Journal of Nano- and Electronic Physics
Vol. **15** No 4, 04016(4pp) (2023)

Журнал нано- та електронної фізики
Том **15** № 4, 04016(4cc) (2023)

Detection of Transmission Control Protocol XMAS Attack Using Pattern Analysis with MONOSEK

Chandrappa S[1], Guru Prasad M S[2], Naveen Kumar H N[3], Praveen Gujjar J[4], M. Anand Kumar[5], Anurag Kukreti[2]

[1] *Dept. of Information Science and Engg., GSSS Institute of Engineering and Technology for Women, Mysuru, Indian*
[2] *Dept. of Computer Science and Eng., Graphic Era (Deemed to be University), Dehradun, India*
[3] *Dept. of Electronics and Communication Eng., Vidyavardhaka College of Engineering, Mysuru, India*
[4] *Faculty of Management Studies, JAIN (Deemed-to-be University), Bengaluru, India*
[5] *Dept. of Computer Application, Graphic Era (Deemed to be University), Dehradun, India*

(Received 17 June 2023; revised manuscript received 14 August 2023; published online 30 August 2023)

Electronic physics play the major role in data transmission between the hosts. The TCP XMAS scan involves determining the TCP traffic pattern in order to find out which ports are open. Based on this information, it can assess whether or not an XMAS attack is being attempted. In network data is transmitted in the form electrical and electronic signals. Using proposed system, one can ascertain both the hosts that are accessible on the network and the services that can be obtained from those sites. MONOSEK is used to perform analysis not only on sessions but also on packets. In this research, the benefits of utilizing MONOSEK rather than Snort and Wireshark are brought to light for comparison and evaluation. The cyber-security tool MONOSEK is capable of identifying a wide variety of network and cyber-attacks. The XMAS attack is identified in order to both stop operating system fingerprinting and examine online services. For the convenience of the user, a graphical user interface (GUI) is developed and used to examine the ports that have been opened on the list of available IP addresses in the network.

Keywords: XMAS, TCP, Electronic physics, MONOSEK, Network, Traffic Analyzer, Cyber Attack.

DOI: 10.21272/jnep.15(4).04016 PACS number: 07.05.Mh

1. INTRODUCTION

The Most networks prioritize security as a top priority. Therefore, it is essential to do network analysis, fault fixing, maintenance, and monitoring of both local and external networks. Analysis of network traffic involves listening to and evaluating the data being transmitted over a network. It provides visibility into network traffic to help diagnose performance issues, track down security vulnerabilities, examine application activity, and map out future capacity requirements. Network analysis, often called protocol analysis, is a tool used by IT administrators to improve network performance and security.

TCP XMAS scan deals with identifying the TCP traffic pattern to determine the ports open, upon which it detects if there is a XMAS attack attempted or not. SPI and XMAS attacks are two techniques to identify vulnerabilities in the router. The XMAS attack sends packets with urgent, push and fin flags set. Different operating systems or router firmware (Linux/Cisco/Windows/Juniper) will respond differently to those options. When the attacker has identified the operating system and the ports open, it can try to exploit known vulnerabilities in this specific system or application.

XMAS attack is a XMAS tree packet also known as a TCP packet with every flag set. Christmas tree packets are always causing for concern from the perspective of network security because they point to the presence of a high likelihood of activities related to network reconnaissance. It makes no sense to set all flags. These days they are used for OS fingerprinting as different operating systems respond differently to various packets.

A network processor that operates on the basis of network packet processing and an analysis system for network sessions, MONOSEK was developed. Over a communication channel, signals and data traffic can be captured and analysed with the assistance of a tool called a protocol analyzer. A channel like this could be anything from a local computer bus to a satellite link; it would provide a means of communication by utilising a protocol that is considered to be standard. Each communication standard has its own specialised data-gathering and analysis programme. MONOSEK can be used as a cyber-security tool capable of detecting various network and cyber-attacks. Using MONOSEK extensible APIs, an application can be created which can scan the open ports using pattern analysis techniques.

XMAS scan has already been implemented on Wireshark but in Wireshark, the notification is not evident and it can only gather information from the network but cannot send information to the network.

