SOC Home Lab

By

Abdelrahman Magdy Gouda

LinkedIn:

https://www.linkedin.com/in/abdelrahman-magdyy/

Table of Contents

Introduction

In today's cybersecurity landscape, defending an organization from advanced threats requires continuous monitoring, detection, and response capabilities. A Security Operations Center (SOC) provides these capabilities, leveraging real-time data and analysis to safeguard critical systems. To understand the SOC workflow and how attackers exploit vulnerabilities, a home lab simulation was deployed on AWS.

This lab includes the following key components:

- **Windows Server**: Victim machine for the attack.
- **Splunk**: SIEM solution for monitoring and log analysis.
- **Mythic C2**: Command and Control server used to manage the attack.
- **Kali Linux**: Attacker machine used for reconnaissance and exploitation.

The scenario simulates a real-world attack involving multiple phases, from information gathering to data exfiltration. This report documents the steps taken in each phase, illustrating how an attacker can exploit misconfigurations and gain control over a Windows Server while evading detection.

SOC Home Lab

2-Lab Topology

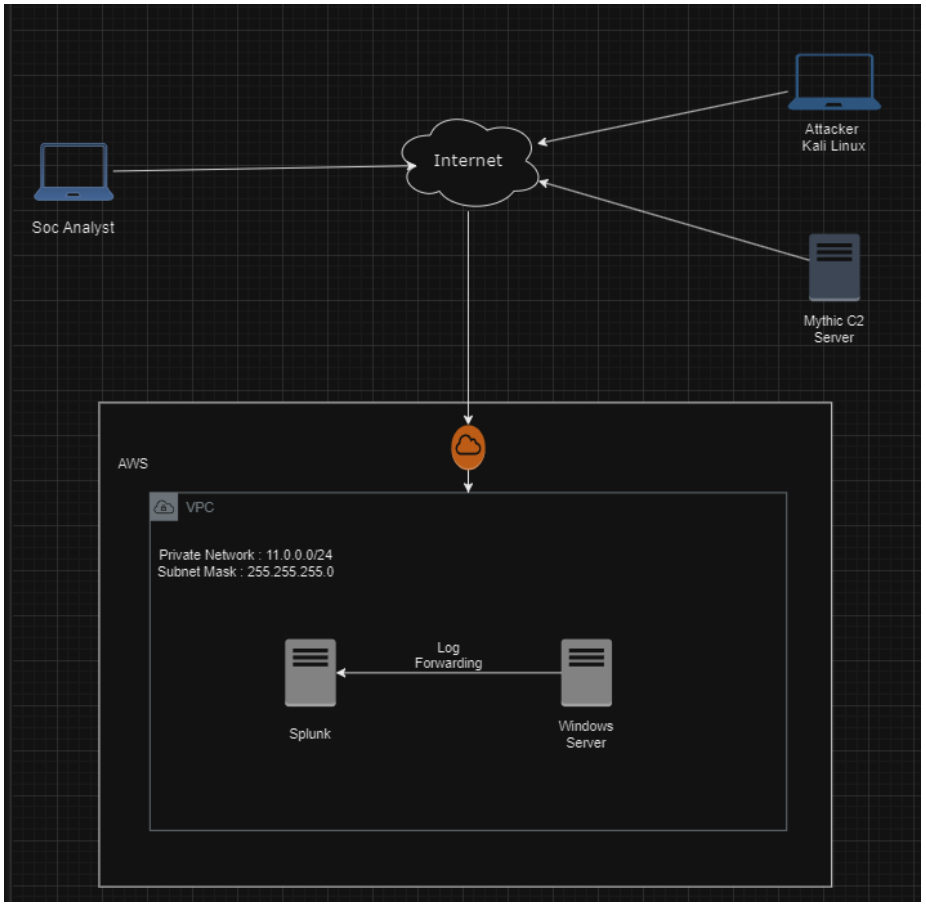
This lab is deployed on AWS, and it consists of:

1- Kali Linux (Attacker)

2- Mythic C2 Server (Command & Control Server)

3- Splunk (SIEM Solution)

4- Windows Server 2022 (Victim)

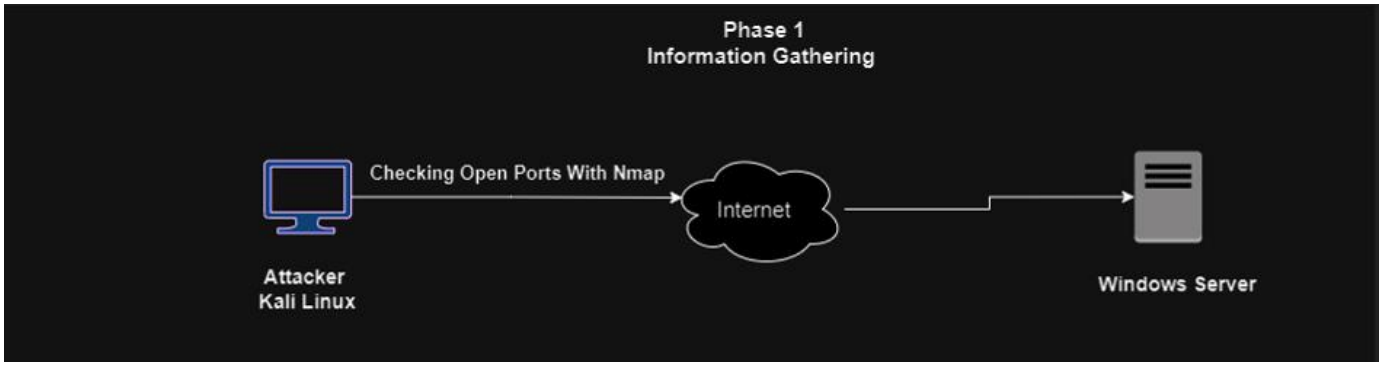


3-Attack Scenario Breakdown

Phase 1: Information Gathering

The attacker starts by identifying potential entry points. Using **Nmap** from the Kali Linux machine, the attacker performs a port scan on the Windows Server to discover open ports. After analyzing the scan results, the attacker finds that **Remote Desktop Protocol (RDP)** is open on the server.

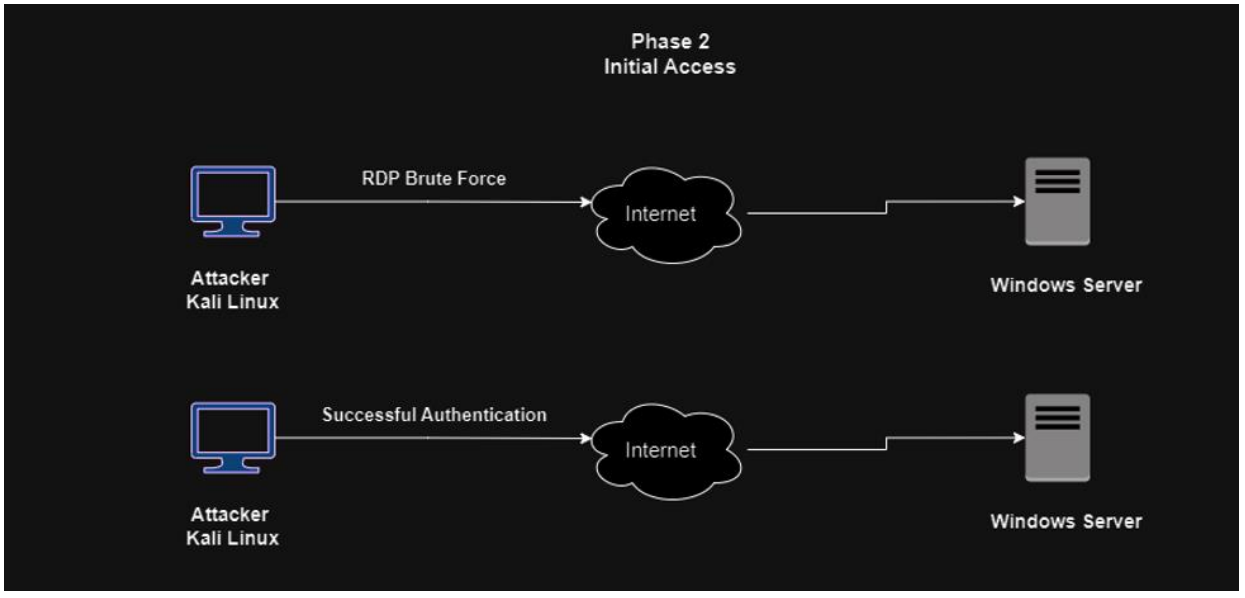
- **Tools Used**: Nmap
- **Objective**: Identify open ports on the Windows Server.



Phase 2: Initial Access

With the RDP port open, the attacker launches an **RDP brute-force attack** to guess the administrator's password. After multiple attempts, they successfully authenticate and gain access to the Windows Server.

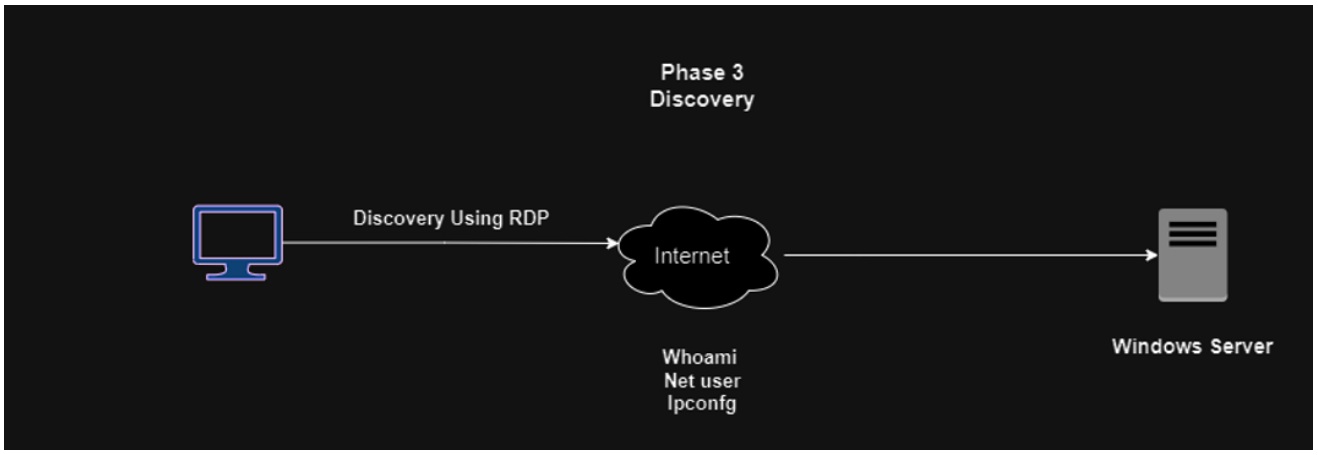
- **Tools Used**: Crowbar
- **Objective**: Exploit weak RDP credentials to gain unauthorized access.



Phase 3: Discovery

Once inside the Windows Server, the attacker leverages basic commands such as whoami, net user, and ipconfig to gather information about the machine, its users, and its network configuration. This helps in formulating the next steps of the attack, ensuring further access and privilege escalation.

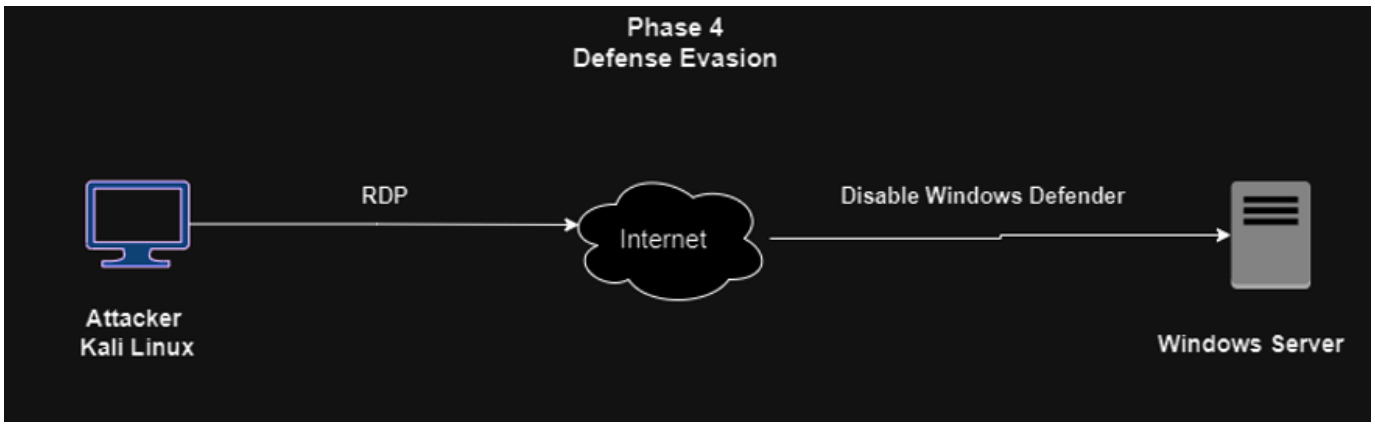
- Tools Used: Built-in Windows commands (whoami, net user, ipconfig)
- Objective: Gather internal information for further exploitation.



Phase 4: Defense Evasion

To evade detection by the server's security mechanisms, the attacker disables **Windows Defender** using the RDP session. This ensures that future malicious actions, including malware installation, remain undetected.

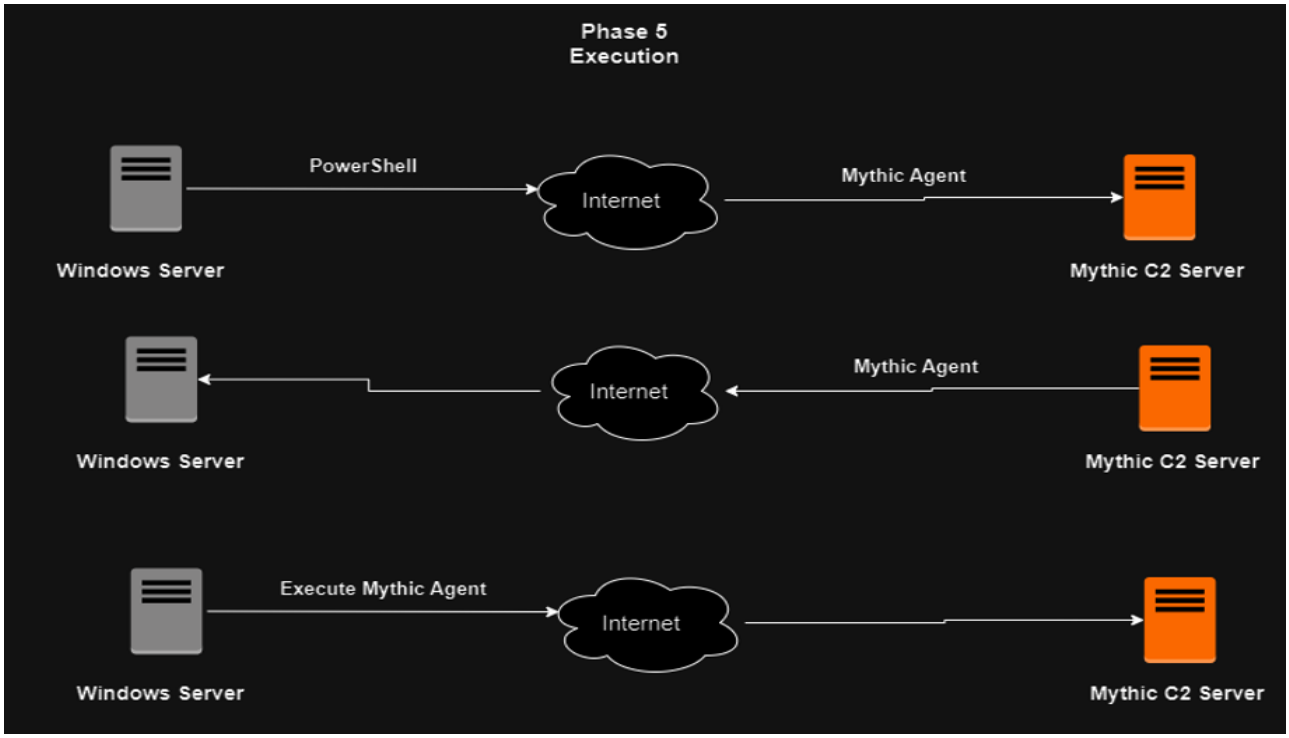
- **Commands**: Disabling Windows Defender via PowerShell or manual configuration
- **Objective**: Evasion of endpoint protection measures.



Phase 5: Payload Execution

The attacker proceeds by crafting a payload on the **Mythic C2 Server**. Using **PowerShell**, the attacker remotely downloads and executes the payload on the Windows Server. This establishes a persistent backdoor on the target machine, allowing continuous access.

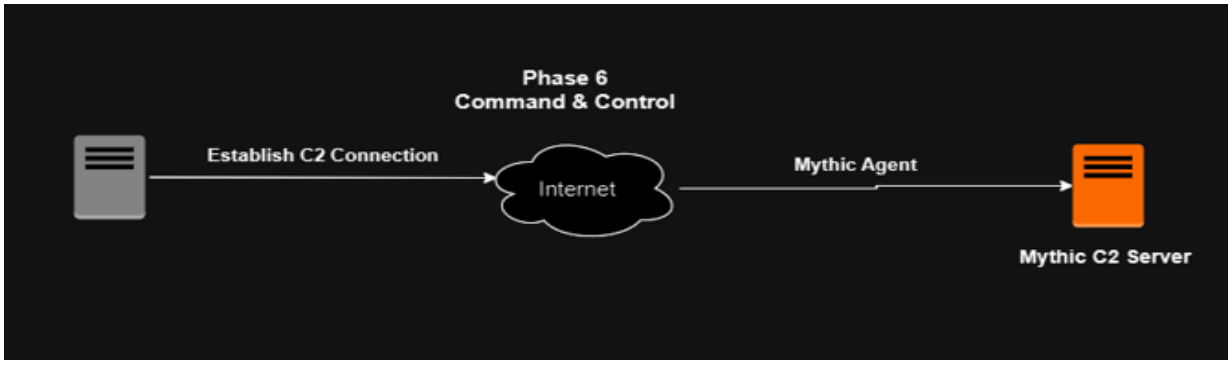
- **Tools Used**: Mythic C2, PowerShell
- **Objective**: Gain persistent access to the compromised server.



Phase 6: Command & Control (C2)

Once the payload is executed, an open session is established between the Windows Server and the Mythic C2 server. The attacker can now control the server remotely, issuing commands and gathering sensitive information.

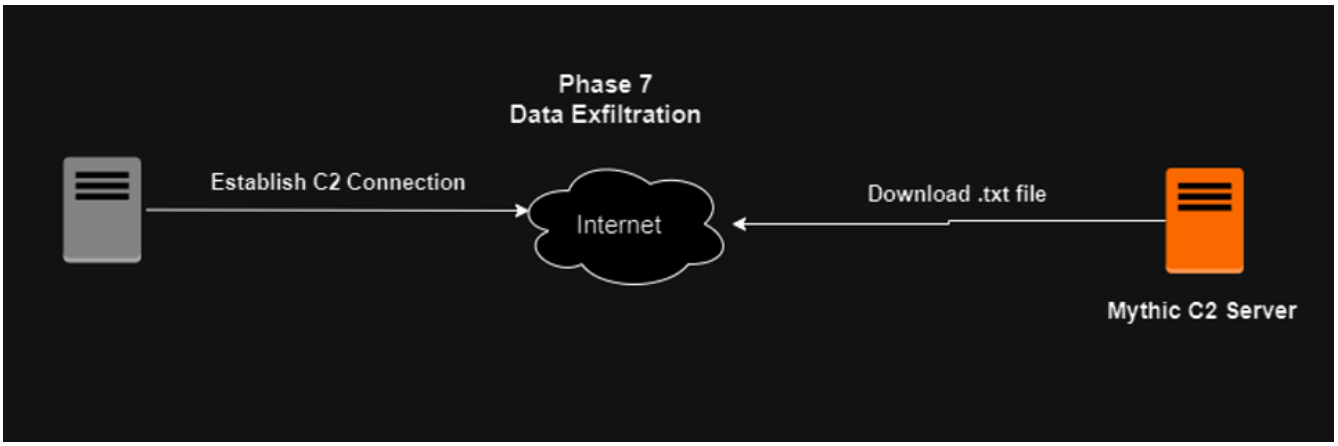
- **Tools Used**: Mythic C2
- **Objective**: Maintain control over the Windows Server.



Phase 7: Data Exfiltration

Finally, the attacker identifies a sensitive file (passwords.txt) on the Windows Server. Using the established C2 session, the file is exfiltrated to the C2 Server.

- **Tools Used**: Mythic C2
- **Objective**: Extract sensitive information from the server.



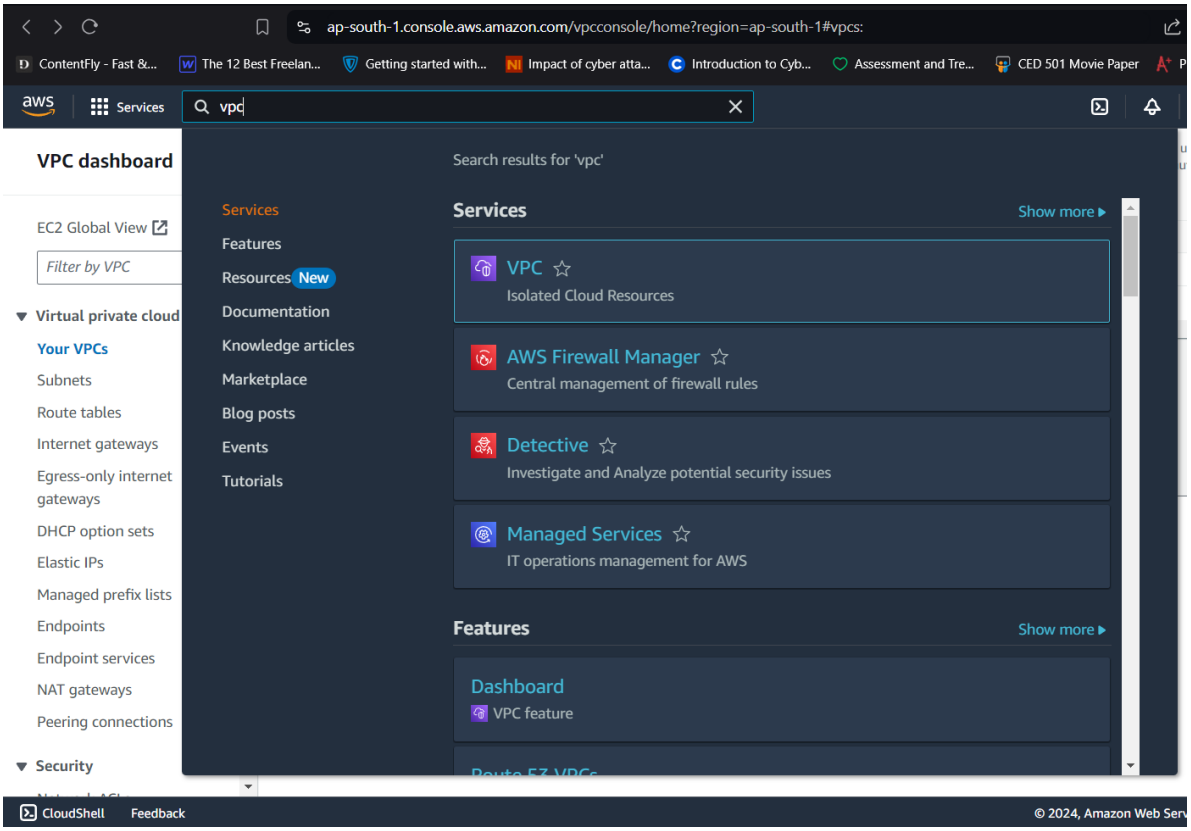
4-Windows Deployment

I will start by creating the VPC that our machines will be placed in.

