Attack Methodology Frameworks

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.

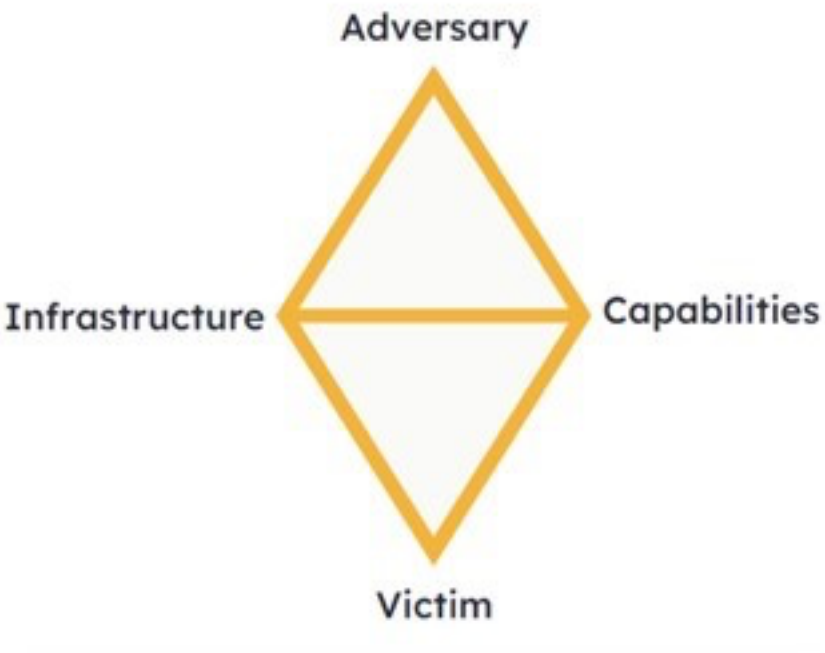
7. Action

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

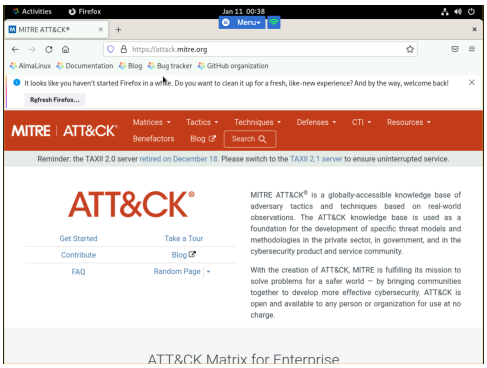
In this task, I explored the MITRE ATT&CK website.

