Final Project

- Student Info
  1. Student ID: 310555024
  2. Student Name: 林廷翰

- Secenario

  Exposed RDP with weak password and Discovery

- Indicator of Compromise (IoC)
  1. Attacker’s IP address → `192.168.1.55`

     透過event.code - 4625，找到多筆由192.168.1.55嘗試登入失敗紀錄 (event.code - 4625其意義為failed to login)，故推測attacker’s IP address為192.168.1.55，嘗試使用的filter如下:

     

  2. Port of RDP Service → `3389`

     RDP預設的port為3389，嘗試利用192.168.1.55及3389作為關鍵字，得到多筆winlog.event_data.DestinationPort為3389的資料，filter如下:

     

  3. Command that execute for information discovery → `C:\WINDOWS\system32\cmd.exe /c ""C:\Users\victim\Desktop\discover.bat" “`

     先嘗試利用192.168.1.55搜索，在15:53:47 (RDP brute-forcing)後仍有多筆操作，故懷疑是在成功登入後進行的操作， 並發現這幾筆資料有一個共通性是winlog.event_data.CurrentDirectory皆為C:\Users\victim\Desktop\，再嘗試利用

C:\Users\victim\Desktop\作為關鍵字，找到一筆 winlog.event_data.TargetFilename為C:\Users\victim\Desktop\discover.bat，再嘗試使用dicover.bat作為關鍵字，找到一筆 winlog.event_data.ParentCommandLine為C:\WINDOWS\system32\cmd.exe /c ""C:\Users\victim\Desktop\discover.bat" “的資料。

- Detailed Timeline of the Attack
  1. Start/End timestamp of RDP brute-forcing.
     - Start Timestamp (serverTimestamp) → `Mar 31, 2022 15:50:52`
     - End Timestamp (serverTimestamp) → `Mar 31, 2022 15:53:47`

     透過4625 (event.code), 192.168.1.55 (attacker’s IP address)，可以找到 RDP brute-forcing開始和結束時間。
  2. Timestamp of login → `Mar 31, 2022 15:53:53`

     利用4624 (event.code)，其代表的意義為成功登入，並透過RDP brute-forcing結束及info discovery開始時間來夾擊出可能的login時間，fliter如下:

  3. Start/End timestamp of information discovery.
     - Start Timestamp (serverTimestamp) → `Mar 31, 2022 15:55:08`
     - End Timestamp (serverTimestamp) → `Mar 31, 2022 16:12:23`

     透過discover關鍵字搜索，共搜索到四筆資料，並得出開始及結束時間，filter如下：

- Possible Detection Method
  1. Your detection method

我的detection method是基於用戶多次嘗試登入且登入失敗的audit log。正常來說，如果是正常使用者，不會有非常多次嘗試登入但皆登入失敗的狀況。

2. Which system/network behavior implies the attack

   利用event.code - 4625作為關鍵字過濾audit log，原因是4625即代表failed to login，符合我們的detection method。

3. Which normal (benign) usage leads to false positives in your method

   如果其為正常用戶，但真的忘記密碼，導致多次輸入錯誤密碼，衍生出一堆event.code為4625的audit code，可能造成錯誤判斷。

4. Proof of Concept (PoC) of your detection method

   從此次的project，我們可以得到，如果在短時間內，多次嘗試且失敗， 很可能即為RDP brute-forcing，原因次一般人無法在短時間內做多筆密碼登入嘗試，這不符合實際場景。

- Feedback

  此次project其實還滿有趣的，後來發現final project的三個場景應該是互相連貫，而非各自獨立。因此從一開始的phishing到中間的RDP brute-forcing, discover到最後的file collection和exfiltration，這是三個連續的攻擊，了解到攻擊可能是多個不同攻擊的組合。

  從過濾log的過程學習到很多，除了熟悉woodpecker平台的操作，也了解到每筆log的property代表的意義，並透過不同的filter來過濾出我們想要的資料，思考其背後代表的意義。

  Spec和PPT也寫得很清楚，PTT中的提示也相當有用，可以在一開始比較沒有頭緒時有一個比較正確的開始方向。