

Attack Methodology Frameworks

By: Keziah Rogers

This lab includes information about: **Attack Methodology Frameworks & OWASP Testing Framework**

TASKS:

- Explore the MITRE ATT&CK Website
- Detect Web Server Vulnerabilities

After completing this exercise, I have further knowledge of:

- Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK Framework
- Open Source Security Testing Methodology Manual (OSS TMM)
- OWASP Testing Guide

Exercise 1 - Attack Methodology Frameworks

As a Cybersecurity Analyst, I must proactively protect against threats. I will have to discover and use different attack methodology frameworks as manuals for incorporating cybersecurity principles.

I used virtual machines to complete this lab also.

Lockheed Martin originally designed the Cyber Kill Chain, the most commonly referenced cybersecurity framework. The framework consists of the methodology of a cybersecurity attack and describes the attack timeline.



The seven steps for the Cyber Kill Chain are the following:

1. Reconnaissance

The attacker will gather information on the intended target and identify possible vulnerabilities that can be exploited. The reconnaissance steps are the most critical part of the Cyber Kill Chain, which can be done online or offline. The information gathered can be from harvesting emails to more advanced methods such as the deployment of information-gathering applications.

2. Weaponization

Once the relevant information has been gathered, the attacker will formulate a strategy for exploiting the intended target. This may be in the form of developing malware that can be used to exploit the target.

3. Delivery

After the attack strategy has been finalized, the next stage will be delivering the intended malware or gaining access to the target's network. Gaining access may involve hacking into the network or exploiting detected vulnerabilities.

4. Exploitation

After the network has been breached, the cybersecurity criminal will then exploit the network further by detecting further vulnerabilities.

5. Installation

The next phase of the attack is to install malicious applications to gain further control of the systems on the network. These malicious applications can include Trojan Horses, Backdoors or any additional tools that can be used for the exploit.

6. Command & Control

The crucial part of the attack occurs when the attacker tries to take control of the compromised systems. This will allow the attacker to remotely track and control the maliciously deployed software and will be broken down into two phases:

- Obfuscation - The attacker will cover their tracks to prevent detection of the breach
- Denial of Service (DoS) - The attacker will cause distractions to draw the attention away from the primary attack.

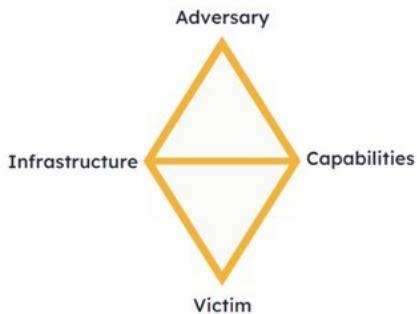
7. Action

The last phase of the attack is when action is taken on the compromised system, and the attack's goal is executed. The following are some examples:

- Data exfiltration
- Data encryption
- Data deletion

Diamond Model of Intrusion Analysis

The diamond model of intrusion analysis provides companies with an effective, accurate analysis of a cybersecurity incident. Using this approach, every incident is depicted as a diamond consisting of the following components, adversary, capability, infrastructure, and victim. These different components are delineated to describe the relationship with each other, which can be examined analytically to gain insights into the incident.



Adversary

An adversary is the cybersecurity criminal or threat actor responsible for the cyber incident.

Capability

The capabilities identify the tools and techniques the cybersecurity criminal or threat actor used to facilitate the capability.

Infrastructure

Infrastructure refers to physical or logical communication structures facilitated by the threat actor to achieve the capability aspect.

Victim

A victim is an entity that has been exploited or the vulnerabilities have been exposed. It can be a person, organization, or organization's assets.