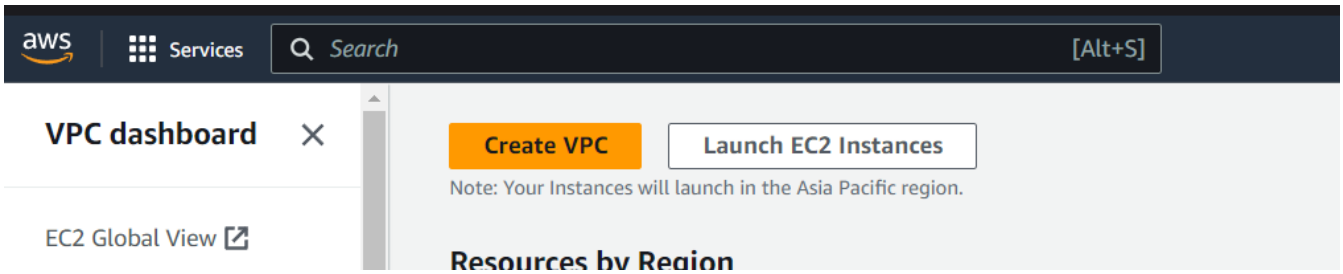
Steps

First

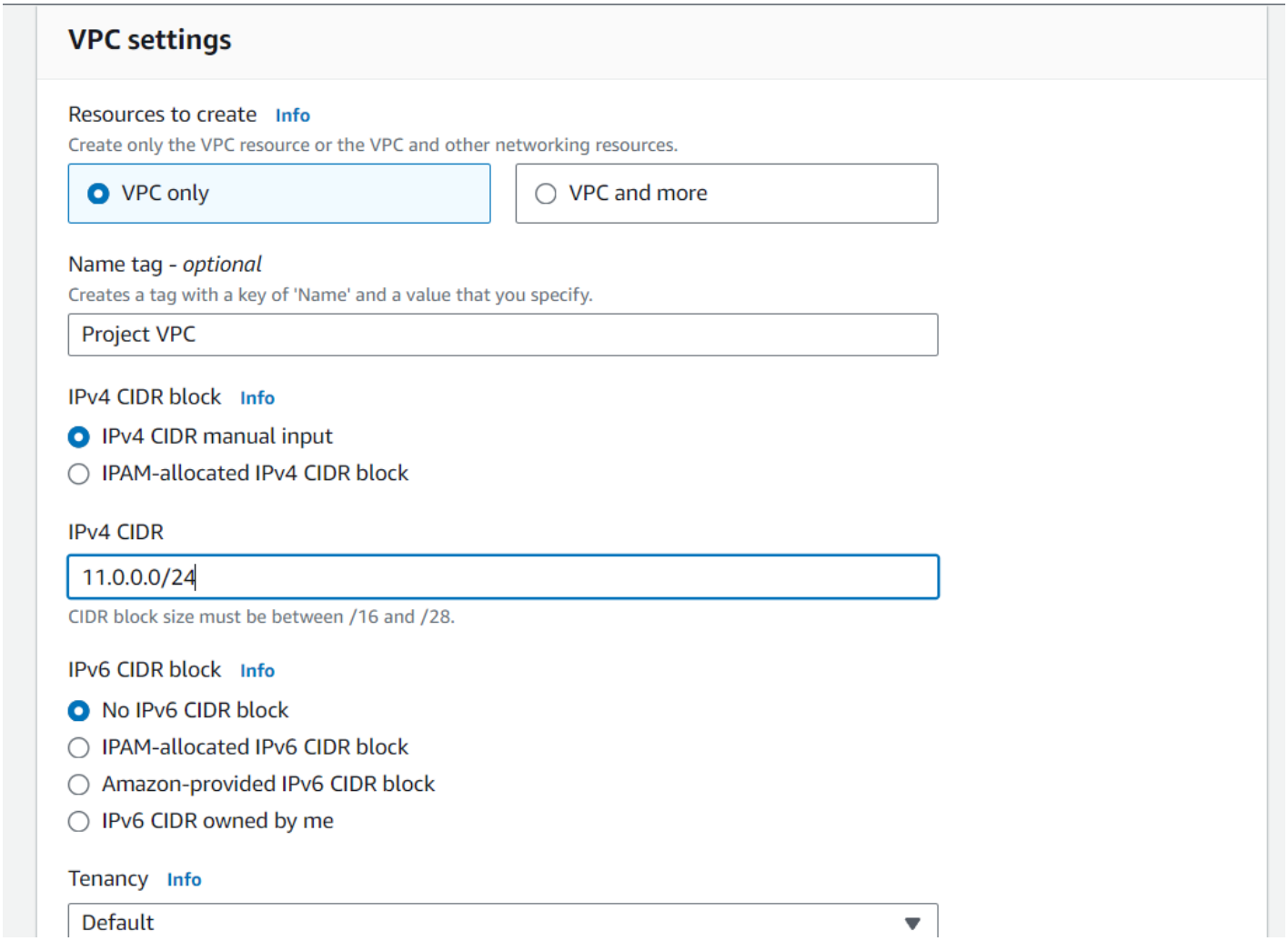
1- We login into our AWS account and Search for VPC



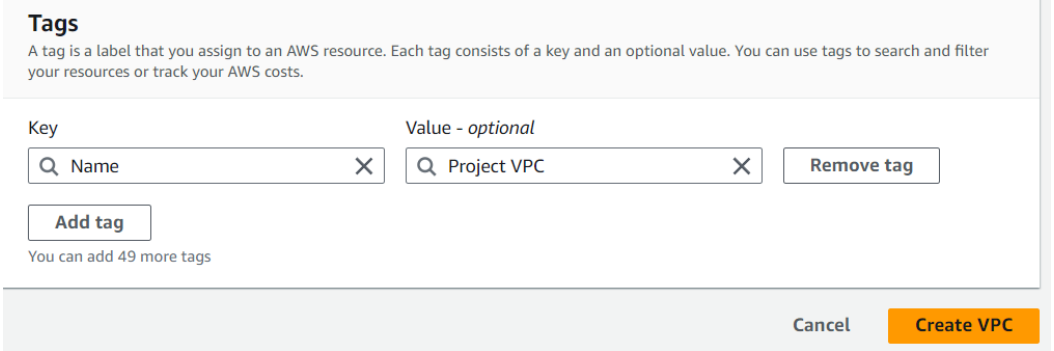
2- Click on VPC then click on ‘Create VPC’



3- Configure our VPC

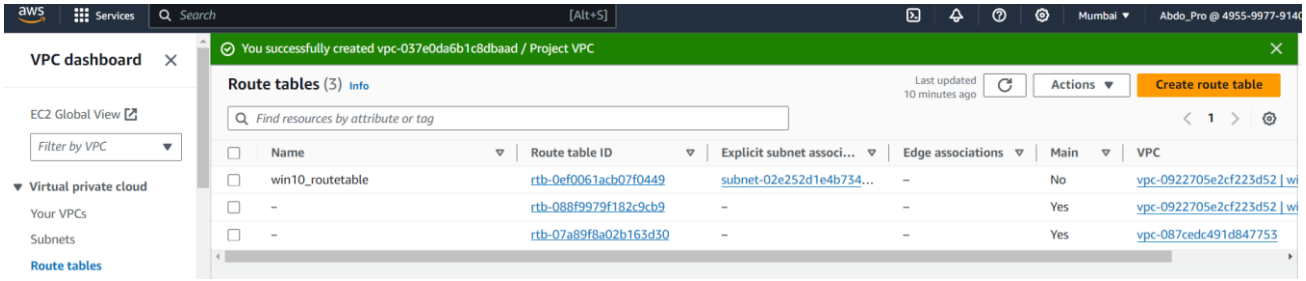


4- Then, click on **Create VPC**

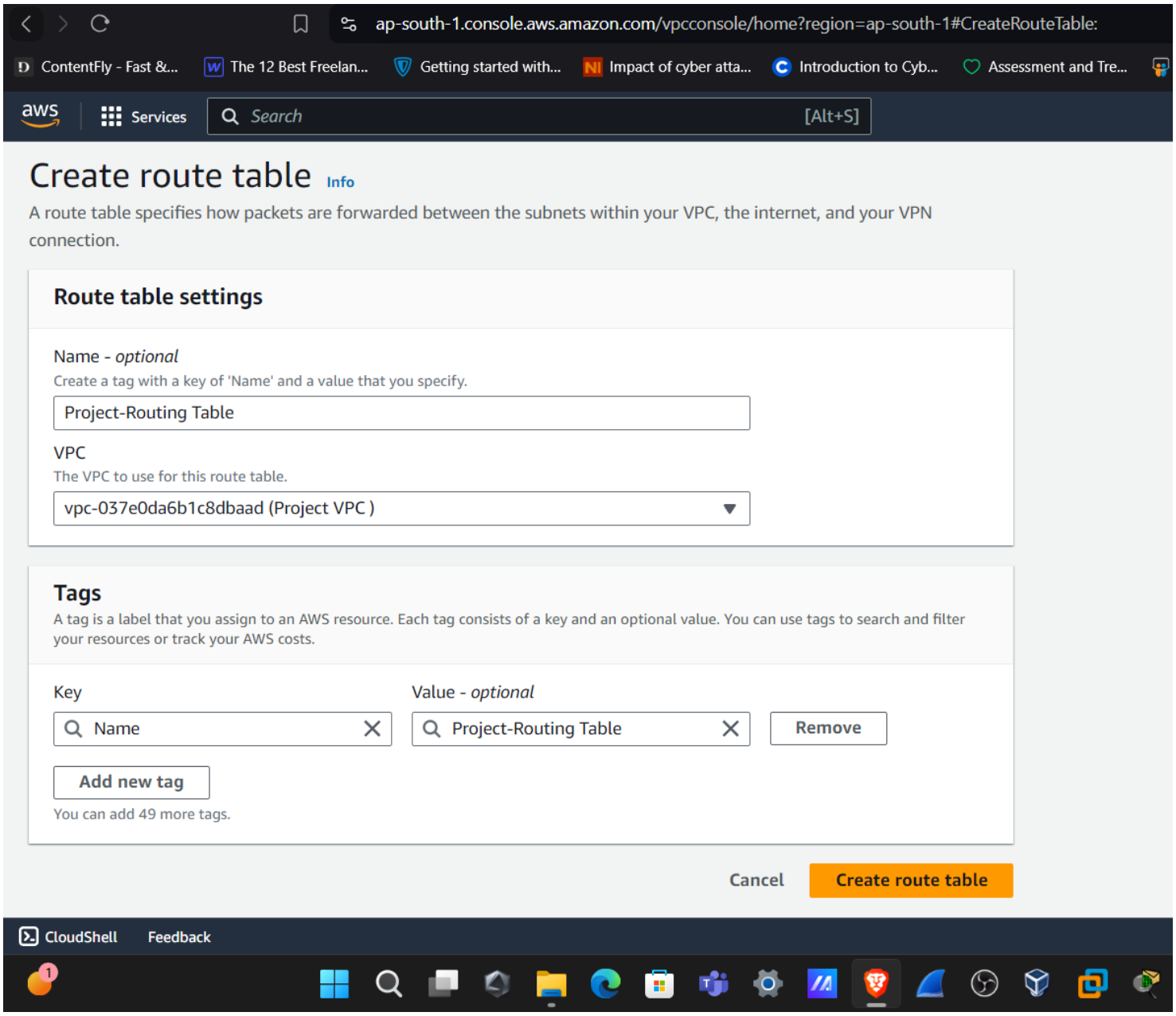


Second

1- Create our Routing Table, to direct our network traffic

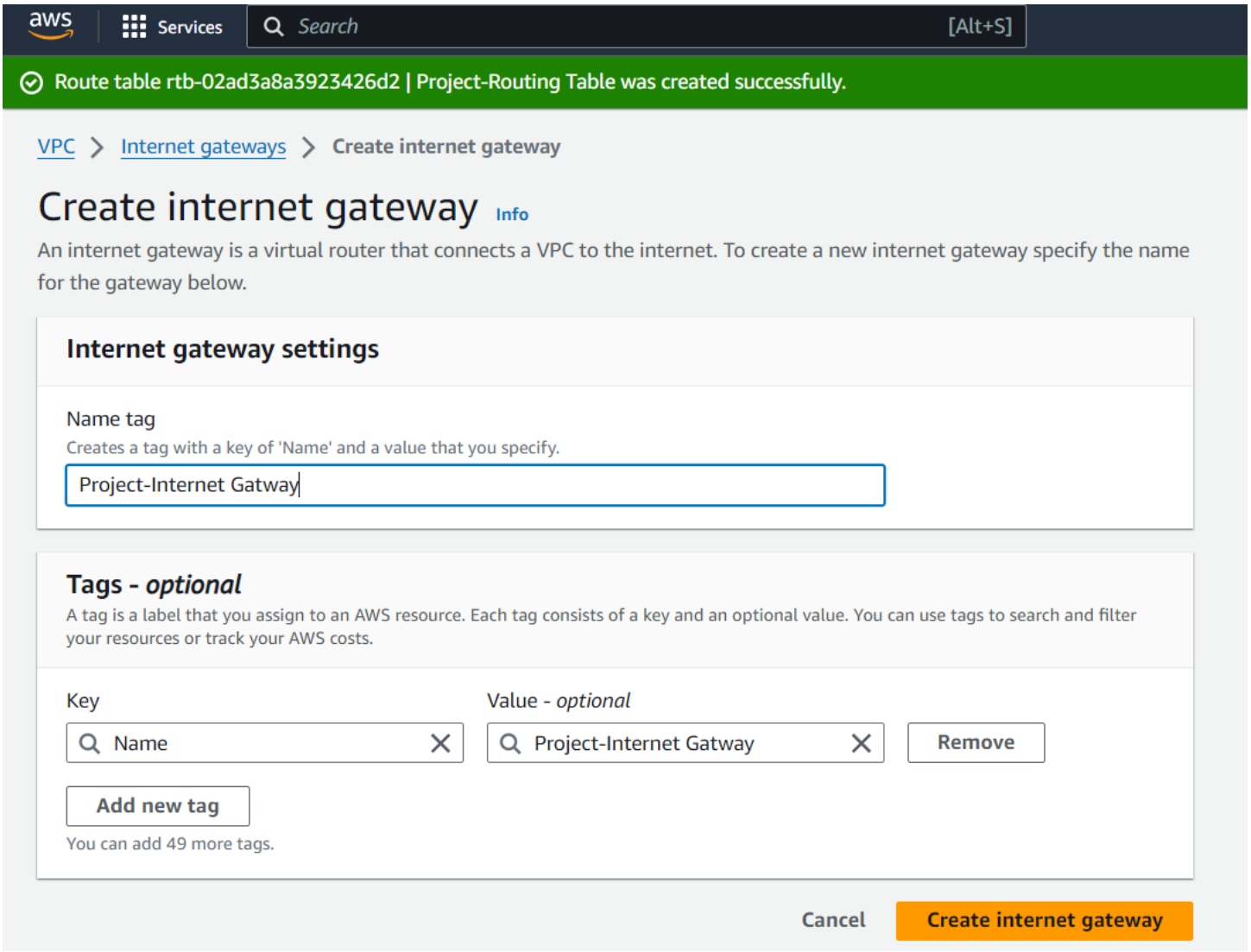


2- Configure Route table and then click on **Create route table**

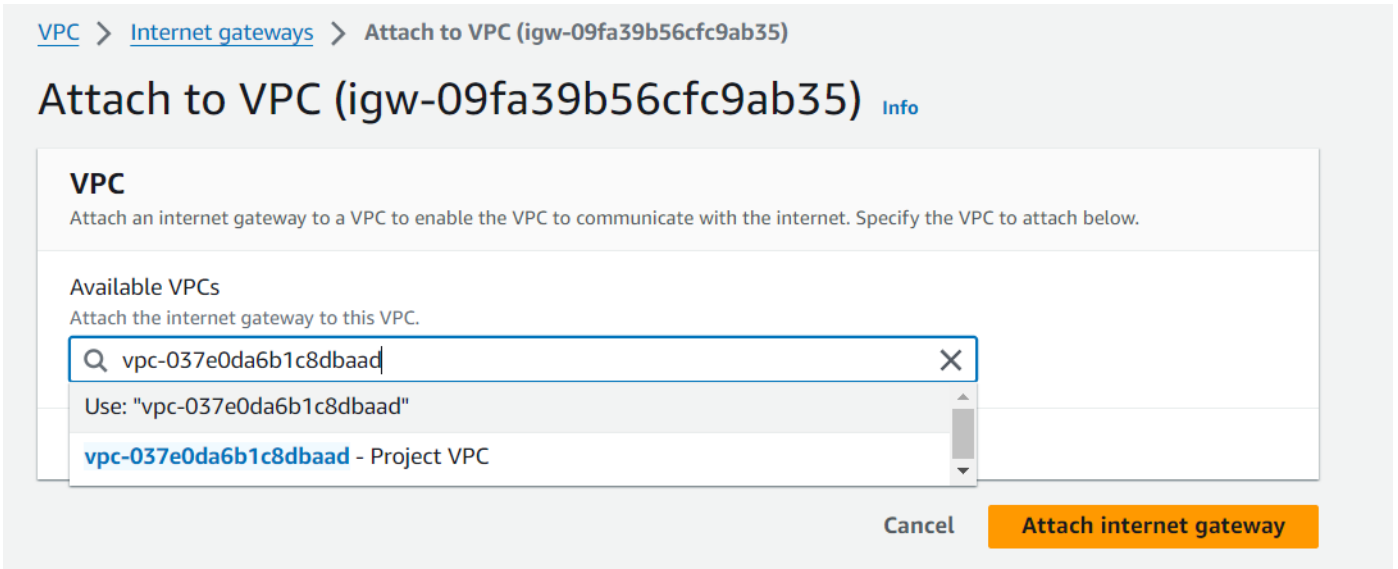


Third

1- Create Internet Gateway



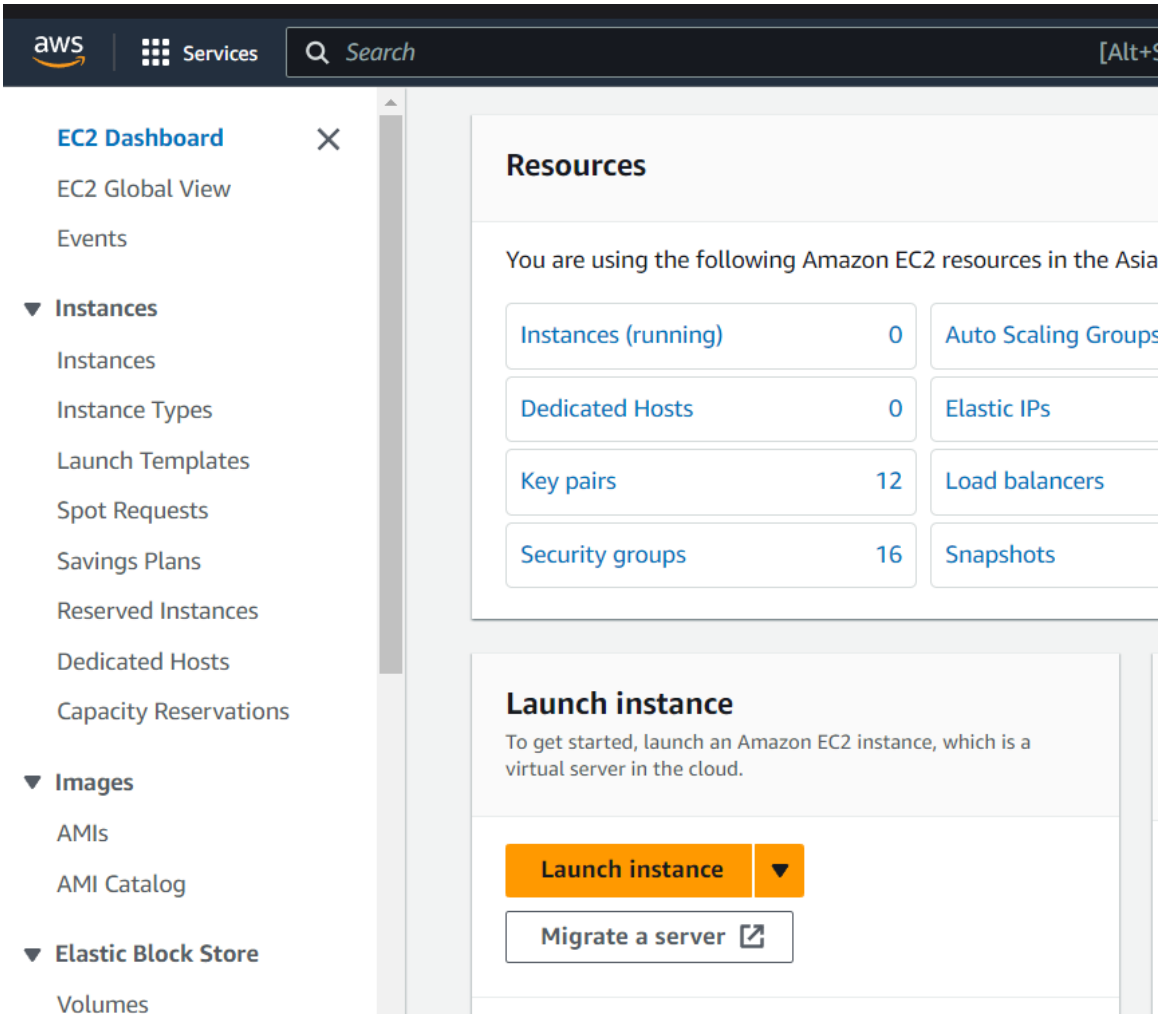
2- Attach it to our VPC (Project VPC)



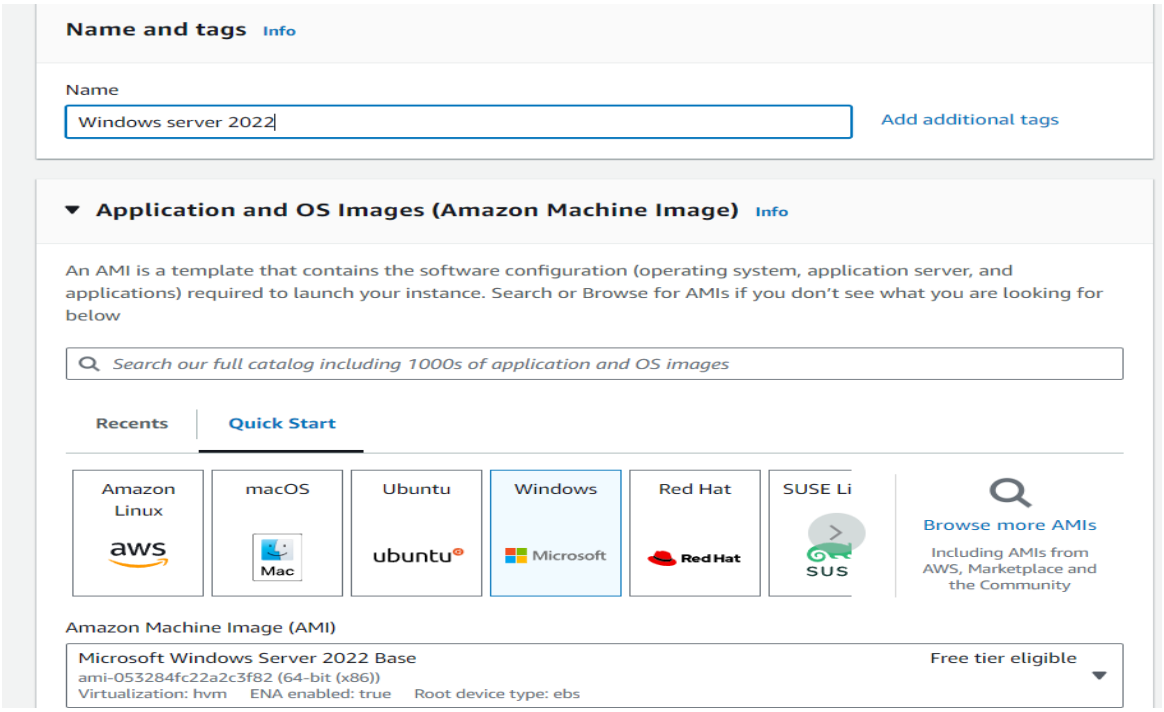
Fourth

1- Now we will create our machines (EC2)

Search for EC2 and then click on Launch Instance



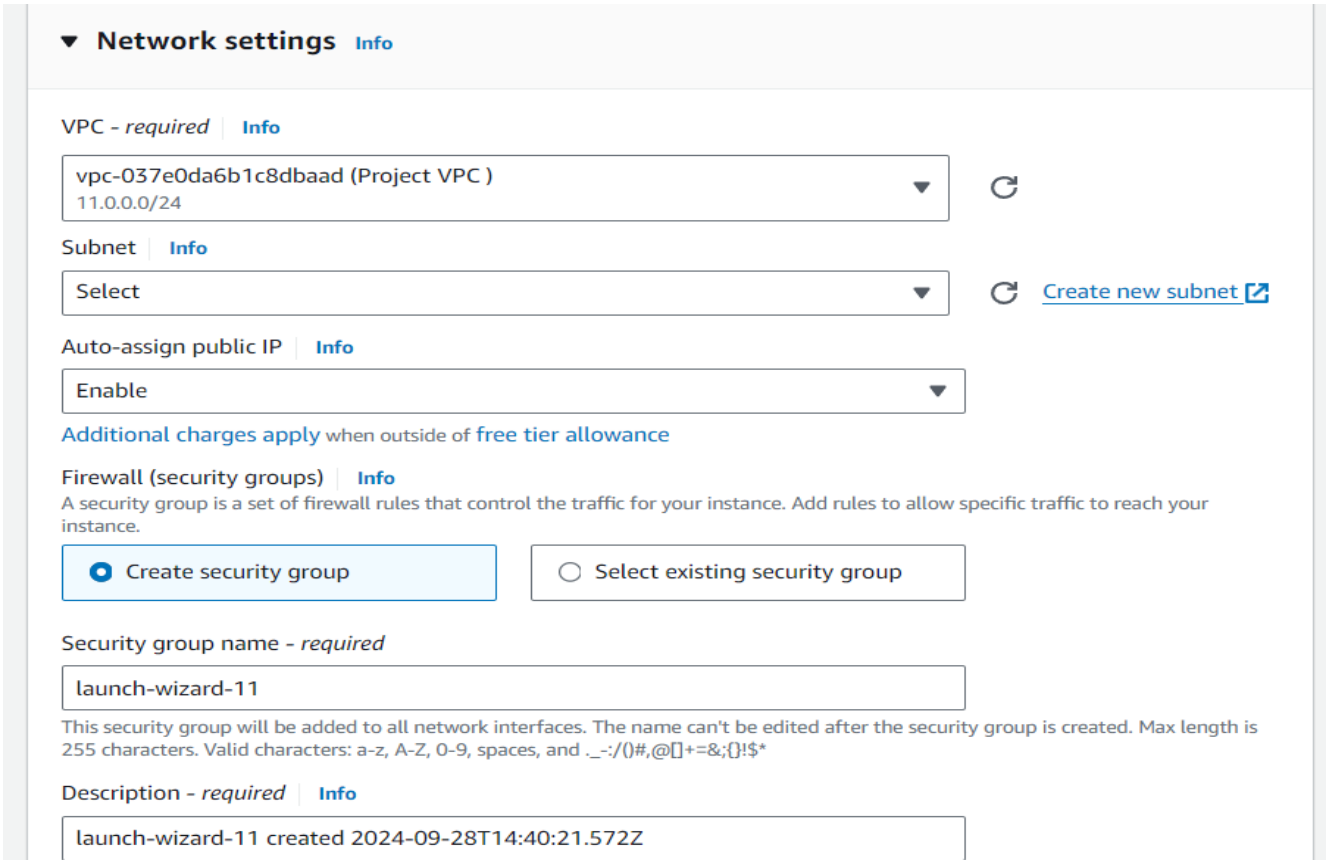
2- Create Windows Server 2022 instance and configure it

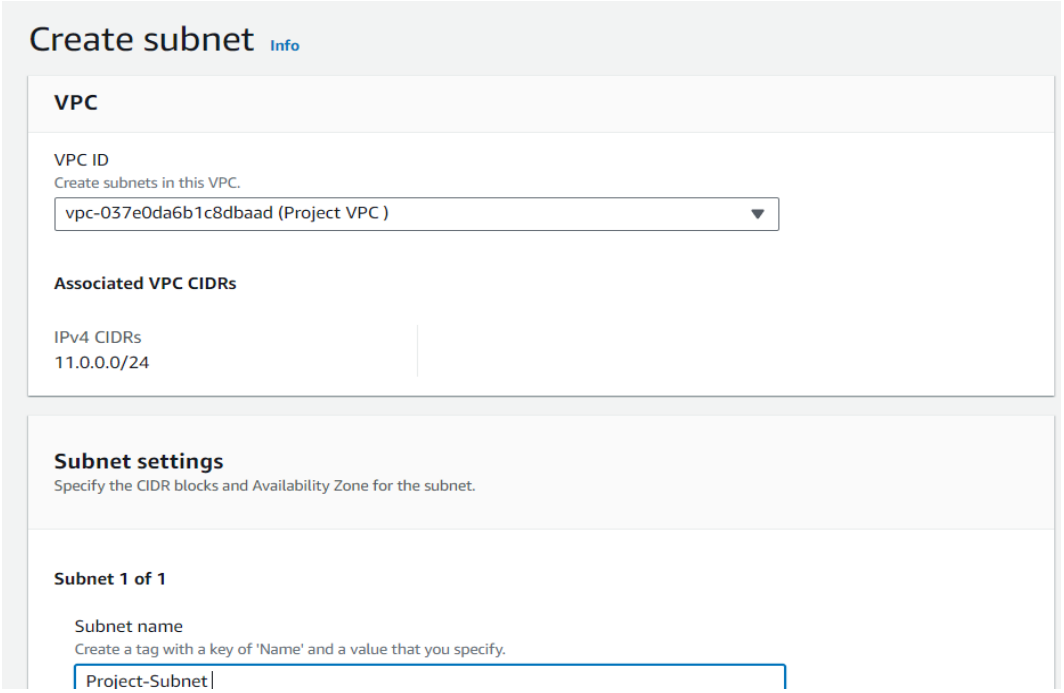


3- Create a key pair so you can access it

4- Configure the network settings and create a subnet

5- After creating the subnet, now click on Launch Instance.





