Evaluating firewall tools and techniques in enhancing network security

Dr.Kamalakannan Machap
School of Technology
Asia Pacific University of Technology
and innovation (APU)
Kuala Lumpur, Malaysia
dr.kamalakannan@staffemail.apu.edu.my

Hua Qiang
School of Technology
Asia Pacific University of Technology
and innovation (APU)
Kuala Lumpur, Malaysia
tp062850@email.apu.edu.my

***Abstract*— Currently the network is indispensable and possibility of ignoring the limitation of distance for communication, and organization, etc. The advancement of technology that the network has brought countless conveniences. Computer networks have become the norm in today's corporate world, and networks now carry more traffic than ever before, not only from computers, but also from smartphone is also becoming a significant element of it. However, in addition to providing consumers with convenience, the Network also poses several risks and obstacles. These problems manifest themselves in a variety of ways, including ransomware, phishing attempts, and malware attacks. In the network environment, users can employ tools and security technologies to solve security issues and obstacles. Although it is difficult for a network to achieve complete security, we can employ the most up-to-date techniques and technology to reduce the likelihood of security threats. The most significant reasons to secure our network security are the continual update of tools and the ongoing evolution of technology. Network attacks are a possibility in many network fields. Hackers can attack the destination by employing attack methods based on network technology advancements. It can be difficult for users to tell which virus is being disguised by the attacker. It may not be effective if the user is using improper technologies or old tools to protect the machine. This paper will present some suggested tools or strategies for resolving network problems and obstacles.**

Keywords*—Network attacks, DDOS, Firewall, IDS, traffic analysis, Replay attack.

I. Introduction

The Network is used more and more frequently in life, whether it is for individuals, businesses, schools, or other organizations. The emergence of network attacks has also become more serious. If appropriate measures are not taken to prevent network attacks, it is easy to cause loss of personal privacy data or economic losses. Therefore, network security is extremely important everywhere [1].

Today, the number of network attacks has reached epidemic proportions. According to a report, the number of new malwares released every month exceeds 20 million, and the total number of existing malwares are close to 900 million variants. Since 2005, more than 11.5 billion records have been exposed. In 2019, four-fifths of organizations have experienced at least one successful network attack, and more than one-third of organizations have suffered six or more successful network attacks. It is estimated that by 2021, a company will be attacked by ransomware every 11 seconds. [2]. Network security is to start with authorization for network security, including regulations and strategies adopted by network administrators to prevent and monitor the unauthorized access, modification, misuse or rejection of computer networks and network-accessible resources [3].

II. Literature Review and Research

A. *Network Protection*

The term "network security" refers to a wide range of technology, equipment, and procedures. In other terms, it is a set of rules and configurations that use software and hardware to safeguard the integrity, confidentiality, and accessibility of computer networks and data [4].

Information on a computer network is kept safe via network security. The host server and connected computer terminals can only be managed and accessed by the system administrator and his helpers. This will help prevent unauthorized users from altering the server's data [5].

B. *Challenges of network security*

Network attacks are one of the most serious threats to network security today. The number of people assaulted by the Network has risen dramatically as the Network's popularity has grown. According to studies, network crime will cost the globe $6 trillion per year between 2015 and 2021, an increase of 100% in just 6 years. DDoS attacks, for example, are a prevalent sort of network attack. The first known distributed denial of service assault took place in 1996, when Panix, one of the first network service providers, was knocked offline for many days by a SYN flood (a tactic that has since become a standard DDoS attack). According to Cisco's statistics and projections, the overall number of DDoS attacks in 2018 was 7.9 million, and that number is expected to rise to 15 million by 2023.

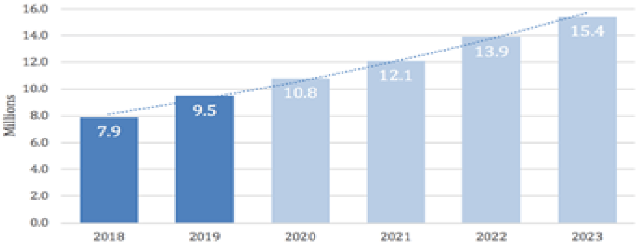


Fig 1. Cisco's analysis of DDoS total attack history and predictions

C. *Trojan Horse Attack*

Active attacks, such as Trojan horse attacks, are also a sort of active attack. As if hiding soldiers in a Trojan horse, the attacker hides harmful software in the download link, therefore this assault type is known as a Trojan horse attack.

