An Analysis of Network Defensive Techniques Towards Organisational Security

Attlee M. Gamundani [1], Andreas Joseph[2]

[1]Lecturer, Computer Science Department, Namibia University of Science and Technology Windhoek, Namibia, E-mail: *agamundani@nust.na*

[2]Chief System Administrator, Division of Information Technology Services, Ministry of Agriculture, Water and Forestry, Windhoek, Namibia, E-mail: *josephA@mawf.gov.na*

Abstract: Network security is by far among the critical components any organization are in this technological age forced to invest in. The need to protect and secure corporate data and information is equally critical as protecting the organization's reputation to retain effective business presence. It is very important for an organization to make sure that all the defensive mechanisms put in place are indeed effective, hence the need to carry out vulnerability and penetration assessment. This research employed a case study approach, where a particular organization network was assessed to inform the position of this paper. Data was collected using open source vulnerability and penetration tools, which were analyzed to verify the presence of network threats in the selected network setup. The results of data analysis indicated the presence of vulnerability and attacks from outside with an attempt to compromise the network resources. It was noted that, the defensive techniques applied to this particular network, were mainly firewalls and antiviruses. As a recommendation from the findings of this research, the need to perform penetration testing and hardening an organization's networks is critically important.

Keywords: Defensive, Firewall, Network, Security, and Vulnerabilities.

I. INTRODUCTION

Investment into network security is no longer a second thought, as the growth and vulnerabilities thrive under Internet enabled platforms, as by nature the Internet was never built to be secure but advance communication [1]. The need to protect the organization's information as well as data is critically important, as any loss or access gained to such valuable organizational assets will compromise the competitive position of any business's operations. Henceforth, the need to protect the organizational network against malicious activities and attacks has to be considered from all angles [2].

A look at the conventional network defensive tools such as the popular antivirus solutions and intrusion detection tools will reveal that, their main thrust is on vulnerability curbing and the task of intrusion detection becomes limited as their functionality become limited. The use of proxy network settings in organizations has seen the implementation of firewalls as a first line of defense for Internet attacks as depicted by a model in figure 1. Some of the efforts towards network security are the development and upgrading of Internet communication protocols [3]. The domain of network security is becoming big and very broad a subject and the dimensions to consider are becoming diverse especially as new communication pathways are growing like the Internet of Things (IoT) networks where billions and billions of gadgets are capable of being interconnected [4].

Given an organizational setup that the concept of Bring Your Own Device (BYOD) is growing, indeed the source of threats to network security becomes multiplied. Network and computer users have been identified to be the weakest link in network security because of manipulations [5]. With the growth of social networks, computer networks can easily be attacked with information gained from these social interactions [6]. Network attacks does not only compromise systems and data but also affect the network bandwidth [7]. SYN flood and ICMP flood are some of the classic example of protocols-based bandwidth attacks [8]. Apart from SYN and ICMP, there are also some common network attacks such as reconnaissance, access, denial-of-service (DoS) and data manipulation attacks [9].

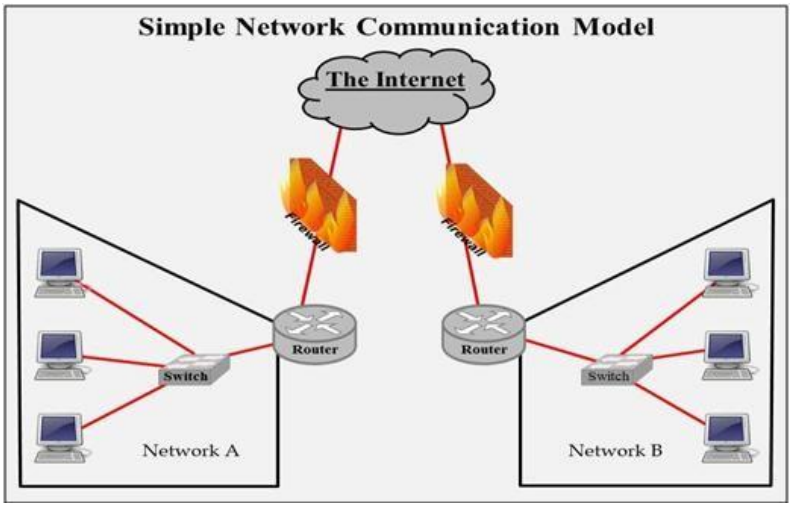

Figure 1: Network Communication Model

DoS attack is very severe and critical attack where a network resources are flooded with requests which it cannot handle, causing network resources to be unavailable to the intended users. Figure 2 is a clear representation of the severity of DoS as an attack. Despite several efforts to try and find solutions to network threats and attacks [10], the efforts by many researchers and security designers are indeed appearing futile as intruders are equally working hard to subvert some of those solutions [11]. As a result, network security becomes an ongoing concern and demands constant improvement within an organization.

