

NetworkSecurity_Project1_Report

網工所碩一 309552005 吳偉誠

Set of events:b、d、f、h、j

A part

(b) Logoff : Sign out.

| Time | fields.hostname | event.code | event.action |
|------------------------------|-----------------|------------|--------------|
| > Oct 7, 2020 @ 17:42:27.738 | _309552005 | 4,634 | logged-out |

- Descriptions :

event.code 4634 : An account was logged off

message

帳戶已登出 :

主旨 :

| | |
|----------|----------------|
| 安全性識別碼 : | S-1-5-90-0-4 |
| 帳戶名稱 : | DWM-4 |
| 帳戶網域 : | Window Manager |
| 登入識別碼 : | 0x55079A |

message : can see "帳戶已登出" information

- Method :

- win+R and input gpedit.msc :
open the The Local Group Policy Editor
- Change the audit event(Audit logout)
 1. 電腦設定 > windows設定 > 安全性設定 > 進階稽核原則設定 > 系統稽核原則-本機群組原則物件 > 登入/登出 > 稽核登出
 2. set 稽核登出 to "成功" and "失敗"
- Log out and log in of my account
- Can see log in the logstash

(d) Screensaver dismissed : Dismiss a screen saver.

| Time | fields.hostname | event.code | event.action |
|------------------------------|-----------------|------------|---------------------------|
| > Oct 7, 2020 @ 19:12:58.274 | _309552005 | 4,803 | Other Logon/Logoff Events |

- Descriptions :

`event.code` 4803 : The screen saver was dismissed
`message`

已解除螢幕保護裝置。

主旨：

| | |
|---------|--|
| 安全性識別碼： | S-1-5-21-1702212169-1769259126-3245154374-1002 |
| 帳戶名稱： | wulearn |
| 帳戶網域： | DESKTOP-95M00R5 |
| 登入識別碼： | 0x613AA7 |

`message` : can see "已解除螢幕保護裝置" information

- Method :

- `win + R` and input `gpedit.msc`:
open the The Local Group Policy Editor
- Change the audit event(Audit other login/logout events)
 1. 電腦設定 > **windows**設定 > 安全性設定 > 進階稽核原則設定 > 系統稽核原則-本機群組原則物件 > 登入/登出 > 稽核其他登入/登出事件
 2. set 稽核其他登入/登出事件 to "成功" and "失敗"
- Let the screen enter the saver and wake it up
- Can see log in the logstash

(f) Close the specific application : Close the calculator.exe.

| Time | fields.hostname | event.code | event.action |
|------------------------------|-----------------|------------|----------------|
| > Oct 7, 2020 @ 19:21:15.900 | _309552005 | 4,689 | exited-process |

- Descriptions :

`event.code` 4689 : A process has exited

| <code>event.action</code> | <code>process.name</code> |
|---------------------------|---------------------------|
| exited-process | Calculator.exe |

`process.name` : can see the application is "Calculator.exe"

- Method :

- `win + R` and input `gpedit.msc`:
open the The Local Group Policy Editor
- Change the audit event(Audit process tracking)
 1. 電腦設定 > **windows**設定 > 安全性設定 > 本機原則 > 稽核原則 > 稽核程序追蹤
 2. set 稽核程序追蹤 to "成功" and "失敗"
- Open Calculator.exe and close it
- Can see log in the logstash

(h) Change file name : Change a existed file's name.

