111學年度大學部專題競賽

Semi-Automated Auxiliary Penetration Testing Tool

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

CONTENT

01 Introduction to Penetration Testing

02 Research Motivation and Objectives

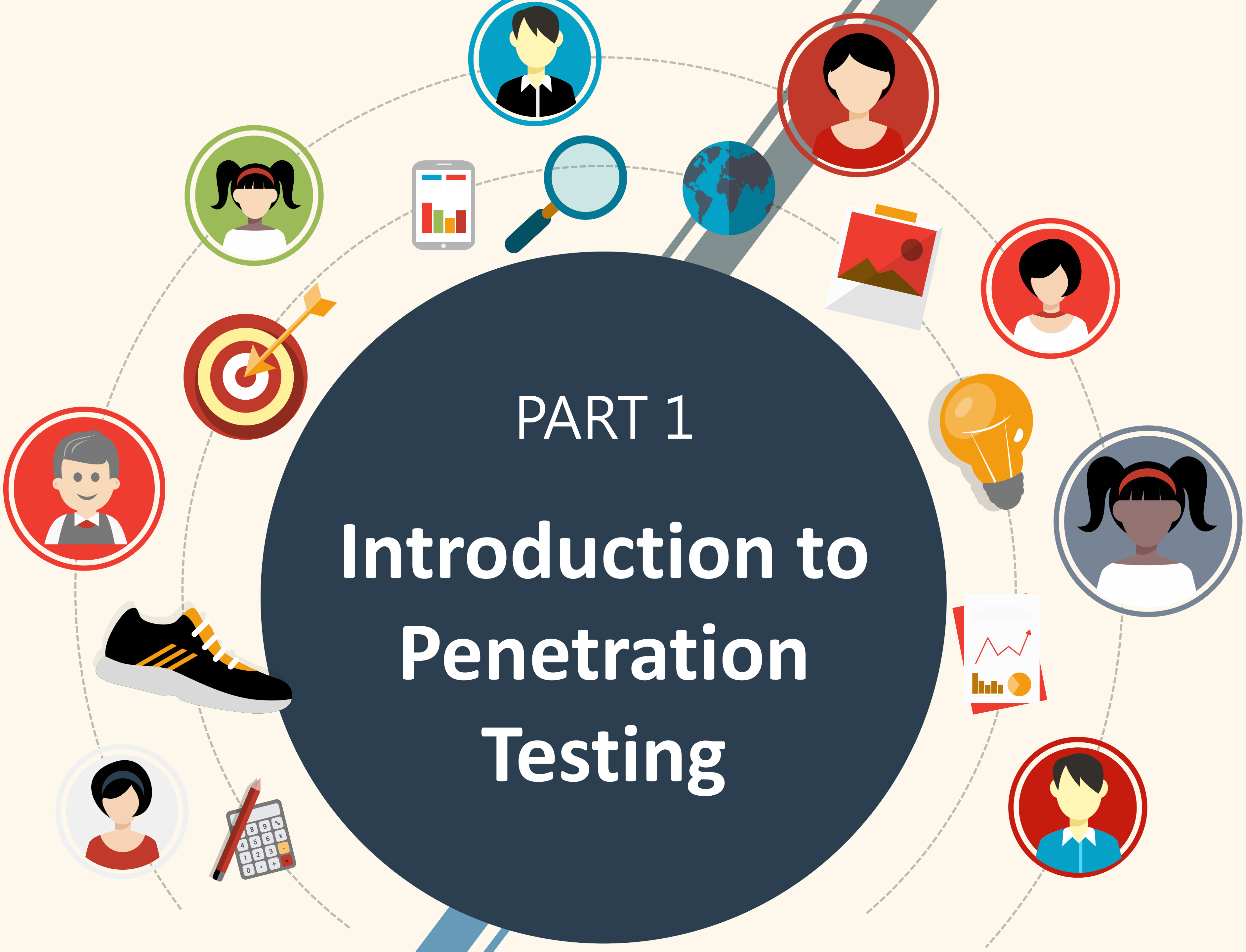
03 Overview of Related Research

04 Design and Architecture

05 Results

06 Conclusion

07 Q&A

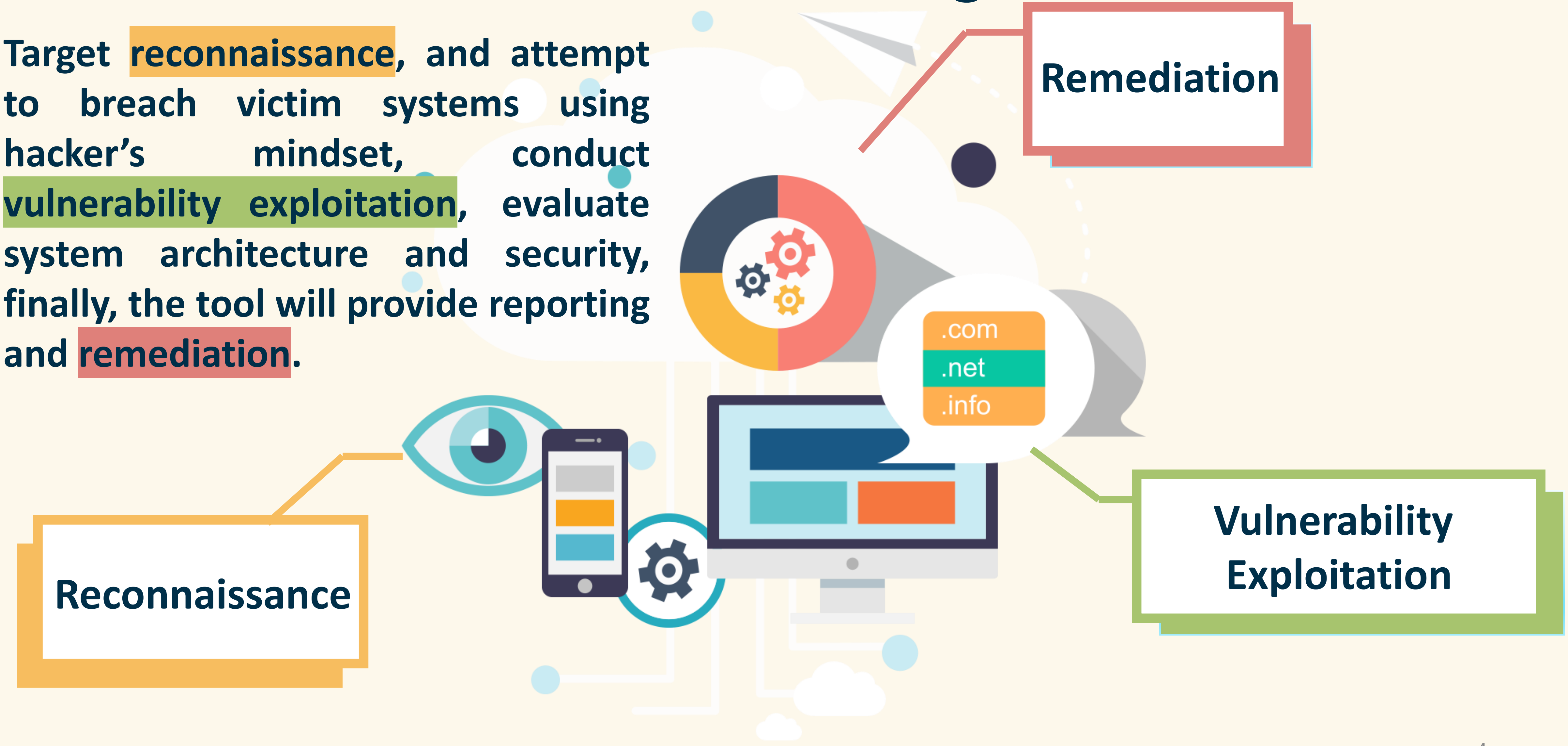


PART 1

Introduction to Penetration Testing

Introduction to Penetration Testing

Target reconnaissance, and attempt to breach victim systems using hacker's mindset, conduct vulnerability exploitation, evaluate system architecture and security, finally, the tool will provide reporting and remediation.



