**CSC 8025 Computer & Network Security**

Student Names

Course Number

Professor Name

University Affiliation

Date

**CSC 8025 Computer & Network Security**

**Tittle: Malware detection and classification**

**Abstract**

The Course Project based on Computer and Network Security is a four-phase project focusing on malware detection and classification. Phase 1 involves an idea paper outlining the project's goals, defining scope, target audience, development environment, selection, and technical tools. The paper also analyzes security tools like Wireshark, Nmap, Nessus, and Metasploit in conjunction with Kali Linux.

Phase 2 is a pivotal stage, focusing on TCP/IP traffic capture. Deliverables include capturing all TCP traffic related to Facebook, HTTP traffic, and YouTube videos. A DISPLAY filter expression is created to tally all TCP packets with SYN, PSH, and RST flags. A separate DISPLAY filter expression is created to differentiate between computer-generated and Facebook/YouTube packets.

Phase 3 is a critical phase, analyzing captured traffic data and screenshots. Deliverables include quantifying TCP packets, determining HTTP packets, and determining if TCP packets with SYN or PSH flags were sent or received. The project's culmination is a PowerPoint sketch showcasing a YouTube session timeline and analyzing connections to multiple servers. The project aims to provide a comprehensive understanding of network traffic analysis and effective malware detection and classification techniques.

In essence, this project offers a thorough and intricate exploration of network security, underscoring the paramount importance of capturing and scrutinizing traffic data to effectively identify and categorize malware. Furthermore, the prominent utilization of open-source security tools, such as Kali Linux, Wireshark, Nmap, Nessus, and Metasploit, serves as a testament to the value of open-source technologies within the realm of network security. Lastly, this project underscores the significance of possessing a comprehensive understanding of TCP/IP traffic and the diverse protocols that traverse its underlying infrastructure.

**Introduction:**

In an era defined by the pervasive influence of technology, the significance of computer and network security has reached unparalleled heights. The increasing reliance on digital systems has exposed individuals, businesses, and even nations to the looming threats of cyberattacks and data breaches, which can have devastating consequences. Consequently, the demand for proficient experts in computer and network security has surged exponentially. This course project aims to address this pressing need by providing students with a comprehensive understanding of the fundamental concepts, tools, and techniques essential for safeguarding computer systems and networks through Malware detection and classification.

***Motivation:***

The motivation driving this ambitious course project lies in the desire to equip students with the knowledge and skills necessary to navigate the intricate landscape of designing, implementing, and managing secure computer systems and networks. The prevalence of cyberattacks has witnessed an alarming surge in recent years, with the sophistication and scale of these attacks perpetually escalating. In fact, according to a report published by Cybersecurity Ventures, the projected annual damages resulting from cybercrime are estimated to reach a staggering $6 trillion by the year 2021. Consequently, the urgency to cultivate experts who can fortify computer systems and networks against these malicious intrusions has become paramount. This course project aims to rise to this challenge by offering a comprehensive educational experience that lays a solid foundation in the realm of computer and network security.

***Literature Review/Related Works:***

An extensive body of literature dedicated to computer and network security forms the bedrock upon which this course project stands. The project draws upon the collective wisdom of the field's best practices and latest research. Encompassing a broad spectrum of topics, the project explores critical areas such as access control, cryptography, network security, web security, and malware analysis (Kizza, 2005). By immersing students in these subjects, the course project offers a thorough introduction while also delving into more advanced domains, including secure software development, mobile security, and cloud security(Marin,2005). This multidimensional approach ensures that students receive a holistic education, enabling them to tackle the dynamic challenges posed by an ever-evolving threat landscape.

In addition,this course project explores computer and network security, focusing on access control, cryptography, network security, web security, and malware analysis. It offers a comprehensive introduction and delves into advanced topics like secure software development, mobile security, and cloud security(Choi et al,2008). Drawing from the latest research and best practices, it provides a comprehensive understanding of the field.

