個案分析-

Y 大學大量對外進行 SSH 攻擊的主機事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/5

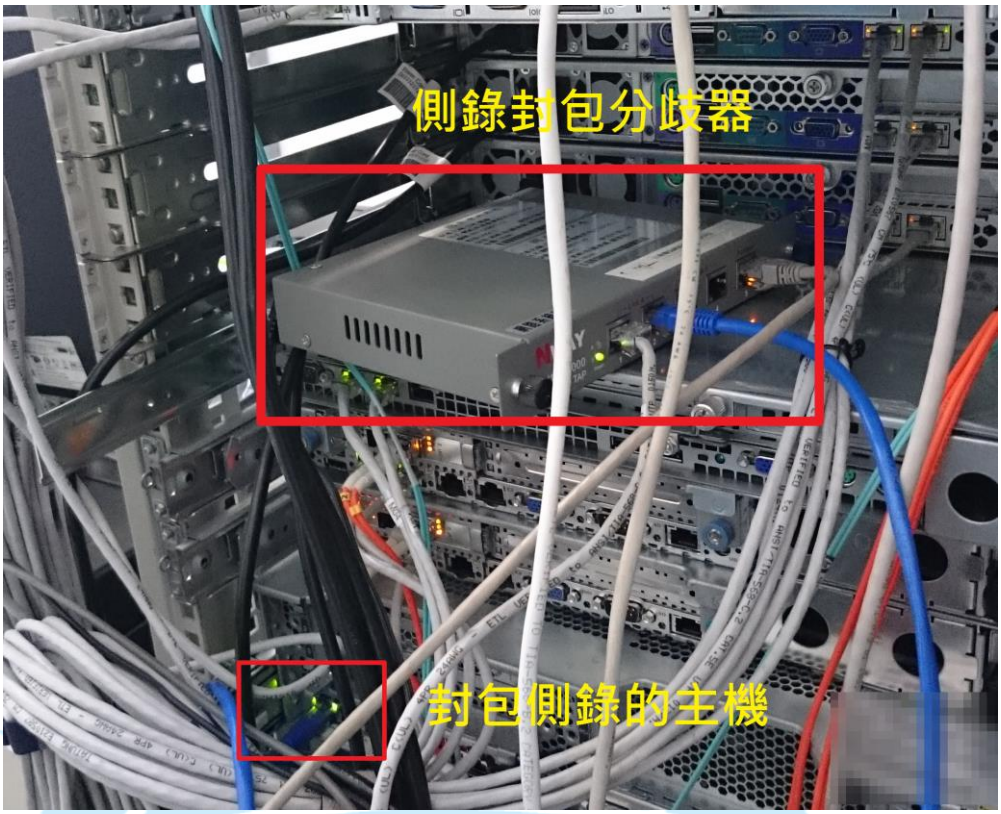
I. 事件簡介

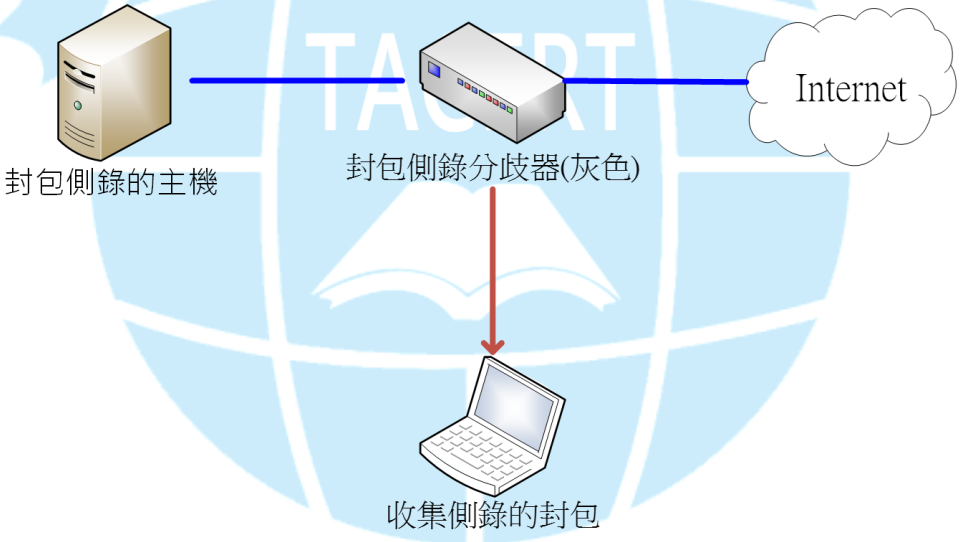
1. 該校被偵測單位開立兩張資安事件單，一張是 INT 對外攻擊事件單，而另一張 EWA 資安預警事件單，主要描述有大量對外攻擊行為。

原發布編號	ASOC-INT-201504-	原發布時間	2015-04-
事件類型	對外攻擊	原發現時間	2015-04-22
事件主旨	通報:[國立 大學]140. 161 資訊設備疑似對外攻擊警訊通知		
事件描述	ASOC 發現貴單位(國立 大學)資訊設備 140 .161 疑似對外部主機 TCP 22 Port 進行攻擊		
手法研判	該電腦對外部主機TCP Port 22(SSH服務)嘗試猜測系統帳號密碼。		