When a user clicks on a malware-infected download link, the malware is swiftly installed on the user's device. The backdoor Trojan is the most frequent. Through the backdoor Trojan, the attacker can gain basic access to the user's device. Rootkit is the most common sort of Trojan attack. Once Rootkit has infiltrated a user's device, the attacker can take control of the system, change computer settings, view any files or images, and monitor user activity without the user's knowledge [6].

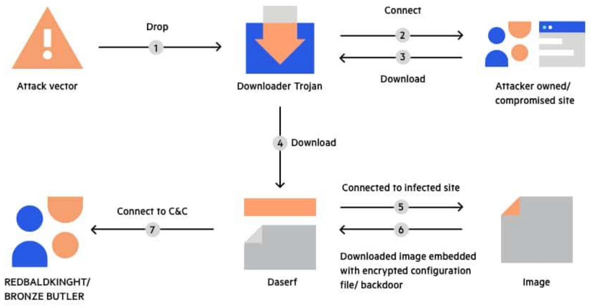

Attack vector
Drop
1
Downloader Trojan
Connect
2
3
Download
Attacker owned/ compromised site
4 Download
Connected to infected site
5
6
Downloaded image embedded with encrypted configuration file/ backdoor
Image
Daserf
Connect to C&C
7
REDBALDKINGHT/ BRONZE BUTLER

Fig 2. How the attacker used the Trojan horse to attack

D. Replay Attack

A replay attack is a malicious or deceptive network assault that repeats or delays legitimate data. The attacker does not need advanced expertise to decrypt the information intercepted in the network using this attack method. To complete the attack, the attacker just needs to intercept the data and then retransmit it. It appears to be extremely simple, but it can result in big financial losses. For example, the CEO of a company sends encrypted information to the financial administrator to complete the authorization of a transfer. The attacker eavesdropped on the information and then captured it. The attacker can complete the authorization for the financial administrator to transfer money to himself by resending the encrypted information [7].

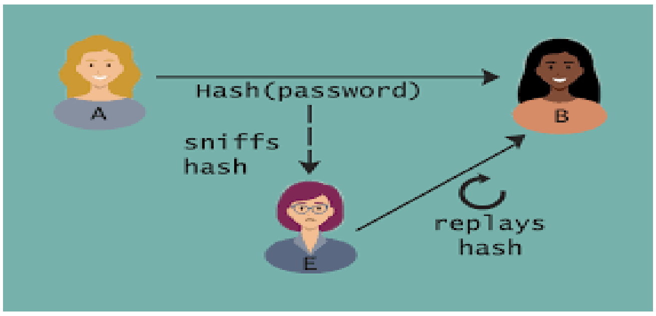


Fig 3. Example image of replay attackTraffic Analysis

E. Traffic analysis

is a process in which an attacker infers effective information through intercepted and inspected information. This process can be performed even if the information intercepted by the attacker is encrypted. The intercepted information includes but is not limited to the identity and geographic location of the sender and receiver. Generally speaking, the more information the attacker observes and the richer the intercepted information, the more effective information can be obtained through traffic analysis [8].

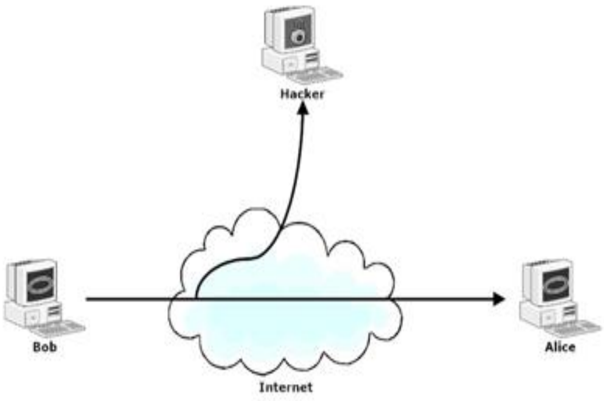


Fig 4. Traffic analysis in passive attacks

Another sort of passive attack is the dissemination of information. Eavesdropping is a traffic analysis attack tactic. The dissemination of information is a form of surveillance. Using malware or other viruses, the attacker installs the software on the target device and then watches its data. Message chats, the transmission of personal information and knowledge files, or e-mails, for example. These sent data or files could contain sensitive or confidential information about the target user. Attackers can exploit this information to achieve their objectives [9].

