OFFENSIVE SECURITY

Penetration Test Report for   
Tre 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)

[192.168.128.84 – Alpha 3](#_Toc92471628)

[Initial Access – Credentials on web directory allow SQL query 3](#_Toc92471629)

[Privilege Escalation – Write permission on startup file 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, local files stored on the public facing website allowed for login credentials to be exploited for a SQL query. The query disclosed system credentials that allowed remote access to the local user on the network. A sudo privilege for the user allowed for remotely restarting the system on command. A user writeable file was found for the root user that runs during startup. Changing the script allowed for administrative level access to the system by changing the suid setting on bash. 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 with two ports and ssh service that was able to be reached externally for the network.

## 192.168.128.84 – Alpha

### Initial Access – Credentials on web directory allow SQL query

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.38 (Debian) and Mantisbt. There was a configuration file stored on the mantisbt/config directory that contained the login credentials for the admin user.

Text

Description automatically generated

Using the credentials, it was possible to log into the mysql adminer.php site to do a sql query for user credentials contained in the database. A local user was found that allowed for remote access into the network.

Text

Description automatically generated

This allowed for retrieval of the local.txt contents.

Text

Description automatically generated

### Privilege Escalation – Write permission on startup file

Checking the sudo permissions showed they had control over restarting the machine. With this, writeable configurations or processed were checked. This led to finding the check-system function that was edited to add a suid setting to the bash binary.

Graphical user interface, text

Description automatically generated

On restarting the system, the bash binary was able to be used to get a root shell.



### Post-Exploitation

Graphical user interface, text

Description automatically generated