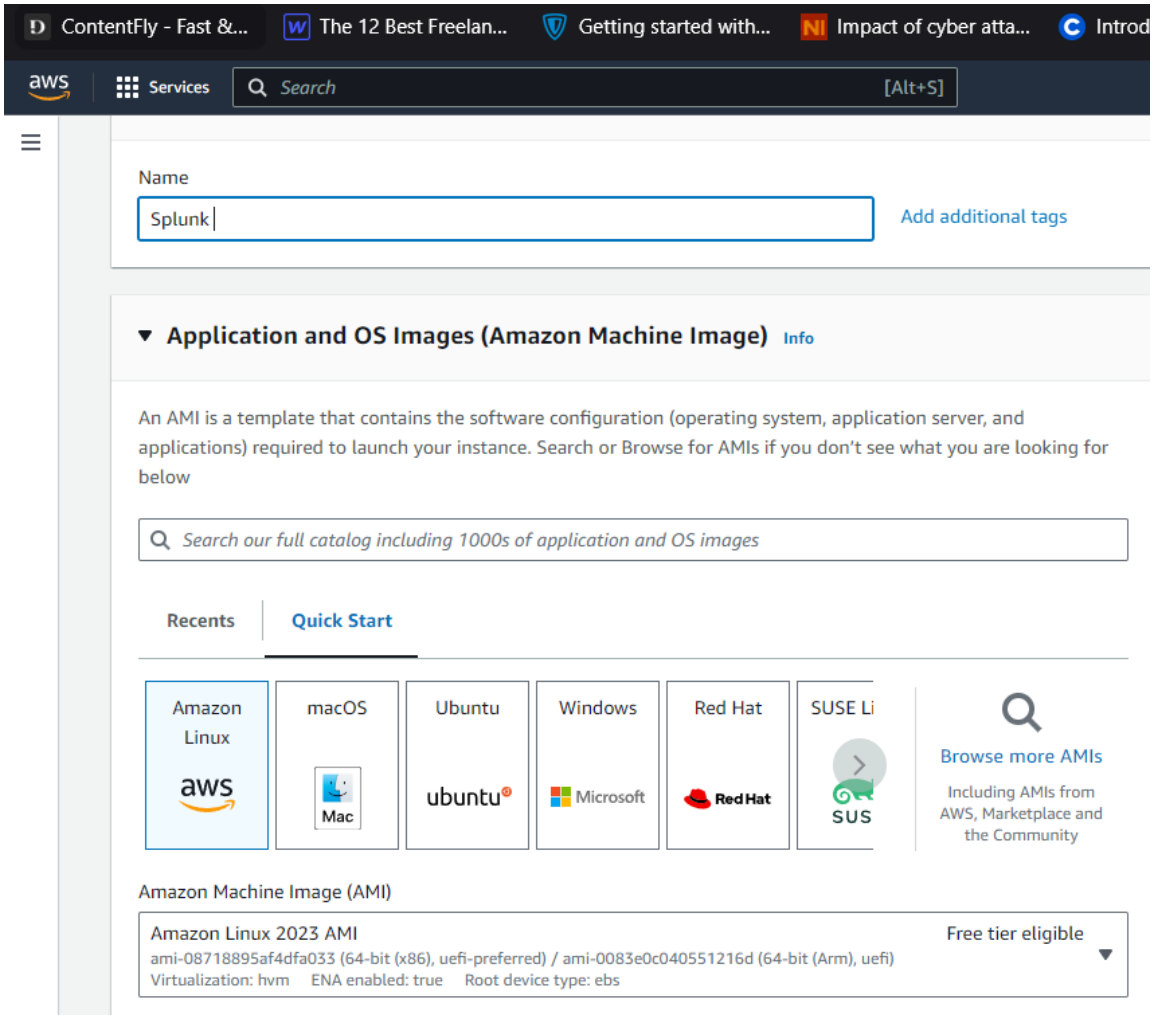
6- Click on Launch Instance

Notice: Same steps for other instances

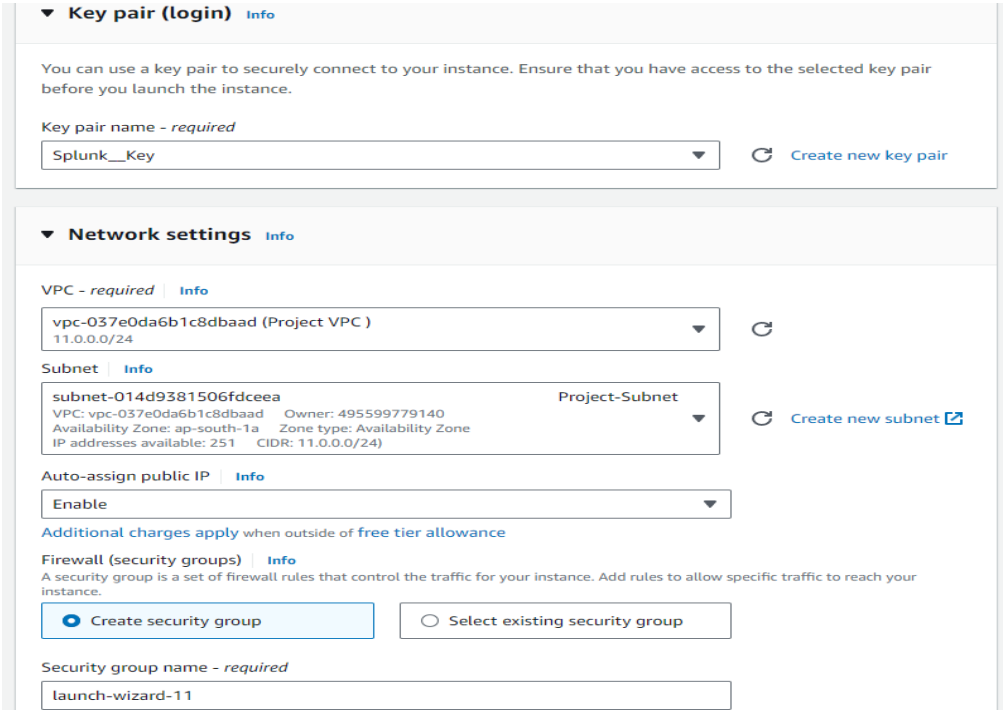
5- Splunk Deployment

For Splunk, I will use Amazon Linux Server, or you can use Ubuntu Server

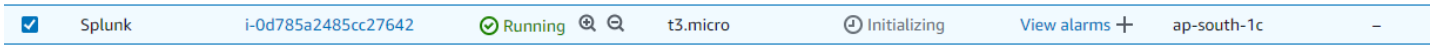
1- From Instances, choose Amazon Linux



2- Configure Settings and Create Key Pair

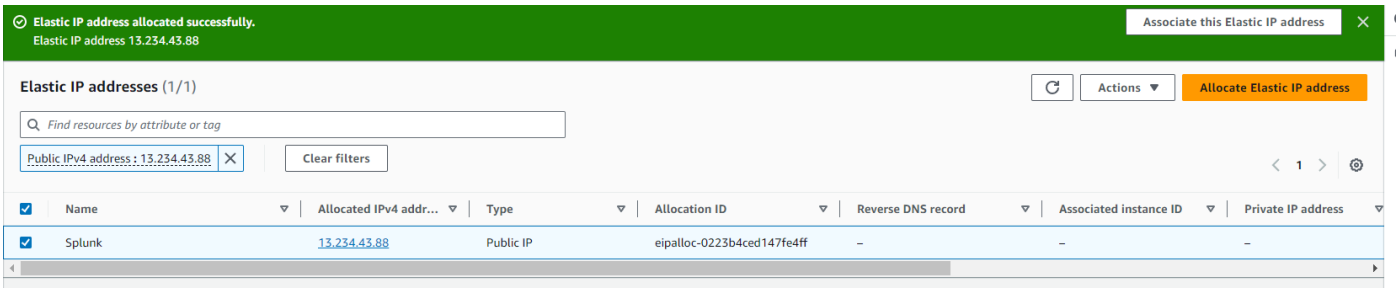


3- Click on ‘Launch Instance’ then start it

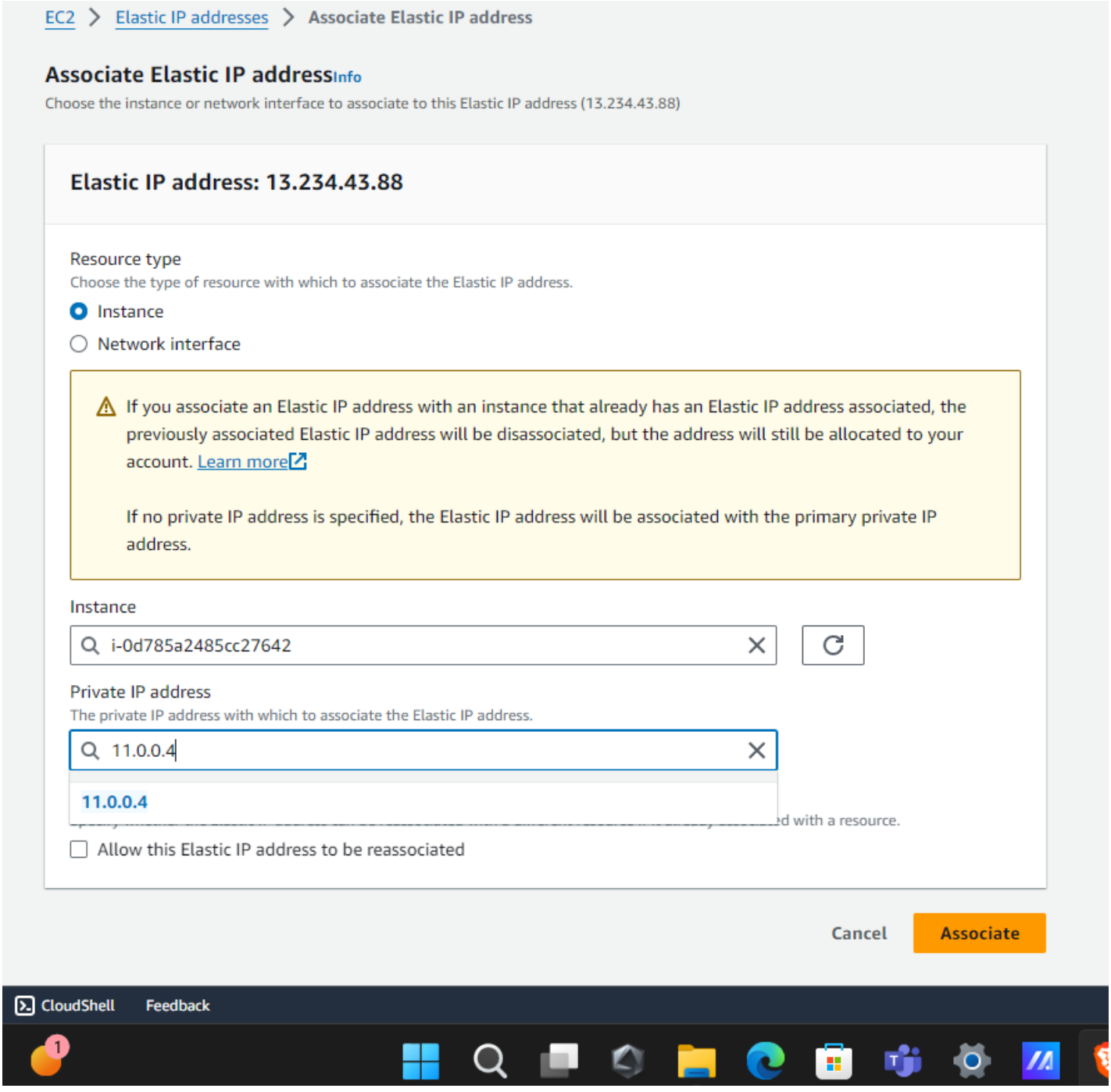


4- Assign an Elastic IP for the instance to avoid conflicts

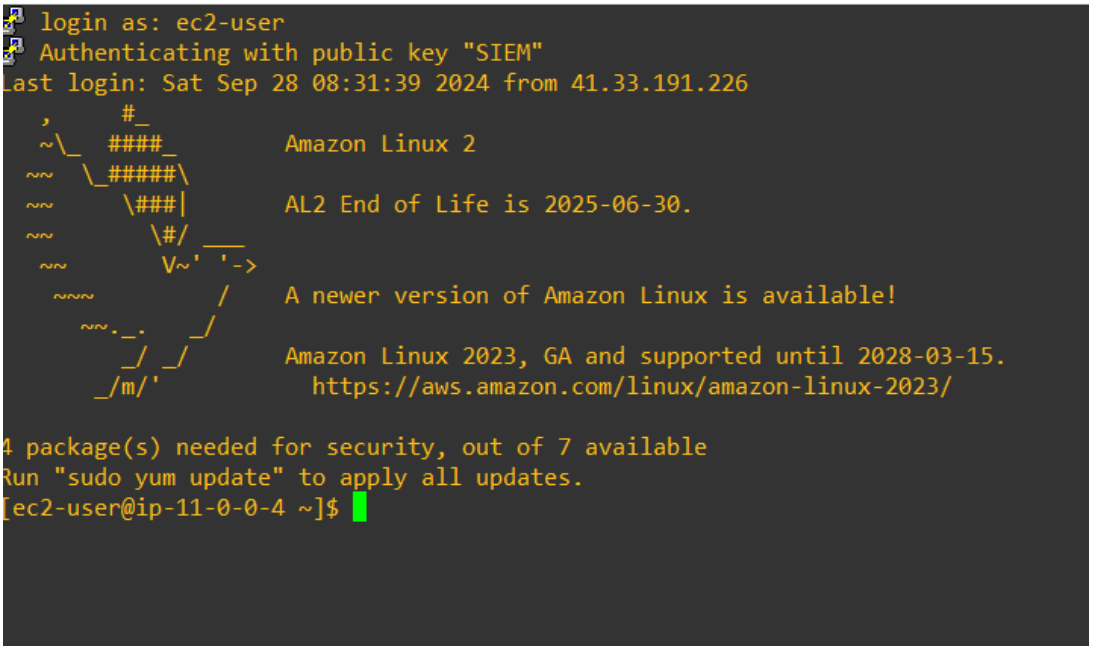
5- Click on **Allocate IP**



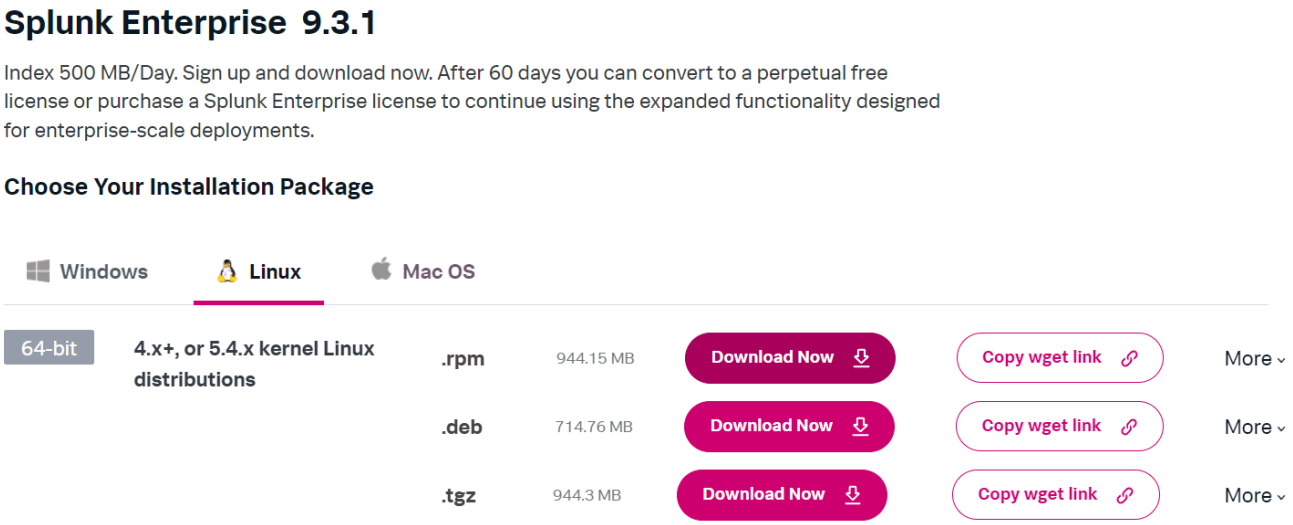
6- Now, Associate the IP to your Splunk Instance



7- Now, you can access the machine through SSH with the key pair, or you can you Putty



8- Go to **Splunk website** and choose the **download page**, choose **Splunk Enterprise**



9- Choose the .rpm version then **Copy Wget link** and paste it in your terminal

10- After the download is complete, do the following commands

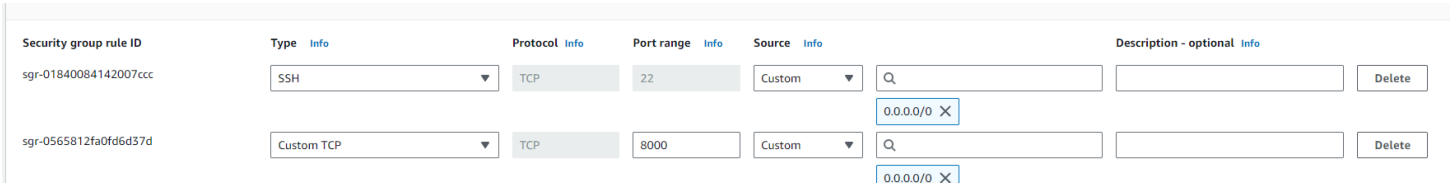
```
ec2-user@ip-11-0-0-4:~
[ec2-user@ip-11-0-0-4 ~]$ ls
splunk-9.3.0-51ccf43db5bd.x86_64.rpm
[ec2-user@ip-11-0-0-4 ~]$ sudo yum install ./splunk-9.3.0-51ccf43db5bd.x86_64.rpm
```

11- Afte the installation process is completed, do the following commands

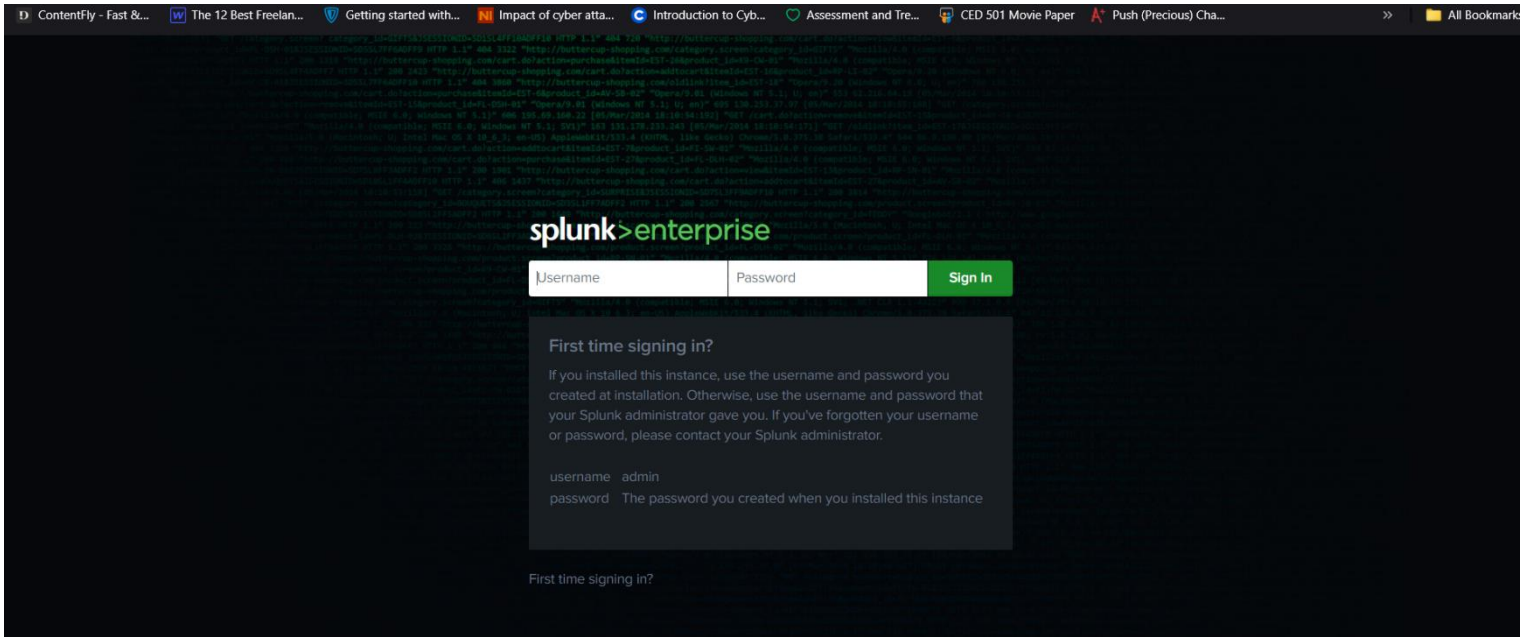
```
[ec2-user@ip-11-0-0-4 ~]$ sudo su
[root@ip-11-0-0-4 ec2-user]# cd /opt
[root@ip-11-0-0-4 opt]# cd splunk/
[root@ip-11-0-0-4 splunk]# cd bin/
[root@ip-11-0-0-4 bin]# ./splunk start --accept-license --answer-yes
```

12- After it finishes, choose the username and password

13- Allow port 8000 in the instance security rules, so you can log into Splunk

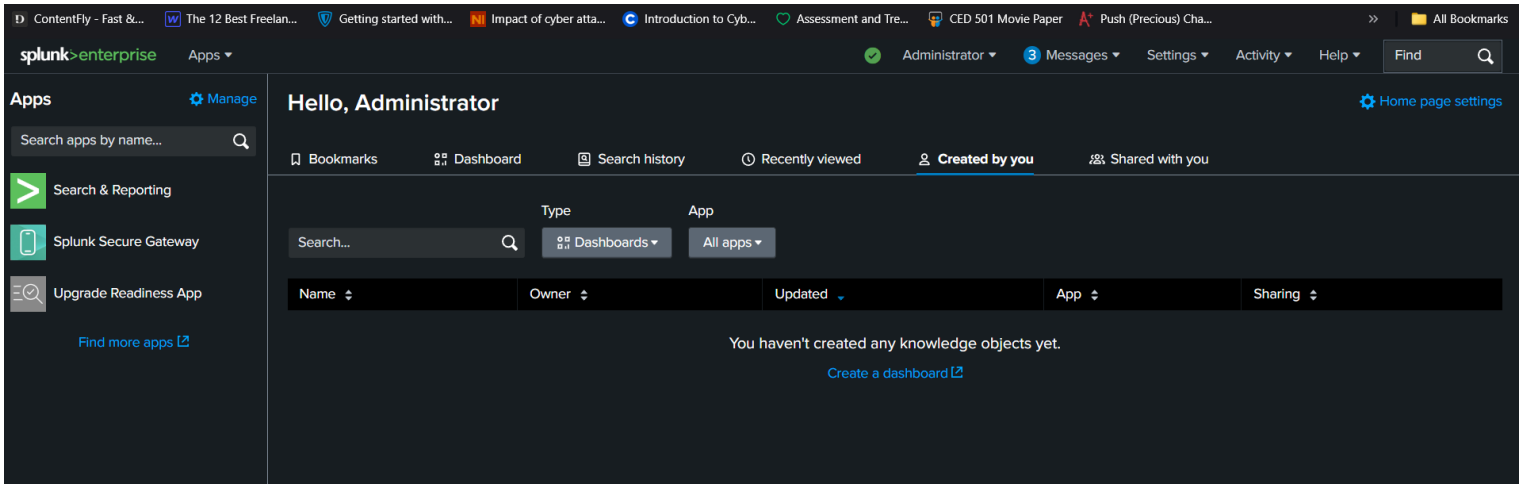


14- Now you can access Splunk without any problems



15- Write down your credentials and Sign In

16- Welcome to Splunk

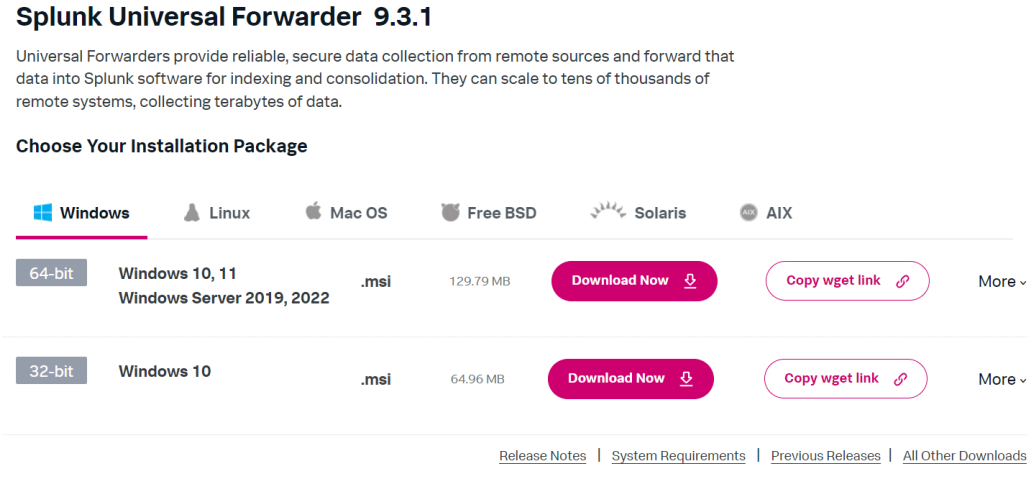


Installing Splunk Forwarder on Windows Server

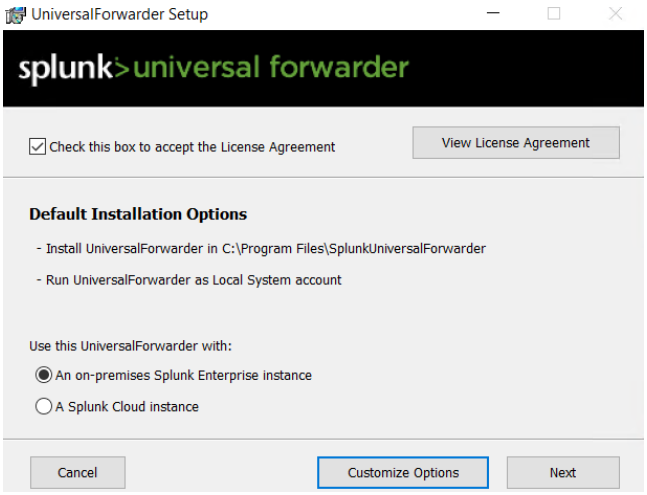
Steps

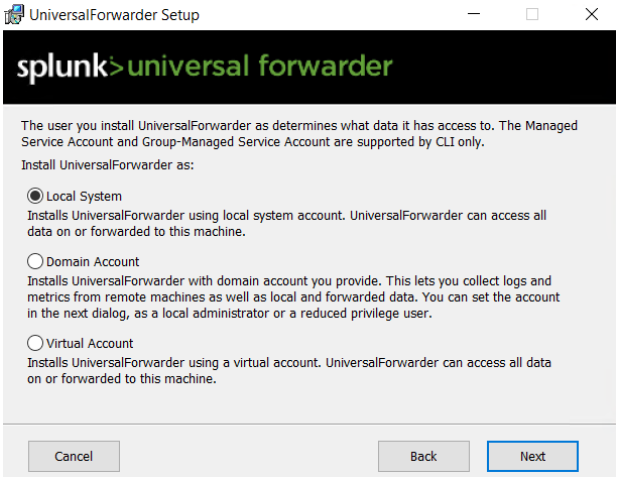
1- Access your Windows instance with RDP

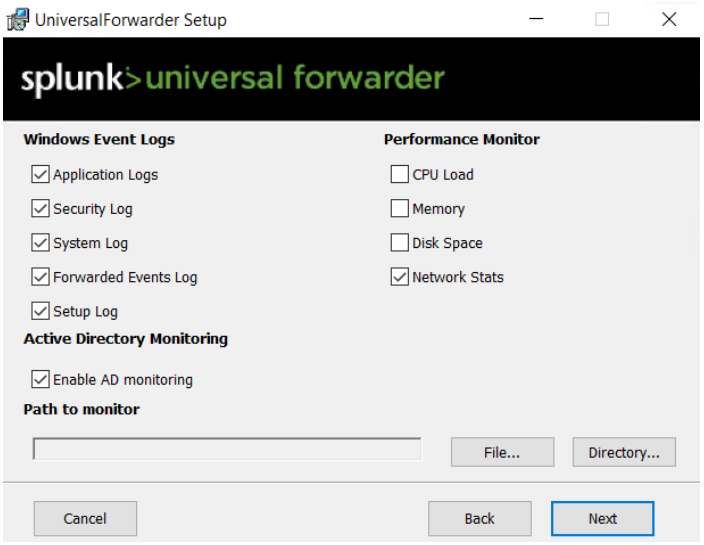
2- Go to Splunk Website and check the **download page** then look for **Universal Forwarder**

