Research Report 2 Wireshark by Masyn Grisel

What did you do?

Before installing and using Wireshark, I watched a video titled “Wireshark Tutorial For Beginners” by Anson Alexander. This was done to gain a better understanding of Wireshark and it’s capabilities before using it. According to his website, Anson Alexander “specializes in technology education and provides free text and video training tutorials covering various applications and devices.” Next, I installed Wireshark and began capturing packets on my home Wi-Fi because this is the network I use. While I waited about 5 minutes for Wireshark to finish, I researched what exactly Wireshark does. It was important for me to understand how the software works, so I could better analyze the results. Next, I turned to another video. This video was titled “Network Sniffing: Using Wireshark to Find Network Vulnerabilities” by David Hoelzer. I used this video because I needed to know how to use my Wireshark results to find weaknesses in my network. The first video I watched was more about how to use Wireshark, and the second video is about how to analyze the results from Wireshark. Next, I researched which ports were the most vulnerable to cyber attacks. I am fairly new to ports and cybersecurity, so I did not know how to tell which ports were normal to be used and which were not. To do this, I found an article titled “Packet Analysis Using Wireshark” by Temitope Adegoke, who is a Junior Security Analyst at RDB Concepts Ltd. I used the ports I found to be vulnerable as a filter on Wireshark which allowed me to see exactly how many packets were sent to these ports. After breaking down the results from my Wireshark capture, I researched methods to strengthen my network’s weaknesses and prevent attacks.

What are the results?

Here is a paragraph from comptia.org explaining what Wireshark does: “Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.”

To begin my research, I started running Wireshark on my Wi-Fi, not Ethernet because we all use Wi-Fi in my house. After about 5 minutes of letting Wireshark capture my packets, I had the results. The total packets captured was 5302. To analyze the results, I added filters. The filters that I chose to add came from two sources, blog.newtrix.com and linuxhint.com. These websites go into detail about which ports are the most vulnerable and why. Below I will list each filter and the results:

* Port 53: 42/5302 (0.8%)
* Port 20: 0/5302
* Port 22: 0/5302
* Port 80: 0/5302
* Port 443: 1690/5302 (31.9%)
* Port 7: 0/5302
* tcp.flags==0x012 : 7/5302 (0.1%)
* tcp.flags==0x004 : 0/5302
* arp.packet-storm-detected : 0/5302

After obtaining the results for each filter, I broke down what my vulnerabilities were. First is port 53. “Port 53 is for Domain Name System (DNS). It’s a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks(Schrader, 2022).” Although this port is vulnerable to attacks, only 0.8% of my packets went to this port.

Next, I analyzed ports 80 and 443 together. Even though port 80 resulted in 0%, I thought it best to analyze them together based on their uses. Port 443 accounted for 31.9% of my packets, which is a large amount. This number is large because, according to clickssl.com, “Port 443 allows data transmission over a secured network, while Port 80 enables data transmission in plain text. Users will get an insecure warning if he tries to access a non-HTTPS web page.” Basically, these ports are a security measure when accessing a webpage.

Tcp.flags==0x012 is a filter I obtained from Temitope Adeoke on LinkedIn as a method of “syn scanning.”. He states, “SYN scanning involves the establishment of a half connection with the destined target i.e. three-way handshake wasn't completed. Attackers can use it to determine open ports at a fast pace and also can be use to cause harm to computer/server.” This port made up 0.1% of my results, which is a relatively low percentage. However, it is alarming because it shows that I do have open ports which can be vulnerable.

Here is a brief description of the ports that resulted in 0% of my capture that I filtered for:

Port 20 and (mainly) port 22 are File Transfer Protocol (FTP) ports that let users send and receive files from servers.

“FTP is known for being outdated and insecure. As such, attackers frequently exploit it through:

* Brute-forcing passwords
* Anonymous authentication (it’s possible to log into the FTP port with “anonymous” as the username and password)
* Cross-site scripting
* Directory traversal attacks “(Schrader, 2022)

Port 7 was filtered for to detect ping sweeps. According to Temitope Adegoke, “Bad actors who are trying to get into a network also use ping sweeps to determine which computers are online and where to focus their attacks.” This is good for me because a hacker can not tell that I am online, which matches the results obtained from my Shields Up report.

Tcp.flags==0x004 is used “when a server indicates that a port is closed and secured by sending a RST packet from that port. In these situations, the hacker sends an enormous amount of SYN packets, which the server accepts, but there is no communication or connection formation between the client and serve(Adegoke 2023).” Any results on this scan would be alarming as they would signal a direct attempt to hack my network.

The last filter, arp.packet-storm-detected was used to detect an ARP storm. “Arp storm is an attack which causes DoS or DDoS attack. Arp storm is a network problem which an attacker causes within a local network by generating broadcast messages with IP address in that network range or sending it to IP address not present in that network range(Adegoke 2023).”

Overall, the results of my home network scan using Wireshark were what I expected. There were no direct cyber attacks detected because they did not show up on the filters I looked for. However, this does not mean my network is completely secure, as seen by the number of packets sent to ports 53 and 443. This does mean, in order to be extra cautious, it would be best to install a firewall to protect my network by blocking unwanted traffic.

What did you learn?

Throughout my research, I learned about the various vulnerabilities in my home network and how they can be exploited. I learned how to use tools like Wireshark to dive deep into my network and understand the details behind it all. Like I stated earlier, I am fairly new to the cybersecurity world, so it was important for me to research everything I was doing. This helped me gain an understanding of what my Wireshark capture results mean, so I am able to analyze the results. In the future I believe it will be critical to use these tools on a network that is business related rather than my home network. If I were in a situation where I had valuable and sensitive information on my network, it would be important to constantly make sure I am protecting that network. I believe frequent use of Wireshark would help continually understand the strengths and weakness of my network. Understanding how to utilize these tools will be valuable to an organization because it can help prevent any cybersecurity attacks.

Resources:

Alex, Anson. "About AnsonAlex." AnsonAlex.com, AnsonAlex.com, Accessed 3 March 2024, <https://ansonalex.com/about/>.

"What is Wireshark and How to Use It." CompTIA.org, CompTIA, Accessed 3 March 2024, <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it#:~:text=Packet%20Capture%3A%20Wireshark%20listens%20to,random%20live%20data%20using%20filters>.

Hoelzer, David. "Network Sniffing: Using Wireshark to Find Network Vulnerabilities." YouTube, uploaded by David Hoelzer, 2012, <https://www.youtube.com/watch?v=qzonPrKNhwc>

Varonis. "How to Use Wireshark." Varonis Blog, Varonis Systems, Accessed 3 March 2024, <https://www.varonis.com/blog/how-to-use-wireshark#filters>.

LinuxHint. "How to Filter by Port in Wireshark." LinuxHint, Accessed 3 March 2024, <https://linuxhint.com/filter_by_port_wireshark/>.

Adegoke, Temitope. "Packet Analysis using Wireshark." LinkedIn, Accessed 3 March 2024, <https://www.linkedin.com/pulse/packet-analysis-using-wireshark-temitope-adegoke>.

Netwrix. "Open Port Vulnerabilities List." Netwrix Blog, Netwrix, 4 August 2022, <https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/#:~:text=Port%2053%20is%20for%20Domain,particularly%20vulnerable%20to%20DDoS%20attacks>.

ClickSSL. "Port 80 HTTP vs Port 443 HTTPS." ClickSSL Blog, ClickSSL, Accessed 3 March 2024, <https://www.clickssl.net/blog/port-80-http-vs-port-443-https#:~:text=Port%20443%20allows%20data%20transmission,a%20non%2DHTTPS%20web%20page>.