OFFENSIVE SECURITY

Penetration Test Report for   
My-CMSMS Lab

v.1.0

student@youremailaddress.com

OSID: XXXXXX



Copyright © 2022 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

Table of Contents

[Offensive Security Lab Penetration Test Report 2](#_Toc92471625)

[1. Objective 2](#_Toc92471626)

[2. Lab Network 3](#_Toc92471627)

[192.168.191.74 – Alpha 3](#_Toc92471628)

[Initial Access – Phtml file upload for shell access 3](#_Toc92471629)

[Privilege Escalation – Lateral escalation to local user for sudo root 4](#_Toc92471630)

[Post-Exploitation 4](#_Toc92471631)

# 

# Offensive Security Lab Penetration Test Report

## 1. Objective

OS-XXXXXX was tasked with performing an internal penetration test towards Offensive Security Labs. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security’s internal lab systems – the THINC.local domain. The overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security’s network. When performing the attacks, OS-XXXXXX was able to gain access to the device through multiple methods, primarily due to outdated patches and poor security configurations.  During the testing, OS-XXXXXX had administrative level access using two different exploit paths. All systems were successfully exploited and access granted.

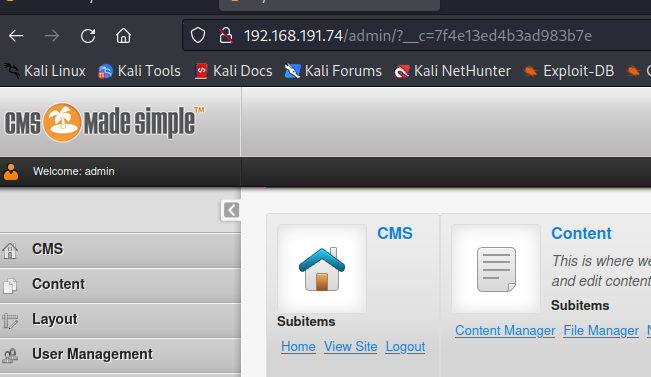
# 2. Lab Network

The over-all set-up for this network contained one device on the 192.168.191.0/24 network that was available for testing. This consisted of a web server and ssh service that was able to be reached externally for the network.

## 192.168.191.74 – Alpha

### Initial Access – Phtml file upload for shell access

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.38 (Ubuntu) with CMS made Simple version 2.2.13. Brute force with hydra was used against the http-port-form after mysql shut off following brute force attempt. This succeeded in finding the admin password, which allowed log-in and administrative control of the website.



Following the exploit listed on the exploit-db, a phtml shell code file was uploaded using file manager, which allowed for successful access on activating it through the browser.

Graphical user interface, application, Teams

Description automatically generated

### Privilege Escalation – Lateral Escalation to local user for sudo root

Following enumeration checks, it was determined there was a file that showed a base 64 encoded string of characters. Decoding them provided the credentials for the local user on the system. Escalating laterally to this user then allowed for abuse of the sudo function with python to generate a root shell. This allowed for access to the proof.txt file.

### Text Description automatically generated

### Post-Exploitation

Graphical user interface, text

Description automatically generated