學術網路資安事件案例分析&主機檢測工具

北區ASOC 二線工程師：劉家維

外部攻擊趨勢

- 以針對IOT或網路設備的弱點掃描攻擊占大宗。
- 從趨勢圖中可以發現幾個異常攻擊事件增加的時間與該設備爆發漏洞的時間相符。
- 例如：

1. 一月中旬的DVR影像主機漏洞
2. 四月的DrayTek路由器，與DD-WRT韌體漏洞

惡意軟體行為

1. 加密勒索
2. 散播BOT
3. 挖礦劫持
4. 竊取資料

目標式勒索病毒攻擊台灣企業

趨勢揭露鎖定臺灣企業的勒索軟體攻擊行動，事故是否有關

鎖定石化工業與高科技製造業的攻擊，從5月4日開始接連發生，其中有些是利用勒索軟體發動的攻擊。趨勢科技也發現一波新的勒索軟體攻擊行動，發生時間也是在5月初，不過沒有指出這起行動與前述攻擊事件有無關連

文/ 周峻佑 | 2020-05-08 發表

讚 6.1 萬 按讚加入iThome粉絲團

TREND MICRO SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Search:

Home | Categories

Home » Malware » Targeted Ransomware Attack Hits Taiwanese Organizations

Targeted Ransomware Attack Hits Taiwanese Organizations

Posted on: May 6, 2020 at 5:00 am Posted in: Malware Author: Trend Micro

自由財經

首頁 > 財經政策

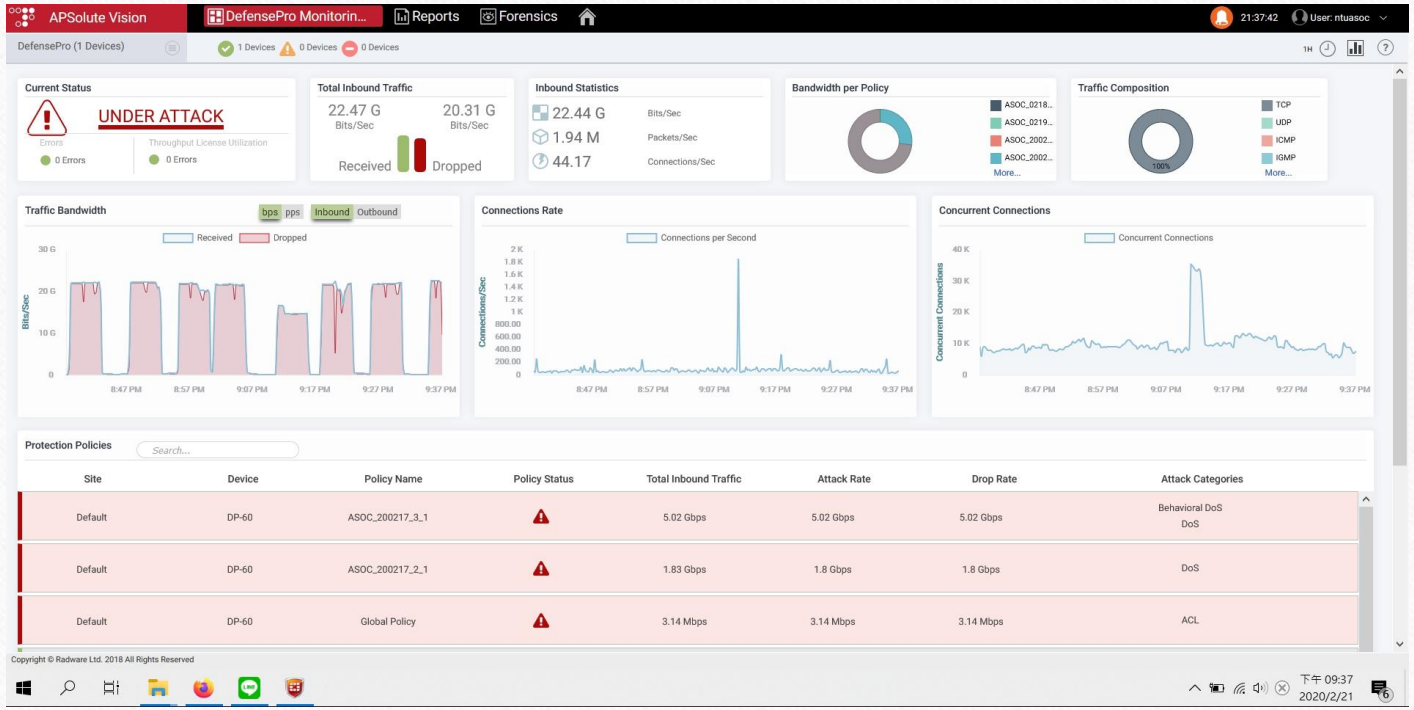
中油、台塑、力成 連遭勒索病毒攻擊

2020-05-06 05:30

中油及台塑四日起陸續遭惡意軟體攻擊，國安及資安體系研判此非個案，不排除是針對五二○蔡英文總統就職典禮前的

視訊監控主機遭駭，成為DDoS攻擊幫兇

實際偵測之DDoS攻擊流量



利用IoT搜尋引擎查詢攻擊來源

175.183.80.178 175-183-80-178.adsl.dynamic.seed.net.tw

self-signed

City	Nantou
Country	Taiwan
Organization	Taiwan Infrastructure Network Technologie
ISP	New Century InfoComm Tech. Co.
Last Update	2020-03-14T00:03:25.712607
Hostnames	175-183-80-178.adsl.dynamic.seed.net.tw
ASN	AS18049

Ports

80 443 554

Services

80
tcp
http

```
HTTP/1.1 401 Unauthorized
Server: mini_httpd/1.19 19dec2003
Date: Thu, 12 Mar 2020 01:39:31 GMT
Cache-Control: no-cache,no-store
WWW-Authenticate: Basic realm="DVR"
Content-Type: text/html; charset=%s
Connection: close
```

443
tcp
https

```
HTTP/1.1 401 Unauthorized
Server: mini_httpd/1.19 19dec2003
Date: Sat, 14 Mar 2020 00:09:09 GMT
Cache-Control: no-cache,no-store
WWW-Authenticate: Basic realm="DVR"
Content-Type: text/html; charset=%s
Connection: close
```

DVR影像主機案例

異常DVR主機封包範例

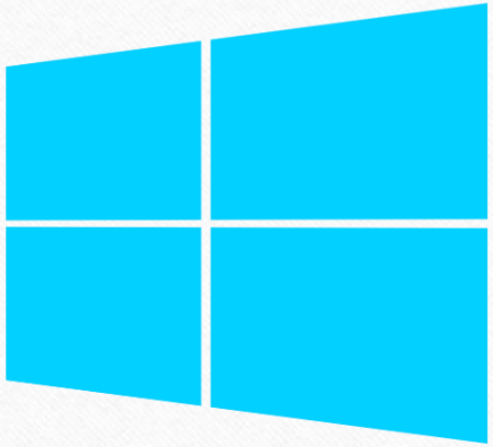
關鍵字：uc-httpd 1.0.0、雄邁韌體漏洞

No.	Time	Source	Destination	Protocol	Length	SourcePort	DestinationPort	Info
4601	2020-02-27 07:09:58.503515	140.112.254.4	163.28.16.80	DNS	89	53	42228	Standard query response 0x1998 A xmsecu100.net A 156.255.121.99
4602	2020-02-27 07:09:58.503559	140.112.254.4	163.28.16.80	DNS	168	53	42228	Standard query response 0x1de8 AAAA xmsecu100.net SOA monovm.mars.orderbox-dns.com