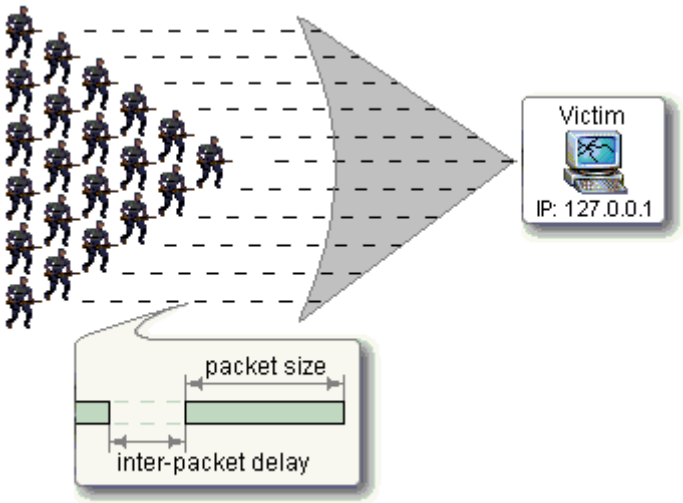

Figure 2: DoS attack representation [12]

One of the pro-active approaches to combat network threats is to have proper intrusion detection systems in place. This will help to detect the attempt as well as malicious activities on the network. Network firewalls still remain the most essential component of network as a line of first defense towards ensuring network security, especially those summarized in Figure 3.

