



Command & Control in Purple Teaming

Workshop on SIEM, C2 Servers, and Real-Time Detection

- Chinamay Joshi

Deputy Manager - Red Teaming

Whoami!

Introduction:

- 4+ years in Red Teaming, VAPT, and SOC operations.
- Worked with major banks, government agencies, and the BFSI sector.

Professional Experience:

- Simulated advanced attacks, Thematic and goal based Red Team simulation.
- Specialized in exploiting vulnerabilities, lateral movement, and bypassing security controls.
- Hands-on with SIEM, XDR.
- Secured networks and endpoints in high-stakes environments.

Contributions to the Field:

- Published CVEs :
- CVE-2023-37569
- CVE-2023-37570



Agenda

- Intro to Purple Teaming.
- Blue Team Phase: SIEM (Elastic Stack, Fleet, Sysmon).
- Red Team Phase: C2 Servers, Payloads, Exploits.
- Purple Teaming: Detection and Log Analysis
- Bonus Content
- Conclusion
- Q&A & Giveaway



When you see a long agenda
but you're here for the memes.



What is Purple Teaming?

Purple Teaming combines both Red Team (offensive) and Blue Team (defensive) strategies to improve security detection, response, and overall defense mechanisms. The collaborative bridge between Red and Blue Teams. Red identifies gaps, while Blue refines defensive strategies, working together to improve overall detection and response capabilities.



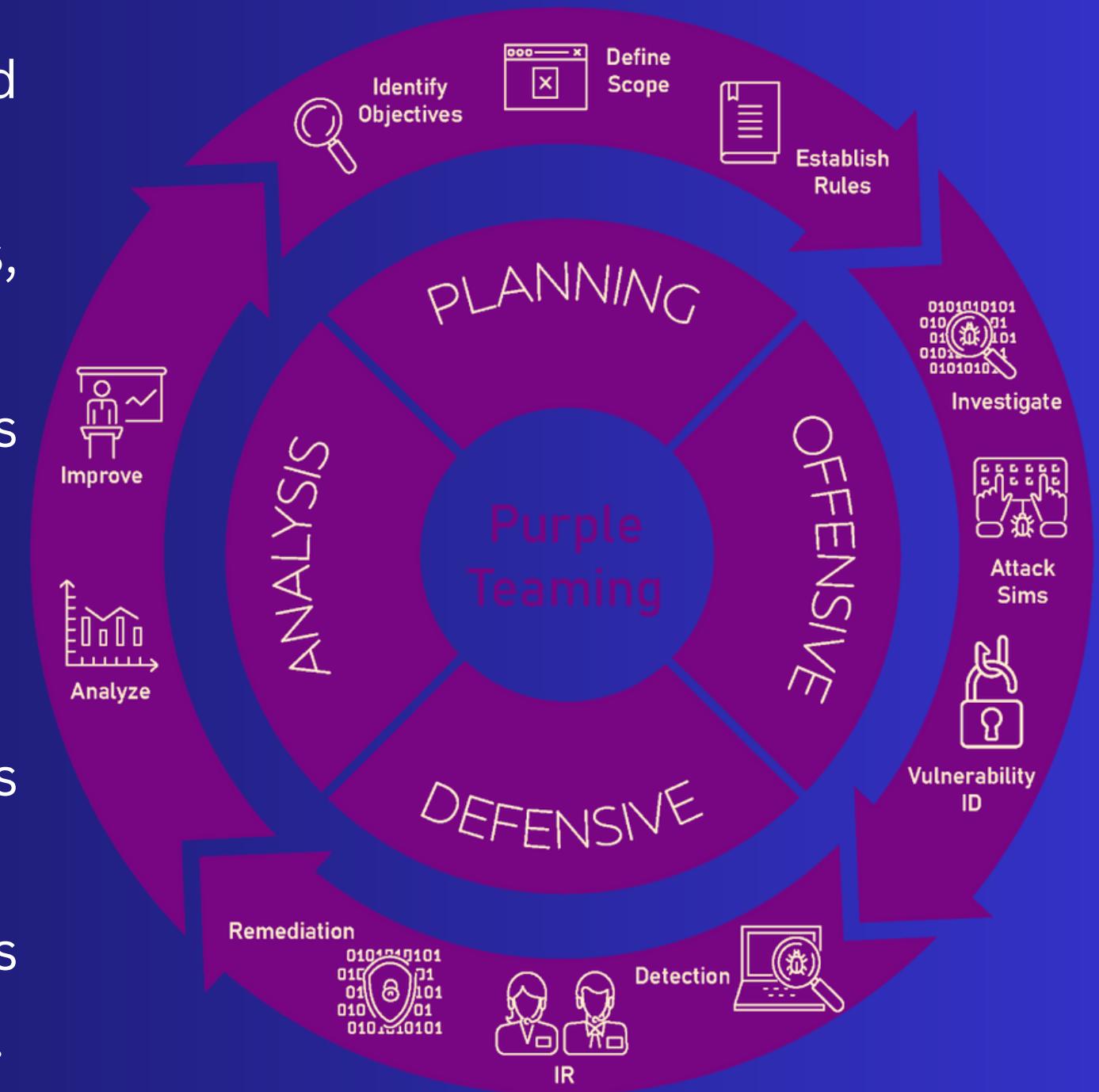
Why Purple Teaming is Critical?