Step 1

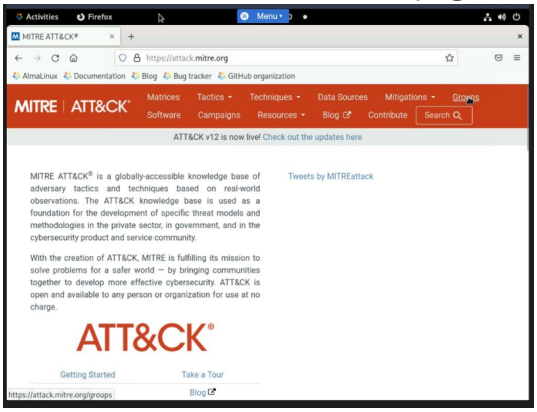
I connected to **ACIALMA.**

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

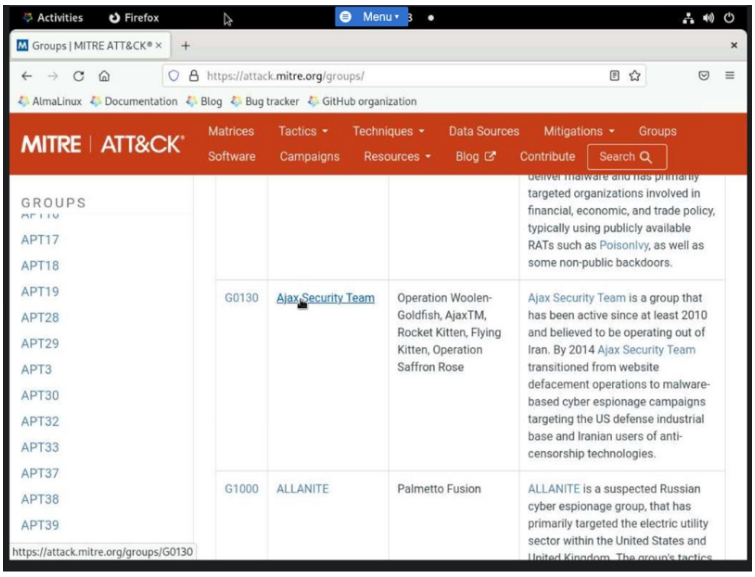
In the FireFox browser, I typed in: https://attack.mitre.org



On the **MITRE ATTC&K** web page, I clicked the **Groups** link.

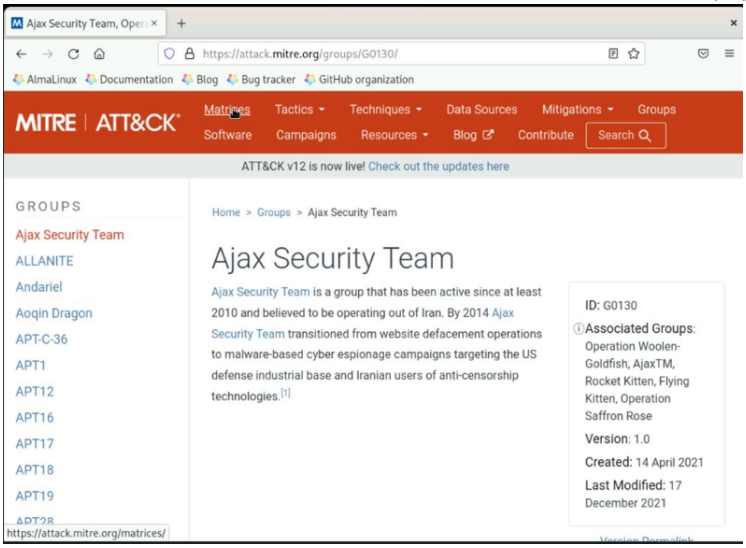


On the **Groups** page, I scrolled down and clicked **Ajax Security Team**.



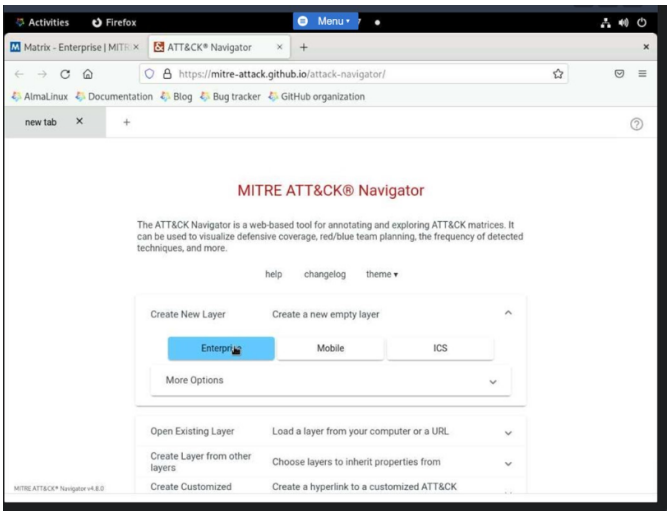
By selecting a specific group I was able to gain more information on the types of exploits the group has conducted on the website

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

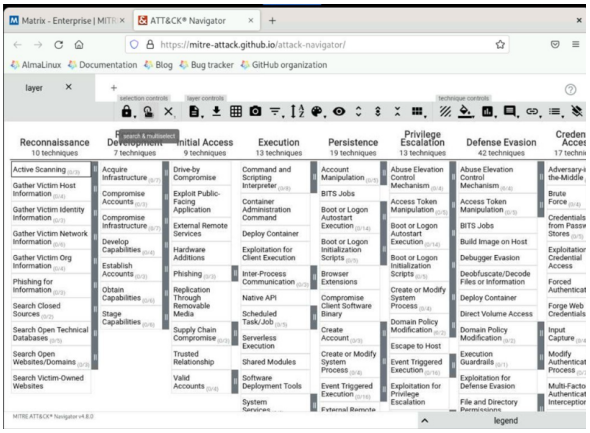


I then clicked the **View on the ATT&CK - Navigator** link in the right pane.

