International Journal of Applied Engineering Research ISSN 0973-4562 Volume 16, Number 4 (2021) pp. 267-270
© Research India Publications. https://dx.doi.org/10.37622/IJAER/16.4.2021.267-270

Network Intrusion Detection and Prevention

Akarshita Shankar[a] and Akshay Shankar[b]

[a]*Specialist Programmer, Infosys Limited, Plot No.44, Hosur Road, Electronic City, Bengaluru, Karnataka – 560100, India*

[b]*Computer Science Engineering, RV College of Engineering, Mysore Road, RV Vidyaniketan Post, Bengaluru, Karnataka – 560059, India*

Abstract:

Network Intrusion is cybercrime, which involves hacking into users' systems and stealing their sensitive and confidential information. The information could include credit card details, username, and passwords, bank details, etc. These attacks occur via malicious viruses installed in the user's system without his/her knowledge, blocking the network traffic to a legitimate site, etc. After obtaining the information, the attacker could commit crimes such as financial losses and identity theft. The target could be an individual, an organization, or a cluster in an organization. This paper provides an explanation of network intrusion, detection, and prevention to overcome them.

Keywords: Phishing, Network Intrusion, Flooding, Routing Detection, Intrusion Prevention, Trojan Horse, Worms

I. INTRODUCTION

The word 'Intrusion' in English means "*The act of thrusting oneself in without any invitation or permission*". Network Intrusion is similar to that. Network Intrusion is an unauthorized activity on digital or computer network using the machine address of the system in that particular domain. This type of intrusion can be either active or passive. The active form of attacking includes modifications to the network resources are affected and the passive form of attacking includes penetrating into the system without detection. This can occur from outside the designated network structure or it can occur from inside the network structure like a customer, employee or a business partner.

Network Intrusion immensely benefits the attacker. Usually, unwanted activity steals the valuable resources of the network to threaten and jeopardize the network security and the associated data. The data includes sensitive information such as the personal data, password, bank accounts, etc. This data can be obtained either in one-time basis or constantly like a parasitic relationship that continues to siphon off data until it is discovered. The attackers deceive the end-users by impacting crafted code like malware that is used to steal password, open applications, record keystrokes, etc.

Loss of sensitive data comes with a massive cost. The countries and organizations affected by data breach is increasing each year. Malicious Digital Attacks are the most expensive and most common type of attack. When an organization or country is affected by it, they incur a loss of approximately $4.45 million per incident. Data breach can also affect an individual when he/she has lost sensitive data and is being threatened by the attacker. This leads to Identity Theft or Identity Fraud.

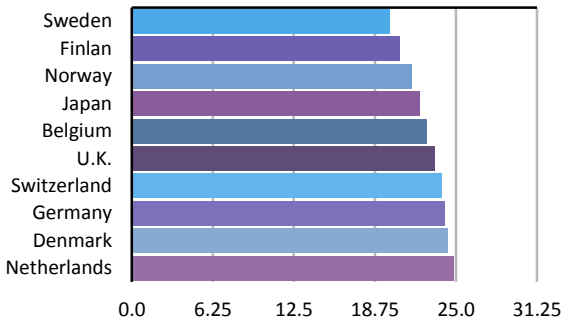

Figure 1

Figure 1 is a chart that shows the percentage of top 5 countries that contribute to network intrusion from the year 2016 - 2019. China has majority of the hackers in the year 2017 and 2018 while United States of America has it in the year 2016 and 2019.

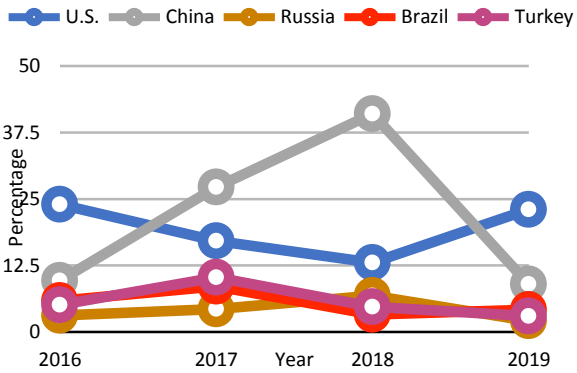

Figure 2

Figure 2 demonstrates the countries that have been affected by various forms of network intrusion. Nearly 25% of the data breaches have occurred in Netherlands.

