WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

Types and Methods of Detecting the Penetration of Malicious Cargoes

Hasanain M. J. Alfouadi[1], Marwah Nafea Saeea[2] Ali Fahem Neamah[3*] and Ihtiram Raza Khan[4,]

[1]University of Al-Qadisiyah, Computer Center Iraq, Diwaniyah, 58002

[2]University of Wasit, College of Physical Education and Sports Sciences Iraq, Wasit, 52001

[3]University of Wasit, computer science and IT faculty Iraq, Wasit, 52001

[4]Department of Computer Science & Engineering,School of Engineering Sciences & TechnologyJamia Hamdard Delhi,India

*Corresponding Author: Ali Fahem Neamah

DOI: https://doi.org/10.52866/ijcsm.0000.00.00.000

Received: August 2023; Accepted: November 2023; Available online: December2023

ABSTRACT: Intrusion detection systems are management programs that detect possible attacks on networks and computers, and usually do so by identifying information in the header of packages. But the cargo of packages containing the main information can help detect abnormal traffic. This article examines the types of malicious cargo and the different types of penetration detection systems and the methods offered to detect based on cargo. At the end of this article, we will also introduce the Metasploit Framework, which is a framework used by testers and even attackers and contains a variety of ready-made cargoes for different systems.

Keywords: cargo, intrusion detection system, anomaly detection

1. INTRODUCTION

When data is sent over the internet, each transfer package includes both header information and ash event information. The information of the incident of the correction of the cargo is unknown. Header contains the information and specifications of the package. As an example, in a package in the TCP protocol the header can contain information such as the origin and destination addresses, window sizes, flags, and so on... The shipment also includes the main information of the package and can be checked by the intended user, e.g., Figure 2. of the structure of the T-protocol-based packages Three It shows the structure of the header and its cargo. The cargo of internet packages can sometimes contain malicious information, and this is if the protective layers of computer systems and networks do not usually check the contents of the cargo due to their high volume. Malicious shipments with several different hacks may be used by the attacker [1]. Good protection of the system of current computers can be achieved using layered defense. The main components of this defense are four acetate processes: prevention, detection, reaction, and recovery [1]. The intrusion detection system is a part of the ash detection layer, and is defined as a type of management system for computers and networks that detects possible security incidents by collecting and analyzing incoming information. Penetration detection systems have different types based on what part of the information they use or what method they use to detect. [2]

2. DESTRUCTIVE SHIPMENTS

It was said earlier that the packets in the network consist of two parts: metadata and payload. And in some cases, the payload of network packets may contain malicious information. A malicious payload is a component that can cause damage to the victim's system. Malicious payloads can sometimes remain latently inactive for a while, until they are activated by a specific event. Viruses, worms, malware and emails can also contain malicious payloads. Malicious payloads

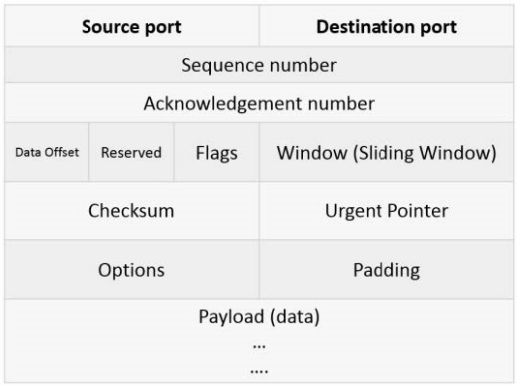

FIGURE 1. **(header and payload structure in a TCP packet)**

can cause problems for the victim's system in different ways [3]:

2.1 INFORMATION THEFT

The usual header of a malicious payload is usually to steal sensitive information such as login information or bank information from the victim's system.

2.2 MONITORING THE VICTIM'S ACTIVITIES

A malicious payload may monitor a system after execution. This can be done for espionage, internet threats, etc.

2.3 SHOW ADS

Some malicious payloads do not harm the victim's system after being transferred, but they can contain displays of unwanted advertisements that can be annoying to the user of the system.

2.4 DELETE OR EDIT INFORMATION AND FILES

It is one of the most heinous acts that some malicious cargoes do. Malicious cargo can delete or edit system files, files that may be part of the essential files of the operating system and in case of problems with them, they may prevent the operation of the operating system.

