OFFENSIVE SECURITY

Penetration Test Report for   
Stapler 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 – Brute force on local user 3](#_Toc92471629)

[Privilege Escalation – Write access for logrotate cron job 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 due to anonymous access to MySQL and weak password on one of the users.  During the testing, OS-XXXXXX had administrative level access to the device utilizing 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 multiple services, with the main ones exploited being a SAMBA service and ssh service that was able to be reached externally for the network.

## 192.168.128.148– Alpha

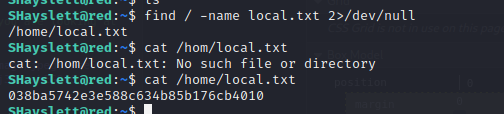
### Initial Access – Brute force on Local User

Initial checks were made on the website that returned the version of 5.5 or later for the PHP server running on port 80. During the enumeration of its directories, the SAMBA service was checked and found to allow access for enum4linux, which returned multiple usernames. One of these usernames was able to be brute forced, and allow access into the network.

Text

Description automatically generated

This then allowed access to the contents of the local.txt file on the system.



### Privilege Escalation – Write access for logrotate cron job

Numerous vulnerabilities were found due to outdated patches that allowed pwnkit to generate a root shell. Further checks were made that found a writeable cron job for log rotation that runs every 5 minutes with root privilege. A shell code was added into the file, and on being called created a root shell to the system.

Text

Description automatically generated

### Post-Exploitation

Graphical user interface

Description automatically generated with medium confidence