The Modern Threat Landscape:

- Cyberattacks are becoming more advanced, persistent, and sophisticated.
- Traditional Red and Blue Team approaches often work in silos, leading to slower detection and responses.
- Attackers exploit gaps in defenses quickly, and organizations must adopt more agile strategies to respond.

Challenges with Traditional Approaches:

- Red Teaming: Focuses on finding vulnerabilities but often lacks involvement in remediation.
- Blue Teaming: Detects and responds to incidents but may miss advanced techniques or be overwhelmed by the volume of data.
- Problem: Without collaboration, crucial insights may not be shared, leaving gaps in defenses.



Purple Teaming's Role:

- Continuous Feedback Loop: Red Teams simulate attacks, Blue Teams detect and defend, and both provide instant feedback to each other.
- Helps quickly identify, patch, and improve security gaps with hands-on collaboration.
- Empowers the organization to improve detection and response mechanisms in real-time.

Improving Security Posture:

- Enables proactive defense against evolving threats.
- Results in stronger incident response capabilities, better defense tactics, and quicker remediation.
- Increases understanding of attacker behavior, leading to more refined defensive strategies.



THIS IS WHERE THE FUN BEGINS.

SIEM Overview (Elastic Stack)

What is a SIEM? (Security Information and Event Management)

- A SIEM is a centralized platform that collects, analyzes, and correlates security data from across your network.
- It helps organizations detect, analyze, and respond to potential security threats in real-time.

Key Features:

- Log collection from multiple sources (hosts, applications, network devices).
- Event correlation and alerting.
- Forensic analysis and incident response.



ITS ELASTIC STACK.

Why Elastic Stack (ELK) as a SIEM?

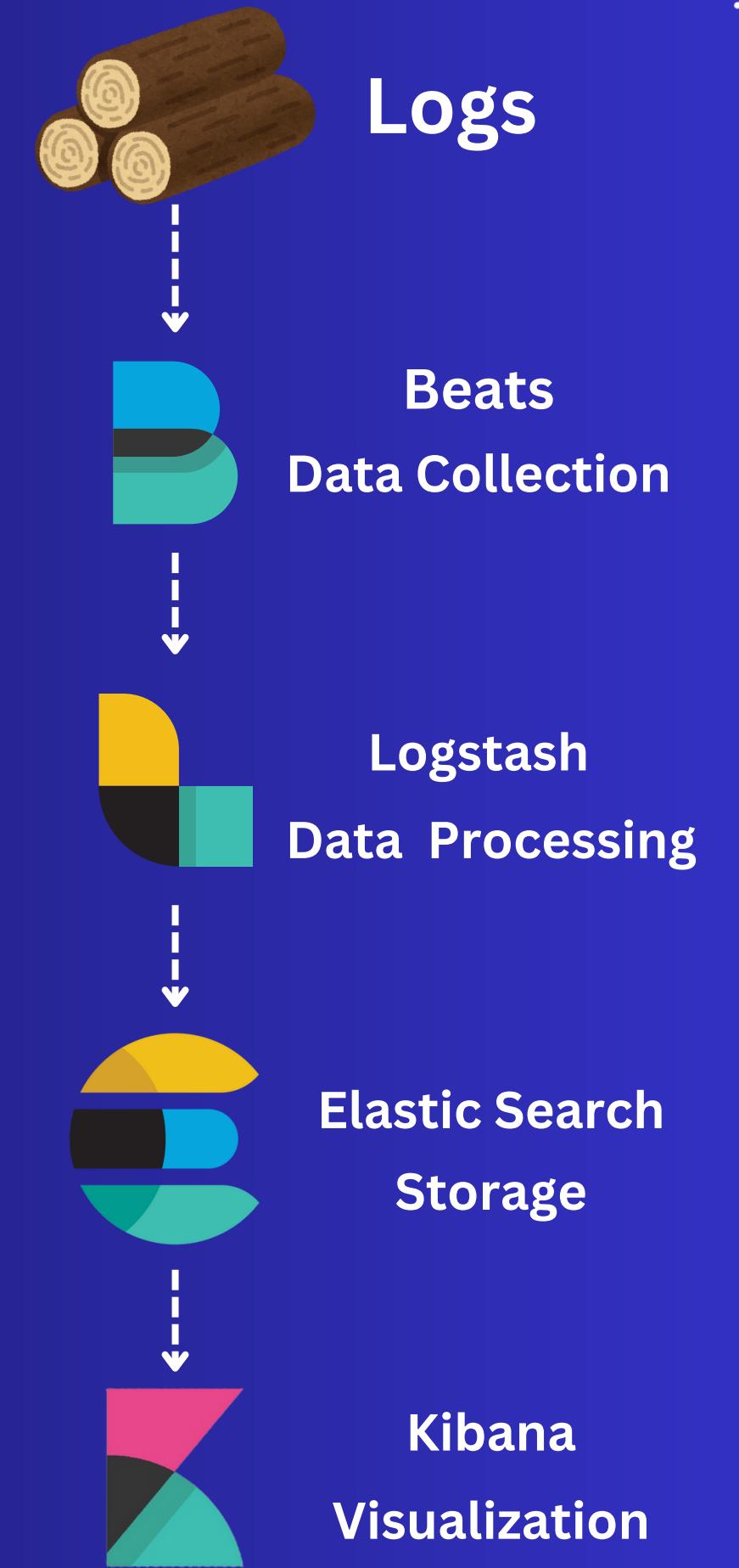
- Elastic Stack (also known as ELK) is a powerful open-source solution consisting of:
 - Elasticsearch: Stores and searches data.
 - Logstash: Gathers and processes logs from multiple sources.
 - Kibana: Visualizes and analyzes data in real-time dashboards.