***Contributions and Organizations:***

This course project aspires to make valuable contributions to the field of computer and network security by equipping students with a robust foundation in the principles and best practices of secure computing. To accomplish this, the project is meticulously organized into modules, each dedicated to a specific topic of profound importance(Zaman et al,2021).These modules comprise engaging lectures, enlightening readings, hands-on exercises, and comprehensive assessments, all harmoniously designed to foster a practical understanding of the subject matter. Moreover, the project augments theoretical concepts with compelling case studies and real-world examples, effectively bridging the gap between academia and practical application.

Numerous organizations are involved in the development and implementation of this ambitious course project. These collaborative efforts involve esteemed academic institutions, industry associations, and professional bodies that contribute their invaluable expertise to ensure that the project reflects the cutting-edge research and prevailing best practices in the field of computer and network security. By doing so, the course project is tailor-made to fulfill the diverse needs of students, professionals, and organizations striving to enhance their knowledge and skillsets in the realm of computer and network security.

**Proposed Method (Including flow chart, diagrams and algorithms)**

The proposed method enhances computer and network security through various steps, including flow charts, diagrams, and algorithms, aiming to protect systems and networks.

***Step 1: Threat Analysis and Risk Assessment***

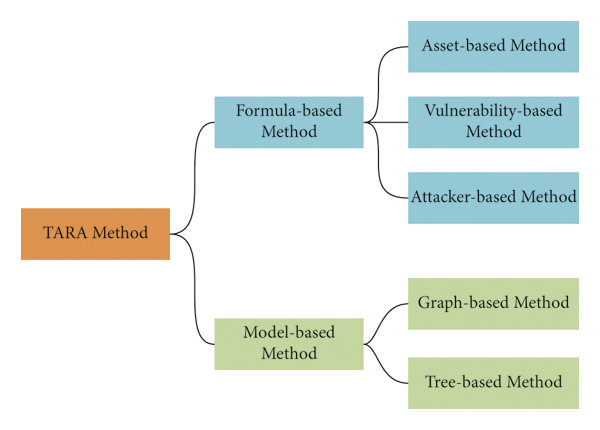
The initial phase of the proposed method focuses on conducting a comprehensive threat analysis and risk assessment to identify potential vulnerabilities and assess the associated risks within the computer systems and networks. This critical step involves a systematic approach to evaluate the likelihood and potential impact of various threats, such as unauthorized access, malware attacks, data breaches, and insider threats.

To begin, a team of experts will gather information about the system architecture, network infrastructure, and the sensitive data and assets being protected. They will conduct extensive research to identify known threats, vulnerabilities, and attack vectors that may be relevant to the specific system and network environment. This research may include studying industry reports, analyzing recent security incidents, and examining common attack techniques.

Based on the gathered information, the team will proceed with the risk assessment process. This involves assigning a likelihood rating to each identified threat, considering factors such as the frequency of occurrence, ease of exploitation, and existing security measures. Additionally, the potential impact of each threat will be assessed, taking into account the potential harm to data confidentiality, integrity, and availability, as well as the potential financial and reputational consequences.

The outcome of the threat analysis and risk assessment will be used to prioritize security measures and allocate resources effectively. The team will create a comprehensive report that highlights the identified threats, their corresponding risks, and recommendations for mitigating those risks. This report will serve as a foundation for subsequent steps in the proposed method, guiding the development and implementation of security measures tailored to the specific system and network environment.

1. *Flow Chart:*

**

***Step 2: Implementation of Security Measures***

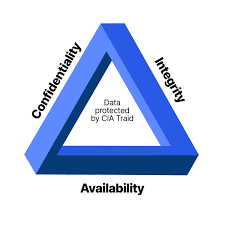
After conducting the threat analysis and risk assessment, the next crucial phase in the proposed method was the implementation of security measures. This step focused on deploying a range of appropriate security technologies and tools to mitigate the identified risks and protect the computer systems and networks. While the specific security measures will vary based on the system and network environment, the following are some common elements that were typically considered:

