Project RaVen Boot2Root

By Hoeun A. Kim

08/24/2019

Executive Summary

In this exercise, users are tasked with gaining access to and reading files from a vulnerable virtual machine - Raven 1. The machine was vulnerable to attack via it's Open SSH, Wordpress, MySQL Database, and weak user passwords and administrative permissions. Attackers are given the ability to read and modify local files. These local files included system configuration files for the WordPress PHP, System Permission and groupsets, and SQL Database tables and information.

All accounted for, this machine poses as an immediate weak point that can cause detrimental damage to the business, in the loss of Confidentiality, Integrity and Availability of system information and accessibility. At any time, an attacker could gain ADMINISTRATIVE ACCESS, and bring down important network devices and services, lock users out, and can obtain important and confidential information with ease.

It is important to IMMEDIATELY update and close the vulnerabilities. This includes and is not limited to:

- Strengthening User Password Policies
- Remove ability for users to gain Admin access to other users
- Updating off OpenSSH 6.7p1

- Scrub metadata from Wordpress site
- Remove low level access to configuration files
- Modify SQL Databases to remove plaintext and Hashed data

Attack Narrative

This assessment involved the attempted compromise of multiple machines on the target subnet. Each phase of the test is documented below.

Reconnaissance

General Reconnaissance

- Local Attack Machine - 192.168.56.104
- Victim Machine - 192.168.56.106
- NMAP of 192.168.56.106 discovered opened ports on 22, 80, and 111

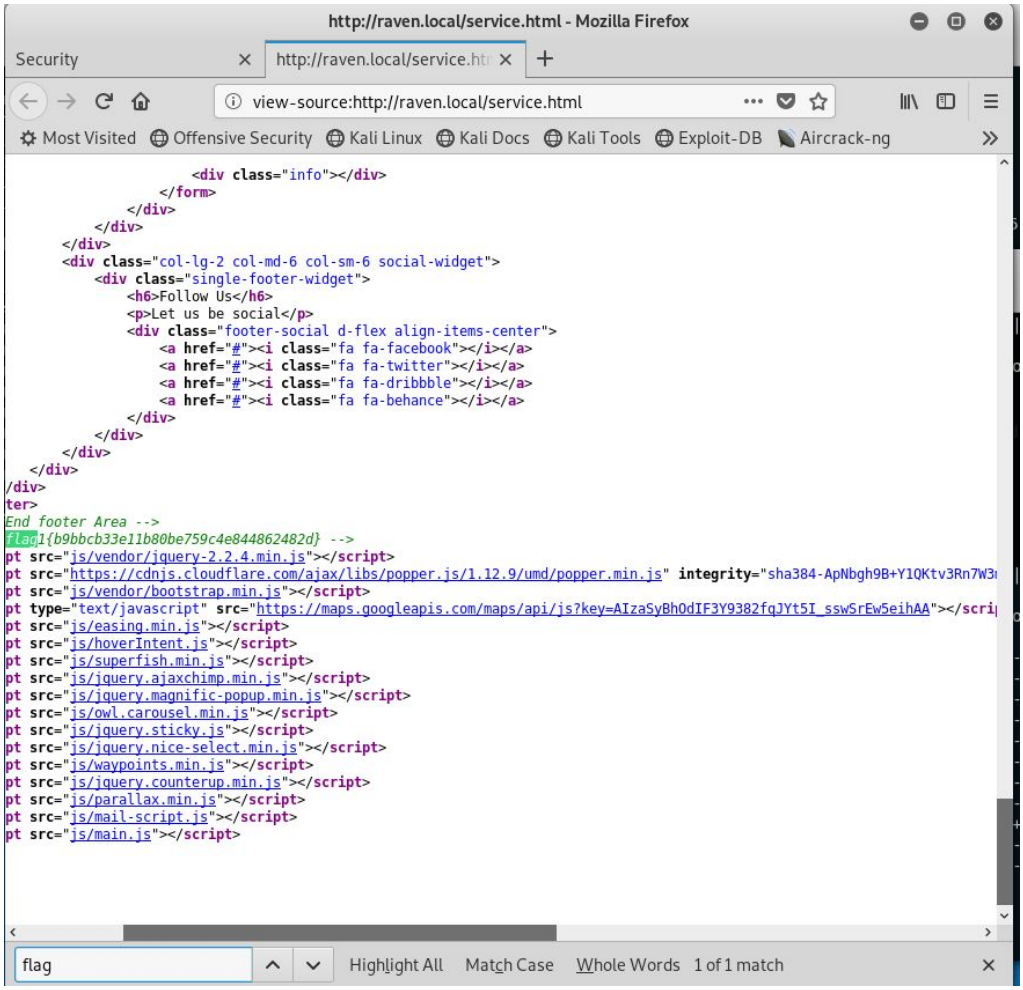
Enumeration and Vulnerability Analysis

This section summarizes the most critical vulnerabilities affecting the target network.