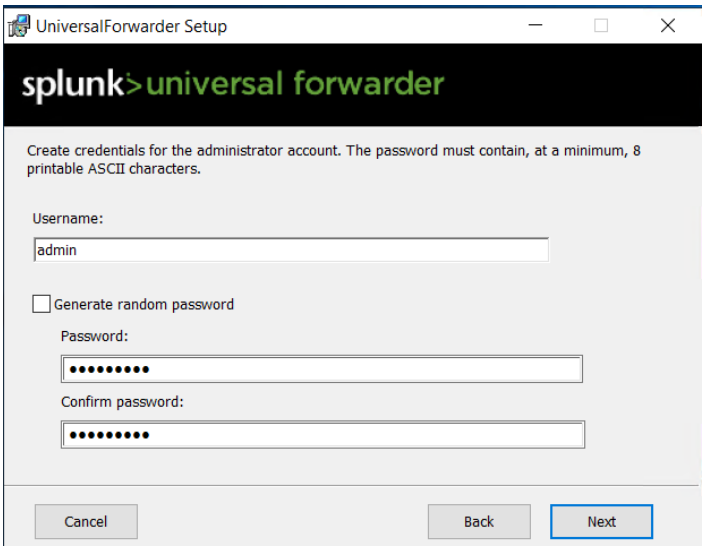


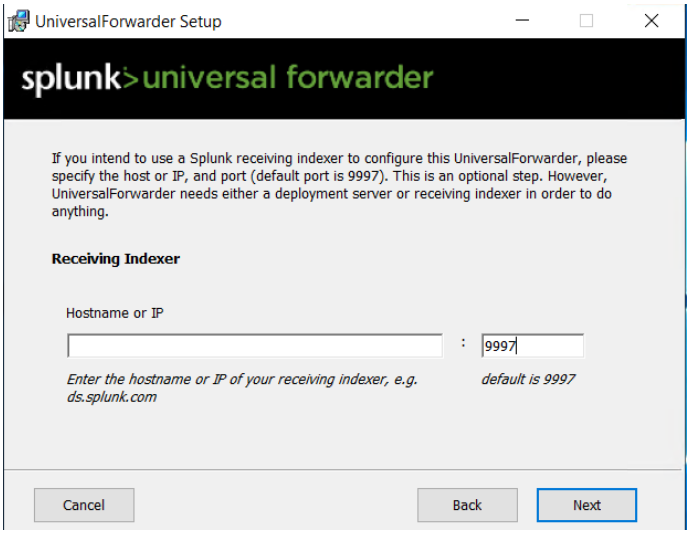
3- Download windows version then start the setup

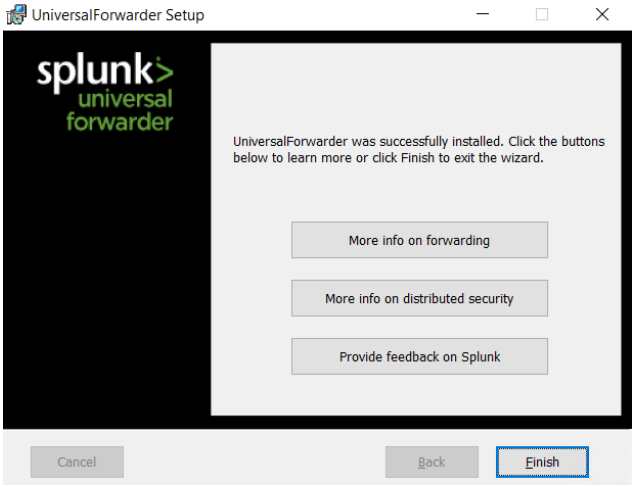






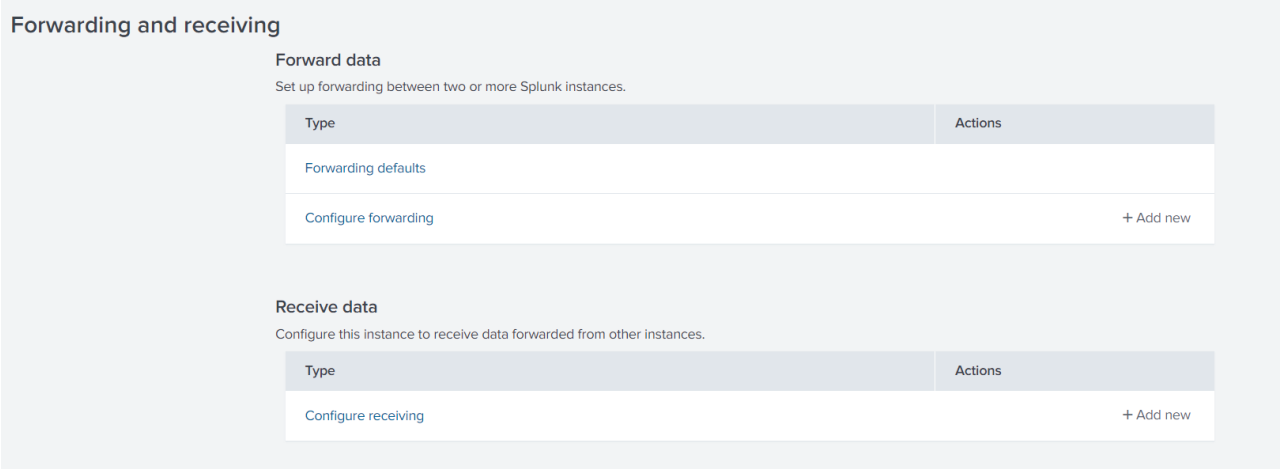




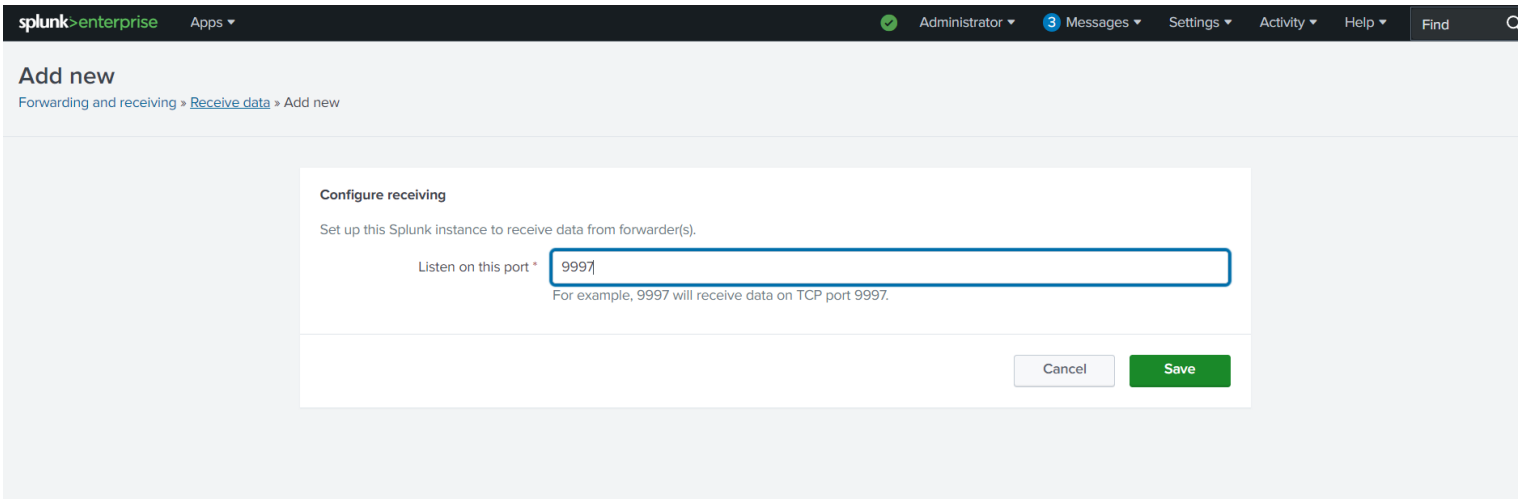


Enter the Public IP of your Splunk Instance

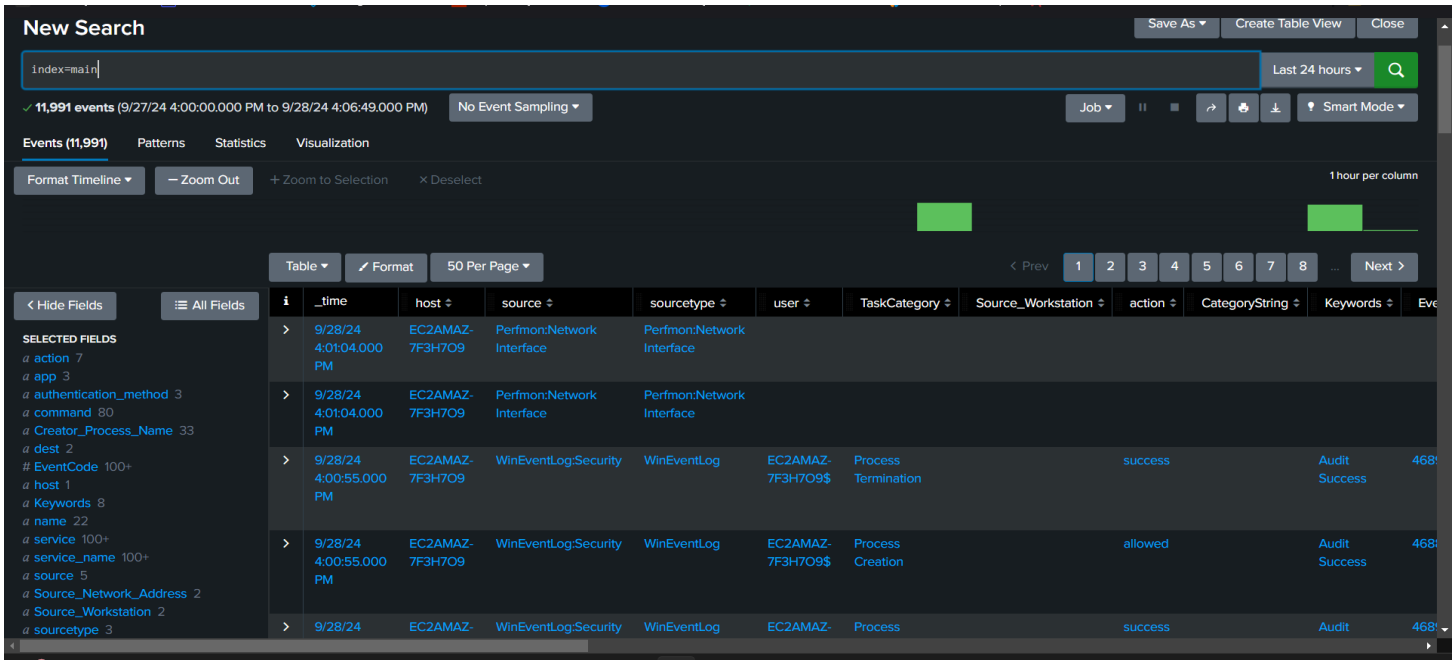
4- Go to Splunk Console and Open **Forwarding and Receiving** from settings



5- From **Receive data**, click on **Configure receiving** then click on **New Receiving Port**



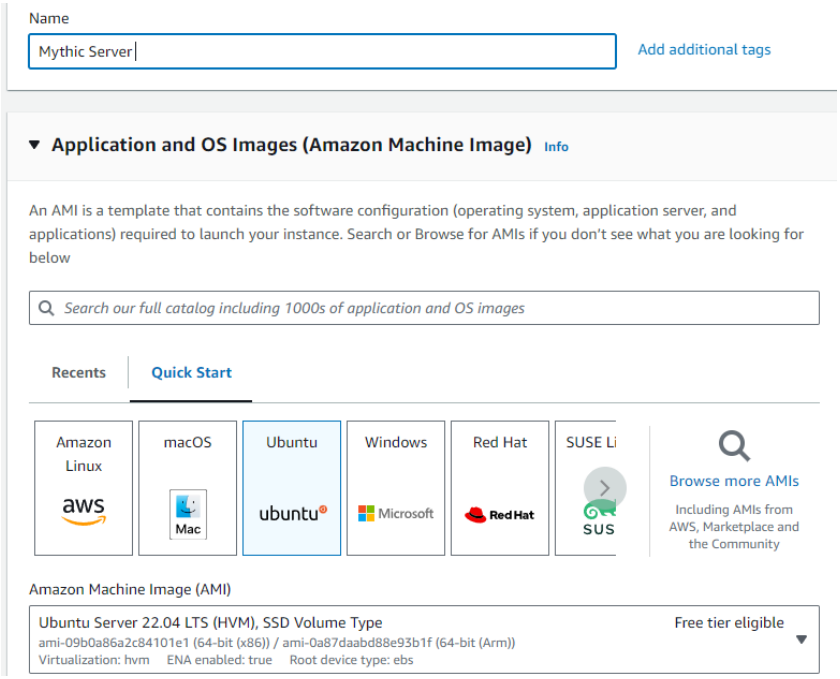
6- Save, now all the logs will be forwarded to Splunk on **port 9997**



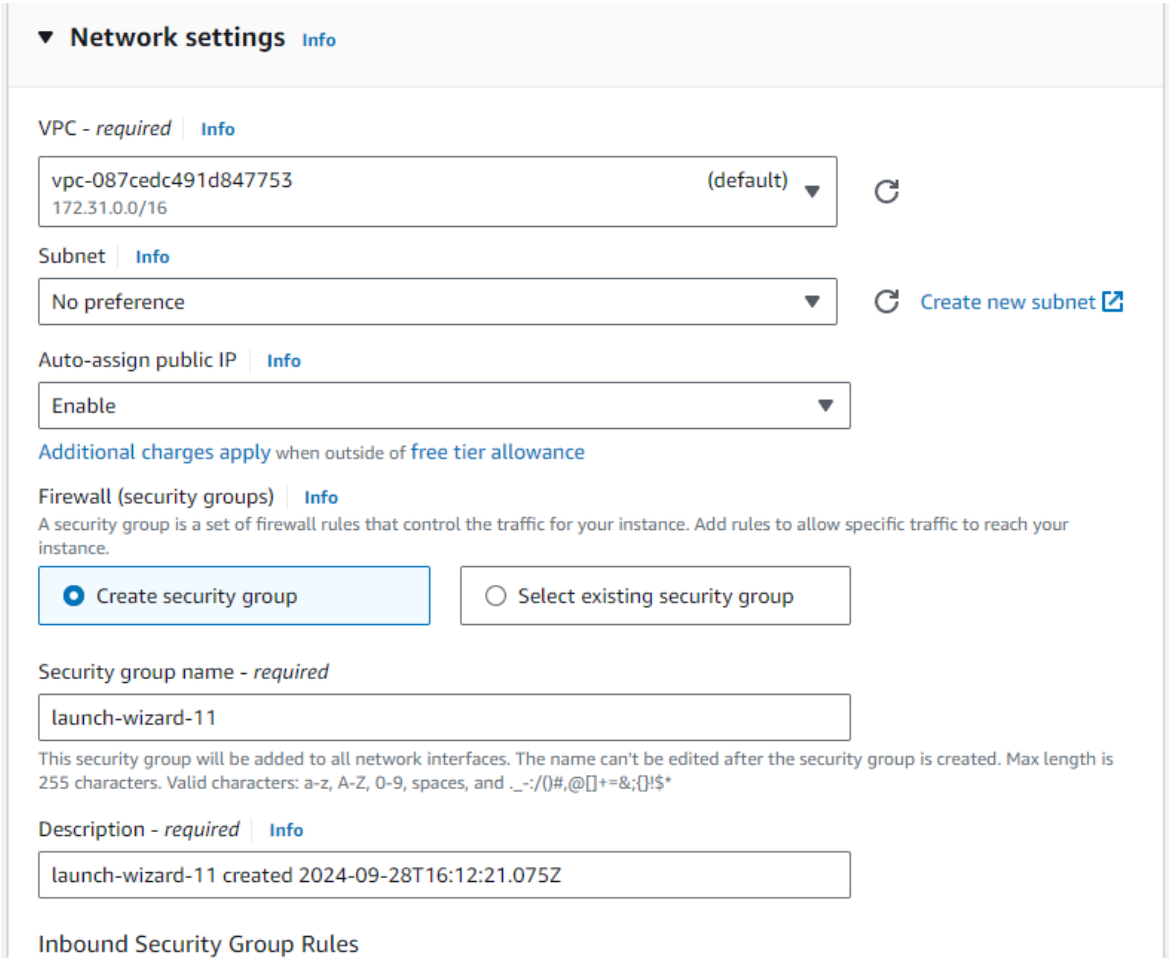
6-Mythic C2 Server Deployment

I will use Ubuntu Server 22.04 to deploy Mythic on it

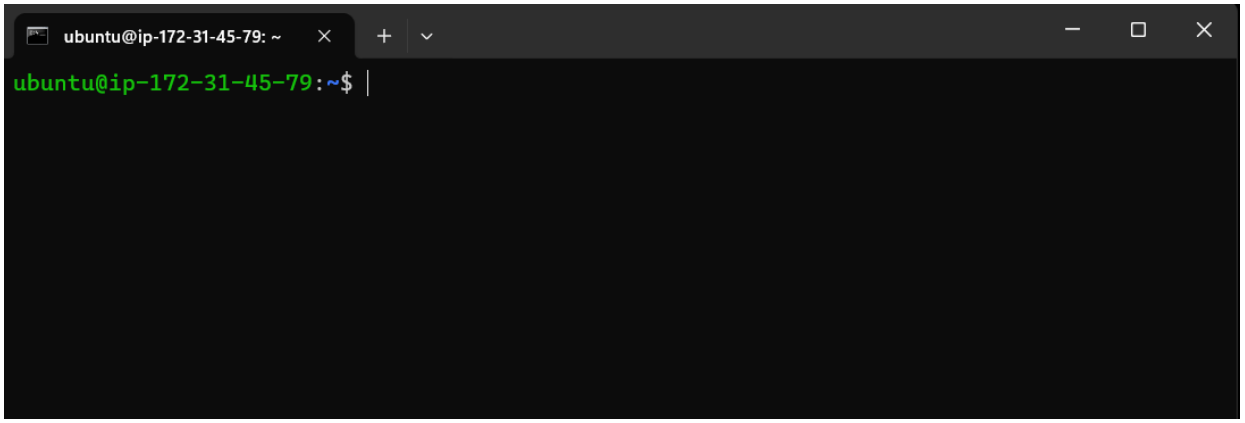
1- Launching Instance



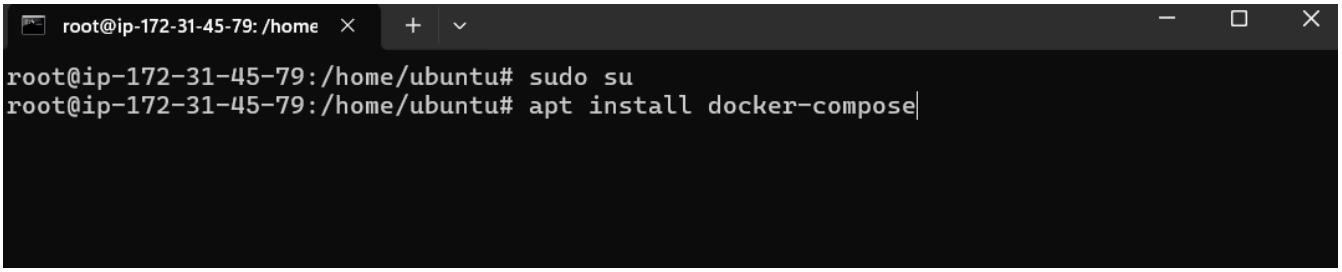
2- Create key pair and configure network but make sure to deploy the server in another VPC, not the same VPC we used it for Splunk and Windows



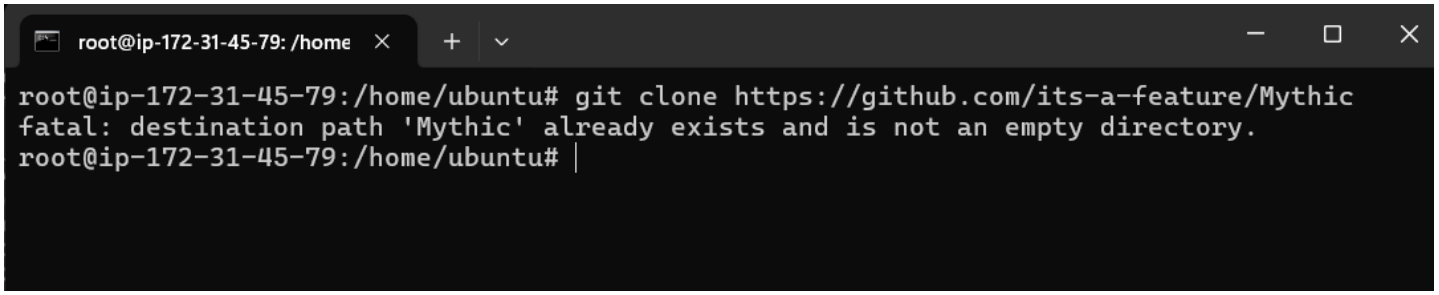
3- Access it with SSH

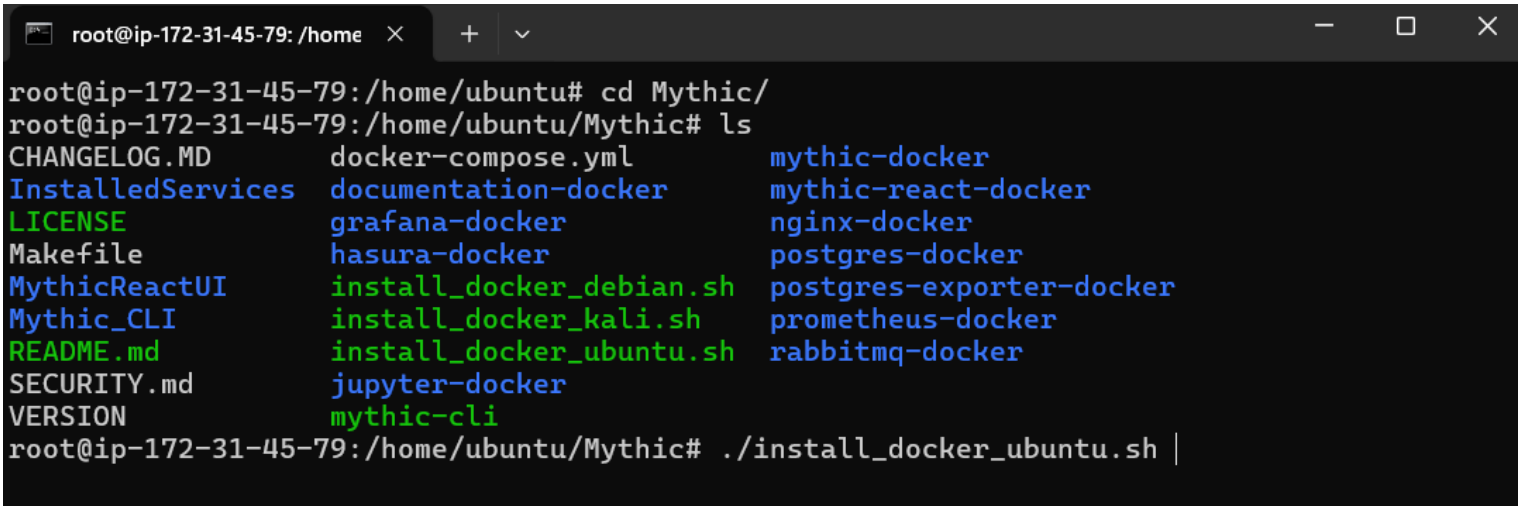


4- Do the following commands

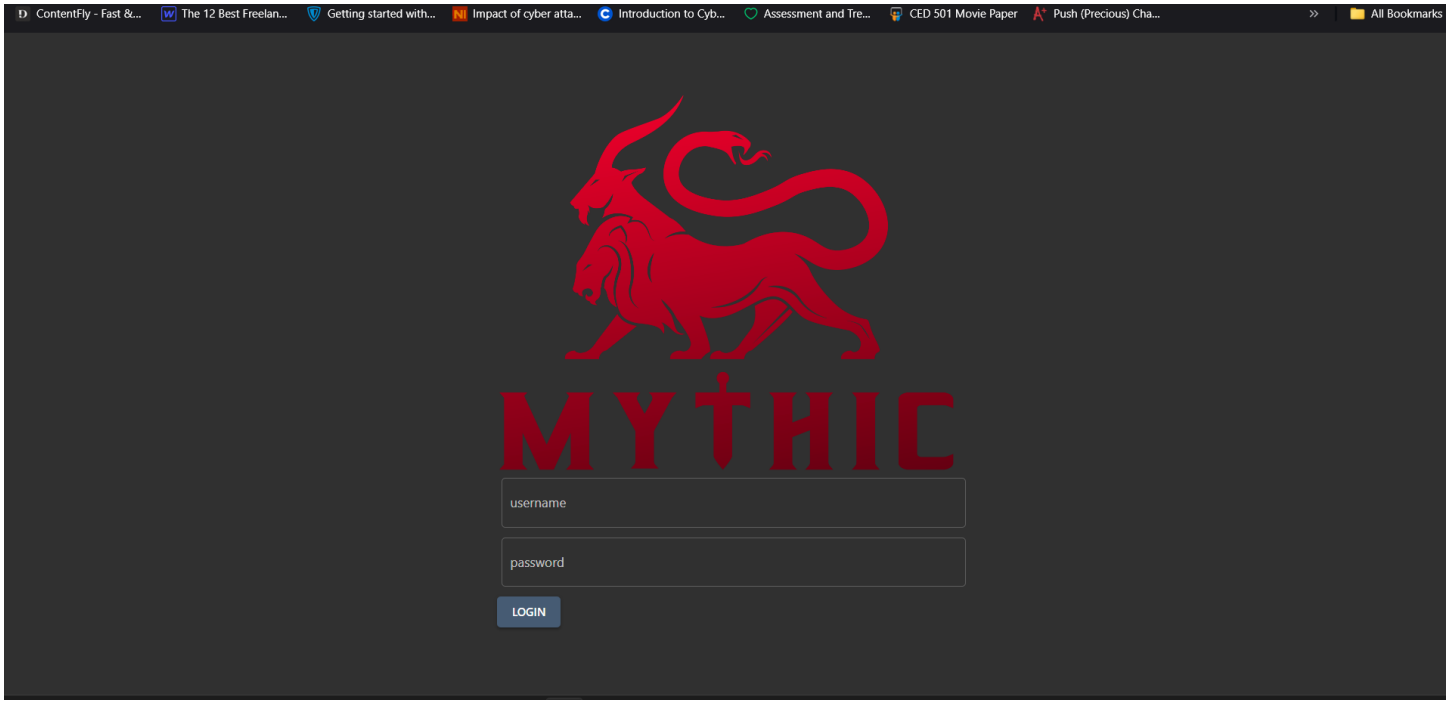


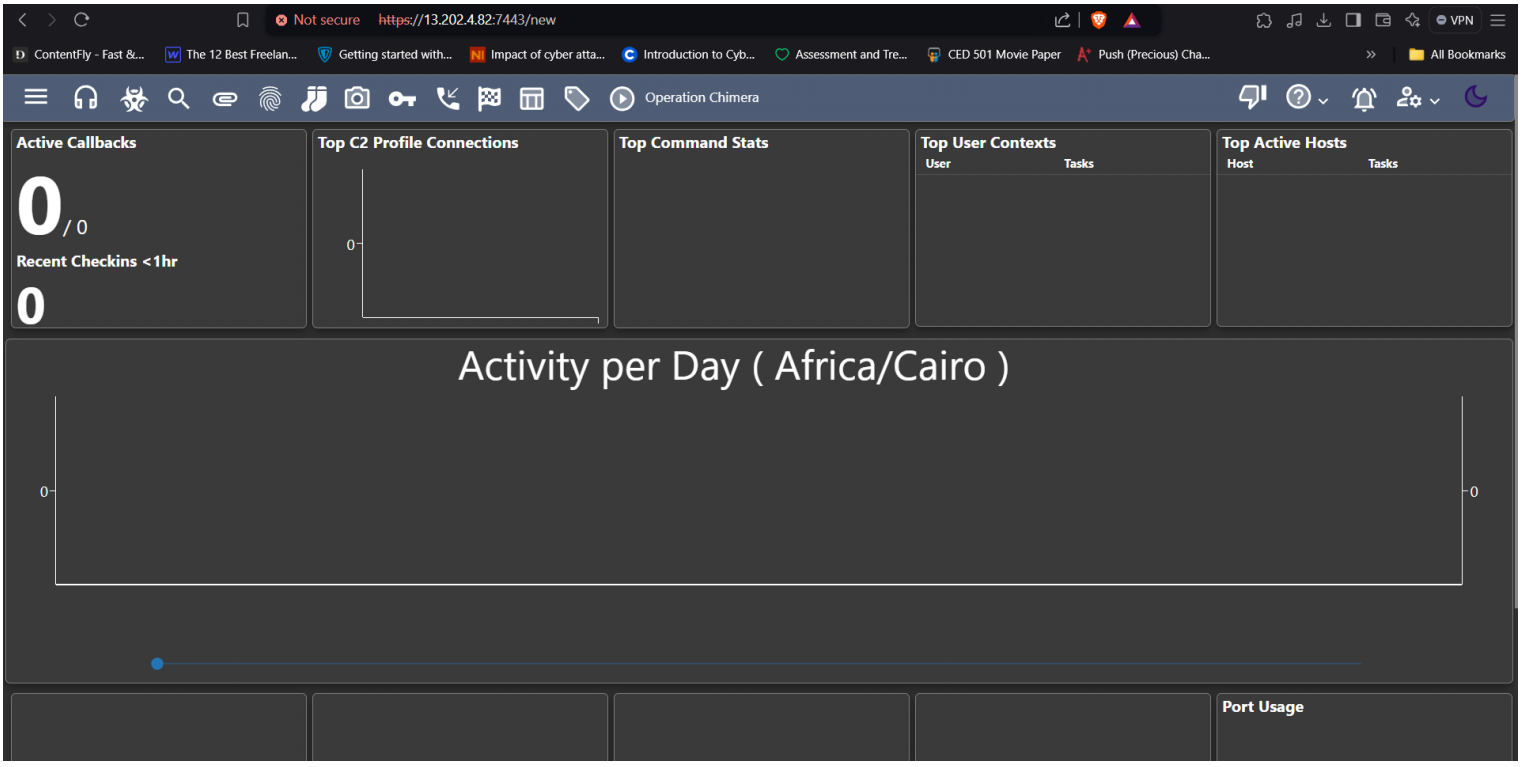
5- After it finishes installation, do the following



