Firewall

Cristina Laing

Cybersecurity Principles

CYSE 600

August 6, 2021

Dr. George Mikulski

Author Note

This is my own work and has been done solely by me. This paper has been written for the Old Dominion University's CYSE 600 Cybersecurity Principles class and not used for any other purposes.

Cristina Laing

Abstract

This paper analyzes two firewall research papers: Denial of Firewalling Attacks (DoF): The Case Study of the Emerging BlackNurse Attack and Online meta-learning firewall to prevent phishing attacks. The content of each paper will be summarized and further explained for better understanding. Limitations, challenges, and difficulties faced by the research will be stated and further explained. Key themes shared by both papers will also be discussed. The authors' conclusions will be compared and reviewed; further research recommended.

Firewall

Introduction

What is a firewall? A firewall is a network security tool that monitors and controls both incoming and outgoing network traffic based on a list of prearranged security rules. Functions of a firewall include:

- Establish a barrier between a trusted internal network and a non-trusted external network.
- Prevent unauthorized access to or from a private network.
- Software program that regulates traffic through port numbers and applications.
- Hardware is installed between a network and gateway.

The primary benefit of a firewall is that all traffic that comes in and goes out is monitored. Monitoring is helpful against cyber-attacks because it prevents harmful connections. A firewall is also useful when there is a need for digital forensic investigations; firewall logs may pinpoint the time and date a breach occurred.

Not all firewalls are the same; as mentioned above, some firewalls come as software programs and others as hardware. Additionally, there are different services a firewall can accomplish depending on the type. Below is a list of types of firewalls:

- Packet filtering firewall
- The most common and basic firewall examines packets.
- Next-generation firewall

- Combination of packet filtering firewall, deep packet inspection, and intrusion prevention/detection systems.
- Proxy firewall
- Detects malicious data at the application level.
- Network address translation firewall
- It hides IP addresses and acts as an intermediary between a private network and a public network.
- Stateful multilayer inspection firewall
- Examines packets to make sure they are coming from trusted sources.

Literature Review

The popularity of the internet has led to the increased complexity of threats that thrive in an ever-changing environment. The need for a security tool to guard assets and to prevent disruptions is understood by all. However, as the arms race between attackers and those who seek to defend themselves from attacks is ever-evolving, so should the security tools. Unfortunately, traditional security tools and their technology fall behind and can often fail to detect serious threats. That is why a new era of research has emerged, research that seeks to take traditional security tools and bring them to the present day by incorporating machine learning and meta-learning.

In the paper by Zhu, Online meta-learning firewall to prevent phishing attacks, research proposes the online meta-learning firewall to prevent phishing attacks. The author explains that phishing attacks are well-known attacks that take advantage of human psychology and emotion to secure data access. The author states that technology and human emotion should not be related

or influenced by one another. Through social engineering, it is possible to influence an unsuspecting user to help in a breach. Therefore, the author suggests counteracting phishing attacks with firewalls outfitted with self-adjusting memory algorithms or meta-learning algorithms. In other words, creating firewalls that learn about learning the purpose of the system is to understand the nature of an unknown situation and classify it based on the most relevant characteristics that come directly from the unknown environment.

Trabelsi et al., research warns of attacks on firewalls like attacks on networks, Denial of Firewalling (DoF) attacks like Distributed Denial of Service (DDoS) attacks. In specific, the research paper explores the DoF called the BlackNurse attack. The BlackNurse attack takes advantage of Internet Control Message Protocol (ICMP) messages to degrade firewall performance. The BlackNurse attack consumes the targeted firewall's Central Processing Unit (CPU) to a point where the firewall becomes completely unresponsive, leaving the network it protects open for attack or cutoff (Trabelsi et al., 2019). The authors propose a rule with a dynamic time-to-defend duration estimated based on current and historical attack statics and severity parameters. In other words, firewall rules that are in constant change, active, and learning to better detect early on BlackNurse attacks.

Discussion

Key themes found in both papers are firewalls, firewall rules, vulnerabilities in firewalls, machine learning, and meta-learning. The authors realize there are gaps and limitations to firewalls in the present state; even though firewalls have significantly advanced throughout the years, they still can improve further. Both phishing and DoF attacks are challenging to detect because one targets the user, and the other is a slow, lengthy process that appears like regular

activity to a firewall. The research for both papers did run into challenges and limitations, mainly concerning the configuration, and preserving of firewall and their rules by IT and security professionals. Trabelsi et al. state that the purpose mitigation solution for BlackNurse attacks mainly involves detecting the attack yet defending from the attack in a time frame has not been done yet.

In contrast, Zhu's research also acknowledges difficulties to their proposed meta-learning firewall solution. They were pointing out that some attackers or malicious users themselves can obtain authentic certificates of authenticity. In addition, the system proposed needs continued optimization of parameters for a more efficient, accurate, and faster classification process.

Summary

Firewalls are essential security tools in today's interconnected world. Firewalls are imperfect and can be susceptible to some of the same attacks as networks. However, installing and maintaining a firewall is critical, and deploying multiple firewalls with different security services is better. Administrators and computer professionals in charge of firewall rules and logs need to keep up to date on attacks and advances in firewall technology. The two research papers analyzed here look to mitigate different issues concerning firewalls by using machine learning and meta-learning. All authors emphasize the continued research around firewalls and dynamic algorithms. Overall, the fundamental purpose of both research is faster detection of attacks to a system and firewall immunity.

References

Trabelsi, Zouheir, Zeidan, Safaa, & Hayawi, Kadhim. (2019). Denial of Firewalling Attacks (DoF): The Case Study of the Emerging BlackNurse Attack. IEEE Access, 7, 61596-61609.

Zhu, Hongpeng. (2020). Online meta-learning firewall to prevent phishing attacks. Neural Computing & Applications, 32(23), 17137-17147.