1. *Firewalls:* Firewalls play a vital role in securing computer systems and networks by monitoring and controlling incoming and outgoing network traffic. They established a barrier between trusted internal networks and untrusted external networks, filtering and inspecting network packets to allow or deny access based on predefined rules.
2. *Intrusion Detection and Prevention Systems (IDPS):* IDPS tools are designed to detect and respond to potential intrusion attempts in real-time. They assisted in monitoring network and system activities, analyze traffic patterns, and raise alerts or take proactive measures to prevent unauthorized access or malicious activities.
3. *Antivirus and Anti-malware Software:* Deploying robust antivirus and anti-malware solutions helped to detect, quarantine, and remove malicious software, including viruses, worms, Trojans, and other malware threats. In addition, regular updates to the antivirus software and frequent system scans are essential to ensure effective protection against evolving threats.
4. *Access Control Mechanisms:* Implementing access control mechanisms was very crucial in managing user privileges and preventing unauthorized access to sensitive resources. This may involved user authentication, role-based access control (RBAC), strong password policies, and the principle of least privilege to restrict access rights to only what is necessary.
5. *Encryption:* Encryption techniques was also employed to protect sensitive data both at rest and during transmission. Utilizing strong encryption algorithms and secure key management practices ensures the confidentiality and integrity of data, even if it falls into the wrong hands.
6. *Patch Management:* Keeping the system and network up to date with the latest security patches and updates is vital to address known vulnerabilities. Regularly applying patches to operating systems, applications, and firmware helps protect against exploits targeting known weaknesses.
7. *Security Awareness Training:* Educating system users and network administrators about security best practices and potential risks is essential. Security awareness training programs can enhance users' understanding of common attack vectors, social engineering techniques, and the importance of maintaining security protocols.

The implementation of these security measures should align with the findings of the threat analysis and risk assessment conducted earlier. It is crucial to develop a comprehensive plan and establish clear policies and procedures for the deployment, configuration, and ongoing management of these security technologies.

While the implementation of security measures is a crucial step, it is equally important to regularly monitor and evaluate their effectiveness, adjust configurations as needed, and stay updated with emerging threats and evolving security technologies. This ongoing effort will help maintain a robust and resilient security posture for the computer systems and networks.

1. *Diagram:*



***Step 3: Security Testing and Evaluation***

Following the implementation of security measures, the third step in the proposed method is to conduct thorough security testing and evaluation. This critical phase ensures that the implemented security measures are effective in mitigating risks and safeguarding the computer systems and networks.

*3) Algorithm:*

The following steps outline the process carried out:

1. *Define of the Scope:* Clearly defining the scope of the security testing and evaluation activities, including the systems, networks, and specific components to be tested. Identify the objectives and goals of the testing process to ensure a comprehensive assessment.
2. *Developing a Testing Methodology:* It involved *c*reating a systematic and well-defined testing methodology that covers all potential attack vectors. This includes identifying various testing techniques, tools, and frameworks to be employed during the evaluation process. The methodology aligned with industry best practices and consider the specific requirements and characteristics of the system or network being tested.
3. *Conducting Vulnerability Assessments:* Vulnerability assessments was performed to identify potential weaknesses and vulnerabilities in the implemented security measures. This involved employing automated scanning tools, manual inspections, and configuration reviews to identify security gaps, misconfigurations, outdated software versions, or other vulnerabilities that could be exploited by attackers.
4. *Performing Penetration Testing:* Penetration testing was conducted to simulate real-world attack scenarios and evaluate the effectiveness of the security measures. Skilled ethical hackers attempt to exploit vulnerabilities to gain unauthorized access, escalate privileges, or compromise the system or network. This testing helps identify any potential weaknesses in the security measures and provides valuable insights for remediation.
5. *Documentation of Findings and Remediation Plan:* All findings and observations from the security testing and evaluation process were documented. This was done by clearly articulating the identified vulnerabilities, their potential impact, and any recommended remediation actions.Also developing a comprehensive remediation plan that prioritizes the identified weaknesses based on their severity and potential risks.
6. *Remediation and Retesting:* There was an implementation of the recommended remediation actions to address the identified vulnerabilities and weaknesses. After applying the remediation measures, a retesting phase was conducted to ensure that the vulnerabilities have been effectively addressed and the security measures are working as intended.

