Penetration Testing Practice
滲透測試實務應用

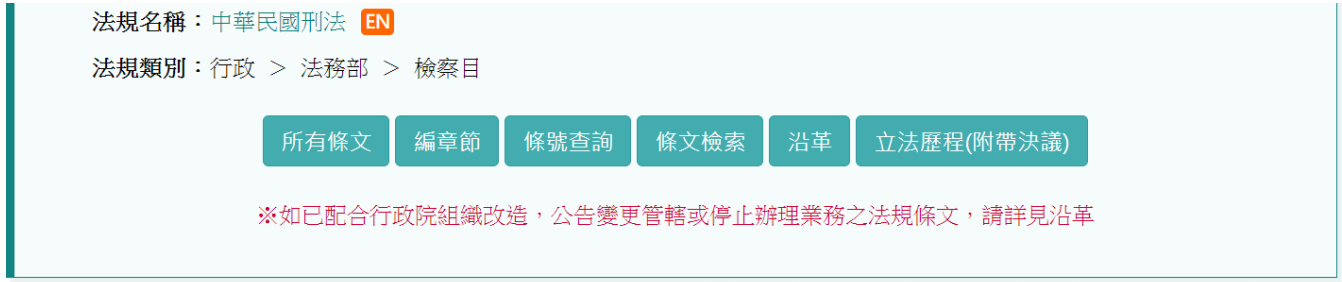
03 網路資訊蒐集

孫士勝
Shi-Sheng Sun, Ph.D.
sssun@nccu.edu.tw

課程聲明
Disclaimer

- 本課程所教授之滲透測試相關技術僅能於課堂中進行，若有任何超出範圍的動作，皆屬個人行為。
  The penetration testing techniques taught in this course are only to be used within this course. Any actions taken outside of this scope are the sole responsibility of the individual.

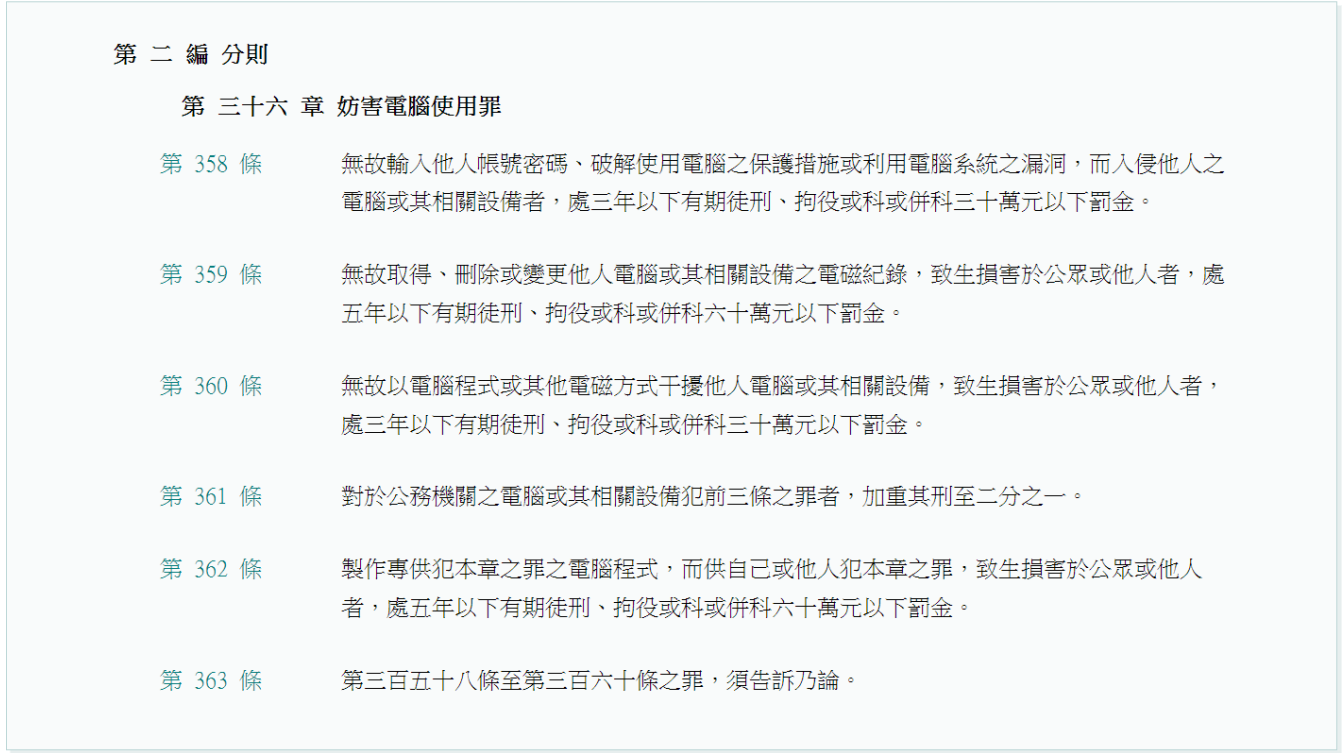
- 學員於課後使用任何網路攻擊技術對任何資訊設備進行攻擊，皆屬個人行為。
  Students are solely responsible for any network attacks carried out on any equipment after the course using any network attack techniques.