XMAS scan was also implemented using Snort. But the installation of snort is complex and it cannot be suitable for all platforms.

The proposed system focuses to design an application that scans the open ports and detects TCP XMAS attack by analyzing the traffic pattern in the network.

By using the network traffic analyzer MONOSEK, notification can be provided to the victim. Using MONOSEK the session and the network pattern can be analyzed.

To identify whether a port is open or closed using TCP XMAS scan. To analyze the network traffic patterns & sessions using MONOSEK. To create a GUI for user to check the ports open on list of available IP address in the network.

TCP traffic pattern is being analyzed to detect

The results were presented at the 3rd International Conference on Innovative Research in Renewable Energy Technologies (IRRET-2023)

whether XMAS attack has been attempted. An alert message is displayed on the server.

MONOSEK is a system for the processing of network packets and the analysis of network sessions that is based on a network processor. Over a communication channel, signals and data traffic can be captured and analysed with the assistance of a tool called a protocol analyzer. Both MONOSEK1 and MONOSEK 2 are able to make effective use of high-end network processing cards such as the Netronomes NFE-3240, which possesses 40 micro engines for parallel packet processing. Softwares that are embedded and used for packet analysis, session analysis, and deep packet inspection. It has the capability of being connected to the network either passively (in parallel) or inline (in series).

MONOSEK captures and analyzes the packets and makes this analyzed information available to the caller through MPE packet structure.MPE packet consists of MPE header and MPE payload. MPE header consists of analyzed and extracted information for the packet and MPE payload consists of raw packet including Ethernet header.

The programmable interface of MONOSEK 2 is written in C/C++. The MONOSEK tool gives programmers access to information about sessions that have been analysed in packets. This is extremely helpful for developers because it enables them to create C programmes that are able to operate on real time packets and utilise the analysis that has already been performed by MONOSEK1.

Surveys of related work are illustrated in this section. Q. M. Algaolahi et.al [1], presented detecting port scanning attacks by using different machine learning algorithms and comparing between them to find the best one. M. u. Nisa et.al [2], proposed an approach to detect the slow port scanning attacks not just over the static time interval but also all the attacks that are made with a gradual increase or decrease in the time duration. Rizwan Iqbal et.al [3], the presented work done on the enhanced security of SDN networks and develop a framework that will protect home user devices from attacks by implementing SDN based firewall. Proposed firewall design and made simulation model to present the results. S. Liao et. al [4], presented a Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments. Authors [5-7], explained the port scanning methods and attack detection techniques. An author's [8-14], illustrates areas where the MONOSEK can be used for data protection.

2. SYSTEM DESIGN

The architecture of the system that can detect a TCP XMAS attack is shown in Figure 1. For the purpose of identifying the XMAS attack, a local sandbox environment is developed. Both the attacker and the victim have their devices connected to a 24-port switch that is mirrored. When a network switch is configured with port mirroring, it will send a copy of the network packets that are observed on one switch port to a network monitoring connection that is established on a different switch port. This is utilised for the purpose of monitoring the traffic on the network as well as locating any intruders. The switch's first port and its 24th port are connected in a mirroring configuration. The mirrored port on the MONOSEK server is connected to the NIC 1 port of the server. The MONOSEK server performs an audit of the traffic pattern on the network and conducts an analysis of the packets. It determines the attacker's Internet Protocol address and displays that information alongside an alert message.

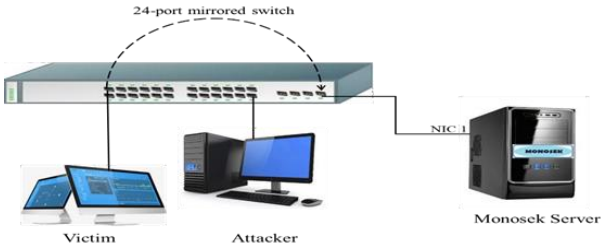

Fig. 1 – System architecture for detection of TCP XMAS attack

The components of proposed system are as follows:

Attacker:

The attacker sends the packet to the victim by setting URG, PSH, and FIN flags in TCP header. If the target port is closed, then there will be no response from the victim system. If the port is open, the attack is done.