2.5 DOWNLOAD MORE MALICIOUS FILES

In some cases, the attacker is not able to enter much information in the Internet packet payload. But it can put a light payload in it to load the main malicious information from a specific address on the victim's system after running on the victim's system.

2.6 RUNNING PROCESSES IN THE BACKGROUND

Sometimes, malicious payloads can only run in the background and perform time-consuming tasks such as electronic currency mining.

3. TYPES OF INTRUSION DETECTION BASED ON SYSTEM LOCATION IN THE NETWORK

Based on the fact that the location of the intrusion detection system in the network can be of two types based on the host or based on the network [4].

3.1 HOST-BASED INTRUSION DETECTION

These types of systems are installed on every machine to be protected and use log files to search between signatures. These types of intrusion detection systems are software-based, because they must be installed on the operating system of

the machine they protect [5].

3.2 NETWORK BASED INTRUSION DETECTION

These types of systems monitor the information available in the network as well as the input information of the machines in the network. These types of systems check every packet that enters the network to detect attacks [5].

3.3 HYBRID INTRUSION DETECTION

Hybrid intrusion detection uses methods used in both host-based and network-based methods to have a more secure solution for individual systems as well as the entire network [4].

4. TYPES OF INTRUSION DETECTION BASED ON THE METHOD

However, intrusion detection systems based on the detection method can be of two types: signature-based and anomaly-based, each of which has advantages and disadvantages [5].

4.1 INTRUSION DETECTION BASED ON SIGNATURE

Systems based on signatures do not work with the use of previously known signatures. Their method is that databases of characteristics and signatures of abnormal traffic and malicious information have been placed for them, the incoming traffic to these systems is compared using their database, and in case of similarity, it is identified as abnormal traffic. - Be These types of systems are not suitable for detecting serious attacks that have different signatures [6].

4.2 INTRUSION DETECTION BASED ON ANOMALY

These types of systems detect abnormal behavior in the network by using the traffic behaviors of the network entities that are defined for them. This type of intrusion detection systems considers all traffic as normal traffic and if the current traffic is abnormal based on the considered model, they warn the system administrator. Intrusion detection methods based on anomalies are suitable for new attacks, but sometimes some normal traffic can be detected as attacks [6] and [5].

5. DETECTION METHODS BASED ON CARGO

In addition to the detection of intrusion based on metadata, Bracha's cargo methods are one of the anomaly-based methods that were introduced to increase the accuracy of malicious traffic detection. Although these methods have a low speed in general and reduce the operational capacity of the network, but the number of false alarms in this type of system is less and due to the fact that their accuracy is high, they have been given a lot of attention [5].

5.1 ORGANIZATIONAL SELF-MAPPING METHOD

Labib and Vemuri proposed a method to use self-organizing mapping, which is an artificial neural network-based method for mapping input data to data with a lower number of dimensions (usually two dimensions). They used this method to classify input data from a network. Ethernet used a classification system that determines the class of network traffic into normal and aggressive mode [7].

5.2 N. GRAHAM PEEL METHOD

One of the intrusion detection methods based on the payload is PILE, which was presented by Wang and Estolfo [8]. The main purpose of this system is to extract a series of features from network packets. The working method of this intrusion detection system is to categorize the shipments by using a series of characteristics in the network packets such as the port number, length of the shipment, incoming or outgoing traffic, and using 1 gram (these grams are traces of N bytes of information) are from the payload, here it is equal to 1 (of the contents of the payload, they tried to create a machine learning model from it. For example, Figure 2-2 shows some grams of the payloads. They tried to build a model for create normal traffic in the form of unsupervised learning, and then the incoming traffic is compared with the created model, and the distance to Mahan polis is calculated, and if it exceeds the limits, this traffic is identified as abnormal traffic. They evaluate this method from the set They used the 1999 DARPA IDS data and reached a diagnostic accuracy of nearly 100% with 0.1% of false positive diagnoses [8].

