111學年度大學部專題競賽

輔助滲透測試半自動化工具

歐家秀 108062338
徐　祈 108000232
梁家燕 108062337
莊晴雯 108062281
林妍廷 108060017

CONTENT

PART 1

滲透測試介紹

滲透測試介紹

偵查目標，並以駭客思維嘗試攻破受害者系統，進行漏洞利用，評估系統結構與安全性，最後進行回報與修補。

修補

偵查

漏洞利用

PART 2

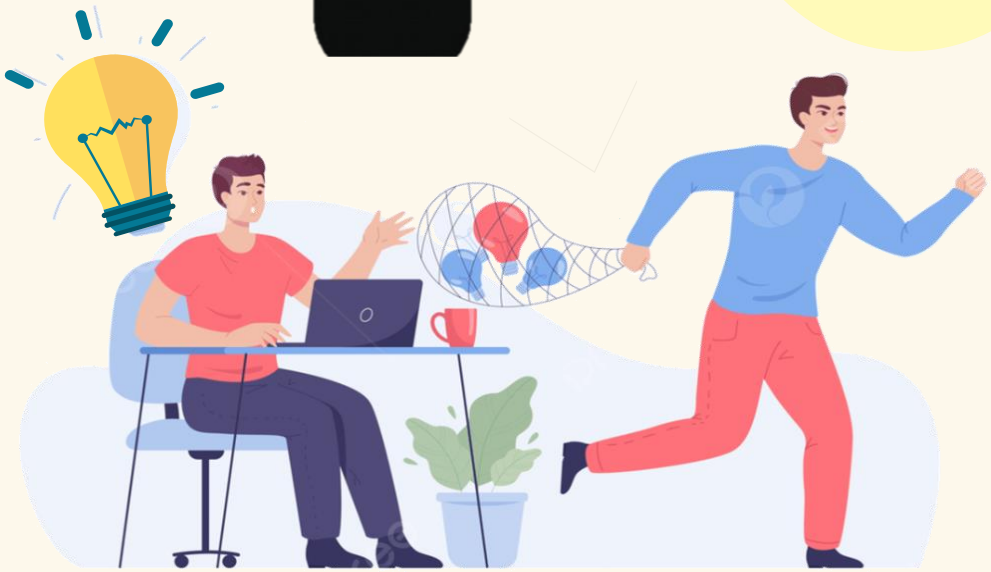
研究動機與目的

研究動機與目的

Q 一間滲透測試公司，老手辭職後，造成新人技術經驗銜接困難