II. STAGES OF NETWORK INTRUSION

1. Reconnaissance

The first stage of network intrusion involves in attacker

focusing and analyzing his target. This stage is vital for the attacker since he/she spends several weeks or months to gather information on the target which includes his name, phone number, email address, company/organization he/she is working for, etc. After deciding his target, the attacker collates information by examining the documents and email addresses associated with the target. The goal of the attacker is to be more familiar with the target network than the technicians who run and maintain it. By doing so, they not only learn the technology's weaknesses and vulnerability, but also methods on how to successfully exploit to their advantage. As the first step, the attacker pings the target network to peruse the hosts, ports and the systems connected to the network. Using this data, the attacker will create an entry point for his attack.

2. Initial Exploitation

Using the entry point created in the previous step, the attacker uses various methods to exploit the network. The most common methods include:

Phishing: A popular method that involves in sending fraudulent emails to the target to bait them into sending sensitive information including back account details and passwords. The attacker deceives the target by sending the emails that appear to come from a creditable source.

Watering Hole: In this method, the attacker compromises a website that is frequently visited by the target. When the target visits the infected website again, the attacker gains access to the target's network using the credentials obtained in this process.

Other forms of getting such unauthorized access includes SQL Injection, Social Engineering and Spear Phishing.

3. Establish Persistence

At this point, the attacker has access to the target's network and is determined on gaining additional access to continue the intrusion. They gain the additional access through privileged escalation, running scripts or finding the Run Keys, and is able to penetrate deeper into the system to take further control. He/she takes advantage of the flaws in the system to get extra privilege or access that is not intended for the user.

4. Install Malicious Tools

The attackers that have invaded the target's network install tools so that they do not get caught for their malicious activities. The installation of tool affects the system in various ways including running scripts and programs that slows down the system, install and activate the virus in the system.

5. Move Laterally

Using the tools that the attacker has installed in the system, he/she moves laterally around the system to gather the target's sensitive information or the data that they need to get. At this stage, the attacker has succeeded in his/her mission and the required sensitive information is obtained by compromising the target's network.

6. Collect Data and Exploit

This is the final stage of network intrusion where the attacker has obtained all the required information from the target's machine. The attacker leaves the system without being detected.

III. TYPE OF NETWORK INTRUSION ATTACKS

1. Asymmetric Routing

Asymmetric Routing is when network packets leave one path and take up a different path, whereas in symmetric routing the packets of the network use the same entry and exit path to travel. Although asymmetric routing is highly efficient, it is redundant. There are quite a number of problems which arise.

Asymmetric Routing Detection: Asymmetric Routing can be detected by using automated detection techniques. If asymmetry is detected, it will first pass through the unoptimized asymmetric traffic which allows the TCP connections' work to continue. During the detection process, the first TCP connection might be dropped for a set of addresses. On time out of that particular asymmetric routing cache's entry then the connections between these hosts are optimized.

Buffer Overflow Attacks: Buffers are temporary memory storage regions which hold data during the transfer from one place to another. The overflow error occurs only when the amount of storage available of the memory buffer is exceeded by the amount of data. When this issue occurs, the program starts to overwrite the memory locations adjacent to the original location where the memory needed to be written.

2. Traffic Flooding

Network flooding attacks have long been consistently used by attackers for denying service to legitimate users. This attack is performed in two ways:

a. A huge block of traffic at a service or a specific server with the main goal as to exhaust the resources which are focusing on trying to respond to false traffic in order to prevent it from processing legitimate service requests.

b. The other way is to send a huge block of traffic to a particular segment of network with the aim as to create a lot of network congestion that is a legit traffic block which is unreachable target server or service.

Flood Preventing Techniques: To prevent flood attacks, mainly Default Packet Handling page, we can have particular thresholds that allow a number of packets per service for various types of traffic. When the specified thresholds are exceeded by the packet numbers there is a drop in traffic of the device of that particular interface.

3. Trojans

A Trojan horse or trojan is a software that is made to look legitimate but in reality, is malicious and can cause a user to lose control of your computer. It cannot be duplicated and can be executed when the command is initiated by the user.