III. SECURITY TOOLS AND TECHNIQUES

Network assaults have resulted in losses of more than $6 trillion USD worldwide, surpassing the losses incurred as a result of natural disasters. Individuals and corporations alike rely heavily on data. It also includes your personal information. It is considerably more critical in the workplace; it is practically every company's lifeblood. The availability of network security tools and technologies can help us not only secure sensitive information, but also protect the general functioning of our equipment, preserve the company's reputation, and keep the business running normally.

A. Intrusion Detection System

IDS might be a piece of software or a piece of hardware. It searches for suspicious behaviours and known dangers by monitoring traffic on the network and through the system. Network attacks, such as Trojan horse attacks, can be prevented by IDS [10]. For example, if a firm's device downloads malware-linked software for phishing attacks, IDS can detect an issue with the software's traffic and notify the security team when a known attack against the organisation is detected. "The overall goal of IDS is to alert IT personnel to potential network intrusions." (AT&T Vice President Brian Rexroad). IDS can be classified into two types depending on the definition above: host-based and network-based. The IDS sensor can be put on the host/endpoint or on the network, which is the difference between the two. Despite the fact that IDS can monitor traffic between the organisation and the outside world, we must mention that we must examine it critically. It also has certain drawbacks, such as false positives and threats that are overlooked. To learn what threats exist, IDS requires a specific database. [10].

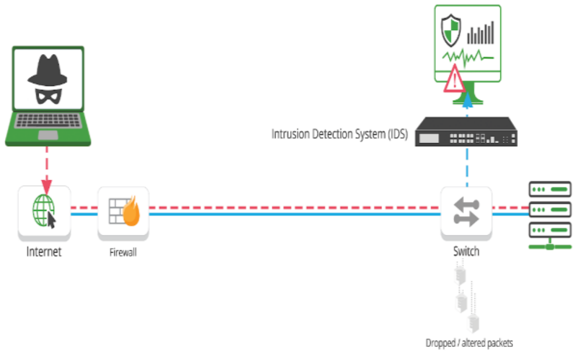


Fig 5. IDS working diagram (from Todd Cain)

B. *Firewall*

A firewall is a network security system that monitors and regulates incoming and outgoing network traffic based on user-defined security rules. Firewalls are commonly used to separate trustworthy and untrusted networks, such as the company's local area network and the Internet [11].

The firewall may protect the device using custom rules, which means it can prevent most network threats if rules are set up by someone with professional network security experience. A DDoS firewall, for example, is an active protection system designed to counter multiple DDoS attacks.

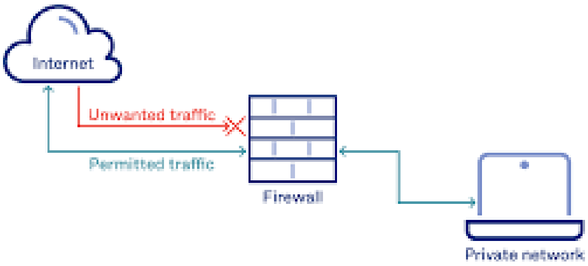
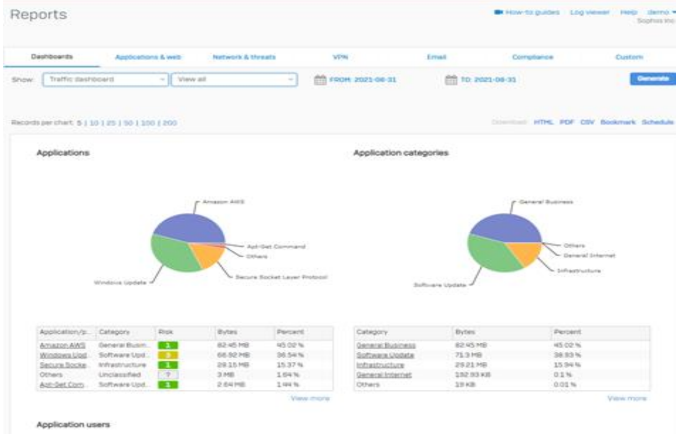


Fig 6. How Firewalls Work (from Okta)

C. *Use tools with simulated data*

The firewall simulator produced to see the user activities, Web, and Reports.