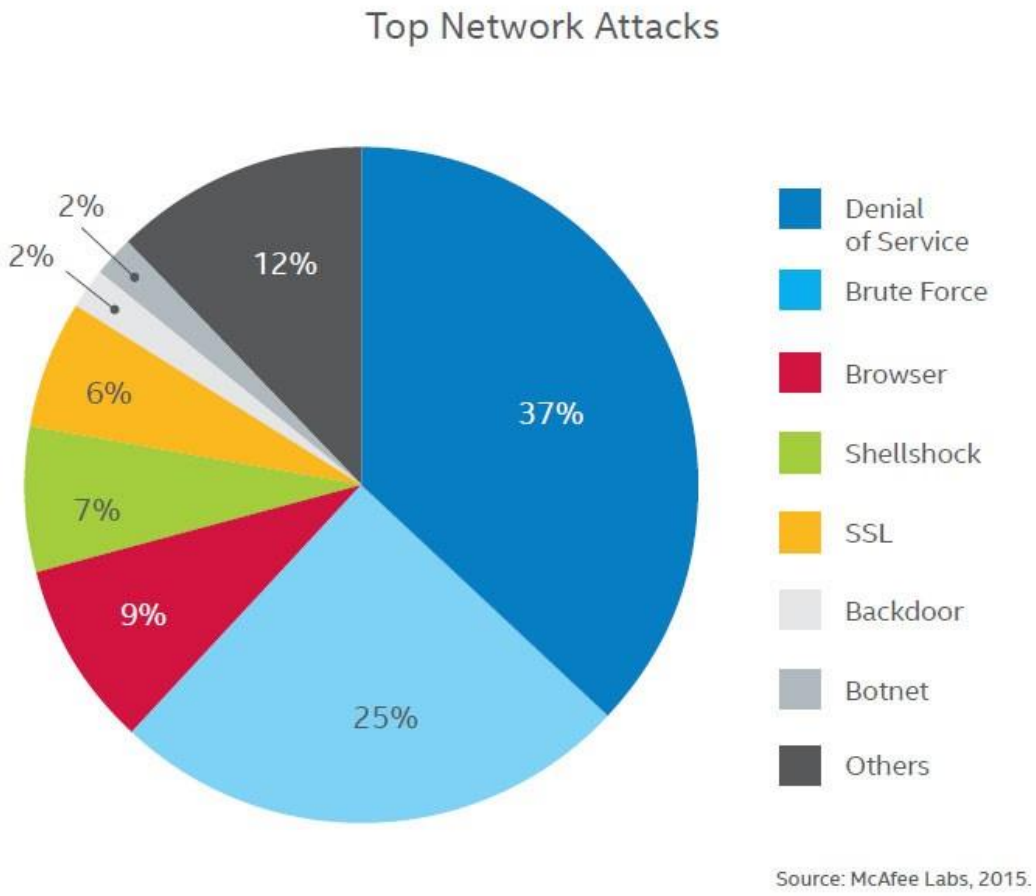

Figure 3: Classified network attacks [13]

II. MOTIVATION FOR THE RESEARCH

The noted driving force behind any intrusion to a given network is the desire to steal information which can be achieved by first destabilizing the organizational network which gives them maximum control of their target network. Network vulnerability therefore can be said to be proportionally equivalent to the strength required for any proposed defensive techniques to be applied to any network. Research has it that, the main obstacle facing organizations is the challenge of deploying of suitable network defensive tools as well as lack of understanding of different types of network attacks to their networks.

In this research, the attempt is to find out how effective some of the network defensive techniques are in terms of organizational network and information protection was the main thrust. The main question that was central to this research was whether the current deployed defensive techniques, effective enough to protect an organizational network?

III. METHODOLOGY

This research made use of secondary data as well as primary data collected from operational networks: (A case study of one of the Government institution of the Republic of Namibia) and some few selected networks. A limited network vulnerability testing and network scanning was carried out in this research to identify some vulnerability in some of the Government institutional networks. Intruder's attempt in this network was recorded and information gathered from network scanning was analyzed. Network setup and topology was used in this research as it played a role in the effectiveness of the defensive mechanism deployed. For result analysis, a footprint was used to trace back the originality of the intruders detected in the sampled networks. One of the online tools used was IP figure print, which was used to trace the origin of particular intruders.

IV. RELATED WORK

As stated by [14], there is need to invest and consider cyber security as equally an operational unit of an organization that demand equal attention especially vulnerability assessments for solid network security. As postulated by [15], the growth of network communication as witnessed with Internet's borderless communications has spurred the need to focus on collaborative applications that focus on trust and reputation of the connections being propagated. As emphasized by [15], vulnerability testing should be holistic in nature, covering even network topology and many components that directly and indirectly affect the network operation. As clearly pointed by [16] the fact that security will never be 100% perfect, clearly indicate the need to continuously refine existing and new solutions.

One of the hardest threats to overcome in todays' Internet is a Distributed Denial of Services (DDoS) whose impact can be proportionally severe on any network [17 & 18]. The assertions that network security continue to increasingly gain attention due to the growth of Internet. On the contrary, it is noted that security technologies are software based whereas hardware is commonly used in some of the attacks being perpetrated to organizational networks. The use of security tools like firewalls, intrusion detective systems and authentications will prove effective in guarding intellectual properties for the foreseeable future. [17] on the other hand have expressed the importance of network firewall as not just a perimeter device for data center, but must be merged into the fabric of the organization's network from end to end in order to offer is comprehensive encapsulated security layer. It is further suggested by [19] that there is need for firewall evolutions that complement set policies for security with performance and rapid scaling for high security.

The field of network security has seen a significant attention based on the previous research. It was concluded in most cases that, there will be no completely secure network in the world and as the high security is achieved, bad guys (Hackers) are also hard at work trying to find ways into organizational networks [20]. Hence, there is need to invest in network security and implement effective network defensive mechanisms.

V. RESULTS AND ANALYSIS

Due to the expansion and growth of network security threats, security managers need to constantly monitor their network by collecting information from their networks using network scanners and vulnerability testing tools. This information collection and gathering need to be analyzed to determine and pin point vulnerabilities in the network. It was however noticed that, all networks scanned for vulnerabilities had IPv4 protocol which date back to the 1970s. Different types of testing tools need to be used in order to get as much information as possible. Each tool can possibly collect different

information such as: number of TCP connections to one given host; live IP addresses on the network with the corresponding device name and MAC address; all the ports which are open on each device as well as applications running. For the purpose of this research, the data and information collected were interpreted and analyzed based hence informs the results presented here.