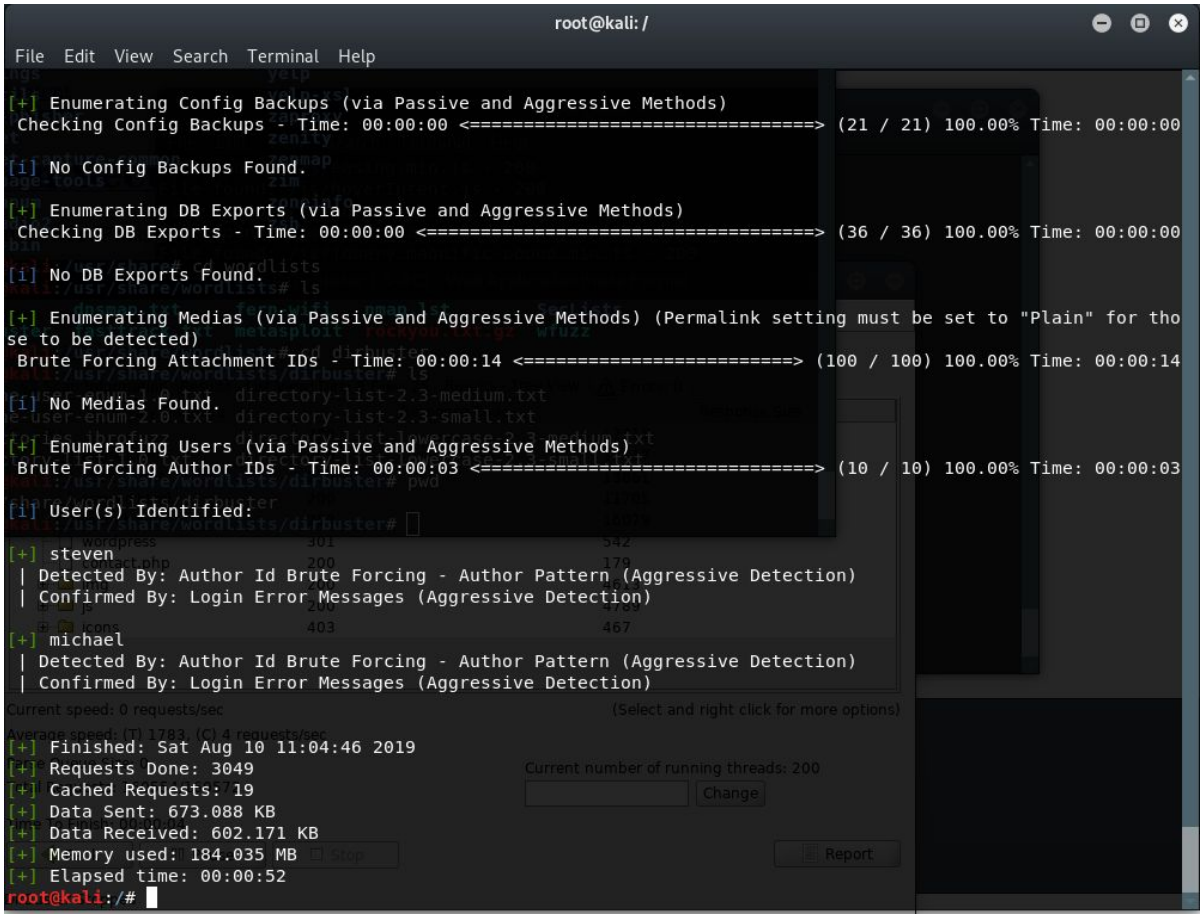
IP Address	Operating System	Vulnerabilities	Risk (Low/Med/High)
192.168.56.106	Linux	Open SSH 6.7p1	High
		MySQL	Medium
		WordPress Web Server version 4.8.7	High
		Weak passwords	High