4604	2020-02-27 07:09:58.505223	8.8.8.8	163.28.16.80	DNS	89	53	42228	Standard query response 0x1998 A xmsecu100.net A 156.255.121.99
4605	2020-02-27 07:09:58.505816	163.28.16.80	8.8.8.8	ICMP	117	53	42228	Destination unreachable (Port unreachable)
4606	2020-02-27 07:09:58.508626	8.8.8.8	163.28.16.80	DNS	165	53	42228	Standard query response 0x1de8 AAAA xmsecu100.net SOA monovm.mars.orderbox-dns.com
4607	2020-02-27 07:09:58.509182	163.28.16.80	8.8.8.8	ICMP	193	53	42228	Destination unreachable (Port unreachable)
4631	2020-02-27 07:10:22.822996	163.28.16.80	140.112.254.4	DNS	75	33559	53	Standard query 0xc9d4 A 54cq.zhaoyx.xyz
4632	2020-02-27 07:10:22.823042	163.28.16.80	8.8.8.8	DNS	75	33559	53	Standard query 0xc9d4 A 54cq.zhaoyx.xyz
4633	2020-02-27 07:10:22.823069	163.28.16.80	140.112.254.4	DNS	75	33559	53	Standard query 0xce84 AAAA 54cq.zhaoyx.xyz
4634	2020-02-27 07:10:22.823131	163.28.16.80	8.8.8.8	DNS	75	33559	53	Standard query 0xce84 AAAA 54cq.zhaoyx.xyz
4635	2020-02-27 07:10:22.824036	140.112.254.4	163.28.16.80	DNS	139	53	33559	Standard query response 0xce84 AAAA 54cq.zhaoyx.xyz SOA ns1.myhostadmin.net
4636	2020-02-27 07:10:22.824134	140.112.254.4	163.28.16.80	DNS	262	53	33559	Standard query response 0xc9d4 A 54cq.zhaoyx.xyz A 45.113.200.137 NS ns3.myhostadmin.
4638	2020-02-27 07:10:22.824989	8.8.8.8	163.28.16.80	DNS	139	53	33559	Standard query response 0xce84 AAAA 54cq.zhaoyx.xyz SOA ns1.myhostadmin.net
4639	2020-02-27 07:10:22.825020	8.8.8.8	163.28.16.80	DNS	91	53	33559	Standard query response 0xc9d4 A 54cq.zhaoyx.xyz A 45.113.200.137
4640	2020-02-27 07:10:22.825648	163.28.16.80	8.8.8.8	ICMP	167	53	33559	Destination unreachable (Port unreachable)
4641	2020-02-27 07:10:22.825691	163.28.16.80	8.8.8.8	ICMP	119	53	33559	Destination unreachable (Port unreachable)
4682	2020-02-27 07:11:23.207650	163.28.16.80	140.112.254.4	DNS	73	41536	53	Standard query 0x8d91 A www.duote.com
4683	2020-02-27 07:11:23.207693	163.28.16.80	8.8.8.8	DNS	73	41536	53	Standard query 0x8d91 A www.duote.com
4684	2020-02-27 07:11:23.207718	163.28.16.80	140.112.254.4	DNS	73	41536	53	Standard query 0x9291 AAAA www.duote.com