A. Firewall intrusion detection system

Part of the data collection and gathering exercise, was to obtain data and statistics from security devices on the network. This data was collected from Microsoft Threat Management Gateway (MTMG) software firewall as well as from Fortinet / Fortigate 500 Hardware/Software firewall. These are the critical devices in any network setup as they filter the traffic from and to a private local area network (LAN); these devices detect intrusion from the network and take action based on the rules defined.

Based on the results, one of the computers in the network was sending too much HTTP requests. This is a sign of malicious attack, which had infected the computer within LAN network, and it was trying to send too much traffic back to the outside network. The other conclusion that can be drawn from the results is the number of TCP connections a particular computer was trying to establish. The results show that, the number of TCP connections per minute was exceeded by one of the client computer. These findings suggest the possible attacks may not easily be visible till a tougher investigation is conducted. One of the critical evidence of network attack in the results obtained is the number of intruders detected. There are numbers of outside IP addresses that were trying to access the local network. During data collection, some of the results lead to further investigations, which traced the origin of some of the intruders, as indicated in figure 4 and figure 5.

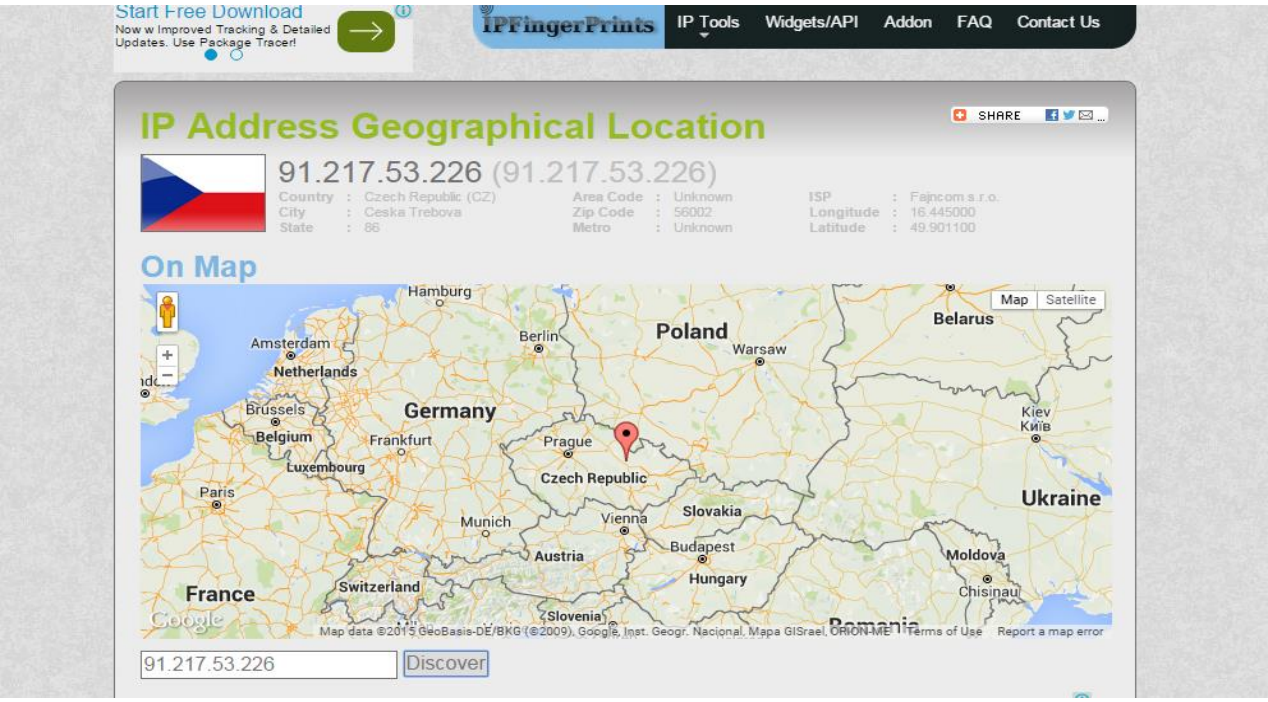

Figure 4: Network attack from Czech

Figure 5: Network attack from China

The other evidence of intruders from the results is the instant logon failures were also noted. This result indicates that, there was login attempt almost every five minutes. These attempts cannot be regarded as successful attacks as they clearly indicate that was "logon attempt failed". The other useful data was captured from the bandwidth usage as could be noted from Internet daily, weekly, monthly usage statistics.