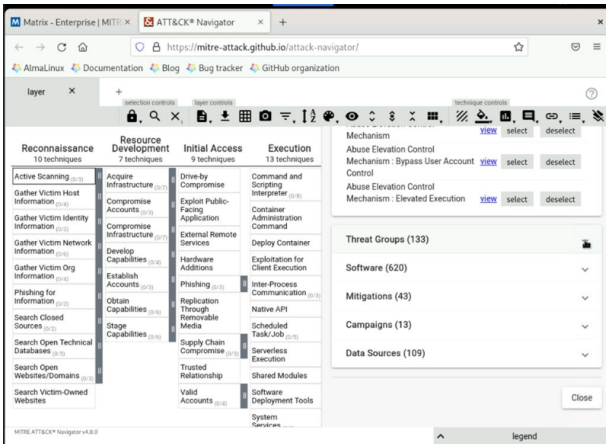
On the **MITRE ATT&CK Navigator** page, select Enterprise in the Create New Layer drop-down menu.



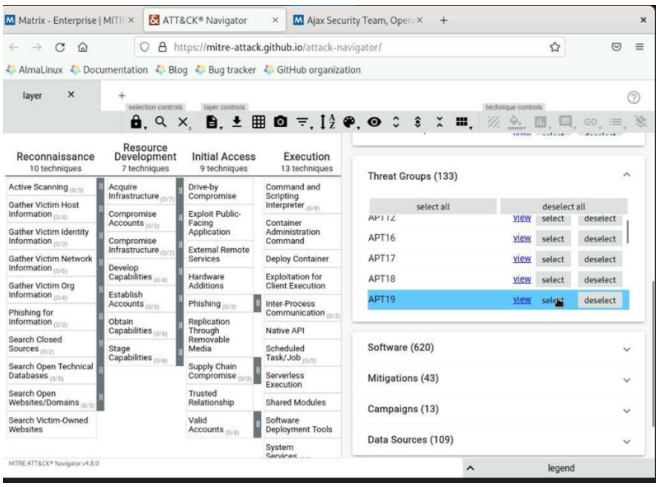
The website opened to a new tab. I selected **Search & Multiselect** from the toolbar menu.



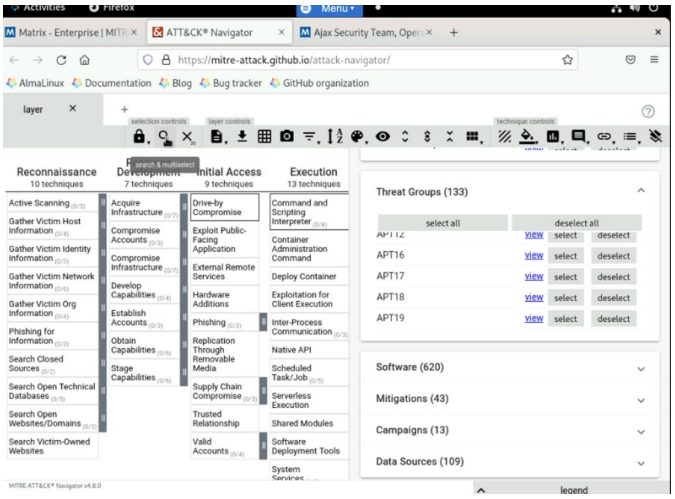
I scrolled down and expanded the **Threat Groups** drop-down menu in the **Search** fly-out menu.