Goal

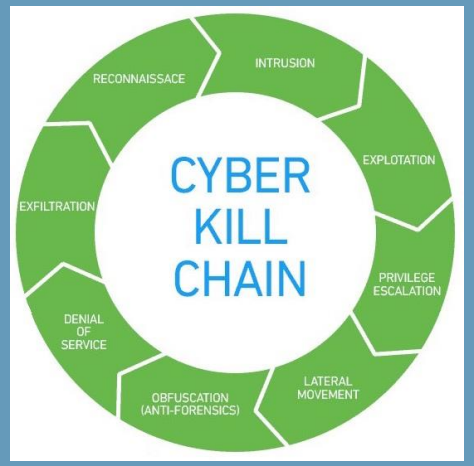
用工具儲存滲透測試步驟，並讓部分步驟自動執行。



PART 3

相關研究概況

相關研究概況



可將網路攻擊和防禦分解成易於解釋的階段和模式。

Cyber-Kill Chain

基於真實情境的敵方戰術和技術知識庫，提出更詳細、統一的分類標準。

ATT&CK

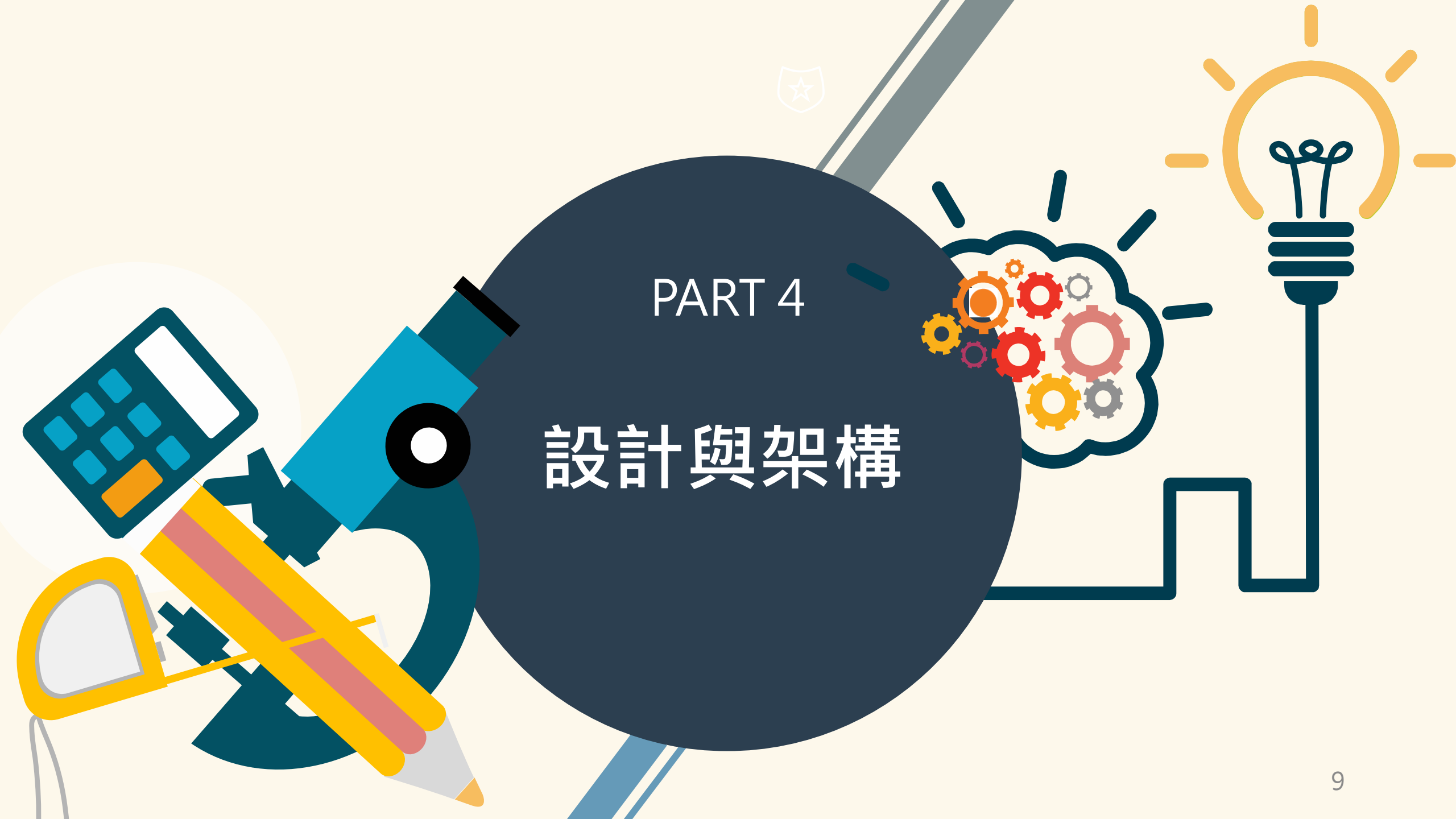
Automated
Attack Path
Planning
and Validation