PART 2

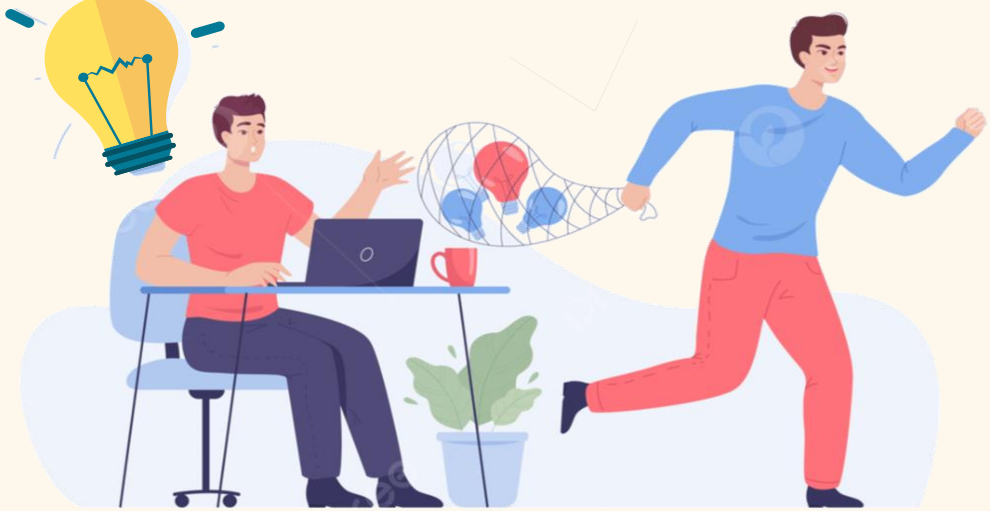
Research Motivation and Objectives

Research Motivation and Objectives

Q After an experienced penetration testing employee resigned from a company, it caused difficulties in bridging the gap for new employees' technical experience.

Goal

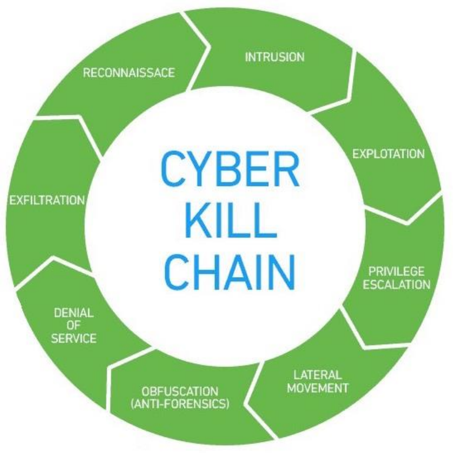
Store penetration testing steps in tools and automate some steps to be executed automatically.



PART 3

Overview of Related Research

Overview of Related Research



Decompose network attacks and defenses into easily explainable stages and patterns.

Cyber-Kill Chain

ATT&CK™

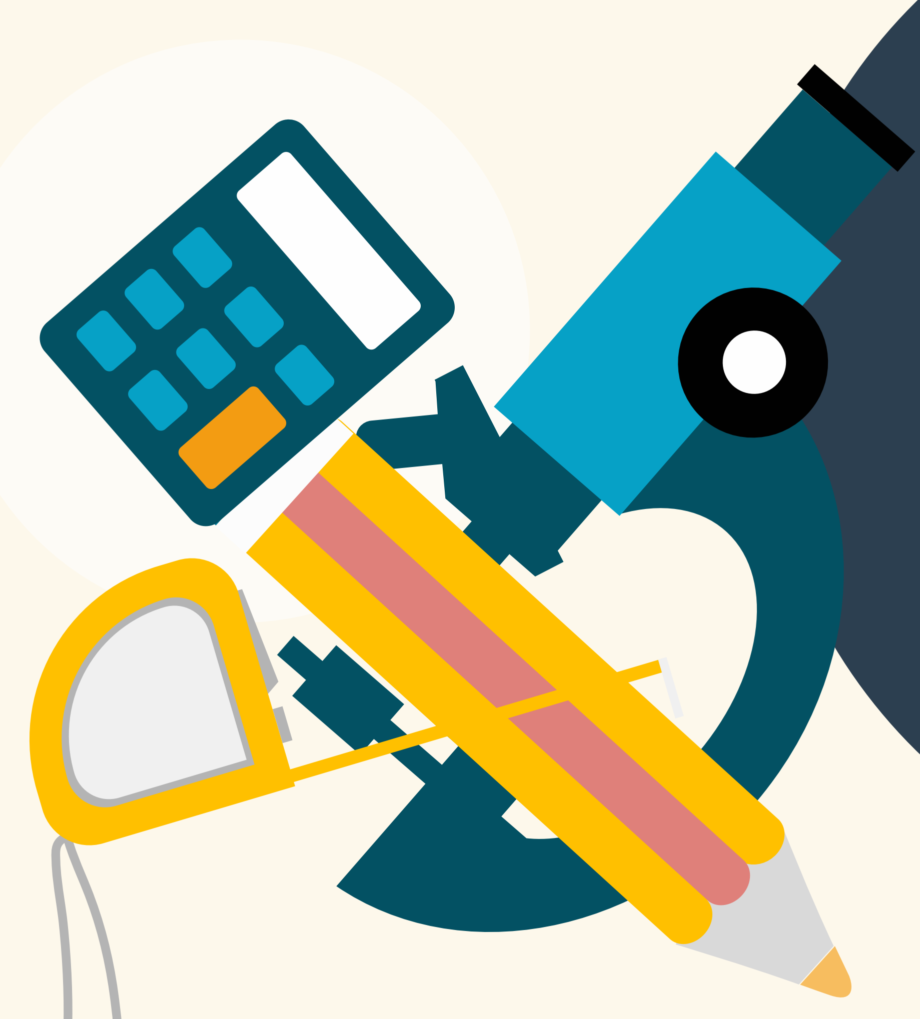
Based on real-world scenarios, propose more detailed and unified classification standards for enemy tactics and technical knowledge base.

ATT&CK

Automated
Attack **P**ath
Planning
and **V**alidation

Determine a sequence to simplify the attack process based on the target. However, it is not practical as it requires manual input of network device topology in XML format.

