OFFENSIVE SECURITY

Penetration Test Report for   
Election1

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 – Shellshock on Apache’s CGI 3](#_Toc92471629)

[Privilege Escalation – Unsecured Credentials 3](#_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 When performing the attacks, OS-XXXXXX was able to gain access to the target machine, primarily due to outdated patches and poor security configurations.  During the testing, OS-XXXXXX was able to escalate privileges to root through three different methods. The system was successfully exploited and access granted.

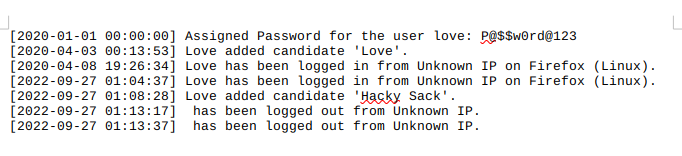
# 2. Lab Network

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.

## 192.168.191.211 – Alpha

### Initial Access – SSH credentials stored on website logs directory

After inspecting the HTTP headers of the landing page on port 80 we discovered that it is running under Apache/2.4.29 (Ubuntu). Scans were made on the base webpage, with a list of possible directories under the robot.txt file. The directory came up during gobuster scans. A new search was launched targeting this directory, which found login credentials for the website. A log directory was found during the search, that contained credentials for the love user.



Using these credentials supplied in the log file, remote access was achieved through the SSH service to gain access to the local.txt file.

Text

Description automatically generated with medium confidence

### Privilege Escalation – Outdated sudo and pkexec, suid-set Serv-u

### Checks were made on the various services and binaries, which showed that the sudo and pkexec binaries were older version that were susceptible to exploits. These exploits were uploaded and successfully achieved root access on the device.

Further checks were made which showed the Serv-u binary was set for suid privilege on it. An exploit code was manually entered into the ssh session which spawned a root shell.

Text

Description automatically generated

### Post-Exploitation

Graphical user interface, text

Description automatically generated