原發布編號	ICST-EWA-201504	原發布時間	2015-04-24
事件類型	疑發起對外攻擊	原發現時間	2015-04-24
事件主旨	140. 161用戶資訊設備疑似對外攻擊警訊		
事件描述	技術服務中心接獲外部情資，教育部 註冊 IP 140. 161 疑於2015-04-24 對外產生攻擊行為。 為避免不必要之資安風險，請針對該系統進行詳細檢查並加強相關防範措施。		
手法研判	回復措施： 1.檢查該系統上是否有不明程式正大量對外建立網路連線，若有則停止該程式並刪除系統上該不明程式檔案。 2.由於所得資訊有限，無法提供較明確之回復措施，請依該系統平台參考相關檢查暨回復措施。		

2. 該校的主機管理者請本單位協助解決，並且進行主機的數位鑑識。
3. 經詢問該主機為一台 Ubuntu Linux 的作業系統，並且有架設 Centos 虛擬機提供對外學生的遠端桌面服務。
4. 上層的 Centos 虛擬機透過 NAT 方式與底層 Ubuntu 共用對外實體 IP，故必須同時對兩個作業系統進行檢測。
5. 該主機檢測前以先斷開網路線，至本單位安裝網路分歧器(灰色)進行封包側錄後才恢復網路。





II. 事件檢測

1. 恢復網路後進入底層主機 terminal 介面，透過 netstat 指令先觀察是否有可疑的網路連線。因管理者告知該主機有重新啟動過，故一開始並無發現可疑連線。
2. 該主機有啟用 port 21、22、3389 的服務，分別為 FTP、SSH 及 RDP 服務讓管理者能夠登入使用，因此猜測駭客可能透過這些服務漏洞入侵。

3. 檢查 Ubuntu 的登入記錄檔 auth.log，確實發現到資安事件單派發日期前有可疑的 IP 登入紀錄。帳號 test 分別有兩筆紀錄在 22 號以前成功以 SSH 方式登入主機，IP 分別是中國的 119.147.144.101 和香港的 59.188.237.12。

```
root@ubuntu:~# less /var/log/auth.log.1 | grep Accepted
Apr 20 10:46:07 ubuntu sshd[3703]: Accepted password for test from 119.147.144.101 port 57956 ssh2
Apr 20 14:27:46 ubuntu sshd[20930]: Accepted password for test from 59.188.237.12 port 1508 ssh2
Apr 22 00:13:46 ubuntu sshd[32213]: Accepted password for test from 59.188.237.12 port 4899 ssh2
Apr 23 22:31:15 ubuntu sshd[9673]: Accepted password for [redacted] from 36.238.142.236 port 9162 ssh2
root@ubuntu:~#
```

4. 檢查主機內是否有可疑的檔案或自動執行排程，結果相當乾淨找不出有問題檔案。故研判應為駭客一次性入侵執行程式，一旦程式被關閉則不留痕跡。將主機閒置一段時間並觀察是否會再次被入侵，果然發現帳號 test 有再次被登入的紀錄 59.188.237.12 為上次相同登入的香港 IP，並且記錄中有使用 sftp 協定植入後門程式，確定為駭客故意入侵行為。

```
root@ubuntu:~/kevin# less /var/log/auth.log | grep Accepted
Apr 27 16:38:18 ubuntu sshd[32742]: Accepted password for test from 140.[redacted] port 62083 ssh2
Apr 27 16:41:39 ubuntu sshd[909]: Accepted password for test from 140.[redacted] port 19161 ssh2
Apr 27 16:44:45 ubuntu sshd[1426]: Accepted password for test from 140[redacted] port 51318 ssh2
Apr 27 16:58:42 ubuntu sshd[3595]: Accepted password for test from 140[redacted] port 19857 ssh2
Apr 27 17:37:08 ubuntu sshd[8609]: Accepted password for test from 59.188.237.12 port 1971 ssh2
root@ubuntu:~/kevin#
```

5. 主機管理者告知說 test 初始是替廠商創立維護使用。但隨後維護結束後已透過指令 userdel 將帳號疑除，實地檢查帳號 test 的家目錄的確已被移除。然而檢查 /etc/passwd 帳號管理檔案卻能發現 test 依然存在，實地測試依舊能夠透過 SSH 登入，只是沒有家目錄存在。該 test 帳號能夠輕易被入侵主要原因之一是使用 test1234 的弱密碼。