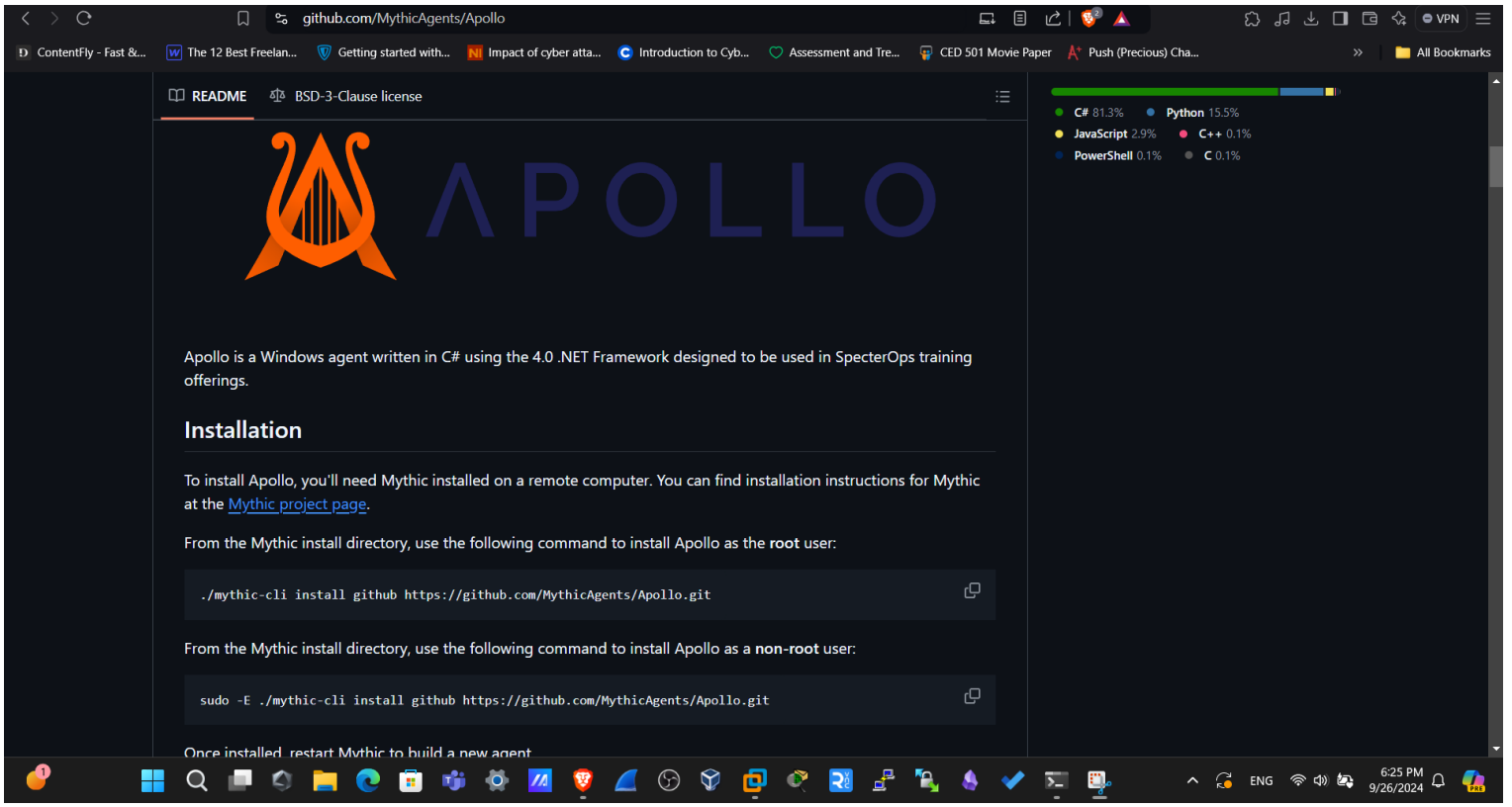


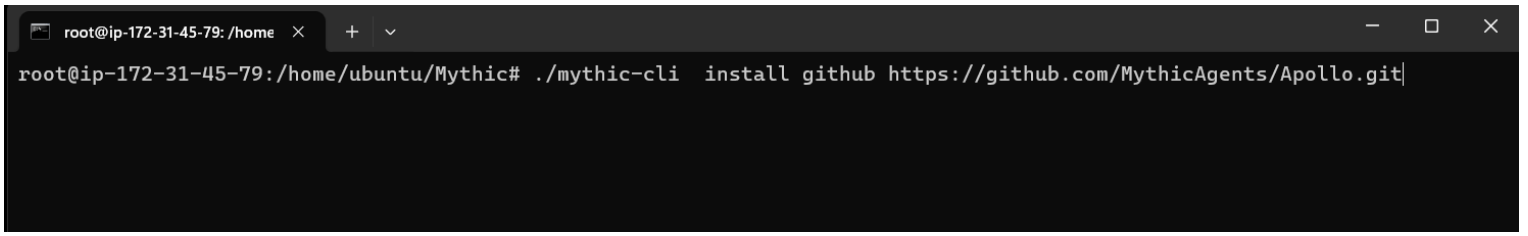
6- After the installation is complete

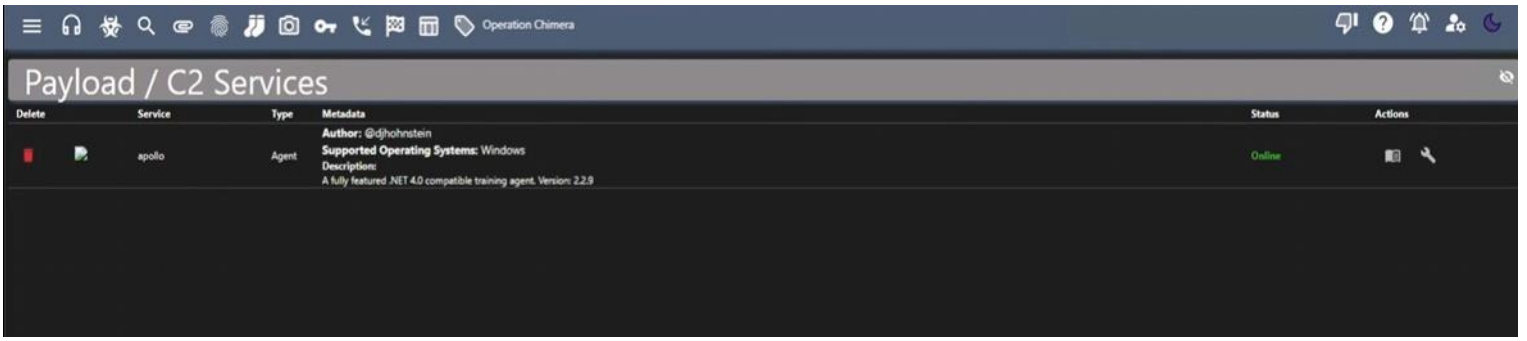




7- Now, I will download Apollo agent to create payload with it



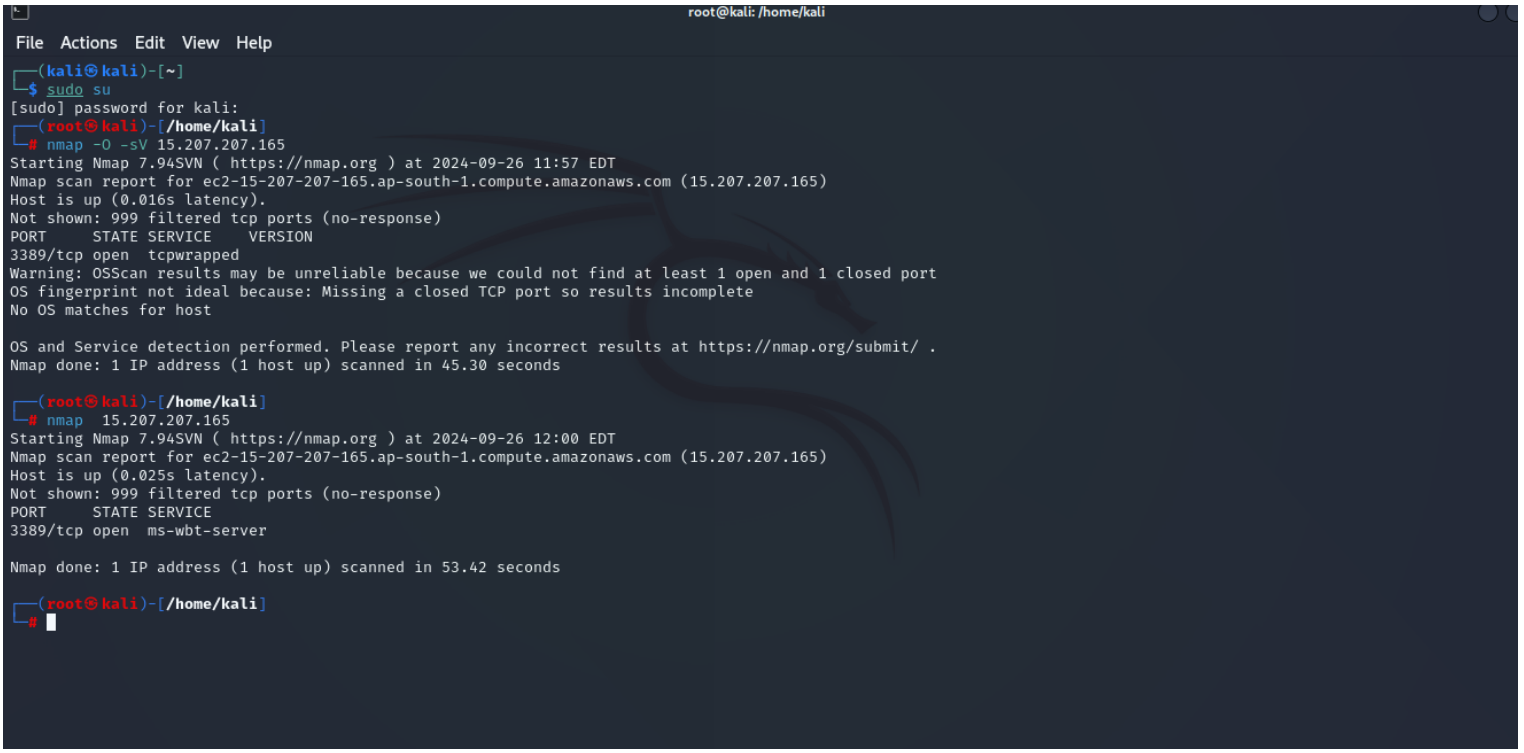




7-Practical Attack Implementation

Phase 1: Information Gathering

1- I Opened Kali Linux from My VMware and used Nmap to look for any open ports



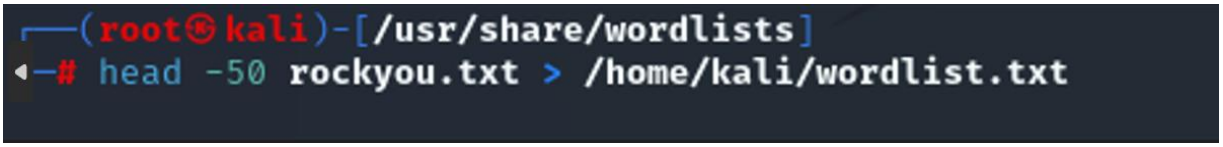
- We found out that Port 3389 is open, now we will try to brute force it in the next phase

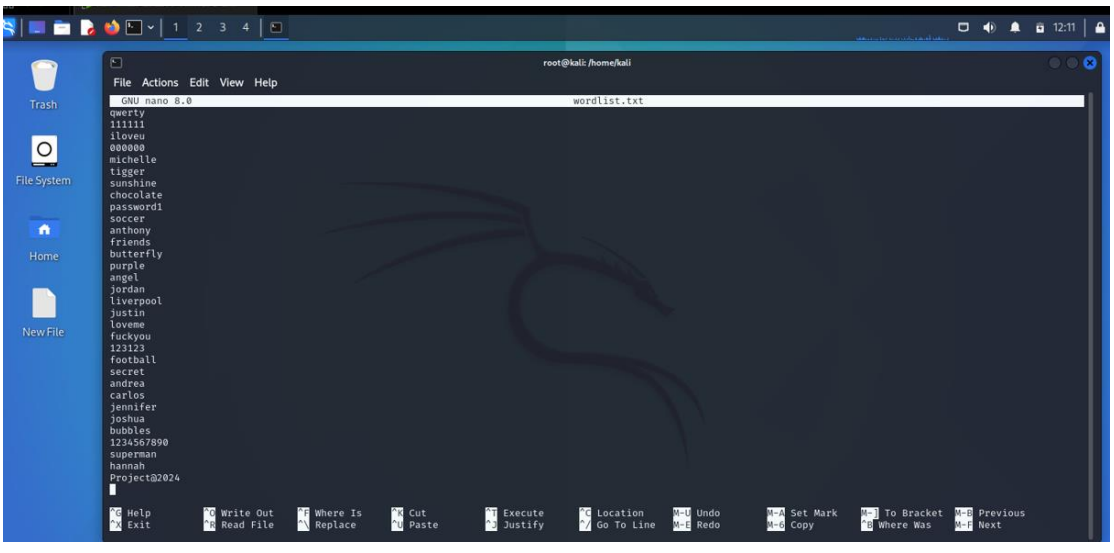
Phase 2: Initial Access

Using Crowbar, I successfully brute forced the RDP password

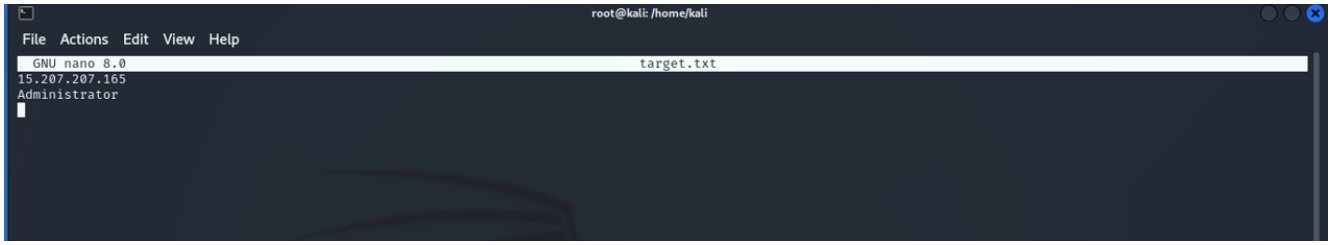
Steps

1- Preparing the word list

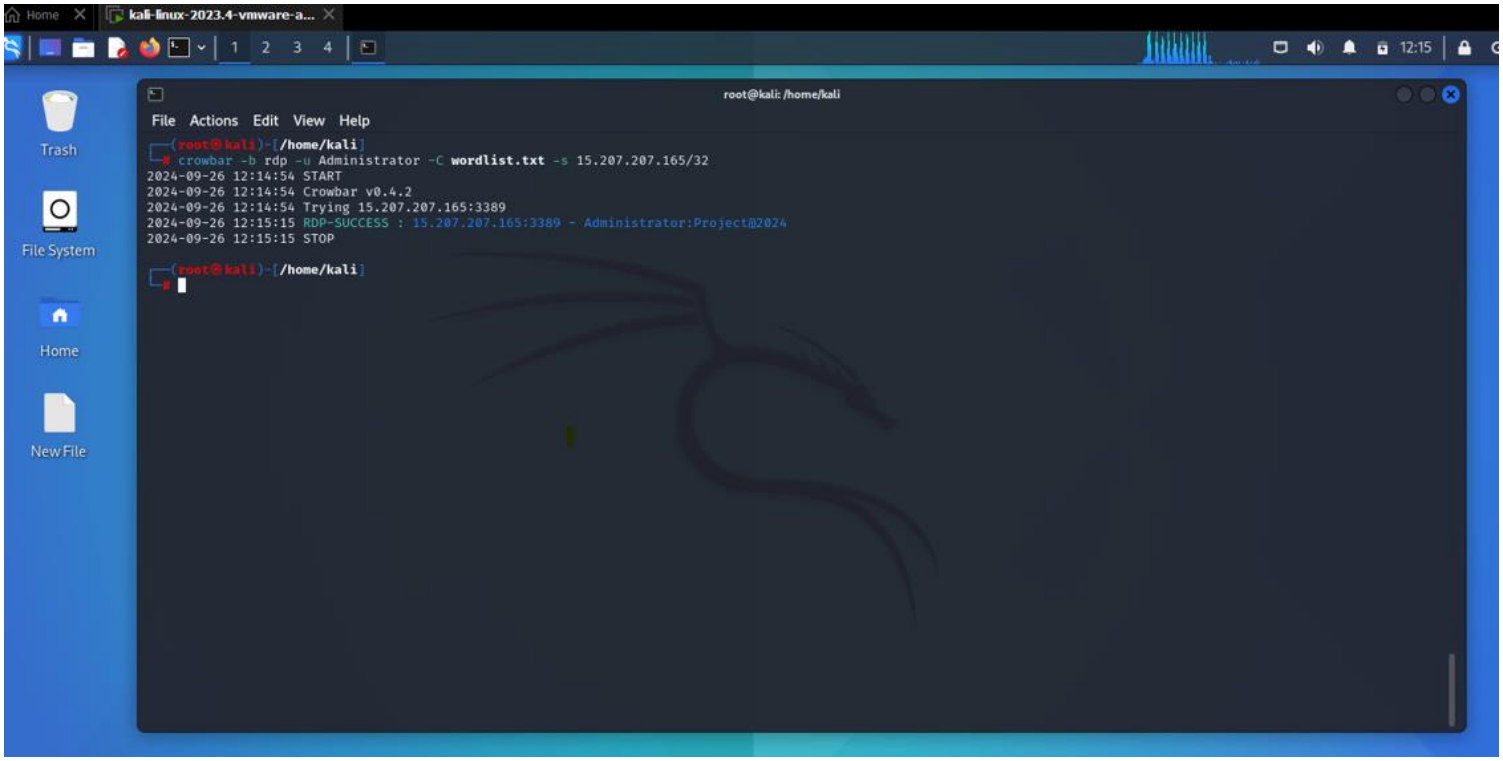




2- Preparing the target list

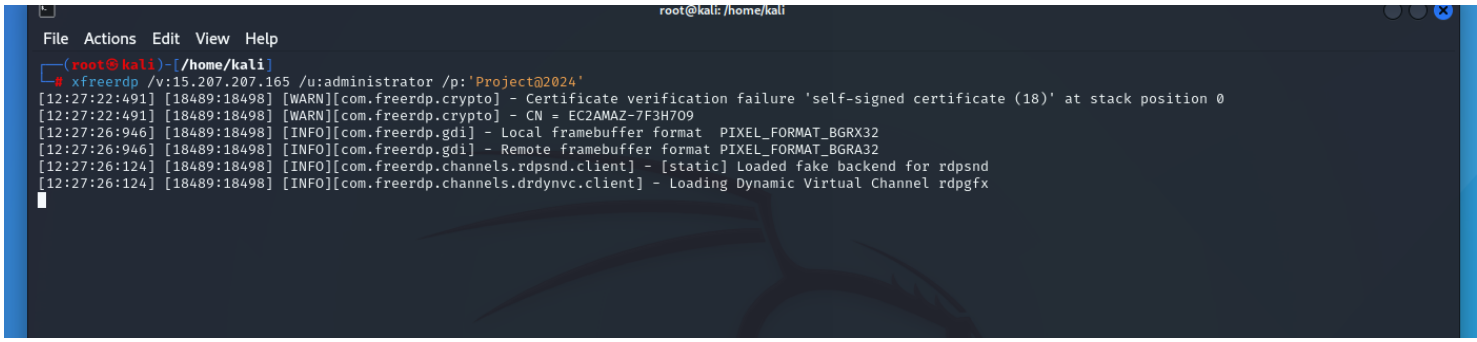


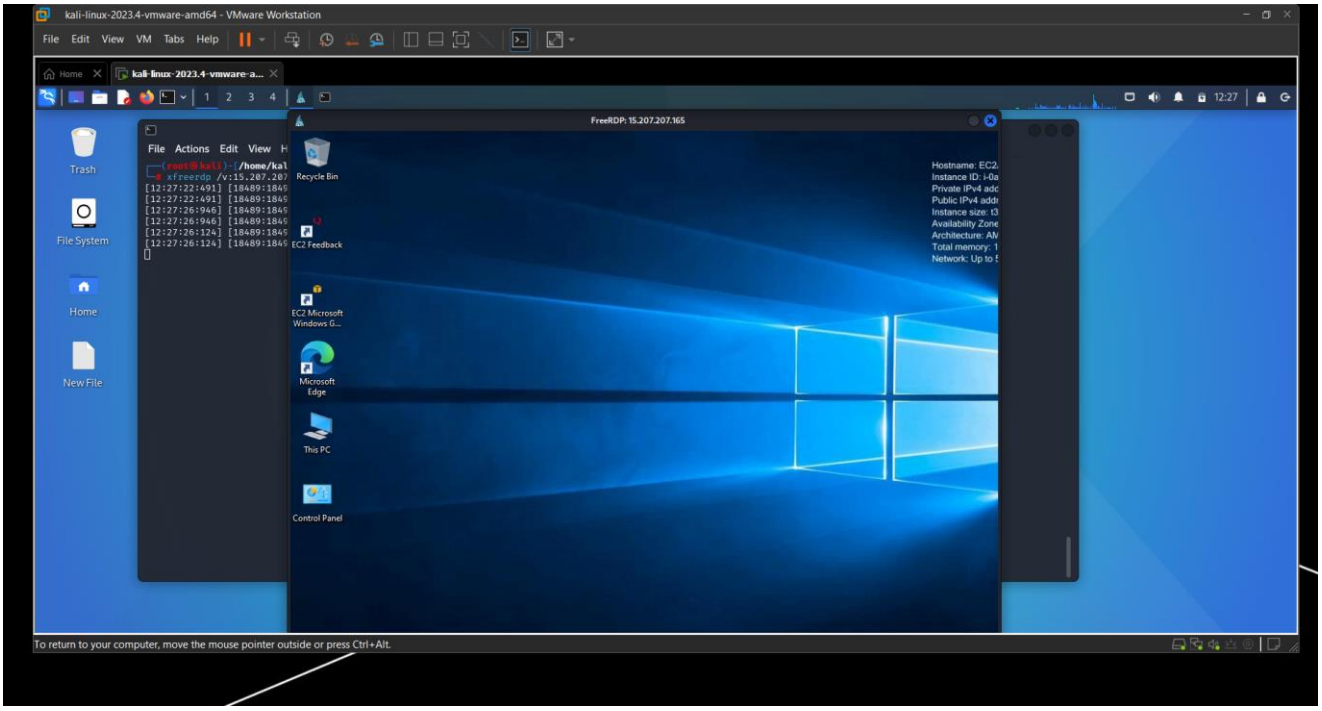
3- Initiating the attack



- As shown, I successfully brute forced the password

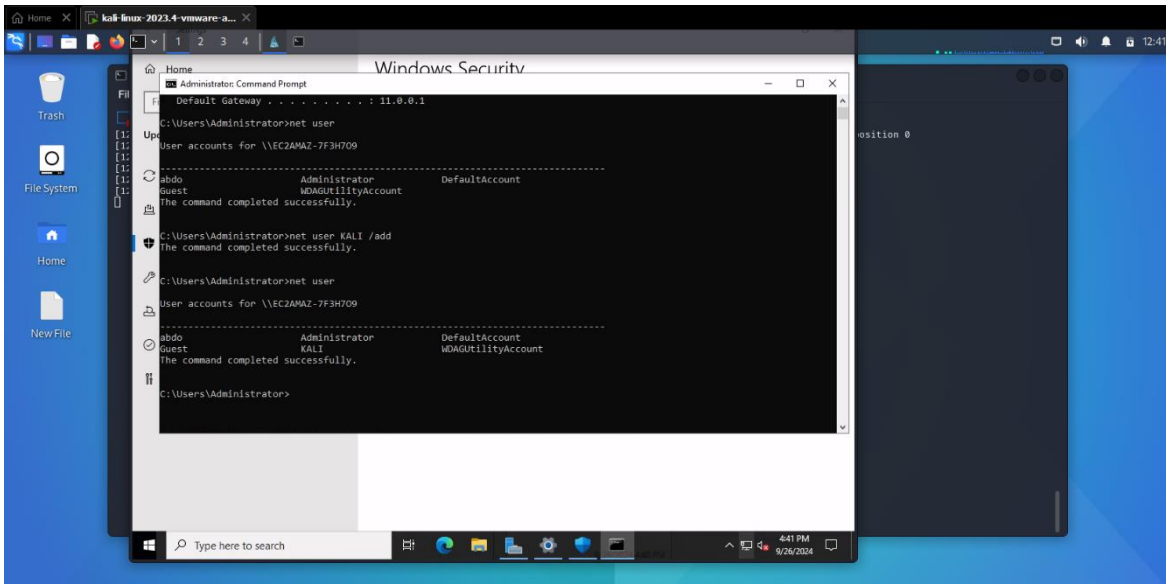
4- Now, we access our victim machine from Kali Linux using **xfreerdp**