Advantages of ELK:

- Open-source, highly customizable, and scalable.
- Real-time data ingestion and visualization.
- Can be used for both offensive and defensive security monitoring.
- Popular among Red and Blue teams for its flexibility and integration capabilities.

How Elastic Stack Fits into Purple Teaming:

- Red Team Perspective: Helps attackers simulate and monitor post-exploitation activities, such as detecting whether defensive mechanisms are in place.
- Blue Team Perspective: Acts as the detection and response platform to catch these activities in real-time.





Installation of Elastic Stack Using Docker

Using Docker :

Normally, Elastic Stack can be installed using Docker to containerize and manage its services easily.

However, due to limited resources on the local laptop, we will use the Elastic Cloud Free Trial instead. This provides a fully managed environment without needing to manage local infrastructure.



LOG ALL THE THINGS.

Fleet Server Configuration and Agent Installation

Overview of Fleet

Fleet serves as a powerful, centralized management tool within the Elastic Stack, designed to streamline the administration of Elastic Agents.

Deployment and Data Collection

Deploy Elastic Agents across diverse hosts seamlessly.

Agents collect crucial data types including logs, metrics, and security-related information, ensuring comprehensive visibility across your environment.

Simplified Management and Monitoring

Manage all agent configurations from a single, unified location.

Monitor the health and performance of all agents, making it easier to maintain system integrity and reliability.

The screenshot shows the 'Agent policies' tab in the Fleet interface. It displays a table with three rows:

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Agent policy 1 rev. 4	Oct 09, 2024	0 / 2 (2)	2	...
Fleet Server Policy rev. 1	Oct 09, 2024	0 / 0 (0)	2	...

Below the table, there are buttons for 'Reload' and 'Create agent policy'.

The screenshot shows the 'Agents' tab in the Fleet interface. It displays a table with three rows:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Offline	DESKTOP-PJ73A6T	Agent policy 1 rev. 4	N/A	N/A	1 hour ago	8.15.2	...
Offline	DESKTOP-PJ73A6T	Agent policy 1 rev. 1	Outdated policy	N/A	22 hours ago	8.15.2	...

Below the table, there are filters for 'Status', 'Tags', 'Agent policy', and 'Upgrade available'. There are also buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent'.



INSTALL COMPLETE.



What is Sysmon and Why It's Overlooked by Many SOCs

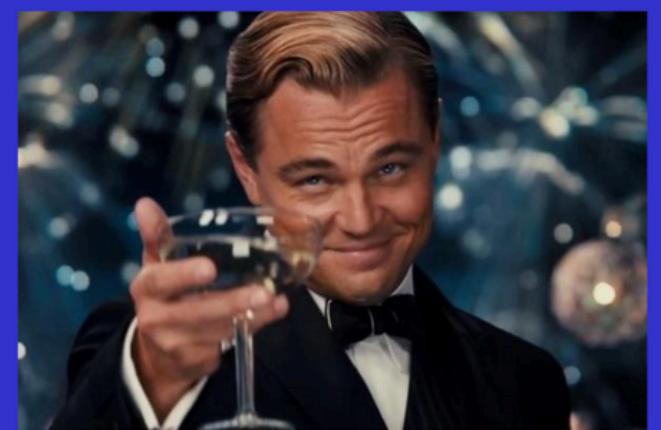
What is Sysmon?

Sysmon, or System Monitor, is a robust Windows service designed by Microsoft to provide detailed logging of system activity. It tracks and logs events such as process creation, network connections, and file modifications, aiding in forensic analysis and security monitoring.

Why Sysmon is Often Overlooked ?

- **Complexity in Configuration:** Setting up Sysmon can be intricate, requiring detailed knowledge of system events and security implications.
- **Visibility vs. Utility:** While Sysmon provides invaluable data for security professionals, its utility might not be immediately apparent to general IT teams or management, leading to underutilization.
- **Resource Requirements:** Continuous detailed logging can consume system resources, which might deter its use in environments where performance is a priority.

