OFFENSIVE SECURITY

Penetration Test Report for   
Noname 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)

[192.168.162.15 – Alpha 3](#_Toc92471628)

[Initial Access – Command Injection on website 3](#_Toc92471629)

[Privilege Escalation – Suid bit set on find binary 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 to the machine through an exploit on the website superadmin.php file.  During the testing, OS-XXXXXX had administrative level access to network after successfully exploiting the find binary with suid setting. All systems were successfully exploited and access granted.

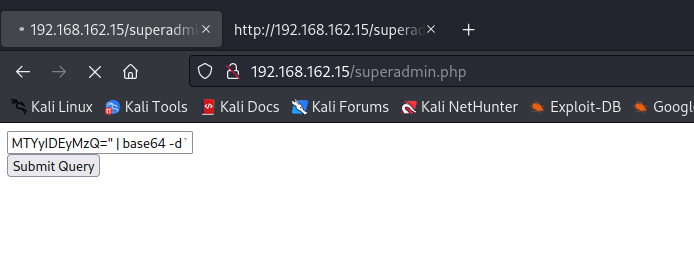
# 2. Lab Network

The over-all set-up for this network contained one device on the 192.168.162.0/24 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.

## 192.168.162.15 – Alpha

### Initial Access – Command Injection through website

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.29 (Ubuntu). Checking through the base directories contained a notification to try harder. With no viable exploits, a new dirsearch was performed with a larger wordlist that found the superadmin.php application. A base64 encoded netcat shell command was injected into the file.



This generated a shell with gave local level access to the device, and made it possible to get the contents of the local.txt file.

Text

Description automatically generated

Text

Description automatically generated

### Privilege Escalation – Suid setting on find binary

Once the local flag had been received, the search then turned to possible privilege escalations. Checking the suid set binaries on the system turned up that find function was set for it.

Text

Description automatically generated

This was exploited to successfully generate a root shell.

### Text Description automatically generated

### Post-Exploitation

Text

Description automatically generated