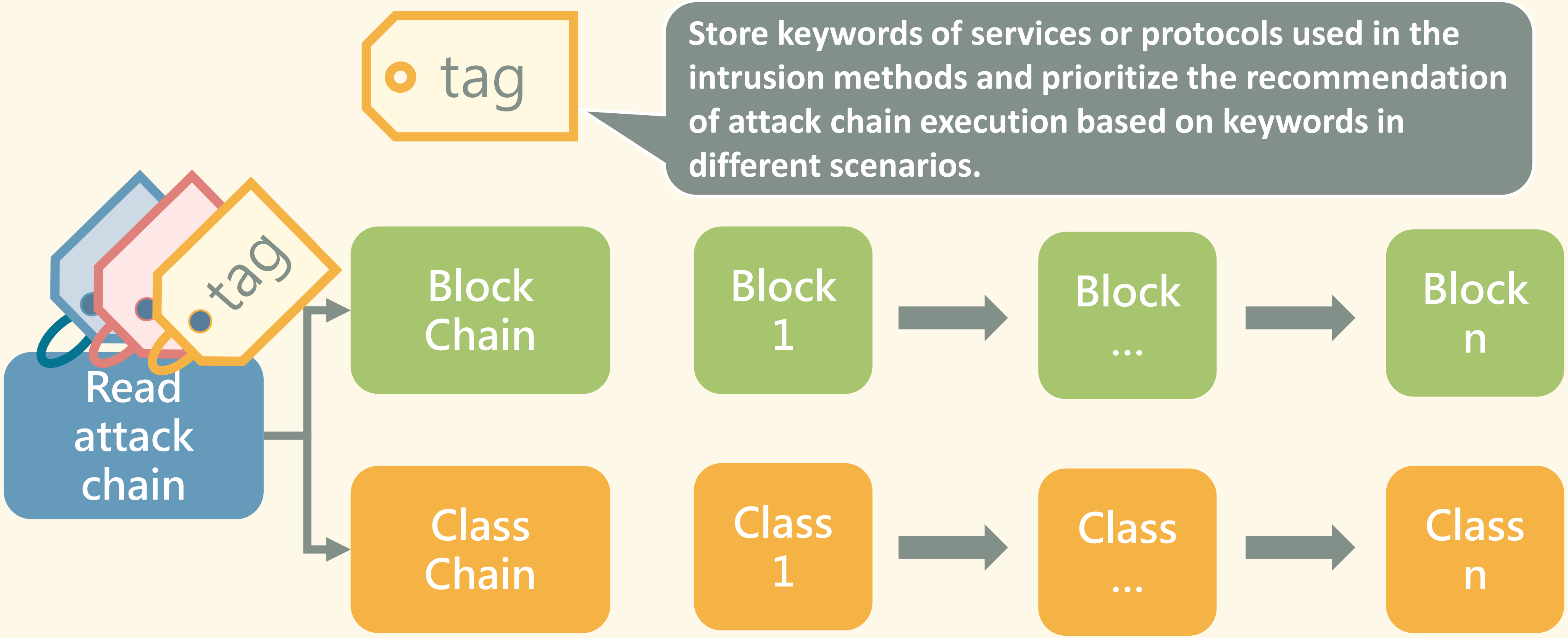
A2P2V



PART 4

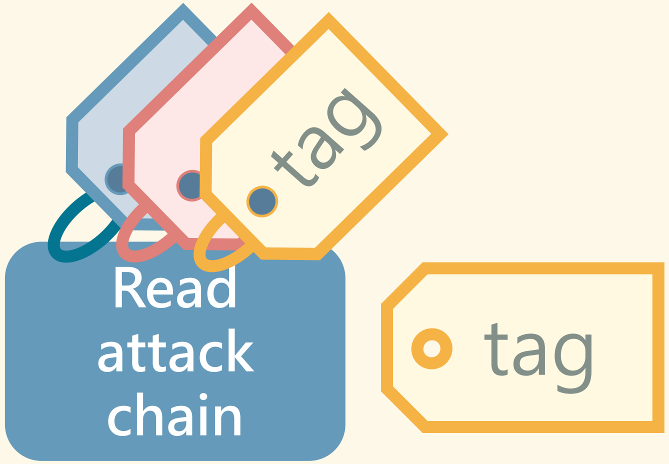
Design and Architecture

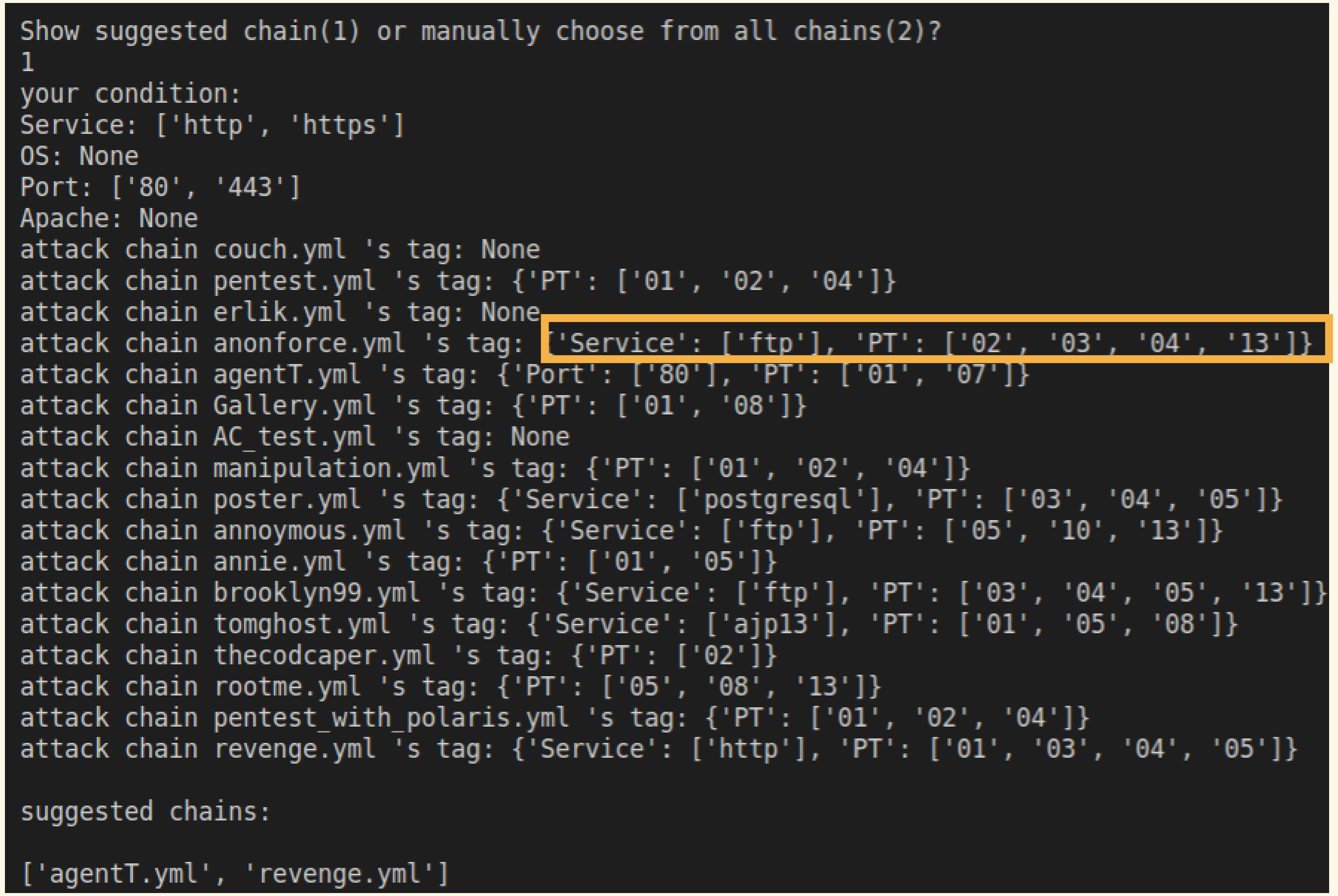
Design and Architecture



Store keywords of services or protocols used in the intrusion methods and prioritize the recommendation of attack chain execution based on keywords in different scenarios.

