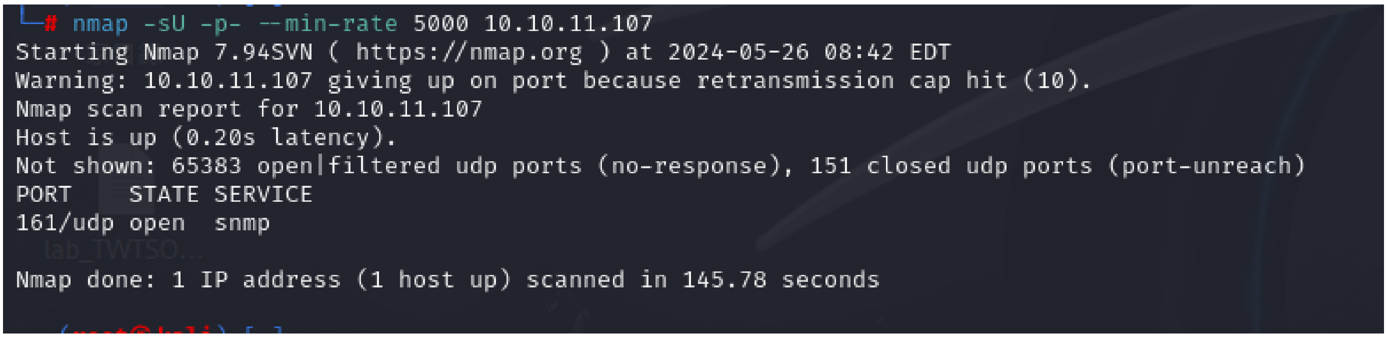


```
┌──(root㉿kali)-[~]
└─# telnet 10.10.11.107
Trying 10.10.11.107...
Connected to 10.10.11.107.
Escape character is '^]'.

HP JetDirect

Password: admin
Invalid password
Connection closed by foreign host.
```

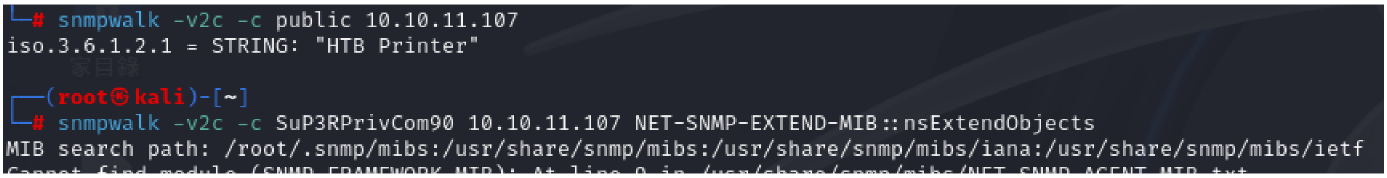
針對UDP掃描有snmp port



```
└─# nmap -sU -p- --min-rate 5000 10.10.11.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-26 08:42 EDT
Warning: 10.10.11.107 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.107
Host is up (0.20s latency).
Not shown: 65383 open|filtered udp ports (no-response), 151 closed udp ports (port-unreach)
PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 145.78 seconds
```

參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-snmp/snmp-rce



```
└─# snmpwalk -v2c -c public 10.10.11.107
iso.3.6.1.2.1 = STRING: "HTB Printer"

┌──(root㉿kali)-[~]
└─# snmpwalk -v2c -c SuP3RPrivCom90 10.10.11.107 NET-SNMP-EXTEND-MIB::nsExtendObjects
MIB search path: /root/.snmp/mibs:/usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf
Cannot find module (SNMP-FRAMEWORK-MIB): At line 0 in /usr/share/snmp/mibs/NET-SNMP-AGENT-MIB.txt
```