DVR影像主機蘊含的風險

- DVR廠商，共用韌體情形嚴重。
- 使用者經常為修改預設密碼
- 設備內部主機板及韌體多為中國公司出品。
- 設備韌體未經改寫，當漏洞爆發時，將造成受害範圍擴大。
- 設備暴露於Internet且管理網頁未設定ACL限制存取。

Windows 系統基礎檢測



Windows 檢測步驟

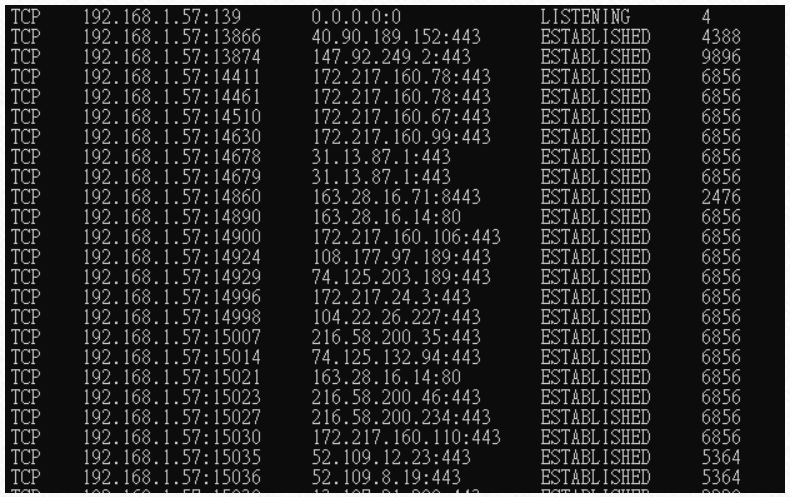
1. 檢查是否有異常的對外連線行為
2. 檢查是否有異常的process
3. 檢查登錄擋是否遭串改