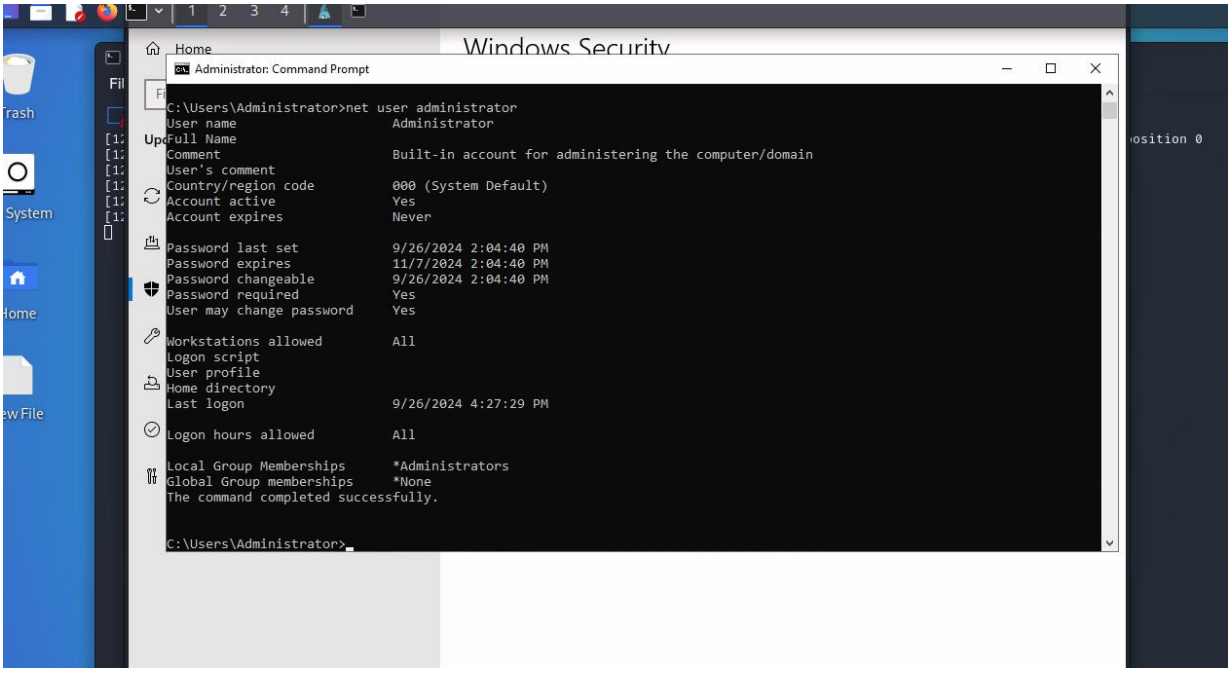




Phase 3: Discovery

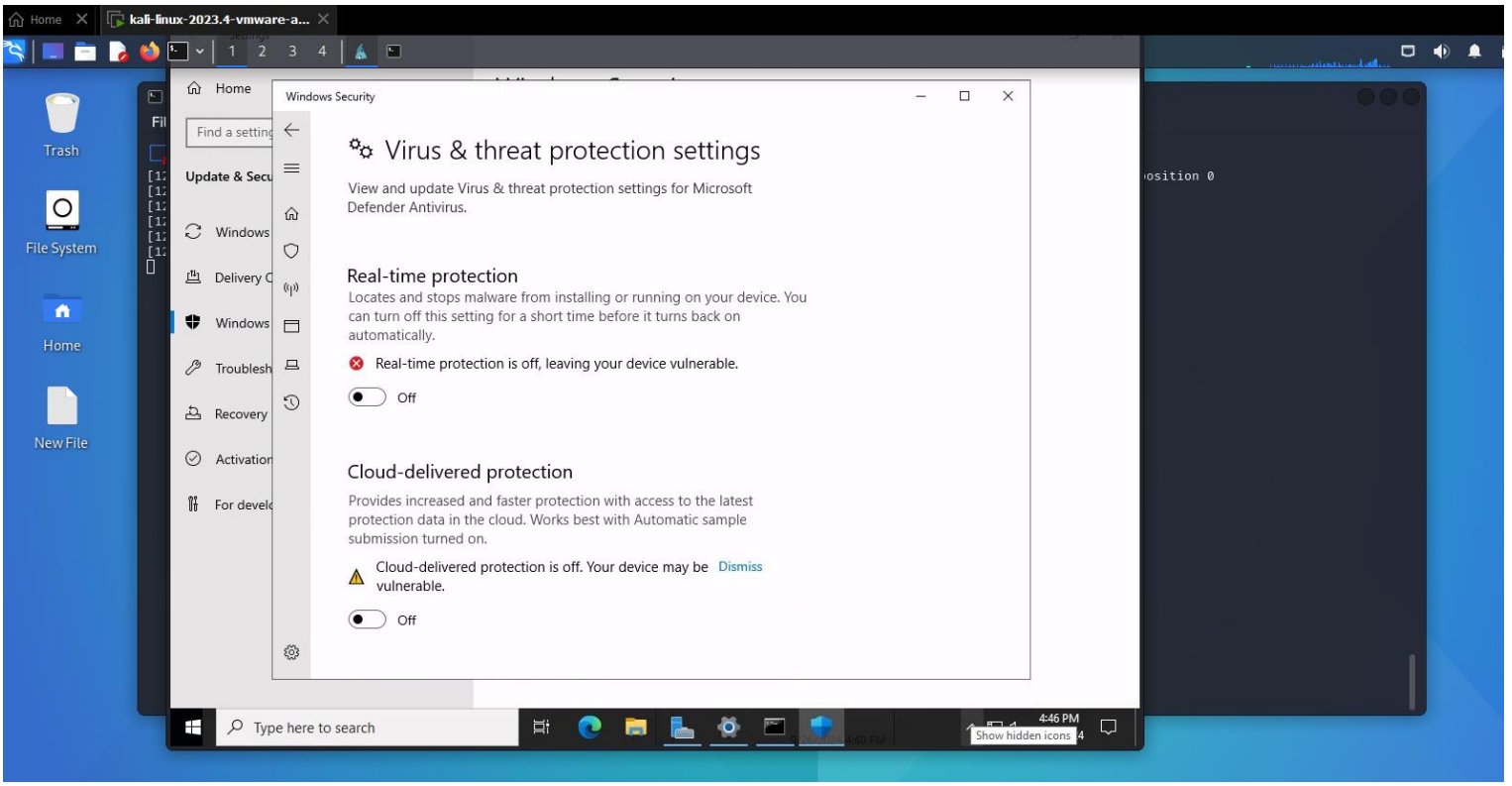
Now, we will enter some commands via cmd to discover our victim





Phase 4: Defense Evasion

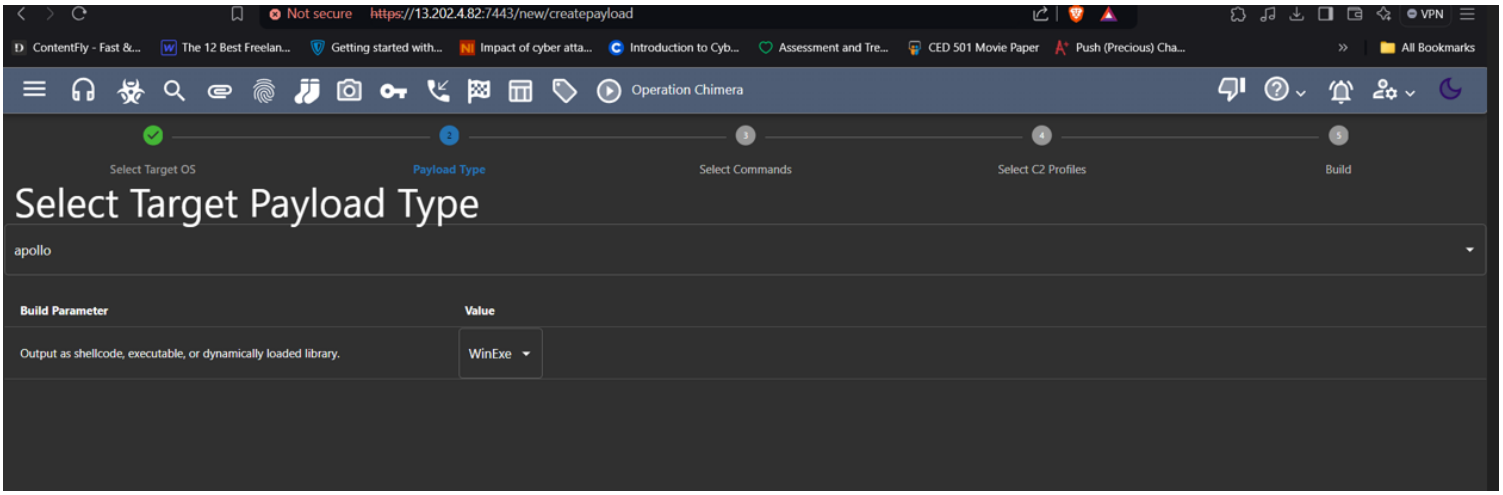
In this phase, I disabled the Windows defender manually to make sure that, I won't be detected when I run the **payload**



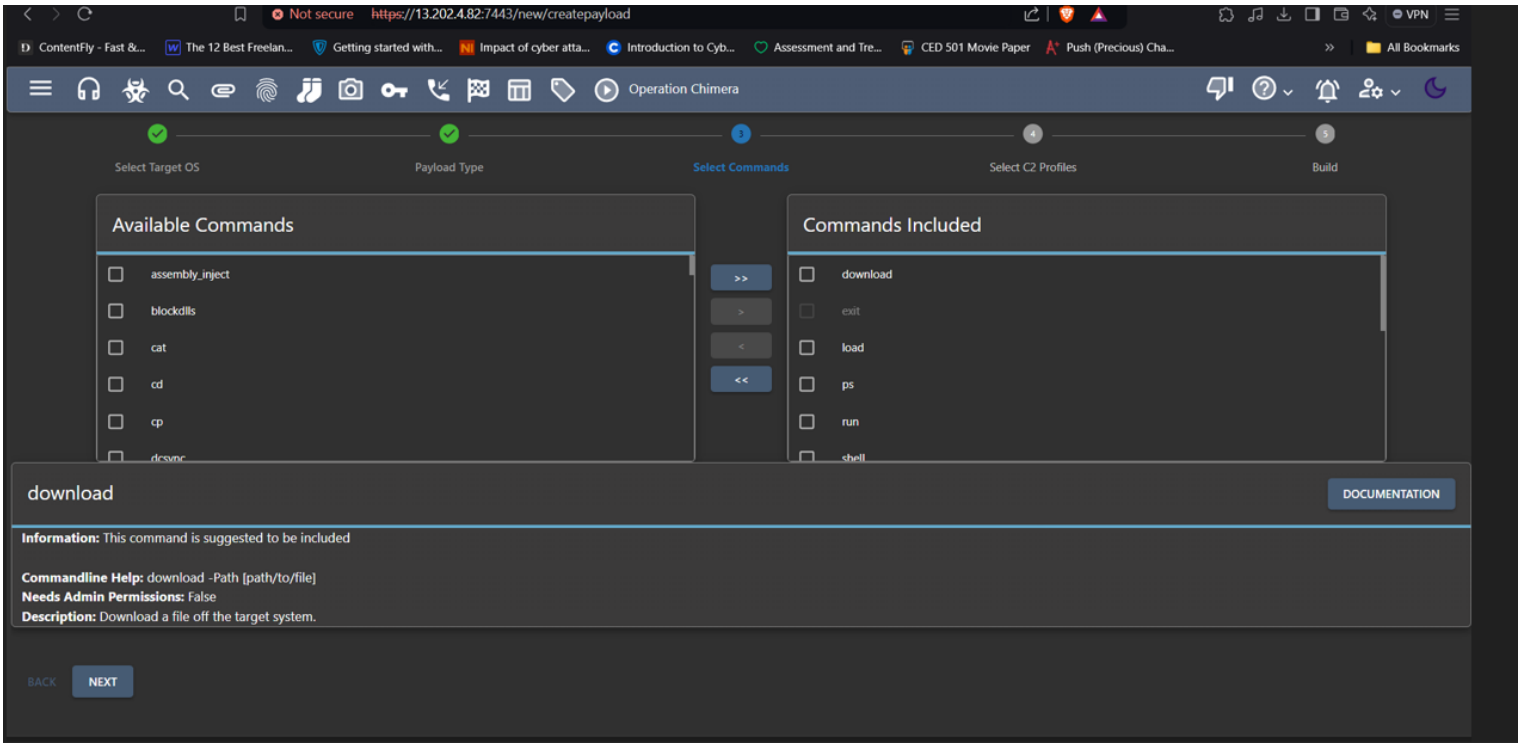
Phase 5: Payload Execution

Now, I will create the payload with the help of Apollo (Mythic Agent)

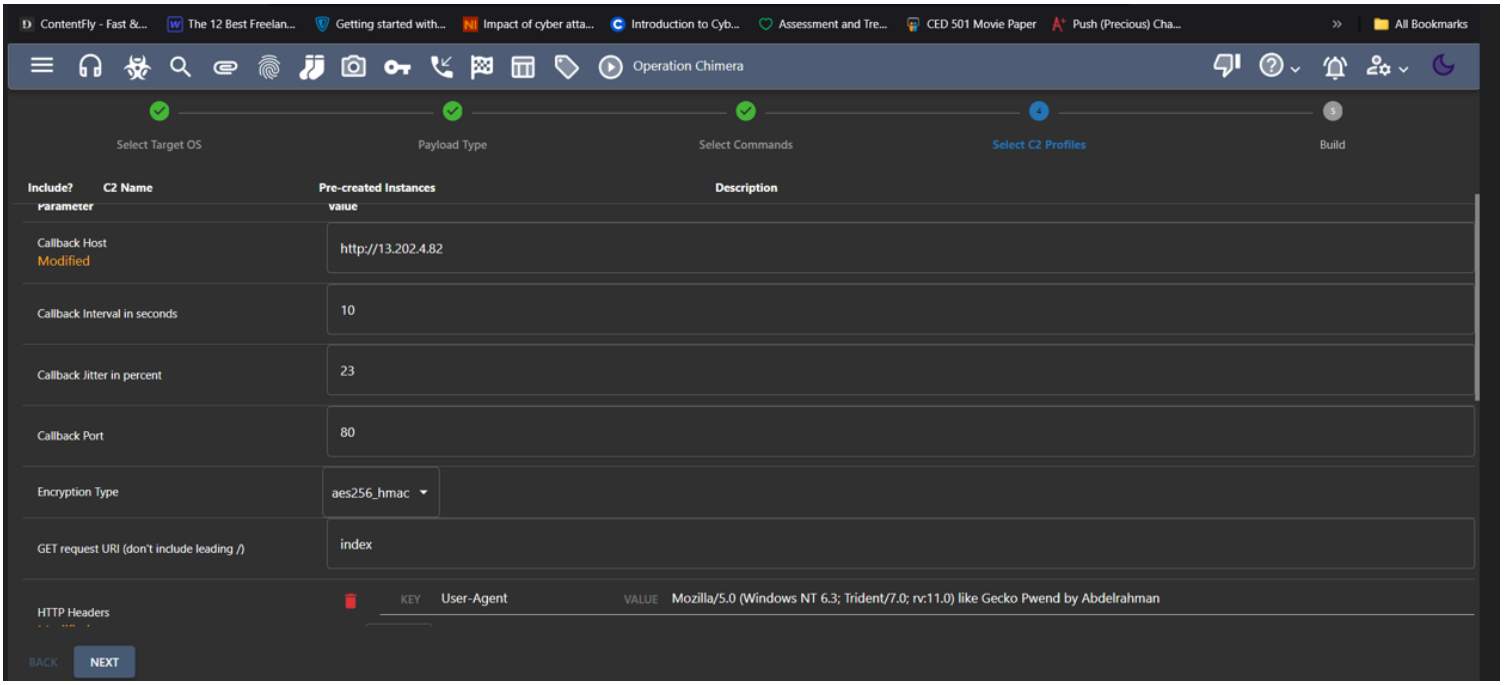
1- Click on Payload Icon



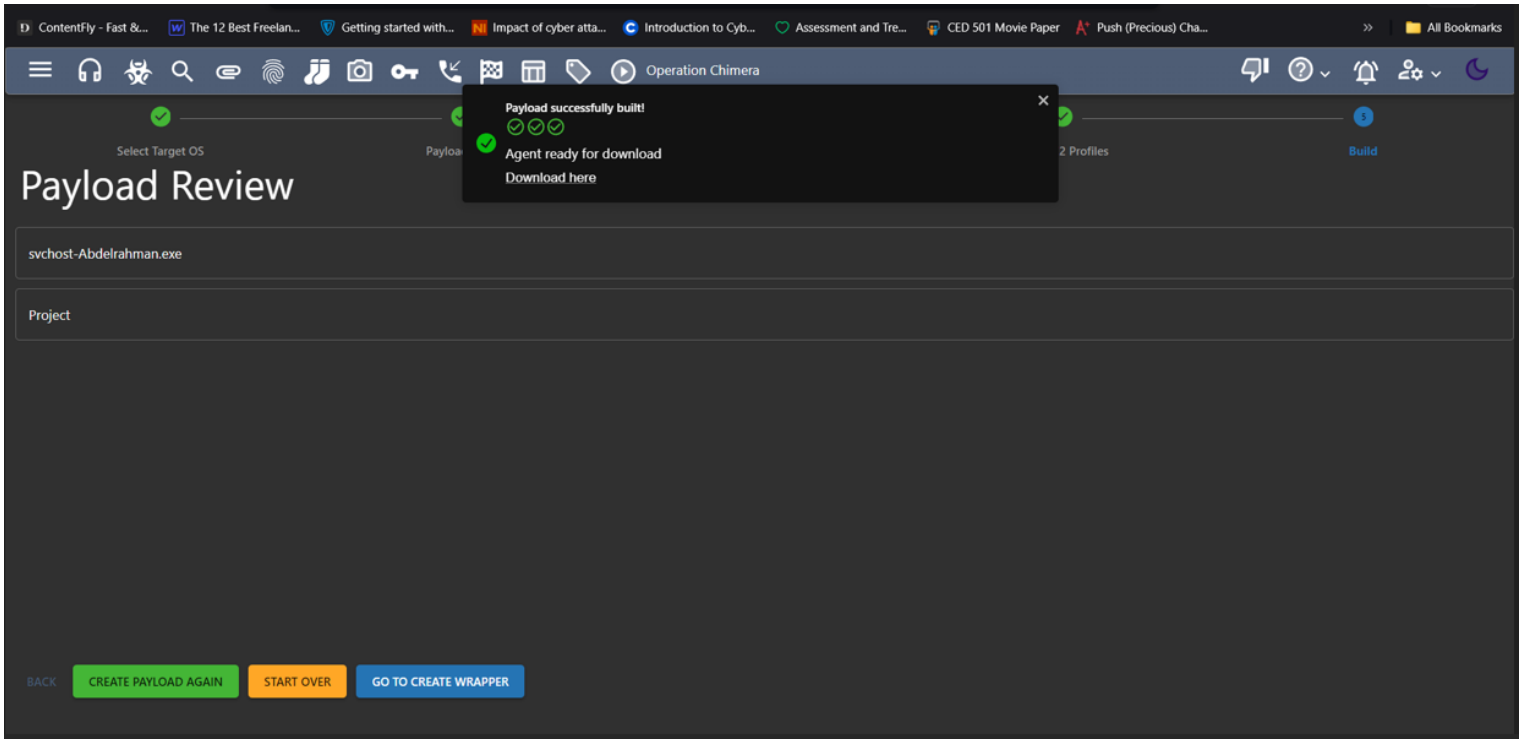
2- Choose the commands that we want to execute on our victim



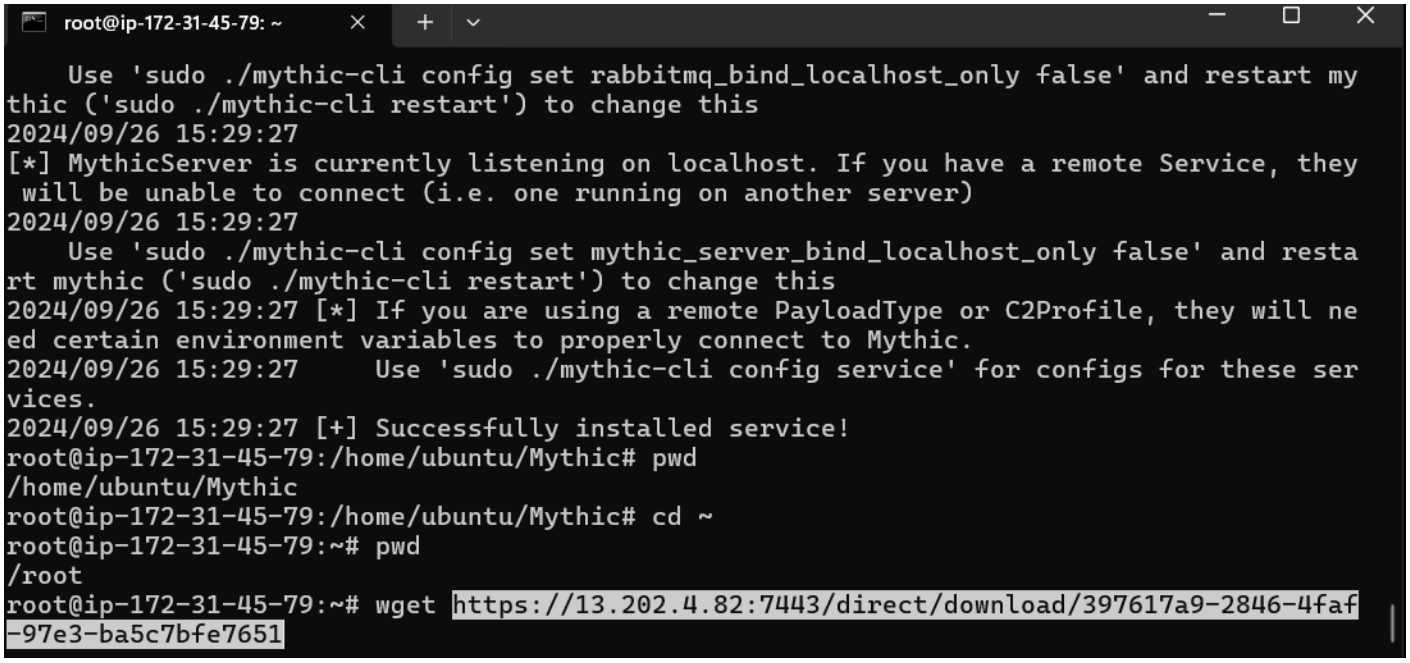
3- Configuration

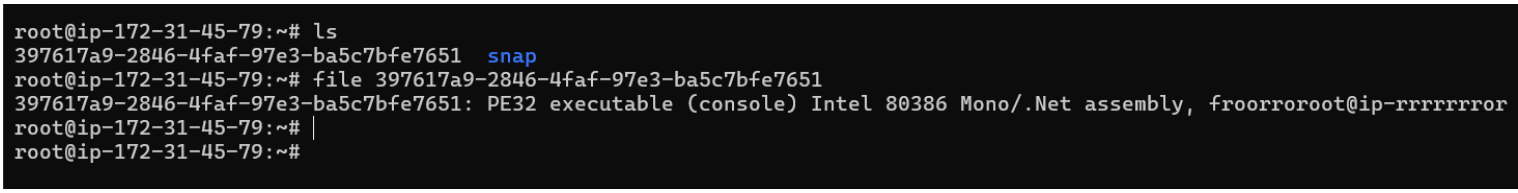


4- Rename the payload and download it

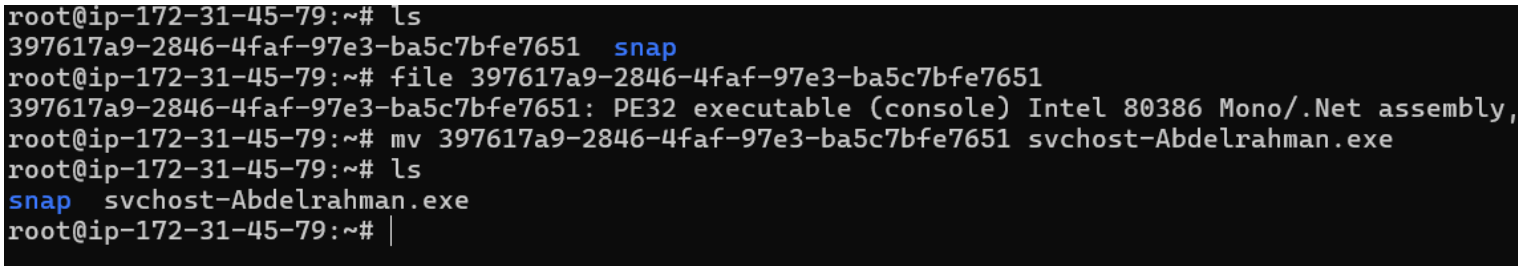


5- Now, I will download the Payload in our Ubuntu to change its name

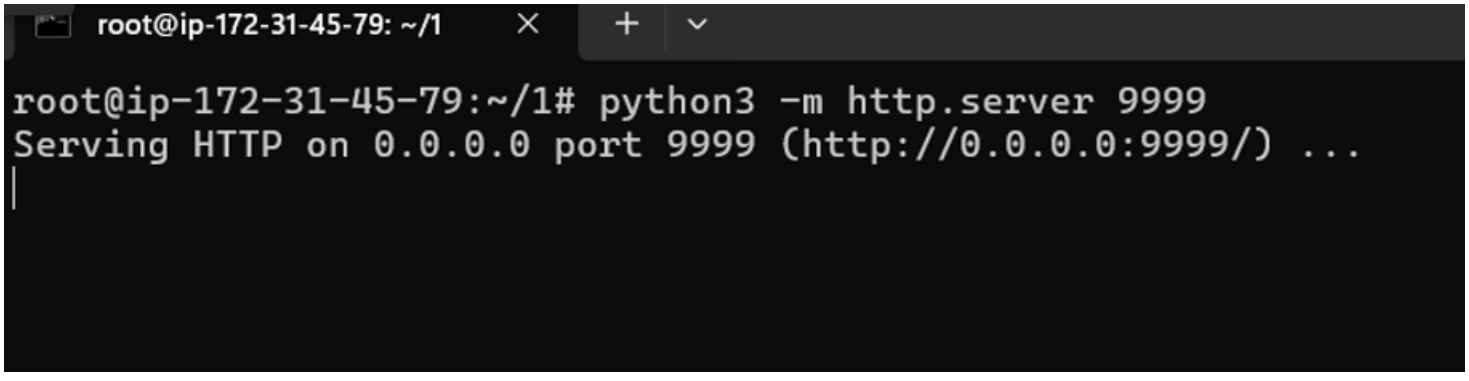




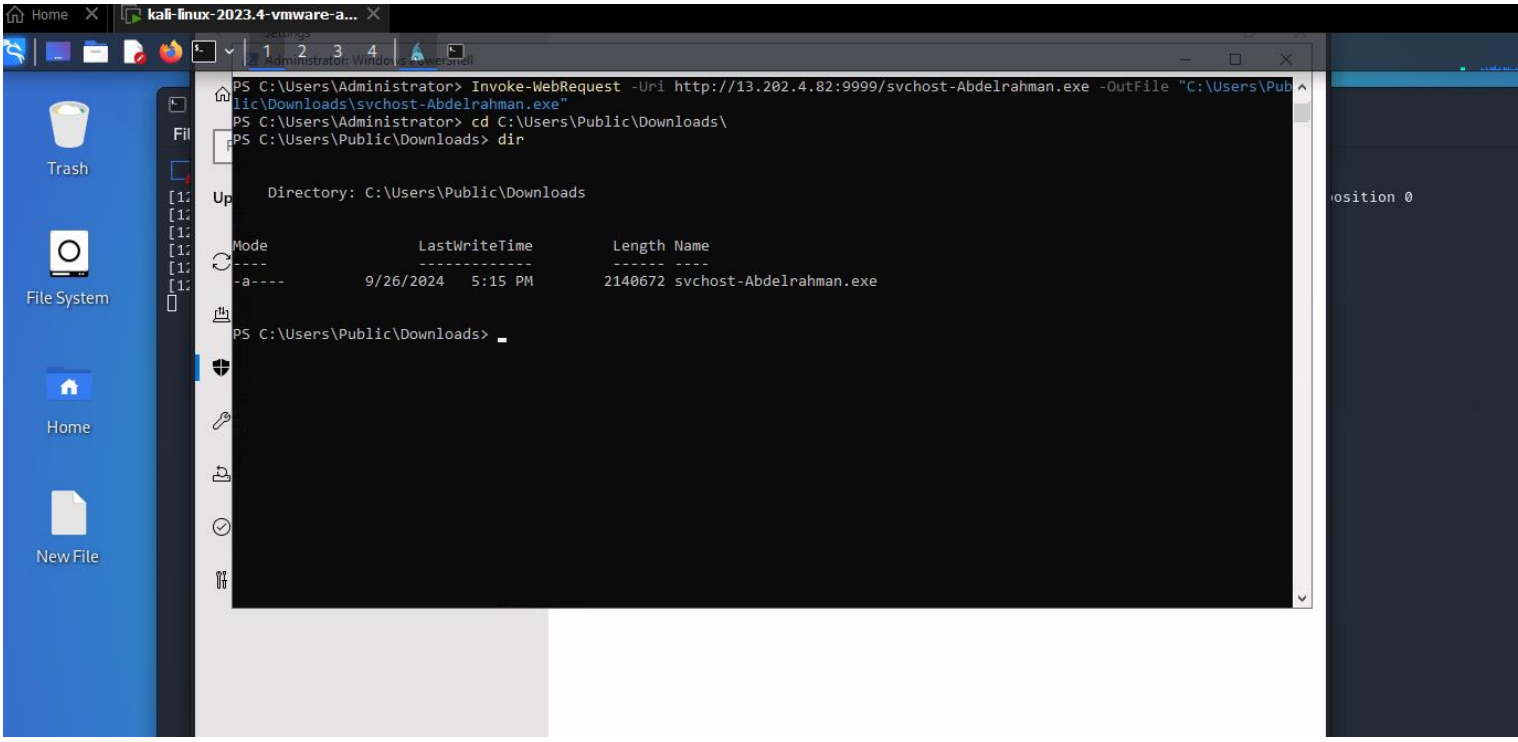
- As shown above, it's a PE32 executable file



