OFFENSIVE SECURITY

Penetration Test Report for   
Assertion101 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 – Command injection through website php file 3](#_Toc92471629)

[Privilege Escalation – Suid binary allows over-writing passwd file 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 system through command injections in the web browser php file due to no sanitization of the input parameters.  During the testing, OS-XXXXXX had administrative level access to the system through multiple exploit vectors, due to outdated patches and improper suid values on a binary. All systems were successfully exploited and access granted.

# 2. Lab Network

The over-all set-up for this network contained one device on the 192.168.129.0/24 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.

## 192.168.128.94 – Alpha

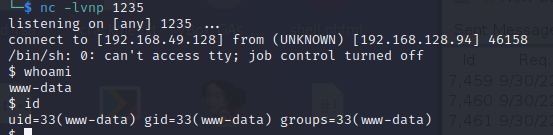
### Initial Access – Command injection through website php file

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.29 (Ubuntu) and Colorlib framework. Various exploits were attempted on the site, with path traversal and xss not showing any success. Command injection based on path traversal responses led to a shell command being sent.

Text

Description automatically generated

This successfully created a shell into the system.



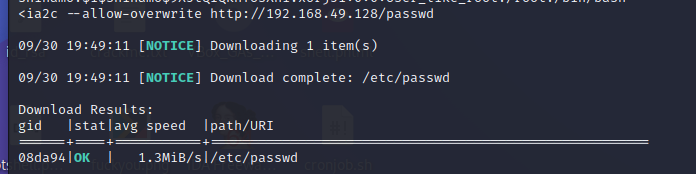
The contents of the local.txt file was retrieved for proof of local level access on the system.

Text

Description automatically generated

### Privilege Escalation – Suid binary allows over-writing passwd file

Multiple exploits allowed root access with pwnkit and baron samedit successfully granting root access. Further checks showed there was a SUID set binary that was outside the norm. Checks showed it was possible to exploit it, but the common method failed. Using it to upload a modified /etc/passwd file with a new user added succeeded in bypassing the permissions on the passwd file.



Various hash methods were tried, with perl hash being the normal standard for previous penetration testing success.

Text

Description automatically generated

Using this new user, it was possible to switch over to a user with root level permissions on the system.

Graphical user interface, text, application

Description automatically generated

### Post-Exploitation

Graphical user interface

Description automatically generated