Homework 7 - Challenge VM #1 Walkthrough Report

Author: Moses Kunfah

Target: Ubuntu 12.04 vulnerable machine (10.0.0.8)

Objective: Gain root access and capture the flag from /root/root.txt

Overview

# Information Gathering

# Port Scanning (22, 80)

# Enumeration (HTTP → Shellshock)

# Exploitation (Shellshock Reverse Shell)

# Post-Exploitation (Privilege Escalation using Dirty COW)

# Root Shell Access and Flag Retrieval

# References

# Step 1: Reconnaissance

To begin identifying the target, I used netdiscover to find live hosts in the local network. Once the target IP was confirmed as 10.0.0.8, I used Nmap to scan for open ports and services.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

This revealed that ports 22 (SSH) and 80 (HTTP) were open. The HTTP server was running Apache 2.2.22.

# Step 2: Enumeration

Next, I performed directory brute-forcing on port 80 using Gobuster:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

I found a /cgi-bin/ directory. I then ran Nikto to check for web server vulnerabilities:

A screenshot of a computer

AI-generated content may be incorrect.

Nikto reported that the Apache server was vulnerable to Shellshock in the /cgi-bin/test script.

A screenshot of a computer screen

AI-generated content may be incorrect.

# Step 3: Exploitation - Shellshock

To exploit Shellshock, I navigated the internet and downloaded dirtycow and crafted a reverse shell payload using curl and executed it against the vulnerable CGI script:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer screen

AI-generated content may be incorrect.

I had python web server host listener on port 8000:

A computer screen with white text

AI-generated content may be incorrect.

I had a Netcat listener on port 4444:

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

The payload successfully triggered vulnerability and gave me a reverse shell as the www-data user.

# Step 5: Dirty COW Exploit (CVE-2016-5195)

I encountered an issue.

A screenshot of a computer

AI-generated content may be incorrect.

Now, it has bypassed successfully

A screenshot of a computer

AI-generated content may be incorrect.

# Step 6: Root Access & Flag Retrieval

Upgraded shell with Python PTY. Switched to firefart. Retrieved flag.

A screenshot of a computer screen

AI-generated content may be incorrect.

# Conclusion

Successfully exploited Shellshock to gain a reverse shell. Escalated to root using Dirty COW, and retrieved the root flag: {Sum0-SunCSR-2020\_r00t}

References:

* Shellshock Vulnerability: <https://nvd.nist.gov/vuln/detail/CVE-2014-6271>
* Dirty COW <https://www.exploit-db.com/exploits/40839>
* Nmap Documentation: <https://nmap.org/book/man.html>
* Nikto Web Scanner: <https://github.com/sullo/nikto>
* Gobuster Tool: <https://github.com/OJ/gobuster>