Introduction to Packet Capture and Intrusion Detection/Prevention Systems

Malicious Network Activity Report

Introduction

Information technology has evolved into one of the critical aspects of the modern organizational structure. Today, enterprises use different systems and techniques to improve the effectiveness and efficiency of workers (Hassan, Ahsan, & Rahman, 2012). In addition, the networks have enhanced different processes and actions that contribute to the meeting of the specific needs of customers. However, there is a wide range of risks that are associated with the use of technology including an cyber attacks and misuse of employees. In some instances, workers access the internet for purposes not related to work using the existing organization's workstation.

These actions can expose the enterprise to risks and affect the security and efficiency of the entire systems (Gandhi, Suri, Golyan, Saxena, & Saxena, 2014). In other cases, the networks are exposed to problems like malware, injection of spyware, and different types of attacks (Gandhi et al., 2014). The occurrence of these events may adversely affect the operations of an enterprise. In the financial sector, for instance, it can lead to loss of funds and delay essential transactions. In the long run, the impact of these attacks and intrusions may be noticeable in one sector and the whole country.

When network performance issues and attacks occur, it is not strange to find employees and relevant authorities pointing fingers at each other. The IT team may blame workers while the managers may direct their fingers towards those tasked with managing the systems. Therefore, the best method to deal with the challenge and avoid its adverse effects on productivity and performance is to improve network monitoring methods and processes. The process entails looking at the packets that are either sent or received in the network to guarantee its security and efficiency. The idea behind network monitoring is that most problems that affect IT systems start at the packet level (Kaur & Saluja, 2014).

Thus, packet analysis can play a crucial role in ensuring that an organization's IT system is kept safe at all times. The network analysis entails collecting raw binary data from the wire and converting it into a readable form that can be analyzed. The analysis is critical in investigating and detecting errors and bugs while also checking the efficacy of the network (Chappell, 2012). This report presents the evidence of the analysis that was done on the interfaces belonging to one of the banks in the United States that had been experiencing risks of intrusion and attacks. Besides, the reports highlight the primary weaknesses in the network that may have contributed to the problem that is currently faced by some of the organizations in the financial sector.

Network Architecture Overview

The events that have been reported in the US over the recent years show that networks systems are always at risk of attack from different people including cybercriminals. The effects of the intrusions can be catastrophic if not properly managed (Chappell, 2012). For this reason banks have taken it upon themselves to come up with systems and interventions that can be used to prevent and monitor potential threats (Chappell, 2012). The process of monitoring and analysis network traffic usually allows an organization to differentiate the legitimate data exchanges from those that may harm the system. It is upon the network administrators to fortify the systems so that they can prevent unwarranted access through the use of different tools and techniques (Chappell, 2012). However, for many enterprises the biggest challenges is to keeping up with the technological changes that influence the ability of the system to detect and prevent malicious activity. The bank whose system forms the basis of this particular report has been facing a growing number of cases of cyber-attacks coming in different forms such as data exfiltration and intrusions in the given period

of time. Likewise, it may be the case with any other financial institutions because such interventions may have far-reaching effect on the operations of the bank, customers, and the economy of the nation. Thus, it was prudent to carefully analyze the mechanism that the organization used to monitor its systems and determine the possible reasons for the rising cases of cyber-attacks.

The bank under review in this report utilizes Wireshark as its packet analyzer. This open-source tool uses cross-platform structure to protect systems and networks from intrusions and attacks. It can run on the Microsoft Windows and other operating systems such as Mac OS, BSD, and Linux. Wireshark uses the GTK+ widget to implement a user-friendly interface that is compatible with a wide range of computer systems and networks (Tanenbaum & Wetherall, 2011). In the selected bank, Wireshark is used to capture and carefully filter live data traffic, create input/output graphs and statistics, and color packets based on protocols. In addition, the analyzer can export packet data in various file formats, follow names, and provide expert information on the operations and effectiveness of the system. The Wireshark platform used by the bank has a graphical user interface (GUI) that is easy to use (Orzach, 2013). Besides, The GUI simplifies and speeds up the process of analyzing packet data while also supporting a wide range of protocols. The figure below sets out the architecture of Wireshark resource that the bank users carry out network monitoring and analysis.

