# Ex050

Joshua Main-Smith

2020-10-01

## Contents

# Technical Report

## Risk Assessment

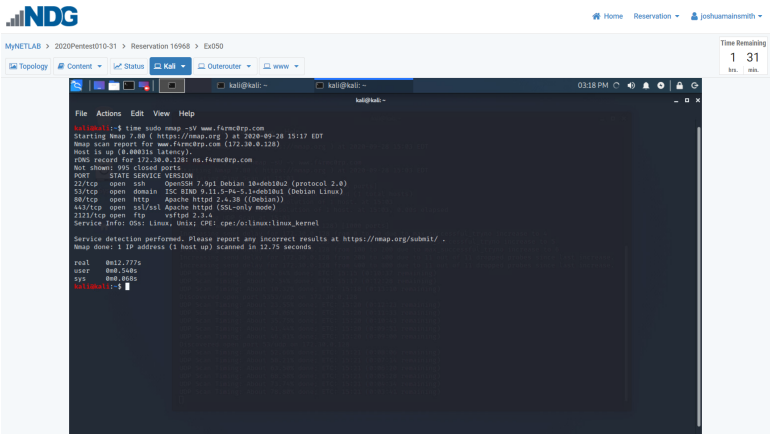
### Vulnerability Description

There were vulnerabilities found in a few of the open TCP ports when scanning **www.f4rmc0rp.com**.
Port 22 is running an SSH service with version OpenSSH 7.9, which is susceptible to a man-in-the-middle attacks and allows remote servers to bypass access restrictions (relevant CVEs: CVE-2019-6111, CVE-2019-6110, CVE-2019-6109, CVE-2018-20685).
There appears to be vulnerabilities surrounding the use of BIND 9.11.5.P4, but all ISC releases are unaffected which port 53 uses.
Port 80 uses Apache httpd 2.4.38, which is vulnerable to multiple slashes being used for services, such as LocationMatch and RewriteRule, need to account for regular expression and servers will end up collapsing them (relevant CVE: CVE-2019-0220).
Port 2121 was running an FTP service with version vsftpd 2.3.4, which is vulnerable to a remote Metasploit backdoor execution command. Further, we were able to connect to the FTP service and login using the default login credentials.

# Attack Narrative

## TCP Version Scan

The first thing we did was run a version scan against **www.f4rmc0rp.com**, using the Linux command **time sudo nmap -sV www.f4rmc0rp.com** (we included time at the beginning to show the difference in scanning time between a TCP and and an UDP scan). As can be seen in the image below, the open TCP ports out of the 1000 scanned are 22, 53, 80, 443, and 2121.



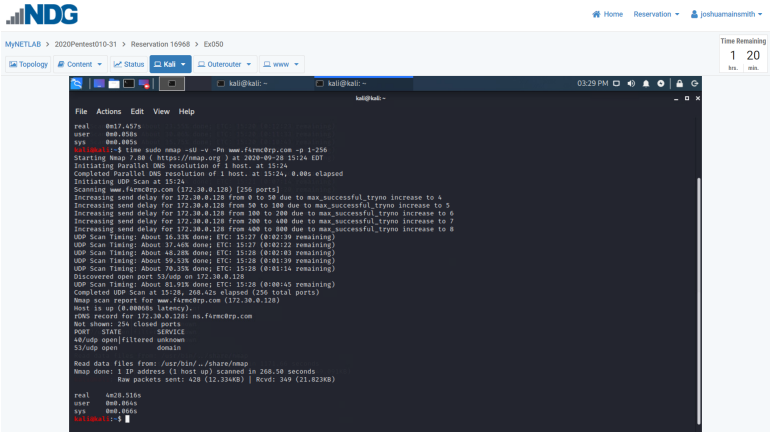

Each port with its service and OS Version are listed in the table below.

| Port | Service | OS Version |
|---|---|---|
| 22 | ssh | OpenSSH 7.9 |
| 53 | domain | ISC Bind 9.11.5 |
| 80 | http | Apache httpd 2.4.38 |
| 443 | ssl | Apache httpd |
| 2121 | ftp | vsftpd 2.3.4 |

Something interesting to note is that it's atypical for an FTP service to be used over port 2121. FTP is usually used over ports 20 or 21. There are also some vulnerabilities associated with this version of FTP used, which is discussed under the vulnerability assessment above. In fact, we were able to connect to the FTP server by simply executing the command **ftp -p 172.30.0.128 2121** and providing the default login credentials. We were able to read and download a file located there. So, any sensitive information stored there is subject to exposure.

