DETECTION OF HOME-BASED INTRUSION USING SNORT

Mohd Nizam Omar
InterNetworks Laboratory & The Optical Computing and Technology Research Laboratory, School of Computing, Universiti Utara Malaysia, 06010 Universiti Utara Malaysia Sintok, Kedah, Malaysia
(niezam@uums.edu.my)

Nur Haryani Zakaria
InterNetworks Laboratory, School of Computing, Universiti Utara Malaysia, 06010 Universiti Utara Malaysia Sintok, Kedah, Malaysia

Angela Amphawan
The Optical Computing and Technology Research Laboratory, School of Computing, Universiti Utara Malaysia, 06010 Universiti Utara Malaysia Sintok, Kedah, Malaysia

ABSTRACT

Most of home users currently depend on the anti-virus or/and firewall to secure their internet environment which is not enough to provide a secure environment. Another layer of protection suggested in this paper. By introducing the basic of Intrusion Detection System (IDS), this paper proposing IDS as the solution. Although IDS widely used in larger scale of network environment, the capabilities of IDS should be also be introduced to the end user, similar to how the end user knows about the anti-virus and the firewall. By using Snort as the IDS, several kinds of home-based attacks have been identified and selected as to show the true capabilities of the IDS compared to existing anti-virus and firewall. By using general steps of the methodology, this research begins with the collection of the related information on IDS. Then, it is followed by the designing of the suitable IDS to be used in home-based environment. After that, related kinds of attacks have been selected to be tested together with anti-virus and firewall as to show the capabilities of IDS compared to antivirus and firewall. Next, the result between Snort, antivirus and firewall will be compared. Finally, the conclusion of the experiment will be concluded. By producing this research, hopefully, user will be more knowledgeable in term of a new solution for protecting their own internet environment.

KEYWORDS: Intrusion Detection System, Snort, Home-based intrusion

1. INTRODUCTION

Network security is one of the major concerns in these days due to challenging attacks and threats are becoming more noticeable. New equipment and methods have been designed to ensure security and privacy. However, there seems to be no silver bullet solution. In general, there are three stages to attain network security; prevention, detection and correction. Prevention is superior compared to the other two, but quite unbearable as attacks are getting erudite each day. In addition, with the swift development of wireless networks, prevention becomes very puzzling due to the openness of the wireless medium, configuration, complexity system and manipulation by legal users, administration errors, lack of centralized surveillance, dynamically. Detection techniques on the other side, offer more precise results in detecting malicious attackers than correction techniques (Perrig, Stankovic, & Wagner, 2004). Current security tools for home-based depend on the antivirus and/or the firewall which is not enough to protect current security attack. Intrusion Detection System (IDS) at the meantime
has been used for large scale of the network. This paper proposes the used of IDS in the home-based network environment to protect home users from security attacks.

2. HOME-BASED SECURITY TOOLS

This section will discuss about current tools that have been used by the end user at home. The tools such as antivirus and firewall are then being used by home user right now. We are introducing IDS as another layer of protection that should be used by the user.

2.1 Antivirus

Antivirus is a piece of software designed to prevent viruses entering a computer system or network (Publishers, 2018). Most of the user will install the antivirus for protecting their device to the virus. The example of antivirus software that have been used by the user currently are Total AV (TOTALAV, 2018), PCPROTECT Antivirus Pro 2018 (PROTECT, 2018), McAfee (McAfee, 2018), Scanguard (SCANGUARD, 2018), Kaspersky (Lab, 2018) and so forth.

Most of the antivirus depends on the antivirus definition to detect the virus. In other words, user needs to keep the antivirus up to date if they want to make sure that the antivirus can detect the computer virus (Flores, Ramos, Lozada, & Flores, 2017). Therefore, any intrusion that not in the list of antivirus definitions will be not detected as the computer virus.

2.2 Firewall

A firewall is a computer system or program that automatically prevents an unauthorized person from gaining access to a computer when it is connected to a network such as the Internet (Collins, 2018). Most of the Internet users will choose the firewall as the second layer after the antivirus. Most of the operating system such as Windows also provide an inbuilt firewall to be used by the user. In addition, some antivirus software, such as Kaspersky Internet Security (Lab K., 2018) provides the combination of the antivirus and the firewall.

