ATTACKERS INTENTION RECOGNITION
BASED ON REAL—TIME NETWORK DATA

T. DHARSHINI, G. MANISHA, A.R. ANITHA
Bachelors of Engineering, Bachelors of Engineering, Bachelors of Engineering
Computer Science and Engineering,
Thiagarajar College of Engineering, Madurai, India.

ABSTRACT: A system could be misused in various ways. Data in the system could be accessed in different forms. Proper measures are to be taken to secure our system data from illegitimate users. The main objective is to detect an attack and take necessary steps to stop the hacker from hacking the data. Prediction is made in the early stage so that a quick action can be taken. There are legitimate users and hackers who try to access data, only the hacker is found and he is stopped. Any kind of unusual activity is detected in the system and immediately the user is notified. The java code in the system is used to detect unusual activities and with the help of packet capturing tool, captured data is manipulated. All these activities happen automatically in the system when a system boots, so the user need not be aware of the procedures of how the system is periodically checked.

Index Terms – Intention prediction, threshold, hackers, intimate, unusual activities.

1. INTRODUCTION:

The paper is about identifying the intention of the hackers and prevents them from doing such activities. We have different types of attacks like spoofing, data modification, man-in-the-middle, etc., which helps the hackers to steal the data. As the technology develops day by day, the techniques of stealing the data also develops. Every person who steals the data must have a reason for doing such activities. So we thought it is very important to find the intention of the hackers, so that when someone else who try to do the same thing, it would be easy for us to identify it earlier and stop such activities. Only when we know the intention of the hacker, we can divert them by providing certain data that are similar but not the exact one which they are searching for.

So, to find the intention of the hacker, we capture all the packets that request for the service of the server in a constant time interval using packet capturing tool. The captured packets are stored as file and we process this. From the file we collect all the sources, destinations and the protocol types along with the unique count of each. And then we find the sources which have requested the same destination for the same type of request. With this data we find the intention of the hackers. When we keep track of the path in which the hacker attacks the data and the types of files that they access, gives us the intention of them.

Packet capturing tool will be started at every boot process and it keeps capturing the packets continuously in a constant time interval. When there is any suspicious activity like a single source repeatedly requests the same destination for a same type of files, then we will try to divert the particular person by providing a similar data that they request and check if the person is a hacker or a genuine user. If the person is a genuine user we will allow the user to continue with the work that they do. If we predict the person as a hacker, then we will keep providing them only the similar data, but not the exact one that they are requesting for.

2. DIFFERENT TYPE OF ATTACKS:-

2.1. Remote Accessing:-

Remote access is a method that is being used to access a personal system from another system. By using this method we can see all the data that is allowed for access. All these activities will be stored in the system logs that keep track of all the activities that happen in a particular system. There are different types of logs located in a system.
2.1.1. Auth logs:

In this log all the authentication activities will be stored. Whenever the system asks for authentication the access permission will be allowed only if the correct password is being provided. This log stores how many times the user has provided a password, whether the password was right or wrong, at what time the person has tried to log in. If we try to access a system from other system, then this log will be stored in the auth logs along with the system details like source address, system name, etc.

2.1.2. Sys Logs:

The actions that are performed in the system will be stored in the system log. If an application is opened or if any action is performed in the system, it will be stored in the system logs. If anyone access our system and do some suspicious activities, it will be stored in the sys logs. By analyzing this logs we can know the source address of the hacker.
2.2. Flooding:

Flooding is one of the important attacking techniques that are followed by the hackers. This technique can be implemented in two different ways which is being followed by most of the attackers.

2.2.1. DOS Attack:

In DOS attack, the hacker attacks the server by giving a continuous request to that server. That is, the hacker connects to a specific network as an external user and sends continuous request to that server. By doing this, the hacker can make the server stop its service to the other users. As the servers follow “First come, first served” technique, the server will keep on serving the requests of the hacker as he will be continuous requesting for the service of the server.
2.2.2. DDOS Attack:

In DDOS attack, the hacker attacks the server in the same way as DOS attack. But, the main difference is that, in DOS attack the hacker request the service of the server from the same system. But in DDOS attack the hacker uses multiple systems to attack the server. That is, the hacker uses multiple systems to send request to the server. As the hacker keeps on requesting for service from different systems, other users cannot get the service of the server. This happens because, the hacker will send request continuously without leaving any gap in such a way that other users request does not interrupts their attack.
3. INTENTION RECOGNITION AND ATTACKER PREVENTION MODEL:

Intention recognition is the most important work in attack prevention. This will help us to protect the data from other hackers who try to attack the similar kind of data. Only when the intention of one hacker is known, it can be stopped or prevented from other hackers who try to do the same kind of activity. Only when it is known that some unwanted work is being held in the system, one can predict and prevent the hacker from accessing the data. So it is important to analyze the activities that are being held in the system.

Since this takes a lot of time when it is performed manually, it is better if it is performed automatically. It is also important that, one should identify the attack as early as possible. Since, it could be of no use, if we do that after the hacker does all the works. So, here is an idea proposed to find the intention of the hacker and also prevent them in an early stage.
Figure 5. The proposed idea of intention recognition and attack prevention

This idea could help the server or the user whose system contains some confidential data, to find the attacker and also prevent them from attacking the data. Start the packet capturing application automatically by making the application as a start up application. This will help to capture all the requesting packets which can be stored for analyzing.

The saved data can be analyzed for checking the requesting source address and the destination address. If the same source request for the same data to the same destination continuously, it can be predicted as an attack. Make the packet capturing application store the capturing data once for every 5 minutes. And then fix a threshold level for the number of request that can be made by a source. If the user’s number of request crosses the threshold limit, then declare it as an attack.
By analyzing the type of data that they try to access, the intention of the hacker can be predicted. With the type of protocol that they have requested, one can predict the type of file that they have tried to access. By analyzing the logs that are stored in the system, the data that was accessed by the hacker can be found.

When an attack happens, the packet capturing application captures it and gives us certain information. The captured packets will be saved and sent for processing. During processing the packets will check the count of the request sent by the hacker. This will help the admin to differentiate a user and a hacker.
4. CONCLUSION:

The system will be monitored continuously and any kind of unusual activity is detected in the early stage itself. Necessary steps will be taken to protect the data in the system. All these activities are automated in the system and the user need not be aware of it. DOS attack, Dictionary attacks can be identified with this work. By analyzing the different types of protocols which was requested by the attacker, the intention of the attacker can be found. Once the intention is identified it would be easy to stop the attacker from hacking the data. Since the attack is being detected in the early stage, the hackers cannot get a large amount of data that they need which can help them take any unauthorized data.
5. REFERENCES:


© 2018 IJCRT | Volume 6, Issue 2 April 2018 | ISSN: 2320-2882