| | | | | | |
|--|------------|-------|---------------------|-------------|---------------------------------------|
| > Oct 7, 2020 @ 20:14:54.481 | _309552005 | 4,663 | File System | 嘗試存取物件。 | C:\Users\wulearn\Desktop\new_name.txt |
| 主體: 安全性識別碼: S-1-5-21-1702212169-1769259126-3245154374-1002 帳戶名稱: wulearn 帳戶網域: DESKTOP-95MOOR5 登入識別碼: 0x613AA7 | | | | | |
| > Oct 7, 2020 @ 20:14:54.481 | _309552005 | 4,658 | File System | 物件控制代碼已關閉。 | - |
| 主體: 安全性識別碼: S-1-5-21-1702212169-1769259126-3245154374-1002 帳戶名稱: wulearn 帳戶網域: DESKTOP-95MOOR5 登入識別碼: 0x613AA7 | | | | | |
| > Oct 7, 2020 @ 20:14:54.473 | _309552005 | 4,658 | File System | 物件控制代碼已關閉。 | - |
| 主體: 安全性識別碼: S-1-5-21-1702212169-1769259126-3245154374-1002 帳戶名稱: wulearn 帳戶網域: DESKTOP-95MOOR5 登入識別碼: 0x613AA7 | | | | | |
| > Oct 7, 2020 @ 20:14:54.472 | _309552005 | 4,690 | Handle Manipulation | 嘗試複製物件控制代碼。 | - |
| 主體: 安全性識別碼: S-1-5-21-1702212169-1769259126-3245154374-1002 帳戶名稱: wulearn 帳戶網域: DESKTOP-95MOOR5 登入識別碼: 0x613AA7 | | | | | |
| > Oct 7, 2020 @ 20:14:54.472 | _309552005 | 4,658 | File System | 物件控制代碼已關閉。 | - |
| 主體: 安全性識別碼: S-1-5-21-1702212169-1769259126-3245154374-1002 帳戶名稱: wulearn 帳戶網域: DESKTOP-95MOOR5 登入識別碼: 0x613AA7 | | | | | |
| > Oct 7, 2020 @ 20:14:54.472 | _309552005 | 4,656 | File System | 已要求物件控制代碼。 | C:\Users\wulearn\Desktop\old_name.txt |
| 主體: 安全性識別碼: S-1-5-21-1702212169-1769259126-3245154374-1002 帳戶名稱: wulearn 帳戶網域: DESKTOP-95MOOR5 登入識別碼: 0x613AA7 | | | | | |

- Descriptions :
As can be seen from the above figure, in less than a second, the file name changed from "old_name.txt" to "new_name.txt" (which experienced many processes)
- Method :
 - win + R and input gpedit.msc:
open the The Local Group Policy Editor
 - Change the audit event(Audit object access)
 1. 電腦設定 > windows設定 > 安全性設定 > 本機原則 > 稽核原則 > 稽核物件存取
 2. set 稽核物件存取 to "成功" and "失敗"
 - Change file audit
 1. 檔案 -> 右鍵 -> 內容 -> 安全性 -> 進階
-> 稽核 -> 新增 -> 主體 -> input "使用者名稱" -> 確定
 2. audit select all
 - Change the file's name(old_name.txt) to "new_name.txt"
 - Can see log in the logstash

(j) Visit http website : The website is require to be <http://www.fybus.com.tw/>

| Time ▾ | fields.hostname | event.code | event.action |
|------------------------------|-----------------|------------|----------------|
| > Oct 7, 2020 @ 20:44:30.564 | _309552005 | 4,689 | exited-process |
| > Oct 7, 2020 @ 20:44:30.546 | _309552005 | 4,689 | exited-process |
| > Oct 7, 2020 @ 20:44:30.058 | _309552005 | - | network_flow |

- Descriptions:

`event.action` : network_flow

| event.action | destination.ip |
|------------------------|----------------|
| exited-process | - |
| exited-process | - |
| network_flow | 192.168.56.101 |
| network_flow | 192.168.56.101 |
| network_flow | 140.113.235.1 |
| can see exited-process | |
| network_flow | 61.221.112.46 |
| created-process | - |

can see created-process

`destination.ip` : 61.221.122.46(the WEB address)

- Method :

- Install "packetbeat" and "win10pcap"
- Run packetbeat.exe
- Go the WEB(<http://www.fybus.com.tw/>)
- Can see log in the logstash

- Check :

- ping www.fybus.com.tw can see the address : 61.221.122.46

```
PS C:\Users\la4865> ping www.fybus.com.tw

Ping www.fybus.com.tw [61.221.112.46] (使用 32 位元組的資料):
回覆自 61.221.112.46: 位元組=32 時間=5ms TTL=51
回覆自 61.221.112.46: 位元組=32 時間=5ms TTL=51
回覆自 61.221.112.46: 位元組=32 時間=5ms TTL=51
回覆自 61.221.112.46: 位元組=32 時間=6ms TTL=51

61.221.112.46 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 5ms, 最大值 = 6ms, 平均 = 5ms
```

B part

1. kibana server is not ready yet :

After completing the setting of the ubuntu part, I found that this will happen when kibana is turned on. Later, I left it and went out to buy dinner and it was normal...haha.I guess the server may not be ready

2. Logstash not work :

When I found this problem, I was stuck for a long time, so I went to the issue of github to see if any other students had this problem. Later I found that it really happened and someone gave the correct answer and direction. This is useful to me!