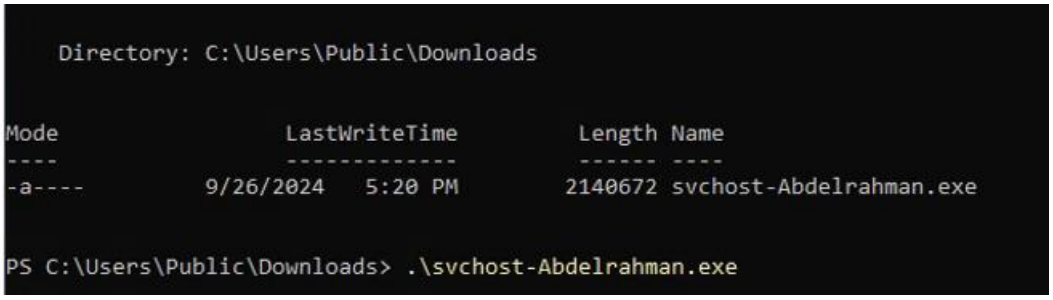
6- Now, I will use a module in python to open a session and listen from our payload



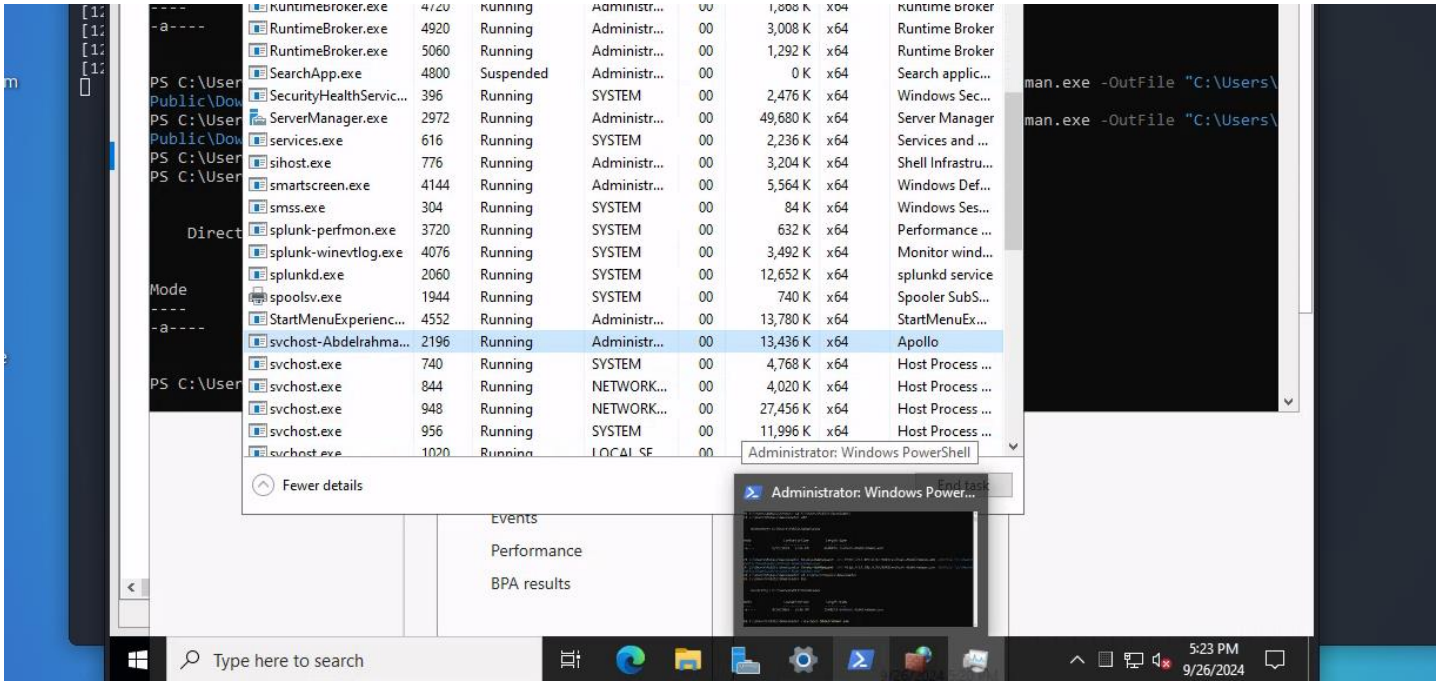
7- I will download the Payload now using PowerShell Function ‘Invoke-WebRequest’



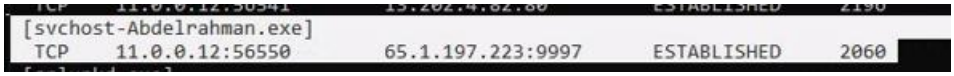
- The Payload is downloaded, lets run it



8- If we check the running process, we will see our Payload

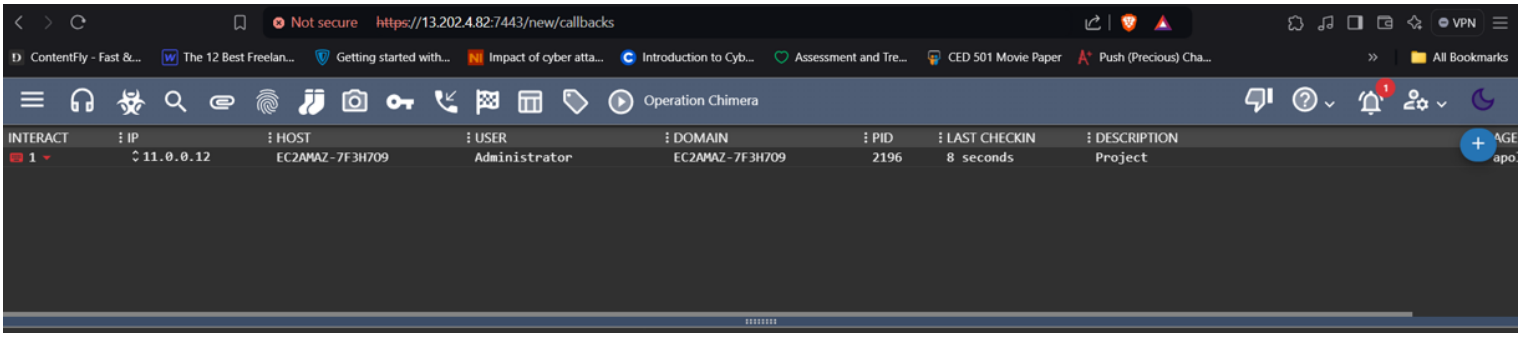


9- By checking the network connection with ‘netstat -anob’ we will see that the connection is established between our C2 Server and Victim

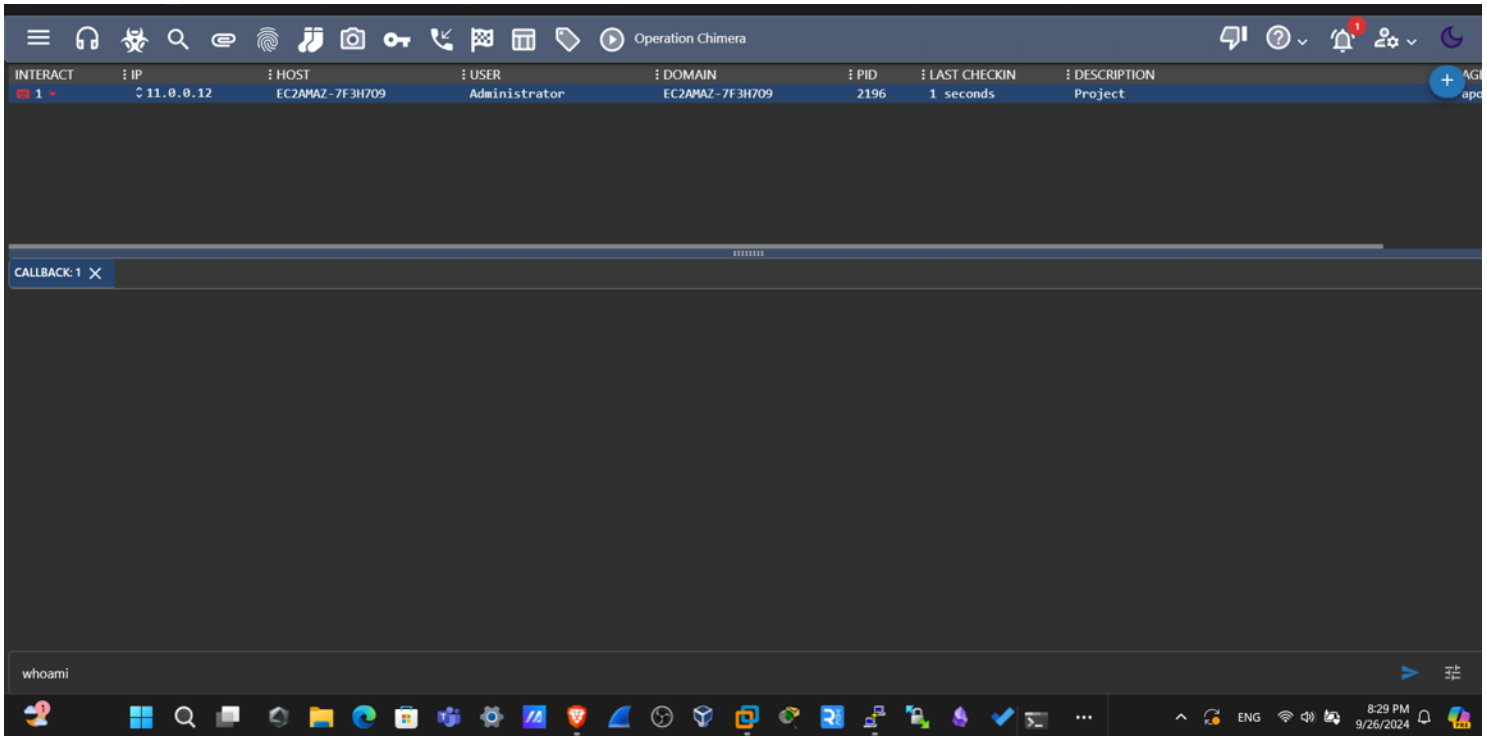


Phase 6: Command & Control (C2)

After establishing a session between C2 server and Victim, we can control the victim using our C2 Server

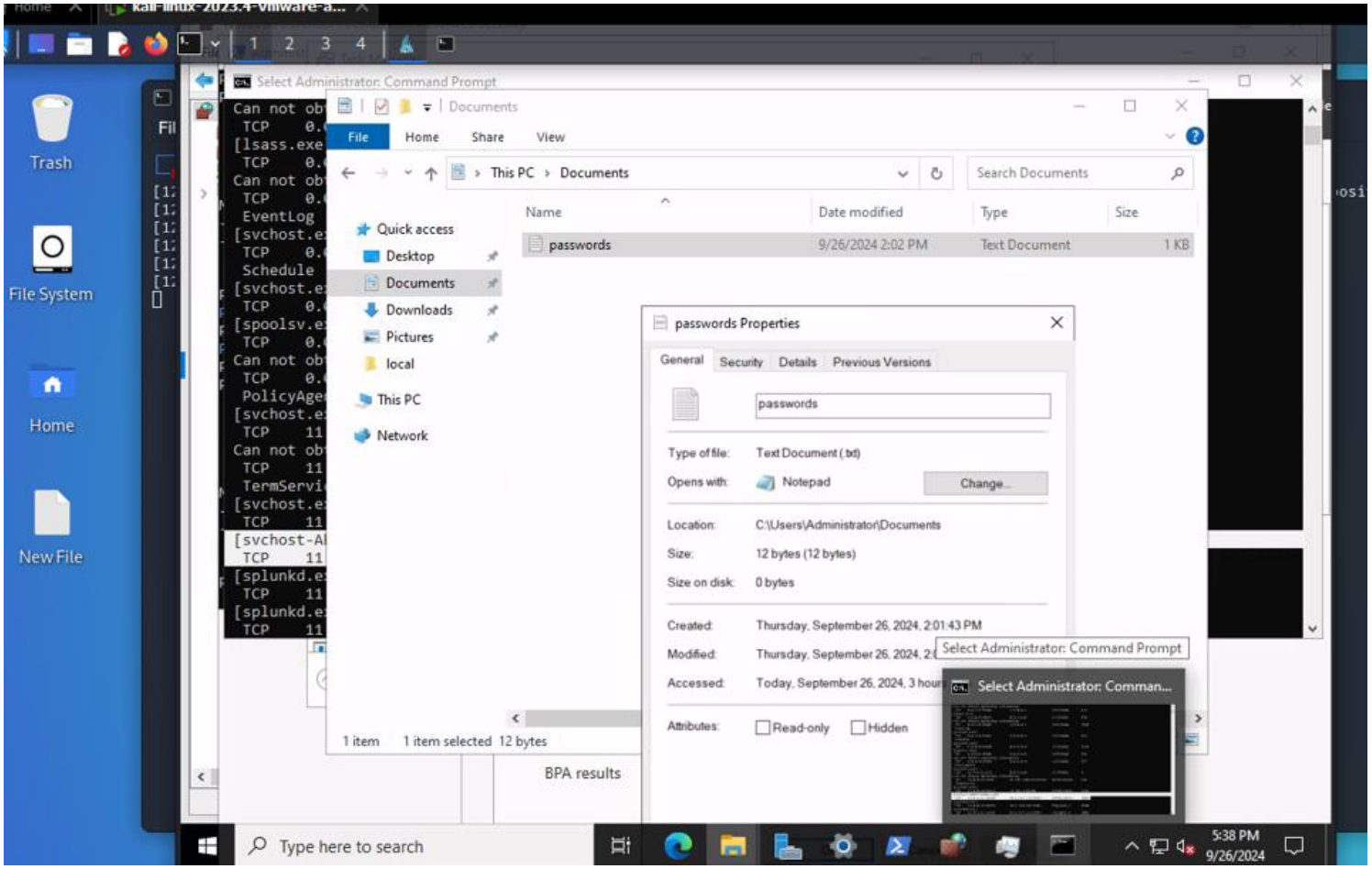


- Performing ‘Whoami’ command from C2 Server

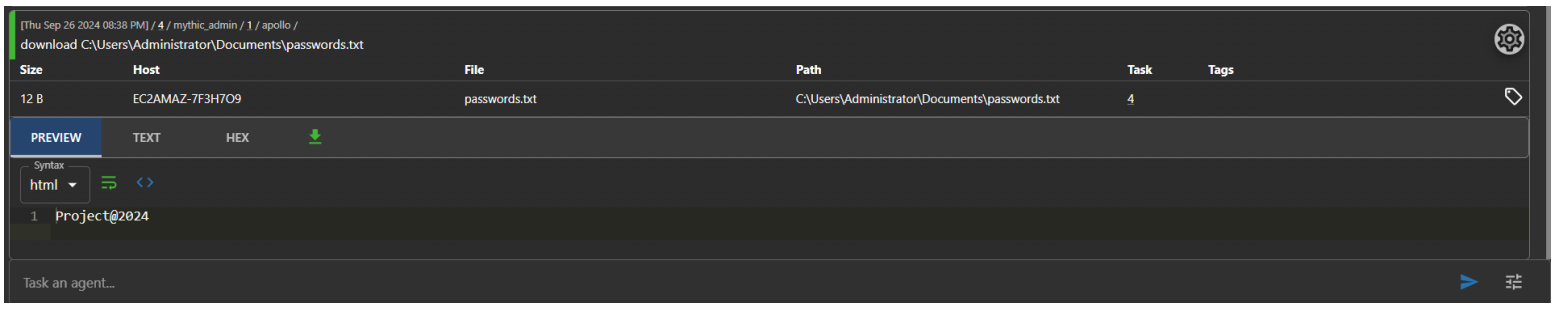


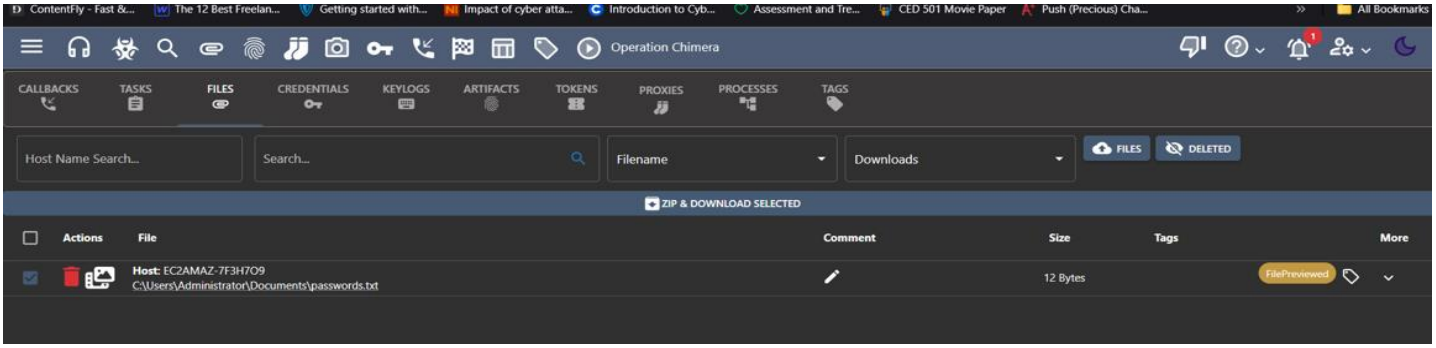
Phase 7: Data Exfiltration

After searching in our victim machine, I found an interesting file (Passwords.txt), So I will send this file to Mythic C2 Server.



- By using the following command ‘download C:\Users\Administrtator\Documents\passwords.txt’ I exfiltrated the file to C2 Server

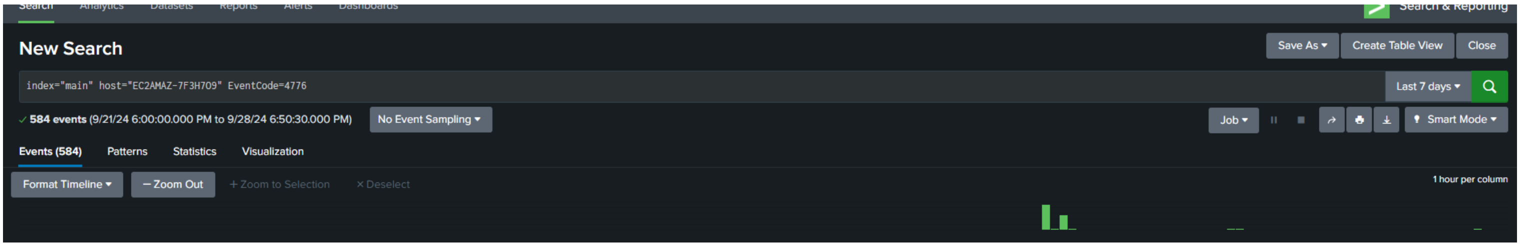


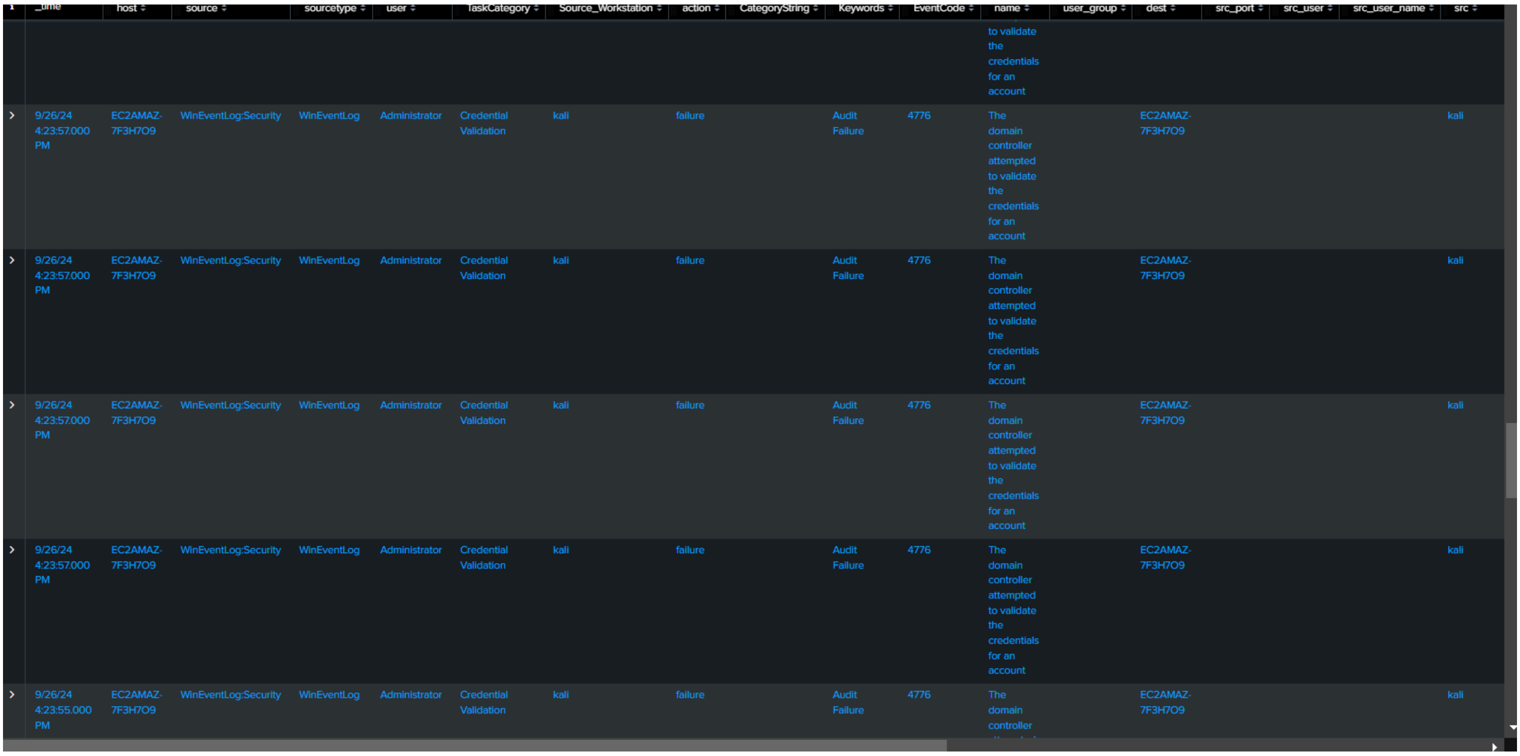


8-Detection Phase

From the logs that has been generated and forwarded to Splunk, we can detect the Attack happened

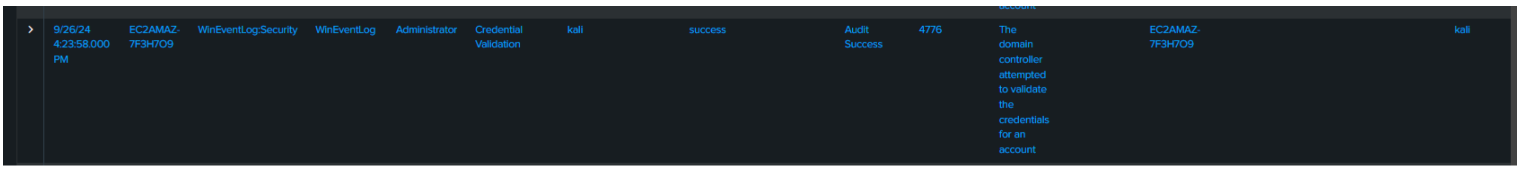
We will check Event Code = 4776, which used for credential validation