法規名稱：中華民國刑法 EN

法規類別：行政 ＞ 法務部 ＞ 檢察目

所有條文 | 編章節 | 條號查詢 | 條文檢索 | 沿革 | 立法歷程(附帶決議)

※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革


第 二 編 分則

第 三十六 章 妨害電腦使用罪

第 358 條　無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 359 條　無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 360 條　無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 361 條　對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條　製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 363 條　第三百五十八條至第三百六十條之罪，須告訴乃論。

ACM 道德與專業行為準則
ACM Code of Ethics and Professional Conduct

- 1.1 增進人類社會福祉(Contribute to society and human well-being.)
- 1.2 避免傷害任何人(Avoid harm to others.)
- 1.3 誠實與值得信任(Be honest and trustworthy.)
- 1.4 公平且無犯罪意圖的行動(Be fair and take action not to discriminate.)
- 1.5 尊重智慧財產權(Honor property rights including copyrights and patent.)
- 1.6 維持智慧財產的完整性(Give proper credit for intellectual property.)
- 1.7 尊重他人隱私(Respect the privacy of others.)
- 1.8 遵守保密原則(Honor confidentiality.)

http://ethics.acm.org/code-of-ethics

課前問券

- 網路資訊蒐集課前問券
- https://forms.gle/kXoH4JJ5xLWesfwg8

網路掃描技術與方法

- 透過掃描技術，可知道目標主機之各種TCP/IP port的分配與開啟狀態、使用者所開放的服務、服務軟體版本及作業系統資訊。
- 可透露出目標主機所存在的安全問題。
- 了解目標伺服器所在的網路(網段)、作業系統以及可能的服務或軟體的狀況。
- 通常是作為惡意攻擊的第一步驟。

常見TCP ports

PortNumber	名稱	說明
20	ftp-data	FTP 資料連接埠
21	ftp	檔案傳輸協定(FTP)連接埠
22	ssh	Secure Shell (SSH) 服務
23	telnet	Telnet 服務
25	smtp	Simple Mail Transfer Protocol (SMTP)
53	domain	網域名稱服務(Domain Name Server)
69	tftp	TFTP(Trivial File Transfer Protocol)是Cisco公司開發的一個簡單檔傳輸協議，類似於FTP
80	http	WWW 服務
110	pop3	收信Mail 通訊協定
115	sftp	安全的檔案傳輸協定(SFTP)服務
123	ntp	網路時間協定(NTP)

常見TCP ports

PortNumber	名稱	說明
138	netbios-dgm	NETBIOS 資料包服務
139	netbios-ssn	NETBIOS 工作階段服務
143	imap	網際網路訊息存取協定 (IMAP)，用於接收電子郵件的通訊協定
443	https	HTTP
445	microsoft-ds	透過TCP/IP 的 SMB
1433	ms-sql-s	Microsoft SQL Server
3306	mysql	MySQL 資料庫服務
3389	rdp	Windows系統遠端桌面
8080	http	常用於替代Port 80，亦可用於web代理 (Proxy)
8443	https	常用於替代Port 443

Scanning

- 藉由掃描可以取得特定的IP 、作業系統、網路和主機系統架構以及主機上所開啟的服務等等
- 掃描首先搜尋目標主機網路上可以連接到的主機，然後利用這些資訊來查出主機開啟哪些通訊埠，並且進一步偵測目標主機上所利用的作業系統類型和版本
- 掃描大略分為以下種類
  - Ping掃描：探測主機的上線狀態
  - Port掃描：探測主機的通訊埠開啟狀態及其可能對應的services
  - 作業系統辨識：探測作業系統類型
  - 網路架構掃描
  - 弱點掃描