Different to the antivirus that depend on the antivirus definition, the firewall just filtering ingoing and outgoing traffic from/out the host or network. However, a firewall cannot filtering the intrusion that define at the legitimate connection. For example, the connection to the web browser is allowed by the firewall for the user. Then, the user uses the allowed connection to do intrusion. A firewall cannot detect the intrusion, but only works to filter connection entering or/and going a host or network.

The example of firewall that user can use, including ZoneAlarm (Zone Labs, 2018), GlassWire (GlassWire, 2018), TinyWall (TinyWall, 2018) and so forth. Based on the discussion on the antivirus and the firewall, the antivirus only can detect the computer virus based on the updated virus definition and the firewall only can do the filtering the connection coming and out to/from a host or a network. These kind of protection currently cannot overcome the current type of intrusion that possible to execute by the intruder. Therefore, this research proposing Intrusion Detection System (IDS) as the additional layer for protecting the home user.
3. INTRUSION DETECTION SYSTEM (IDS)

This part will discuss generally about the IDS. This includes the introduction of the IDS, types of IDS, and freeware IDS.

3.1 Introduction to the IDS

The idea of IDS was initially presented by (Anderson, 1980) to set off straight computer security methods. Afterwards, (Rehman, 2003) defined intrusion as any action of the group attempting to breach confidentiality and or integrity of particular resources and or integrity of particular resources. IDS evaluates all the system activities in order to sense the intrusion. It examines for security violation events and recognizes illegal access. The intrusion can be put in different forms such as workers who do not have access rights to a particular resources trying to access resources on a system or network or malicious programs that spoils the system incomes by damaging the system.

The IDS have been focused on outsider intrusion detection for operators, network and database systems and less attention has been given to intrusion detection for application systems such as banking and finance systems. Unfortunately, these application systems based are normally contained lots of business security information. Even when the prototype of the intrusion detection field has developed, focusing on such application, most of the intrusion detection approaches still focus on outsider intrusion, but not a great deal is available for insider intrusion, such as malicious codes created by malicious software engineers (Puketza, Zhang, Chung, Mukherjee, & Olsson, 1996).

3.2 Types of IDS

There are several types of IDS. Active IDS is also famous as Intrusion Detection and Prevention essential administered by an operator (Ramachandran, 2010). IDPS offer the benefit of real-time corrective action in response to an attack. IDPS is designed mechanically to block any suspected attacks. Passive IDS on the other hand is administered by a single observer to monitor the network traffic action and make aware of operator for any future weaknesses and attacks (Joshi, Jindal, Chowkwale, Shethia, Shaikh, & Ved, 2016). A passive IDS is not capable of showing any defensive or reactive functions by its own. Network Intrusion Detection System (NIDS) is commonly comprised of a network appliance with network interface controller operating in promiscuous mode and a spread management interface (Raghunath & Mahadeo, 2008). This type of IDS is commonly placed along a section of the network segment to examine all traffic. Host Intrusion Detection System (HIDS) is a software application which is normally installed on the terminals (Torkaman, Bahrololum, & Tadayon, 2014). The terminal will display the operational system and writing data to log files and/or trigger alarms.

3.3 Freeware IDS

This part will discuss about available freeware IDS that home user can download and use directly. There are Snort, Sax2, Suricata and so on that can be downloaded free by home user to secure their home-based network.
3.3.1 Snort

Snort is a network based IDS that scan the traffic and tries to find suspicious activities using a set of rules. A rule set is a collection of specific byte pattern that indicates a particular attack. This type of IDS usually uses the signature based IDS. Snort can also be configured to work as a packet sniffer and packet logger. Snort protocol will examine, matching or content searching, and is usually used to vigorously block or passively sense a diversity of attacks and probes, such as buffer overflows, stealth port scans and web application (Cisco, 2018).

3.3.2 Sax2

Sax2 is another freeware IDS that provide an intrusion system in real-time packet capturing, 24/7 network monitoring, advanced protocol analyzing and automatic expert detection (Corporate, 2018).

3.3.3 Suricata

Suricata is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection, inline intrusion prevention, network security monitoring and offline pcap processing. Scuricata inspects the network traffic using a powerful and extensive rules and signature language and has powerful Lua scripting support for detection of complex threats (Suricata, 2018).

From Snort, Sax2 and Suricata, Snort will be used further in this research experiment. This is because most of the researcher uses Snort more than Sax2 and Suricata. One of the main factor is because Snort provides flexibility more compare to Sax2 and Suricata.

