Research Report 2 Wireshark

1. What did you do

For this assignment, I used Wireshark to explore a network, protocol identification, and packet capturing. First, I installed Wireshark on my computer. I then launched Wireshark and selected my network interface to capture packets from my home network. I allowed the scan to run for 5 minutes. While the scan ran I browsed a few websites and streamed a YouTube video to help generate content. After saving the scan I proceeded to look over it. The computer I used has a wireless internet/Bluetooth card and a single network jack. The capture was done on the single network jack.

Wireshark is a network packet analyzer, a tool able to capture packets on a network and preserve as much detail about them as possible. It will use a library called Libecap to actually capture the packets, and then filter and analyze the captured information. Wireshark also is able to decode packets and display the contents in a readable format.

1. What are the results

After running for 5 minutes Wireshark captured 407,603 packets. The average packet size was 1079Bytes.

A screenshot of a computer

Description automatically generated

It looks like I was able to capture packets associated to 94 different IPs. The most popular 2 10.0.0.51, my desktop, at 407,095 packets and 146.75.106.133 at 386,926 packets.This second IP appears to a cloud platform that provides a content delivery network based in Sweden. It looks like that would be mostly the video I was streaming. The third highest packet count goes to 192.195.76.30 at 3430. This is the IP for login.wtamu.edu. Of the 94 IPs 9 where local. It did find my local DNS server at 10.0.0.10 with only 183 packets.

Wireshark found 23 different protocols. The majority at 391,251 where sent via TCP. This makes since since a video would need to confirm the packets are being received so it can resend them. The second highest is TLS, Transport Layer Security version 1.2 and 1.3. These are encrypted packets being sent between devices or applications. Wireshark can see the encrypted data but it is unreadable. The third highest was QUIC (Quick UDP Internet Connection) at 626 packets. QUIC is a low latency protocol primarily used by streaming site, VoIP, and online gaming. It seems to be an encrypted protocol as well.

As far as I can tell my packet capture does not contain any hacking, but I am no expert on packet captures. From the bit of research, I did to see what to look for I found that there is hardly ever one specific thing to look for. It is also very difficult to impossible to see if I’ve already been hacked already. Most of the IPs and protocols seem to be from legitimate sources to me.

1. What did you learn

Every time a packet is sent in or out of my network could be a potential attack surface. All it would take is someone scanning the traffic in my network or even from my network. This is one of the reasons everyone talks about needing a VPN, Virtual Private Network, since all your data will be encrypted. From just a 5 minute scan I could have very good idea of what a user is doing and what devices are active on a network. All it would take is time and someone could easily steal my data.

Something I’ve been thinking about is the role that AI could play in all of this. This is a large amount of data being captured and I wonder if an AI could be trained to look for hacking or malicious content. It could also potentially scan live or close to it.

I’ve installed SonicWall Firewalls before and their price always shocked me especially when compared to the speed at which they can fully scan a network. Four years ago a almost $1000 SOHO SonicWall with licenses would scan at only 50mbps. In 2018 I had gigabit symmetric internet. After doing this I have a better understanding and appreciate for a firewall and the active protection it provides.

References

Chapter 4. Capturing Live Network Data. (n.d.). [Www.wireshark.org](http://Www.wireshark.org). <https://www.wireshark.org/docs/wsug_html_chunked/ChapterCapture.html>

How Wireshark Works – A Simple Guide. (n.d.). Alphr. https://www.alphr.com/how-wireshark-works/

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch01\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650746\_1/xid-51650746\_1

Jennex, M. (2023). Why Computers Are Vulnerable r3 [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650747\_1/xid-51650747\_1

Jennex, M. (2023). CIDM6341 Introduction [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650748\_1/xid-51650748\_1

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch12\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646267-dt-content-rid-51650758\_1/xid-51650758\_1