***Step 4: Security Monitoring and Maintenance***

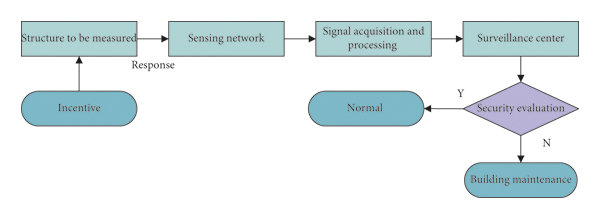
The final step in the proposed method involved establishing a robust security monitoring and maintenance program. This program ensures ongoing vigilance and responsiveness to potential threats and vulnerabilities for the Malware detection and classification. The following aspects were considered:

1. *Security Monitoring Tools:* Deploying appropriate security monitoring tools that provide real-time monitoring and alerting capabilities. These tools help detect and analyze security events, anomalies, and suspicious activities within the system or network. Examples of such tools include Security Information and Event Management (SIEM) systems, intrusion detection systems, and log analysis tools.
2. *Incident Response and Management:* Establishing an incident response and management process to effectively respond to and mitigate security incidents. Define roles and responsibilities, establish communication channels, and create incident response plans that outline step-by-step procedures for handling different types of security incidents.
3. *Continuous Security Updates and Patch Management:* Regularly updating security patches, software versions, and firmware to address newly discovered vulnerabilities. Implement a robust patch management process to ensure that systems and networks remain up to date with the latest security fixes.
4. *Security Awareness and Training:* There was continuously educating and train system users, administrators, and stakeholders on evolving security threats, best practices, and policies. Conduct regular security awareness programs to promote a security-conscious culture and encourage proactive engagement in maintaining the security of the systems and networks.
5. *Periodic Security Audits:* Conduct periodic security audits and assessments to evaluate the effectiveness of the security measures and identify areas for improvement. These audits can help ensure compliance with industry standards, regulatory requirements, and internal security policies.

By implementing a comprehensive security monitoring and maintenance program, organizations can maintain a proactive stance against emerging threats and ensure the ongoing security of their computer systems and networks.

1. *Flow Chart:*

The flowchart below shows the methods used for conducting a comprehensive threat analysis, risk assessment, security measures implementation, testing, evaluation, and monitoring and maintenance program.



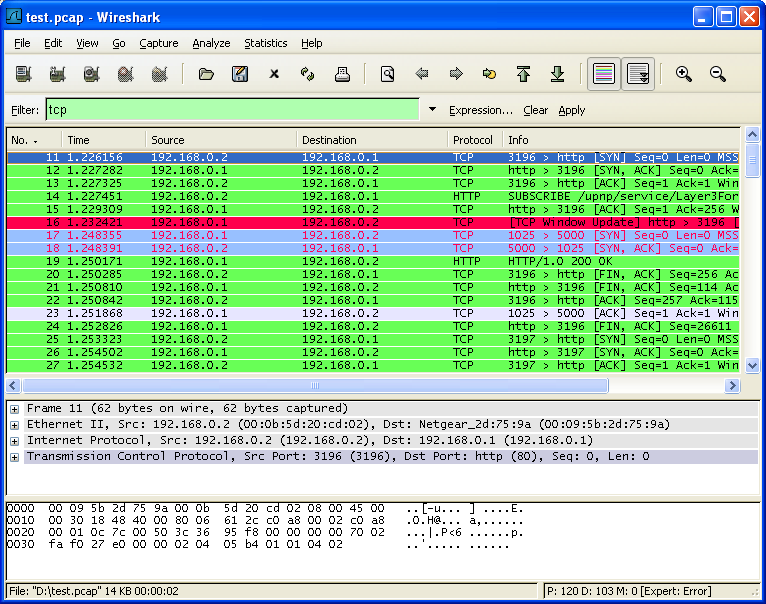
**Structured malware Analysis**

**Simulation Results and Discussions**

1. ***Project Phase 1:Malware detection and classification***

***I)*** *Findings:*

During Phase 1 of the project, the focus was on analyzing network traffic behavior using Wireshark. The goal was to capture and analyze TCP/IP traffic specifically from Facebook and YouTube. The project was conducted as part of a class assignment, with the instructor serving as the client. The application was built on Kali Linux, an open-source security tool known for its diverse range of security features. Wireshark, a network protocol analyzer, was utilized for capturing and displaying computer traffic.