MONOSEK Scanner:

MONOSEK scanner scans the packets sent by attacker. It checks whether the packet is TCP or UDP. It drops the packet when the packet is UDP. If the packet is TCP, then it checks

Whether the port is open or closed. If the port is closed then the packet is dropped by scanner. If the scanner finds the port open then it checks the flags (URG, PSH, and FIN) set. Scanner displays a message "XMAS attack attempted" when it finds the UPF flags set.

Victim:

XMAS attack is attempted on the victim which results in Internet dropouts and exploiting of known vulnerabilities. OS fingerprinting is also a major threat of XMAS attack on the victim system. The network traffic of the victim is analyzed by the MONOSEK server.

One type of diagram that can be used to represent an algorithm, workflow, or process is called a flowchart. A flowchart is a diagrammatic representation of an algorithm, which is another definition for the term. Specific criteria for identifying an XMAS attack is illustrated in following sections.

For the attack to succeed, the adversary must have logical access to the target network. Because XMAS scanning relies on the use of raw sockets, it is incompatible with certain versions of the Windows operating system (Windows XP SP 2, for example). Any manipulation of a raw socket on Unix or Linux needs to be done with root privileges.

This attack can be carried out using a network mapper or scanner, as well as raw socket programming in a scripting language. Alternatively, it can be carried out using a scripting language. Tools that are used for packet injection can also be helpful for this purpose. It is possible that sniffing the network will be required in order to view the response, but this will depend on the method that was used.

The Figure 2 depicts the Flowchart of detection of TCP XMAS attack. The scanner will check whether the protocol is TCP, If TCP then port open/close is checked. If the attacker sends UDP packets then the packet is dropped. If the port is open, then again it checks the flags set. If the

Urgent, Push and Finflags are set then XMAS attack is detected and an alert message is displayed in the server. Packets are dropped for closed ports.

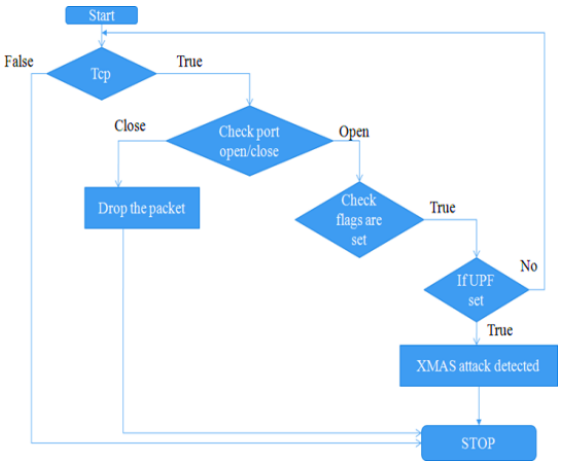

Fig. 2 – Flowchart of TCP XMAS attack

In Unified Modeling Language (UML), a sequence diagram is a type of interaction diagram that demonstrates how processes interact with one another and in what order. Sequence diagrams are used to document the flow of data. It is a component of a Message Sequence Chart that has been constructed. There are a few alternative names for sequence diagrams, including event diagrams, event scenarios, and timings diagrams. It presents a chronological order of the object interactions that are shown.

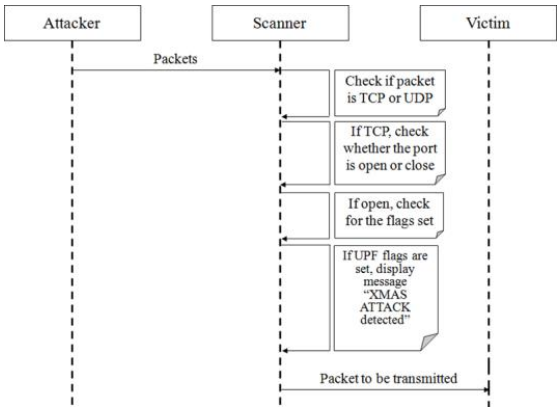

Fig. 3 – Sequence diagram of TCP XMAS scan attack

Attacker, Scanner, and Victim. Attacker sends the packets to the Victim. The scanner scans the packets sent by the attacker and checks the whether the packet is TCP or UDP. If the packet is TCP, then it checks whether the port is open or closed. If the port is open, then it checks for the flags (URG, PSH, and FIN) are set. If the UPF flags are set then the message "XMAS attack detected" is displayed. If the flags are not set, then the packet is transmitted to the victim.

