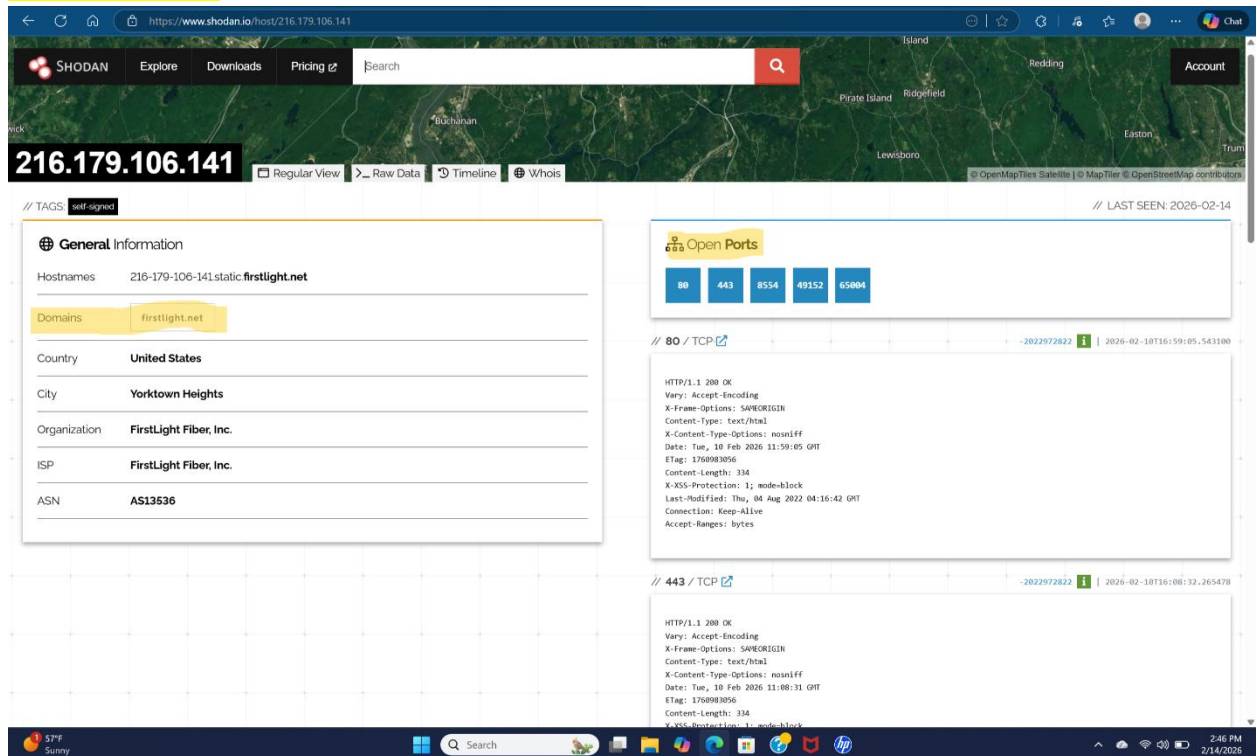


### Lab 3: Passive Reconnaissance

Total Points: 30

**Question 1:** Login to Shodan (<https://www.shodan.io/>) using your Gmail account or any other account you have created with the portal. Search **Web Camera** or **Web Cam** in the search bar, and you will be shown a report where a number of accessible web cameras are listed.

- **Task 1:** Find a device where there is at least one open port and the domain name (URL) is displayed. If you find multiple such devices, just choose one arbitrarily. Take a screenshot highlighting the domain name and the open ports. Attach the screenshot in your submission.



4 points

- **Task 2:** Using WHOIS (<https://who.is/>) or Netcraft (<https://sitereport.netcraft.com/>), find the IP address of the domain name you found in Task 1. Take a screenshot highlighting the IP address and attach it in your submission. Go through the complete report you retrieved from WHOIS or Netcraft. Do some research online about the vulnerabilities or weakness the device has. Briefly describe all the security weakness or vulnerabilities you

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing

found.