根據目標確定一組序列簡化攻擊流程。需手動輸入網路設備拓譜xml檔，不實用。

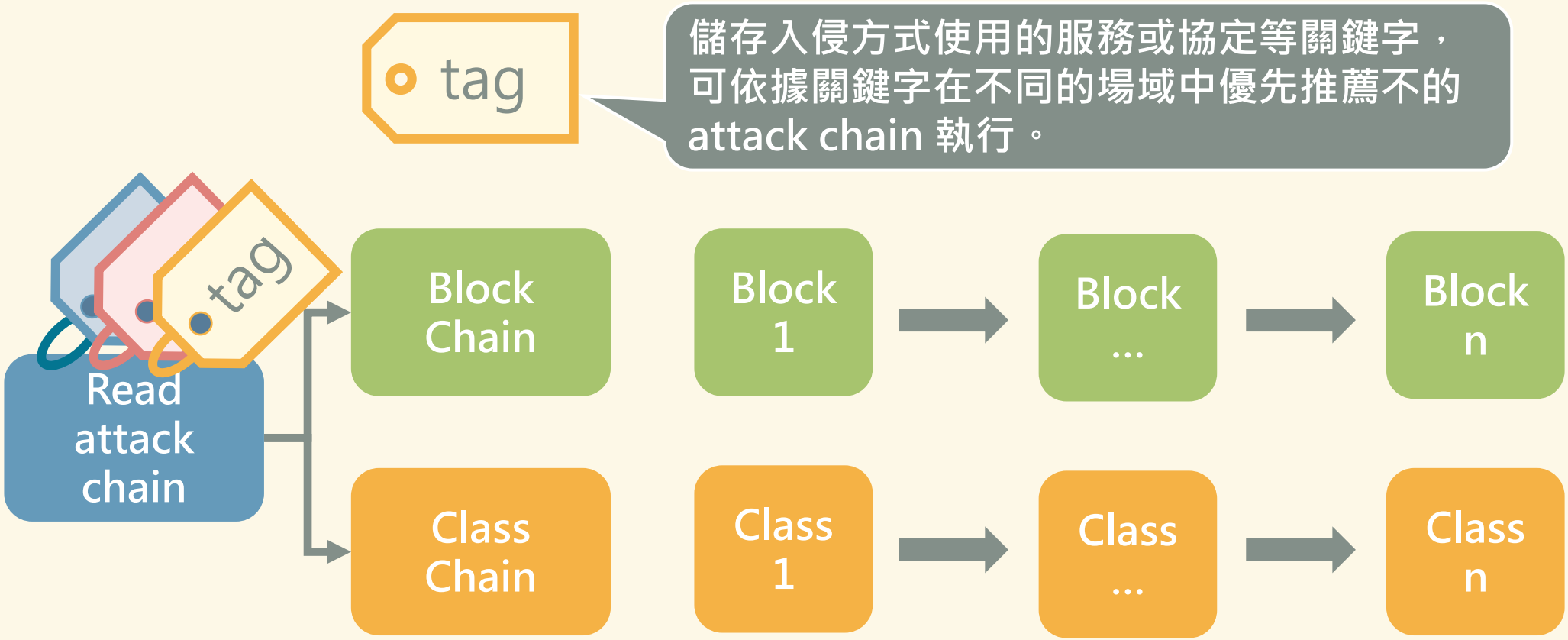
A2P2V

PART 4

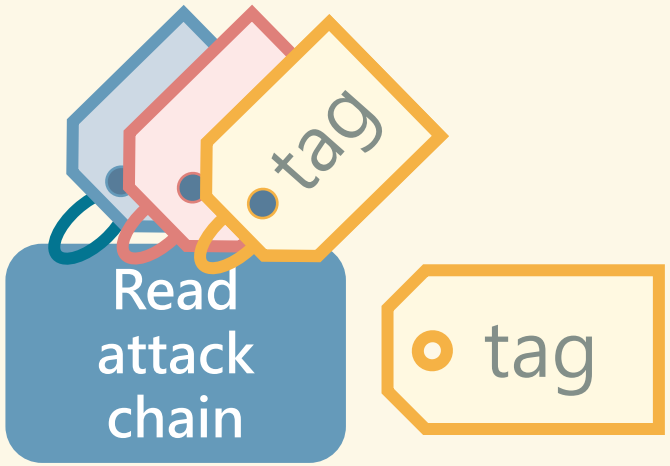
設計與架構



設計與架構


tag
儲存入侵方式使用的服務或協定等關鍵字，可依據關鍵字在不同的場域中優先推薦不的attack chain 執行。
tag
Read attack chain
Block Chain
Block 1
Block ...
Block n
Class Chain
Class 1
Class ...
Class n