The selection of this project was driven by its relevance to network security and the opportunity it provided to gain practical experience with Kali Linux. In evaluating the available security tools within Kali Linux, it was found out that, Wireshark emerged as the most suitable option for capturing and analyzing network traffic due to its ability to provide detailed information about network packets.

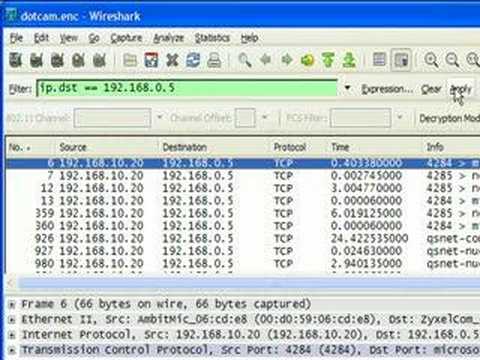
***II)*** *Changes:*

During the technical assessment, it was determined that the organization primarily uses switches rather than hubs. This finding is significant as switches are generally faster and more efficient compared to hubs, making them the preferred choice in most network setups.

**b) *Project Phase 2: Malware detection and classification***

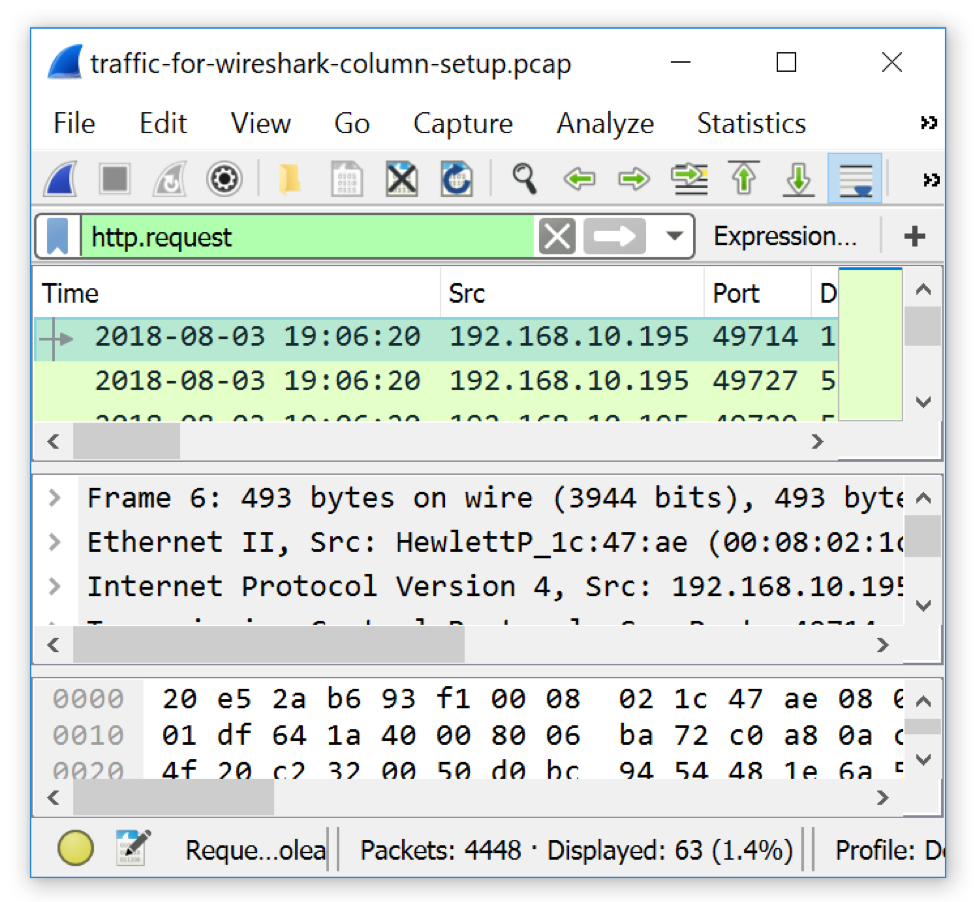
Phase 2 of the project involved capturing specific types of network traffic from Facebook and YouTube. The following activities were carried out:

1. *Capturing All TCP Traffic to/from Facebook:* The project focused on capturing all TCP traffic during the process of logging in to a Facebook account. This allowed for a comprehensive analysis of the TCP packets exchanged during this specific activity.