When your SIEM catches everything.



What is a C2 Server? Real-World Use

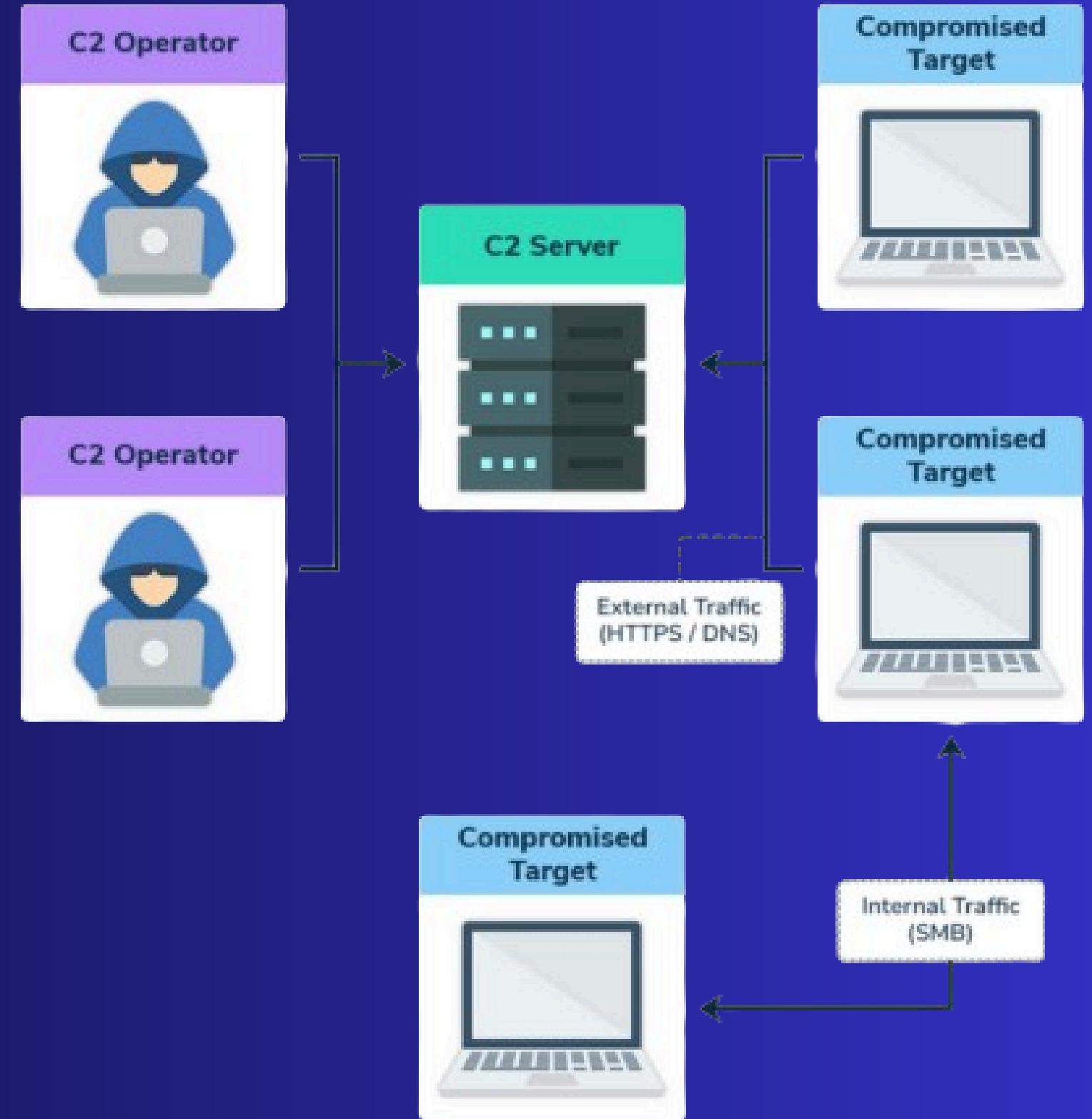
Definition:

A Command and Control (C2) server is used by attackers to manage and control compromised systems remotely.

Use Cases:

After compromising a target, attackers use the C2 server to issue commands, collect data, and maintain persistence.

C2 servers are integral to real-world attacks where adversaries need to control multiple systems.



Havoc C2 Server Overview

What is Havoc C2?