3. RESULTS

XMAS attack occurs only when all the 3 flags such as Urgent, Push, Finish are set. If any one of the flag is not set XMAS attack will not be detected. As only Urgent and Fin flags are set alert message is not displayed. So the victim system will not be prone to attack.

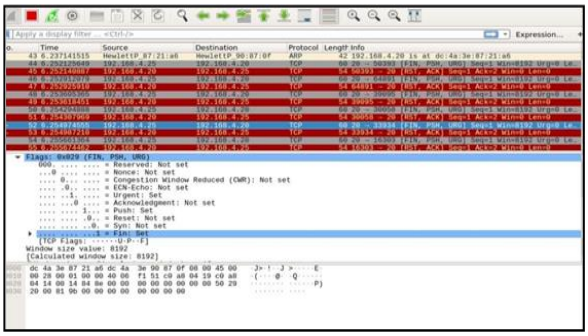

Fig. 4 – Detection of XMAS attack in Wireshark

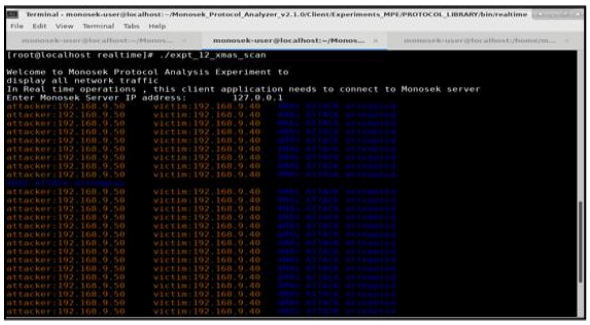

Fig. 5 – Detection of XMAS attack in terminal of MONOSEK server

The Figure 4 depicts Detection of XMAS attack in Wireshark tool. Wireshark is an open source packet analyzer. As a proof of concept, Detection of XMAS attack in wireshark has been implemented in the project. Red coloured line shows that the RST and ACK flags are set. If RST flags are set, the port is open otherwise it is a closed port. The grey coloured lines show that Fin, Push and Urgent flags are set. When these 3 flags are set, it looks like a lit up Christmas tree and hence this attack gets its name as XMAS attack.

The Figure 5 displays detection of XMAS attack in the terminal of MONOSEK server. When the client application connects to the MONOSEK server, the server displays the attacker IP address and Victim IP address. An alert message "XMAS attack attempted" is displayed on the terminal. Methodologies used to compare MONOSEK to other network traffic analysis tools are Platforms Supported, Categories and Network Critical.

4. CONCLUSION AND FUTURE WORK

Network security is one of the major issues in today's cyber era. Detection and prevention of various kinds of cyber-attacks is the most challenging task in Network security. Our project deals with detection of TCP XMAS attack which is a kind of DOS attack. XMAS attack is a XMAS Tree Packet which is also known as a TCP packet with Urgent, Push and Finish flags set.

TCP XMAS scan deals with identifying the TCP traffic pattern to determine the ports open, upon which it detects if XMAS attack has been attempted or not. It's possible that attackers will try to conceal their port scanning operation from naive detection methods by shuffling the or-

der in which destination IP and port probes are performed. Christmas tree packets are always causing for concern from the perspective of network security because they point to the presence of a high likelihood of activities related to network reconnaissance. Using MONOSEK extensible API's, an application has been developed to scan the open ports and analyze the traffic pattern in order to detect XMAS attack.

