FORTINET
Training Institute

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

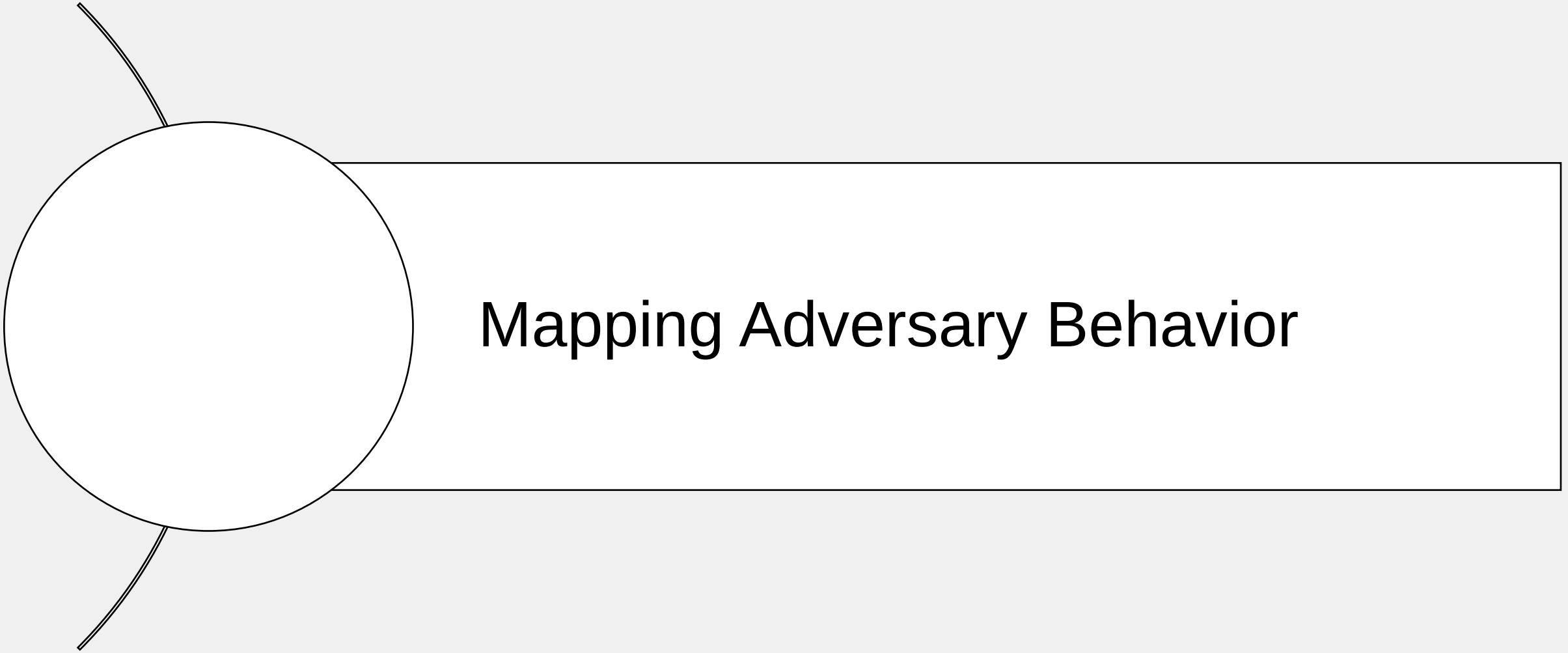
Security Operations Analyst

MITRE Mapping Adversary Behavior

FortiAnalyzer 7.4

Last Modified: 21 January 2025

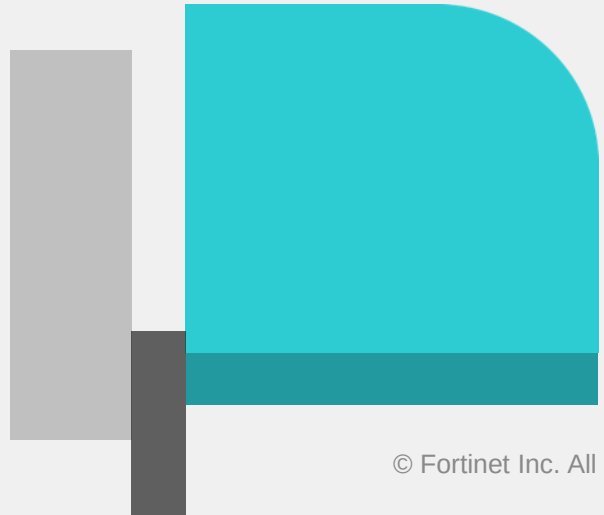
Lesson Progress



Mapping Adversary Behavior

Objectives

- Review a simulated attack
- Understand how to use the ATT&CK Navigator



Mapping Adversary Behavior

- Understanding adversary behavior is a crucial step in protecting your network and data