## UDP Scan

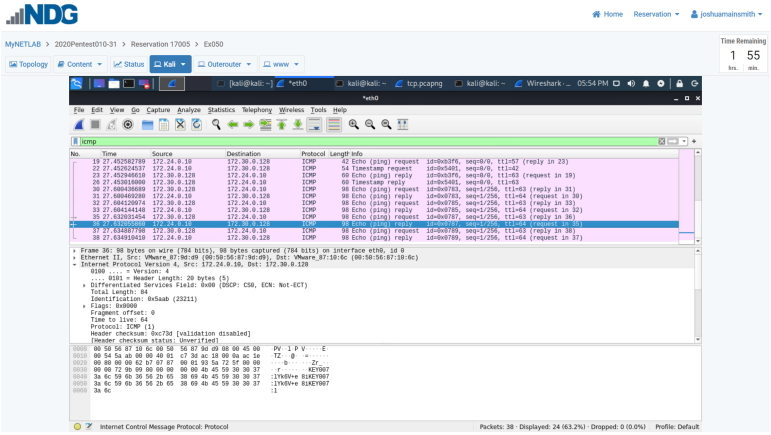
Now, scanning for UDP ports we executed **time sudo -sU www.f4rmc0rp.com -p 1-256**. Even though we only scanned 256 ports for UDP (as compared to the 1000 ports for TCP), the UDP scan still took considerably longer. This is due to the fact that TCP is a connection-oriented protocol whereas UDP is a connectionless protocol, a screenshot of which can be seen below.

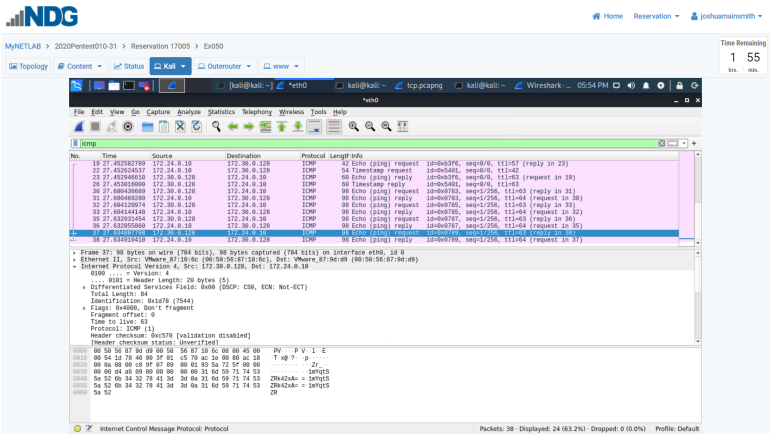


After the completion of the UDP scan over ports 1-256, we discovered that ports 40 and 53 were open. A table of each port with its service is listed below.

| Port | Service |
|---|---|
| 40 | unknown |
| 53 | domain |

Something interesting to note from this is the service that port 40 is offering is unknown. To get a better idea of what's going on with this port, we used Wireshark to analyze the packet response generated over port 40. We used the Linux command **sudo nmap -sU www.f4rmc0rp.com -p 40**, and took a look at what the server response is. Looking at the echo request from our host machine (172.24.0.10) to our target machine (172.30.0.128), we found something interesting from the server response of port 40 under the data section of ICMP packets. Particularly, we found what appears to be a key with the value **KEY007:lYk6V+e8i1mYqtSZRk42xA==**. These responses can be seen in the two screenshots that follow.





# Zoom Link

September 28, 2020