Web Server Analysis

Upon discovering the IP address for the victim machine, it is possible to view and obtain additional information for the WordPress site. Flag #1 could be found under the Services.html

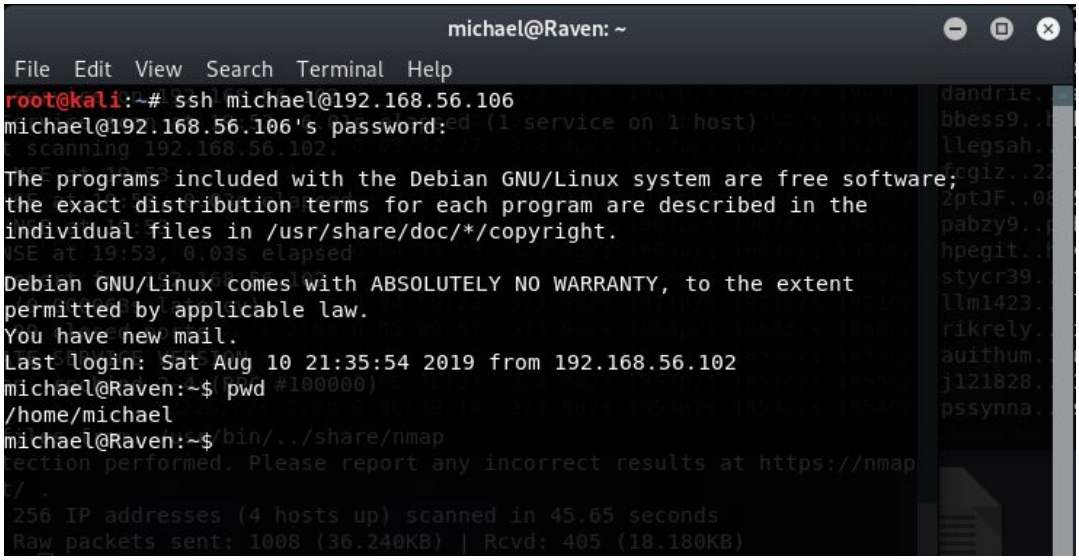


Using this information, I was able to run the tool Dirbuster to enumerate the directory information for the WordPress WebServer. I was able to run WPScan to enumerate vulnerabilities and users found on the WordPress Site. From this we discovered Michael and Steven as the users:

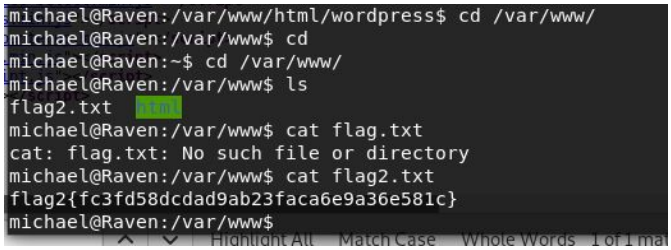


Network Analysis

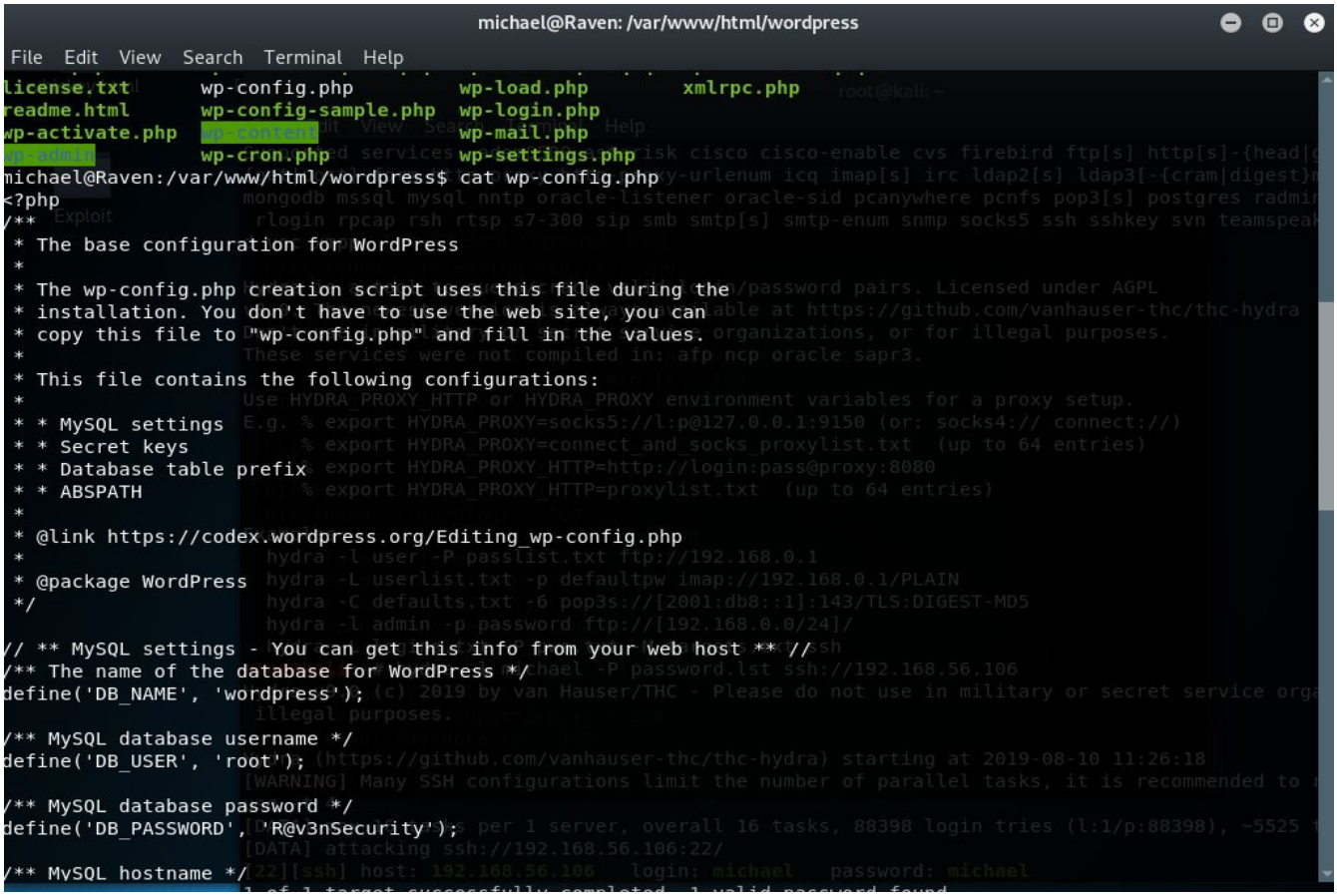
Using the knowledge for the open SSH port and the two users, built a wordlist to brute force the login for Michael (michael:michael). Logged into Raven1 via SSH:



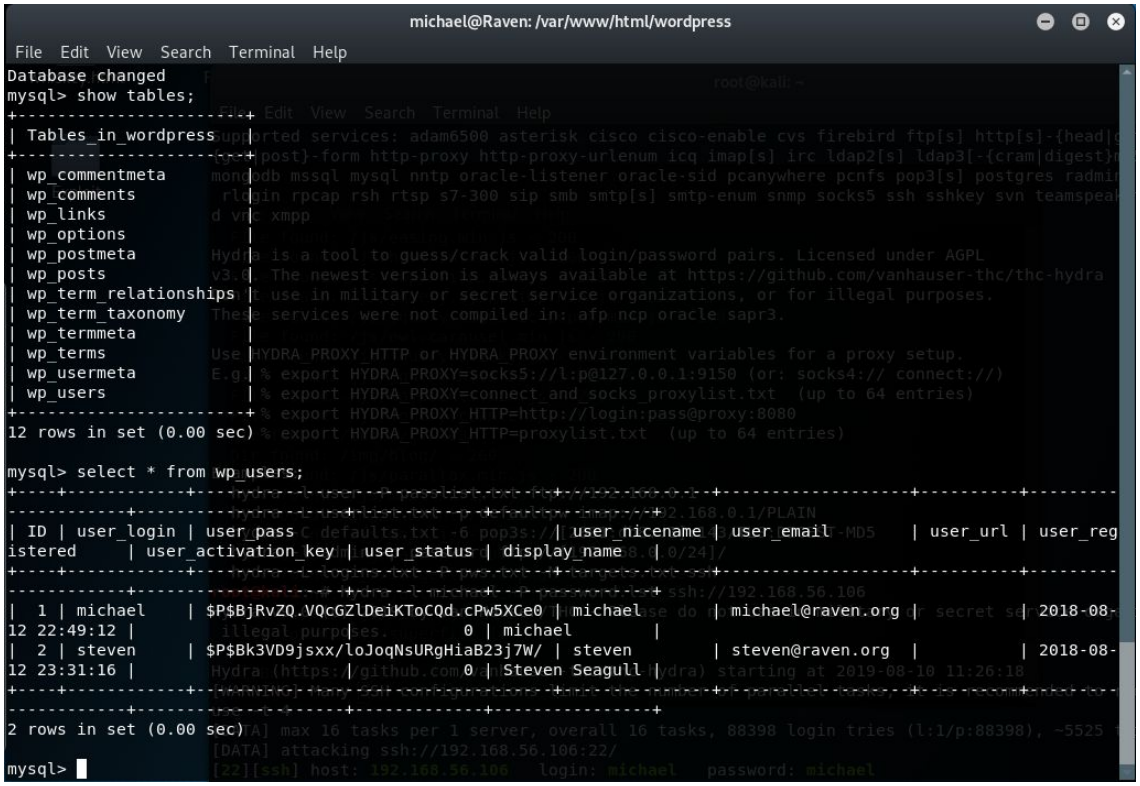
Flag #2 is found under the Var/www information