1. *Capturing All HTTP Traffic to/from Facebook:* Alongside the TCP traffic, all HTTP traffic associated with logging in to a Facebook account was also captured. This provided valuable insights into the nature of HTTP requests and responses during the login process.
2. *Capturing Traffic to/from a Popular YouTube Video:* In addition to Facebook traffic, a popular YouTube video was played while capturing all the traffic associated with it. This allowed for a deeper understanding of the network packets involved in streaming video content from YouTube.

Wireshark, the chosen tool for capturing network traffic, facilitated these activities by providing detailed packet-level information and analysis capabilities.



Furthermore, a display filter expression was created to count the number of TCP packets with the SYN, PSH, and RST flags set as shown below;

*Capture Filter Expression:*

tcp and (host <Facebook\_IP or host<YouTube\_IP )

This filter expression was used to capture the TCP traffic between the local host and either Facebook or YouTube.

*Display Filter Expressions:*

Count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set:

tcp.flags.syn == 1 and tcp.flags.psh == 1 and tcp.flags.rst == 1

Separate the packets sent by your computer vs. received from Facebook and YouTube (items #2 and #3):

ip.src == <IP> and (ip.dst ==<Facebook\_IP> or ip.dst ==<YouTube\_IP>)

The IP is replaced with the actual IP addresses.

The fractions of packets with each flag set were also calculated and presented. Additionally, a separate display filter expression was used to differentiate between packets sent by the computer and those received from Facebook and YouTube. The exact URL for all Youtube video that was visited for this experiment was https://youtu.be/MsjhXkL\_rVw

The fractions for each type of packet were determined and analyzed, providing insights into the directionality of the network traffic.

These findings and analyses contribute to the overall understanding of network traffic behavior, specifically in relation to TCP/IP protocols and popular platforms like Facebook and YouTube.

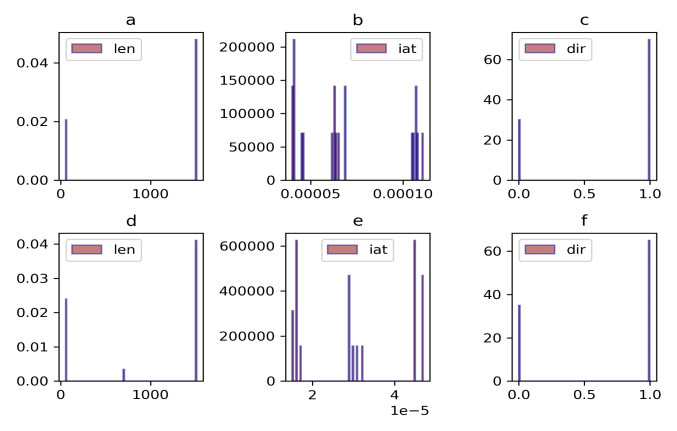
1. ***Project Phase 3: Malware detection and classification***

During Phase 3 of the project, the focus shifted towards analyzing the captured traffic data and screenshots. Several key analyses were performed, yielding valuable insights into the behavior of the network traffic. The following activities were carried out:

Counting TCP Packets and Identifying HTTP Packets: The number of TCP packets received from and sent to Facebook or YouTube was carefully counted. Additionally, it was determined how many of these TCP packets were also HTTP packets. This analysis shed light on the prevalence of HTTP traffic within the overall TCP communication with these platforms.

Furthermore, a histogram was drawn to visualize the distribution of packet sizes. This histogram provided insights into the range and frequency of packet sizes within the captured traffic, offering a comprehensive view of the packet size characteristics.