The screenshot shows the who.is website interface for a WHOIS domain lookup. The browser address bar shows 'https://who.is/whois/firstlight.net'. The page title is 'WHOIS Domain Lookup'. Below the title, it says 'Look up registration details, contacts, and nameservers for any domain name'. There is a search bar with the placeholder 'Enter a domain name...' and a 'Search' button. The results for 'firstlight.net' are displayed. The WHOIS Information section shows the IP Address: 104.198.111.62. Below this, there are tabs for 'Whois', 'RDAP', 'DNS Records', 'Uptime', 'Diagnostics', and a 'Hide Contact Info' button. A 'Refresh Data' button is also present. To the left of the main content, there is a sidebar with a 'TYPE PHONE NUMBER' section and a 'Search Free' button. To the right, there is a 'Join 50,000+ shareholders' banner. At the bottom, there is a 'Registrar Information' section showing 'Registrar: Tucows Domains Inc.' and 'WHOIS Server: whois.tucows.com'. The bottom of the screenshot shows a Windows taskbar with various application icons and a system tray showing the date and time as 2:59 PM on 2/14/2025.

6 points

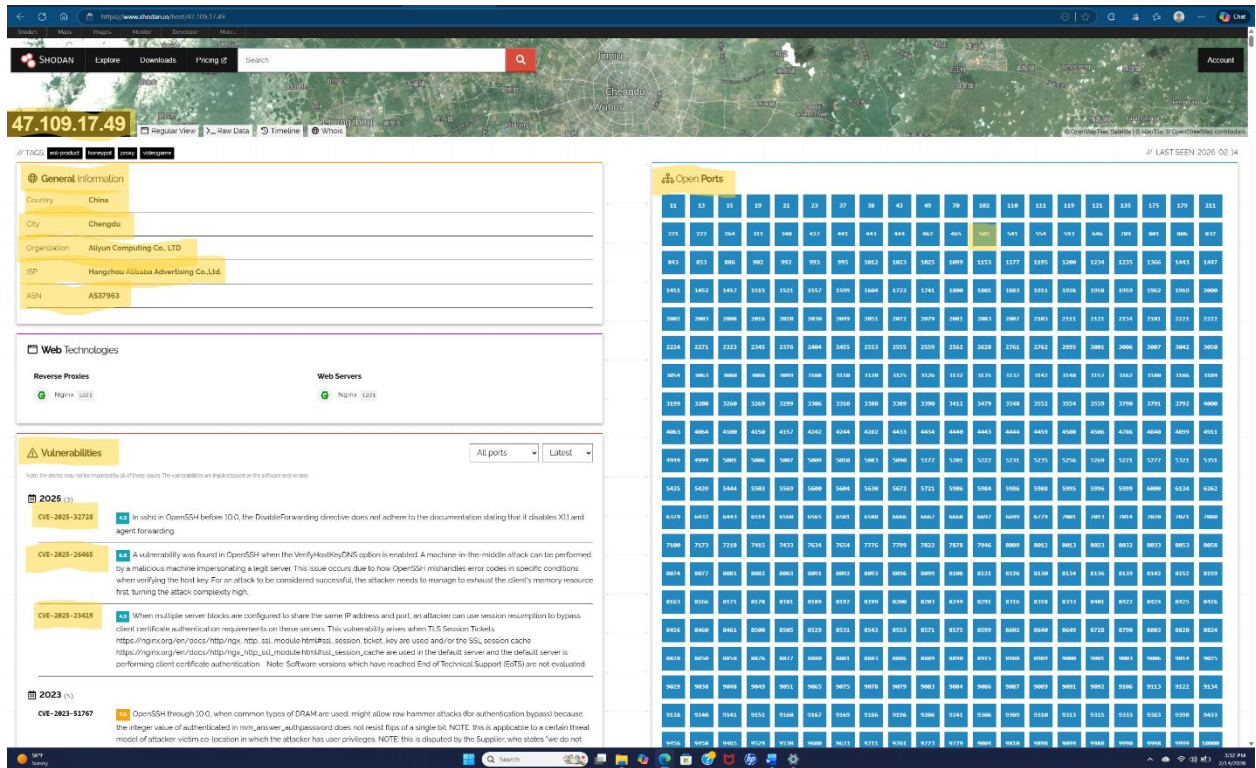
When I looked through the Whois report for Firstlight.net there were no specific vulnerabilities or weaknesses except the basic concerns of public files and records like web server exposure due to a public IP address, DNS and network server risk. I did discover that in September 2025 the company was involved in a ransomware attack by Lynx ransomware group where they threatened to fully leak the companies data unless their demands were met. This event led to the company publicizing their Immutable Backup and Insider Protection capabilities to protect data from such events.