4. TYPES OF ATTACK

There are many types of attacks can be considered in the network intrusion. For example, denial of service (DoS), backdoor attack, Domain Name Server (DNS) attack, Scans, Secure Socket Layer (SSL) attack, and so forth. However, the home user network is not to be vulnerable to all kinds of attack. Two types of attacks that have been identified to be the main attack to the home-based network are brute force and backdoor attack. The brute force attack is a trial and error method used by application or user to decode encrypted data or password. In a term of home user environment, brute force attack is possible to occur in the user’s router interface. Figure 1 shows the ordinary user’s router interface.

By referring to Figure 1, any connected user to the network just needs to find the default gateway IP to get to this router interface. This is the place where users can do the brute force attack to get entered to the router control. By getting control to this interface, the user can do anything include install backdoor script to allow illegal log in in the future. The attacker can do a brute force attack without the antivirus and firewall know about it. Therefore, in this research, antivirus, firewall and Snort will be executed concurrently when brute force takes part.
5. METHODOLOGY

The methodology was adopted from (Vijay Vaishnavi, 2004). There are five steps involved in the methodology. Each of the steps is meant for different function. In the first phase, the problem was identified so as to understand the purpose and scope of the research. It is important because the problem will be the main agenda that requires solutions in the research carried out. This phase was done mainly through systematic literature reviews.

The second step involves the identification of suitable IDS software to be used. As mention in the previous section, Snort will be chosen compared to Sax2 and Sucirata because of the flexibility in the Snort. By using Snort, specific kind of attack or intrusion can be detected through the usage of right detection script. For that reason, the script for wrong password and attempting to access host will be developed. This is followed by the third step whereby a set of script or signature has been developed. The script will be embedded into Snort so that Snort can detect to the chosen wrong password and attempting to access the host kind of attack.

In the fourth steps, the evaluation and testing will take part. An experiment to evaluate the effectiveness of the proposed script/signature will be executed. The evaluation process includes with the comparison with two others tools; antivirus and firewall. Finally, the last phase involves the analyzing of the result, followed by the conclusion based on the executed experiment. The research also includes the limitation and future work for this research.

6. SCRIPT/RULE DEVELOPMENT USING SNORT

This section will entail a specific discussion on how the entire system has been developed in terms of the rule configurations. Snort IDS can be used as a detection system to monitor all packets that are sent or received. The Snort engine is distributed both as source code and as binary distributions windows. It is authoritative to note that the Snort engine and Snort rules are spread separately. The following Figure 2 shows the flow of the process involved in the prototype development (Alsafasfeh & Alshbatat, 2011).
Based on Figure 2, the detail explanation for each step will be discussed further in next parts.

6.1 Snort Installation and Configuration

It is necessary to make sure that the installation of Snort successful. The installation of Snort will enable Snort functioning correctly in capturing packet, and monitoring network traffic.

6.2 Configuration of snort.conf File

Snort.conf file is the main file in the Snort operation and must be configured before the application file starts running. This file will be used by the detection engine and preprocessors. Snort.conf file is located in etc folder in Snort’s installation path. Snort.conf file contains several samples of Snort configuration. To create a custom configuration, the network variable must be set and the decoder needs to be configured. The configuration includes the base detection engine, dynamic loaded libraries, preprocessors and output plug-in. Then several items need to be customized such as the rule set, preprocessor, decoder rule set and shared object rule set.

6.3 Running Snort

Snort is a system works as a firewall to control access. By using Snort, a new rule contains all specifications and requirements for the operation must be prepared. To make Snort has been configured as a firewall; a new set of rules needs to be configured. The first configuration is used to monitor website access and this will be used as a guide to inform the network administrator about the whole connections between network nodes and the external network. The second configuration one is to block access to a specific website.

6.4 Configuration for Monitoring Access

Snort is host-based IDS that based on a set of rules which hold a set of operations that allow network administrators to monitor all network traffics. To create a new rule that has the authority to monitor all accesses from our network to external networks, all primary contents of the rule header and rule options must be configured. This will eventually change Snort into a monitoring system that is has the ability to inform the network administrator who is trying to access the network (Muthuregunathan, S, R, & SR, 2009).

For this research, new rules have been created to allow Snort to monitor access and produce alerts to system administration. The alert file contains all data that describe the connection between two entities that is the IP address for two entities (sender and destination) and the access time. The detection engine in Snort has checked packet contents with the rule options and when matching is found, the Snort engine will send an alert to the network administrator with messages in order to inform the administrator what going on.

