OFFENSIVE SECURITY

Penetration Test Report for   
DC-4 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)

[192.168.162.195 – Alpha 3](#_Toc92471628)

[Initial Access – Web application misconfiguration allowing write access 3](#_Toc92471629)

[Privilege Escalation – Sudo privilege exploited to edit /etc/passwd 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 and edit files through the website, due to using client-side validation instead of server-side.  During the testing, OS-XXXXXX had administrative level access to the system, along with multiple compromised local accounts. All systems were successfully exploited and access granted.

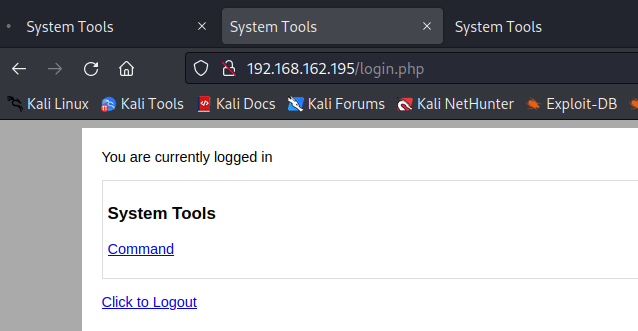
# 2. Lab Network

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.

## 10.11.1.71 – Alpha

### Initial Access – Web application misconfiguration allowing write access

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under nginx 1.15.10. Directories were scanned with no interesting results, so the login page was targeted for access. The login credential packet was intercepted through burpsuite and run through hydra to determine the password for access. Hydra looked to error out with multiple password found; but dropping the proxy showed admin authentication was successfully carried out.



The command tool was checked for values in the inspection window, and the values were found to be loaded client side. Various checks were run to find users in the passwd file, followed by checks of their home directories. From there, it was determined the best entry point would be editing the test.sh file within jim’s directory to generate a shell.

Graphical user interface, text

Description automatically generated

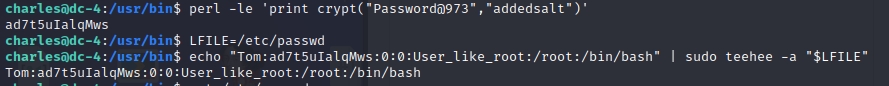
This succeeded in getting access to the local.txt flag located in the /home/jim directory.

Text

Description automatically generated

### Privilege Escalation – Sudo privilege exploited to edit /etc/passwd

The backup password file in jim’s directory was used to find the credentials to log in as jim. Checking around did not point to any vulnerabilities easily exploitable, but an email from Charles contained the password for that user. On logging in with that user, it was found they had sudo privilege for the teehee binary. Checking its function showed it to be the same as tee, and so the exploit for that program was successfully implemented to generate a root shell.



### Post-Exploitation

Graphical user interface, text

Description automatically generated