# Unit 3 Activity

## Port Scan

| TCP Port | IPV4 State | Service |
|---|---|---|
| 21 | FILTERED | ftp |
| 22 | FILTERED | ssh |
| 23 | FILTERED | telnet |
| 25 | FILTERED | smtp |
| 53 | FILTERED | domain |
| 80 | FILTERED | http |
| 110 | FILTERED | pop3 |
| 137 | FILTERED | netbios-ns |
| 138 | FILTERED | netbios-dgm |
| 139 | FILTERED | netbios-ssn |
| 443 | FILTERED | https |
| 445 | FILTERED | microsoft-ds |
| 587 | FILTERED | submission |
| 993 | FILTERED | imaps |
| 995 | FILTERED | pop3s |
| 1080 | FILTERED | socks |
| 1433 | FILTERED | ms-sql-s |
| 1701 | FILTERED | l2f |

| | |
|---|---|
| OPEN | An application is listening for connections on that port |
| CLOSED | No application listening on that port |
| FILTERED | The port is blocked by firewall or other network obstacle |

All the ports that showed up were marked as **filtered.** I'm not the most concerned with these results. This is because filtered means that a firewall service is blocking them. This is good because it means I have something protecting them. But I can't be 100% fine, because there is always some way for intrusion, no matter how protected you think you are.

## Mac Address

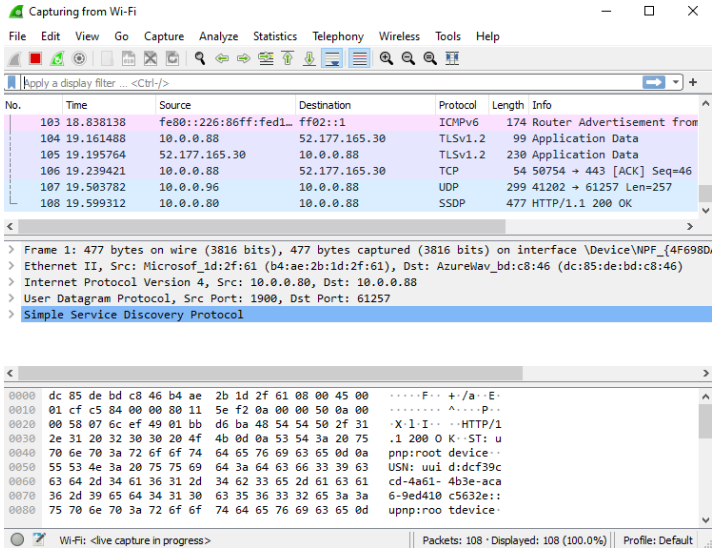
| | |
|---|---|
| Manufacturer: | Intel Corporation |
| Description: | Intel(R) Wireless-AC 9260 160MHz |
| Driver version: | 21.120.0.9 |
| Physical address (MAC): | 58-A0-23-D9-F7-8D |

Copy

For where I am supposed to go in and spoof my address, I can't do that. Since I use my school computer, those settings are blocked by my school.

For if spoofing in this case is ethical, I think it depends. If you are doing it for good intentions or protection, I think it's fine. But if you are doing it to get some benefit out of it (not in the greatest way), then it may be a problem.

# WireShark




I learned that there are tons of packet being transferred between my computer and the internet every second. That's how information is transferred between the two destinations. A packet sniffer can be beneficial in Cybersecurity because they can help misemployment to the network, and can also monitor the usage of the network to see what is going on.