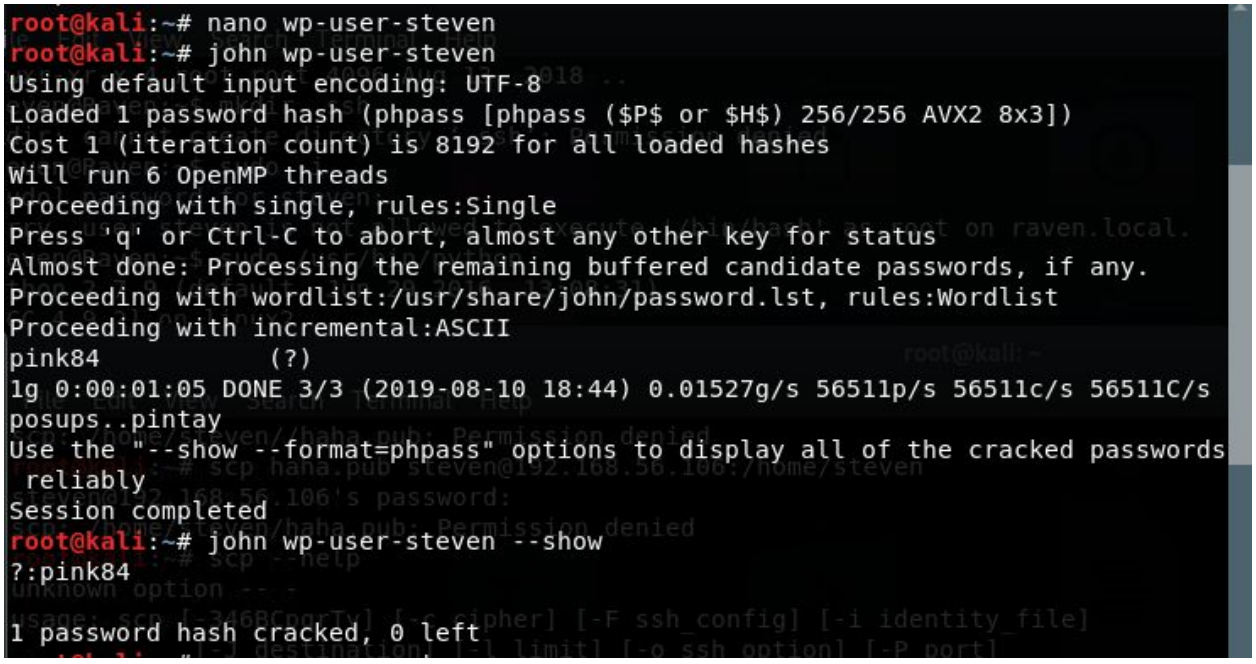
Under the further folders, one is able to find the WP-Config which hosts the MySQL Root user and password information:



