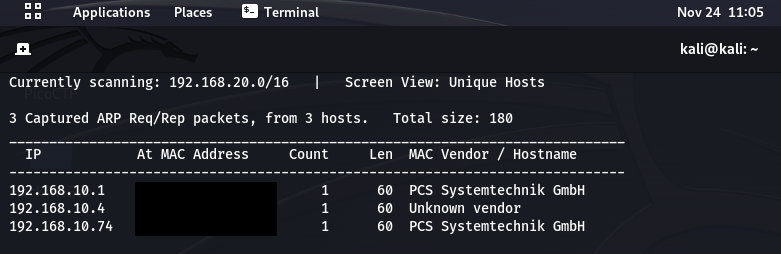
Name: Scriptkiddie

Release Date: 2021.07.20

Author: 0815R2d2

Description: This is a very simple machine that effectively showcases the functioning of the Metasploit framework. The entire process to gain root access takes approximately 5-10 minutes.

First, let's identify the machine using the 'netdiscover' command

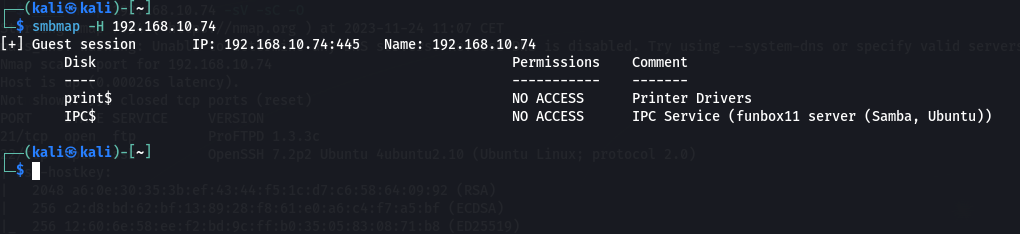


Following this, use the 'nmap' command to check for open ports:

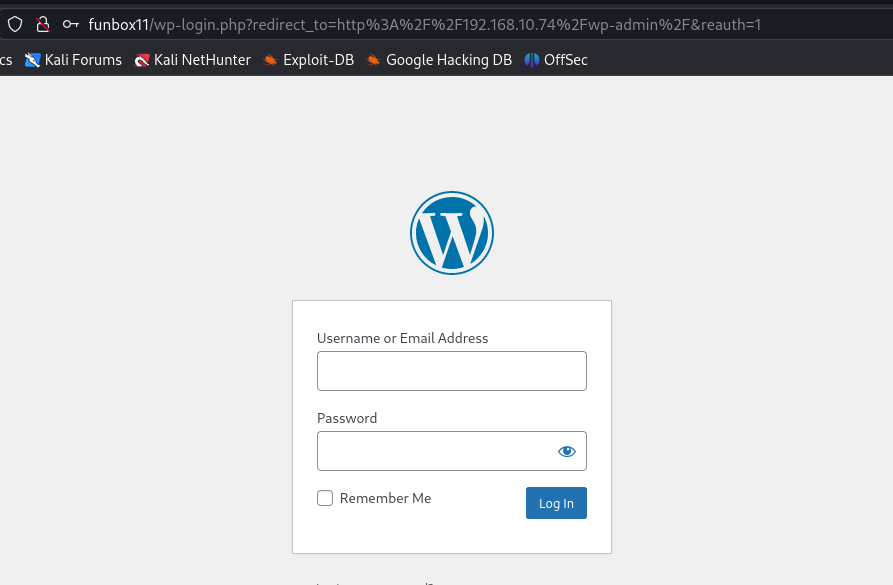
**sudo nmap 192.168.10.74 -sV -sC –O**

****

Several ports are open. I checked several of these but couldn't find anything useful. The website is a Wordpress site, but I couldn't identify any vulnerabilities there.



**smbmap -H 192.168.10.74**

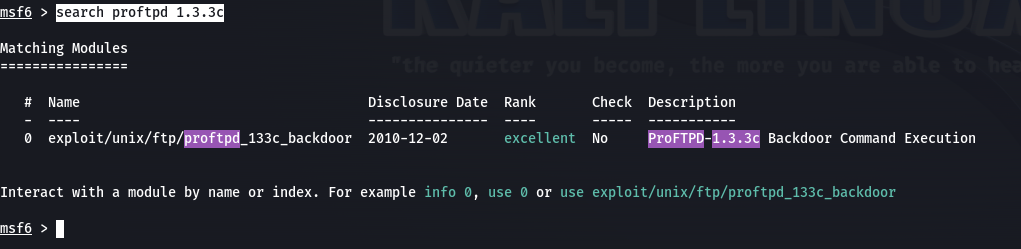


The key lies in the FTP (21) port. A quick internet search reveals that it is vulnerable and allows Remote Code Execution. All we need to do is open Metasploit.

**msfconsole**

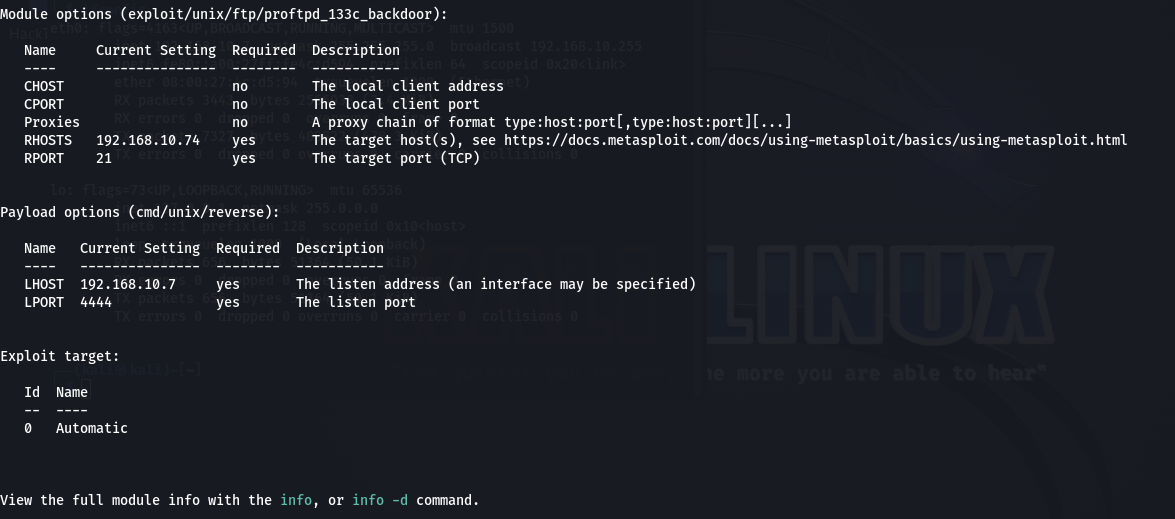


**search proftpd 1.3.3c**



Next, using the 'use {exploit}' command, we can select it. Upon typing 'options', it displays what needs to be configured. With the 'set {option name} {data}' command, we can configure these settings. Then, using 'show payloads', we select a payload which we can set with 'set payload {payload}'.

https://docs.metasploit.com/docs/pentesting/metasploit-guide-setting-module-options.html



Finally, the 'run/exploit' command executes the script. If everything is configured correctly, we successfully gain access to the system with immediate root privileges.