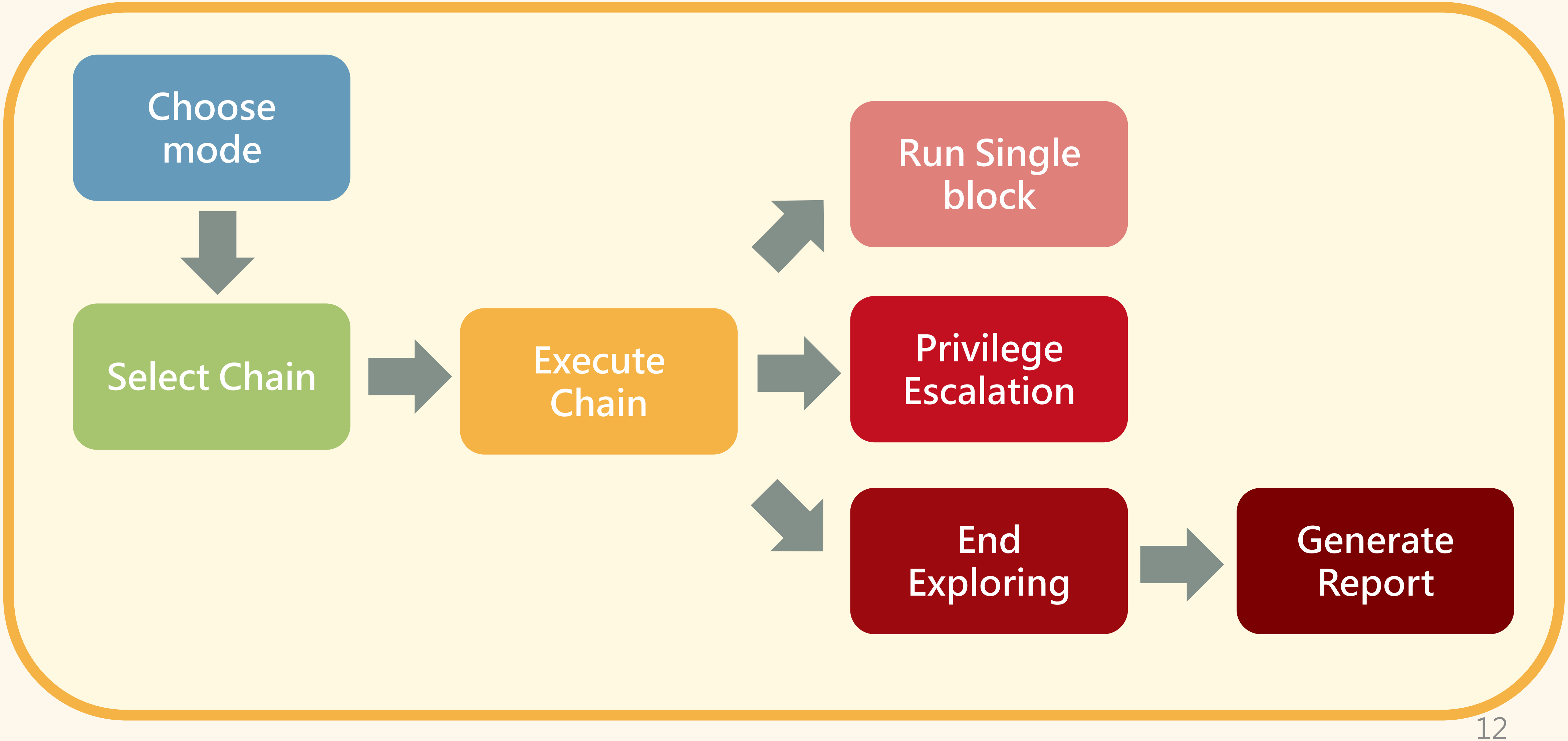
Design and Architecture



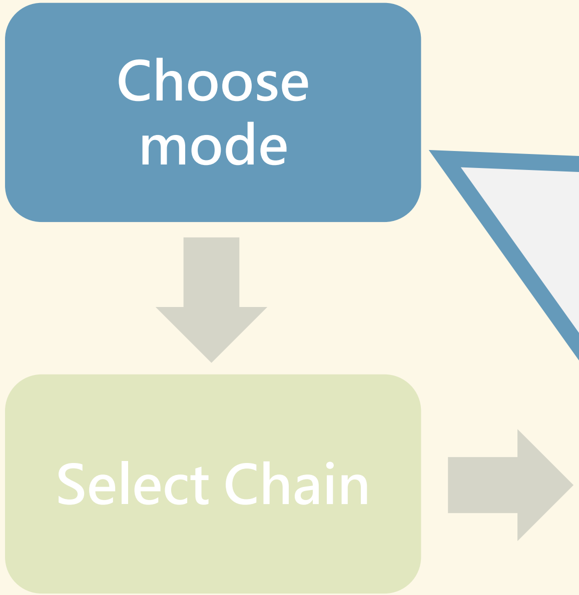


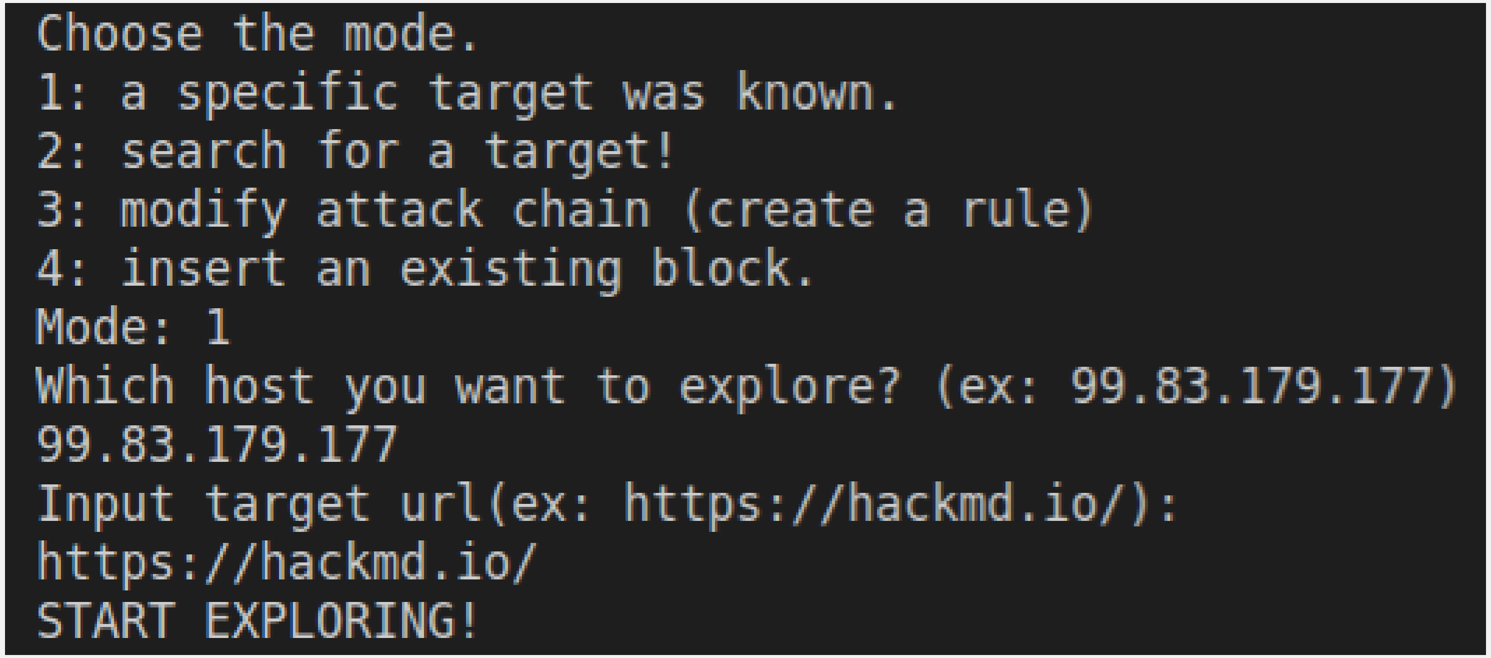
```
Show suggested chain(1) or manually choose from all chains(2)?
1
your condition:
Service: ['http', 'https']
OS: None
Port: ['80', '443']
Apache: None
attack chain couch.yml 's tag: None
attack chain pentest.yml 's tag: {'PT': ['01', '02', '04']}
attack chain erlik.yml 's tag: None
attack chain anonforce.yml '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']