Ping Scan

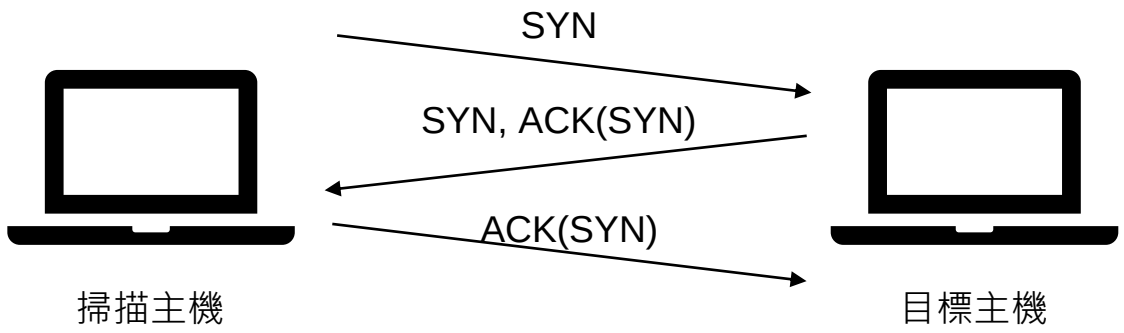
- ICMP(Internet Control Message Protocol) 屬於Network Layer
  - 與IP 屬於同一層，常用在網路傳輸發生異常時，作為警示訊息通訊
  - 透過ICMP，管理者可以對網路的問題作出診斷，然後採取適當的措施解決
- ICMP Echo
  - 對目標主機發送ICMP Echo Request 封包，等待ICMP Echo Reply的封包
- ICMP Sweep
  - 使用ICMP Echo Request 封包對多部目標主機進行大範圍掃描
- Broadcast ICMP
  - 利用ICMP廣播，探測網路範圍內的主機，網路中的上線主機將會予以回應。但此種掃描通常適用於UNIX/Linux系统

Port Scan

- 想要滲透一部主機時，通常會透過如nmap這類的工具傳送一連串的訊息，以測試此主機上有執行哪些網路服務
- 解析port將可了解該port所提供的服務，並嘗試拿到相關資訊
- 主要可以區分為兩類
  - TCP
    - 全連接掃描
    - 半連接掃描
  - UDP

TCP Scan：全連接掃描

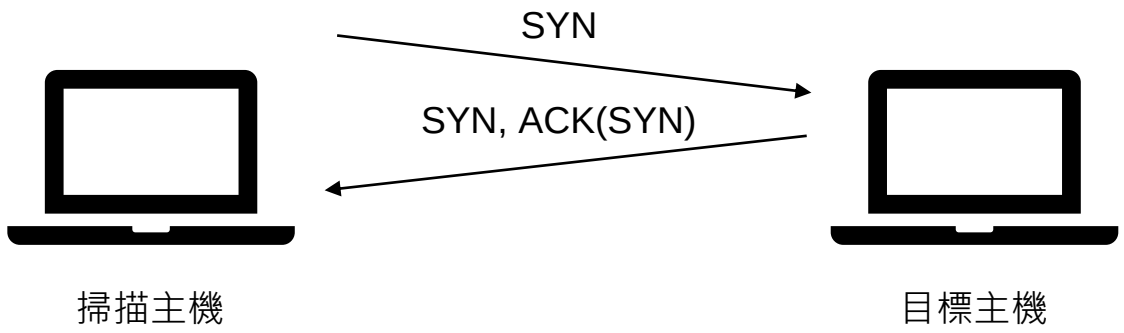
- 透過掃描工具中TCP Connect() Scan功能，掃描工具透過TCP的三向交握(Three Way Handshaking)與目標主機的指定port建立連接
- TCP封包有控制旗標位元(Code bits)，可以決定封包的類型，可產生包括URG、ACK、PSH、RST、SYN及FIN類型的封包 針對目標主機送出SYN類型封包的全連接掃描
- 優缺點：全連接掃描的結果準確，但會被目標主機的日誌記錄



針對目標主機送出SYN類型封包的全連接掃描

TCP Scan：半連接掃描

- TCP還有另一種掃描方式，是在三向交握途中只進行前兩次交握，在進行第三步驟前，掃描主機端就中斷此次連接，使這次連接沒有完全建立完成（SYN Scan）
- 這種掃描方式被稱為半連接掃描，這種掃描給掃描工具全權控制封包發送和等待回應時長的權限，允許更詳細的回應。
- 與全連接掃描比起，半連接掃描進行連線的紀錄較少，速度也比較快
- 優缺點：半連接掃描的結果較不準確，在安全機制不嚴謹的主機下不容易被日誌留下掃描記錄