VI. CONCLUSION

In conclusion, the research was chiefly informed by review of literature as well as results obtained from the case study site, which strongly indicate the importance of network security and the emphasis to make it the first priority. The defensive policies and techniques deployed in any network need to be constantly updated and adjusted to respond to modern network threats. Threats to the network security were based on the objectives of the intruders and their interest on what they can get from your network in terms of data and information. The overall conclusion, which can be drawn from this research, is the fact that, the more the business world interacts with one another in terms of information sharing and the use of social medias, there will be no end to network and Internet based threats. Hence, the need to continue exploring new types of network defensive techniques based on the current threats in order to protect the organizational data and information.

VII. RECOMMENDATIONS

Due to continuous and new emerging threats, the study therefore recommends based on the findings the followings.

1. The importance to carry out a penetration testing and vulnerability assessment more frequently as a proactive measure to new threats. There is need to adjust defensive mechanisms to the current threats by either updating the security rules, policies, etc.

2. Most intruders take advantage of some open ports, which are left open either as default settings. Different vulnerability and penetration testing tools can be used to determine the possible threats present in network. The need to harden the organizational networks becomes critical.

3. User awareness campaigns inside organizations are critical as some of the threats thrive because of the human element.

ACKNOWLEDGMENT

All the support rendered from all the units at Namibia University of Science and Technology for the successful completion of this research. A special recognition of the Digital Forensics and Information Security research cluster for nurturing the research culture and all the financial support.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical statement: The authors declare that they have followed ethical responsibilities

REFERENCES

[1] Handley, M. (2006). Why the Internet only just works. BT Technology Journal, 24(3), 119-129.
[2] Liu, D., Ning, P., & Du, W. K. (2005, April). Attack-resistant location estimation in sensor networks. In Proceedings of the 4th international symposium on Information processing in sensor networks (p. 13). IEEE Press.
[3] Birman, K. P. (1997, March). Building secure and reliable network applications. In International Conference on Worldwide Computing and Its Applications (pp. 15-28). Springer Berlin Heidelberg.
[4] Gamundani, A. M. (2015, May). An impact review on internet of things attacks. In Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on (pp. 114-118). IEEE.
[5] Arce, I. (2003). The weakest link revisited [information security]. IEEE Security & Privacy, 1(2), 72-76.
[6] Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of Information: The case of Privacy and Security in Social Media. In Proc. of the History of Information Conference (pp. 283-310).
[7] Ioannidis, J., & Bellovin, S. M. (2002, February). Implementing Pushback: Router-Based Defense Against DDoS Attacks. In NDSS.
[8] Vuong, S., & Bai, Y. (2004, February). A survey of VoIP intrusions and intrusion detection systems. In 6th International Conference on Advanced Communication Technology.
[9] Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31-43.
[10] Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8), 805-822.
[11] Bhattasali, T., & Chaki, R. (2011, July). A survey of recent intrusion detection systems for wireless sensor network. In International Conference on Network Security and Applications (pp. 268-280). Springer Berlin Heidelberg.
[12] http://www.kalitutorials.net/2014/04/denial-of-service-methods-icmp-syn.html
[13] Gangan, S. (2015). A review of man-in-the-middle attacks. arXiv preprint arXiv:1504.02115.
[14] Phillips, C., & Swiler, L. P. (1998, January). A graph-based system for network-vulnerability analysis. In Proceedings of the 1998 workshop on New security paradigms (pp. 71-79). ACM.

[15] Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. ACM Computing Surveys (CSUR), 42(1), 1.
[16] Atighetchi, M., Pal, P., Webber, F., & Jones, C. (2003, May). Adaptive use of network-centric mechanisms in cyber-defense. In Object-Oriented Real-Time Distributed Computing, 2003. Sixth IEEE International Symposium on (pp. 183-192). IEEE.
[17] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 44(5), 643-666.
[18] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.
[19] Sheth, C., & Thakker, R. (2011, February). Performance evaluation and comparative analysis of network firewalls. In Devices and Communications (ICDeCom), 2011 International Conference on (pp. 1-5). IEEE.
[20] Stallings, W., & Brown, L. (2008). Computer security. Principles and Practice.

