nmap□□□

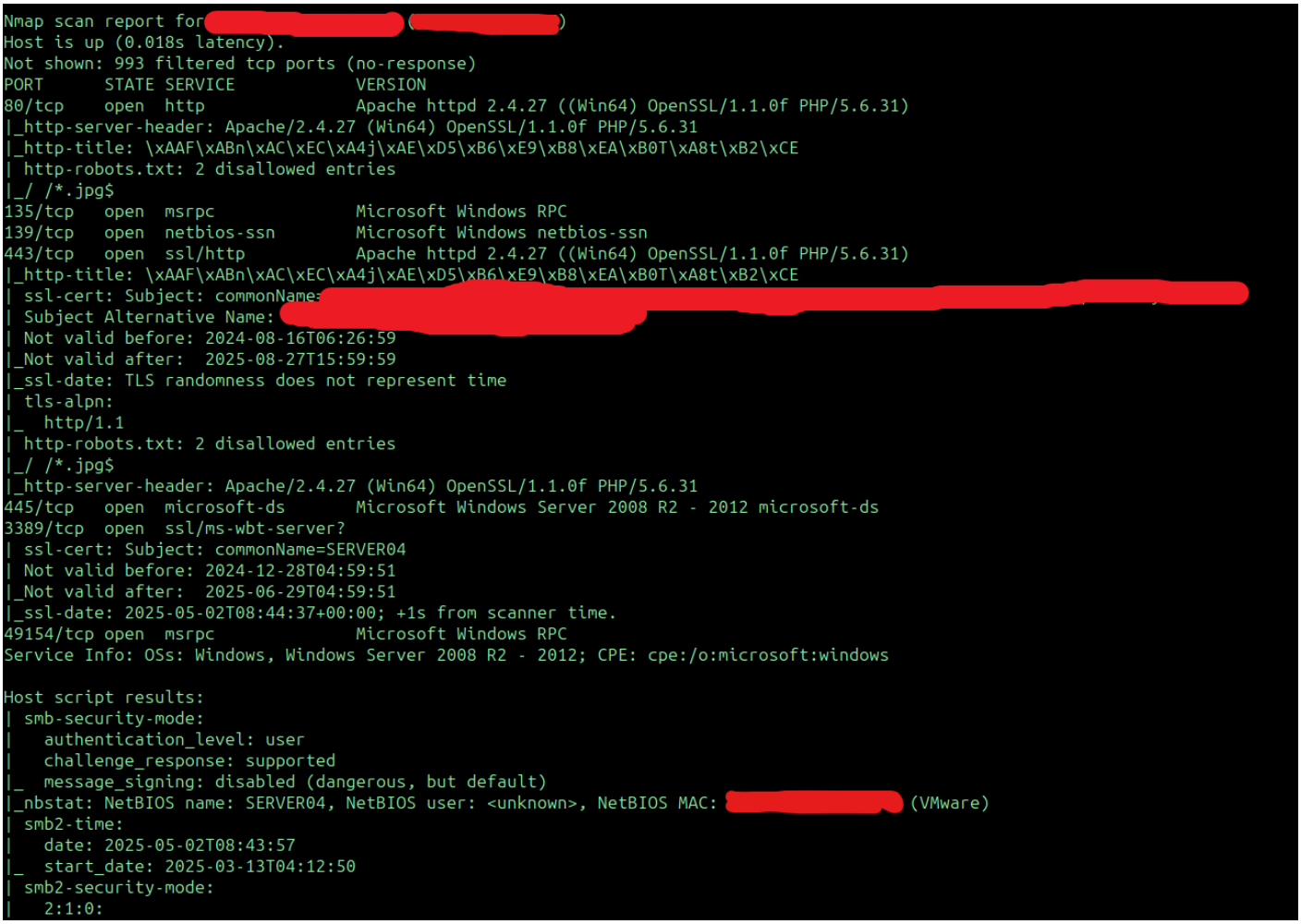
□□□□□

```
nmap -v www.hinet.net
```

```
nmap -A ip□□(□□□□port□□□□□□□□□□□□)
```

EX:□-A -Pn□□

```
nmap -A -Pn {IP}
```



□□□□

```
nmap 192.168.0.* --exclude 192.168.0.100
```

使用排除名單

```
nmap -iL hostlist.txt --excludefile excludelist.txt
```

檢測是否有使用防火牆

```
nmap -sA scanme.nmap.org
```

掃描有防火牆的主機

```
nmap -PN scanme.nmap.org
```

偵測主機是否開機(ping scan)

```
nmap -sP 140.115.35.0/24
```

```
nmap -F www.hinet.net
#快速掃描 也可以使用-T5, 預設-T3
```

按照port做掃描

```
nmap -p 80,443 192.168.1.1
nmap -p 80-200 192.168.1.1
```

使用tcp掃描

```
nmap -p T:80 192.168.1.1
```

使用udp掃描

```
nmap -p U:53 192.168.1.1
```

最常用的10port

```
nmap --top-ports 10 192.168.1.1
```

綜合掃描

```
nmap -sS -P0 -sV -O 192.168.56.102
param:
-sS: Scan Syn
-sV: Determine OS Version
```

```
-P0: Protocol Scan
-O : Operation System
```

script scan

```
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
          directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
          <Lua scripts> is a comma-separated list of script-files or
          script-categories.
```

驗證所有使用的TLS版本

```
nmap --script ssl-enum-ciphers -p 443 {url}
```

如果要驗證整個網段，可以先產生出txt檔。比如10.0.0.0/16的tls

```
echo 10.0.{1..254}.{1..254} >> iplist.txt
```

建立一個sh檔（此例子只檢查tls1.0-1.如需要檢查不一樣的加密方式可以自行增減）

```
#!/bin/bash

IPLIST=($(cat iplist.txt))
TLS_VER=(TLSv1.0 TLSv1.1 TLSv1.2)
SCAN_PORT="443"
NMAP_OPS="--host-timeout 3000ms --max-rtt-timeout 3000ms --script ssl-enum-ciphers -p ${SCAN_PORT}"
OUTPUT="output.csv"

for (( i = 0; i < ${#IPLIST[@]}; i++ )); do
  SUP_TLS=$(nmap $NMAP_OPS ${IPLIST[i]} | egrep "${TLS_VER[0]}|${TLS_VER[1]}|${TLS_VER[2]}" | cut -c 5-11)

  if [[ ! -z $SUP_TLS ]]; then
    echo -ne "\n${IPLIST[i]}" >> $OUTPUT
```

```
    for (( j = 0; j < ${#SUP_TLS[@]}; j++ )); do
      echo -n ",${SUP_TLS[@]}" >> $OUTPUT
    done
  fi

  unset SUP_TLS
done
```

參考網址

用 nmap 驗證支援的 TLS 版本和 Ciphers (Mr.沙先生)

Revision #5
Created 26 October 2024 09:09:34 by Ron
Updated 14 May 2025 01:21:20 by Ron