MITRE ATT&CK Framework

The **MITRE ATT&CK framework** was developed with a more granular approach to describe attack behaviors when compared to the Cyber Kill Chain framework. Specific improvements have been implemented in this framework which include the following:

- In-depth coverage of host attack behaviors
- Granular description of attack behavior
- Detection and mitigation strategies for attack behavior

The MITRE ATT&CK framework consists of the following stages:

1. Privilege escalation
2. Defense evasion
3. Credential access
4. Discovery
5. Lateral movement
6. Exfiltration
7. Impact

The attack framework describes attack behaviors and suggests detection and mitigation techniques. Mitigation strategies are individually tagged and cross-referenced with MITRE ATT&CK tactics and techniques.

Task 1 - Exploring the MITRE ATT&CK Website

In this task, I explored the MITRE ATT&CK website.

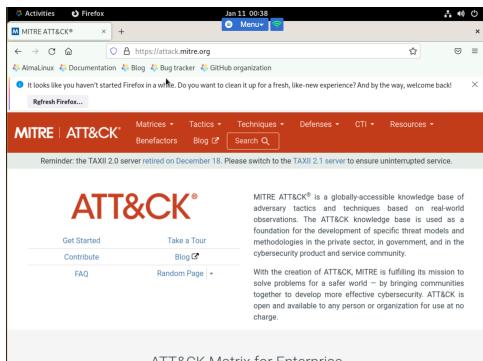
Step 1

I connected to **ACIALMA**.

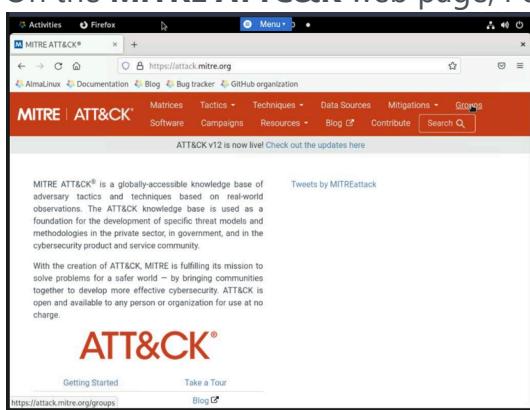
Opened **Firefox** in the **Activities** window.



In the FireFox browser, I typed in: <https://attack.mitre.org>



On the **MITRE ATT&CK** web page, I clicked the **Groups** link.



On the **Groups** page, I scrolled down and clicked **Ajax Security Team**.

The screenshot shows the MITRE ATT&CK Groups page. The URL is https://attack.mitre.org/groups/. The top navigation bar includes links for Activities, Firefox, Menu, Groups, Matrices, Tactics, Techniques, Data Sources, Mitigations, Software, Campaigns, Resources, Blog, Contribute, and Search. On the left, there's a sidebar titled 'GROUPS' listing various groups like APT1, APT17, APT18, etc. The main content area displays two groups: G0130 (Ajax Security Team) and G1000 (ALLANITE). The Ajax Security Team row contains a detailed description: "Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies." Below the table is a link to the group's page: https://attack.mitre.org/groups/G0130.

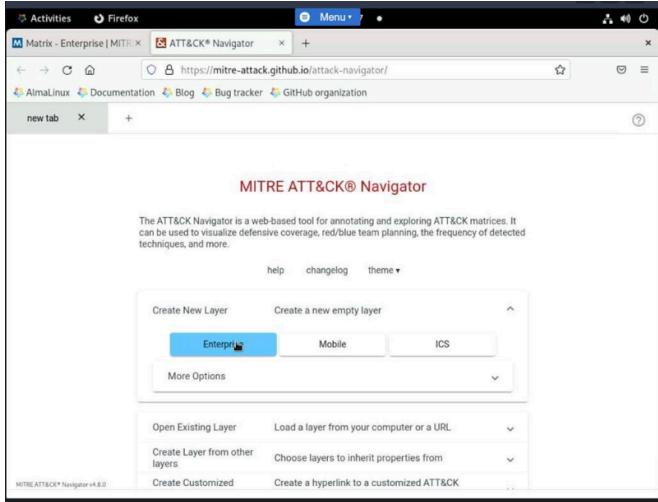
By selecting a specific group I was able to gain more information on the types of exploits the group has conducted on the website

In the **Firefox** browser, I clicked **Matrices** in the top pane.