REFERENCES

1. Q.M. Algaolahi, A.A. Hasan, A. Sallam, A.M. Sharaf, A.A. Abdu, A.A. Alqadi, *2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)* (Sana'a, Yemen: 2021).
2. M.U. Nisa, K. Kifayat, *2020 International Conference on Cyber Warfare and Security (ICCWS)* (Islamabad, Pakistan: 2020).
3. Rizwan Iqbal, et al., *Journal of Xi'an Shiyou University, Natural Science Edition* **18** No 9 (2022).
4. S.M. Liao, C. Zhou, Y. Zhao, Z. Zhang, C. Zhang, Y. Gao, G. Zhong, *2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 64 (2020).
5. Urupoj Kanlayasiri, Surasak Sanguanpong, Wipa Jaratmanachot, *A Rule-based Approach for Port Scanning Detection* (2017).
6. Elias Bou-Harb, Mourad Debbabi, Chadi Assi, *Cyber Scanning: A Comprehensive Survey* (2018).
7. Weijun Zhu, *On the model-checking-based IDS* (2018).
8. S. Chandrappa, L. Dharmanna, Anami Basavaraj, *International Journal of Image, Graphics and Signal Processing (IJIGSP)* **14** No 1, 26 (2022).
9. L. Dharmanna, S. Chandrappa, T.C. Manjunath, G. Pavithra, *International Journal of Modern Education and Computer Science (IJMECS)* **8** No 1, 55 (2016).
10. M.S. Guru Prasad, H.N. Naveen Kumar, K. Raju, et al., *SN Comput. Sci.* **4**, 192 (2023).
11. S. Chandrappa, M.S. Guruprasad, H.N.N. Kumar, et al., *SN Comput. Sci.* **4**, 154 (2023).
12. S. Chandrappa, L. Dharmanna, U.V. Shyama Srivatsa Bhatta, M. Sudeeksha Chiploonkar, M.N. Suraksha, S. Thrupthi, *International Journal of Modern Education and Computer Science (IJMECS)* **9** No 4, 50 (2017).
13. S. Chandrappa, Lamani Dharmanna, Vital Poojary Shubhada, N.U. Meghana, *International Journal of Education and Management Engineering (IJEME)* **7** No 5, 45 (2017).
14. S. Chandrappa, L. Dharmanna, K.I.R. Neetha, *2019 1st International Conference on Advances in Information Technology (ICAIT)*, 551 (Chikmagalur, India: 2019).

Виявлення XMAS-кібератаки на протокол керування передачею сигналів: використання аналізу шаблонів з MONOSEK

Chandrappa S[1], Guru Prasad M S[2], Naveen Kumar H N[3], Praveen Gujjar J[4], M. Anand Kumar[5], Anurag Kukreti[2]

[1] *Dept. of Information Science and Engg., GSSS Institute of Engineering and Technology for Women, Mysuru, India*
[2] *Dept. of Computer Science and Eng., Graphic Era (Deemed to be University), Dehradun, India*
[3] *Dept. of Electronics and Communication Eng., Vidyavardhaka College of Engineering, Mysuru, India*
[4] *Faculty of Management Studies, JAIN (Deemed-to-be University), Bengaluru, India*
[5] *Dept. of Computer Application, Graphic Era (Deemed to be University), Dehradun, India*

Електронна фізика відіграє основну роль у передачі даних між хостами.Сканування TCP XMAS передбачає визначення шаблону трафіку TCP для можливості визначити, які порти відкриті. На основі цієї інформації можна оцінити, чи була спроба XMAS-кібератаки. У мережі дані передаються у вигляді електричних і електронних сигналів. Використовуючи запропоновану систему, можна розпізнати як хости, доступні в мережі, так і послуги, які можна отримати з цих сайтів. MONOSEK використовується для аналізу сеансів і пакетів. У цьому дослідженні переваги використання MONOSEK, а не Snort і Wireshark представлені для порівняння та оцінки. Інструмент кібербезпеки MONOSEK здатний ідентифікувати широкий спектр мережевих і кібератак. Атака XMAS ідентифікується, щоб зупинити відбитки пальців операційної системи та перевірити онлайн-сервіси. Для зручності користувача розроблено графічний інтерфейс користувача (GUI), який використовується для перевірки портів, які були відкриті в списку доступних IP-адрес у мережі.

Ключові слова: XMAS, TCP, Електронна фізика, MONOSEK, Мережа, Аналіз трафіка, Кібератака.