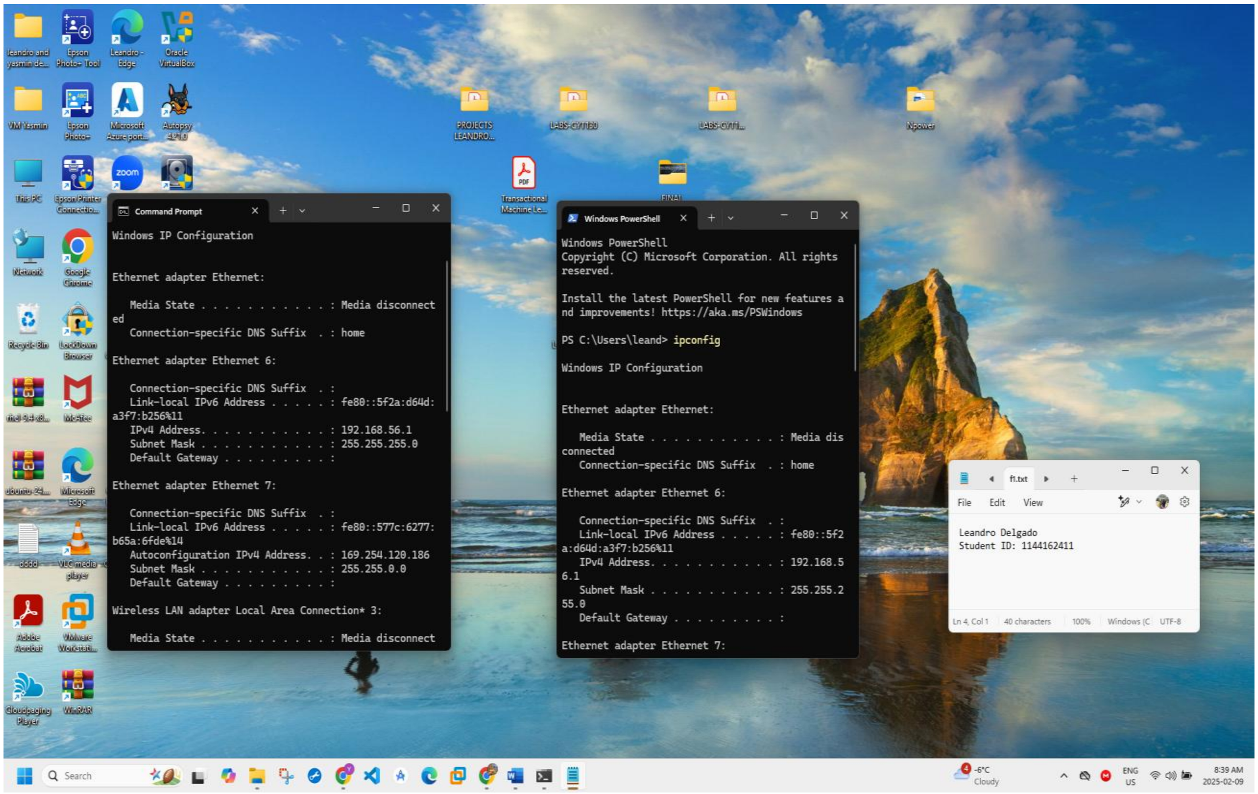
Lab 4- MITRE Cyber Analytic Repository (CAR-2021-01-001)

Elaborated by:
Leandro Delgado
114416241

Tatiana Outkina
CYT-250/Threat Investigation

I hereby confirm that this submission is my original work and complies with Seneca College's Academic Integrity Policies.



```
Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnect
ed
   Connection-specific DNS Suffix  . : home

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5f2a:d64d:
a3f7:b256%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 7:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::577c:6277:
b65a:6fde%14
   Autoconfiguration IPv4 Address. . : 169.254.120.186
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnect
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights
reserved.

Install the latest PowerShell for new features a
nd improvements! https://aka.ms/PSWindows

PS C:\Users\leand> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media dis
connected
   Connection-specific DNS Suffix  . : home

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5f2
a:d64d:a3f7:b256%11
   IPv4 Address. . . . . . . . . . . : 192.168.5
6.1
   Subnet Mask . . . . . . . . . . . : 255.255.2
55.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 7:
```

```
Leandro Delgado
Student ID: 1144162411
```

CYT250 Lab4 Winter 2025 – 4%

Individual work

Your task:

- **You see below the List of Cyber Analytics which is given to your review and practice. The samples are different in terms or required technical skills.**
- **Review the list of samples of CAR cases below. Select a sample for your work. At the end, you should be able to simulate the issue and run detection implementation on your own computer.**

Your workflow:

Perform the following activities on your own identified sample. Note, that all information required to complete Part 1 and Part 2 is available in the CAR document you have selected. Just read, understand, and say in your own words.

