Penetration Testing Report: Agent T

Overview

This write-up is a step-by-step guide based on notes from a penetration test conducted on the target IP **10.10.19.115**. It's designed for beginners, providing detailed instructions and explanations at each step.

Tools Required

- Nmap
- Feroxbuster
- Python 3

Step 1: Initial Scan with Nmap

Start by conducting an aggressive Nmap scan to gather information about the services running on the target machine.

Command

nmap -A 10.10.19.115

Results

PORT STATE SERVICE VERSION

80/tcp open http PHP cli server 5.5 or later (PHP 8.1.0-dev) |_http-title: Admin Dashboard

Analysis

The scan reveals a single open port (80) running a PHP CLI server version 8.1.0-dev, with an accessible admin dashboard.

Step 2: Expanded Nmap Scan

Since the initial scan was limited, we expand our scope to search a larger range of ports.

Command

nmap -p 1-9999 10.10.19.115

Result

No additional interesting ports or services were discovered.

Step 3: Directory Enumeration

Next, we use Feroxbuster to enumerate directories on the web server.

Command

feroxbuster --url http://10.10.19.115 --wordlist /usr/share/wordlists/dirb/common.txt

Result

The directory enumeration did not reveal any notable directories or files.

Step 4: Searching for Exploits

Upon discovering the PHP version (8.1.0-dev), we search for relevant exploits.

Resource

Exploit DB, specifically EDB-ID: 49933

Action

Download the exploit script (49933.py) from Exploit DB.

Step 5: Exploitation with Python Script

Run the downloaded Python exploit script to gain access to the server.

Command

sudo python3 49933.py

Interaction

When prompted, enter the target URL: **http://10.10.19.115**. This should grant root access to the server.

Step 6: Locating the Flag

With root access, the next task is to locate the flag file on the system.

Command

find / -name flag.txt 2>/dev/null

Result

The command should reveal the location of **flag.txt**, which contains the flag you're searching for.

Conclusion

Following these steps, you should be able to conduct a basic penetration test against a target running a vulnerable PHP server.