```

Design and Architecture



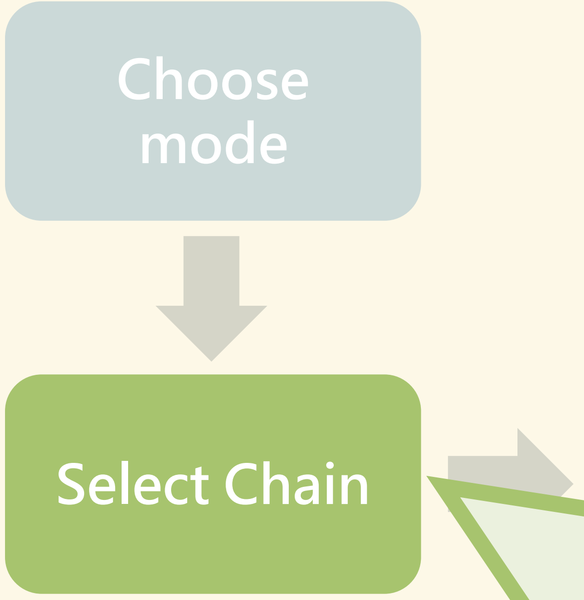
Design and Architecture





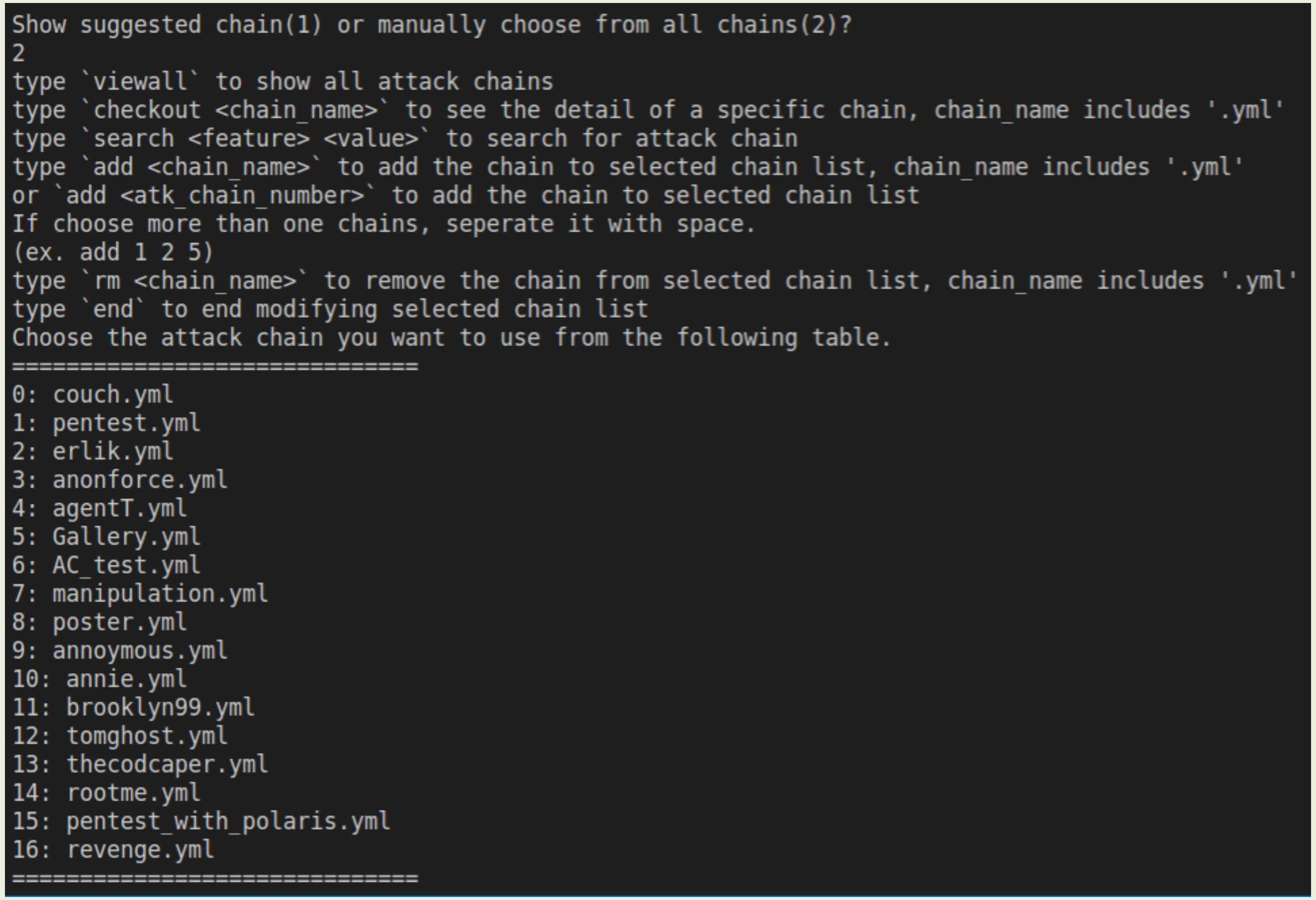
```
Choose the mode.
1: a specific target was known.
2: search for a target!
3: modify attack chain (create a rule)
4: insert an existing block.
Mode: 1
Which host you want to explore? (ex: 99.83.179.177)
99.83.179.177
Input target url(ex: https://hackmd.io/):
https://hackmd.io/
START EXPLORING!
```

