TRYHACKME - MR ROBOT ROOM

Successfully completed the Mr. Robot CTF on TryHackMe! Here's a step-by-step breakdown of how I did it:

1. Enumeration is Key: Started with a comprehensive Nmap scan ("nmap -sC -sV -oA nmap IP") to identify open ports and services running on the target machine. Discovered port 80 for HTTP and port 443 for SSL open, with port 22 for SSH closed.

2. Exploring Web Services: Visited the IP address on port 80 and stumbled upon the "robots.txt" file, revealing hidden directories like "fsocity.dic".

3. Brute Forcing Directories: Employed Gobuster to brute force directories, uncovering additional hidden paths. Explored "/wp-login" URL, knowing it's a WordPress site.

4. WordPress Brute Force: Utilised "fsocity.dic" as a wordlist to brute force the WordPress login, leveraging Elliot's username. Successfully gained access to the WordPress admin panel.

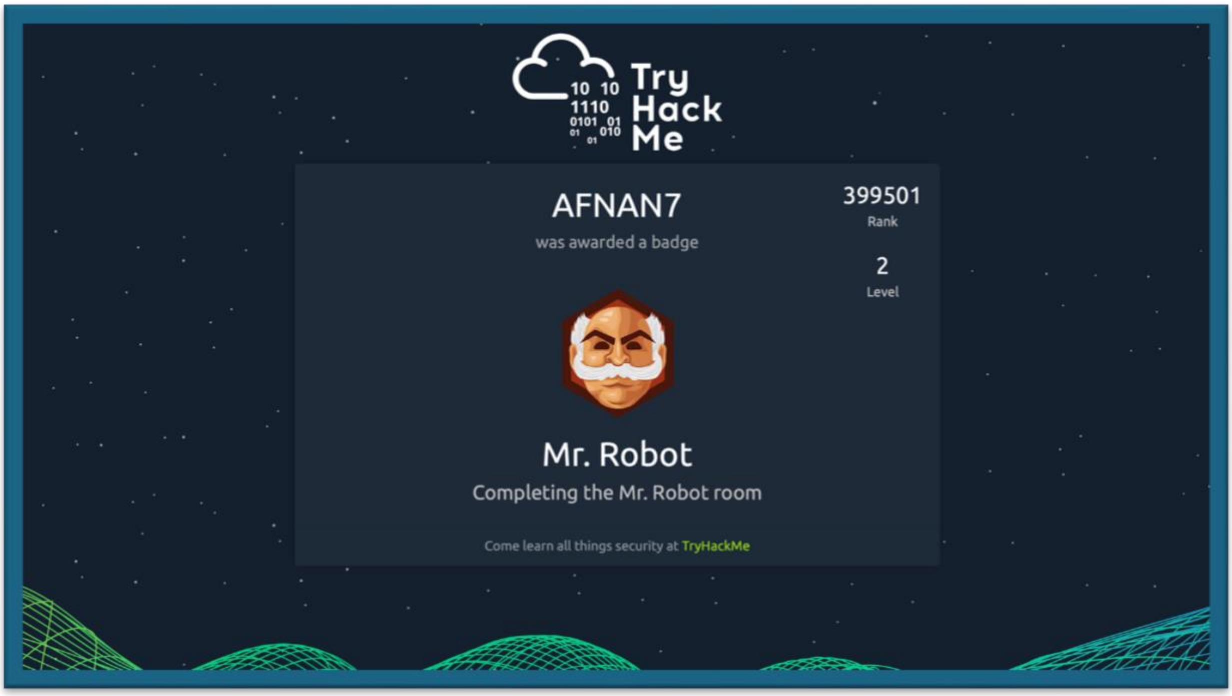
5. Exploiting Web Shell: Modified the 404 template in the Appearance/Editor section of WordPress to inject a reverse shell code.

6. Establishing a Reverse Shell: Set up an ncat listener ("nc -nvlp port") and accessed the modified URL ("IP/404.php") to trigger the reverse shell, gaining initial access to the system.

7. Privilege Escalation: Explored the home directory to find the second key but faced permission issues. Cracked hashed passwords, escalating privileges to access restricted files.

8. Root Access: Investigated SUID files and GTFOBins, eventually navigating to the root directory to find the final key.

Completing the Mr. Robot CTF was not just about solving challenges but also a journey of learning and applying various techniques in cybersecurity. Thanks to TryHackMe for providing such an immersive experience!



AFNAN7

was awarded a badge

399501

Rank

2

Level

Mr. Robot

Completing the Mr. Robot room

Come learn all things security at TryHackMe