Mission Name

FindtheCitizen

Historical Background

In a high-stakes operation within the confines of Sylvarcon's Eband Department, Ethan takes on a covert mission to infiltrate the Lazarus citizens' portal. With precision and expertise, Ethan exploits a vulnerability in the site through SQL injection, aiming to erase specific data linked to a level 7 access card. This daring act is part of a broader scheme to navigate through the layers of security undetected.

Technical High-Level Overview

Claire, working against the clock, is tasked with extracting crucial information about a level 7 citizen from the compromised system. Despite her success in retrieving the name and address within the allotted time, the system's security protocols forcefully eject her, leaving behind only a trace of the perpetrator's IP address. The challenge now lies in dissecting the Apache web server logs to pinpoint the exact IP address responsible for the SQL Injection attack, a critical piece of evidence in their quest.

Short Mission Description

Your objective is to delve into the Apache web server logs that have been compromised by Ethan's calculated attack. The mission: identify and extract the IP address that executed the SQL Injection, providing a pivotal lead in understanding the breach's scope.

Mission Description

Ethan's foray into the Lazarus citizens' portal was marked by a strategic breach, aimed at altering the status of a level 7 access card. As the fallout settles, your task is to meticulously analyze the Apache web server logs, compromised during Ethan's incursion. The key to unraveling this digital puzzle lies in identifying the IP address used in the attack, a crucial step in piecing together the events that unfolded.

Location

SYLVARCON | EBAND DEPARTMENT - RECON HQ

Tools

- CAT
- GREP
- AWK

Questions

Which HTTP method was used by Ethan?

- GET

When did Ethan perform the attack? No time, just date in format dd/mm/yyyy.

- 03/09/2049

Looking deeply into Apache Logs, could you provide the name of the Web Application used?

- Wordpress

Items

1. Locates the most important traces for attacking a web application.
2. Distinguish between public and private IP addresses.
3. Searches for the IP address that is sending a SQL Injection with UNION command.

Write Up

To tackle this challenge, players must analyze Apache web server logs to pinpoint the IP address responsible for an SQL Injection attack on the Lazarus site. This first challenge requires familiarity with command-line tools and basic log analysis techniques. Here's how players can systematically identify the attacker's IP address:

Step 1: Extract Public IP Addresses from Logs

Utilize `cat`, `awk`, `sort`, and `uniq` commands to list all unique IP addresses that accessed the site. This step helps in identifying potential suspects by narrowing down the list to unique visitor IPs.

- cat Apache.log | awk '{print $1}' | sort | uniq

Step 2: Highlight the Suspect IP Address

Among the listed IP addresses, players should look for any IP highlighted in red or otherwise indicated as suspicious. This visual cue points to the IP address likely involved in the hack.

Step 3: Investigate Logs for the Identified IP Address

Once the suspicious IP address is identified (e.g., `129.219.36.184`), the next step involves diving deeper into the logs to find entries related to this IP. The `grep` command filters the log entries pertaining to the IP in question.

- cat Apache.log | grep 129.219.36.184

Step 4: Confirm SQL Injection Attack

The final confirmation comes from analyzing the log entries for signs of SQL injection, which might include typical SQL injection payloads like `SELECT`, `UNION`, or other SQL keywords and syntax embedded in the request URL or parameters. The presence of such data linked to the IP `129.219.36.184` confirms it as the perpetrator of the SQL Injection attack.

Flag Information

Flag{129.219.36.184}