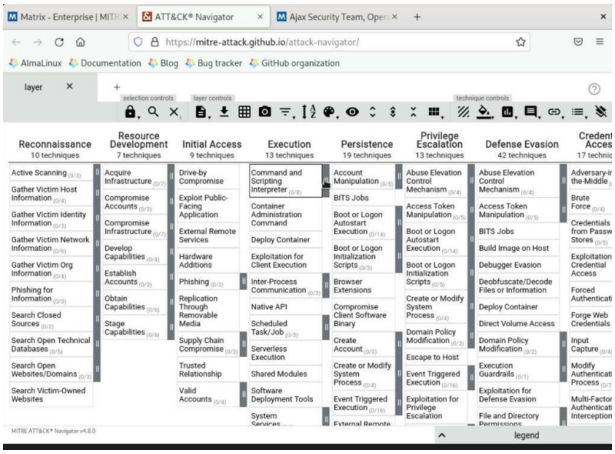
I clicked **Select** next to the **APT19** Threat Group in the Threat Groups pane.



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



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



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.

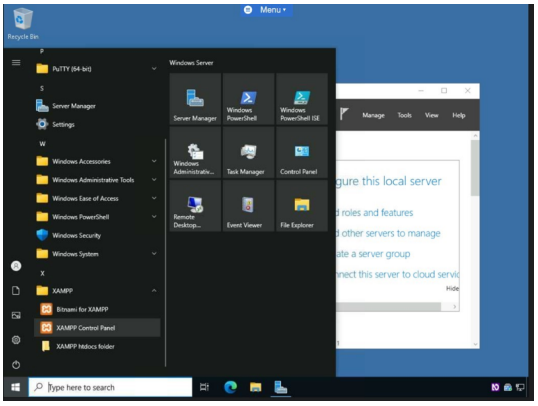
Task 1 - Detecting Web Server Vulnerabilities

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

Step 1

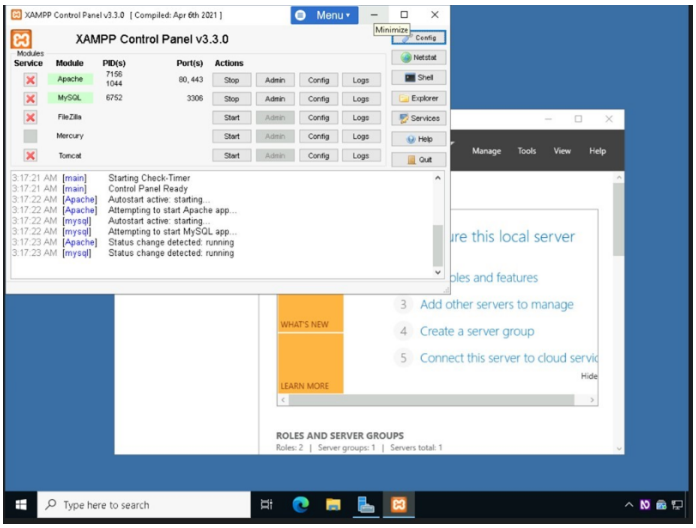
I connected to **ACIDM01.**

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.