Design and Architecture



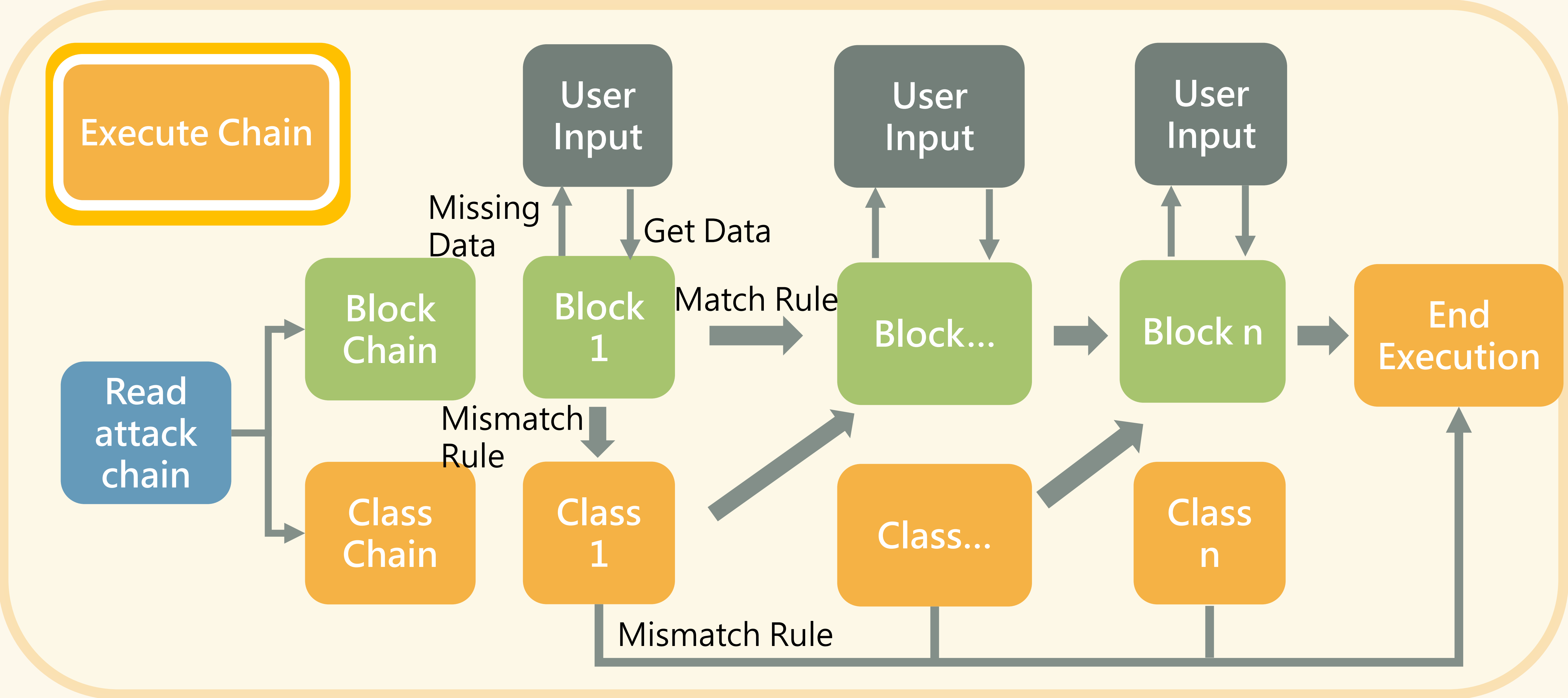
Choose mode

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
==============================
```

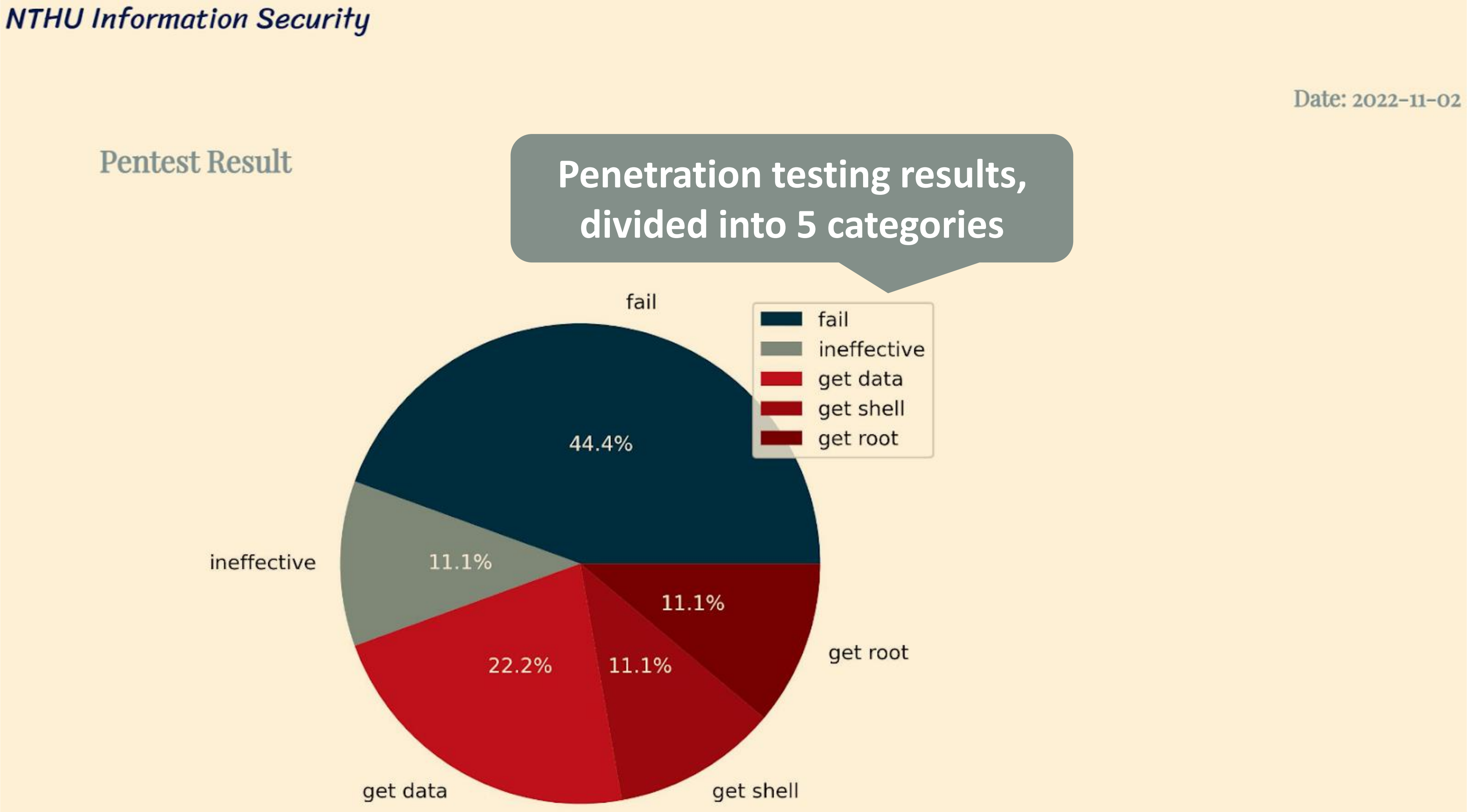
Design and Architecture



PART 5

Results

Results



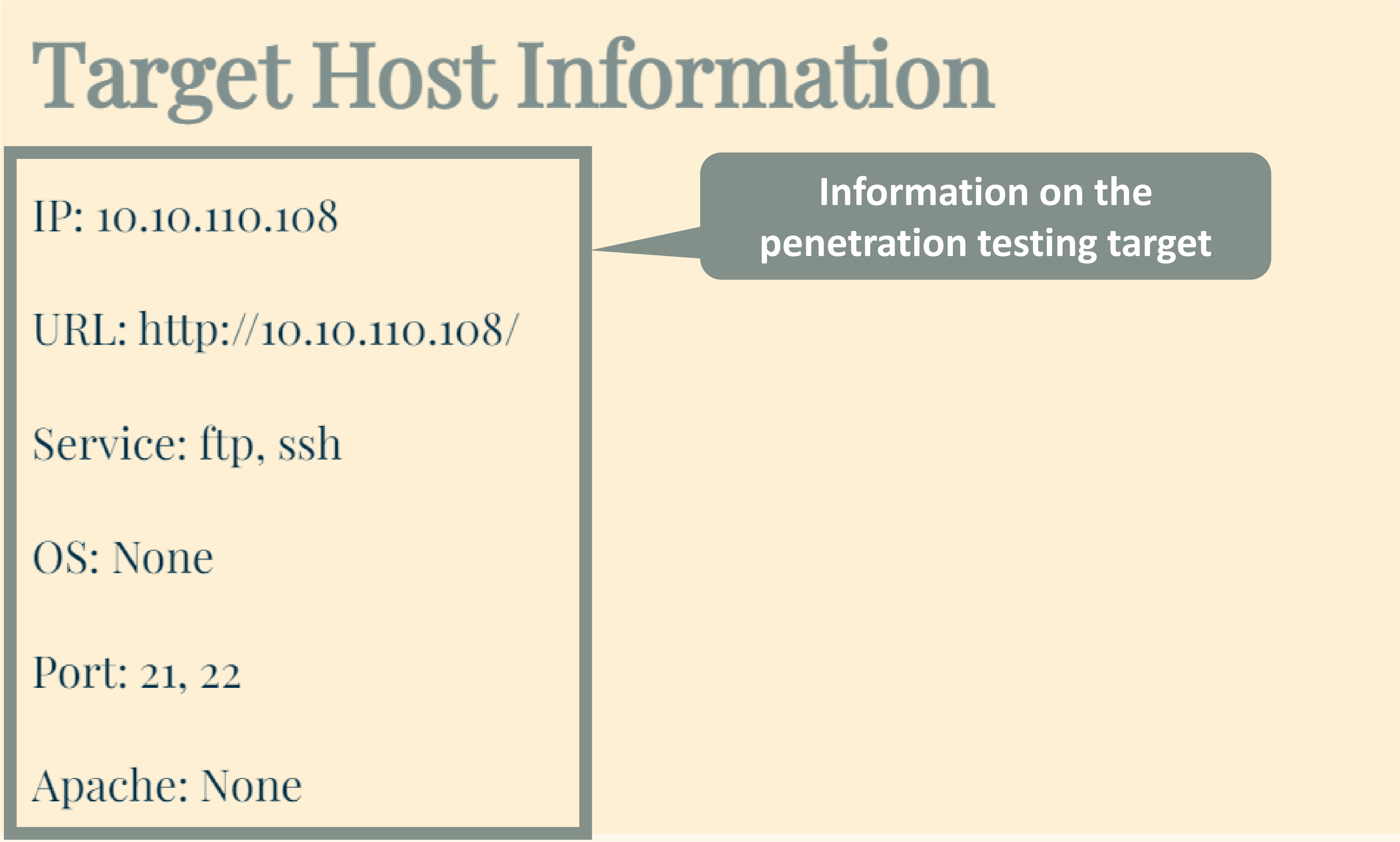
NTHU Information Security

Date: 2022-11-02

Pentest Result

Penetration testing results, divided into 5 categories

Results



Target Host Information

IP: 10.10.110.108

URL: http://10.10.110.108/

Service: ftp, ssh

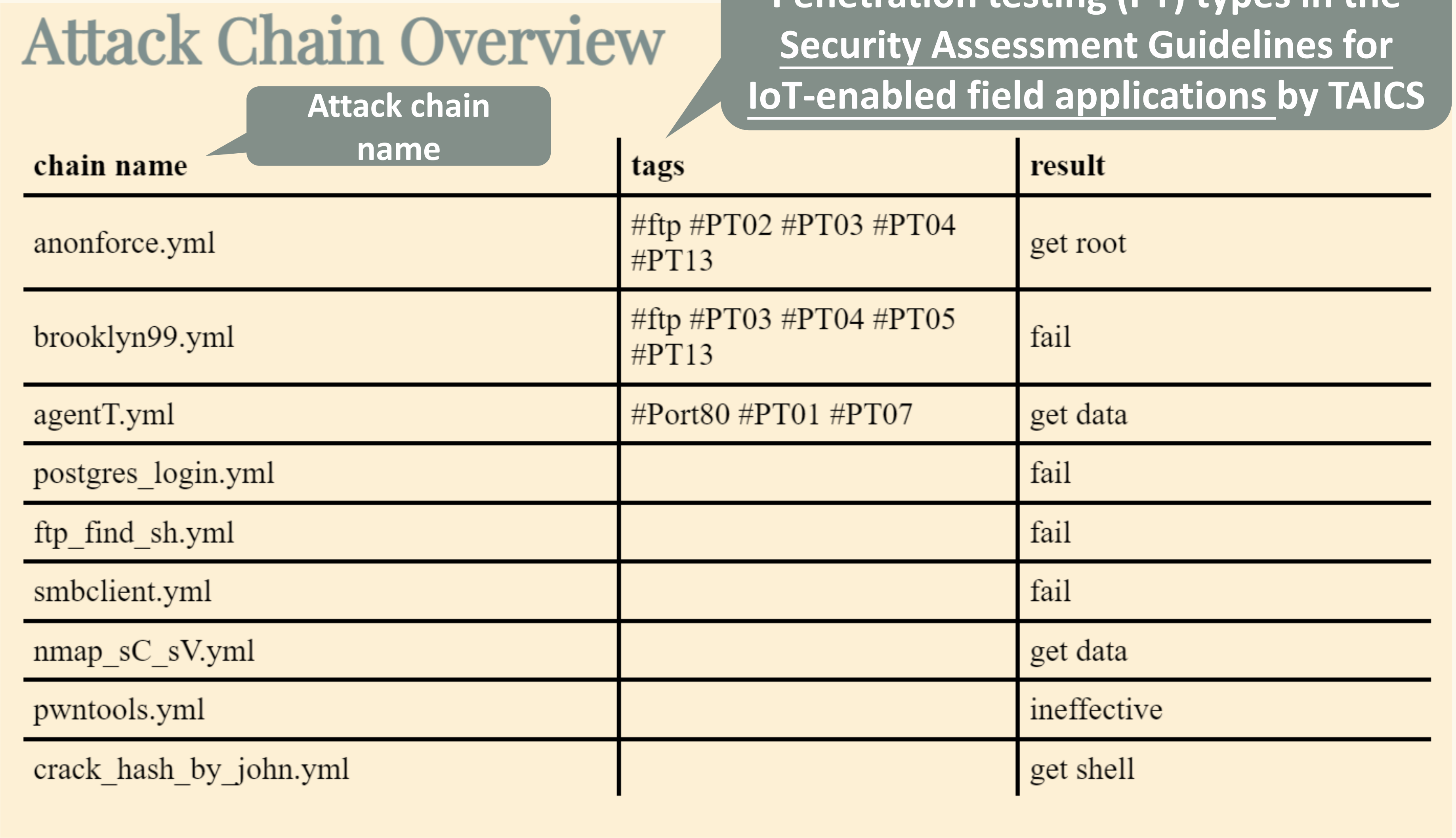
OS: None

Port: 21, 22

Apache: None

Information on the penetration testing target

Results



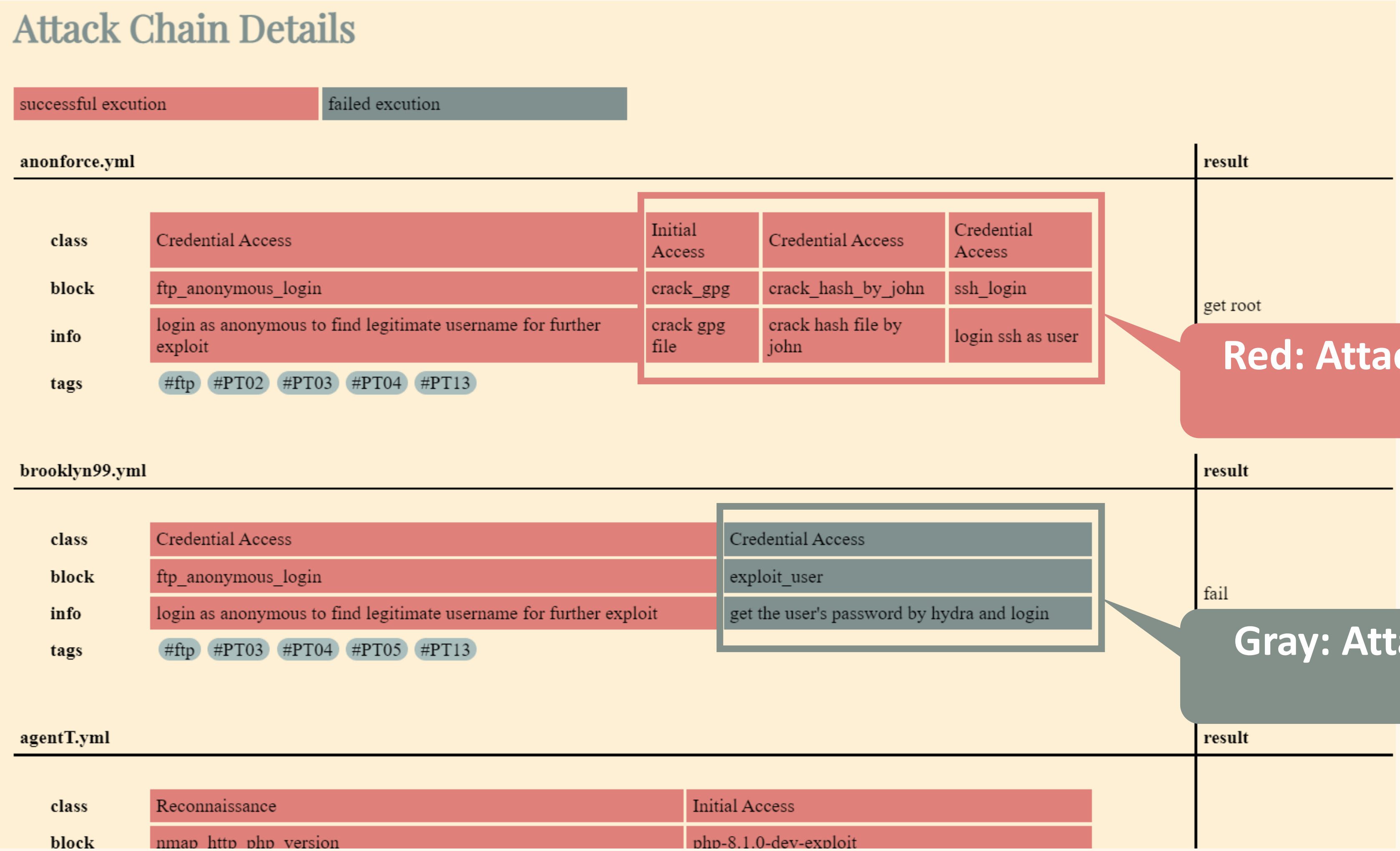
Attack Chain Overview

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