- Ask these two questions:
  - *Why?* What is the technical goal (*tactic*) of the threat actor?
  - *How?* What actions (*technique* or *subtechnique*) is the threat actor taking to achieve their goal?

- The more you understand the techniques and the tools bad actors use, the more effective you will be when formulating your strategy against threats

- In this section, you will review a use case to learn how to map adversary behavior to a mock report

Use Case—Healthcare Sector

Cybercriminals are attempting to use a phishing attack to hold private data from your organization, a hospital, for ransom.

Threat: Potential breach exposing thousands of patients' data and putting patients at risk

Your goal: Prevent your computer systems from breaking down, prevent data from being compromised, and avoid disaster

Domain: Enterprise

Attacker: Group ABC

Mock Security Threat Report

This threat report describes a simulated attack by the fictional **Group ABC**. You will use this report to map the behavior.

This report builds upon threat research information that describes observed tactics, techniques, and procedures associated with Group ABC.

"Group ABC initially *performs passive reconnaissance to gather information about their target*, such as researching the employees and downloading publicly available files hosted on their corporate website. Group ABC then *probes their potential target's email systems in search of valid email accounts*, most likely based on lists of common usernames. Once they confirm valid email addresses on the target organization, Group ABC starts a *spearphishing* campaign against select users. The following are some common characteristics found in similar campaigns:

a) The *spearphishing* emails usually contain an *attached malicious macro-enabled document*.

b) Group ABC usually tries to leverage potential hierarchy or power relationships to *lure targets into downloading and opening malicious files*. They couple this with email content that conveys a sense of urgency, familiarity and/or penalties to the *email recipient* if they do not act immediately and as the message advises. Group ABC commonly sends the email to accounts that potentially belong to system administrators, management, HR, and so on.

c) Group ABC generates *a new version of the malicious artifact* for each campaign, in order to prevent static detection based on file hash. However, the files look the same in terms of content and they all include malware identified in *CVE-2018-16858*.

Mock Security Threat Report (Contd)

After execution, the malware *establishes a reverse TCP control channel with a C&C server*. The channel uses TCP po*rt 443* in order to evade basic security controls that may block communication to nonstandard ports on the internet.

After establishing initial access through *spearphishing* and malicious file execution, Group ABC uses a dropper *to install a new service on the target system*. *This process establishes persistence of the C&C channel*, even when the initially compromised host restarts.

After establishing persistence, Group ABC *tries to clear the security audit log* on the compromised target in order *to evade detection*.

