OFFENSIVE SECURITY

Penetration Test Report for   
Sunset Midnight 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)

[192.168.128.88 – Alpha 3](#_Toc92471628)

[Initial Access – Akismet Plugin editing for web shell 3](#_Toc92471629)

[Privilege Escalation – Path hijacking a suid set binary 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 machine through editing the plugin on the wordpress website, primarily due to weak passwords used for the mysql service.  During the testing, OS-XXXXXX had administrative level access to the device. All systems were successfully exploited and access granted.

# 2. Lab Network

The over-all set-up for this network contained one device on the 192.168.128.0/24 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.

## 192.168.128.88– Alpha

### Initial Access – Akismet Plugin editing for web shell

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.38 (Ubuntu) and Wordpress 5.4.2. Initial checks proved the admin account, but no disclosed exploit was found to gain access. Mysql was then brute forced for the admin account, which gained admin access to the web page. The Ajax plugin was edited to add a shell command, then activated.

Graphical user interface, text, application, email

Description automatically generated

With the plugin activated on the edited code, a shell for the web user was gained into the network. From there, the contents of the local.txt were available for retrieval.

Text

Description automatically generated

### Privilege Escalation – Path hijacking a suid set binary

Checking through the system found the baron samedit vulnerability spawned a root shell. Further checks for other privilege escalation paths found the password for the local user within the wordpress config file. With the lateral privilege escalation, a binary was found that the user had suid setting for a root file. Checking the contents showed that it made several calls to local processes.

A copy named file was added into the /tmp folder, and then the PATH updated to prioritize this directory. When calling the suid binary, it generated a root shell using the custom script added into /tmp.

1

### Post-Exploitation

A picture containing text

Description automatically generated