**TOC**

Penetration Test Report

Machine: THM | Blueprint

Nov 5, 2024

# 

Table of Contents

Title. [1](#_21pr7inr5jnb)

TOC. 2

Executive Summary. 3

SOW. 4

Scope. 5

Active Reconnaissance. 6

Initial Access. 11

Actions on Objectives. 13

Executive Summary

Summary:

Out-of-date software led to a vulnerability for multiple open-source exploits that exist online which are low-complexity and have severe impact.

Remediation / Recommendations:

Ensure all software components of production servers remain up-to-date and patched as soon as possible.

Statement of Work

# Introduction:

This penetration test targets the Windows machine “Blueprint” on TryHackMe by user: “MrSeth6797.” Assessment conducted 11/5/2024.

# Scope of Work:

No SOW provided. Objectives are to find and decrypt the “Lab” user NTLM Hash and find the root.txt flag.

# 

Scope

# IP Address Scope:

10.10.104.44

# Rules of Engagement:

All TTPs allowed.

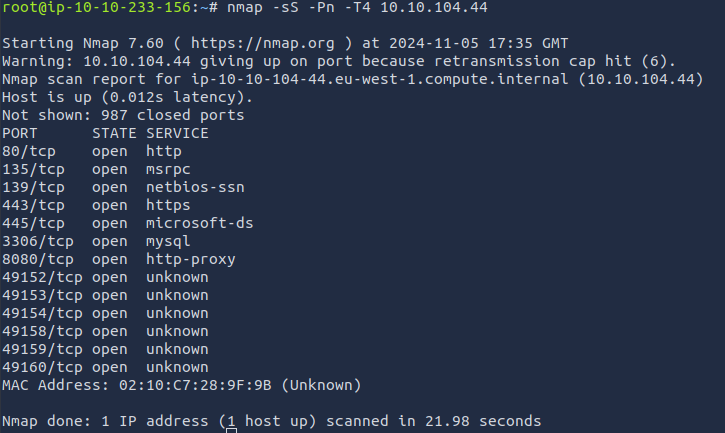
Active Reconnaissance

# Scanning and Analysis:

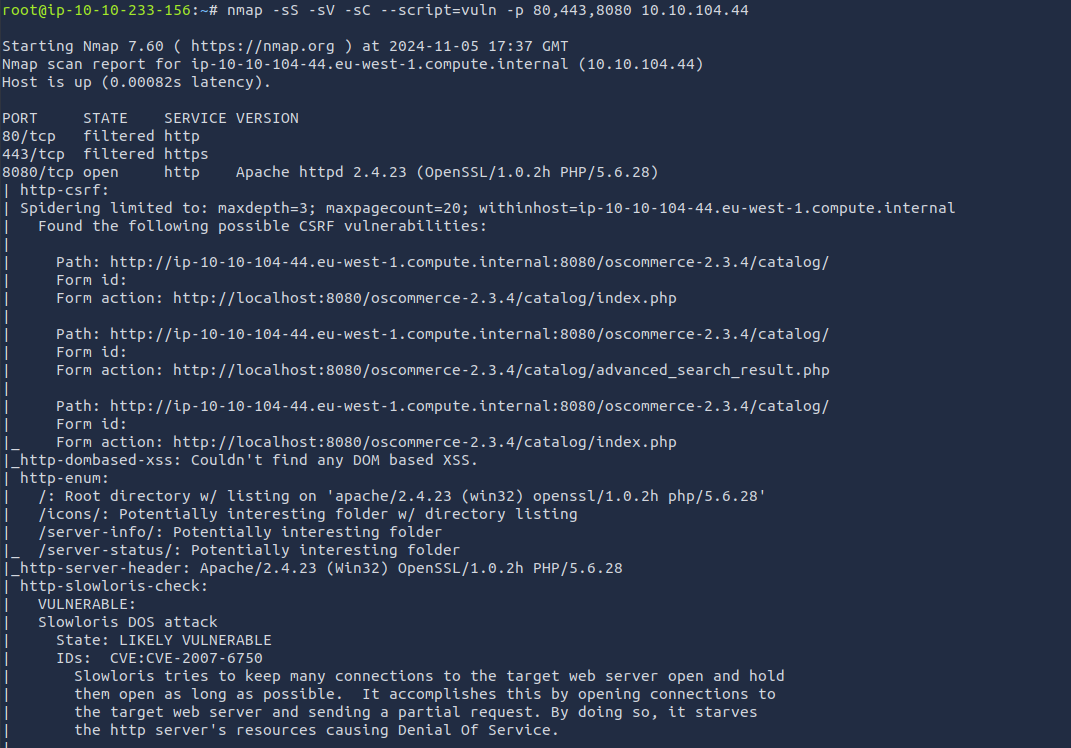
Started engagement at 12:23 EST.