7. RESULT
The result of this research can be looked based on two kinds of home-based intrusion; Wrong password and attempting host access.

7.1 Wrong Password

As mention previously, wrong password (under a brute force kind of attack) is one of the attacks that possible to occur in the home-based network. This is a kind of attack where the attacker attempts to log in to the router’s management interface as shown in Figure 1.

**Figure 3: Snort’s Alert Failed Login**

Based on Figure 3, it is shown that every fail login to the router interface will be notified by the Snort. This on the other hand proven the rule/signature that has been developed before fully functioning to this kind of attack. The notification ‘Failed Login’ shows that there is a wrong password attack occurs. As mention previously, the wrong password attack also been tested together with the antivirus and the firewall. The result for both tools will be further discussed in the next section.

7.2 Attempting Host Access

Similar to the previous kind of attack (wrong password attack), attempting host access is a kind of attack used by the attacker to access to user host (PC, smart phone, tablet, etc.). This is possible to execute the attack by just connecting to victim’s host using the victim’s IP address. We always put ourselves in this environment through shared Internet environment such as in free Wi-Fi connection in our office, mamak stall, fast food restaurant and any place that provides free Wi-Fi connection. As mention previously, the wrong password attack also been tested together with the antivirus and the firewall. The result for both tools will be further discussed in the next section.

**Figure 4: Attempting Host Access Attack**

By referring to Figure 4, the host attempt attack has been detected by Snort when the notification of “ATTACK in Host command attempt” appear. Similar to the previous section, host attempted attacks also been tested together with the antivirus and the firewall. The result for both tools will be further discussed in the next section.

8. ANALYSIS

This section will analyze the results. The main concern in the analysis is to compare the detection of a wrong password and attempting host access kind of attack between IDS (Snort), antivirus (AVG), and firewall (Windows). The analysis divided according to wrong password and attempting host access.

8.1 Wrong Password
Table 1 shows the overall analysis between IDS, Antivirus and Firewall on wrong password attack.

Table 1: Comparison Between IDS, Antivirus and Firewall on Wrong Password Attack

<table>
<thead>
<tr>
<th>Tools</th>
<th>Detection on Wrong Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS</td>
<td>Yes</td>
</tr>
<tr>
<td>Antivirus</td>
<td>No</td>
</tr>
<tr>
<td>Firewall</td>
<td>No</td>
</tr>
</tbody>
</table>

From the Table 1, it is clear that only IDS (Snort) has a capability to detect the wrong password kind of attack. This is as shown in Figure 3. As mention previously also, the antivirus and the firewall cannot detect the wrong password attack because antivirus depend on the signature embedded in the antivirus and the firewall just filtering the connection outgoing and ingoing the host or network.

8.2 Attempting Host Access

Table 2 shows the overall analysis between IDS, antivirus and firewall on attempting host access attack.

Table 2: Comparison Between IDS, Antivirus and Firewall on Attempting Host Access Attack

<table>
<thead>
<tr>
<th>Tools</th>
<th>Detection on Wrong Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS</td>
<td>Yes</td>
</tr>
<tr>
<td>Antivirus</td>
<td>No</td>
</tr>
<tr>
<td>Firewall</td>
<td>No</td>
</tr>
</tbody>
</table>

From the Table 2, similar to the previous table, it shows that only IDS (Snort) has a capability to detect attempting host access kind of attack. This is as shown in Figure 4. As mentioned in previous part, the antivirus and the firewall cannot detect the wrong password attack because antivirus depends on the signature and the firewall just filter the connection outgoing and ingoing in/or host or network.

9. CONCLUSION AND FUTURE WORK

This research proposes an additional layer of security in the home user Internet environment. By using IDS (Snort) as the second layer of protection, home user Internet environment becomes more secure than before. Currently, home user just depend on the antivirus and the firewall as the only layer of protection against intrusion. By looking at the experiment that has been executed using most kind of home user attack; wrong password and attempting host access attack, it is proven that only Snort has a capability to detect this kind of research.

For the future work, further kind of rule/signature that related to the home user attack will be explored. Not only that, Snort will be produced to be so light and suitable enough to overcome the home user attack. This is necessary because current Snort is ready to overcome to all kind attack that sometime more than necessary for the home user Internet environment.

RUJUKAN