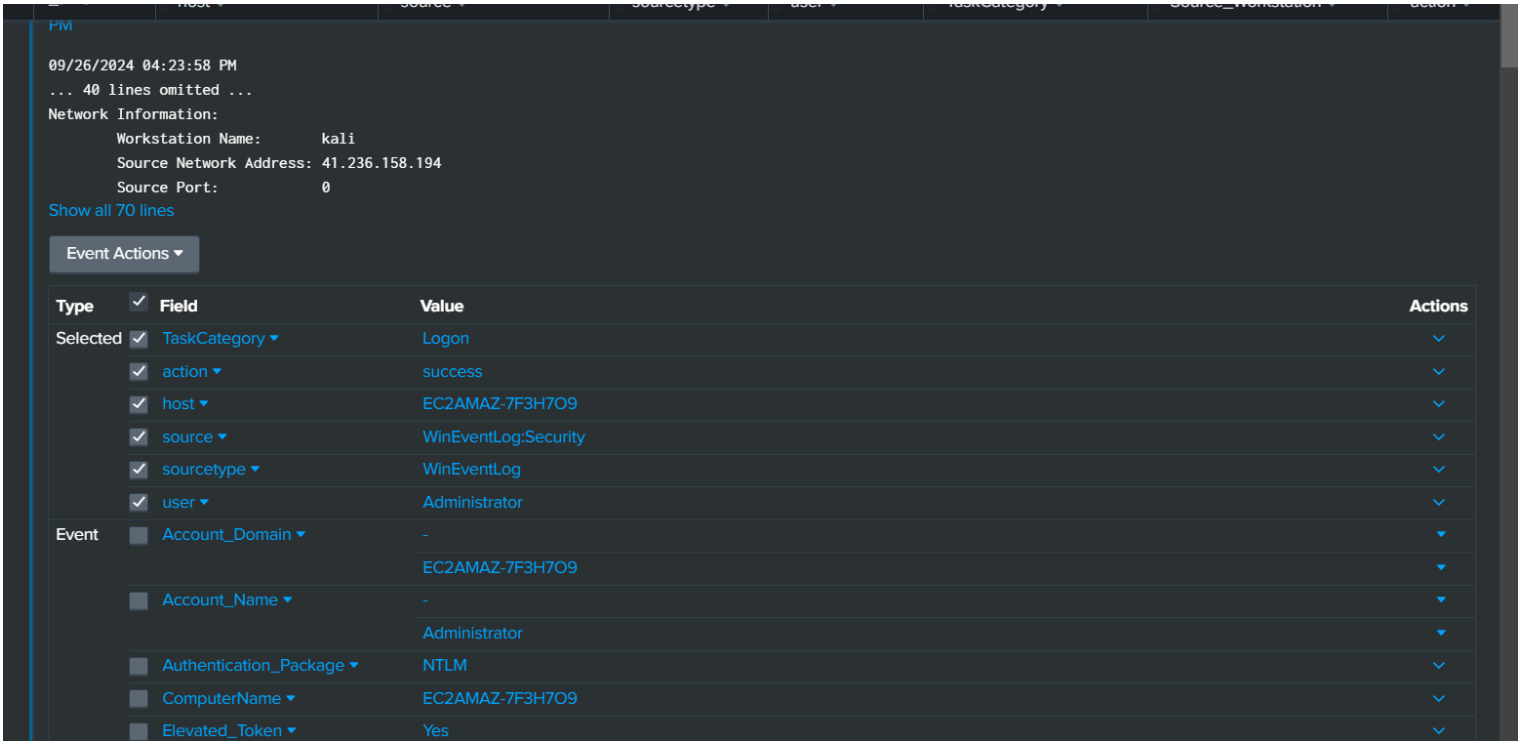


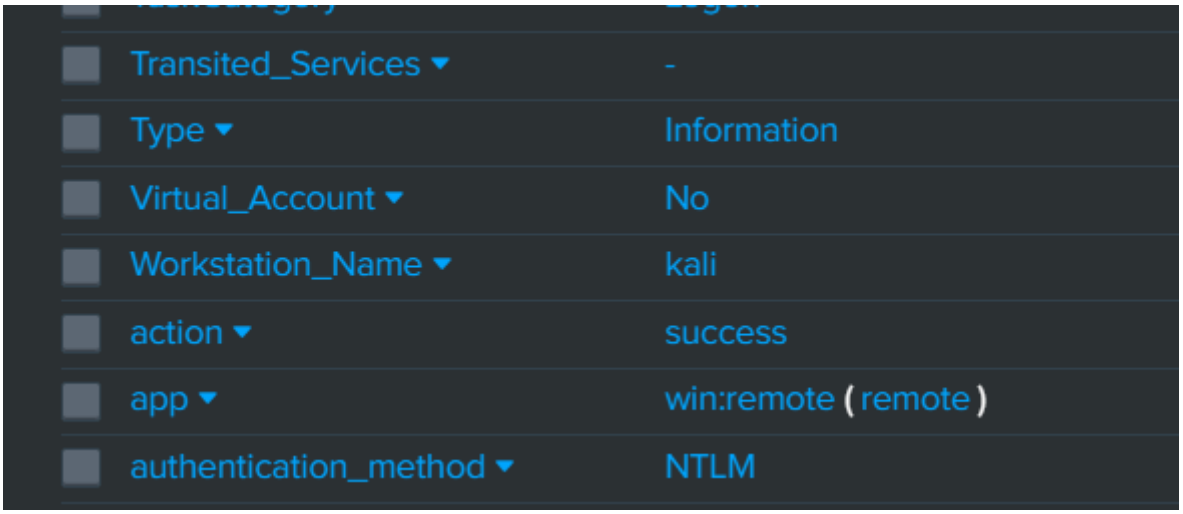
- If we took a closer look at the logs above, we could detect some unusual behavior

1- The time stamp is so close in each log
2- Repeated failure action
3- After many frequent failure actions, there is a Success action



Analyzing the logs





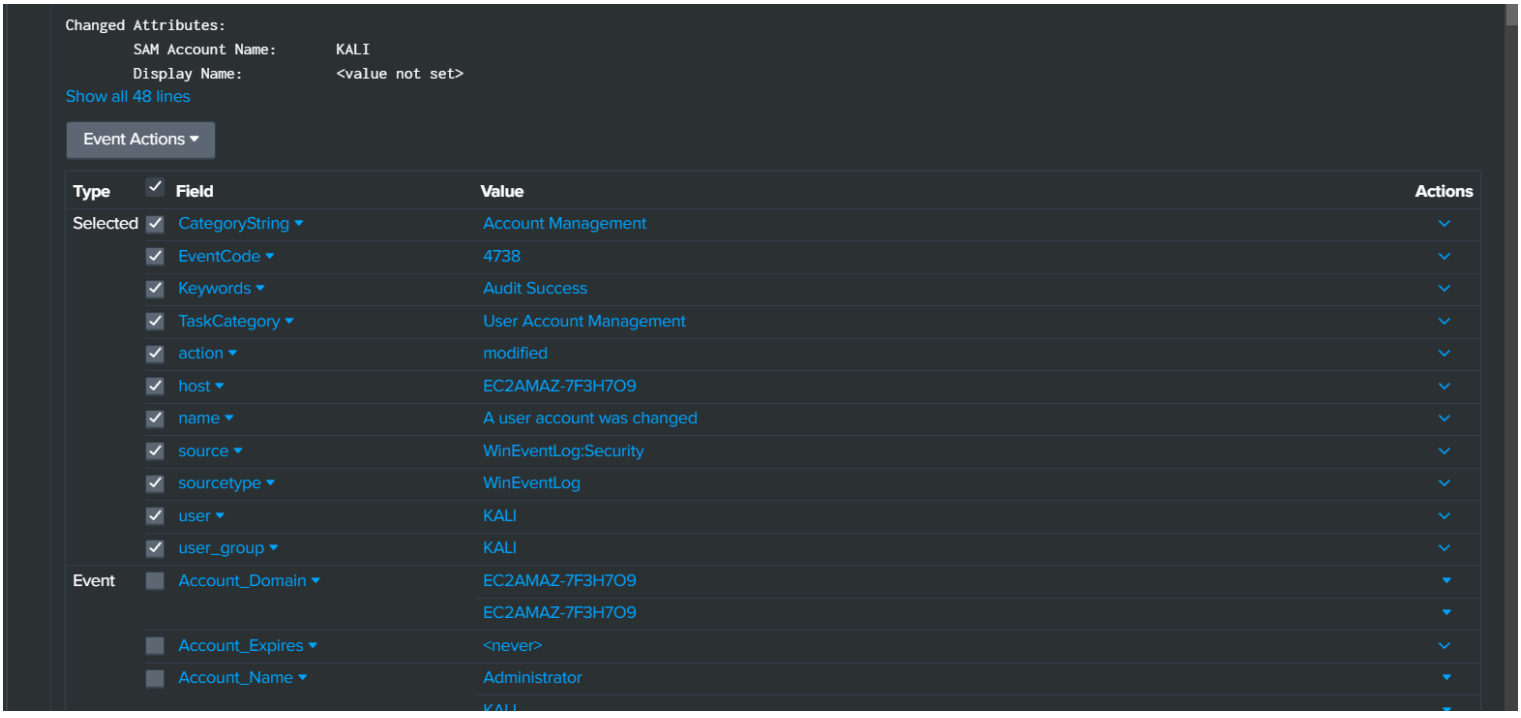
- We deduce that the attacker after many frequent failures, he successfully brute forced the password and logged into the machine
- Attacker_Workstation_Name = Kali
- Attacker_IP_Address = 41.236.158.194

- Now we would try to find if the attacker gained unauthorized privilege or created any other users

Table ▾ | Format | 50 Per Page ▾ | < Prev | 1 | 2 | 3 | 4 | 5 | Next >

i	_time	host	source	sourcetype	user	TaskCategory	Source_Workstation	action
>	9/26/24 4:41:19.000 PM	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	KALI	User Account Management		modified
>	9/26/24 4:41:19.000 PM	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	KALI	User Account Management		modified
>	9/26/24 4:41:19.000 PM	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	KALI	User Account Management		created
>	9/26/24 4:23:58.000 PM	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	Administrator	Logon		success
>	9/26/24 4:23:58.000 PM	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	success
>	9/26/24 4:23:57.000 PM	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	Administrator	Logon		failure
>	9/26/24	EC2AMAZ-7F3H7O9	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	failure

- As shown above the attacker after gaining access to the victim machine, he created a new User called ‘KALI’



```
Changed Attributes:
        SAM Account Name:       KALI
        Display Name:           <value not set>
```

Show all 48 lines

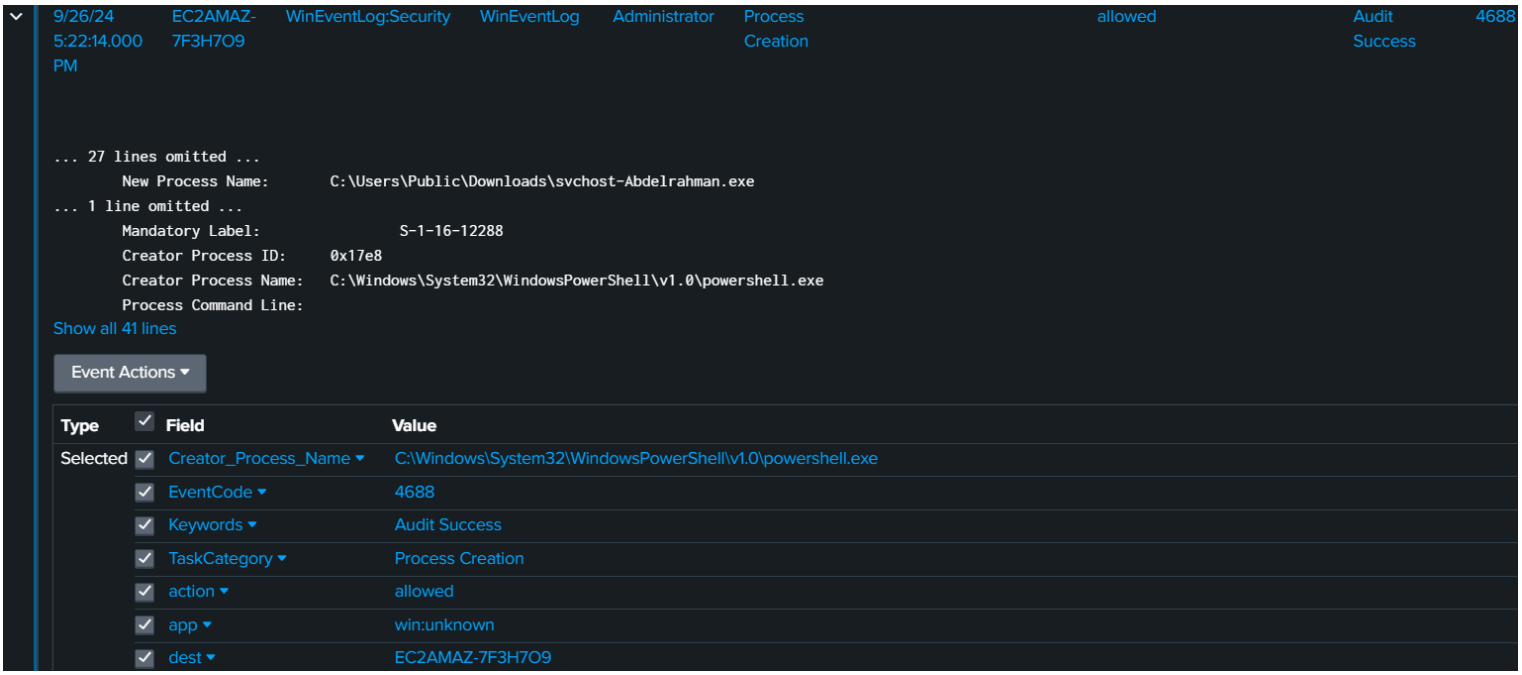
Event Actions ▾

Type	Field	Value	Actions
Selected	CategoryString ▾	Account Management	
	EventCode ▾	4738	
	Keywords ▾	Audit Success	
	TaskCategory ▾	User Account Management	
	action ▾	modified	
	host ▾	EC2AMAZ-7F3H7O9	
	name ▾	A user account was changed	
	source ▾	WinEventLog:Security	
	sourcetype ▾	WinEventLog	
	user ▾	KALI	
	user_group ▾	KALI	
Event	Account_Domain ▾	EC2AMAZ-7F3H7O9	
		EC2AMAZ-7F3H7O9	
	Account_Expires ▾	<never>	
	Account_Name ▾	Administrator	
		KALI	

Checking unusual processes

process_exec	count	percent
SecurityHealthService.exe	1	0.017816
Taskmgr.exe	1	0.017816
svchost-Abdelrahman.exe	1	0.017816

- We can see a process called ‘svchost-Abdelrahman.exe’ which is a malicious process related to the payload we have created

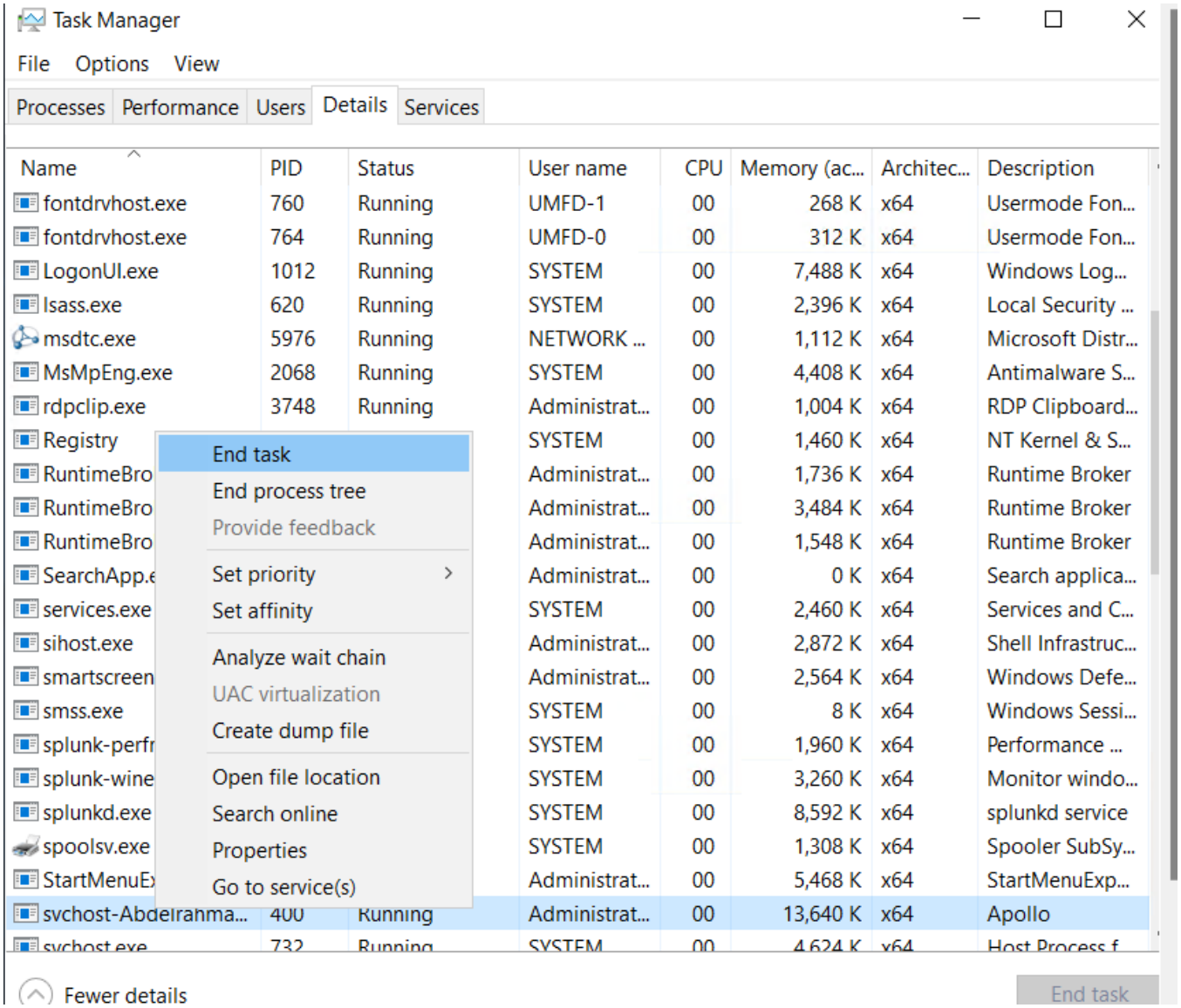


9-Containment Phase

In this phase, we will see how to contain this incident to avoid spreading it in our network.

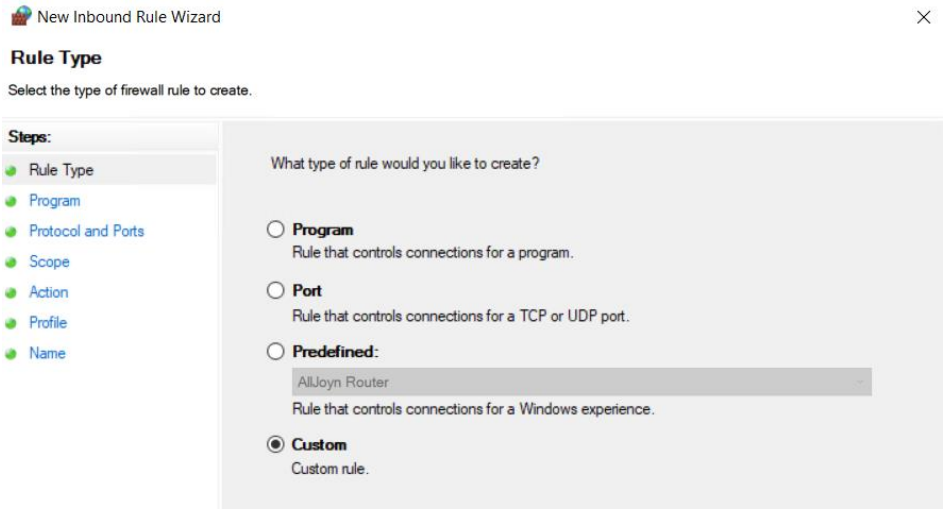
Steps

1. The first step in containment is to isolate the affected **Windows Server** to prevent the attacker from continuing to interact with it and spreading further into the network.
2. Once the server is isolated, it is essential to terminate any **active C2 connections** between the attacker and the server.

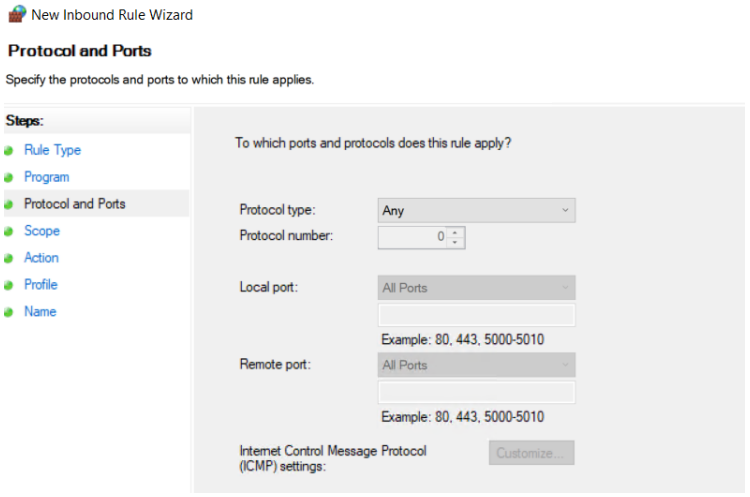


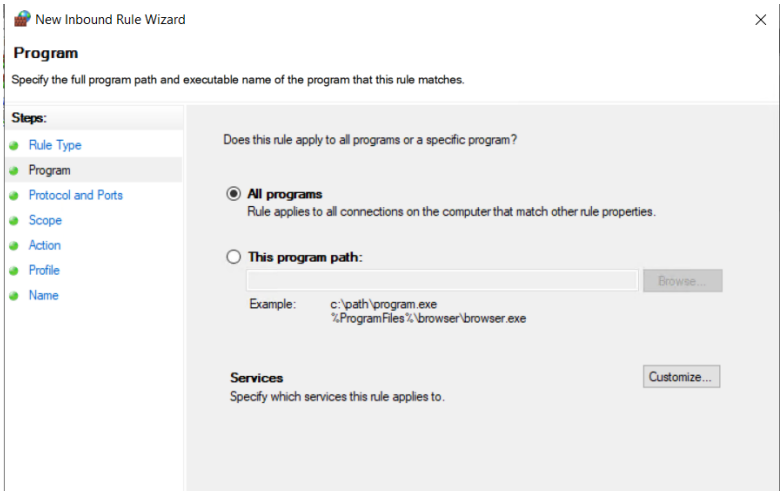
3. Since the attack originated from the **Kali Linux machine**, its IP address can be blocked to prevent any further communication attempts with the compromised server.

   1- Open windows firewall, click on **Inbound Rules** then **New Rule**

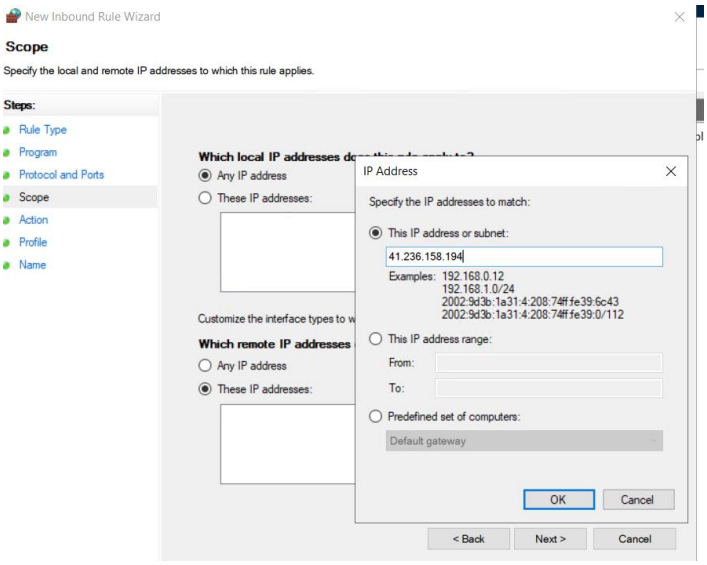


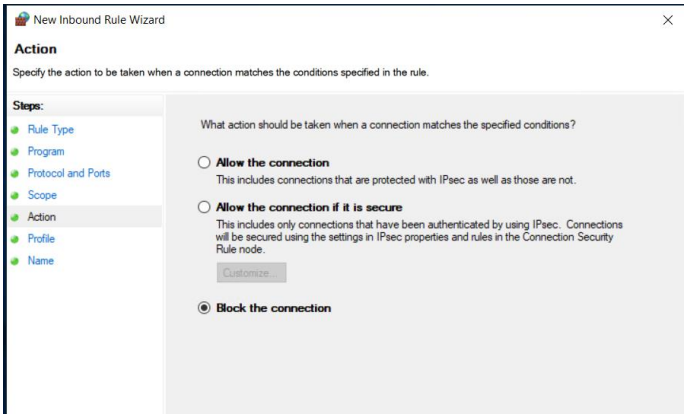
   2- Choose custom rule

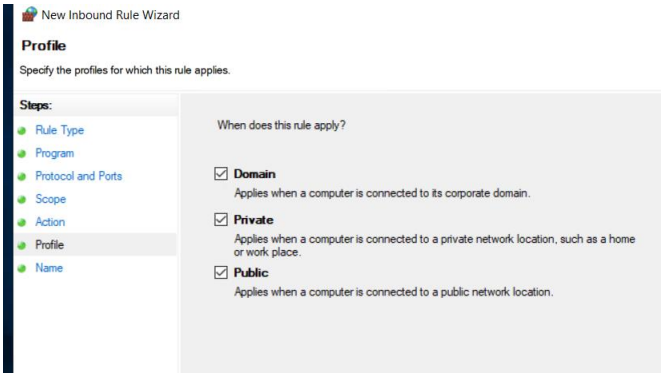


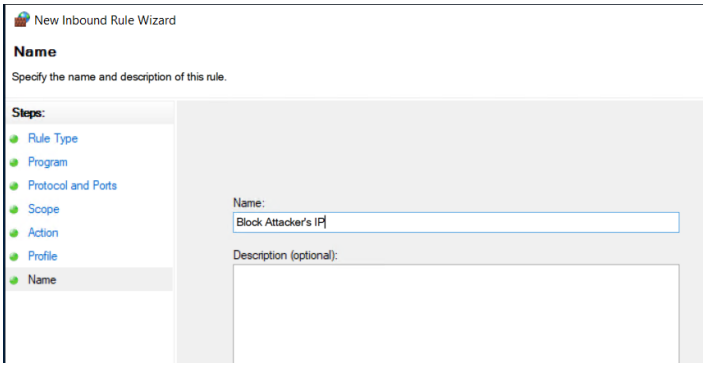


3- Add the attacker's IP address to block it

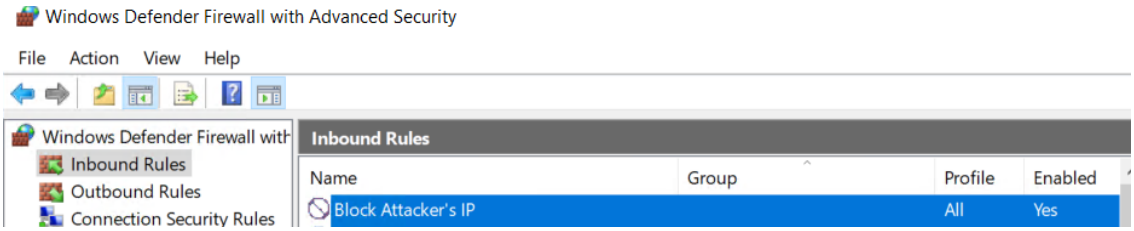








4- The rule we created



4- Remove any unauthorized users

5- Since the attacker disabled **Windows Defender**, it must be re-enabled to provide protection against further malware or persistence mechanisms.

6- Use Complex Passwords and a strong Group Policy

10-Lessons Learned

1- **Importance of Strong Authentication and Access Controls**

Lesson: The attack was successful due to weak authentication mechanisms (brute-force vulnerability on RDP). This demonstrates the necessity of robust authentication methods and ensuring that sensitive services like RDP are not exposed to the internet.

Action: Implement **multi-factor authentication (MFA)** for RDP and all privileged accounts. Consider **disabling RDP** or exposing it only through secure methods like **VPN** or **bastion hosts**.

2- **Early Detection and Monitoring are Essential**

Lesson: The attacker disabled **Windows Defender**, which remained undetected. Better endpoint monitoring and alerting mechanisms could have detected the attacker's presence earlier, before deeper compromise occurred.

Action: Deploy **endpoint detection and response (EDR)** solutions across critical systems. Ensure **real-time monitoring** for suspicious activities, such as disabling security services, unexpected PowerShell commands, or abnormal RDP sessions.

3- **The Need for Regular Vulnerability Assessments**

Lesson: The attacker gained initial access by exploiting an open RDP port, showing that regular vulnerability assessments and hardening processes should be part of routine operations.

Action: Conduct regular vulnerability scans to identify and remediate open ports, weak services, and other misconfigurations.

4. Defense Evasion Techniques Must Be Anticipated

Lesson: The attacker used defense evasion techniques, such as disabling Windows Defender and bypassing security controls. Anticipating and detecting these types of evasion tactics is key.

Action: Set up security baselines and implement continuous integrity monitoring to detect any unauthorized changes in security configurations.