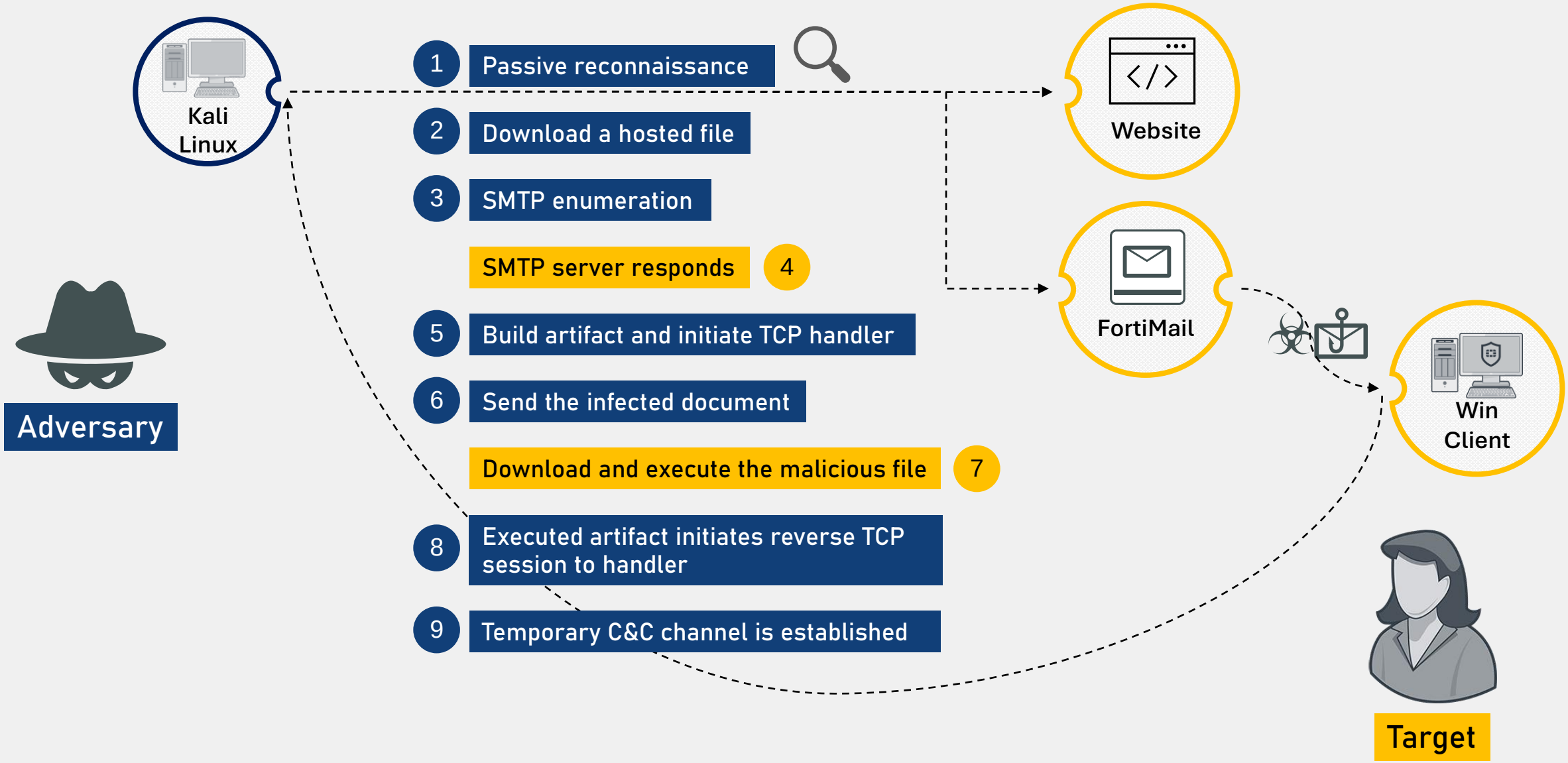
With a persistent connection to the network, Group ABC will try to discover high priority targets using *active reconnaissance* and *moving laterally on the network to those targets*. They will use dictionary attacks to discover credentials.

After this initial setup, Group ABC *proceeds to exfiltrate confidential data that can be sold or ransomed*.