**Question 2:** Login to Shodan again, but this time search for **port:502**. Select a device that meets the following criteria:

1. There is at least some information in the **device identification** field.
2. There is at least one **CVE** listed in the **Vulnerabilities** section.

- **Task 1:** Capture some screenshots showing the device id, open ports, and the CVE lists. Attach the screenshots in your submission.

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing



5 points

- **Task 2:** Do some research about the device you chose and describe the device type and found vulnerabilities in a paragraph. Try to keep the paragraph limited into 5-10 sentences. The IP address 47.109.17.49 is a cloud host server hosted in Chengdu, China as a part of the Aliyun computing company. It is a cloud host server used to run proxy services for testing or trapping message traffic. There are a few CVE notes from 2020-2025, one of which being CVE-2025-26465 which affected OpenSSH. This vulnerability happens when the VerifyHostKeyDNS option is enabled. Which allows A machine-in-the-middle attack to be performed by a malicious machine impersonating a legit server. The issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key where the attacker can impersonate a legitimate server.

5 points

- **Task 3:** Select a CVE from the CVE list shown in the *Vulnerabilities* section and search for that CVE in <https://cve.mitre.org/>. Identify the attack/vulnerability described in the CVE. Go to <https://attack.mitre.org/matrices/enterprise/network/> and find the attack from the matrix. If the attack is not listed there, try to search in other attack matrices given in the MITRE ATT&CK website. Once you find the attack listed as a **technique**, try to find out one relevant **detection** and one **mitigation** methods. Take screenshots showing the detection id and the mitigation id. Attach your screenshots in your submission and

# Old Dominion University

## CYSE 450: Ethical Hacking and Penetration Testing

briefly summarize the selected detection and mitigation methods.

The screenshot displays the MITRE ATT&CK website, specifically the 'Adversary-in-the-Middle' technique page and its associated detection strategies.

**Technique Page: Adversary-in-the-Middle (T1557)**

- Sub-techniques (4):** LLMNR/NBT-NS Poisoning and SMB Relay, ARP Cache Poisoning, DHCP Spoofing, Evil Twin.
- Description:** Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.<sup>[1]</sup>
- Example:** For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirection users from accessing legitimate sites and/or pushing additional malware.<sup>[2][3][4]</sup> Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens (Steal Application Access Token) and session cookies (Steal Web Session Cookie).<sup>[5][6]</sup> Downgrade Attacks can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.<sup>[7][8][9]</sup>
- Procedure Examples:**

| ID    | Name       | Description                                                                                                                                                    |
|-------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C0046 | ArcaneDoor | ArcaneDoor included interception of HTTP traffic to victim devices to identify and parse command and control information sent to the device. <sup>[1][2]</sup> |
| S0281 | Dok        | Dok proxies web traffic to potentially monitor and alter victim HTTP(S) traffic. <sup>[1][3][2]</sup>                                                          |

- Metadata:**
  - ID: T1557
  - Sub-techniques: T1557.001, T1557.002, T1557.003, T1557.004
  - Tactics: Credential Access, Collection
  - Platforms: Linux, Network Devices, Windows, macOS
  - Contributors: Daniil Yugoslavskiy, @yugoslavskiy, Atomic Threat Coverage project; Mayuresh Dani, Qualys; NEC
  - Version: 2.5
  - Created: 11 February 2020
  - Last Modified: 24 October 2025