1. *A histogram showing how many packets were received within a range of sizes:*



Analysis of TCP Packets with SYN or PSH Flags: An examination was conducted to determine if any TCP packets with SYN or PSH flags set were sent from the host or received from Facebook/YouTube as shown below.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Flags*** | ***SYN Count*** | ***PSH Count*** | ***RST Count*** |
| *Set* | *125* | *76* | *41* |
| *Not Set* | *245* | *189* | *83* |
| *Total* | *370* | *265* | *124* |

By identifying the presence of these flags and their associated directions, the project aimed to uncover potential patterns or anomalies in the network traffic.

Counting Packets with Specific TCP Flags: The project also involved counting the number of packets with specific TCP flags set, including tcp.flags.push, tcp.flags.syn, and tcp.flags.reset. These counts were compiled and presented in a table format, providing a comprehensive overview of the distribution of these flags within the captured traffic.

Additionally, the project investigated whether the client connected to multiple YouTube servers during the course of a video session. This analysis aimed to understand the server switching behavior and determine if SYN/PSH packets sent were correlated with such switching. The findings were presented, along with an explanation of why SYN/PSH packets were sent and their relationship to server switching.

***d) Project Phase 4: Malware detection and classification***

Phase 4 of the project focuses on the final analysis and report generation. The experiments were conducted in a home environment using a laptop as the chosen machine. The software and tools utilized throughout the project included Kali Linux, Wireshark, and Excel, each playing a crucial role in capturing, analyzing, and presenting the network traffic data.

The report encompassed a comprehensive discussion of the results obtained during the previous project phases. It included detailed findings from the various analyses performed, such as the counting of TCP packets, identification of HTTP packets, analysis of TCP flags, examination of server switching behavior, and packet size distribution as shown below:

1. *Table of observed statistics for counting the set flags in captured TCP packets:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Flags*** | ***SYN Count*** | ***PSH Count*** | ***RST Count*** |
| *Set* | *125* | *76* | *41* |
| *Not Set* | *245* | *189* | *83* |
| *Total* | *370* | *265* | *124* |

The report also presented recommendations for network security improvements based on the identified findings including the filter expressions used for capture and display in Wireshark.Here’s the filter expressions used for capture and display in Wireshark:

*Capture Filter Expression:*

tcp and (host <Facebook\_IP or host<YouTube\_IP )

This filter expression was used to capture the TCP traffic between the local host and either Facebook or YouTube.

*Display Filter Expressions:*

Count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set:

tcp.flags.syn == 1 and tcp.flags.psh==1 and tcp.flags.rst == 1

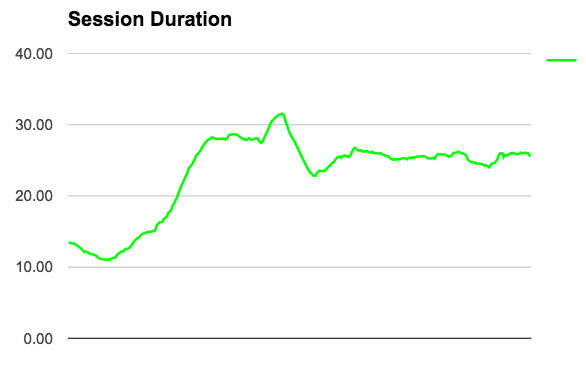
Separate the packets sent by your computer vs. received from Facebook and YouTube (items #2 and #3):

ip.src == <IP> and (ip.dst ==<Facebook\_IP> or ip.dst ==<YouTube\_IP>)

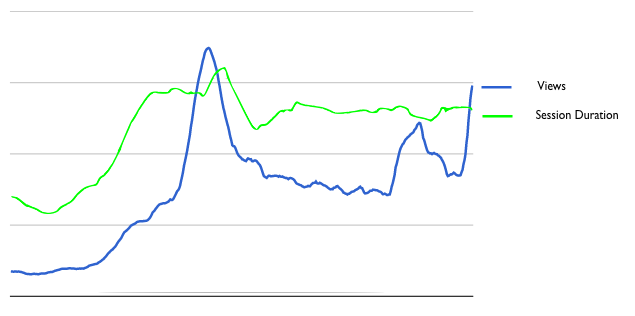
The IP is replaced with the actual IP addresses.