Part 1. Review the selected case documentation and make your own description in a structured manner to address:

- **What is a *hypothesis* which explains the idea behind the given analytic?**

Based on the list provided by the instructor, I decided to focus on **CAR-2021-01-001:** Identifying port scanning activity. This is a recognized technique used by adversaries to not only identify open ports but also services as targets on a machine or network. If an unusual number of connection attempts to different ports is detected within a short time, it may indicate an automated scanning activity, possibly by an attacker looking for vulnerabilities.

- **What is the *information domain* or the primary domain the analytic is designed to operate within (e.g. host, network, process, external)?**

In this analysis, you work in the network domain which focuses on monitoring network traffic rather than files, processes, or user activity on a particular computer. By watching incoming and outgoing connections, you look for patterns that indicate a scan is happening. This is useful for firewalls, intrusion detection systems (IDS), and security monitoring tools like Suricata, Zeek, or Splunk.

- **What is the Analytic type?**

This analysis is focused on anomalies that detect behavior that is considered unusual such as: frequent failed connection attempts, meaning there is a significant increase in failed connection attempts coming from a known or trusted source. This is useful considering that attackers often try to use tools that allow them to hide their scan times randomly but, maintaining an anomaly-based approach that allows them to be detected over time.

- **What are tactics and techniques that the analytic detects?**

This analytic helps detect early signs of an attack by spotting reconnaissance activity. It aligns with MITRE ATT&CK techniques. Specifically, through active scanning T 1595 which allows attackers to scan networks for open ports or services that are running before carrying out an attack or instruction. It also emphasizes network discovery such as (T1046) which helps criminals to be able to map a network and thus design their next intrusion steps. In general, these scans provide a useful tool to identify different types of port scans that attackers use to evade detection. An example of this is easily found in a SYN scan, which is a quick and stealthy way of checking open ports without establishing a full connection, while through a UDP scan it allows intruders to identify open services that do not require a handshake such as DNS or SNMP. It is important to mention that today it is possible to access advanced scanning tools such as XMAS, which manipulate packet flags to avoid security tools. Finally, we have the FIN tool, which tries to trick firewalls by sending unexpected termination packets. By detecting this type of activity considered suspicious or unusual early on, it allows security teams to intervene before a failure occurs in a fast and real time, seeking to block all the actions that an attacker can perform and thus strengthen the networks.

- **What threat management processes are covered by the selected analytic?**

This analysis is useful in several ways. First, through detection, it helps spot an attack early, which buys the time needed to implement containment actions long before a criminal tries to break in and breach security. Second, through investigation, security teams can scan the logs to identify where the scan originated and what its main target was. Third, through mitigation, once the scan is confirmed, both firewalls and security tools can block attackers' IP addresses to prevent them from causing significant damage. Finally, companies can automate alerts on intrusion detection systems to stop repeated scan attempts by attackers.

- Based on the technique description, do threat modeling for the given case. To the best of your ability, follow the structure from the slide 4 of the weekly PPP:
    - **Entry points**

In this first step, attackers start scanning from the internet, trying to find public-facing servers with weak spots. Inside the network – If they have already gained access, they continue scanning to find internal systems that can be exploited. Finally, if a compromised device is accessed, such as a printer, IoT device, or an old PC in the company, it can be used to scan the network.

- **Potential attack goals**

It is interesting to see the behavior of attackers once they have performed the scan, as they determine which ports are open, for example: SSH, RDP, or a database that could be exposed. They also analyze the services that are being executed and if they have an old version of Apache where they could detect a vulnerability or, ultimately, if there is a weakness in the passwords. Basically, these aspects are meticulously analyzed by attackers to gain valuable information and exploit a system.

- **Vulnerabilities that can be exploited**

We could say that one of the weaknesses found are the weak rules of the firewalls, in case this does not have limits the attackers can probe your entire system. Without an instruction detection system, the scans would go unnoticed. Through the default configurations some systems expose the ports and these are never blocked. Finally, having old versions of software the attackers look for services running outdated software with known security flaws.

