

Exercise 2: Reviewing the FortiAnalyzer MITRE ATT&CK Framework

In this exercise, you will review the MITRE ATT&CK framework on FortiAnalyzer.

MITRE ATT&CK has three matrices: Enterprise, ICS, and Mobile. The focus of this lab is on the Enterprise Matrix.



The Enterprise and ICS matrices are available on FortiAnalyzer. However, note that the ICS functionality requires additional licensing.

In the last exercise, you learned what tactics, techniques, and subtechniques are. You will apply that knowledge to the FortiAnalyzer GUI.

Examine the MITRE ATT&CK Enterprise Matrix

You will examine the **Attack** and **Coverage** tabs of the MITRE ATT&CK Enterprise Matrix. You will also explore how event handlers are mapped to a technique or subtechnique.

To examine the MITRE ATT&CK Enterprise Matrix Attack tab

- On the bastion host, open Chrome, and then log in to the FAZ-MSSP GUI (10.200.4.236) with the following credentials:
 - Username: admin
 - Password: Fortinet1!
- Click **Incidents & Events > MITRE ATT&CK > Attack**.
- In the **Reconnaissance** column, view the **Active Scanning** technique.

Attack	Coverage			
Refresh	Last 1 Week	2024-02-07 14:00:32 - 2024-02-14 14:00:32		
Reconnaissance	Resource Development	Initial Access	Execution	Persistence
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques
Active Scanning ✓ Covered	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation
Gather Victim Host Information ✓ Covered	Acquire Infrastructure ✓ Covered	Exploit Public-Facing Application ✓ Covered	Command and Scripting Interpreter ✓ Covered	BITS Jobs ✓ Covered
	Compromise			Boot or Logon

- Under the technique name, note the **Covered** status.

Active Scanning

✓ Covered

The **Covered** status means that there is at least one event handler on FortiAnalyzer that is classified under this technique.

5. Hover over the **Active Scanning** technique to see more details.

Attack

Coverage

Refresh

Last 1 Week

2024-02-07 16:40:44 - 2024-02-14 16:40:44

Reconnaissance

10 techniques

Active Scanning

Covered

3 Event Handler(s) created. No Attacks detected.

Scanning IP Blocks

Vulnerability Scanning

Wordlist Scanning

Execution

14 techniques

Closure

Administration

Configuration

The three predefined event handlers that cover this technique are listed: **Scanning IP Blocks**, **Vulnerability Scanning**, and **Wordlist Scanning**. Also, **No Attacks detected** indicates that no attacks were detected within the selected time frame (**Last 1 Week**) for this technique. If attacks are detected, they will be indicated here—you will observe this in a later lab.

6. Examine the rest of the matrix.

You may need to scroll to see other parts of the matrix.



Depending on the version of FortiAnalyzer and whether MITRE ATT&CK has been updated, you may see a slight difference between the tactics, techniques, and subtechniques that appear on the FortiAnalyzer GUI and the ATT&CK Navigator.

To examine the MITRE ATT&CK Enterprise Matrix Coverage tab

- 1. Continuing on the FAZ-MSSP GUI, click **Incidents & Events > MITRE ATT&CK > Coverage**.
- 2. In the **Reconnaissance** column, review the **Active Scanning** technique.

Attack

Coverage

Refresh

110 Event Handlers

Reconnaissance

10 techniques

Active Scanning

3

Gather Victim Host Information

1

Gather Victim Identity Information

Resource Development

8 techniques

Acquire Access

Acquire Infrastructure

1

Compromise Accounts

Compromise Infrastructure

Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

3

External Remote Services

2

On the **Coverage** tab, you can see the same tactics and techniques that are on the **Attack** tab. However, the **Coverage** tab includes information about the specific event handlers.

The higher the number (**3** in this example), the more event handlers are associated with the techniques and subtechniques under a tactic.



A higher number is also represented by a deeper shade of green. If there is no color, it means that there is no current coverage from any event handler for that technique or subtechnique.

3. Hover over the **Active Scanning** technique to see more details.

Reconnaissance

10 techniques

Active Scanning

3

Event Handler Count: 3

T1595.001 Scanning IP Blocks (2)

T1595.002 Vulnerability Scanning

T1595.003 Wordlist Scanning (1)



There are three event handlers associated with the T1595 technique. Two of them are associated with the **T1595.001** subtechnique, and the third is associated with the **T1595.003** subtechnique.

4. Double-click the **Active Scanning** technique.

T1595 Active Scanning			
<div>Search...</div>			
State	Event Handler	Description	Technique
Enabled	Default-Recon-Activity-By-Endpoint	Default Handler for Recon Activity dete...	T1595.001 Scanning IP Blocks
Disabled	Default-NMAP-Process-Activity-Detection	NMAP Process Activity detected. NMA...	2 Techniques
Enabled	Default-Web-Server-URL-Scanning-Detect	If a web server received too many 404 r...	T1595.003 Wordlist Scanning

5. Review the active event handlers, including their names, descriptions, and the technique or subtechnique that they are categorized under.