- 推薦工具：Tcpview 、Process Explore、WhatChanged

對外連線檢查

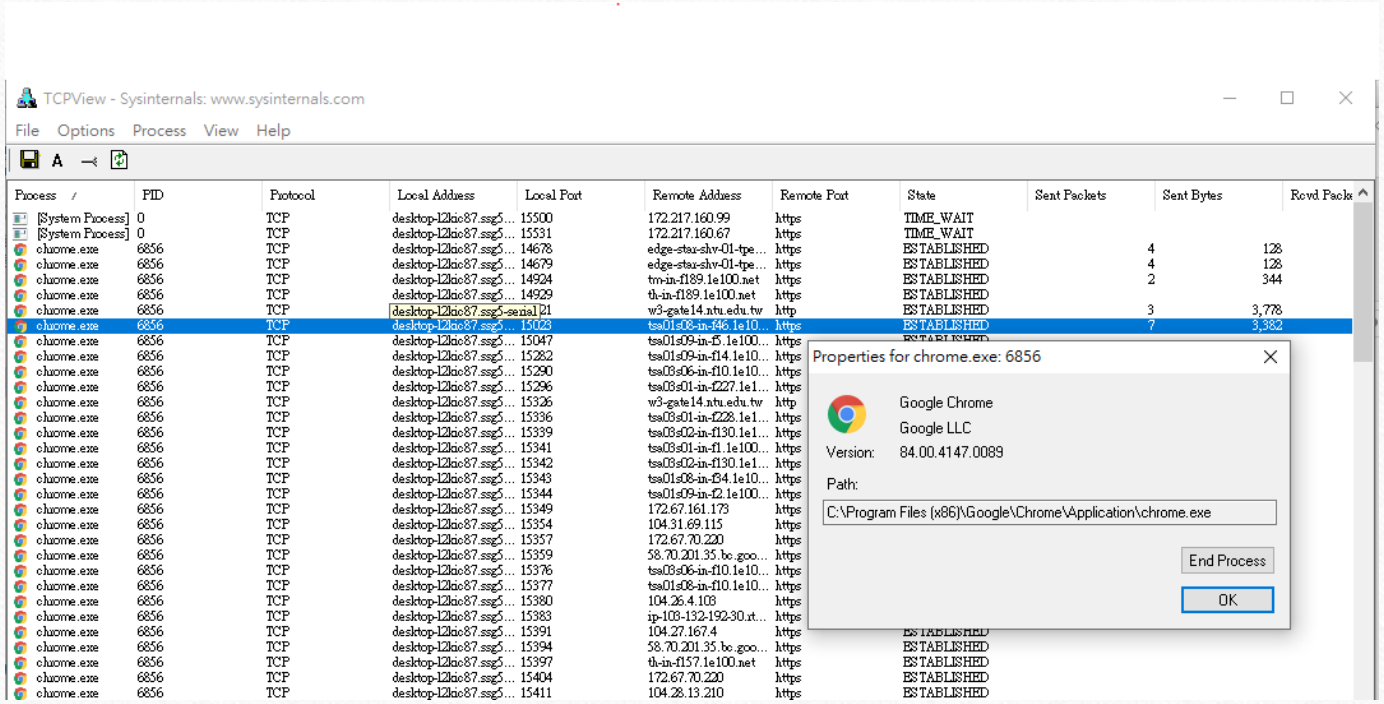
1. 可透過windows 命令提示字元視窗 輸入指令 netstat –ano –p tcp 查看該台設備tcp對外連線情形。

- -ano 表示顯示所有建立的連線、Port、PID
- -p 指定通訊協定例:TCP、UDP、TCPv6、UDPv6



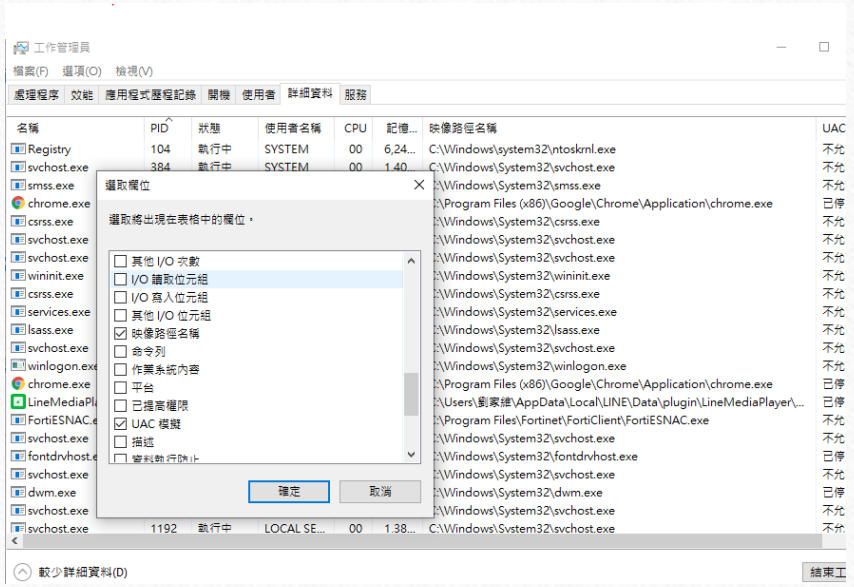
TCP	192.168.1.57:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.57:13866	40.90.189.152:443	ESTABLISHED	4388
TCP	192.168.1.57:13874	147.92.249.2:443	ESTABLISHED	9896
TCP	192.168.1.57:14411	172.217.160.78:443	ESTABLISHED	6856
TCP	192.168.1.57:14461	172.217.160.78:443	ESTABLISHED	6856
TCP	192.168.1.57:14510	172.217.160.67:443	ESTABLISHED	6856
TCP	192.168.1.57:14630	172.217.160.99:443	ESTABLISHED	6856
TCP	192.168.1.57:14678	31.13.87.1:443	ESTABLISHED	6856
TCP	192.168.1.57:14679	31.13.87.1:443	ESTABLISHED	6856
TCP	192.168.1.57:14860	163.28.16.71:8443	ESTABLISHED	2476