針對目標主機送出SYN類型封包的半連接掃描

UDP Scan

- 隨著目前防火牆設定日益嚴格，現今TCP 的port 常不輕易被開放，所以出現了UDP Scan
- 與TCP Scan比較，UDP Scan比較費時，且精準度也較低
- UDP的發送狀況為
  - 如果目的端的port開啟，則成功傳送但不會給任何回應
  - 如果目的端port為關閉，則回應ICMP port unreachable

作業系統辨識

- 透過每個作業系統間處理TCP/IP堆疊(TCP Protocol Stack)不同的特性，可以當作辨識一個作業系統的「指紋(Fingerprint)」，藉以分析作業系統的類型和版本
- 指紋辨識技術依其探測行為的不同，可分為
  - 主動式指紋辨識(Active fingerprinting)
  - 被動式指紋辨識(Passive fingerprinting)

Nmap

- Nmap全名是Network Mapper，是由Gordon Lyon (aka his pseudonym: Fyodor Vaskovich)所開發的一套開放原始碼軟體。
- 可用於檢測本機或網路遠端主機的安全性弱點
- 主要功能是針對來源主機/網段作掃瞄
  - ✓ 目標主機所開放的TCP埠
  - ✓ 取得對應的網路服務類型
  - ✓ 應用軟體名稱與版本
- 可偵測出目標主機所使用的作業系統、封包過濾器及防火牆種類等資訊。

Nmap

- nmap –help 或 man nmap

```
root@kali:~# nmap -help
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

```
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.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
```

Nmap：TCP 全連接掃描

- nmap –sT Target.IP
  - 可使用-p來指定目標的port或範圍

```
root@kali:~# nmap -sT 10.103.140.2
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for 10.103.140.2
Host is up (0.00019s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 02:00:0A:67:8C:02 (Unknown)
```

Nmap：TCP 半連接掃描

- nmap –sS Target.IP

```
root@kali:~# nmap -sS 10.103.140.2
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for 10.103.140.2
Host is up (0.00026s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 02:00:0A:67:8C:02 (Unknown)
```

Nmap

- UDP掃描：
  - nmap –sU Target.IP
- Port及對應服務掃描
  - nmap -sV Target.IP
- 作業系統系統
  - nmap -O Target.IP

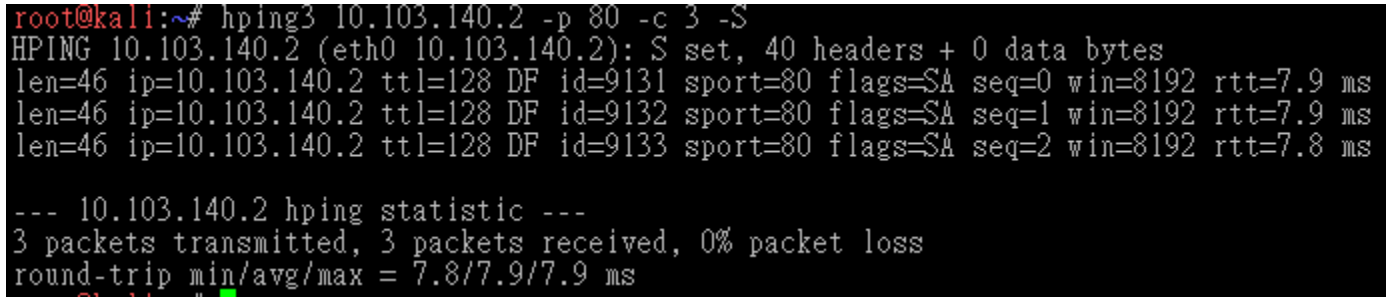
hping/hping3

- hping/hping3是一個網路工具，可以用來測試firewall、網路效能、觀察遠端主機的回應狀態，包括TCP, UDP, ICMP
- hping/hping3可達到以下功能
  - 判斷是否有防火牆保護
  - port掃描
  - 辨別網路協定、作業系統類型、port服務類型
  - 估算路徑上的最大傳輸量
  - 壓力測試
  - 可以由使用者自訂封包格式和偽造IP

hping/hping3

- hping3 10.103.140.2 -p 80 -c 3 -S
  - 發送 TCP SYN 封包到10.103.140.2 的 port 80，以查看它是否處於開啟狀態。如果成功，將收到 TCP SYN/ACK 回應
  - -c 3：指定發送的SYN數量為3
  - -S：使用TCP SYN掃描，向目標主機的port 80發送SYN請求。

- flags：
  - SA 表示port 有開
  - RA 表示port 沒開 (Reset Ack)
- TTL：
  - 128 為 Windows 才有
  - 64 為 Unix



hping/hping3

- 測試網域中存在哪些主機
  - for i in {1..254}; do (ping -c 1 10.103.140.$i | grep "bytes from" &); done