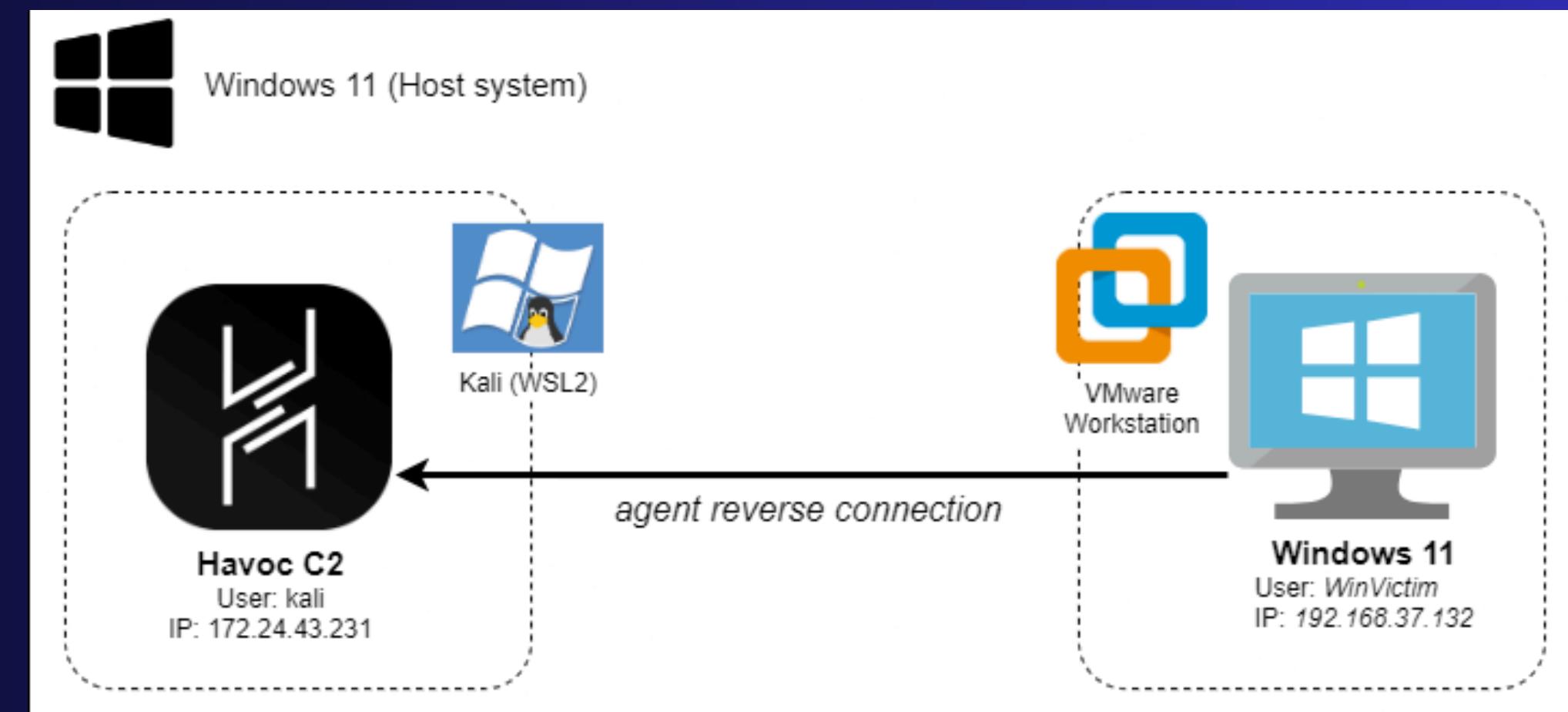
A modern, open-source Command and Control (C2) framework. Designed for Red Team operations with a focus on lightweight, stealthy tactics.

Why Havoc C2?

Ideal for stealthy, efficient Red Team engagements. Offers flexibility and advanced capabilities for adversary simulation.

Demo Overview:

We will generate a payload using Havoc C2. Execute it on a target system to establish a covert connection.





the successful installation of
Havoc and the agent connection.