TCP	192.168.1.57:14890	163.28.16.14:80	ESTABLISHED	6856
TCP	192.168.1.57:14900	172.217.160.106:443	ESTABLISHED	6856
TCP	192.168.1.57:14924	108.177.97.189:443	ESTABLISHED	6856
TCP	192.168.1.57:14929	74.125.203.189:443	ESTABLISHED	6856
TCP	192.168.1.57:14996	172.217.24.3:443	ESTABLISHED	6856
TCP	192.168.1.57:14998	104.22.26.227:443	ESTABLISHED	6856
TCP	192.168.1.57:15007	216.58.200.35:443	ESTABLISHED	6856
TCP	192.168.1.57:15014	74.125.132.94:443	ESTABLISHED	6856
TCP	192.168.1.57:15021	163.28.16.14:80	ESTABLISHED	6856
TCP	192.168.1.57:15023	216.58.200.46:443	ESTABLISHED	6856
TCP	192.168.1.57:15027	216.58.200.234:443	ESTABLISHED	6856
TCP	192.168.1.57:15030	172.217.160.110:443	ESTABLISHED	6856
TCP	192.168.1.57:15035	52.109.12.23:443	ESTABLISHED	5364
TCP	192.168.1.57:15036	52.109.8.19:443	ESTABLISHED	5364