```
root@kali:~# for i in {1..254}; do (ping -c 1 10.103.140.$i | grep "bytes from" &); done
64 bytes from 10.103.140.1: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 10.103.140.2: icmp_seq=1 ttl=128 time=0.230 ms
64 bytes from 10.103.140.3: icmp_seq=1 ttl=64 time=0.090 ms
64 bytes from 10.103.140.4: icmp_seq=1 ttl=64 time=0.141 ms
64 bytes from 10.103.140.5: icmp_seq=1 ttl=64 time=0.174 ms
root@kali:~# 64 bytes from 10.103.140.254: icmp_seq=1 ttl=255 time=0.550 ms
```

hping/hping3

- hping3以每秒100個封包對目標port 80生成sync flooding
  - hping3 -S -p 80 -i u100 10.103.140.2

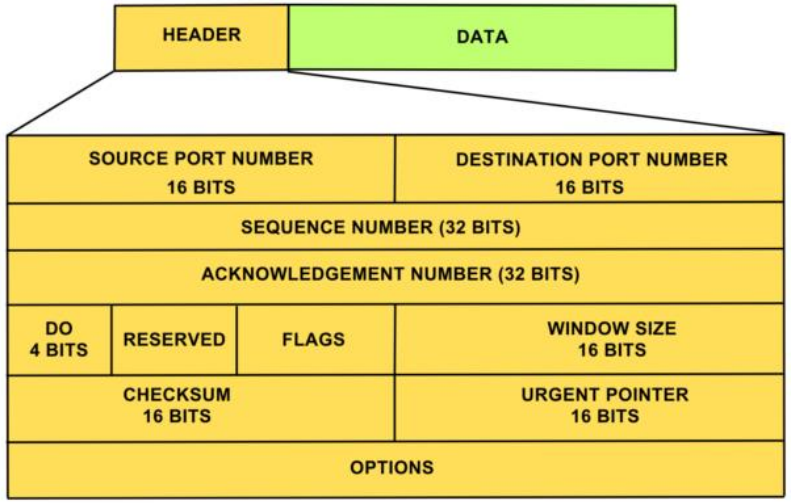
```
len=46 ip=10.103.140.2 ttl=128 DF id=14211 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14205 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14212 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14203 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14204 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14210 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14202 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14207 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14208 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14213 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14215 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14216 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14214 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14221 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14231 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14218 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14227 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14229 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14217 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14224 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