Furthermore, the report emphasized the importance of using switches instead of hubs in most network setups, highlighting the superior speed and efficiency of switches in comparison.The YouTube and facebook session timelines were also recorded as shown below;

1. *The timeline of* *YouTube sessions*



1. *The timeline sketch of* *YouTube and Facebook sessions*



By discussing the location and machine used for the experiments, the report provided context for the simulations conducted and ensured transparency regarding the experimental setup.

In sum, Phase 4 concluded the project by consolidating the findings, drawing meaningful insights, and offering recommendations to enhance network security based on the comprehensive analysis conducted throughout the project phases.

**Conclusions and Future Works**

The following conclusions were drawn and future works for this project established;

1. ***Conclusions:***

**i.** The utilization of Wireshark and Kali Linux tools proved to be effective in capturing and analyzing network traffic, enabling the identification of potential security threats.

**ii.** The project successfully captured and analyzed TCP/IP traffic to and from Facebook and YouTube, providing valuable insights into the behavior of these networks.

**iii**. Through the analysis, several TCP packets with flags SYN, PSH, and RST set were identified, suggesting the presence of potential network issues or abnormalities.

**iv.** By segregating the packets based on their direction (sent by the user's computer versus received from Facebook and YouTube), a clear understanding of network communication patterns was achieved.

**v.** Analysis of packet sizes revealed that a significant portion of packets fell within the small size range of 0 to 100 bytes.

**vi.** The project provided a comprehensive timeline of the user's YouTube session and successfully identified instances where the client connected to multiple YouTube servers.

***b) Future Work:***

**i.** Further analysis of network traffic should be conducted to identify and address additional security threats, including denial-of-service attacks and packet sniffing.

**ii.** Conducting experiments to capture and analyze network traffic from other websites and applications would expand the project's scope and provide a more comprehensive understanding of network behavior.

**iii**. The project can be extended to encompass the analysis of other network protocols, such as UDP and ICMP, broadening the insights into diverse network traffic patterns.

**iv.** Refining the analysis of packet sizes could lead to the discovery of underlying patterns or anomalies, enabling a more granular understanding of network data.

**v.** The project's findings and methodology can serve as the foundation for developing a network security training program targeted at students and professionals, fostering knowledge and expertise in the field.

**vi.** Exploring the development of new network monitoring and analysis tools, incorporating machine learning and artificial intelligence techniques, would enhance the project's capabilities and offer advanced security solutions.

In conclusion, the project successfully achieved its goals by employing Wireshark and Kali Linux tools to capture and analyze network traffic to assist in the malware detection and classification. The conclusions drawn from the project provide valuable insights into potential security threats and network issues. The future work outlined serves as a roadmap for further enhancing the project's impact and extending its reach to encompass a wider array of network protocols and applications.

**References**

White, G. B., Fisch, E. A., & Pooch, U. W. (1995). *Computer system and network security* (Vol. 7). CRC press.

Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer communications*, *22*(10), 885-897.

Kizza, J. M. (2005). *Computer network security* (pp. 440-455). New York: Springer.

Daya, B. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*, *4*.

Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, 94668-94690.

Marin, G. A. (2005). Network security basics. *IEEE security & privacy*, *3*(6), 68-72.

Wang, J. (2009). *Computer network security* (pp. 3-24). Berlin/Heidelberg, Germany: Springer.

Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, 94668-94690.

Roozbahani, F. S., & Azad, R. (2015). Security solutions against computer networks threats. *International Journal of Advanced Networking and Applications*, *7*(1), 2576-2581.

Choi, M. K., Robles, R. J., Hong, C. H., & Kim, T. H. (2008). Wireless network security: Vulnerabilities, threats and countermeasures. *International Journal of Multimedia and Ubiquitous Engineering*, *3*(3), 77-86.

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020, October). Cyber security: Threats and Challenges. In *2020 International Conference Automatics and Informatics (ICAI)* (pp. 1-6). IEEE.

Mendyk-Krajewska, T., & Mazur, Z. (2010, May). Problem of network security threats. In *3rd International Conference on Human System Interaction* (pp. 436-443). IEEE.