OFFENSIVE SECURITY

Penetration Test Report for   
ICMP Internal Lab

v.2.0

Lab write-up

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 1](#_Toc92471625)

[1. Objective 2](#_Toc92471626)

[2. Lab Network 3](#_Toc92471627)

[192.168.191.218 – Alpha 3](#_Toc92471628)

[Initial Access – RCE exploit of Monitorr version 3](#_Toc92471629)

[Privilege Escalation – Outdated SUDO version baron exploit 4](#_Toc92471630)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 When performing the attacks, OS-XXXXXX was able to gain access to the network device, primarily due to outdated patches and poor security configurations.  During the testing, OS-XXXXXX had administrative level access achieved on the system.

# 2. Lab Network

The over-all set-up for this network contained one device on the 192.168.191.0/24 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.

## 192.168.191.218 – Alpha

### Initial Access – Remote Code execution on Monitorr service

Enumeration was performed on the web service which showed there was a directory for the base page redirect. The main webpage listed the version of the Monitorr service, which had two different exploits listed for it. The remote code execution exploit parameters were found by investigating the /mon directory to find the needed application path for the exploit to work.

Text

Description automatically generated

This successfully created a shell access to local level privileges, which compromised the contents of the local.txt file for retrieval.

Text

Description automatically generated

### Privilege Escalation – Outdated sudo command

An exploit was uploaded to the /tmp folder to exploit the version of SUDO on the system that was able to spawn a root shell. This represented a complete compromise of the network device, with all files and folders available for retrieval or modification.

### Text Description automatically generated

### Post-Exploitation

