

### Q1. 問卷填寫(一)

問題描述:

請填寫問卷，貼上完成截圖上傳至 Zuvio 小考三 – Q1

問卷連結:

[https://docs.google.com/forms/d/e/1FAIpQLSfMuvo-5J\\_FLQblba0g72Pn3dvrkRj4-8NS4Rwo4Qbucm6NyQ/viewform?usp=sf\\_link](https://docs.google.com/forms/d/e/1FAIpQLSfMuvo-5J_FLQblba0g72Pn3dvrkRj4-8NS4Rwo4Qbucm6NyQ/viewform?usp=sf_link)

### Q2. 問卷填寫(二)

問題描述:

請填寫問卷，完成後拍照上傳至 Zuvio 小考三 – Q2

### Q3. Client/Server 日期

檢查方式:

請撰寫程式完成題目要求，並在檢查時解釋程式邏輯與展示程式輸出

問題描述:

使用 2 台虛擬機(或一台虛擬機，兩個 Terminal)，1 個 Server，1 個 Client; Client 向 Server 詢問現在日期，由助教檢查完成後，將程式碼上傳至 Zuvio 小考三 – Q3。

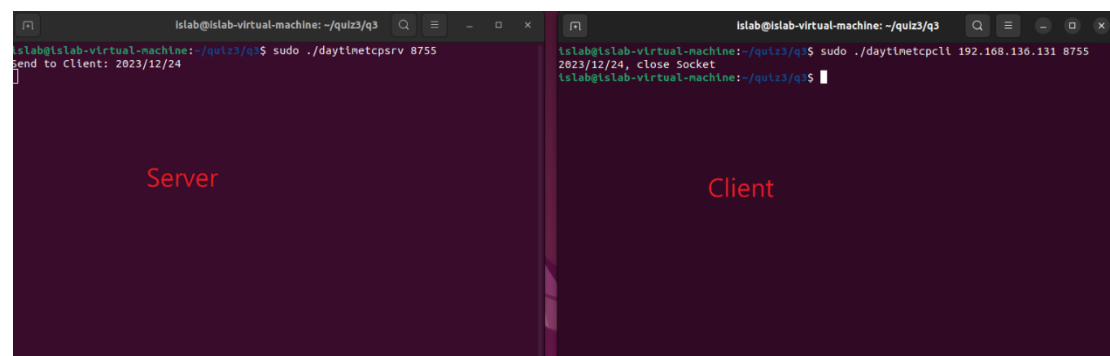
(1) 執行 server 時，須加上 port 號碼作為參數。

(2) 執行 client 時，須加上 server 的 ip 和 port 號碼作為參數。

(3) Server 收到 client 請求，輸出"Send To Client: 西元年/月/日"，並傳"西元年/月/日"給 Client。

(4) Client 收到 Server 傳送的字串後，將其輸出

預期結果:



The screenshot shows two terminal windows side-by-side. The left window is titled 'Server' and shows the command `sudo ./daytinetpsrv 8755` being executed. The output is `Send to Client: 2023/12/24`. The right window is titled 'Client' and shows the command `sudo ./daytinetpccli 192.168.136.131 8755` being executed. The output is `2023/12/24, close Socket`.

### Q4. Client/Server UDP 傳送檔案

檢查方式:

請撰寫程式完成題目要求，並在檢查時解釋程式邏輯與展示程式輸出

問題描述:

使用 2 台虛擬機(或一台虛擬機，兩個 Terminal)，1 個 Server，1 個 Client;

以 UDP 協定傳一張 png 圖片，Server 送圖檔，Client 接收、顯示，檔名由 Server 端執行時輸入，每次傳送 255 Bytes，由助教檢查完成後，將程式碼上傳至 Zuvio 小考三 – Q4。