Attack chain name

Penetration testing (PT) types in the Security Assessment Guidelines for IoT-enabled field applications by TAICS

Results



Attack Chain Details

successful excution | failed excution

anonforce.yml					result
class	Credential Access	Initial Access	Credential Access	Credential Access	get root
block	ftp_anonymous_login	crack_gpg	crack_hash_by_john	ssh_login	
info	login as anonymous to find legitimate username for further exploit	crack gpg file	crack hash file by john	login ssh as user	
tags	#ftp #PT02 #PT03 #PT04 #PT13				

brooklyn99.yml			result
class	Credential Access	Credential Access	fail
block	ftp_anonymous_login	exploit_user	
info	login as anonymous to find legitimate username for further exploit	get the user's password by hydra and login	
tags	#ftp #PT03 #PT04 #PT05 #PT13		

agentT.yml			result
class	Reconnaissance	Initial Access	
block	nmap_http_php_version	php-8.1.0-dev-exploit	

Red: Attack chain successfully executed

Gray: Attack chain execution failed

PART 6

Conclusion

Conclusion

Development Achievements

- The tool can integrate with built-in tools in Kali Linux.
- Allows users to explore the domain.
- Generator function is used to facilitate users in adding attack chains.
- Automated execution of commands or prompts to assist penetration testing.
- Provide a report for users to evaluate the results.

Future Outlooks

- Become an open-source project, open to more user contributions of attack chains.
- Provide more reference materials for beginners who are new to penetration testing techniques.

PART 7

Q & A