6. 此時 netstat 檢查網路連線狀態，確實出現了大量的對外連線，都是連到外部 IP 的 port 22，也就是正在進行 SSH 的暴力破解攻擊。檢查網路使用資源幾乎是耗盡所用頻寬，故導致系統效能降低以及其他人網路變慢。

```
tcp        0      1 140.[redacted]161:33501   200.14.56.140:22        SYN_SENT    10001/squid64
tcp        0      1 140.[redacted]161:60903   157.201.144.87:22       SYN_SENT    9392/squid64
tcp        0    296 140.[redacted]161:59055   78.188.113.17:22        ESTABLISHED 10610/squid64
tcp        0      1 140.[redacted]161:54634   158.79.52.13:22         SYN_SENT    9188/squid64
tcp        0      1 140.[redacted]161:33495   65.179.173.230:22       SYN_SENT    10001/squid64
tcp        0      0 140.[redacted]161:58810   113.88.241.22:22        ESTABLISHED -
tcp        0      0 140.[redacted]161:53531   69.46.19.48:22          ESTABLISHED 8781/squid64
tcp        0      0 140.[redacted]161:39795   128.199.151.10:22       ESTABLISHED 10407/squid64
tcp        0      1 140.[redacted]161:49221   165.77.189.195:22       SYN_SENT    9595/squid64
tcp        0    144 140.[redacted]161:43674   196.29.129.5:22         ESTABLISHED 8985/squid64
tcp        0      1 140.[redacted]161:50128   6.107.104.39:22         SYN_SENT    9392/squid64
tcp        0      1 140.[redacted]161:51542   215.11.166.41:22        SYN_SENT    -
tcp        0      1 140.[redacted]161:50245   35.2.146.71:22          SYN_SENT    9392/squid64
tcp        0      1 140.[redacted]161:41233   16.164.122.50:22        SYN_SENT    8781/squid64
tcp        0     68 140.[redacted]161:59055   54.82.243.2:22          ESTABLISHED 9392/squid64
tcp        0    100 140.[redacted]161:45246   203.196.132.100:22      ESTABLISHED 9392/squid64
tcp        0     21 140.[redacted]161:54282   176.73.166.45:22        ESTABLISHED 9188/squid64
tcp        0     21 140.[redacted]161:50115   83.46.80.25:22          ESTABLISHED 9798/squid64
tcp        0      0 140.[redacted]161:36470   125.62.98.115:22        ESTABLISHED 10001/squid64
tcp        0      0 140.[redacted]161:48557   181.138.122.9:22        ESTABLISHED 9595/squid64
tcp        0      1 140.[redacted]161:42319   197.6.244.139:22        SYN_SENT    9392/squid64
tcp        0     52 140.[redacted]161:56821   118.173.44.59:22        ESTABLISHED 9798/squid64
tcp        0      1 140.[redacted]161:41336   190.6.244.5:22          SYN_SENT    9595/squid64
tcp        0      0 140.[redacted]161:41764   91.18.234.195:22        ESTABLISHED 9392/squid64
tcp        0      1 140.[redacted]161:40036   60.34.79.106:22         SYN_SENT    -
tcp        0    144 140.[redacted]161:47471   81.21.104.17:22         ESTABLISHED 9798/squid64
tcp        0      0 140.[redacted]161:34626   65.210.45.81:22         ESTABLISHED 9392/squid64
tcp        0      1 140.[redacted]161:58342   87.254.89.170:22        SYN_SENT    9188/squid64
tcp        0      1 140.[redacted]161:56370   55.4.152.179:22         SYN_SENT    8985/squid64
tcp        0      1 140.[redacted]161:33601   130.47.201.251:22       SYN_SENT    9188/squid64
tcp        0     21 140.[redacted]161:57541   201.218.62.65:22        ESTABLISHED 9595/squid64
tcp        0      0 140.[redacted]161:42505   83.60.54.157:22         ESTABLISHED 10407/squid64
tcp        0      0 140.[redacted]161:58047   173.165.146.113:22      ESTABLISHED 9798/squid64
```