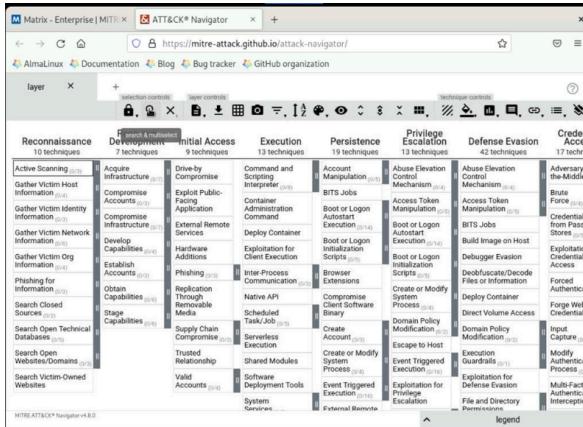
The screenshot shows the MITRE ATT&CK Navigator page. The URL is https://attack.mitre.org/groups/G0130/. The top navigation bar includes links for Activities, Firefox, Menu, Groups, Matrices, Tactics, Techniques, Data Sources, Mitigations, Software, Campaigns, Resources, Blog, Contribute, and Search. A message at the top says "ATT&CK v12 is now live! Check out the updates here". The left sidebar lists groups: ALLANITE, Andariel, Aorqin Dragon, APT-C-36, APT1, APT12, APT16, APT17, APT18, APT19, and APT28. The main content area shows the "Ajax Security Team" page with a detailed description: "Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies." To the right, there's a sidebar with details: ID: G0130, Associated Groups: Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose, Version: 1.0, Created: 14 April 2021, Last Modified: 17 December 2021. At the bottom of the page is a link: https://attack.mitre.org/matrices/.

I then clicked the **View on the ATT&CK - Navigator** link in the right pane.

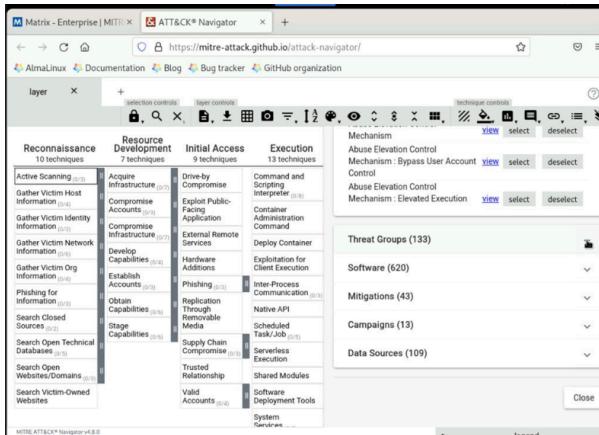
On the **MITRE ATT&CK Navigator** page, select Enterprise in the Create New Layer drop-down menu.



The website opened to a new tab. I selected **Search & Multiselect** from the toolbar menu.



I scrolled down and expanded the **Threat Groups** drop-down menu in the **Search** fly-out menu.



I clicked **Select** next to the **APT19** Threat Group in the Threat Groups pane.

The screenshot shows the MITRE ATT&CK Navigator v4.8.0 interface. The main navigation bar includes tabs for Matrix - Enterprise | MITRE, ATT&CK® Navigator, and Ajax Security Team, Open. Below the navigation bar, there are links for AlmaLinux, Documentation, Blog, Bug tracker, and GitHub organization. The main content area has a sidebar on the left listing various attack techniques under categories like Reconnaissance, Resource Development, Initial Access, and Execution. The right side features a search and multiselect window titled "Threat Groups (133)" which lists threat groups such as APT1, APT16, APT17, APT18, and APT19, each with "view", "select", and "deselect" buttons. Below this are sections for Software (620), Mitigations (43), Campaigns (13), and Data Sources (109). A legend at the bottom right indicates the meaning of the icons used in the interface.

