OFFENSIVE SECURITY

Penetration Test Report for   
SoSimple 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)

[10.11.1.71 – Alpha 3](#_Toc92471628)

[Initial Access – Redirected URL link to exploit 3](#_Toc92471629)

[Privilege Escalation – Sudo command abused for root shell 4](#_Toc92471630)

[Post-Exploitation 5](#_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 When performing the attacks, OS-XXXXXX was able to gain access through an outdated module on the wordpress site, primarily due to outdated patches.  During the testing, OS-XXXXXX had administrative level access through multiple exploits. 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.

## 192.168.128.78 – Alpha

### Initial Access – Redirected URL link to exploit

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.41 (Ubuntu) and wordpress 5.4.2. After running wpscan, it was found that there was a RCE vulnerability in the version of social warfare 4.3.0.

Text

Description automatically generated

The python script was utilized to create a shell session locally on the attack machine.

Text

Description automatically generated

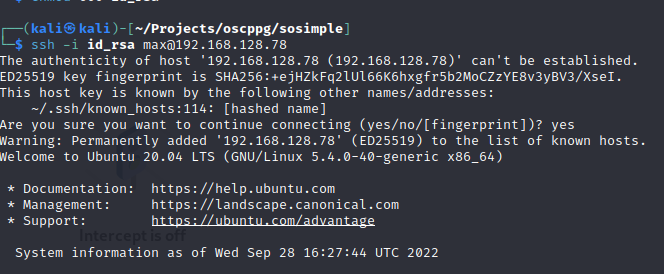
From there, the contents of the local.txt file were available for retrieval.

Text

Description automatically generated

### Privilege Escalation – Sudo command abused for root shell

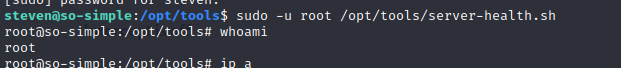
Checking for exploits showed baron samedit successfully spawned a root shell. Further checks found a SSH private key for the max user. Access was gained using this key.



### Sudo permissions were found that allowed a shell session to be created on another user on the local system. Moving laterally to this user, found that there was a sudo permission binary that could be used to spawn a root shell.

**Text

Description automatically generated**



### Post-Exploitation

A picture containing graphical user interface

Description automatically generated