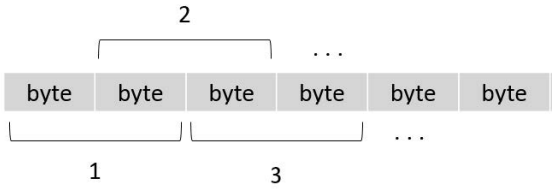

FIGURE 2. (is an example of 2 grams taken from the contents of a shipment)

5.3 POSEIDON INTRUSION DETECTION SYSTEM

This method is a combination of the previous two systems, which consists of two steps. The first step is self-organization mapping, and the second step is a modified method of the Pile method to use the result of self-organization mapping instead of directly using the cargo. In this system, they used self-organization mapping so that there is more mature information for use in the pile stage [9].

5.4 IMPROVEMENT OF N GRAM PCNAD METHOD

Another method was presented by Torat and his colleagues, which is based on the improvement of the Pile system. Pile system used almost all the information in the cargo for modeling. This feature reduces the detection speed, which will not be suitable for high-bandwidth networks, because in some ports such as 80 and 21, the volume of cargo can be very large. In this improved method, which is called PCNAD, parts of the cargo were used for modeling to increase the speed. In PCNAD, they used the method of dividing cargo based on content, which divides cargo into smaller parts based on their content.to reach an accuracy close to Pyle's method. The accuracy of their proposed method using the same data set used for the pile was 97.06% [10].

5.5 ANAGRAM METHOD

Another method is similar to the one used in PALE by the same researchers. with the difference that in PAYL, which is a gram method, the frequency of the bit value is used. If in this system the value of n is greater than 1, it provides more information about the cargo to the modeling and machine learning part. These engrams are given to the next part in this method, which is called the Bloom filter. The reason for using this filter is because, unlike the pile method that used Egrams from the payload, using Ngrams here produces more volume and using this filter reduces the memory overhead. Figure 3 shows the structure of using the Bloom filter in this method [11].

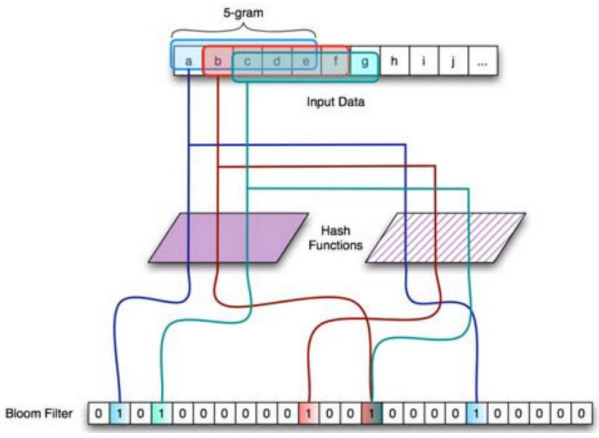

FIGURE 3. (How to use 5 grams and use the Bellum filter in the anagram method)

5.6 RAPID REAL-TIME MULTILEVEL DETECTION SYSTEM

Another method for intrusion detection based on payload was also introduced by Jamdagni et al. to be suitable for real-time intrusion detection with high speed. The system consists of several parts of data preparation, text N.gram classification, three-correct feature selection, profile generation, and traffic classification. This method also used Mahalanobis distance to classify traffic into two classes, normal and attack. They also reached an accuracy of almost 99 percent using the DARPA 1999 dataset [12].

6. INTEGRATED INTRUSION DETECTION SYSTEMS

Intrusion detection methods based on the cargo, despite having high accuracy, in general, due to checking the contents of the cargo, which can be bulky in most cases, they have a low speed and are mostly used as host-based intrusion detection and are used less in the real environment based on the network. But a combined and integrated method of these two methods can make use of the strengths of both. A hybrid method is also presented by Merodek to use the combination of signature-based and anomaly-based intrusion detection systems. In this idea, he has also benefited from the existence of honeypots. The idea is that the traffic is first passed through the detection system based on the signature, then it is given to the system based on the anomaly, because the systems based on the anomaly perform better in identifying new malicious traffic that does not have a signature, and if it is detected as traffic Destroy their information to be stored. to be used for subsequent identifications. This information can also be provided through hanipatas, which are another system and defense layer for networks and act like a trap against the attacker. The information obtained from these parts can be used for decision making [13].