I clicked **Search & multiselect** to close the search fly-out window.

This screenshot is identical to the one above, but the search and multiselect window is no longer visible, indicating it has been closed. The rest of the interface remains the same, showing the threat group list and other data sources.

I clicked next to the **Command and Scripting Interpreter** in the **Execution** column.

The screenshot shows the MITRE ATT&CK Navigator v4.8.0 interface with the Persistence section selected in the execution column. The main content area displays various persistence techniques under categories like Persistence, Privilege Escalation, Defense Evasion, and Credential Access. The sidebar on the left shows the full list of techniques across all categories. The right side of the interface is mostly empty, reflecting the current selection.

Next, I closed the **Firefox** browser after viewing the information available.

Exercise 2 - OWASP Testing Framework

The OWASP testing guide consists of several sub-guides on performing tests to improve an organization's security.

The following are the current OWASP Testing guides:

- Web Security Testing Guide (WSTG)
- Mobile Security Testing Guide (MSTG)
- Firmware Security Testing Methodology

More information regarding these guides can be found by following the link:

https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

In this exercise, I followed the OWASP Web Security Testing guide to determine if there are any security vulnerabilities on different web servers.

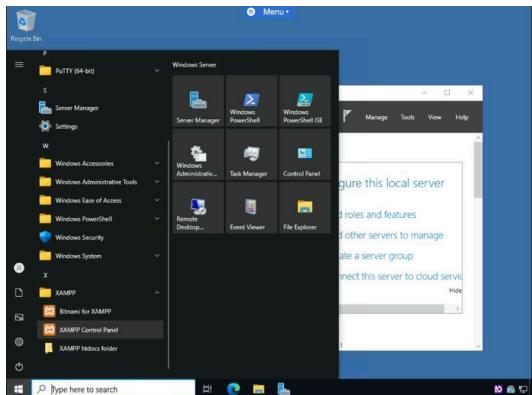
Task 1 - Detecting Web Server Vulnerabilities

In this task, vulnerabilities of a web server will be detected by using the OWASP Testing Framework guidance

Step 1

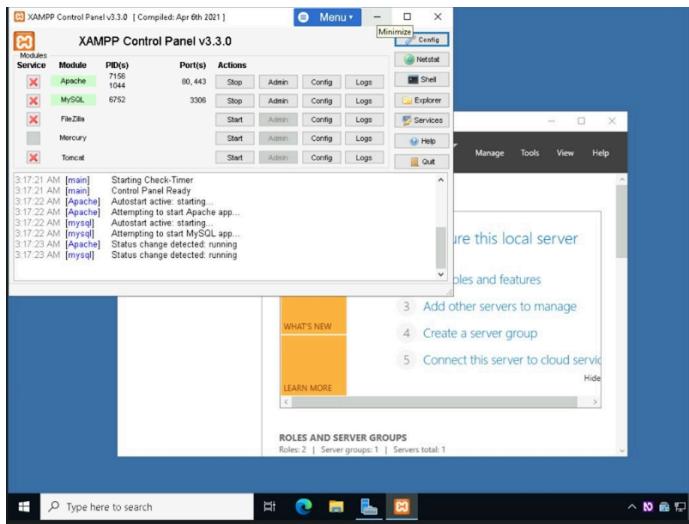
I connected to **ACIDM01**.

I clicked **Start**, selected the **XAMPP** folder, and clicked **XAMPP Control Panel**.



Ensured that the **Apache** and **MySQL** services were running.

Minimized the **XAMPP Control Panel** window.



Connected to **ACIALMA (VM)**.

Selected **Terminal** from the **Activities** window.