Tcpview

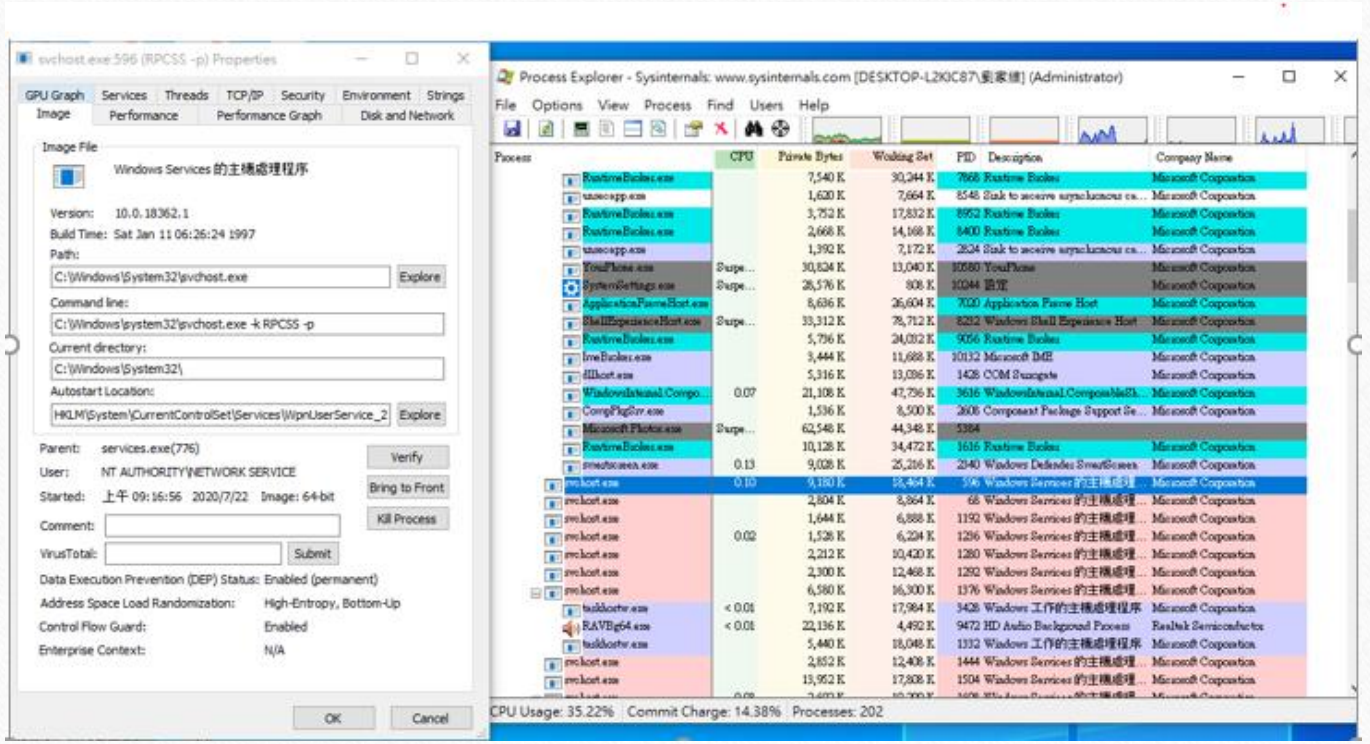

TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process PID Protocol Local Address Local Port Remote Address Remote Port State Sent Packets Sent Bytes Rcvd Packs
[System Process] 0 TCP desktop-l2iac87.ssg5... 15500 172.217.160.99 https TIME_WAIT
[System Process] 0 TCP desktop-l2iac87.ssg5... 15531 172.217.160.67 https TIME_WAIT
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 14678 edge-stau-shv-01-tpe... https ESTABLISHED 4 128
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 14679 edge-stau-shv-01-tpe... https ESTABLISHED 4 128
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 14924 tm-in-f189.1e100.net https ESTABLISHED 2 344
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 14929 th-in-f189.1e100.net https ESTABLISHED
chuome.exe 6856 TCP desktop-l2iac87.ssg5-serial 21 w3-gate14.ntu.edu.tw http ESTABLISHED 3 3,778
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15023 tsa01s08-in-f46.1e10... https ESTABLISHED 7 3,382
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15047 tsa01s09-in-f5.1e100... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15282 tsa01s09-in-f14.1e10... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15290 tsa03s06-in-f10.1e10... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15296 tsa03s01-in-f227.1e1... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15326 w3-gate14.ntu.edu.tw http
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15336 tsa03s01-in-f228.1e1... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15339 tsa03s02-in-f130.1e1... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15341 tsa03s01-in-f1.1e100... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15342 tsa03s02-in-f130.1e1... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15343 tsa01s08-in-f34.1e10... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15344 tsa01s09-in-f2.1e100... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15349 172.67.161.173 https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15354 104.31.69.115 https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15357 172.67.70.220 https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15359 58.70.201.35.bc.goo... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15376 tsa03s06-in-f10.1e10... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15377 tsa01s08-in-f10.1e10... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15380 104.26.4.103 https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15383 ip-103-132-192-30.xt... https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15391 104.27.167.4 https
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15394 58.70.201.35.bc.goo... https ESTABLISHED
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15397 th-in-f157.1e100.net https ESTABLISHED
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15404 172.67.70.220 https ESTABLISHED
chuome.exe 6856 TCP desktop-l2iac87.ssg5... 15411 104.28.13.210 https ESTABLISHED
Properties for chrome.exe: 6856
Google Chrome
Google LLC
Version: 84.00.4147.0089
Path:
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
End Process
OK