7. 我們能透過 netstat 得知觸發網路攻擊的惡意程式為 squid64，使用指令 lsof |grep squid64 觀察 squid64 在背景執行的相關動作，可以看到呼叫該程式的帳號的確為 test，並且不斷持續地向外部 IP port 22 發送封包。值得注意的是惡意程式所存放的位置 /tmp/squid64(deleted) 已經被駭客移除，讓管理者無法得知該檔案內容為何。

```
COMMAND   PID USER   FD   TYPE   DEVICE SIZE/OFF     NODE NAME
squid64  8781 test  cwd    DIR    252,0     4096        2 /
squid64  8781 test  rtd    DIR    252,0     4096        2 /
squid64  8781 test  txt    REG    252,0  2142304 84410421 /tmp/squid64 (deleted)
squid64  8781 test  mem    REG    252,0    52120 31198850 /lib/x86_64-linux-gnu/libnss_files-2.15.so
squid64  8781 test  mem    REG    252,0    47680 31198843 /lib/x86_64-linux-gnu/libnss_nis-2.15.so
squid64  8781 test  mem    REG    252,0    97248 31198848 /lib/x86_64-linux-gnu/libnsl-2.15.so
squid64  8781 test  mem    REG    252,0    35680 31198854 /lib/x86_64-linux-gnu/libnss_compat-2.15.so
squid64  8781 test  mem    REG    252,0  1811128 31198844 /lib/x86_64-linux-gnu/libc-2.15.so
squid64  8781 test  mem    REG    252,0    31752 31195160 /lib/x86_64-linux-gnu/librt-2.15.so
squid64  8781 test  mem    REG    252,0   135366 31198846 /lib/x86_64-linux-gnu/libpthread-2.15.so
squid64  8781 test  mem    REG    252,0    14768 31198865 /lib/x86_64-linux-gnu/libdl-2.15.so
squid64  8781 test  mem    REG    252,0   149280 31198862 /lib/x86_64-linux-gnu/ld-2.15.so
squid64  8781 test  mem    REG    252,0     2272 63311503 /etc/passwd
squid64  8781 test   0u   IPv4  1290611      0t0      TCP ubuntu:36596->client-72-251-175-5.consolidated.net:ssh (CLOSE_WA
squid64  8781 test   1u   IPv4 23781451      0t0      TCP ubuntu:47630->vru.gov.ua:ssh (SYN_SENT)
squid64  8781 test   2u   IPv4 23708416      0t0      TCP ubuntu:56705->106.61.253.109:ssh (SYN_SENT)
squid64  8781 test   3u   IPv4 23779464      0t0      TCP ubuntu:58279->ip-82-151-32-124.cable.texel.com:ssh (ESTABLISHED)
squid64  8781 test   4u   IPv4 23777100      0t0      TCP ubuntu:55944->246.6.87.10:ssh (SYN_SENT)
squid64  8781 test   5u   IPv4 23739150      0t0      TCP ubuntu:39119->123.24.25.164:ssh (SYN_SENT)
squid64  8781 test   6u   IPv4 23781474      0t0      TCP ubuntu:37194->bmp-aggr-ras01-129.btl.net:ssh (SYN_SENT)
squid64  8781 test   7u   IPv4 23781430      0t0      TCP ubuntu:59454->PC-85-202-98-2.siedlce.domtel.com.pl:ssh (ESTABLIS
HED)
squid64  8781 test   8u   IPv4 23773156      0t0      TCP ubuntu:46284->pardey.lnk.telstra.net:ssh (ESTABLISHED)
squid64  8781 test   9u   IPv4 23769029      0t0      TCP ubuntu:38333->246.56.207.74:ssh (SYN_SENT)
```

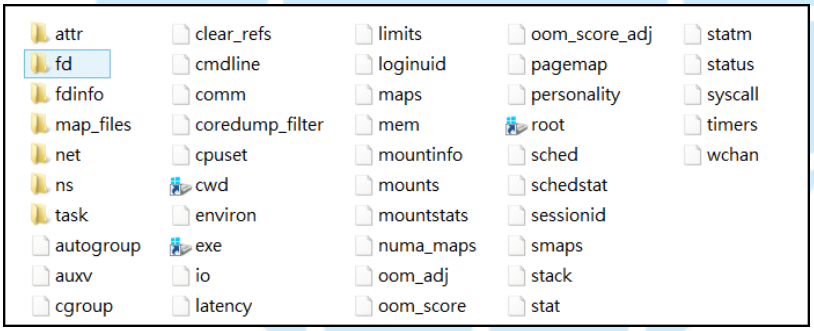
8. 透過指令 ps 查看 squid64 的程序執行狀態，得知駭客會執行 10 次 squid64 後將檔案刪除，只剩下以寫入記憶體的程序留存執行，而每一個程序 PID 都是父程序，底下各自有很多的子程序，故能夠耗盡網路資源對

外發動攻擊。

```
test     11111  5.4  0.0 14046108 10412 ?      Ssl  Apr28  51:58 /tmp/squid64
test     11314  5.4  0.0 13980572 10908 ?      Ssl  Apr28  51:29 /tmp/squid64
test     11517  5.5  0.0 14242716 10912 ?      Ssl  Apr28  52:41 /tmp/squid64
test     11721  5.2  0.0 14373788 10920 ?      Ssl  Apr28  50:21 /tmp/squid64
test     11924  5.4  0.0 14373788 11340 ?      Ssl  Apr28  52:01 /tmp/squid64
test     12127  5.5  0.0 14177180 10932 ?      Ssl  Apr28  52:29 /tmp/squid64
test     12330  6.0  0.0 14570396 11344 ?      Ssl  Apr28  57:56 /tmp/squid64
test     12534  5.3  0.0 14177180 10684 ?      Ssl  Apr28  51:03 /tmp/squid64
test     12737  5.2  0.0 14504860 11144 ?      Ssl  Apr28  49:43 /tmp/squid64
test     12940  5.4  0.0 14177180 10636 ?      Ssl  Apr28  51:57 /tmp/squid64
```

```
        |-squid64(11111,test)-+-{squid64}(11112)
        |                     |-{squid64}(11113)
        |                     |-{squid64}(11114)
        |                     |-{squid64}(11115)
        |                     |-{squid64}(11116)
        |                     |-{squid64}(11117)
        |                     |-{squid64}(11118)
        |                     |-{squid64}(11119)
        |                     |-{squid64}(11120)
        |                     |-{squid64}(11121)
        |                     |-{squid64}(11122)
        |                     |-{squid64}(11123)
        |                     |-{squid64}(11124)
```

9. 檢查其中 11924 的 PID 資料夾 /proc/11924/，此資料夾確實為帳號 test 所擁有，裡面放有許多可疑資料檔案，可能是 PID 執行時產生的工具及記錄。但是這些檔案的大小皆為 0，可能只是暫存檔。