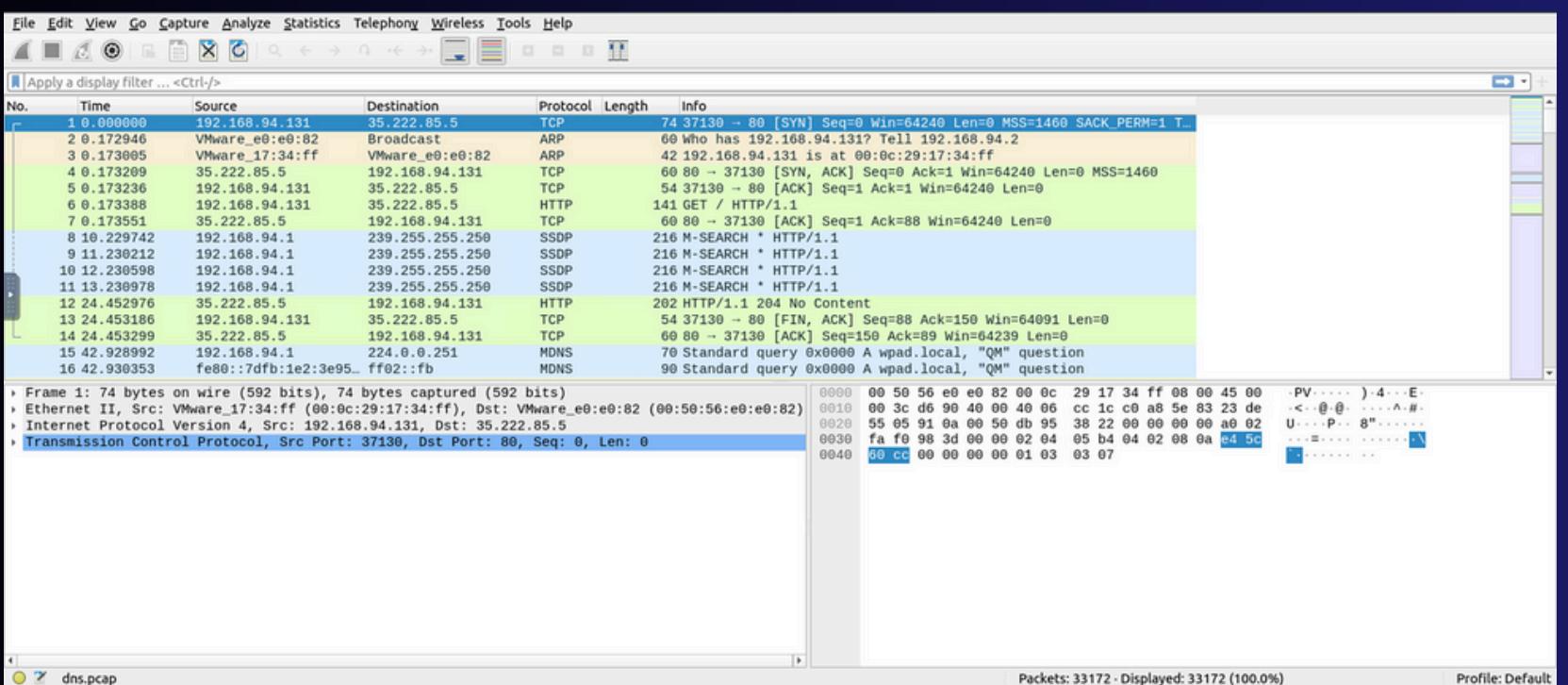


**Right after the agent successfully
communicates with Havoc.**

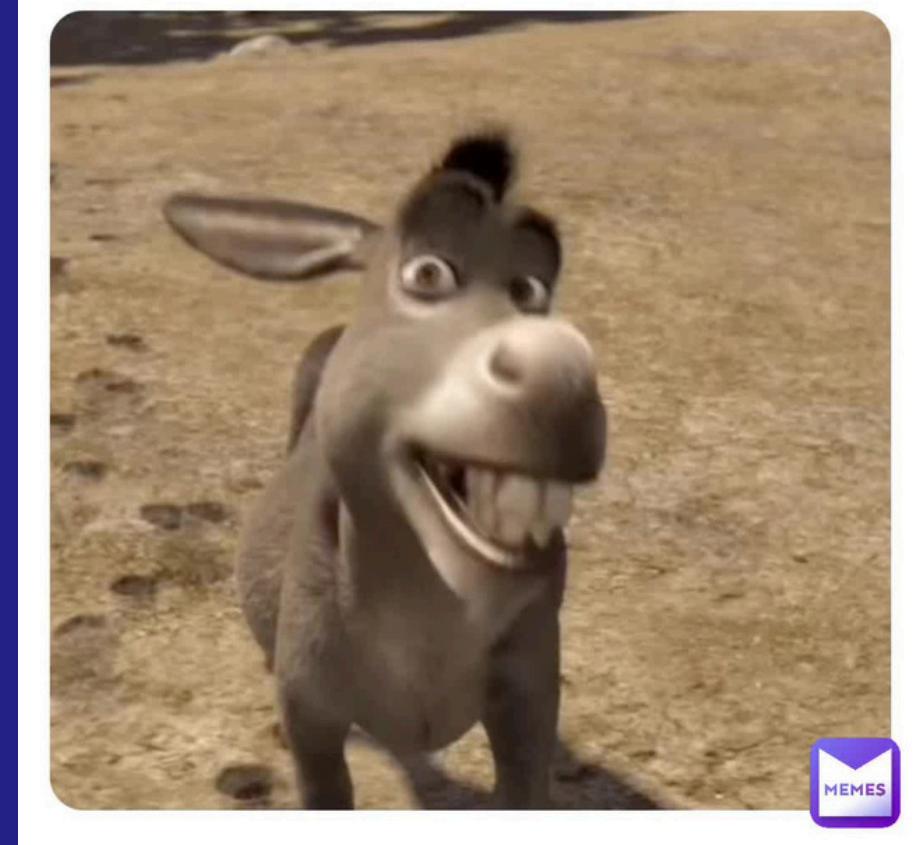


Log Analysis of Payload Execution

- After executing the payload, logs generated from the attack are collected and analyzed.
- Log analysis helps identify malicious activity, such as unusual process creation or outbound network connections.
- Wireshark will be used to capture and analyze network traffic associated with the C2 server.