PROCESS 檢查

- 確認svchost、csrss、wininit 等的映像路徑是否位於 Windows\system32\ 目錄下執行



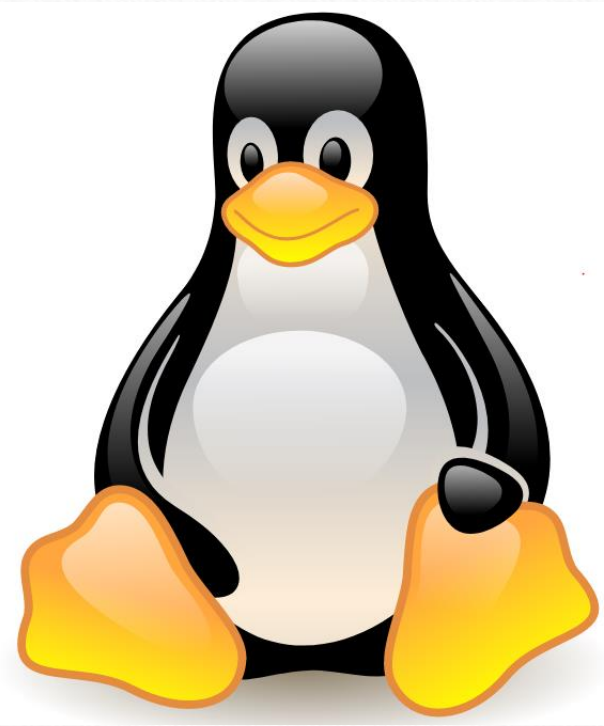
Process Explore範例



登錄機碼檢查

- 於開始選單點擊右鍵”執行” 輸入 regedit 進入登錄碼編輯視窗。

Linux 系統基礎檢測



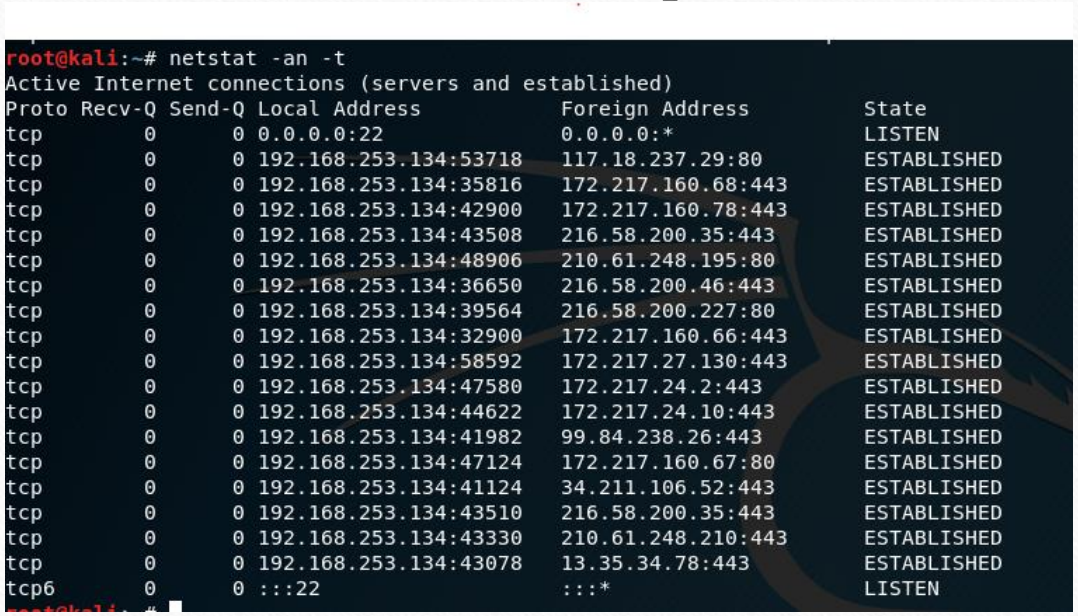
Linux 系統檢測&安全性稽核

1. 檢查是否有異常的對外連線行為
2. 檢查是否有異常的process占用系統資源
3. 檢查系統排程是否有遭到串改
4. 安全設定稽核

- 推薦工具：top、lynis

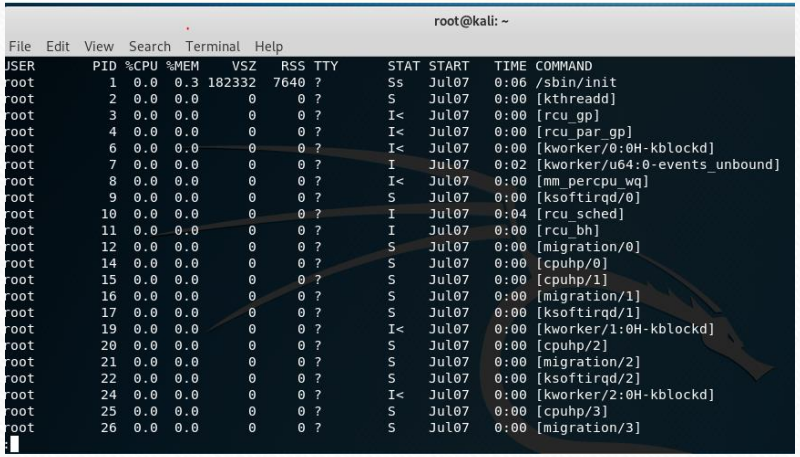
對外連線檢查

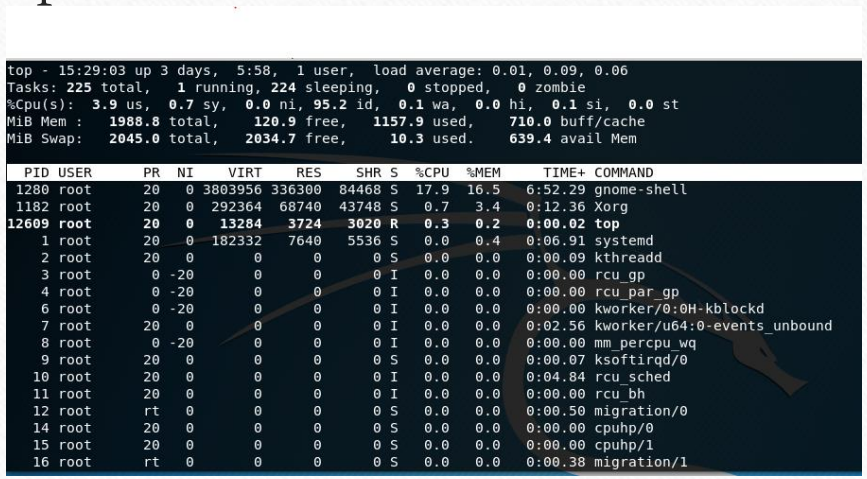
1. 可透過Terminal 輸入指令 netstat –an -p –t 查看該台設備tcp對外連線情形。



