




Mr. Robot CTF Walkthrough

 CTF Challenge Solved: Mr. Robot (Inspired by the TV Series)

 Platform: VulnHub / TryHackMe

 Difficulty: Medium

 Skills Practiced: Web Enumeration | WordPress Exploitation | Privilege Escalation

Challenge Overview

I recently completed the Mr. Robot CTF, a Linux-based machine that closely simulates real-world vulnerabilities. Inspired by the Mr. Robot TV series, the box offers a narrative-driven experience, testing a wide range of penetration testing skills — from web exploitation to root access.

Key Steps in Exploitation

Recon & Scanning

Used nmap to scan open ports → 80 (HTTP), 443 (HTTPS), 22 (SSH)

Discovered a WordPress site hosted on Apache

Enumeration

Found sensitive entries in /robots.txt including fsociety.dic wordlist

Used gobuster for directory discovery

Ran wpscan for user and plugin enumeration

Brute Force Login

Used hydra with fsociety.dic to brute-force login

Successfully accessed WordPress as user elli

Gaining a Shell

Uploaded a PHP reverse shell via the WordPress theme editor

Used netcat to catch a reverse shell session

↑ Privilege Escalation

Identified nmap binary with SUID permissions

Leveraged it to escalate privileges and gain root access

🚩 Flags Captured

✅ user.txt

✅ root.txt

Key Learnings

WordPress vulnerabilities are still prevalent in real-world scenarios

Proper enumeration leads to easy wins (like hidden files and usernames)

Misconfigured binaries (like SUID-enabled tools) can lead to full system compromise

👏 Final Thoughts

Solving the Mr. Robot CTF helped strengthen my understanding of:

- ✓ Gaining initial access via CMS
- ✓ Lateral movement
- ✓ Privilege escalation on Linux machines