

Risk Management with Wireshark

Timothy Pasquel

CSC341 – 020

Abstract

The purpose of this assignment is to apply Risk Management principles (Module 4 from the text and lectures) in conjunction with the analysis from Wireshark's networking packets. The project provides an opportunity to simulate an information security scenario to assess potential issues coming from a network analysis tool, Wireshark, and determine the risk management outcomes. A Packet Capture (PCAP) file from the network is used to illustrate a Distributed Denial of Service (DDoS) attack on a web server. The affected systems risk is then calculated to determine the importance of this impact on a business. Finally, some ways to solve this risk on the affected systems are discussed.

Keywords: *Risk Management*, Wireshark, CSC341, Fall 2023

Table of Contents

1. Section 1 (CSIT-11): Analyze a Complex Problem.....	4
1.1 About Wireshark.....	4
1.2 Advantages and Disadvantages of Wireshark.....	5
1.3 Key Protocols Discovered.....	6
1.4 PCAP Analysis.....	8
2. Section 2 (CSIT-12): Define Principles to Identify Solution.....	9
2.1 Information System Components.....	9
2.2 Weighted Table Analysis (Risk Impact).....	10
2.3 Risk Likelihood (Risk Probability).....	11
3. Section 3 (CSIT-13): Apply Principles to Identify Solution.....	12
3.1 Risk-Rating Factor.....	12
3.2 Risk Treatment/Response.....	13
3.3 Risk Residual.....	13
References.....	15

1. Section 1 (CSIT-11): Analyze a Complex Problem

1.1 About Wireshark

Many tools can be used in the field of Information Security (Info. Sec.). Some tools are used to look at local hard disks, some are used in a forensics sense, and some are used to look over the network. However, there is one network tool that stands above the rest and that tool is Wireshark. The project started in 1998 with major contributions made by Gerald Combs along with assistance from The Wireshark Team once the tool began to gain traction. The group's purpose was to create a network protocol analyzer for both the industry and the masses. The tool has many features such as the inspection of hundreds of protocols, live capture, offline analysis, three-pane packet browser, VoIP analysis, read and write to many different capture file formats, data capture from Ethernet, ATM, Bluetooth, USB, and much more. Furthermore, the software is available on a majority of operating systems such as Windows, OS X, FreeBSD, and NetBSD. Wireshark is a simple yet powerful tool and it can be broken down into simple steps. Wireshark first, listens to the desired live network connection and takes in all of the traffic. Then the users can use a filter on this traffic and sort out what they would like to see such as Transfer Control Protocol (TCP), Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), etc. Finally, Wireshark then can display all of the desired network traffic packets into a nice display that can be analyzed as said before either in real-time or saved and then looked at later on. As it can be seen, Wireshark can be an immensely valuable tool for Info. Sec. Professionals from all sectors of industry can use this tool to help with troubleshooting potential problems on the network, solving performance issues, viewing suspicious network communications, and much more.