**Detection Strategies Page: Detect Adversary-in-the-Middle via Network and Configuration Anomalies (DET0296/AN0823)**

- Technique Detected:** Adversary-in-the-Middle | T1557
- Metadata:**
  - ID: DET0296
  - Domains: Enterprise
  - Analytics: AN0823, AN0824, AN0825, AN0826
  - Version: 1.0
  - Created: 21 October 2025
  - Last Modified: 21 October 2025

**Analytics**

Windows | Linux | macOS | Network Devices

**AN0823**

Detects suspicious DNS/ARP poisoning attempts, unauthorized modifications to registry/network configuration, or abnormal TLS downgrade activity. Correlates changes in system configuration with subsequent unusual network flows or authentication events.

**Log Sources**

| Data Component                             | Name                 | Channel                    |
|--------------------------------------------|----------------------|----------------------------|
| Windows Registry Key Modification (DC0063) | WinEventLog:Security | EventCode=4663, 4670, 4656 |
| Network Connection Creation (DC0082)       | WinEventLog:Sysmon   | EventCode=3, 22            |

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing

The screenshot shows the MITRE ATT&CK website with the URL <https://attack.mitre.org/mitigations/M1042/>. The left sidebar lists various mitigation categories, with 'Disable or Remove Feature or Program' highlighted. The main content area is titled 'Disable or Remove Feature or Program' and includes a description: 'Disable or remove unnecessary and potentially vulnerable software, features, or services to reduce the attack surface and prevent abuse by adversaries. This involves identifying software or features that are no longer needed or that could be exploited and ensuring they are either removed or properly disabled. This mitigation can be implemented through the following measures:'. It then lists four implementation measures: 'Remove Legacy Software', 'Disable Unused Features', 'Control Applications Installed by Users', and 'Remove Unnecessary Services'. A metadata box on the right shows 'ID: M1042', 'Version: 1.2', 'Created: 11 June 2019', and 'Last Modified: 10 December 2024'. The bottom of the page shows a Windows taskbar with the date 2/14/2025.

MITRE ATT&CK

Home > Mitigations > Disable or Remove Feature or Program

## Disable or Remove Feature or Program

Disable or remove unnecessary and potentially vulnerable software, features, or services to reduce the attack surface and prevent abuse by adversaries. This involves identifying software or features that are no longer needed or that could be exploited and ensuring they are either removed or properly disabled. This mitigation can be implemented through the following measures:

Remove Legacy Software:

- Use Case: Disable or remove older versions of software that no longer receive updates or security patches (e.g., legacy Java, Adobe Flash).
- Implementation: A company removes Flash Player from all employee systems after it has reached its end-of-life date.

Disable Unused Features:

- Use Case: Turn off unnecessary operating system features like SMBv1, Telnet, or RDP if they are not required.
- Implementation: Disable SMBv1 in a Windows environment to mitigate vulnerabilities like EternalBlue.

Control Applications Installed by Users:

- Use Case: Prevent users from installing unauthorized software via group policies or other management tools.
- Implementation: Block user installations of unauthorized file-sharing applications (e.g., BitTorrent clients) in an enterprise environment.

Remove Unnecessary Services:

- Use Case: Identify and disable unnecessary default services running on endpoints, servers, or network devices.
- Implementation: Disable unused administrative shares (e.g., CS, ADMIN\$) on workstations.

ID: M1042  
Version: 1.2  
Created: 11 June 2019  
Last Modified: 10 December 2024  
[Version Permalink](#)

My technique according to the described CVE of a OpenSSH is a machine-in-the-middle attack which aligns with an adversary- in-the- middle attack (T1557). The detection strategy DET0296 Detect Adversary in the middle attacks through network and configuration Anomalies like AN0823 which delete suspicious DNS poisoning attempts and abnormal networks. Mitigation is the M1042 which disables and removes programs. Once you configure properly the DNS will remove the vulnerable feature.

- **10 points**