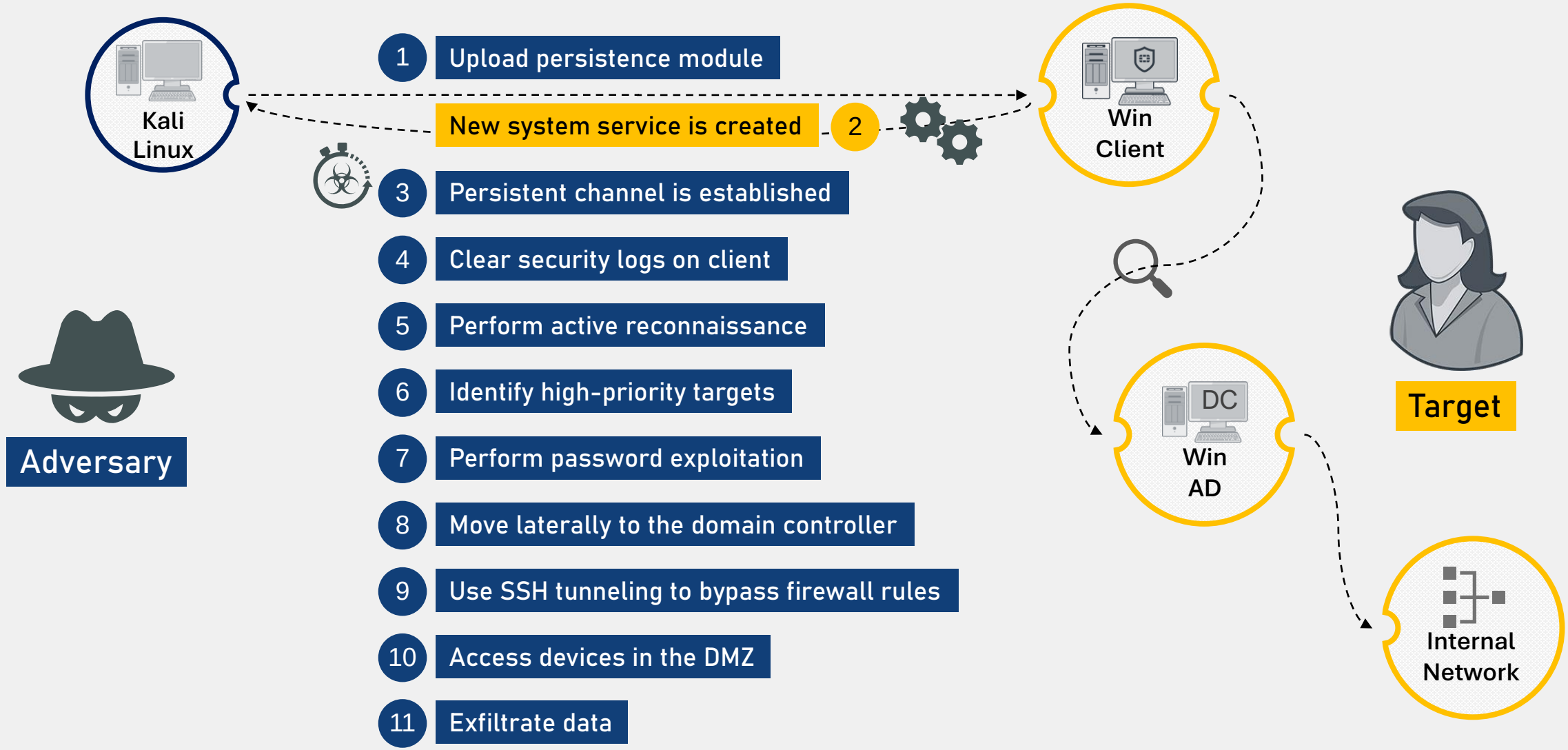
FORTINET Training Institute

The purple team analyzes the threat report and identifies the key elements to build a mapping of Group ABC's behavior using the MITRE ATT&CK for Enterprise matrix