10. 另外用指令 fuser 查看檔案 squid64 存在的位置，確實顯示該檔案已經不存在，這是首次發現惡意程式執行後將自己刪除卻還在背景執行，當惡意程式執行後產生新的程序並寫入記憶體，本體檔案 squid64 就能被刪除。

```
root@ubuntu:~/kevin# fuser -uv squid64
Specified filename squid64 does not exist.
root@ubuntu:~/kevin#
```

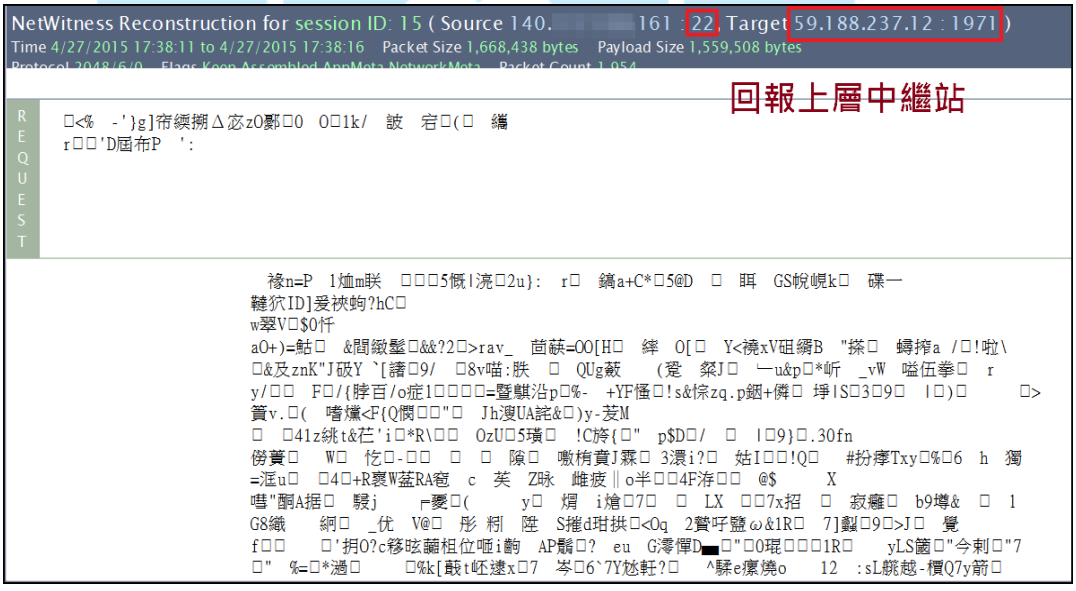
11. 使用指令 find / -username test 查看主機內所有使用者 test 的檔案，可以看到/proc/ 下許多暫存的檔案資料夾(下圖為例)，然而其內容

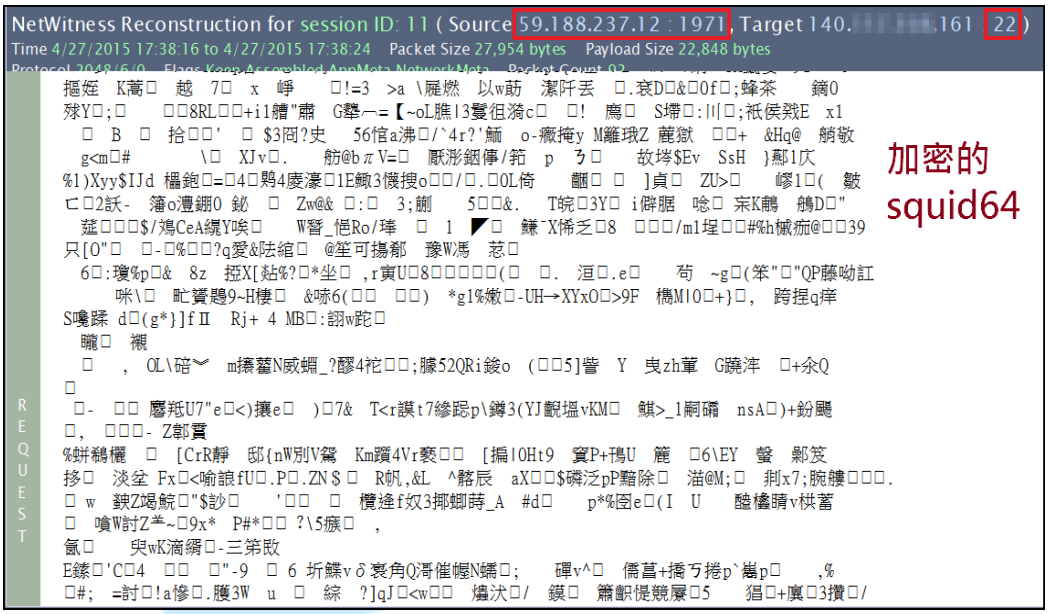
卻是空的，可能為惡意程式將破解到的帳號密碼存入暫存後回傳所用。

·	/proc/10610/task/10793/fdinfo/51
897858	/proc/10610/task/10793/fdinfo/52
·	/proc/10610/task/10793/fdinfo/53
897860	/proc/10610/task/10793/fdinfo/54
·	/proc/10610/task/10793/fdinfo/55
·	/proc/10610/task/10793/fdinfo/56
·	/proc/10610/task/10793/fdinfo/57
·	/proc/10610/task/10793/fdinfo/58
-	/proc/10610/task/10793/fdinfo/59
·	/proc/10610/task/10793/fdinfo/60
·	/proc/10610/task/10793/fdinfo/61

