Cheat Sheet

Summary

## **Attacking WordPress Users**

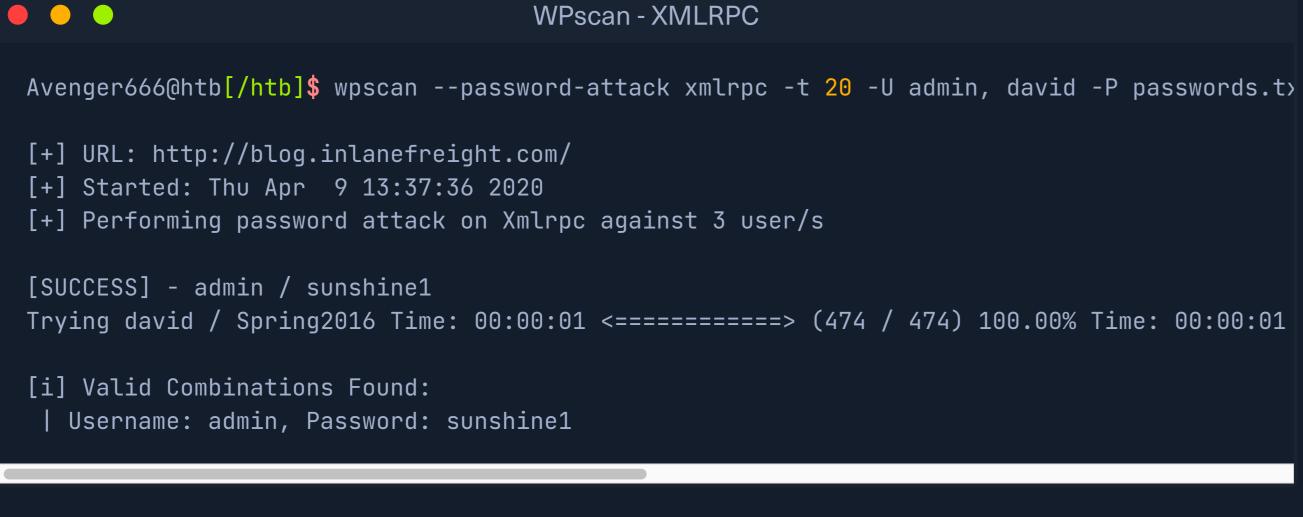
ashboard

## **WordPress User Bruteforce**

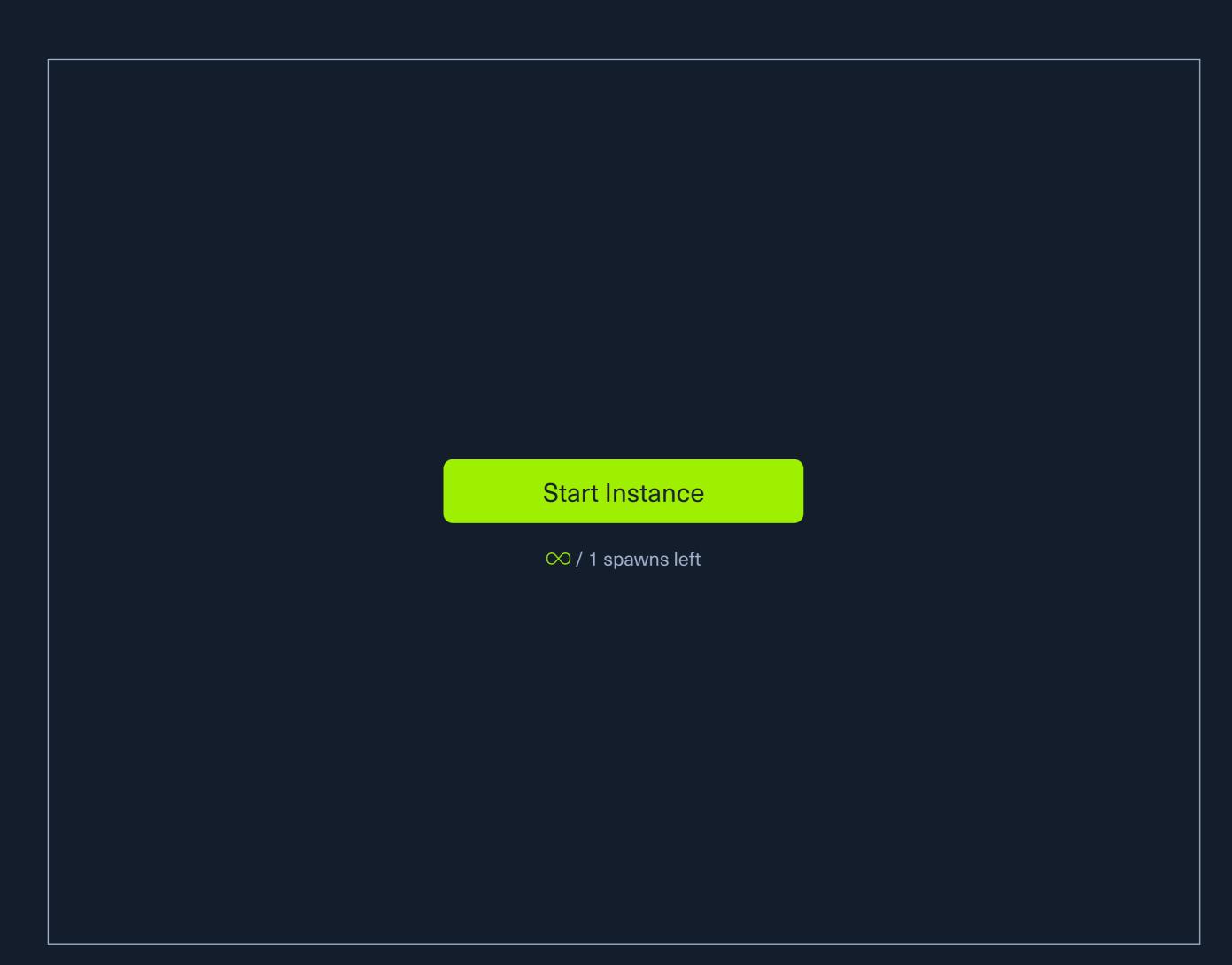
WPScan can be used to brute force usernames and passwords. The scan report returned three users registered on the website: admin, roger, and david. The tool uses two kinds of login brute force attacks, xmlrpc and wp-login. The wp-login method will attempt to brute force the normal WordPress login page, while the xmlrpc method uses the WordPress API to make login attempts through /xmlrpc.php. The xmlrpc method is preferred as it is faster.

Mødules

## WPscan - XMLRPC



Connect to Pwnbox Your own web-based Parrot Linux instance to play our labs.	