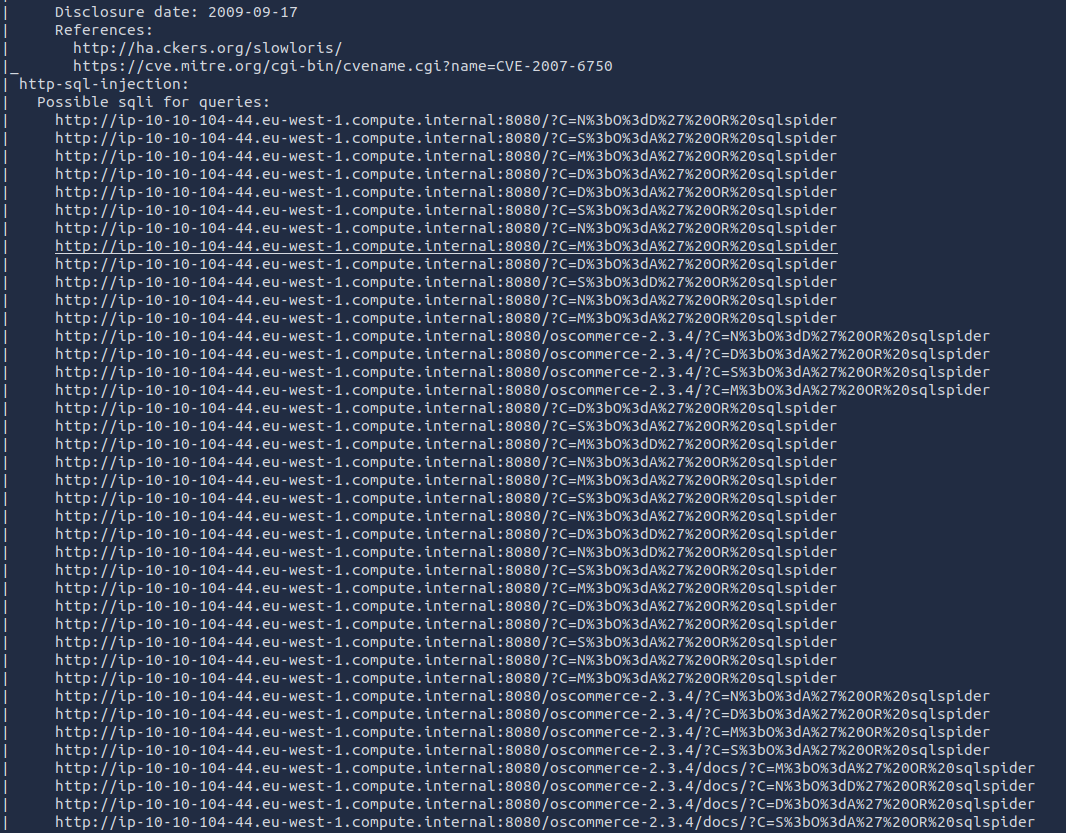
Conducted ping scan at target host to test reachability.

(12:25 EST) - Initiated Nmap scan at target machine to detect most common open ports.