^C
--- 10.103.140.2 hping statistic ---
283502 packets transmitted, 266205 packets received, 7% packet loss
round-trip min/avg/max = 4.7/6.4/7.8 ms
len=46 ip=10.103.140.2 ttl=128 DF id=14220 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
root@kali:~# hping3 -S -p 80 -i u10 10.103.140.2
```

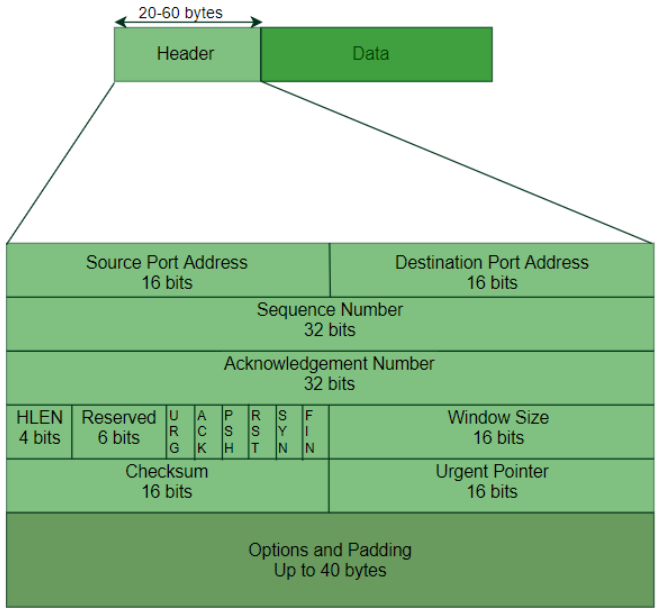
OS Fingerprint

- OS fingerprint（作業系統指紋）
  - 利用各種作業系統版本對收到的封包所產生的不同回應封包內容，可用來區分辨識作業系統的類型或版本。
  - nmap就是利用此原理，以分辨不同版本的UNIX：Solaris、HPUX、AIX、BSD、Linux等，還能夠辨識出不同版本的Linux Kernel或其他作業系統，像是Windows

常見的OS Fingerprint技術

- TCP FIN flag偵測
  - 送出一個TCP FIN封包（或是任何不包含ACK或SYN flag的封包）給目標主機開啟的port，接下來會等待封包的回應。
- BOGUS flag偵測/偽造flag偵測
  - 在SYN封包的TCP標頭中設定一個未定義的TCP旗標(Flag)，Linux2.0.35版之前的舊版本會在回應封包中保持這個旗標，而其他類型作業系統則收到SYN+BOGUS封包後，將目前的連線中斷，然後再重新連線。部份作業系統在收到 SYN+BOGUS 封包時會重置連線，這個行為對辨識它們是相當有用的。





常見的OS Fingerprint技術

- TCP ISN Sampling
  - ISN(Initial Sequence Number)，透過目標系統回應連線需求時，找出TCP連接啟始化序號碼的特徵，以此判斷其作業系統類型
- ICMP Error Message Quenching
  - 對目標伺服器發送一連串封包，統計出一段時間內收到的ICMP unreachable封包，再與作業系統的預設值做比較，即可辦認出作業系統類型與版本

You can also read https://nmap.org/nmap-fingerprinting-article-tw.html

Enumeration (列舉)

- 若靠著前面部分所提到的資料收集以及非惡意性的掃描，都沒辦法取得有用的資訊時，可嘗試利用目標系統的有效資源共享以及使用者帳號，利用Enumeration(列舉)來達到取得有效用的資訊，以便尋找漏洞進行進一步的滲透行為
- 常用的列舉工具包括DNS相關列舉
- 在Windows作業系統中，Netbios相關漏洞常令滲透者建立連線之後，再透過不同的列舉技術來取得資訊，常列舉的資訊項目包含了網路資源與共享、使用者名稱與群組名稱、應用程式等

DNS列舉

- DNS列舉可以收集所有DNS服務和相關項目
- DNS列舉可以幫助使用者收集目標群組織的關鍵資訊
  - 使用者名稱
  - 電腦名稱
  - IP位址

- 前一份投影片所介紹的dig以及nslookup均為這類工具

DNSenum

- DNSenum 是一款強大的域名資訊收集工具，這款工具可以透過Google和字典檔，猜測可能存在的域名，並進行反向查詢。
- 可以查詢網站的主機位址資訊、域名伺服器、郵件交換紀錄。
- 可以利用在域名伺服器上使用axfr請求，透過指令來獲得擴充域名資訊
- 使用這款工具時還有額外的附加選項
  - --threads[number]:設定使用者可以同時執行多個程序數量
  - -r :讓使用者開啟遞迴查詢
  - -d:讓使用者設定WHOIS請求之間的延遲時間
  - -o:讓使用者可以指定輸出位置
  - -w:讓使用者開啟WHOIS請求

DNSenum