Pwnbox Location	
UK	742ms ▼
① Terminate Pwnbox to switch location	



? Go to Questions **Table of Contents** Introduction Intro WordPress Structure WordPress User Roles Enumeration WordPress Core Version Enumeration Plugins and Themes Enumeration Directory Indexing User Enumeration **6** Login **WPScan Overview WPScan Enumeration Exploitation Solution** Exploiting a Vulnerable Plugin Attacking WordPress Users RCE via the Theme Editor

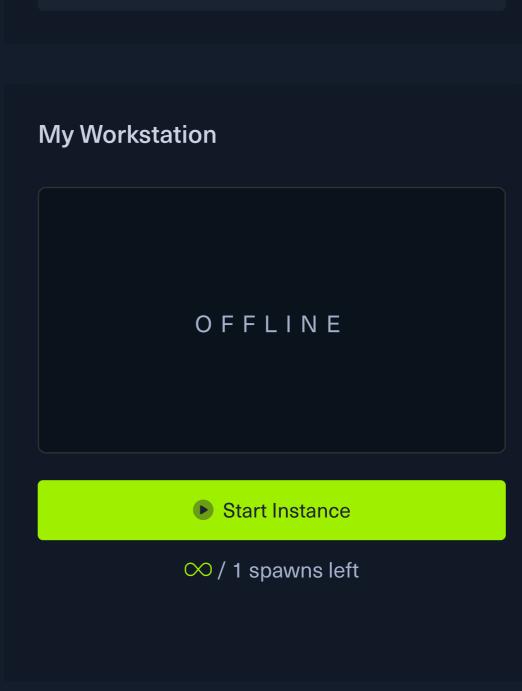
Attacking WordPress with Metasploit

Skills Assessment - WordPress

**Security Measures** 

Skills Assessment

WordPress Hardening



Waiting to start...