Me after I get caught red handed and trying to get myself out of trouble:



Understanding Detection Use Case

1. What is a Detection Use Case?

- A specific security scenario designed to identify and detect suspicious or malicious activity within an environment.
- Focuses on recognizing key indicators of compromise (IoCs) or unusual patterns related to potential threats.

2. Why Detection Use Cases are Important

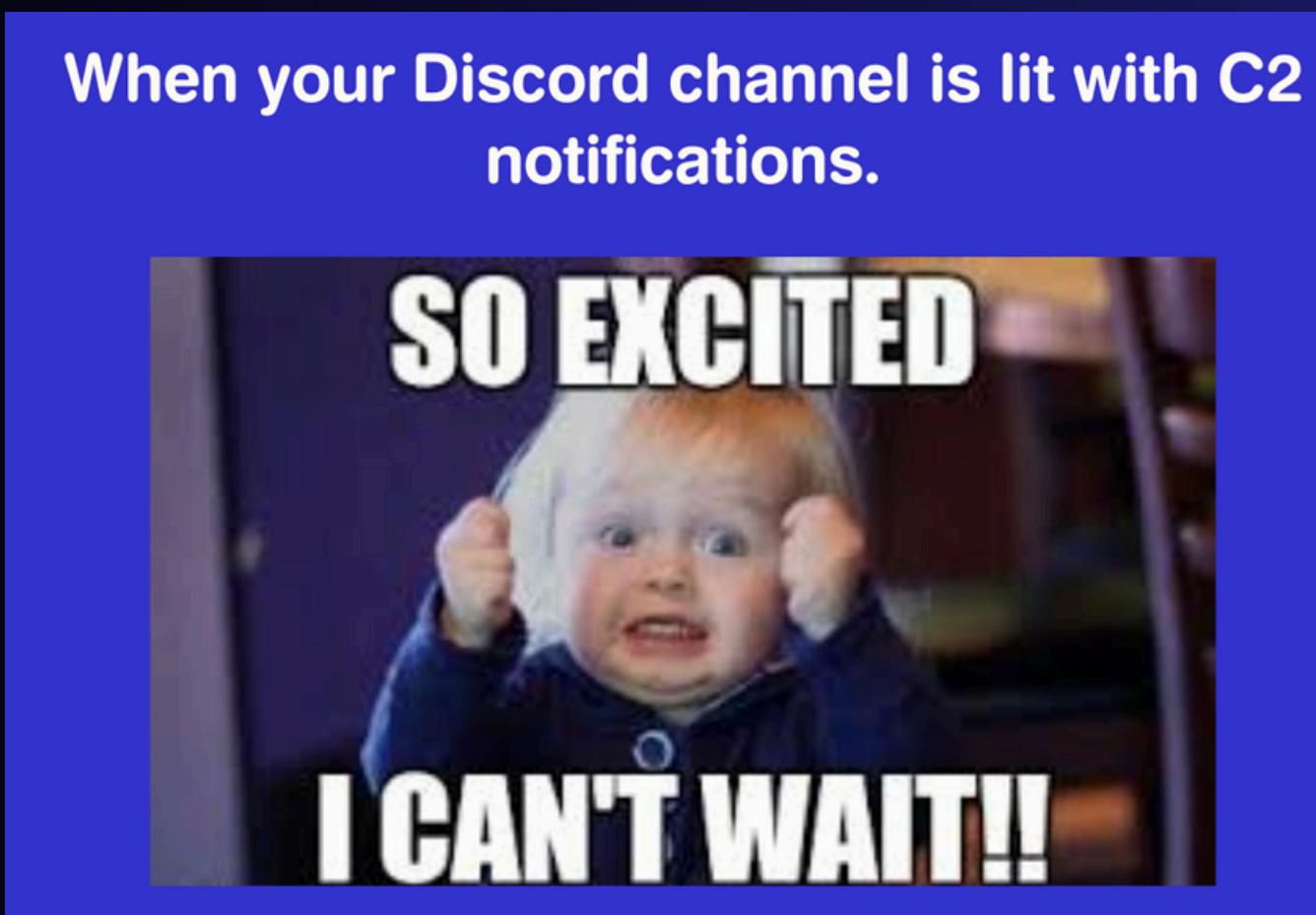
- Enables proactive identification of threats (e.g., malware, C2 activity, privilege escalation).
- Improves response time by alerting security teams to suspicious activity before damage occurs.
- Provides targeted, efficient monitoring by focusing on known threat patterns.

diving deep into log data.



Discord C2 with Custom Script

- This Custom script for Discord C2 allows you to use Discord as a command-and-control server.
- The demo will include payload execution while Microsoft Defender is enabled to test its detection capabilities.
- This provides a unique way to test C2 detection in unconventional channels like Discord.