The goal of the Trojan is to damage, steal, destroy or cause harm to your data or network. It is like a file or an application which would look like a file that the user is familiar with. This is to deceive the user into thinking that there is no malware on

their device, lowering the awareness of the user. As the application looks like a normal file the user allows the Trojan to perform the malicious activities.

Methods of Detecting Trojans by the Users: Trojans is the pathway to setting up different types of malware. However, it can be detected if the user watches out for suspicious activities. The suspicious activities are as follows:

a. If the user's system is not performing as expected, that is, if the system is slow or is encountering errors more often.

b. If the user's system starts acting in an abnormal way where certain programs may not run and certain processes which are not initiated by the user are being run on the system.

c. Random pop-ups or ads which keep appearing on the screen and if the user notices some sort of disturbance from browser pop-ups or spam mails.

4. Worms

Worms are malicious programs which have the ability to replicate themselves. They are capable of adding malicious programs onto the users' system. Worms can be injected into the users' computer through software vulnerabilities or through attachments from emails or instant messages. Upon opening these files, it could redirect to a malicious website and download the worm onto the computer. It then starts to affect the system without the user's knowledge. The effects are similar to Trojan, which is to delete files, modify files, etc. Since they can replicate, worms can be much worse as they start depleting the resources of the system and causing huge problems if the system is using a shared network. It can also create a backdoor, allowing hackers to access the users' system and in addition gain control over the system.

Worm detection and prevention: Worms spread at very high rates which cannot be detected easily by humans. Therefore, the earlier the detection of worms by the Automated Intrusion Detection System, the faster the elimination. The Intrusion Detection System (IDS) raises an alert if there is a virus found, but the IDS must be a desktop antivirus software runs on the host. Many times, worms can still pierce through antivirus which the user must be cautious about. Firewalls are extremely important because they help in scanning or analyzing the presence of worms. One of the main purposes of a firewall would be to filter and to refine the high link speeds and to check if there is any chance for a virus or worms to be present in the system. There are certain other ways for the prevention of worms through network intrusion is to analyze the traffic, to identity or to find any malicious code or programs which may be present, it is also used to detect certain abnormal behaviors which may lead to the infiltration of worms.

IV. NETWORK INTRUSION PREVENTION

Intrusion Prevention System (IPS) are appliances of network security that monitor the system and/or network for any suspicious activity. If it detects any malicious activity, IPS then gathers information about this activity, reports the details and enforces mechanisms to block the malicious activity. Some of the proactive actions that any IPS takes are resetting a connection, sending an alert to the network team or blocking the incoming traffic from the hostile IP address. Other predominantly known IPS are:

- **Network-Based Intrusion Prevention System (NIPS)**

  NIPS is a system that monitors a network for any malicious activity and acts on the malicious activity through a specific set of rules that are provided to it before-hand. In this technique, the Intrusion Prevention system scans the complete network for irregular traffic. It performs this activity using protocol analysis. Since NIPS has a requirement of running thousands of commands at once, it is quick and application based. It helps in detecting any threat or malware.

- **Wireless Intrusion Prevention System (WIPS)**

  WIPS specifically monitors wireless networks for any malicious activities. WIPS is very effective since it performs this monitoring by analyzing wireless networking protocols, detects and shuts down any malicious and unauthorized entries by itself.

- **Network Behavior Analysis (NBA)**

  NBA vigilantly observes the network traffic of the system. While NBA monitors the network, it creates data packets to perform a detailed offline analysis. This helps in reducing the burden of network administrators. NBA is mostly used for identifying threats that generate irregular traffic flows. This helps in detecting Denial of Service Attacks, Policy Breach and Specific forms of Malware.

- **Host Based Intrusion Prevention System (HIPS)**

  HIPS is used for a single host computer. It is a software package that is setup to monitor a single host for any malicious attack. It operates from the network layer till the application layer. It performs the detection by analyzing activities occurring inside the host's network. The activities include the application logs, system calls, file-system modifications, etc.

V. CONCLUSION

Some of the best practices to prevent network intrusion are as follows:

- **Encrypted Transmissions**

  Any incoming data or outgoing data should be encrypted to prevent eavesdropping

- **Antivirus Software**

  Installing an anti-virus software helps in detecting any malicious activity

- **Regular updates**

  Updating the software to its latest version avoids any glitch from the obsolete version, that could be used to exploit the system