(12:37 EST) - Initiated an Nmap scan with vulnerability scripts and service discovery targeting the ports hosting web services. Also performed manual analysis via web browser.

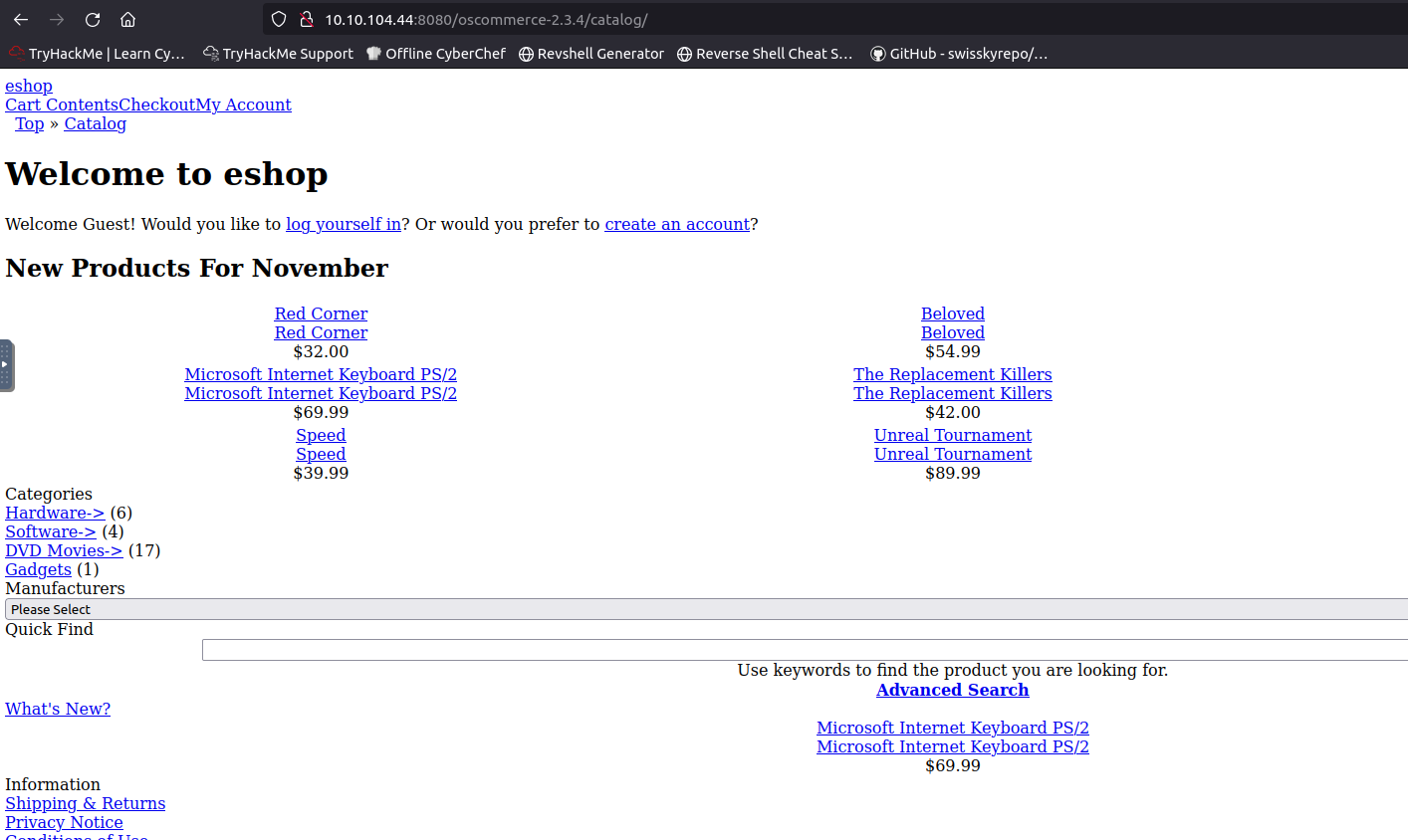




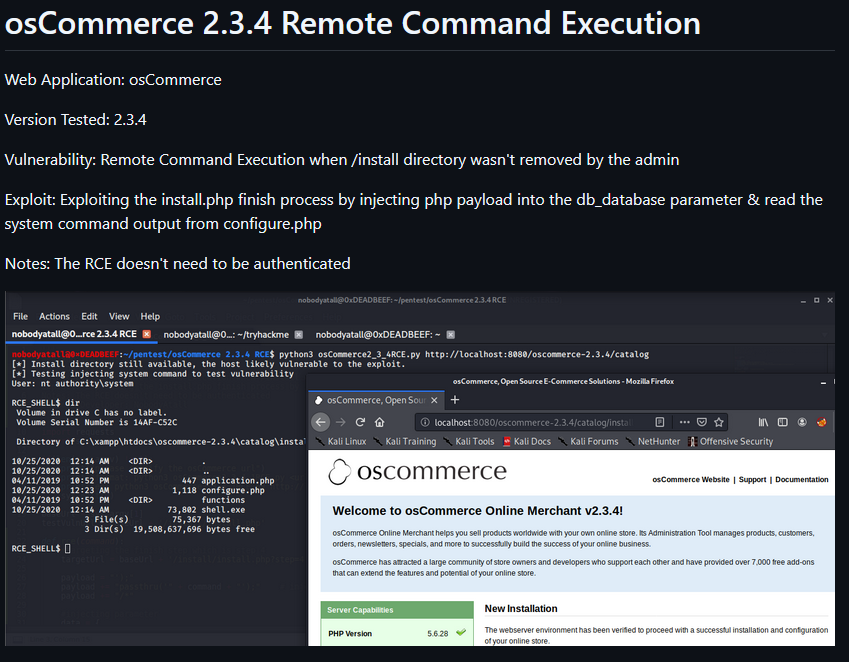
Paused engagement at 13:28 EST.

Resumed engagement at 14:00 EST.