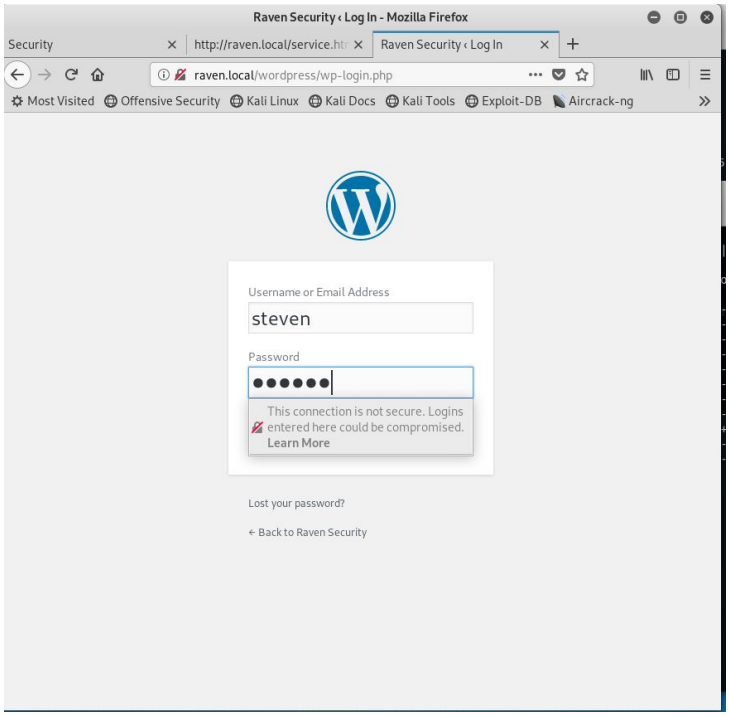
This can be used to obtain the hashed information for the second user, Steven



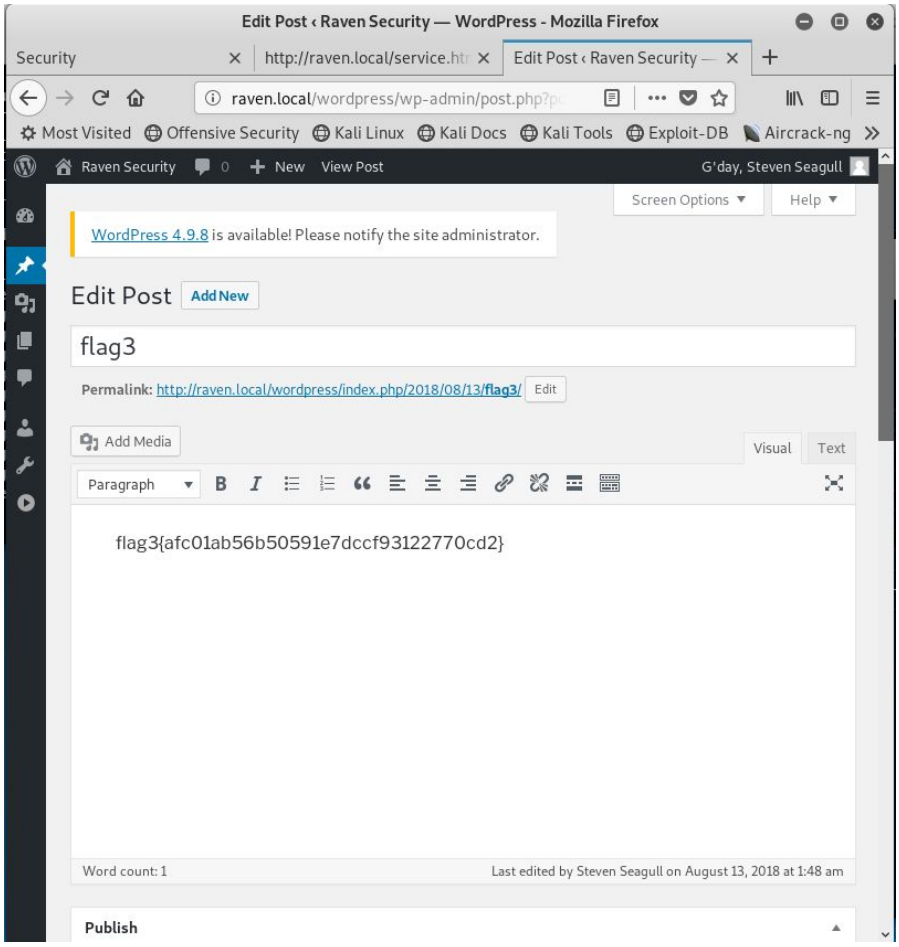
Using the Hashed information, and passing it through John the Ripper, you discover the login for Steven