1.2 Advantages and Disadvantages of Wireshark

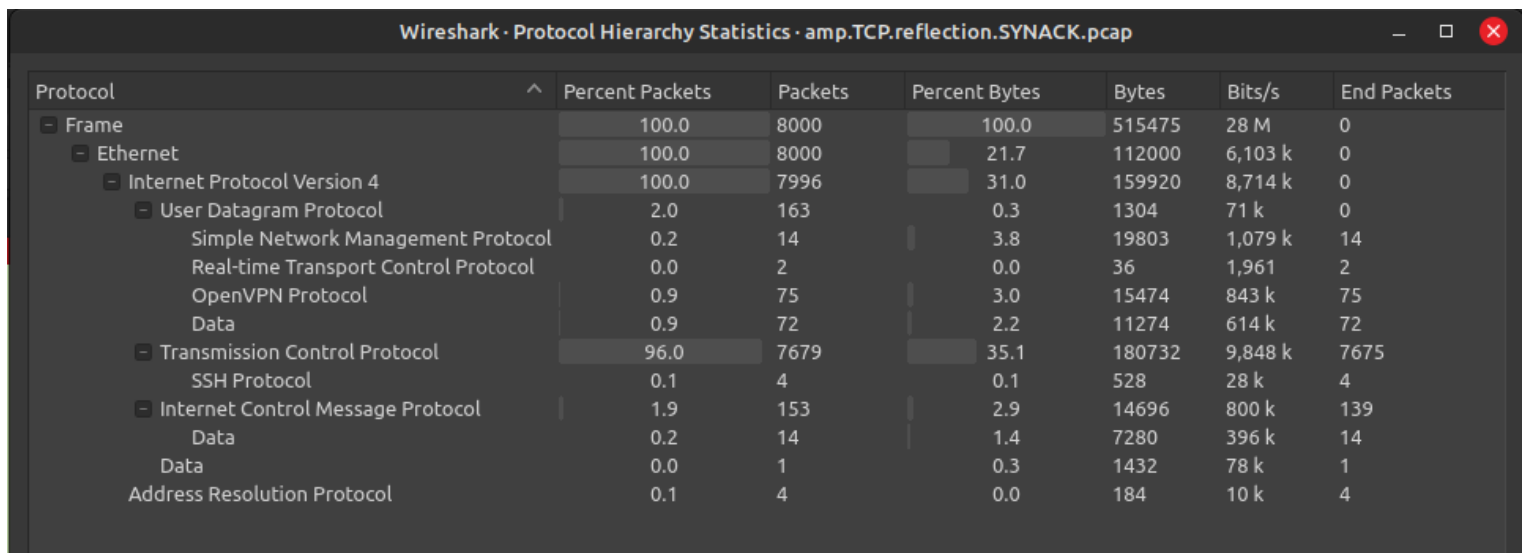
While Wireshark is an important tool for any Info. Sec. Professionals out in the field, it has both its many advantages as well as its disadvantages that need to be discussed. One disadvantage of the tool is that the tool only gives the data on the network, it is up to the person reading the data to determine if there is an issue or vulnerability. One of the more predominant disadvantages of Wireshark is that because it is so widely used and available, hackers or malicious individuals also can use the tool. These hackers and malicious individuals can then survey the network to read packets and possibly find out passwords or trade secrets as well as conduct man-in-the-middle attacks. A man-in-the-middle attack is when hackers intercept a packet change the data inside to the desired contents and resend the packet to its original destination. The last disadvantage of Wireshark is that, unlike the application tcpdump, which is a command-line application similar to Wireshark. Wireshark has a Graphical User Interface (GUI) which hosts many filters, and settings that may not be useful to the user. This means that the user could be overwhelmed with content to look at, making it harder to find what they are looking for. Plus, this could hinder the overall performance of the computer. Tcpdump on the other hand, is a command line application that is much more lightweight on computer resources and displays just the current traffic on the network. Moving onto the advantages of Wireshark, one advantage is that it is a free and open source software, which means that the users have full transparency as to what is written in the application and it is extremely accessible to any users with a computer. Another advantage of the software is that both users and professionals can use the tool to check their own network for malicious activity as well as performance so that those issues can be resolved or patched up. Finally, an advantage for more experienced users is to use the graphs and chart section to help visualize the data on the network. This is a major benefit for professionals, which tcpdump does not have by default, as it makes the communication between management easier to bridge. Overall, Wireshark has some disadvantages but also has a plethora of advantages as well.

1.3 Key Protocols Discovered

During the analysis using Wireshark, it can be seen that there were many different kinds of protocols in the Packet Capture (PCAP). Some of the more prevalent protocols were the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). UDP is the first major protocol listed coming in at 2% of all of the network traffic. UDP is a Transport Layer Protocol that is considered to be unreliable and connection-less. This makes it easy to establish lower latency and lightweight network traffic which makes it a great protocol for simple requests, Voice over Internet Protocol (VoIP), streaming applications, etc. There were also 3 sub-protocols under UDP which are Simple Network Management Protocol with 0.2%, Real-time Transport Control Protocol with 2 packets, and Open Virtual Private Network (VPN) Protocol with 0.9%. Simple Network Management Protocol is an application layer protocol that uses UDP to send its data. Its main purpose is network monitoring, communicating with remote devices, and finding issues on the network. Real-time Transport Control Protocol is another protocol that uses UDP as its base. This protocol allows the messages sent to control the transmission as well as the quality of the data. Furthermore, when the recipients receive the message, they give feedback to the source to see if the quality of data needs to be changed. Lastly under UDP is the OpenVPN Protocol which encrypts network communication. When two clients use OpenVPN, create a tunnel between the two computers using the Secure Socket Layer encryption method which ensures the data remains private. Moving onto the next major section, which created 96% of the network traffic is TCP. TCP uses both the Application layer as well as the Network layer and its purpose is to provide a reliable, connection-oriented service. TCP does this by breaking down data into smaller sections, sending these sections over the network, and reassembling them at their destination. Once, the entire message is received, the data can be read in full without any loss. If a section were to get lost in transit, an entirely new request would be made so that the whole message gets to its intended user. In this example, there is one protocol that uses TCP as a base and that is the