12. 從封包分析來看，駭客用的 test 帳號在 17:38 左右開始向上層中繼站 59.188.237.12 報到傳輸主機資料，時間上大致與 auth.log 紀錄中相同，中繼站收到後開始透過帳號 test 向主機進行 SSH 登入。因為過程中資料都經過加密，合理推測會下載惡意程式 squid64，並且執行後刪除。

```
root@ubuntu:~/kevin# less /var/log/auth.log | grep Accepted
Apr 27 16:38:18 ubuntu sshd[32742]: Accepted password for test from 140.[redacted] port 62083 ssh2
Apr 27 16:41:39 ubuntu sshd[909]: Accepted password for test from 140.[redacted] port 19161 ssh2
Apr 27 16:44:45 ubuntu sshd[1426]: Accepted password for test from 140[redacted] port 51318 ssh2
Apr 27 16:58:42 ubuntu sshd[3595]: Accepted password for test from 140[redacted] port 19857 ssh2
Apr 27 17:37:08 ubuntu sshd[8609]: Accepted password for test from 59.188.237.12 port 1971 ssh2
root@ubuntu:~/kevin#
```

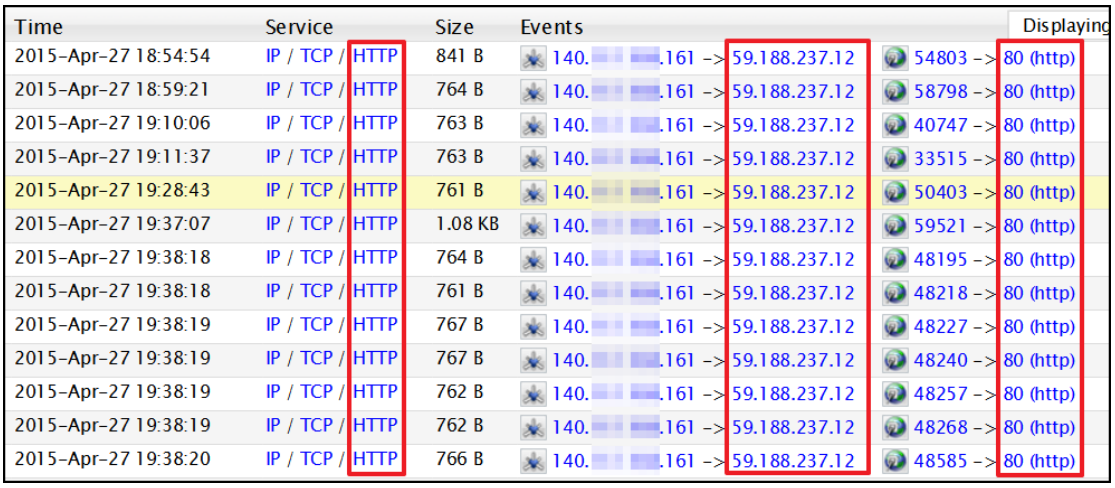




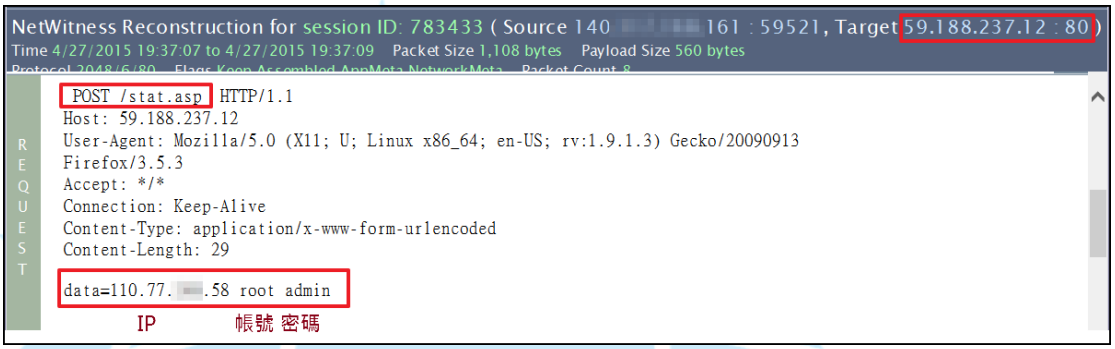
13. 從封包紀錄中可以看到，主機端開始大量對外部 IP 進行 SSH 暴力破解，平均每一個 session 大小約有 3KB，內容應該是包含破解用的密碼字典庫。