Elastic Defend XDR

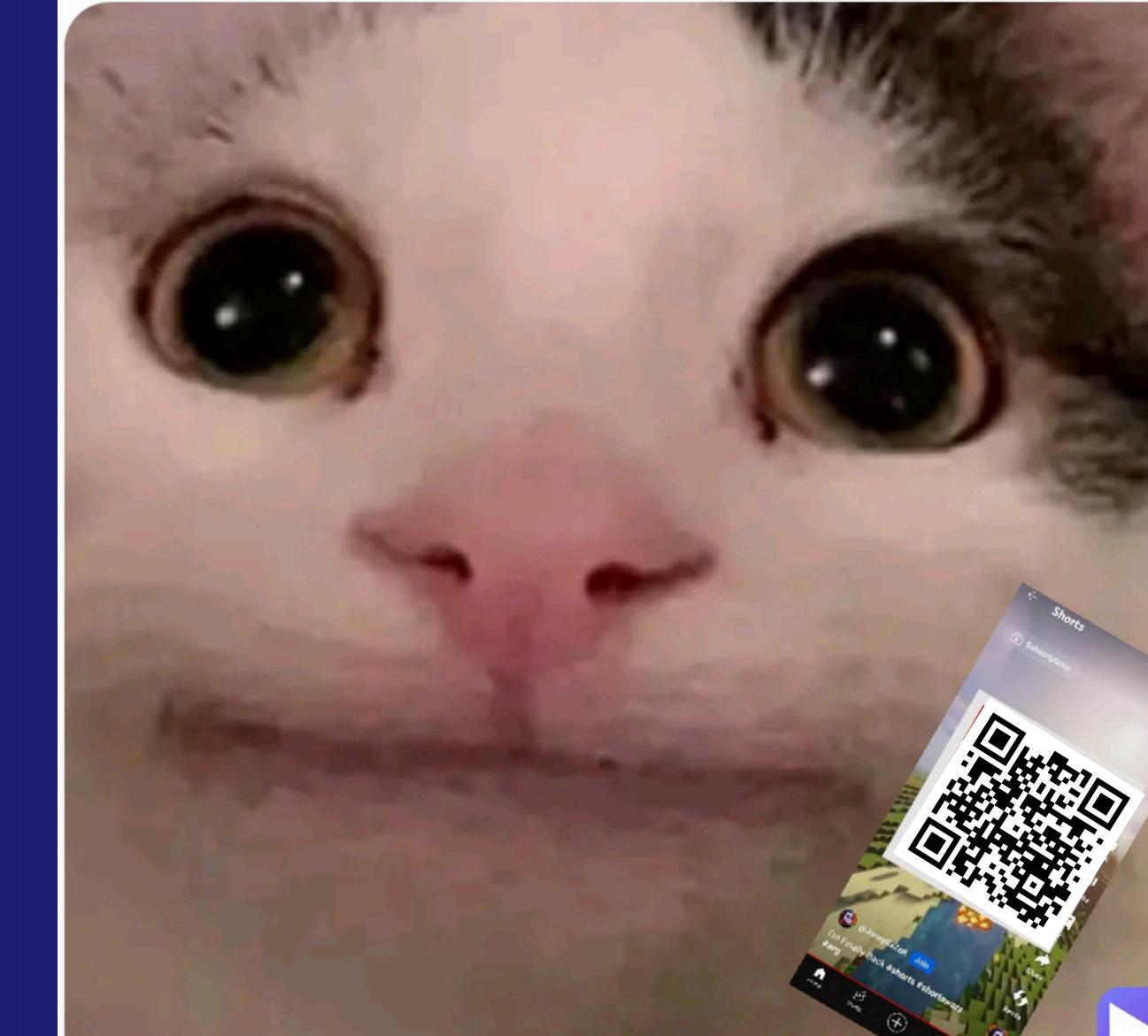
- Introduce XDR (Extended Detection and Response) as a tool that goes beyond traditional SIEM by integrating data from multiple sources.
- XDR provides advanced correlation, visibility, and faster response times.
- In the demo, XDR will be used to detect both Discord C2 and Havoc C2 activities.





SCAN IT

Look at my new QR code





Key Takeaways

1. Bridges the Gap Between Offense and Defense

- Red Team simulates real-world attacks, while Blue Team defends.
- Collaboration ensures both teams learn and improve from each other's insights.

2. Improves Detection and Response

- Red Team challenges defensive strategies, helping identify gaps.
- Blue Team enhances defenses by learning from offensive tactics.

3. Enhances Security Effectiveness

- Constant feedback loop strengthens defenses against evolving threats.
- Ensures that detection tools like Elastic Stack and Sysmon are tuned to catch real-world attacks.

4. Proactive Security Posture

- Instead of waiting for an attack, Purple Teaming continuously tests and refines your defenses.
- Leads to better preparedness against complex attacks with advanced detection (XDR).

Mission accomplished.



Any Questions ?



SAME QR

Guess I'll just ask a question.



Thank You



Scan for Feedback