設計與架構

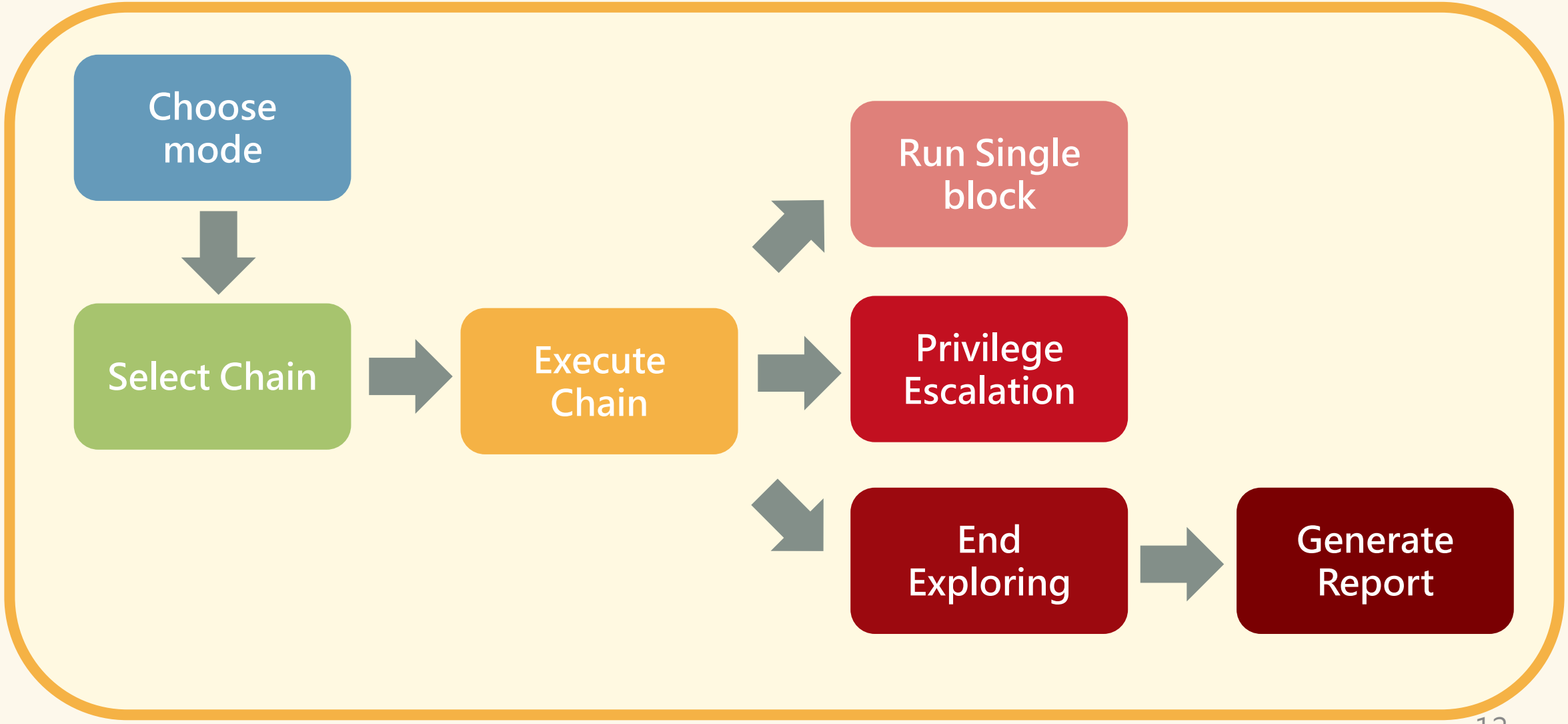



```
Show suggested chain(1) or manually choose from all chains(2)?
1
your condition:
Service: ['http', 'https']
OS: None
Port: ['80', '443']
Apache: None
attack chain couch.yml 's tag: None
attack chain pentest.yml 's tag: {'PT': ['01', '02', '04']}
attack chain erlik.yml 's tag: None
attack chain anonforce.yml 's tag: {'Service': ['ftp'], 'PT': ['02', '03', '04', '13']}
attack chain agentT.yml 's tag: {'Port': ['80'], 'PT': ['01', '07']}
attack chain Gallery.yml 's tag: {'PT': ['01', '08']}
attack chain AC_test.yml 's tag: None
attack chain manipulation.yml 's tag: {'PT': ['01', '02', '04']}
attack chain poster.yml 's tag: {'Service': ['postgresql'], 'PT': ['03', '04', '05']}
attack chain annoymous.yml 's tag: {'Service': ['ftp'], 'PT': ['05', '10', '13']}
attack chain annie.yml 's tag: {'PT': ['01', '05']}
attack chain brooklyn99.yml 's tag: {'Service': ['ftp'], 'PT': ['03', '04', '05', '13']}
attack chain tomghost.yml 's tag: {'Service': ['ajp13'], 'PT': ['01', '05', '08']}
attack chain thecodcaper.yml 's tag: {'PT': ['02']}
attack chain rootme.yml 's tag: {'PT': ['05', '08', '13']}
attack chain pentest_with_polaris.yml 's tag: {'PT': ['01', '02', '04']}
attack chain revenge.yml 's tag: {'Service': ['http'], 'PT': ['01', '03', '04', '05']}

suggested chains:

['agentT.yml', 'revenge.yml']
```