Adversary Attack Flow—Exploitation Phase



Adversary Attack Flow—Post-Exploitation Phase

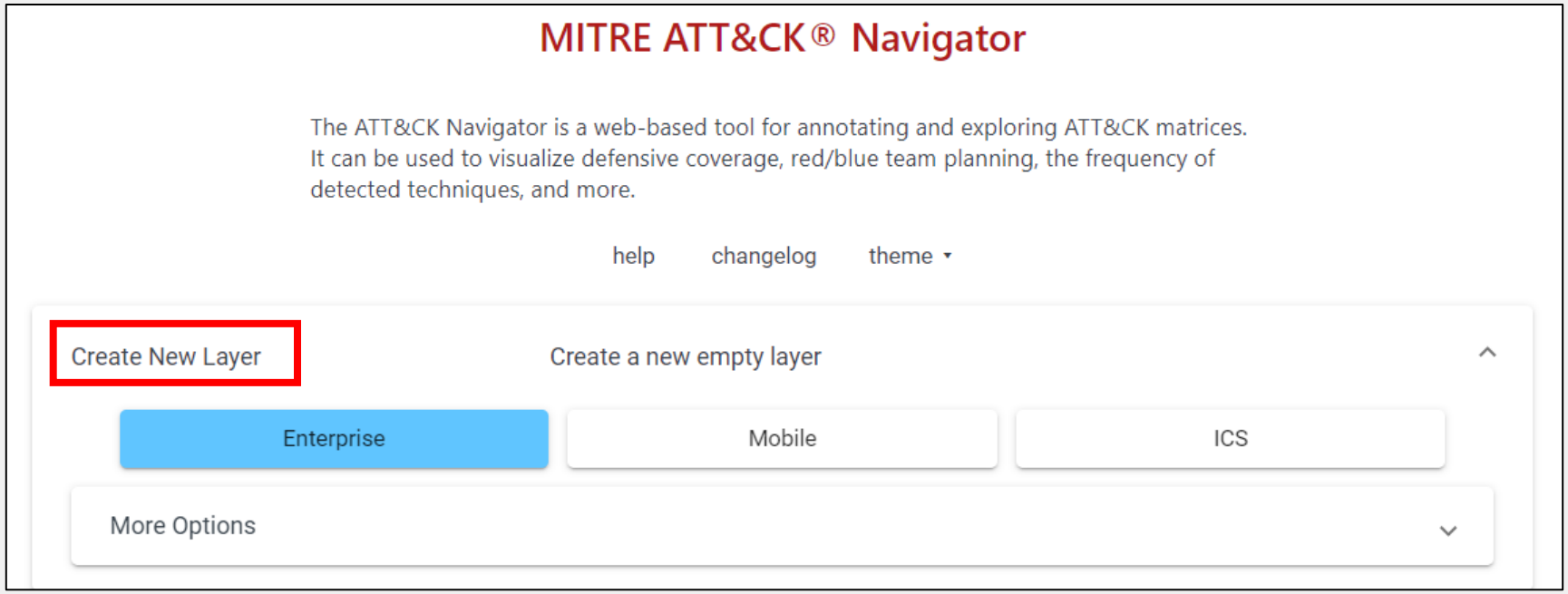


Using the MITRE ATT&CK Navigator

- You can access the MITRE ATT&CK Navigator here:

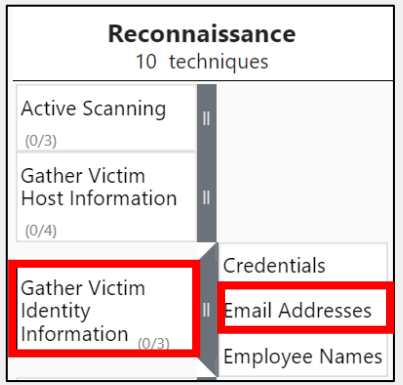
  https://mitre-attack.github.io/attack-navigator/

- There are three matrices:
  - Enterprise, Mobile, and Industrial Control System (ICS)
  - They offer different tactics, techniques, and subtechniques
- Click **Create New Layer** to select the matrix type

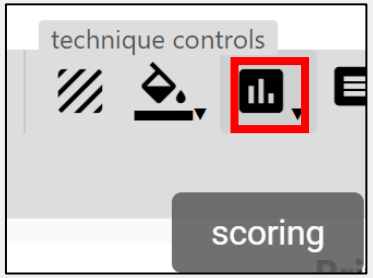


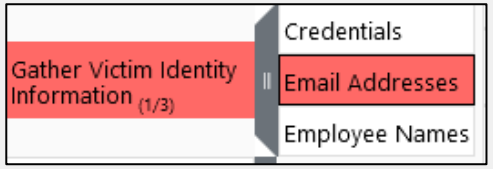
Using the MITRE ATT&CK Navigator (Contd)

- As an example, using information from the mock report, you can create a mapping:
  - Such as selecting the **Gather Victim Identity Information** technique, and the **Email Addresses** subtechnique



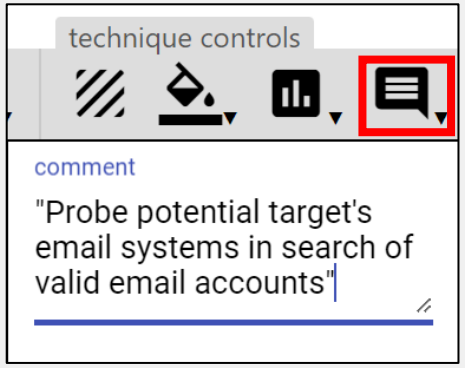
- You can also use the **scoring menu** in the top right-hand corner of the navigator by providing the techniques and subtechniques a score value
  - This will highlight the entries and make your mapping easier to read