```
root@kali:~# dnsenum  -enum zonetransfer.me
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4
Warning: can't load Net::Whois::IP module, whois queries disabled.
Warning: can't load WWW::Mechanize module, Google scraping desabled.

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         7200     IN    A        5.196.105.14


Name Servers:
______________

nsztm2.digi.ninja.                       10078    IN    A        34.225.33.2
nsztm1.digi.ninja.                       10079    IN    A        81.4.108.41


Mail (MX) Servers:
___________________

ASPMX.L.GOOGLE.COM.                      275      IN    A        108.177.125.26
ASPMX4.GOOGLEMAIL.COM.                   293      IN    A        142.250.115.26
ALT2.ASPMX.L.GOOGLE.COM.                 293      IN    A        142.250.141.26
ASPMX3.GOOGLEMAIL.COM.                   293      IN    A        142.250.141.26
ALT1.ASPMX.L.GOOGLE.COM.                 293      IN    A        173.194.65.27
ASPMX5.GOOGLEMAIL.COM.                   293      IN    A        108.177.104.27
ASPMX2.GOOGLEMAIL.COM.                   293      IN    A        173.194.65.26


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA                (
zonetransfer.me.                         300      IN    HINFO          "Casio
zonetransfer.me.                         301      IN    TXT                (
zonetransfer.me.                         7200     IN    MX                 0
zonetransfer.me.                         7200     IN    MX                 10
zonetransfer.me.                         7200     IN    MX                 10
zonetransfer.me.                         7200     IN    MX                 20
zonetransfer.me.                         7200     IN    MX                 20
zonetransfer.me.                         7200     IN    MX                 20
zonetransfer.me.                         7200     IN    MX                 20
zonetransfer.me.                         7200     IN    A          5.196.105.14
zonetransfer.me.                         7200     IN    NS         nsztm1.digi.ninja.
zonetransfer.me.                         7200     IN    NS         nsztm2.digi.ninja.
_acme-challenge.zonetransfer.me.         301      IN    TXT                (
```

snmpwalk

- snmpwalk是一款SNMP的應用程式，他利用SNMP的GETNEXT的請求，查詢指定所有的OID樹資訊(SNMP協定中物件標示)，查詢完後顯示給使用者

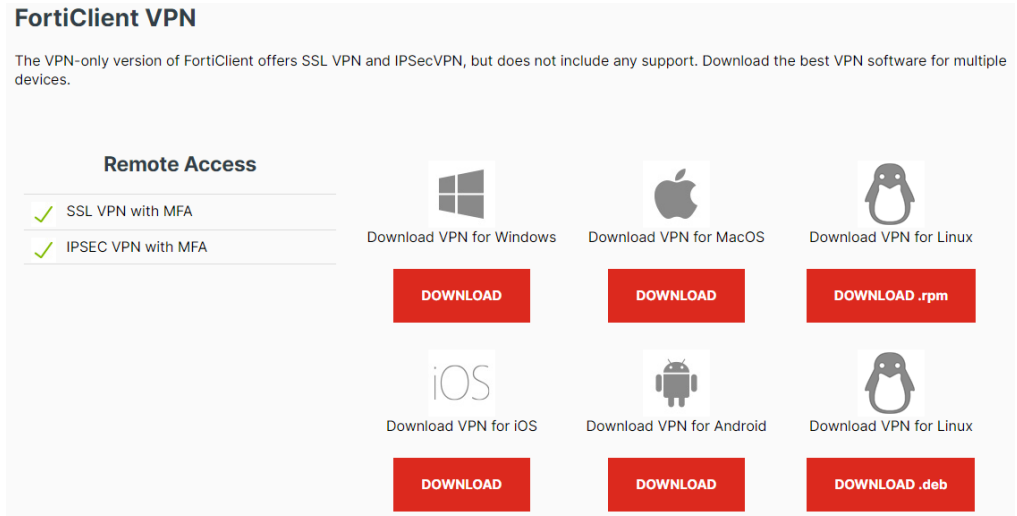
```
root@kali:~# snmpwalk -Os -c public -v 2c 10.103.140.2 |more
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2
iso.3.6.1.2.1.1.3.0 = Timeticks: (2591631) 7:11:56.31
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "metasploitable3"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 27
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.1.13 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.14 = INTEGER: 14
iso.3.6.1.2.1.2.2.1.1.15 = INTEGER: 15
iso.3.6.1.2.1.2.2.1.1.16 = INTEGER: 16
iso.3.6.1.2.1.2.2.1.1.17 = INTEGER: 17
iso.3.6.1.2.1.2.2.1.1.18 = INTEGER: 18