設計與架構


Choose mode
Select Chain
Execute Chain
Run Single block
Privilege Escalation
End Exploring
Generate Report

設計與架構

Choose mode

Select Chain

```
Choose the mode.
1: a specific target was known.
2: search for a target!
3: modify attack chain (create a rule)
4: insert an existing block.
Mode: 1
Which host you want to explore? (ex: 99.83.179.177)
99.83.179.177
Input target url(ex: https://hackmd.io/):
https://hackmd.io/
START EXPLORING!
```

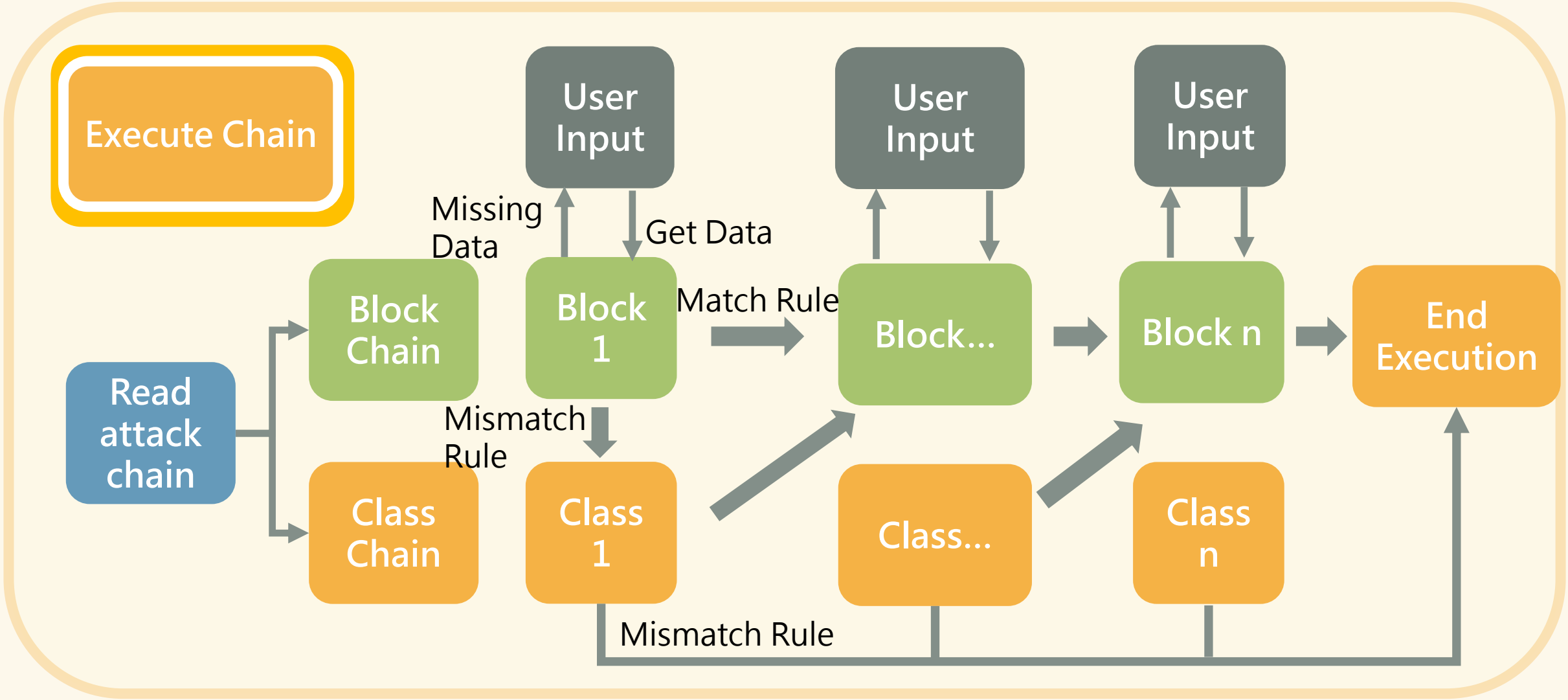
設計與架構

Choose mode

Select Chain

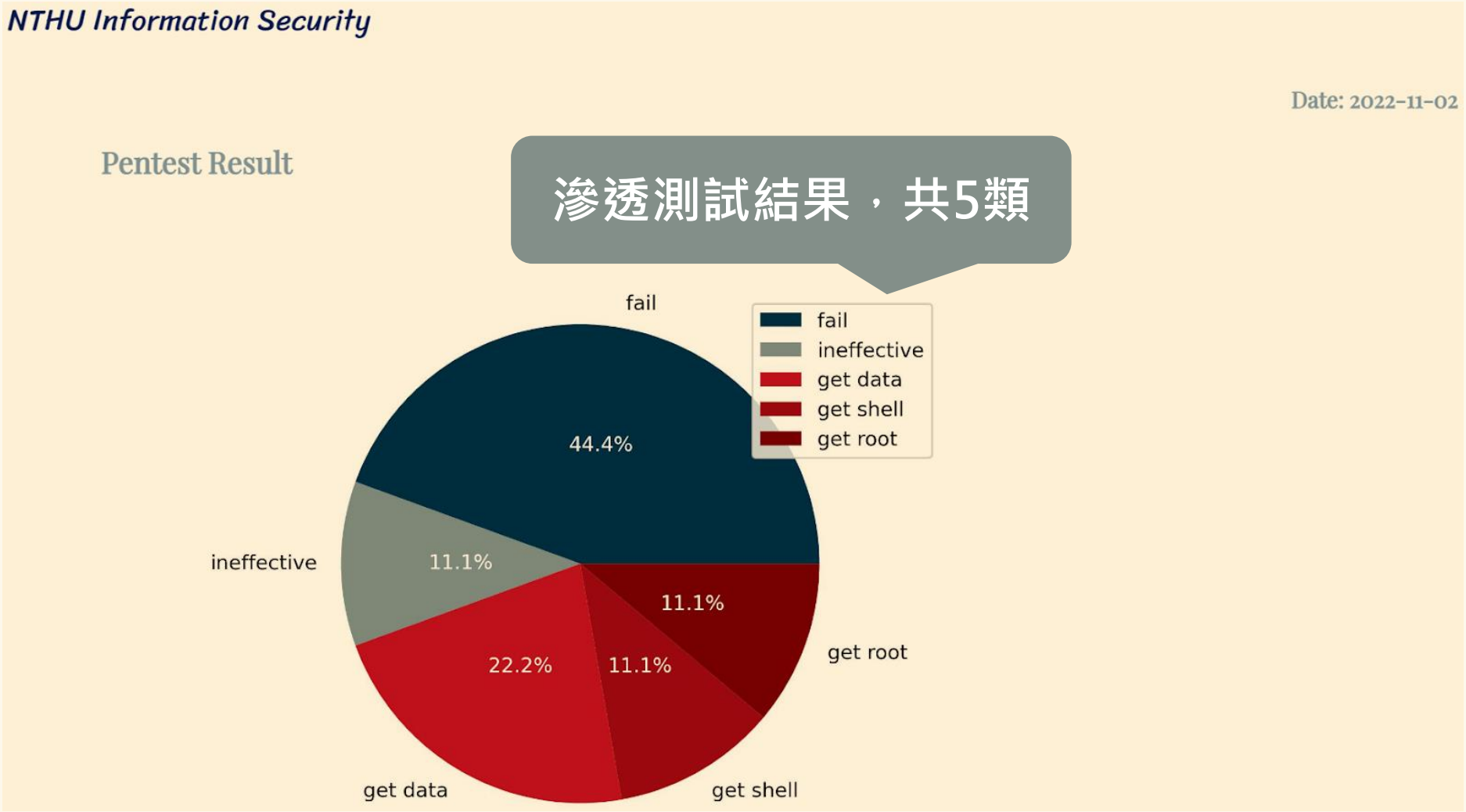
```
Show suggested chain(1) or manually choose from all chains(2)?
2
type `viewall` to show all attack chains
type `checkout <chain_name>` to see the detail of a specific chain, chain_name includes '.yml'
type `search <feature> <value>` to search for attack chain
type `add <chain_name>` to add the chain to selected chain list, chain_name includes '.yml'
or `add <atk_chain_number>` to add the chain to selected chain list
If choose more than one chains, seperate it with space.
(ex. add 1 2 5)
type `rm <chain_name>` to remove the chain from selected chain list, chain_name includes '.yml'
type `end` to end modifying selected chain list
Choose the attack chain you want to use from the following table.
================================
0: couch.yml
1: pentest.yml
2: erlik.yml
3: anonforce.yml
4: agentT.yml
5: Gallery.yml
6: AC_test.yml
7: manipulation.yml
8: poster.yml
9: annoymous.yml
10: annie.yml
11: brooklyn99.yml
12: tomghost.yml
13: thecodcaper.yml
14: rootme.yml
15: pentest_with_polaris.yml
16: revenge.yml
================================
```