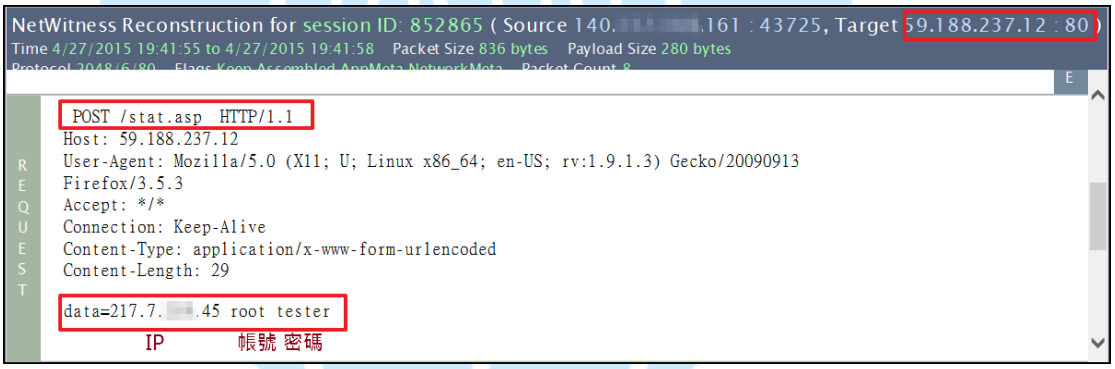
Time	Service	Size	Events
2015-Apr-27 18:41:29	IP / TCP / SSH	3.04 KB	140. 161 -> 183.207.98.102 50268 -> 22 (ssh)
2015-Apr-27 18:41:29	IP / TCP / SSH	3.66 KB	140. 161 -> 50.18.104.40 39643 -> 22 (ssh)
2015-Apr-27 18:41:29	IP / TCP / SSH	3.25 KB	140. 161 -> 61.186.44.66 34219 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	3.73 KB	140. 161 -> 50.18.104.40 39897 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	3.30 KB	140. 161 -> 183.207.98.102 50481 -> 22 (ssh)
2015-Apr-27 18:41:29	IP / TCP / SSH	4.38 KB	140. 161 -> 52.64.39.50 34344 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	3.56 KB	140. 161 -> 49.107.65.101 38245 -> 22 (ssh)
2015-Apr-27 18:41:31	IP / TCP / SSH	3.11 KB	140. 161 -> 183.207.98.102 50760 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	3.45 KB	140. 161 -> 183.156.1.151 53013 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	4.01 KB	140. 161 -> 222.90.136.125 43347 -> 22 (ssh)
2015-Apr-27 18:41:31	IP / TCP / SSH	3.73 KB	140. 161 -> 50.18.104.40 40142 -> 22 (ssh)
2015-Apr-27 18:41:29	IP / TCP / SSH	3.13 KB	140. 161 -> 113.65.232.150 52622 -> 22 (ssh)
2015-Apr-27 18:41:31	IP / TCP / SSH	3.25 KB	140. 161 -> 61.186.44.66 34594 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	4.02 KB	140. 161 -> 97.125.213.46 49002 -> 22 (ssh)
2015-Apr-27 18:41:29	IP / TCP / SSH	4.01 KB	140. 161 -> 95.142.98.153 44212 -> 22 (ssh)
2015-Apr-27 18:41:29	IP / TCP / SSH	2.72 KB	140. 161 -> 41.252.194.78 50161 -> 22 (ssh)
2015-Apr-27 18:41:30	IP / TCP / SSH	2.89 KB	140. 161 -> 217.7.219.45 55183 -> 22 (ssh)

14. 當主機收集完破解 SSH 成功的帳號密碼後，會開始向上層中繼站 59.188.237.12 回傳被攻擊者主機的 SSH 帳號及密碼，而且是用 HTTP POST 明文方式傳送內容，而由/stat.asp 接收，且大多的密碼都是常見的簡單弱密碼。內容格式是“data=[IP 位址][帳號][密碼]”。