7. META EXPLOIT FRAMEWORK

It is a framework that is used by testers to test various computer systems. This framework is also used by attackers for their purposes. Meta exploit has ready-made codes to execute various attacks on different operating systems such as Windows, Linux, etc., as well as ready-made malicious payloads suitable for said operating systems, which can be used along with attacks to execute on the victim's system. In the following, how to launch this framework and introduce an example of attack code for Windows 2003 version and a corresponding payload [14].

7.1 INSTALLING THE META EXPLOIT FRAMEWORK

To install and run this framework, we use a virtual machine on which Ubuntu Linux operating system is installed. We download the Metasploit installation file suitable for this operating system from the site of this framework. The downloaded file has the extension run. Is. To install this file, go to the path where the said file is located and install it with the commands shown in Figure 4.

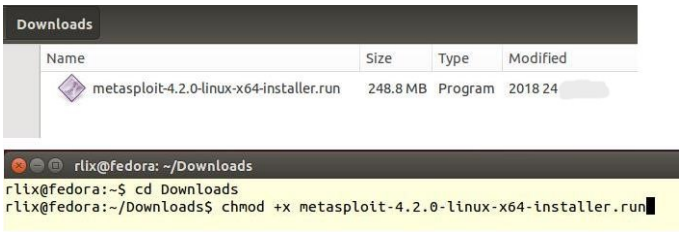

FIGURE 4. ((Meta exploit modules folder)(Meta exploit modules folder)the downloaded file of the Meta exploit framework and how)

7.2 PERFORMANCE

After installing Meta exploit, you can run it through the terminal screen. If we go to the installation location of this framework (Figure 5), there are several other folders in the folder containing the modules. The folders that are located in each of the different modules of this framework. For example, the exploits folder contains modules for executing the attack. The existing folders are from top to bottom, it contains miscellaneous helper modules, modules for encoding information to escape intrusion detection systems, attack modules, naps modules that randomize attack payloads to make them harder to detect, the payloads folder contains various payloads for various operating systems. and modules to execute

after successfully attacking the victim's system. Inside the payloads folder (Figure 6) there are three other folders that show the types of payloads in the meta exploit.

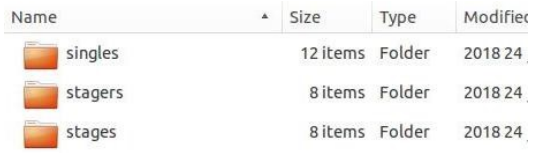

FIGURE 5. (Meta exploit modules folder)

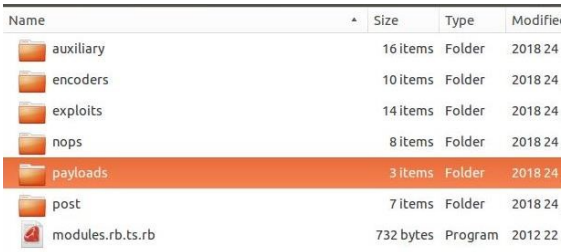

FIGURE 6. (Meta exploit cargo corner)

There are three types of payloads in Meta exploit, single stager and stage. Singles are payloads that can be executed alone on the victim system. These types of payloads are usually used for simple tasks, such as adding a new user to the victim's system; so that the attacker can log into the system later with this username. Stager payloads are small and reliable payloads that, after being executed on the victim's system, create a network connection to the attacker's system, so that the attacker can use this connection for their next actions. And finally, stage shipments are also shipments that may have a larger volume than other shipments and it is not possible to be transferred to the victim's system along with the attack code. These cargoes are downloaded by stager cargoes on the desired system [14].

By executing the MSF console command in the terminal, Meta exploit is executed. Then you can use the search windows command by executing a command to search for suitable attack modules for Windows. For example, Figure 7 is a list of attack modules for Windows.

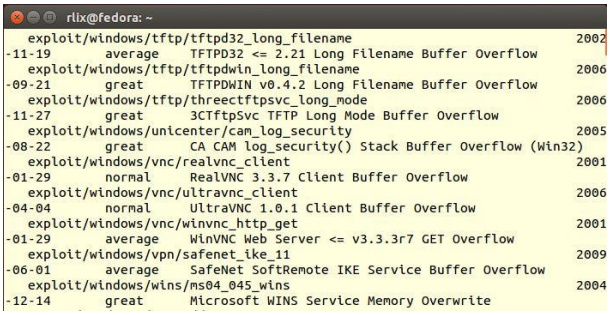

FIGURE 7. (list of attack modules for Windows operating system)

These modules can be used by using the use command. For example, the Net API 58 module is a module that can be suitable for vulnerable versions of Windows 2003. After opening this module with the use command as shown in Figure8, you can see the payloads corresponding to this attack module with the show payloads command.