設計與架構


Execute Chain
User Input
User Input
User Input
Missing Data
Get Data
Block Chain
Block 1
Match Rule
Block...
Block n
End Execution
Read attack chain
Mismatch Rule
Class Chain
Class 1
Class...
Class n
Mismatch Rule


PART 5
成果展示

成果展示


NTHU Information Security
Date: 2022-11-02
Pentest Result
滲透測試結果，共5類
fail
ineffective
get data
get shell
get root
44.4%
11.1%
11.1%
22.2%
11.1%

成果展示

Target Host Information

IP: 10.10.110.108

URL: http://10.10.110.108/

Service: ftp, ssh

OS: None

Port: 21, 22

Apache: None

滲透測試目標資訊

成果展示

Attack Chain Overview

攻擊鍊名稱

物聯網評估指引中的滲透測試(PT)種類

chain name	tags	result
anonforce.yml	#ftp #PT02 #PT03 #PT04 #PT13	get root
brooklyn99.yml	#ftp #PT03 #PT04 #PT05 #PT13	fail
agentT.yml	#Port80 #PT01 #PT07	get data
postgres_login.yml		fail
ftp_find_sh.yml		fail
smbclient.yml		fail
nmap_sC_sV.yml		get data
pwntools.yml		ineffective
crack_hash_by_john.yml		get shell

成果展示

紅色：攻擊鍊執行成功

灰色：攻擊鍊執行失敗

PART 6

結論

結論

開發成果

- 工具可串聯 Kali Linux內建工具
- 可讓使用者探索網域
- 用 Generator function 方便使用者新增攻擊鏈
- 自動執行指令或給予提示的方式輔助滲透測試
- 提供報告給使用者評估成果

未來展望

- 成為開源專案，開放更多使用者貢獻攻擊鏈
- 幫助初入滲透測試技術的新手，能有更多參考資源。

PART 7

Q & A