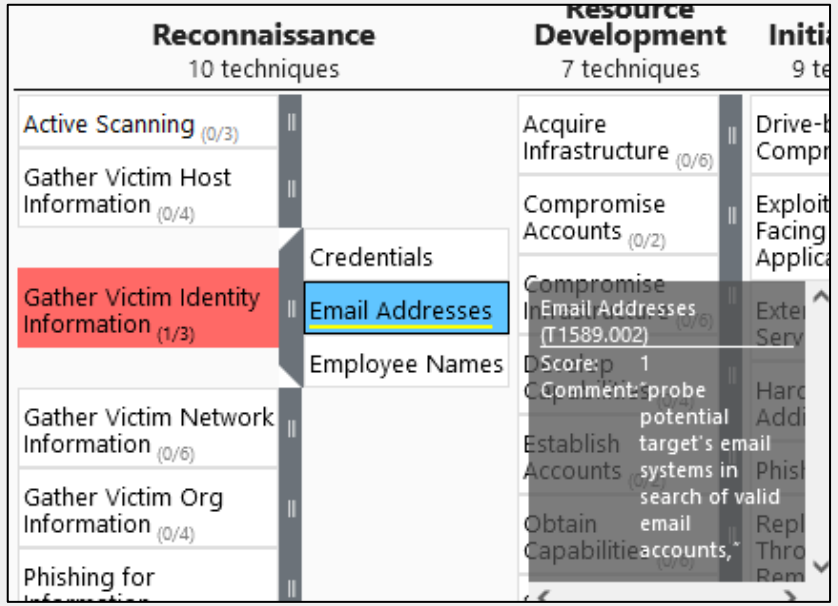


Using the MITRE ATT&CK Navigator (Contd)

- You can also add comments using the icon in the upper-right of the navigator
  - Use comments to detail the adversary procedures

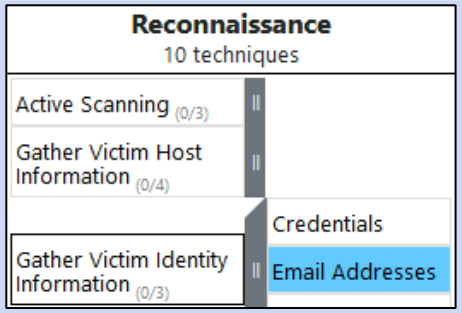


- The example comment is listed under the **Email Addresses** subtechnique

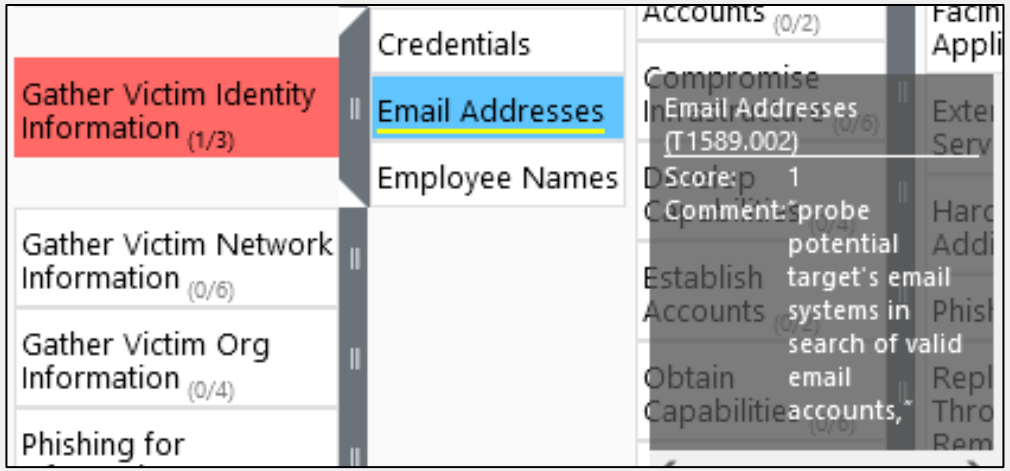


Example Mapping

The purple team identified the following information from the mock report:
Group ABC first performs a Reconnaissance (tactic) by using a list of common usernames to probe the target's email systems, in order to Gather Victim Identity Information (technique) and obtain Valid Email Addresses (subtechnique) existing on the target.