iso.3.6.1.2.1.2.2.1.1.19 = INTEGER: 19
iso.3.6.1.2.1.2.2.1.1.20 = INTEGER: 20
iso.3.6.1.2.1.2.2.1.1.21 = INTEGER: 21
iso.3.6.1.2.1.2.2.1.1.22 = INTEGER: 22
iso.3.6.1.2.1.2.2.1.1.23 = INTEGER: 23
iso.3.6.1.2.1.2.2.1.1.24 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.1.25 = INTEGER: 25
iso.3.6.1.2.1.2.2.1.1.26 = INTEGER: 26
iso.3.6.1.2.1.2.2.1.1.27 = INTEGER: 27
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 53 6F 66 74 77 61 72 65 20 4C 6F 6F 70 62 61 63
6B 20 49 6E 74 65 72 66 61 63 65 20 31 00
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74 20 28 53 53
54 50 29 00
```

國網中心雲端資安攻防平臺使用
Cyber Defense eXercise，CDX

- 請先連線 https://cdx.nchc.org.tw/
  - 帳號：你的學號@nccu.edu.tw
  - 密碼：NCCUpt2025@你的學號
  - 第一次登入後，請更新密碼並牢記之
    - 因應資安法規範，密碼須同時符合以下規則，180天內需變更一次，並請勿與最近3次的密碼重覆
    - 包含英文字母大寫與小寫、包含至少一個數字、包含至少一個特殊符號!@#$%^&*，且密碼長度至少12字元
  - 若遺忘密碼請找助教協助reset

安裝FortiClient VPN連線程式-下載安裝

- 下載網址：
  - https://cdx.nchc.org.tw/download_files/vpn_client.zip
  - 解壓縮後，按自己的筆電作業系統安裝
  - 因國網中心所提供的FortiClient VPN版本較舊，MAC user可能需要自行下載FrotiClient VPN 7.x
    - https://www.fortinet.com/support/product-downloads#vpn



安裝FortiClient VPN連線程式-使用說明

- VPN連線
  - VPN Server IP：140.110.112.1
  - VPN Port Number：443
  - VPN 帳號/密碼：如先前設定
- 設定說明：
  - 可參考CDX教學手冊
  - https://cdx.nchc.org.tw/download_files/cdx_manual.zip

CDX Kali Linux

- 請先以FortiClient VPN連線國網中心VPN Server
- VPN連線後，請下載putty或 MobaXterm, 或在mac下直接以ssh連線
  - IP: 10.103.140.1
  - 帳號: kali
  - 密碼: kali
  - MAC下：
    - ssh root@10.103.140.1

CDX-靶機：CDX-Linux-Metasploitable2-TPML-custom

- IP: 10.103.140.2
- 帳號：msfadmin
- 密碼：msfadmin

Homework#1, due time 3/17 11:59:59 AM

- HW1-1 (20pts)： 請至CDX機器管理頁面 https://cdx.nchc.org.tw/setting_vmmgt_common_voc.php 新增2部虛擬機
  - CDX-Linux-kali-2023.4-TMPL-custom (帳/密: kali/kali)
  - CDX-Linux-Metasploitable2-TPML-custom (帳/密: msfadmin/ msfadmin，本台機器是靶機)
  - 均設定為1核心、4GB記憶體、機器數1台、網路界面選擇CDX-VM-VLAN-1240
  - 完成後請記錄下你的Kali Linux以及靶機IP，並於CDX頁面截圖至作業檔案中

- HW1-2 (20pts)： 參考上一份投影片，請於你的Kali Linux下輸入以下指令
  - dig axfr zonetransfer.me @nsztm1.digi.ninja
  - 截圖並複製至作業檔案中
  - 根據以上結果，說明以下DNS記錄的內容及其意義：
    - IN SOA
    - IN MX
    - IN HINFO
    - IN NS
    - IN CNAME

Note:1. 作業請轉為PDF檔再上傳至Moodle
2. All the references in your homework should be listed

Homework#1, due time 3/17 11:59:59 AM

- HW1-3 (40pts)：請於你的Kali Linux下輸入以下指令，並依序填至作業中
  - nmap -sV -O 你的靶機IP
  - 將以上指令的結果截圖至作業中
  - 逐行說明以上指令的結果，需說明port以及對應service的意義
  - 以上指令的結果中有數個port的service均為http，請用瀏覽器連線 http://你的靶機IP:port 並將這幾個port的顯示結果截圖至作業中
  - 以上指令的結果中，nmap所偵測你的靶機作業系統為何

- HW1-4 (20pts)：利用web.archive.org找到你出生年(+月，如果有月的話)的政治大學首頁，截圖並說明

Note:1. 作業請轉為PDF檔再上傳至Moodle
2. All the references in your homework should be listed

課後問券

- 網路資訊蒐集課後問券
- https://forms.gle/PuPqD7KRSddRSg1y6

Reference Materials

- Thanks to「教育部資訊安全人才培育計畫」&「國網中心雲端資安攻防平臺（Cyber Defense eXercise，CDX）」

“教育部資訊安全人才培育計畫,” https://isip.moe.edu.tw/
“Cyber Defense eXercise，CDX,” https://cdx.nchc.org.tw/index.php

Q & A