Steven's login can be used for the login information for the SSH connection, WordPress Admin page, and for Privilege Escalation

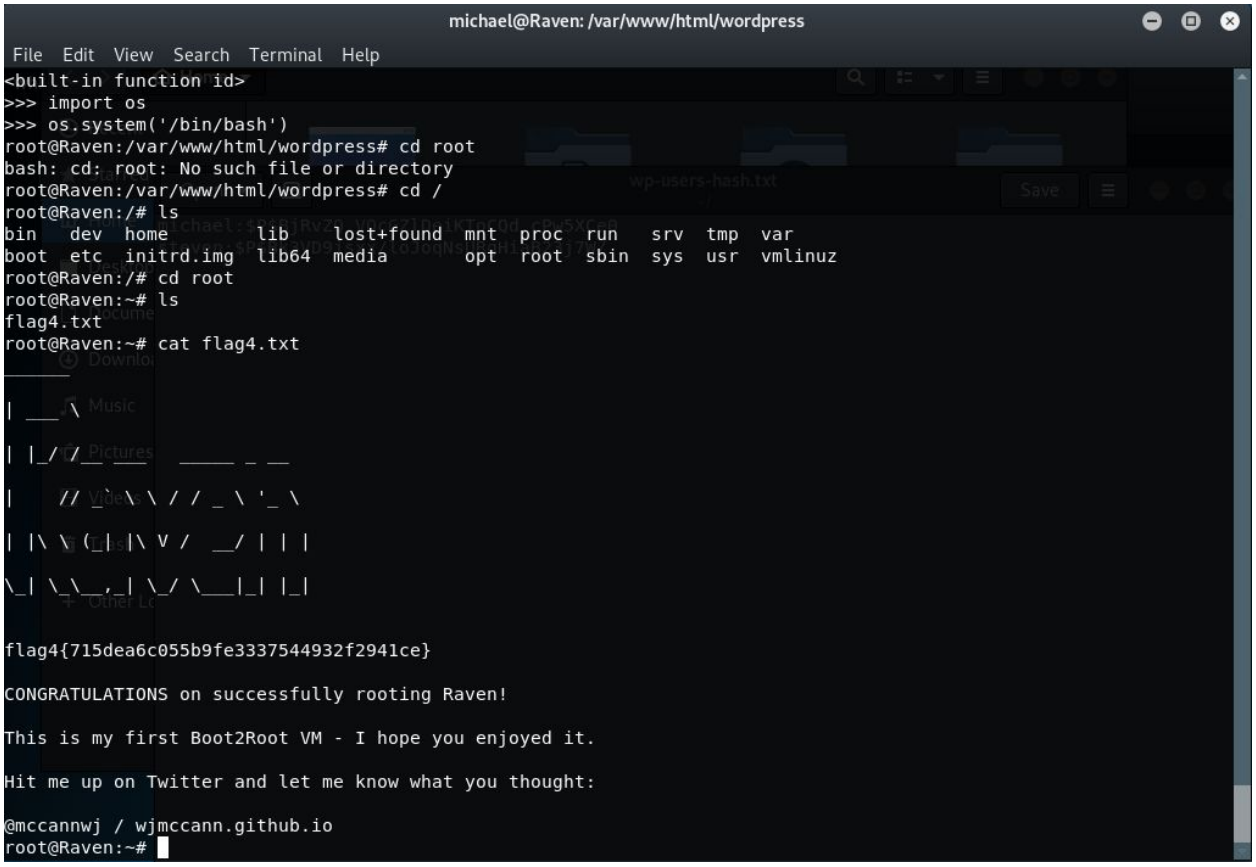


Flag #3 found under the WordPress Posts page



Post-Exploitation Exploration and Privilege Escalation

Considering Steven's privileges and ability, we are able to access Sudo and Python to allow root access to the victim machine, which leads to Flag #4 on the root of the root user.



Conclusion and Recommendations

Based on the results documented above, we recommend the client take the following steps to remediate the vulnerabilities identified on the target machine.

Web Server

- Update Wordpress to a version beyond 5.0

Network Services

- Update OpenSSH beyond version 7.5

Hardening the Server

- Remove user permissions and follow least privileges
- Update passwords to be more difficult
- Remove access to configuration files
- Use stronger password encryption and hashing method for MySQL
- Remove admin access amongst users