Searched through the web server at http:10.10.104.44:8080/ and found that it was running osCommerce version 2.4.3



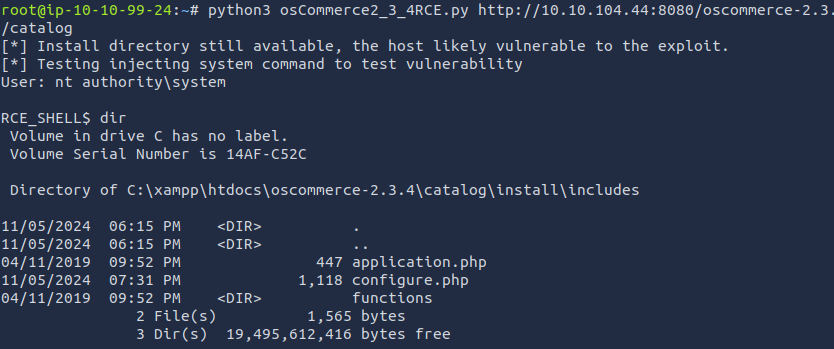
Found a RCE vulnerability with this version of osCommerce on GitHub:



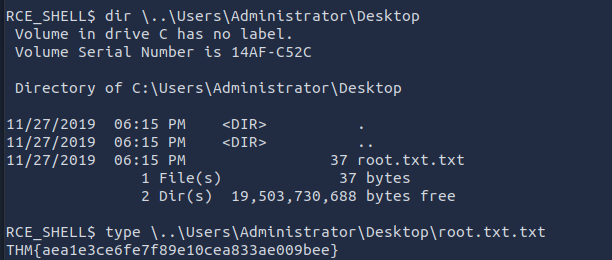
Source: <https://github.com/nobodyatall648/osCommerce-2.3.4-Remote-Command-Execution>