Report Phrase	Tactic	Technique	Subtechnique	Navigator Interface
"***probe potential target's email systems in search of valid email accounts,***"	**Reconnaissance**	**Gather Victim Identity Information**	**Email Addresses**	

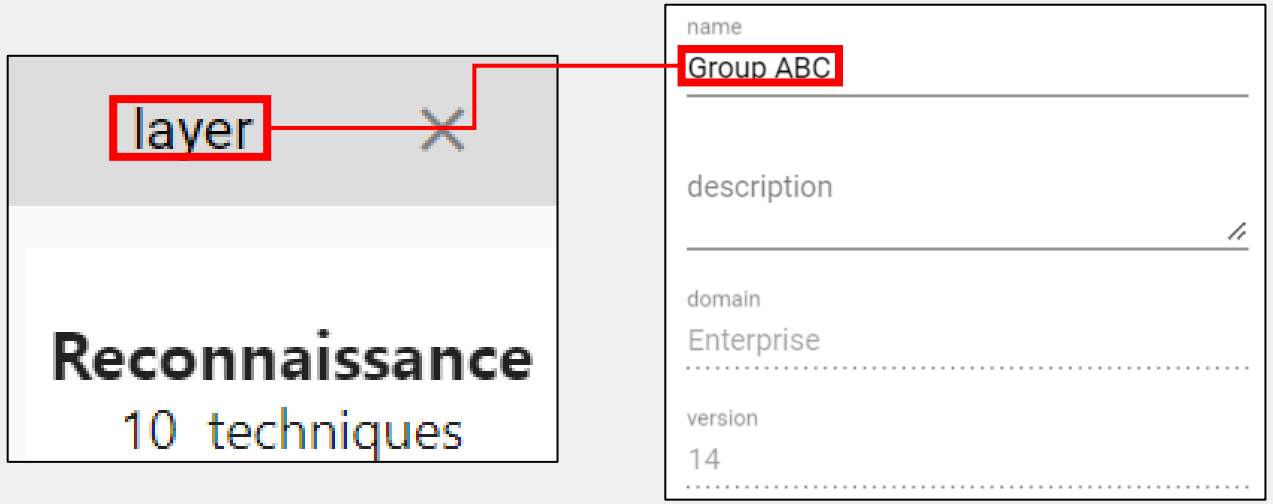
The result of a mapping



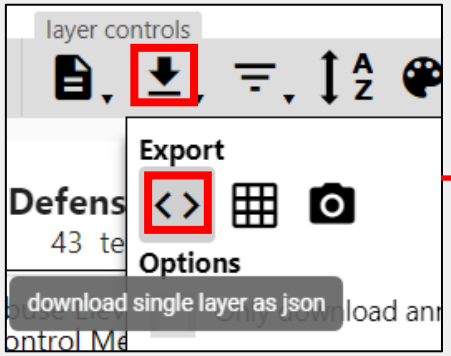
FORTINET Training Institute

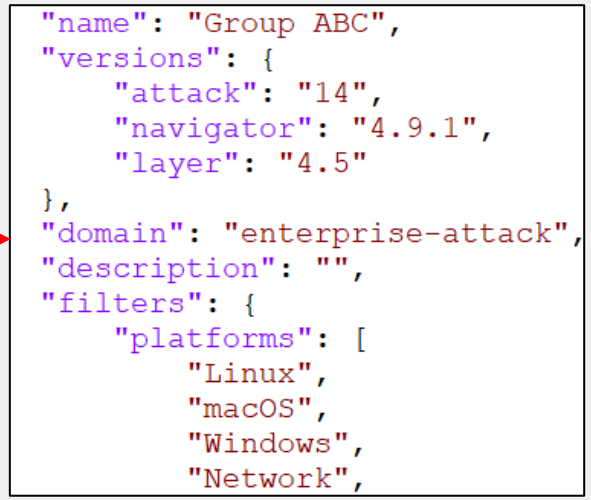
Saving and Exporting the Mapping

- You can rename the layer and export the mapping for future use



- You can also download the mapping and send your findings to other SOC members as a JSON file





```
"name": "Group ABC",
"versions": {
    "attack": "14",
    "navigator": "4.9.1",
    "layer": "4.5"
},
"domain": "enterprise-attack",
"description": "",
"filters": {
    "platforms": [
        "Linux",
        "macOS",
        "Windows",
        "Network",
```

FORTINET Training Institute

Knowledge Check

1. What is reconnaissance in the MITRE ATT&CK framework?
   A. It is a technique.
   B. It is a subtechnique.
   ✔ C. It is a tactic.

2. Which is considered a post-exploitation activity?
   A. Preparing a malicious payload
   ✔ B. Establishing persistence
   C. Sending a phishing email

Lesson Progress

Mapping Adversary Behavior

Review

- ✓ Review a simulated attack
- ✓ Use the ATT&CK Navigator