(The output should be "logstash",and kibana Index patterns should called "logstash*")

3. The correct location of various audit events :

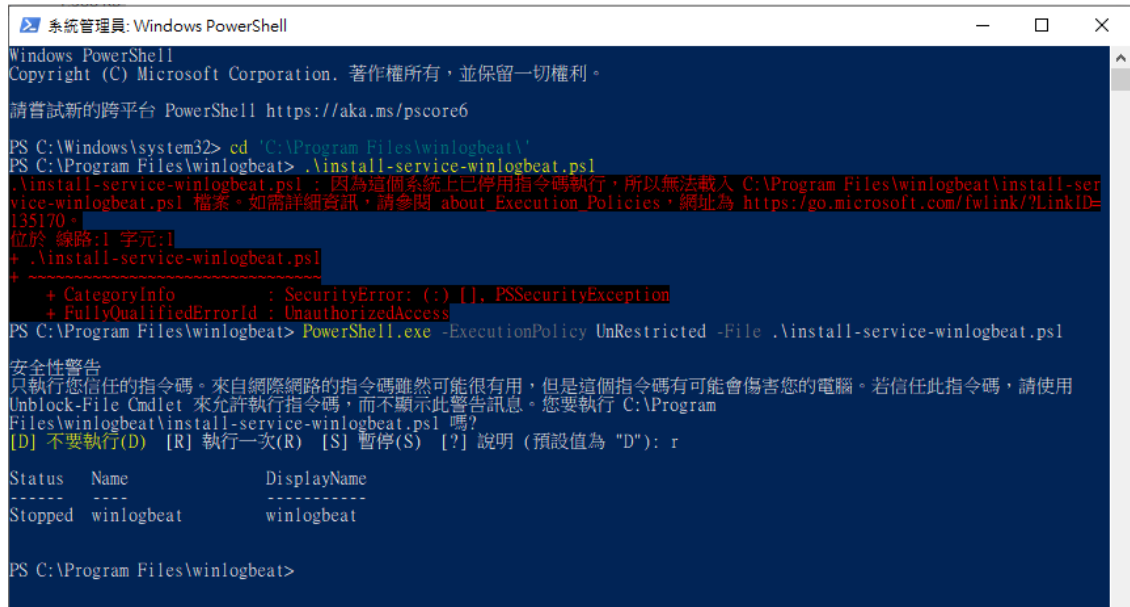
Some of this part of the Internet has information and gives the right direction, but some are "psychic"...haha.

In the "logout" part, I must open a Windows VM under Windows, because my ubuntu is under Windows. When I log out of my account, the server will also be shut down.

4. Install "packetbeat" and "win10pcap" encountered unable to install :

When I followed the steps on the Internet, I found that it could not be installed. Later I posted the error message to Google and found that it was a "security problem". The installation was forced by the command to succeed.

(> XXX -ExecutionPolicy UnRestricted -File ...)



```
系統管理員: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. 著作權所有，並保留一切權利。
請嘗試新的跨平台 PowerShell https://aka.ms/powershell

PS C:\Windows\system32> cd 'C:\Program Files\winlogbeat\'
PS C:\Program Files\winlogbeat> .\install-service-winlogbeat.ps1
.\install-service-winlogbeat.ps1 : 因為這個系統上已停用指令碼執行，所以無法載入 C:\Program Files\winlogbeat\install-ser
vice-winlogbeat.ps1 檔案。如需詳細資訊，請參閱 about_Execution_Policies，網址為 https://go.microsoft.com/fwlink/?LinkID=
135170。
位於 線路:1 字元:1
+ ~~~~~
+ .\install-service-winlogbeat.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\Program Files\winlogbeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

安全性警告
只執行您信任的指令碼。來自網際網路的指令碼雖然可能很有用，但是這個指令碼有可能會傷害您的電腦。若信任此指令碼，請使用
Unblock-File Cmdlet 來允許執行指令碼，而不顯示此警告訊息。您要執行 C:\Program
Files\winlogbeat\install-service-winlogbeat.ps1 嗎?
[D] 不要執行(D) [R] 執行一次(R) [S] 暫停(S) [?] 說明 (預設值為 "D"): r

Status Name DisplayName
-----
Stopped winlogbeat winlogbeat

PS C:\Program Files\winlogbeat>
```