PROCESS 檢查

- 輸入指令ps aux | less 查看正在執行之process ，是否有異常的程式於背景執行
- 也可輸入top及時查看最消耗資源的process





系統排程檢查

- 檢查路徑/etc 下

cron.d、cron.daily、cron.hourly、cron.weekly

cron.monthly等檔案目錄&

crontab 文件是否包含異常工作排程

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo
rt /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo
rt /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo
rt /etc/cron.monthly )
#
```

系統安全稽核工具Lynis

- Lynis 是由 CISOfy 所維護的工具程式
- 提供的主要功能如下：
  1. 法遵測試
  2. 自動稽核
  3. 漏洞檢測
  4. 滲透測試
  5. 改善建議

支援作業係統

- AIX
- FreeBSD
- HP-UX
- Linux
- macOS
- NetBSD
- NixOS
- OpenBSD
- Solaris

安裝使用流程

- 建議利用git clone 指令自 https://github.com/CISOfy/lynis抓取最新版本
- cd至lynis 檔案目錄
- 利用指令新增執行權限 chmod +x ./lynis

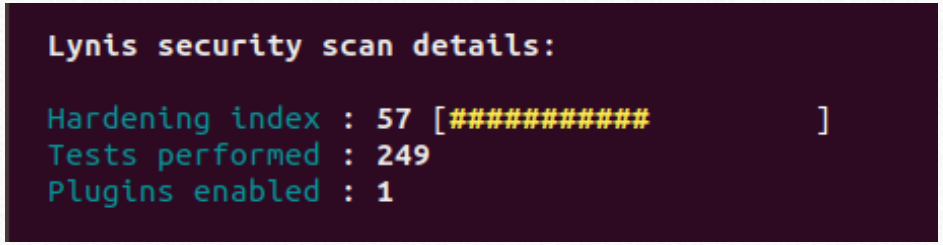
執行檢測

- Lynis 使用上非常簡單，執行時請給予 root 權限以確保取得最佳的檢測效果。
- 執行指令：sudo ./lynis audit system
- 稽核分數：

進度條越滿表示安全性越高

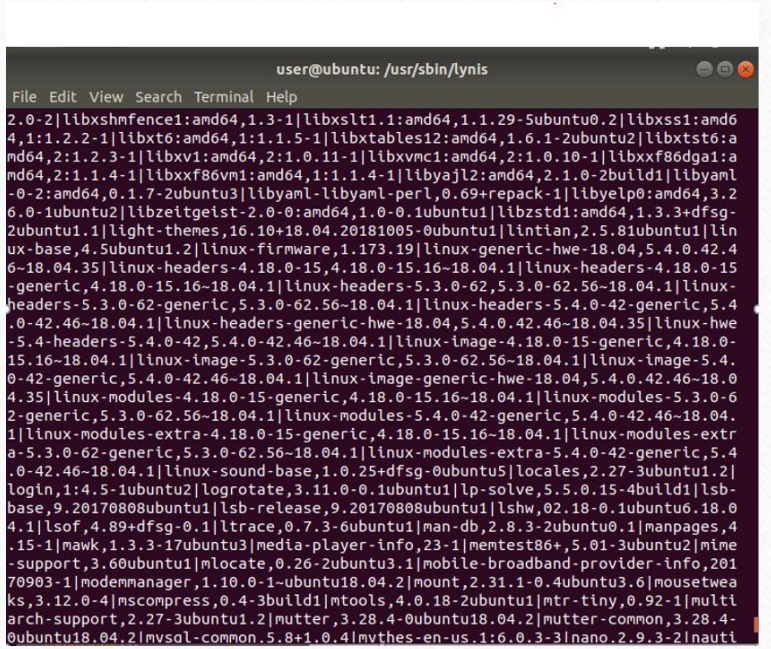
Tests performed 表示總共的測試項目

Plugins enabled 外掛程式啟用數量



檢測報表

- 檢測報告產生於/var/log/lynis.log 路徑下的lynis.log、lynis-report.dat
- 原始報表為純文字檔閱讀不易
- 利用開源工具lynis-report-converter
- 轉換為易於閱讀的格式



報表轉換工具安裝

- 利用 wget 指令安裝 https://raw.githubusercontent.com/d4t4king/lynis-report-converter/master/lynis-report-converter.pl
- 安裝以下函式庫
  1. apt install htmldoc
  2. cpan install HTML::HTMLDoc
  3. apt install libxml-writer-perl
  4. apt install libarchive-zip-perl
  5. capn install Excel::Writer::XLSX

執行報表產出

- 執行指令
  1. ./lynis-report-converter.pl –o report.html
  2. ./lynis-report-converter.pl –E –o report.xlsx