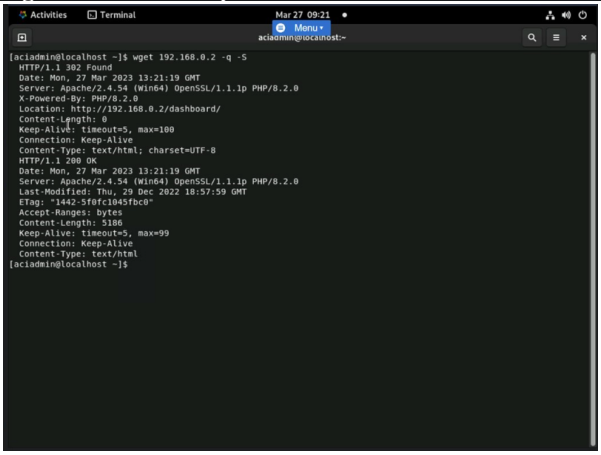


Connected to **ACIALMA (VM).**

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

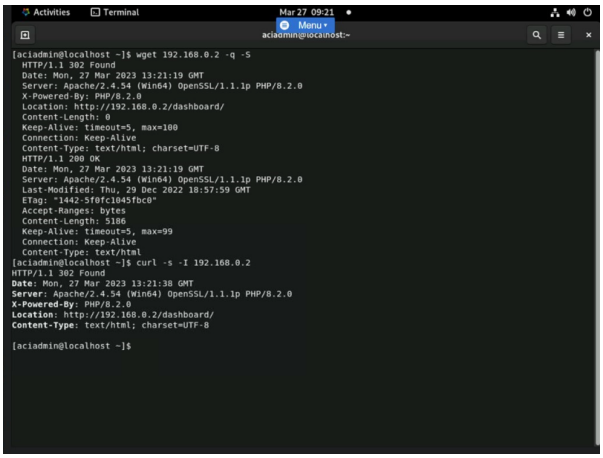
In the **Terminal** window, I typed the following and pressed **Enter**:

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



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

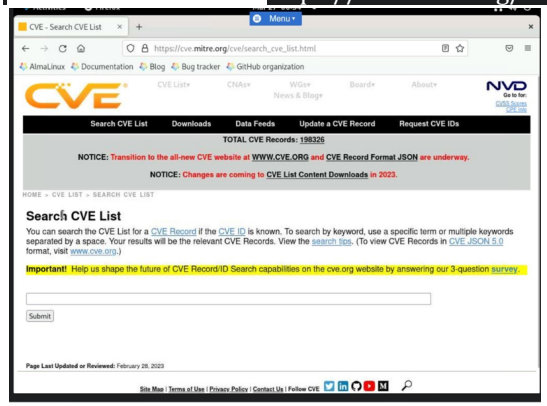
```
curl -s -I 192.168.0.2
```



Curl can also be used to collect web server information

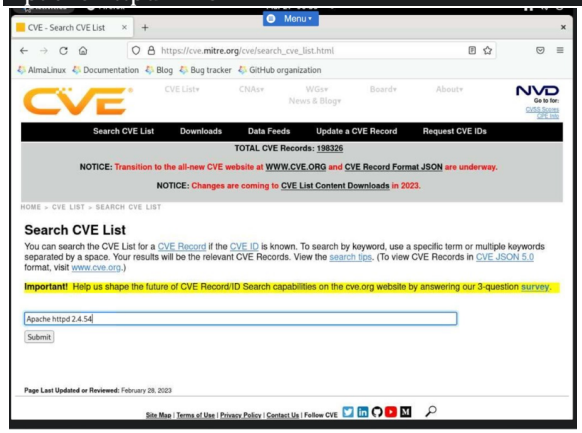
I clicked **Activities** and selected **Firefox**.

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

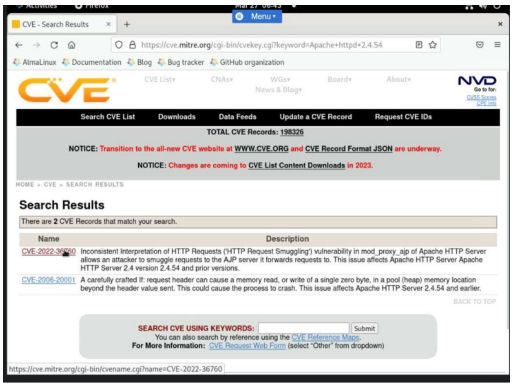


In the **Search CVE List, I** typed the following and pressed **Enter**:

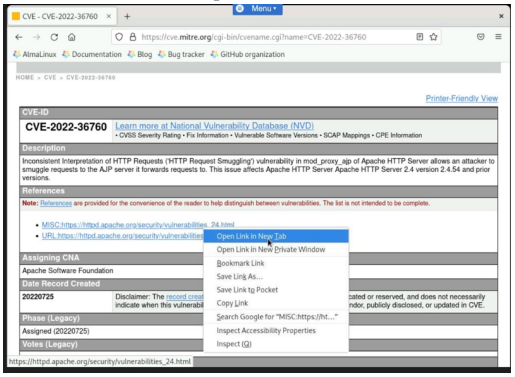
Apache httpd 2.4.54



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



I right-clicked **MISC:https://httpd.apache.org/security/vulerabilities_24.html** URL and selected **Open Link in New Tab**



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