Reports

How-to guides Log viewer Help demo ▾
Sophos Inc

Dashboards | Applications & web | Network & threats | VPN | Email | Compliance | Custom

Show: Traffic dashboard ▾ View all ▾ FROM: 2021-08-31 TO: 2021-08-31 Generate

Records per chart: 5 | 10 | 25 | 50 | 100 | 200

Download: HTML PDF CSV Bookmark Schedule

Applications

Application/p...	Category	Risk	Bytes	Percent
Amazon AWS	General Busin...	1	82.45 MB	45.02 %
Windows Upd...	Software Upd...	3	68.92 MB	36.54 %
Secure Socke...	Infrastructure	1	28.15 MB	15.37 %
Others	Unclassified	?	3 MB	1.64 %
Apt-Get Com...	Software Upd...	1	2.64 MB	1.44 %

View more

Application categories

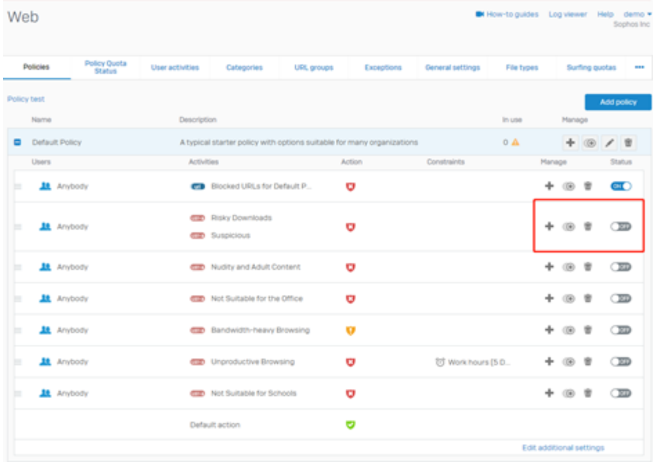
Category	Bytes	Percent
General Business	82.45 MB	45.02 %
Software Update	71.3 MB	38.93 %
Infrastructure	29.21 MB	15.94 %
General Internet	182.93 KB	0.1 %
Others	19 KB	0.01 %

View more

Application users

Fig 7. Reports of one of the firewall activities

In the Web module, the administrator can control user activities within the network. For example, turn off 'risky downloads'.


Web

How-to guides Log viewer Help demo ▾
Sophos Inc

Policies | Policy Quota Status | User activities | Categories | URL groups | Exceptions | General settings | File types | Surfing quotas | •••

Policy test

Add policy

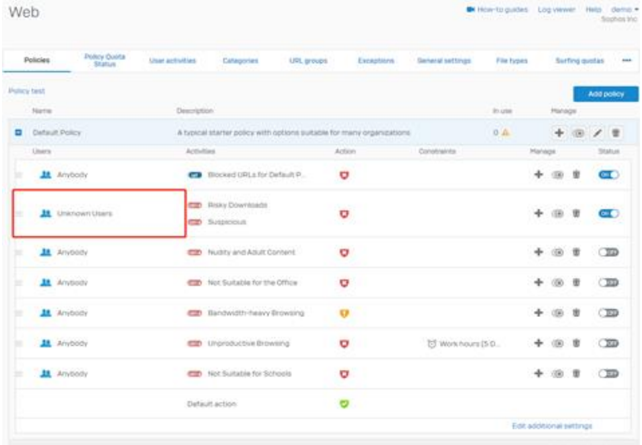
Name	Description	In use	Manage
Default Policy	A typical starter policy with options suitable for many organizations	0 ⚠	✚ ◉ ✎ 🗑

Users	Activities	Action	Constraints	Manage	Status
Anybody	Blocked URLs for Default P...	⛉		✚ ◉ 🗑	ON
Anybody	Risky Downloads Suspicious	⛉		✚ ◉ 🗑	OFF
Anybody	Nudity and Adult Content	⛉		✚ ◉ 🗑	OFF
Anybody	Not Suitable for the Office	⛉		✚ ◉ 🗑	OFF
Anybody	Bandwidth-heavy Browsing	⛉		✚ ◉ 🗑	OFF
Anybody	Unproductive Browsing	⛉	Work hours (5 D...	✚ ◉ 🗑	OFF
Anybody	Not Suitable for Schools	⛉		✚ ◉ 🗑	OFF
	Default action	⛉			

Edit additional settings

Fig 8. Modify activity status

Modify users who allow 'risky downloads'.


