Scanning & Reconnaissance

Storytime (Easy)

- Used `nmap -sV` to find open ports, and find the service running
- Used `ls -a` to find hidden files
- Signed in to **ftp** using `ftt <ip>`
  - Download files in ftp using `get`

Vuln Recon (Medium)

- Used `nmap -sV` to find open ports, and find the service running
- When on Apache.org to find the CVE

Feed (Hard)

- Used `nmap -sV` to find open ports, and find the service running

Enumeration & Exploitation

Break-Fast (Easy)

- Used this Code Detector to find out the program was written in **Ruby**
- Learned about **AES-128-ECB** encryption

Trojan (Medium)

- Extracted a **.exe** file by using `7z x Your.exe`
- Used **Strings** and **grep** to look for ASCII text in the file

Industry Guidelines (Hard)

- Learned **.rs** files are programs written in **rust**

Password Cracking

Common Passwords (Easy)

- Used **John the Ripper** to crack some passwords

- `john hashes.txt --wordlist=rockyou.txt --format=md5crypt`

Web Application Exploitation

Service Up (Easy)

- When to `/robots.txt` to find what directories the web page wants hidden
- Used a **user agent switcher** extension to trick the page to gain access