Secure Shell (SSH) Protocol which took up 0.1% of the network traffic. The SSH Protocol is used for sending commands to a computer over a network in a secure manner. It is useful for controlling servers, managing key Information Technology infrastructure, as well as transferring files from host to host. Another protocol that needs to be mentioned is the Internet Control Message Protocol which had 1.9% of the packets. This protocol function serves as a diagnostics tool in the network layer. It completes error control mechanisms which makes it a support-based service for network devices. Overall, in the analysis, there were a plethora of different kinds of protocols used, however, each one serves its purpose which helps the Internet complete its goals more easily.

PCAP Table/Chart with Percentages



Wireshark · Protocol Hierarchy Statistics · amp.TCP.reflection.SYNACK.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets
Frame	100.0	8000	100.0	515475	28 M	0
Ethernet	100.0	8000	21.7	112000	6,103 k	0
Internet Protocol Version 4	100.0	7996	31.0	159920	8,714 k	0
User Datagram Protocol	2.0	163	0.3	1304	71 k	0
Simple Network Management Protocol	0.2	14	3.8	19803	1,079 k	14
Real-time Transport Control Protocol	0.0	2	0.0	36	1,961	2
OpenVPN Protocol	0.9	75	3.0	15474	843 k	75
Data	0.9	72	2.2	11274	614 k	72
Transmission Control Protocol	96.0	7679	35.1	180732	9,848 k	7675
SSH Protocol	0.1	4	0.1	528	28 k	4
Internet Control Message Protocol	1.9	153	2.9	14696	800 k	139
Data	0.2	14	1.4	7280	396 k	14
Data	0.0	1	0.3	1432	78 k	1
Address Resolution Protocol	0.1	4	0.0	184	10 k	4

Figure 1.1: PCAP Statistics

1.4 PCAP Analysis

In the PCAP, there is one major threat that can be seen in the packets. That threat is a Distributed Denial of Service (DDoS) Attack and this threat can be seen in almost every packet that was captured, packets 1 through 8000. A DDoS attack occurred because when looking at the IPv4 statistics, found in the toolbar of Wireshark, the most popular IP address used was 10.10.10.10 at 100% of the IP addresses used during the capture. This makes it obvious that this address was the victim of the attack. Furthermore, the victim's IP address was used once every 54.4653 milliseconds, which in simple terms means that it was very quickly spammed the entire time of the network capture. Plus, it can be seen that this was a web-based attack as 97.7% of the ports used in the capture were port 80, which is the default HTTP protocol. On the contrary, it can be considered a DDoS attack rather than a regular Denial of Service (DoS) attack because, in this example, all of the requests came from hundreds of different IP addresses, that could be acting as infected bots or zombies that were most likely originally infected from some kind of malware. These bots or zombies then work together and form a group called a botnet that all create similar requests or queries that flood the victim, in this case, IP address 10.10.10.10. In a regular DoS attack, the requests are from one or a few machines at a time. Both DoS and DDoS attacks fall under the threat of sabotage or vandalism. DDoS attacks are terrible threats made to the Information Security (Info. Sec.) team because they can clog an entire system with junk requests to the academic site which ruins the day-to-day tasks and business. The unfortunate part about DDoS attacks is that they are not that difficult to set up. The saboteur could gather a piece of malware online that can masquerade as another official software to gain control of an individual's computer. Then when the saboteur has a target they want to attack, they send out the request to all of the infected computers, and without any notice to the users of these infected computers, thousands of requests are sent to the target. In the end, this PCAP is a great example of a DDoS attack, however, a DDoS attack can ruin the day for the Information Security team as they will end up spending the entire

day restarting the server, closing the affected ports, and finding a way to stop the botnet from sending continuous requests to their server.