The add user payload in the Windows folder is the payload that defines a new user after being transferred to the victim's system by the attack module. As shown in Figure 9, this payload can be connected to the current attack module with the set payload command.

Meta exploit modules each have their own settings. You can view and manipulate their settings with the show options command. Figure 10 shows these settings for the attack module and said payload. For example, the settings related to the username and password of the user that the payload of adding a new user is supposed to use are specified.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                          Disclosure Date  Rank
   ----                                          ---------------  ----
   generic/custom                                                 normal
   generic/debug_trap                                             normal
   generic/shell_bind_tcp                                         normal
   generic/shell_reverse_tcp                                      normal
   generic/tight_loop                                             normal
   windows/adduser                                                normal
   windows/dllinject/bind_ipv6_tcp                                normal
   windows/dllinject/bind_nonx_tcp                                normal
```

FIGURE 8. **(Loads corresponding to the Net API module)**

```
msf  exploit(ms08_067_netapi) > set payload windows/adduser
payload => windows/adduser
msf  exploit(ms08_067_netapi) >
```

FIGURE 9. **(Connecting the payload of adding a user in Windows to the attack module)**

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/adduser):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process,
   PASS      metasploit       yes       The password for this user
   USER      metasploit       yes       The username to create
```

FIGURE 10. **(settings related to attack module and cargo)**

8. CONCLUSION

In this article, an overview of intrusion detection methods based on cargo was discussed. Intrusion detection methods, which due to their low speed in detecting abnormal traffic, are usually used less in real and commercial environments, or even, if possible, they are used as intrusion detection on a host, but due to the greater accuracy of these types of methods and their promising future, they have been discussed a lot theoretically, so that these methods are as efficient and fast as signature-based methods.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] H. Alaidaros, M. Mahmuddin, and A. Al-Mazari *An Overview of Flow-Based and Packet-Based Intrusion Detection Performance in High Speed Networks*.
[2] B. Beigh and M. A. Peer *Intrusion Detection and Prevention System : Classification and Quick Review*, vol. 2, pp. 661–675, 2012.
[3] Cloudflare *What Is A Malicious Payload?*, pp. 7–7, 2019.
[4] C. Figueroa *Intrusion Detection Systems Overview*, 2016.
[5] I. M. Iqbal and R. A. Calix, “Analysis of a Payload-based Network Intrusion Detection System using Pattern Recognition Processors,” *Int. Conf. Collab. Technol. Syst*, pp. 398–403, 2016.
[6] M. Mahoney and P. K. Chan *Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks*, pp. 376–385, 2002.
[7] K. Labib and R. Vemuri *NSOM: A real-time network-based intrusion detection system using self-organizing maps*, pp. 1–6, 2002.
[8] K. Wang and S. J. Stolfo, “Anomalous Payload-based Network Intrusion Detection,” *Comput. Sci. Dep. Columbia Univ*, 2005.

[9] D. Bolzoni, S. Etalle, P. Hartel, and E. Zambon, "POSEIDON: A 2-tier anomaly-based network intrusion detection system," *Proc. - Fourth IEEE Int*, pp. 144–156, 2006.
[10] S. Thorat, K. Kishore, A. K. Khandelwal, and B. Bruhadeshwar, "Payload Content based Network Anomaly Detection," *Cent. Secur. Theory Algorithmic Res*, 2008.
[11] K. Wang, J. J. Parekh, and S. J. Stolfo, "Anagram : A Content Anomaly Detector Resistant to," *Comput. Sci. Dep*, 2007.
[12] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier Real-time Payload-based Intrusion Detection System," *Comput. Networks*, vol. 57, no. 3, pp. 811–824, 2013.
[13] S. Mrdovic, "Data Mining for Anomalous Network Payload Detection," *Univ. Sarajev. Fac. Electr. Eng*, 2018.
[14] 2019.