(1) 執行 server 時，須加上 port 號碼作為參數。

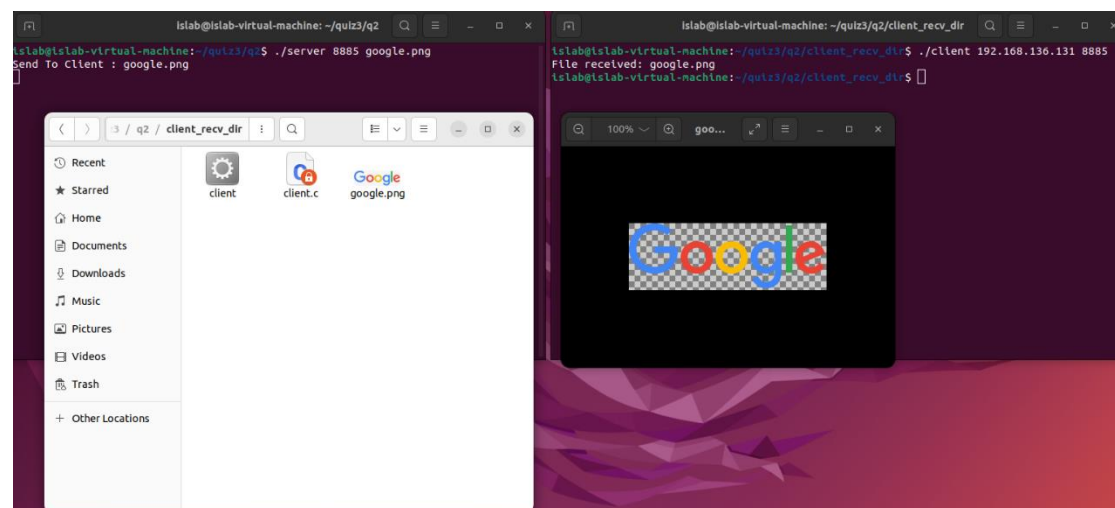
(2) 執行 client 時，須加上 server 的 ip 和 port 號碼作為參數。

(3) Server 收到 client 請求，輸出"Send To Client: +圖片名稱"，並傳圖片檔案給 Client。

(4) Client 收到 Server 傳送的圖片檔案後，將其輸出"File received: +圖片名稱" 圖片網址：

[https://www.google.com.tw/images/branding/googlelogo/1x/googlelogo\\_color\\_272x92dp.png](https://www.google.com.tw/images/branding/googlelogo/1x/googlelogo_color_272x92dp.png)

預期結果：



## Q5. Client/Server Socket 對話

檢查方式：

請撰寫程式完成題目要求，並在檢查時解釋程式邏輯與展示程式輸出

問題描述：

使用 2 台虛擬機(或一台虛擬機，兩個 Terminal)，1 個 Server，1 個 Client; 製作 Client/Server 的 Socket 對話程式，由助教檢查完成後，將程式碼上傳至 Zuvio 小考三 – Q5。

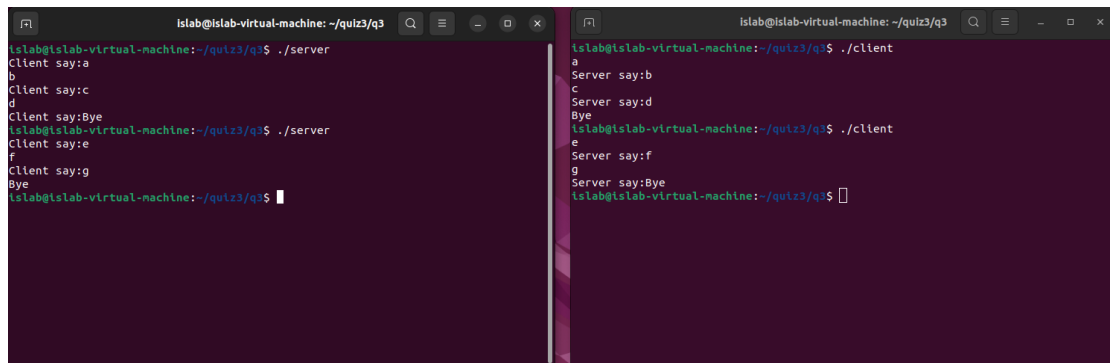
執行順序：

1. client 端使用者輸入資料,傳送到 Server 端。
2. Server 端使用者輸入資料,傳送到 Client 端。
3. client 端使用者輸入資料,傳送到 Server 端。
4. Server 端使用者輸入資料,傳送到 Client 端。

...