2. Section 2 (CSIT-12): Define Principles to Identify Solution

2.1 Information System Components

In section 1.4 above, it can be seen that a DDoS attack can be devastating to the Information Security team, but the specific Information Technology systems and layers that are affected need to be defined. First, of the seven layers of Information Technology, a DDoS attack is considered to affect the Network layer. DDoS attacks affect the network layer because they take up all of the IT system bandwidth as well as traffic so that normal users can not conduct their business on the affected system. As stated before, DDoS attacks can do this because they use malware to infect machines around the globe. Once the attacker has enough bots or zombies to overwhelm their intended target, they then activate every machine to send requests immensely fast and for as long as possible across the network to the targeted server or servers. Once this occurs, regular everyday traffic has to deal with an onslaught of garbage requests, and therefore can not get what they need from the server. In terms of individual organization assets that would be affected, some examples would be Local Area Network (LAN) components, Intranet components, Internet components, Extranet components, Cloud-based components, and many more depending on what is specifically configured in the academic institution. In academia, this would greatly affect them as this is one of the more critical layers that need to stay operational so that students can learn. Without this layer, students and professors will not be able to access the servers online which means that they will be missing out on crucial teaching, grading, reputation, and overall success. In the end, DDoS attacks disrupt the Network layer the most which can temporarily or permanently damage a business or organization.

2.2 Weighted Table Analysis (Risk Impact)

	Criterion	Impact on Teaching	Impact on Grading	Impact on Reputation		
Number (#)	Criterion Weight Information Asset	0.4	0.4	0.2	Total (1.0)	Importance (0-5; Not Applicable to Critically Important)
1	DDoS on Web Server Host	5	5	3	4.6	Critically Important

Table 2.1: Weighted Table Analysis

Impact on Teaching (40% of Total Impact): 1-5 (1 Low Impact – 5 High Impact)

Impact on Grading (40% of Total Impact): 1-5 (1 Low Impact – 5 High Impact)

Impact on Reputation (20% of Total Impact): 1-5 (1 Low Impact – 5 High Impact)

Equation: (Asset Rating * 0.4) + (Asset Rating * 0.4) + (Asset Rating * 0.2) = Total Impact

Total Impact: 1-5 (1 Not Important – 5 Critically Important)

2.3 Risk Likelihood (Risk Probability)

Rank	Description	Percent of Likelihood
0	Not Applicable	0% within 12 months
1	Rare	10% within 12 months
2	Unlikely	25% within 12 months
3	Moderate	50% within 12 months
4	Likely	75% within 12 months
5	Almost Certain	100% within 12 months

Table 2.2: Risk Likelihood

Likelihood: 1-5 (1 Low Chance – 5 High Chance)

Impact: 1-5 (1 Little to No Impact – 5 High Impact)

Equation: Likelihood x Impact = Rating-Risk Factor

Rating-Risk Factor: 1-25 (1 Rare – 25 Extremely Likely)

3. Section 3 (CSIT-13): Apply Principles to Identify Solution

3.1 Risk-Rating Factor

In sections 2.2 and 2.3, it has been discussed that a DDoS attack on a web server would be an event that is critically important to the Info. Sec. Team. The math that determines this is slightly complicated, but when it is explained, it becomes much easier to understand. To determine the importance of an event such as this, the risk team should first determine how much this attack will have an impact on teaching, grading, and reputation. For the example in the table above, teaching has a 40% impact, grading has a 40% impact, and reputation has a 20% impact. The team then determines on a scale of 0 to 5 with 0 being not applicable and 5 being most important how the event will affect each one of these sections. The team then multiplies this rating by the percent impacts and then adds each subsection up to get a total rating. From the example above it can be seen that the impact on teaching would be $(5 * 0.4) = 2$, the impact on grading would be $(5 * 0.4) = 2$, and the impact on reputation would be $(3 * 0.2) = 0.6$. The team then adds all of these numbers and creates a total rating, in this case, a 4.6 rating out of 5, making the event critically important. The second table is the estimation as to how common this event will occur, as determined by business standards and statistics. In this case, a DDoS attack on a web server has a moderate chance of occurring, which is a 3. After these two numbers have been determined by the team, they then multiply them together to determine the overall risk. In this case, that would be $(4.6 * 3) = 13.8$ out of 25 making it a moderate risk. This overall number is important to the administration sector because it provides an easy way to get the message across to everyone in every department, mainly executives, about how important or unimportant some events or information assets are. If an event or information asset proves to reap a low-risk number, then the academic institution does not need to spend a lot of time and money protecting it and can focus on other tasks. On the contrary, if it scored a high number then the academic institution would need to focus its attention on this event so that it does not happen.

