### **Exposed Services**

Nmap scan results for each machine reveal the below services and OS details:

$ nmap ... # TODO: Add command to Scan Target 1

Nmap scan: nmap -sV 192.168.1.0/24

Output: 192.168.1.100 - unknown OS

22 - ssh

9200 - http

192.168.1.105 - unknown OS

22 - ssh

80 - http

192.168.1.110 - linux - target 1 machine

22 - ssh

80 - http

111 - rcpbind

139 - netbios

445 - netbios

192.168.1.115 - linux

22 - ssh

80 - http

111 - rcpbind

139 - netbios

445 - netbios

This scan identifies the services below as potential points of entry:

* Target 1
  + Port 22, SSH could allow connection over username and password which could be exploited with weak passwords or if the username becomes known.
  + Port 80 HTTP this device could be running web applications or services that could be exploited.
  + Port 111 RCP may indicate communication with other devices on the network this could allow avenues of attack from another device. .
  + Port 139, 445 netbios allows for more communication from the target device and possible file transfer.

The following vulnerabilities were identified on each target:

* Target 1
  + Apache is running on port 80 and allowing http traffic through this port. There are two known critical vulnerabilities on this version of apache that allow for path traversal (CVE-2021-41773) There was an attempted patch
  + The device allows any machine to try and connect over SSH on port 22 with password authentication.

### **Exploitation**

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

* Target 1
  + flag1.txt: Please see attached picture within folder for picture.
    - **Exploit Used**
      * Easy to guess password allowed access to the machine.
      * Searching for file with grep -r “flag” /var/www
  + flag2.txt: Please see attached picture within folder for picture.
    - **Exploit Used**
      * From the network scan it showed an apache server running. The location of the data for the server was located in the standard directory.
      * Found file while searching for information about the site.