Client 或 Server 端,使用者輸入 'Bye'結束。

預期結果:



```
islab@islab-virtual-machine: ~/quiz3/q3
islab@islab-virtual-machine:~/quiz3/q3$ ./server
client say:a
b
client say:c
d
client say:Bye
islab@islab-virtual-machine:~/quiz3/q3$ ./server
client say:e
f
client say:g
Bye
islab@islab-virtual-machine:~/quiz3/q3$

islab@islab-virtual-machine: ~/quiz3/q3
islab@islab-virtual-machine:~/quiz3/q3$ ./client
a
Server say:b
c
Server say:d
Bye
islab@islab-virtual-machine:~/quiz3/q3$ ./client
e
Server say:f
g
Server say:Bye
islab@islab-virtual-machine:~/quiz3/q3$
```

## Q6. DVWA SQL Injection

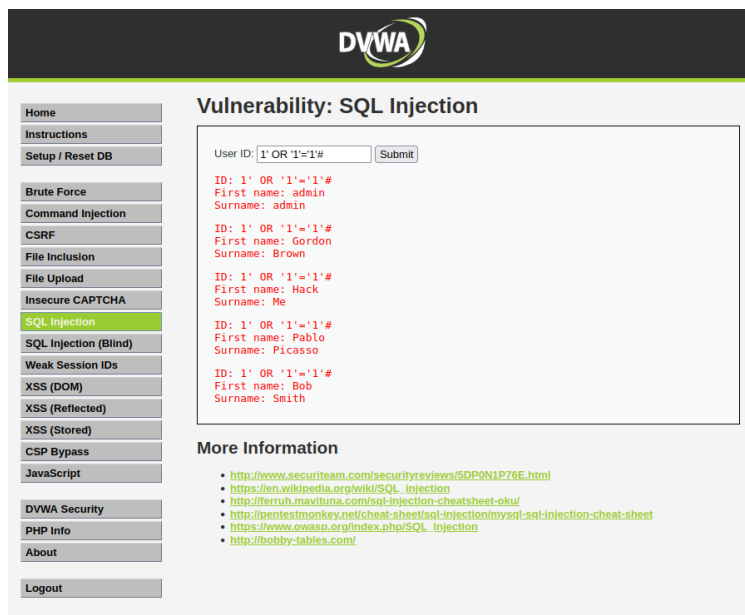
檢查方式:

請開啟 DVWA 畫面，並在 SQL Injection 執行顯示指令後的結果

問題描述:

請使用 DVWA 虛擬機，將 DVWA 啟動後並設定 DVWA Security 為 low，並進入到 SQL Injection 畫面，使用以下指令: `1' OR '1'='1'#`，執行後會顯示使用者 ID、First name、Surname，由助教檢查完成後，將執行結果截圖後上傳至 Zuvio 小考三 – Q6。

預期結果:



## Q7. DVWA Command Injection

檢查方式:

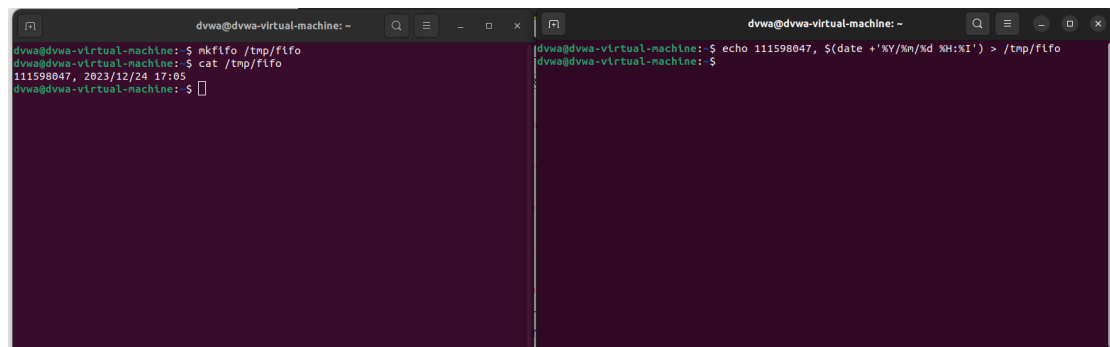
請開啟 DVWA 畫面，並在 terminal 上顯示執行結果

問題描述:

請使用 DVWA 虛擬機，並開啟兩個 terminal，一個 terminal 用於建立 FIFO

管道，另一個 terminal 則輸入訊息到管道，輸出訊息為：你的學號 + YYYY/mm/dd H:I，YYYY/mm/dd H:I 為當天執行日期和時間，Y 為西元年、M 為月份、D 為日期、H 為小時、I 為分鐘，由助教檢查完成後，將兩個 terminal 畫面截圖上傳至 Zuvio 小考三 – Q7。

預期結果:



```
dvwa@dvwa-virtual-machine: ~  
dvwa@dvwa-virtual-machine: $ mkfifo /tmp/fifo  
dvwa@dvwa-virtual-machine: $ cat /tmp/fifo  
111598047, 2023/12/24 17:05  
dvwa@dvwa-virtual-machine: $  
  
dvwa@dvwa-virtual-machine: ~  
dvwa@dvwa-virtual-machine: $ echo 111598047, $(date +%Y/%m/%d %H:%I) > /tmp/fifo  
dvwa@dvwa-virtual-machine: $
```

## Q8. 使用 MICROSOFT THREAT MODELING TOOL 建立威脅模型

### (1) 建立 Data Flow Diagram

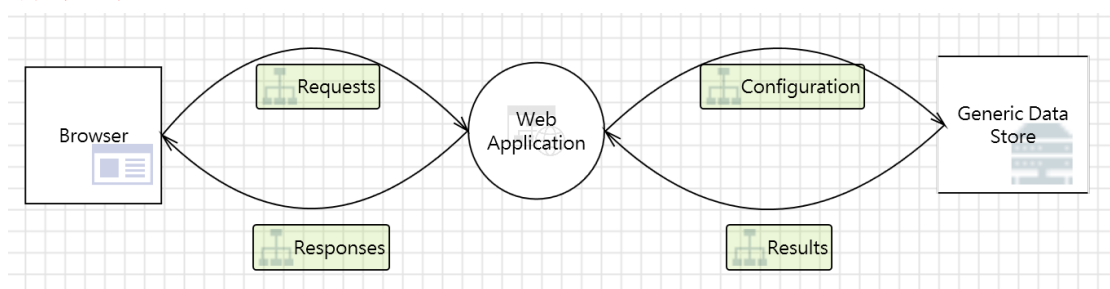
檢查方式:

請完成威脅建模並且符合題目要求

問題描述:

請繪製一個 DFD，威脅模型元素包含 Browser、Web Application、Generic Data Store，並完成資料流的繪製，Browser 與 Web Application 會有 Requests 與 Responses 資料流，而 Web Application 與 Generic Data Store 會有 Configuration 與 Results 資料流，由助教檢查完成後，將 DFD 截圖上傳至 Zuvio 小考三 – Q8-1。

預期結果:



### (2) 完成信任邊界繪製和威脅評估分析

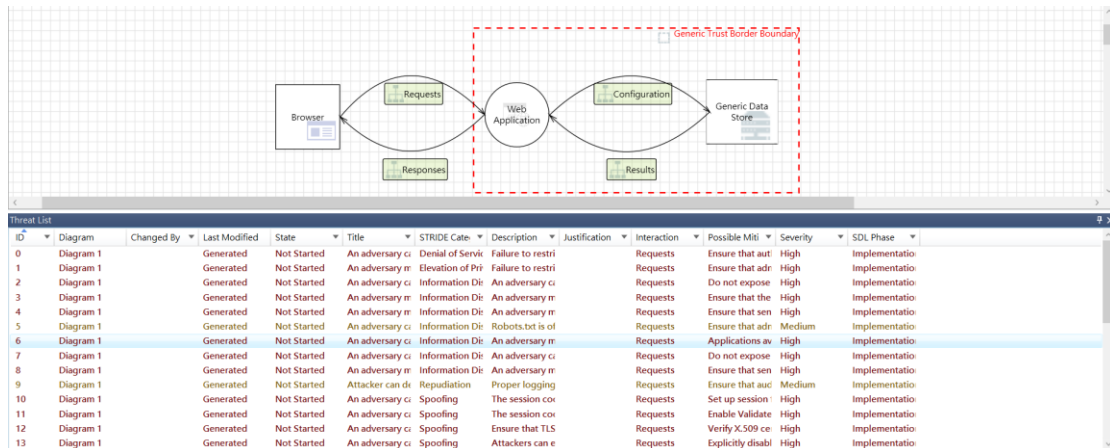
檢查方式:

請完成威脅建模並且符合題目要求

問題描述:

接續(1)，在 DFD 上繪製信任邊界，並且執行威脅評估分析，由助教檢查完成後，將完成信任邊界繪製的 DFD 以及威脅清單畫面截圖上傳至 Zuvio 小考三 – Q8-2。

預期結果:



## Q9. Cuckoo Sandbox Analysis

### (1) Summary report

檢查方式:

請完成 Cuckoo 沙箱的惡意軟體行為分析

問題描述:

請參考惡意軟體行為偵測系統講義，並針對以下檔案連結中的惡意軟體進行惡意軟體行為分析，由助教檢查完成後，惡意軟體行為分析結果截圖上傳至 Zuvio 小考三 – Q9-1。

惡意軟體連結:

[https://drive.google.com/file/d/1SIJVS5bj0Pi\\_7EIyXyMszRVH8c08lNWh/view?usp=drive\\_link](https://drive.google.com/file/d/1SIJVS5bj0Pi_7EIyXyMszRVH8c08lNWh/view?usp=drive_link)

q9.zip 解壓縮密碼: q9

預期結果:

### Summary

File `f71db7e25e720622d7c160761f5c50f72a0c57cd2e87646318df24b368ac1612.e1f`

Summary	Download	Resubmit sample
Size	18.4MB	
Type	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, stripped	
MD5	633d241a171897adbdc737400fb998d7	
SHA1	5a25449709869ef3de55c7a68aed4a23cdf7b01c	
SHA256	f71db7e25e720622d7c160761f5c50f72a0c57cd2e87646318df24b368ac1612	
SHA512	<a href="#">Show SHA512</a>	
CRC32	9EF6584F	
ssdeep	None	
Yara	• vmdetect - Possibly employs anti-virtualization techniques	

#### Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	Dec. 24, 2023, 2:52 a.m.	Dec. 24, 2023, 2:54 a.m.	93 seconds	none	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

#### Signatures

No signatures

### Score

This file appears fairly benign with a score of 0.0 out of 10.

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

### Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

## (2) Behavioral Analysis report

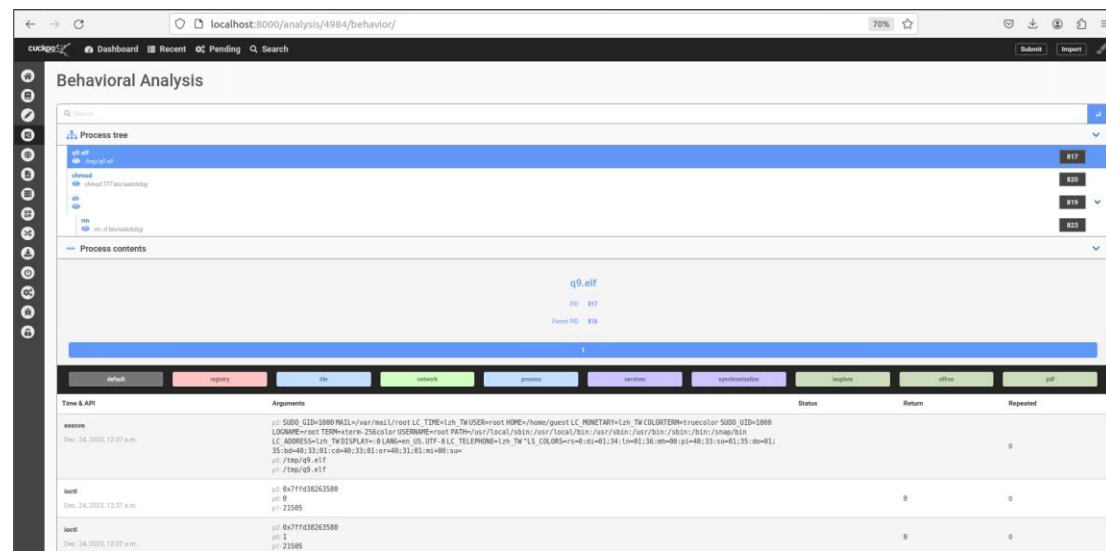
檢查方式:

請完成 Cuckoo 沙箱惡意軟體行為分析並取得惡意軟體行為分析報告

問題描述:

接續(1)，查看 Cuckoo 沙箱分析惡意軟體是否有產出惡意軟體行為分析報告，惡意軟體行為分析報告需含有 Process tree 和 Process contents，由助教檢查完成後，惡意軟體行為分析報告截圖上傳至 Zuvio 小考三 – Q9-2。

預期結果:



## Q10. 惡意軟體行為偵測系統

### (1) 惡意軟體行為偵測系統的技術偵測結果

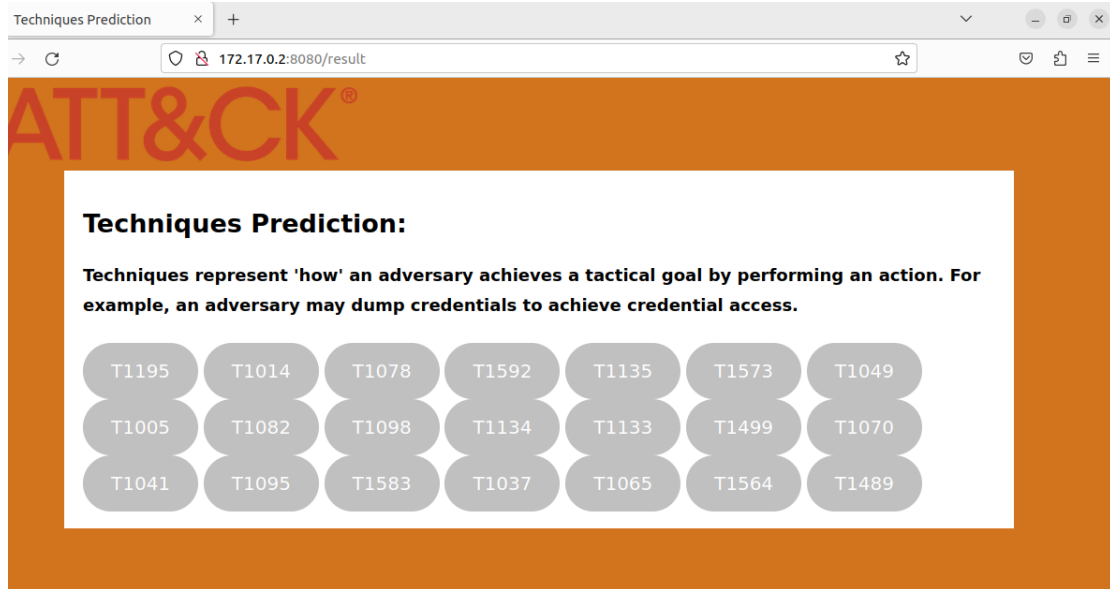
檢查方式:

請完成惡意軟體行為偵測系統對 Cuckoo 沙箱惡意軟體行為分析報告的惡意軟體行為技術偵測的結果

問題描述:

請參考惡意軟體行為偵測系統講義，並使用 Q9 透過 Cuckoo 沙箱所取得的惡意軟體行為分析報告，透過惡意軟體行為偵測系統進行進一步分析惡意軟體行為，並取得惡意軟體行為技術偵測的結果，由助教檢查完成後，惡意軟體行為技術偵測的結果截圖上傳至 Zuvio 小考三 – Q10-1。

預期結果:



## (2) MIRTE ATT&CK 技術偵測的結果說明

檢查方式:

請完成惡意軟體行為偵測系統的惡意軟體行為技術偵測的結果說明

問題描述:

接續(1)，至 MIRTE ATT&CK 網站查看每個偵測的技術，並寫下技術的詳細說明，將每個偵測的技術詳細說明上傳至 Zuvio 小考三 – Q10-2。

**預期結果:**

T1027 為混淆文件與訊息,這個技術描述攻擊者可能嘗試透過加密、編碼或以其他方式混淆系統上可執行檔案的內容,使可執行檔難以被發現或分析。