In the **Terminal** window, I typed the following and pressed **Enter**:

```
wget 192.168.0.2 -q -S
```

A screenshot of a terminal window titled 'Activities Terminal'. The command 'wget 192.168.0.2 -q -S' was run, resulting in the following output:

```
[acisadmin@localhost ~]$ wget 192.168.0.2 -q -S
HTTP/1.1 302 Found
Date: Mon, 27 Mar 2023 13:21:19 GMT
Server: Apache/2.4.54 (Win10) OpenSSL/1.1.1p PHP/8.2.0
X-Powered-By: PHP/8.2.0
Location: http://192.168.0.2/dashboard/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
HTTP/1.1 200 OK
Date: Mon, 27 Mar 2023 13:21:19 GMT
Server: Apache/2.4.54 (Win10) OpenSSL/1.1.1p PHP/8.2.0
Last-Modified: Thu, 29 Dec 2022 18:57:59 GMT
Etag: "442-510fc45fbcb"
Accept-Ranges: byte
Content-Length: 5186
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
[acisadmin@localhost ~]$
```

I continued and typed something else in the terminal and pressed enter.

```
curl -s -I 192.168.0.2
```

```
[aciadmin@localhost ~]$ wget 192.168.0.2 -q -S
HTTP/1.1 200 OK
Date: Mon, 27 Mar 2023 13:21:19 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0
X-Powered-By: PHP/8.2.0
Last-Modified: Sat, 29 Dec 2022 10:57:59 GMT
ETag: "1442-5f0fc1d459bc0"
Accept-Ranges: bytes
Content-Length: 5106
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
[aciadmin@localhost ~]$ curl -s -I 192.168.0.2
HTTP/1.1 200 Found
Date: Mon, 27 Mar 2023 13:21:38 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0
X-Powered-By: PHP/8.2.0
Location: https://192.168.0.2/dashboard/
Content-Type: text/html; charset=UTF-8
[aciadmin@localhost ~]$
```

Curl can also be used to collect web server information

I clicked **Activities** and selected **Firefox**.

I browsed to the URL: https://cve.mitre.org/cve/search_cve_list.html

The screenshot shows the CVE Search CVE List page. The search bar at the top contains the text "Apache httpd 2.4.54". Below the search bar, there is a message about the transition to the new CVE website and a survey notice. The main search form has a text input field containing "Apache httpd 2.4.54" and a "Submit" button. At the bottom of the page, there is footer information and social media links.

In the **Search CVE List**, I typed the following and pressed **Enter**:

This screenshot is identical to the previous one, showing the CVE Search CVE List page in Firefox. The search bar still contains "Apache httpd 2.4.54". The rest of the page content, including the search form, notices, and footer, remains the same.

I selected the **CVE-2022-3760** in the **Search Results** window.

The screenshot shows the CVE Search Results page. At the top, it says "TOTAL CVE Records: 198326". Below that, there are two entries for CVE-2022-3760:

- CVE-2022-3760**: Inconsistent Interpretation of HTTP Requests ("HTTP Request Smuggling") vulnerability in mod_proxy_ap of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
- CVE-2006-20001**: A crash can occur if a client sends a memory read, or write, of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.

At the bottom of the search results, there is a search bar labeled "SEARCH CVE USING KEYWORDS:" with a "Submit" button. Below the search bar, it says "You can also search by reference using the [CVE Reference Manager](#)".

I right-clicked **MISC:https://httpd.apache.org/security/vulnerabilities_24.html** URL and selected **Open Link in New Tab**

The screenshot shows the CVE-2022-3760 details page. The URL in the address bar is <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3760>. A context menu is open over the link, with the option "Open Link in New Tab" highlighted.

I closed the **Firefox** browser after viewing the list of vulnerabilities.

The screenshot shows the Apache HTTP Server 2.4 vulnerabilities page. The URL in the address bar is https://httpd.apache.org/security/vulnerabilities_24.html. The page title is "APACHE HTTP SERVER PROJECT". It lists security vulnerabilities for Apache HTTP Server 2.4. The first item listed is "Apache HTTP Server 2.4 vulnerabilities".