- **Terms and conditions required to achieve the goal**

For an attack to be successful, certain conditions must exist:

- ✓ The target network must have open ports and running services.
- ✓ There must be no active monitoring (e.g., an IDS like Suricata or Snort).
- ✓ The firewall must allow repeated connections from unknown sources.
- ✓ The attacker must remain undetected long enough to complete their scan.

- **Potential attack paths (tactics/technics)**

First, the criminal starts scanning the targeted network using tools like Nmap or Masscan. Second, multiple port connection attempts are detected in a short period of time through analysis. Third, security tools determine any irregular behavior in the scan performed. Fourth, if verified, the attacker's IP address can be blocked or investigated for valuable information. Lastly, preventative actions are taken through firewall rule adjustments or monitoring for suspicious traffic.

Summary:

Port scanning is a warning sign of an attack, and this analytic helps detect it by monitoring network traffic for unusual connection spikes. Instead of relying on known attack patterns, it identifies anomalies, making it effective against stealthy threats. By recognizing tactics like Active Scanning (T1595) and Network Service Discovery (T1046), it spots attackers probing for open ports. The best defense is active monitoring, blocking suspicious IPs, and using tools like Suricata, Zeek, or SIEMs to stop them before they can exploit vulnerabilities.

Part 2. Based on the CA documentation, proceed from the threat model to CA - apply CA methodology (Slide #20 from Week5 PPP):

Once a threat model has been created, it's time to put it into action and understand how we can detect and respond to port scanning using the Cyber Analytic (CA) methodology. This means defining what we're looking for, how we detect it, and what we do when we find it.

- **What is a context-dependent threat model**
  - Think about how to determine legitimate activities from malicious ones in your case

Before identifying any attack, it is critical to identify the normal network behavior of a particular unusual activity. Not all connections necessarily indicate malicious intent, so security teams must define ways to classify legitimate traffic from threats that may be potentially harmful. A normal user may access a few services such as email, web, or internal systems while an attacker will try to connect to thousands of ports in a short period of time looking for vulnerabilities. If a system repeatedly fails to connect to several ports, it may indicate that it is a scan rather than a normal use by some users. The challenge here is to determine how many failed port connections should trigger an alert so that timely security measures can be guaranteed that they are effective and efficient.

- **Describe Data Model for your selected case**
  - What traces (IOCs) of the attack you will be looking for?

To perform port scanning detection, you need to focus on certain patterns in network traffic.
What exactly you need to scan:

- ✓ You need to know the number of attempts executed from the same source.
- ✓ Failed connections that show that the attacker is trying to access the ports.
- ✓ Connectivity to a high number of ports in a short period of time.

- ✓ An unexpected increase in SYN packets.
- ✓ Number of unknown or external IPs that behave in this way.

It is important to be able to identify between a normal network scan and a scanning attack since this will determine the actions to be taken to minimize damage

- **What are the potential sensors**
    - What tools can be used to capture IOCs

Detecting port scans requires tools that monitor network traffic and spot anomalies in real time. Snort helps trigger alerts for known scanning behavior while Wireshark provides deep traffic analysis. Also, Suricata works on network instruction to detect scan patterns and Zeek allow a better network security monitoring to identify unusual network activities, The key here is that choosing the right tool for the network size and security needs will keep systems out of harm's way.

- **Comment a pseudocode description of how the analytic might be implemented (if applicable).**

The basic vision is to monitor network traffic to detect connection attempts. This makes it essential to be able to know the different port number that an IP address accesses. Once the port count is verified and exceeds the established standard number, it would be marked as suspicious, and an investigation would be established to determine how many are normal and how many are considered suspicious to apply preventive actions.

- **Comment a unit test which can be run to trigger the analytic (if applicable)**

To verify the analysis, I must simulate the port scan and check if it can be detected. The process to be performed is as follows:

- ✓ The test configuration is established using a virtual machine in this case it would be Kali Linux. Then the scan is executed through a basic command such as (Nmap -p 1 -1000-T4 <target Ip>).
- ✓ Run a stealthy SYN scan to obtain the number of unusual events or records detected within the connection.

- **Comment any other information included into your sample, e.g. mitigating technique, etc.**

Once a port scan is initially detected, organizations must take action to block potential attacks that put their information at risk. Firewall rules can help block IP addresses that trigger scan alerts while rate limiting the number of connections an IP can make per second. Honeypots help trick attackers into directing them to ports with fake services, which helps reveal the tactics they use for their attacks. The logs these actions generate are analyzed to understand their attack patterns and develop a better defense against these types of tactics. The best response to an attack is to have immediate response actions in place to safeguard the integrity of the systems.