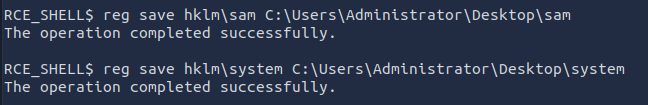
Initial Access

I used the RCE script from GitHub to gain a shell as SYSTEM user on the machine:



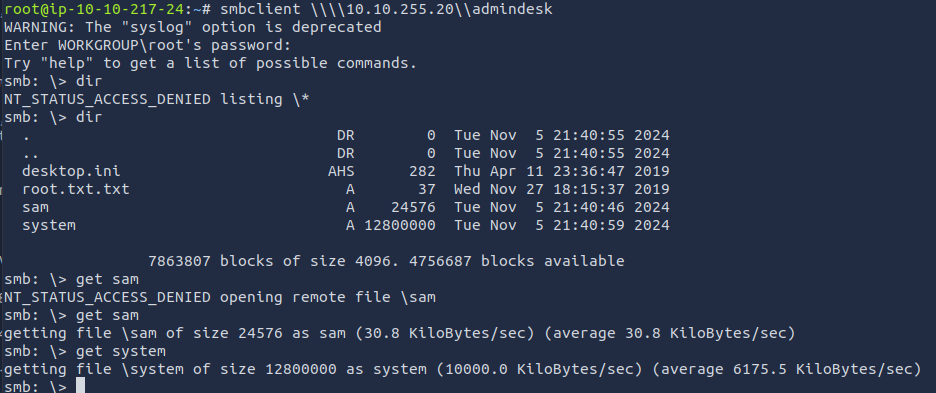
Using RCE vulnerability, I can navigated to the Administrator’s desktop to get the root.txt flag:

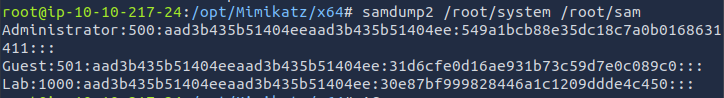


In order to satisfy the other objective (Obtain “Lab” user’s NTLM hash) I first saved the contents of the SAM database:  


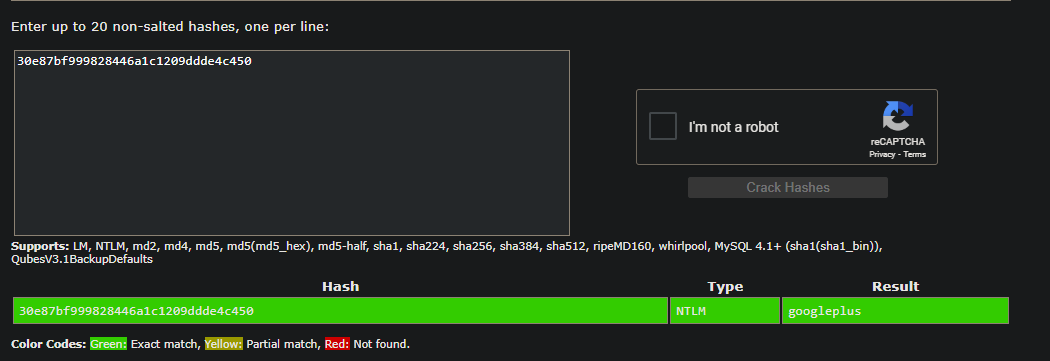
I then created an SMB share on the Administrator’s desktop:



I then connected to this share from my attacking machine and attempted to download the files, and changed the file permissions of the directory that the share is connected to.  


I used samdump2 on the attacking machine to dump the NTLM hashes:  


I input the lab user’s password hash into crackstation:



Lab user’s password: googleplus

Actions on Objectives

13:30 EST - Obtained root.txt via RCE by exploiting a vulnerability in osCommerce version 2.3.4

17:18 EST - Obtained “Lab” user’s NTLM hash by saving the SAM database and dumping it on the attacking machine.