Web

How-to guides Log viewer Help demo ▾
Sophos Inc

Policies | Policy Quota Status | User activities | Categories | URL groups | Exceptions | General settings | File types | Surfing quotas | •••

Policy test

Add policy

Name	Description	In use	Manage
Default Policy	A typical starter policy with options suitable for many organizations	0 ⚠	✚ ◉ ✎ 🗑

Users	Activities	Action	Constraints	Manage	Status
Anybody	Blocked URLs for Default P...	⛉		✚ ◉ 🗑	ON
Unknown Users	Risky Downloads Suspicious	⛉		✚ ◉ 🗑	ON
Anybody	Nudity and Adult Content	⛉		✚ ◉ 🗑	OFF
Anybody	Not Suitable for the Office	⛉		✚ ◉ 🗑	OFF
Anybody	Bandwidth-heavy Browsing	⛉		✚ ◉ 🗑	OFF
Anybody	Unproductive Browsing	⛉	Work hours (5 D...	✚ ◉ 🗑	OFF
Anybody	Not Suitable for Schools	⛉		✚ ◉ 🗑	OFF
	Default action	⛉			

Edit additional settings

Fig 9. Modify user rights

IV. CONCLUSION

The more utilize of Internet in our everyday lives probable to be attacked by the Internet. Need to focused prevention and detection to decrease the risk of network assaults in the face of these network security concerns and challenges. An active attack, the necessitates continual involvement with the equipment to achieve the goal. Some of the most up-to-date tools to scan and detect our own gadget, allowing to locate and resolve it. Because passive attacks are difficult to detect, only defend our information security as much as possible by using proper technologies. Network assaults can affect everyone who uses the internet, whether it's an individual, a company, or another organization. As previously stated, in 2021, the worldwide loss caused by network assaults will outnumber the loss caused by natural disasters. User be the next victim of a network security breach if you undervalue network security and with the passage of time, this has become more of an unseen conflict. User continually update technology and techniques to fend off network threats. Some hackers have been on the lookout for new techniques to break into people's computers to achieve their objectives. Many security tools and technologies as possible is something can do with equipment because the professional organization security team must always be up to date on the latest technology and tools, as well as the most recent network attack methodologies. Although user cannot guarantee that our data is completely secure, stay up with the times and perform best to reduce the risk of network assaults.

REFERENCES

[1] M. V. Pawar and J. Anuradha, “Network security and types of attacks in network,'' Procedia Comput. Sci., vol. 48, pp. 503–506, 2015.

[2] Ciampa, M, “CompTIA security+ guide to network security fundamentals,'' Cengage Learning, 2021 pp. 64-69.

[3] W. Stalings, “Network security essentials, 5th edition 2013,'' pp 204-207. ISBN10:0273793365.

[4] R. Bejtlich, “Practice of network security monitoring,'' 2013.pp.256-261. ISBN10: 1593275099.

[5] C. Mcnab, “Network Security Assessment,'' 3rd edition, pp 96-102. ISBN13:97814910955, 2016.

[6] S. Sajeed, C. Minshull, N. Jain, V Makarov, “Invisible trojan-horse attack. Scientific Reports,'' vol 7(1, pp. 148-152), 2017.

[7] Adams, C, “Replay attack for the challenges in the network security tools and techniques,'' Springer 2011.

[8] Boudriga, Noureddine, “Security of mobile communications. Boca Raton: CRC Press,'' , pp. 32–33. ISBN 978-0849379420, 2010.

[9] McDowell, Mindi, “Understanding Hidden Threats: Rootkits and Botnets,'' US-CERT., pp. 146-153, February 2013

[10] Mary K. Pratt, “Intrusion detection system an IDS spots threats.2018.

[11] J. M. Stewart, D. Kinsey, “Network security, firewalls and VPNs,'' pp 347-349, 2020.