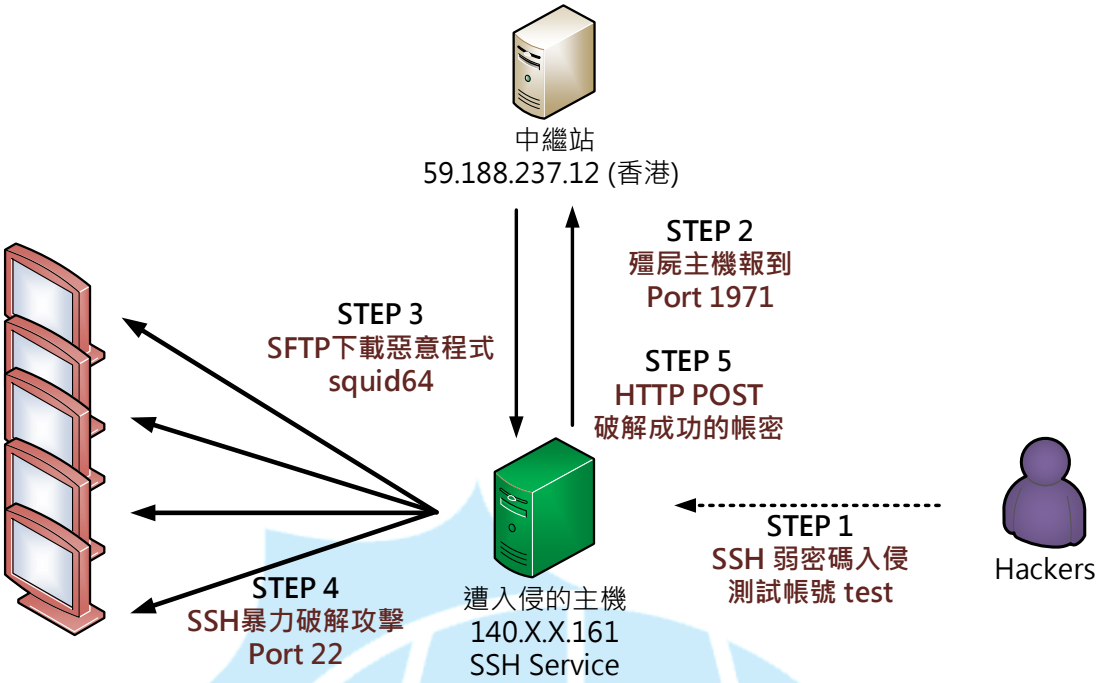


Time	Service	Size	Events	Displaying
2015-Apr-27 18:54:54	IP / TCP / HTTP	841 B	140.[redacted].161 -> 59.188.237.12	54803 -> 80 (http)
2015-Apr-27 18:59:21	IP / TCP / HTTP	764 B	140.[redacted].161 -> 59.188.237.12	58798 -> 80 (http)
2015-Apr-27 19:10:06	IP / TCP / HTTP	763 B	140.[redacted].161 -> 59.188.237.12	40747 -> 80 (http)
2015-Apr-27 19:11:37	IP / TCP / HTTP	763 B	140.[redacted].161 -> 59.188.237.12	33515 -> 80 (http)
2015-Apr-27 19:28:43	IP / TCP / HTTP	761 B	140.[redacted].161 -> 59.188.237.12	50403 -> 80 (http)
2015-Apr-27 19:37:07	IP / TCP / HTTP	1.08 KB	140.[redacted].161 -> 59.188.237.12	59521 -> 80 (http)
2015-Apr-27 19:38:18	IP / TCP / HTTP	764 B	140.[redacted].161 -> 59.188.237.12	48195 -> 80 (http)
2015-Apr-27 19:38:18	IP / TCP / HTTP	761 B	140.[redacted].161 -> 59.188.237.12	48218 -> 80 (http)
2015-Apr-27 19:38:19	IP / TCP / HTTP	767 B	140.[redacted].161 -> 59.188.237.12	48227 -> 80 (http)
2015-Apr-27 19:38:19	IP / TCP / HTTP	767 B	140.[redacted].161 -> 59.188.237.12	48240 -> 80 (http)
2015-Apr-27 19:38:19	IP / TCP / HTTP	762 B	140.[redacted].161 -> 59.188.237.12	48257 -> 80 (http)
2015-Apr-27 19:38:19	IP / TCP / HTTP	762 B	140.[redacted].161 -> 59.188.237.12	48268 -> 80 (http)
2015-Apr-27 19:38:20	IP / TCP / HTTP	766 B	140.[redacted].161 -> 59.188.237.12	48585 -> 80 (http)





III. 網路架構圖



1. 駭客透過 SSH 弱密碼入侵學校主機，並使用測試帳號 test 登入。
2. 被入侵主機回報主機資料給中繼站。
3. 駭客從中繼站下載惡意程式 squid64 並執行後刪除檔案。
4. 主機產生十個 squid64 的 PID 持續對外部大量主機進行 SSH 暴力破解。
5. 破解成功的主機帳號密碼透過 HTTP POST 方式回傳給中繼站。

IV.建議與總結

1. 此案例主機因為測試帳號 test 維護完後並未完全移除，而只移除了帳號的家目錄。
2. 該主機預設有開啟 SSH server 服務讓管理者連入，然而並未限制連入來源端 IP，導致駭客利用帳號 test 以及弱密碼入侵成功。
3. 駭客 SSH 入侵後雖不能存取 root 權限，但能透過 SFTP 向想港中繼站下載惡意程式 squid64 ，並且大量去對外部主機進行 SSH 破解攻擊。
4. SSH 外部攻擊時將破解成功的主機帳號密碼透過 HTTP POST 方式傳輸給上層香港中繼站。
5. 對外 SSH 破解攻擊時占用大量網路頻寬，導致單位對外網路壅塞影響其他

人網路使用。

6. 惡意程式排除方式為，因惡意程式 squid64 主體駭客執行完就已經移除，故只須將正在執行的惡意程式 squid64 的 PID 程序依序 kill 刪除。
7. 漏洞修補方式則是透過將帳號 test 徹底從 /etc/passwd 中移除。
8. 設定 SSH 來源端登入限制，限制特定網段或 IP 能夠存取，避免駭客再次入侵，或者加強帳號的密碼強度防止輕易被破解。