3.2 Risk Treatment/Response

Risk treatment is a necessary process that needs to be done to ensure proper precautions are being taken to manage the risk determined by the Info. Sec. Team. There are four main kinds of risk treatments and they are Risk Mitigation in which the Info. Sec. Team attempts to prevent the vulnerability from occurring with an example being creating a new policy to reduce the risk. Risk Transference in which the Info. Sec. Team shifts the risk to a third-party vendor with an example of this being the use of insurance. Risk Acceptance in which there is nothing other than what the Info. Sec. Team is already doing to stop the risk so they accept the outcome if it occurs. Finally, Risk Termination which is when the Info. Sec. Team removes the threat from the academic environment so that it is not considered a threat anymore with an example being archiving or just deleting old systems and software. In this case, with a risk rating of 13.8, it is suggested that Risk Mitigation is used to deal with the risk. The event impacts a very critical asset to the academic institution, the web server, which means that Risk Termination can not be an option. Risk acceptance should also not be used because it impacts teaching and grading too much. Furthermore, transference should not be used because the problem would be cheaper to solve with mitigation as the insurance would be expensive for the moderate rating. Another action that could be taken that needs to be mentioned is Penetration Testing (Pen. Testing). Pen Testing is when the Info. Sec. Team purposefully tries attack the asset they are trying to protect to see how effective its defense is. In this case, a mock DDoS attack would be valuable as it would prove if more work needs to be done to protect the asset. In the end, out of the four available options, Risk Mitigation would be the most appropriate method of controlling the risk of a DDoS attack as it is the most cost-effective and would be straightforward to implement.

3.3 Risk Residual

As stated before, Risk Mitigation would be the most effective way to deal with a DDoS attack on a web server. However, a more specific Risk Mitigation treatment would be to ensure that the

firewall is well capable of handling a DDoS attack if it comes to it. The Info. Sec. Team could add a component to the firewall that blocks IP addresses for a certain amount of time if they are sending requests to the server too quickly. The team could also increase the web server bandwidth so that it takes more bots or zombies to create a successful DDoS attack as normal traffic could still make its way through if there was more space for it. Finally, the Info. Sec. Team could add a more advanced login system to the web server that requires a Completely Automatic Public Turing Test to Tell Computers and Humans Apart (CAPTCHA). This would make it much more difficult for bots or zombies to attack a web server as they would need to complete this test, which many automated systems are unable to accomplish. Even with all of these specific systems in place to ensure Risk Mitigation, there could still be some risk residue. Risk residue is any leftover risk that occurs even when an updated system is in place, and this will happen with any system no matter how expensive or complex because it is not a matter of if there will be an attack, but rather a matter of when it will occur. In this case, some examples of risk residue would be if the malware used to acquire zombies and bots is so effective and contagious that the amount would overwhelm the bandwidth of the web server, even if it was the largest it could be. Another example would be if improvements were made in bots so that they can read and solve CAPTCHAs, defeating their purpose. To fix either of these risks the team could continue to increase the bandwidth of the server as well as include a more sophisticated log in system such as a two factor authentication that matches up to the customers phone number. In conclusion, no matter the system or the Risk Treatment method, the system will always have risk residue that could affect the academic institution.

References

GeeksforGeeks. (2022, December 6). *Real-time transport control protocol (RTCP)*. GeeksforGeeks.

<https://www.geeksforgeeks.org/real-time-transport-control-protocol-rtcp/>

GeeksforGeeks. (2023a, February 12). *Simple Network Management Protocol (SNMP)*.

GeeksforGeeks. <https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/>

GeeksforGeeks. (2023b, April 20). *What is Transmission Control Protocol (TCP)?*. GeeksforGeeks.

<https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/>

GeeksforGeeks. (2023c, April 27). *Internet control message protocol (ICMP)*. GeeksforGeeks.

<https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/>

GeeksforGeeks. (2023d, May 11). *User datagram protocol (UDP)*. GeeksforGeeks.

<https://www.geeksforgeeks.org/user-datagram-protocol-udp/>

L.F. Haaijer, *DDoS Packet Capture Collection*, (2022). Available from

<https://github.com/StopDDoS/packet-captures>

What is openvpn?. OpenVPN. (2022, April 20). <https://openvpn.net/faq/what-is-openvpn/>

What is SSH? | secure shell (SSH) protocol | cloudflare. (n.d.).

<https://www.cloudflare.com/learning/access-management/what-is-ssh/>

What is wireshark and how to use it: Cybersecurity: CompTia. CompTIA.org. (n.d.).

<https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>

Wireshark · about. Wireshark. (n.d.). <https://www.wireshark.org/about.html>