Figure 1. System used by the bank.

From the figure above, it is evident that the network adopted by the bank is made up of two primary components located at the left and right-hand side of the architecture. The first part, found on the right-hand side of the diagram, is made up of the internet protocols and applications that are run on the computers. The User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are among the components making up the first part of the architecture. The UDP is a protocol that uses simple but effective connectionless transmissions models to provide a checksum for data security and integrity. Since it does not engage in handshaking dialogues, the UDP can expose any unreliability found in the network to the user program.

Another vital feature of the UDP is that its transaction-based nature makes it suitable for using in query-response protocols and for bootstrapping functions within the analyzer. In contrast, TCP offers a reliable communication challenge between two different ends to facilitate the safe delivery of data. The protocol supports the sequencing and error management and control processes in the analyzer. Furthermore, it transports data to the desired destination without causing the dropping or misplacement of the packet information.

The other components in the first section of the architecture are the internet protocol (IP), internet packets, and other physical components such as the ports (Ben-Eid, 2015). The IP is a layer three protocol that facilitates the process of internetwork exchange of data. The bank uses the IPv4 version that allows the analyzer to transfer data between different devices irrespective of the location or the network complexity. The internet packets, on the other hand, are the packaged messages and communicative information that is transmitted from one point to the other through protocols like TCP and IP. The packets make the transmission of information and data within the network faster (Ben-Eid, 2015). The exchange packaged data occur through multiple points that also function as the standard connection devices. When the internet packets get to one port in the hub, it is sent to other different ports in the form of broadcast traffic. Therefore, the analyzer can examine and monitor all devices that are connected to the system.

The second part of the system is the packet sniffer that shows the content of the different fields found in the protocol communications. This part of the network understands the composition and structures of the messages that are exchanged across the protocols (Kumar & Yadav, 2015). The packet analyzer understands the format and functioning of the Ethernet frames as well as the contracts so that it can accurately identify IP datagrams. Besides, the understanding of the IP datagram allows it to successfully extract the TCP sections in the datagram (Orebaugh, 2013). Therefore, it is evident that both parts of the architecture work together to facilitate the successful exchange of information. Furthermore, the two sections allow for the accurate and carefully monitoring of communicative data within the bank's networks.

Network Traffic Monitoring and Results

Banks are exposed to a wide range of cyber attacks that can compromise their operations and causes losses to the customers. Therefore, it might be challenging to monitor and deflect these interventions. The current research performed on the client's system revealed that the attempted attacks fall into three primary categories. The first category is those that are launched by the financially motivated cybercriminals (Ben-Eid, 2015). These are individuals who strive to compromise the system to carry out an electronic theft or fraud. The second group is the politically motivated criminals whose primary goal is to achieve a shared purpose within their grouping. The third category is the espionage attackers (Gandhi et al., 2014). These individuals launch their attacks with the objective of stealing personal data and information and selling it to a third party. The system review shows that banks should always expect attacks from all these groups (Gandhi et al., 2014). The implication is that financial institutions can only survive and effectively carry out their operations when they have a robust IT security system, information privacy capacity, and fraud detection and prevention methods. These interventions and systems will apply all possible means to protect the bank and its clients from the ill motives of the cyber attackers.

A review of the bank system and security architecture also revealed the nature of attacks that have been launched from the cyberspace. One of the common ones was the man in the middle attack where the attacker strived to control the network traffic, modified it and acts as the communication controller (Tanenbaum & Wetherall, 2011). This form of attack is not easy to detect and occurs when the criminal takes a strategic position between two hosts in the network. In such a case, the connection between the client and the web server may be compromised and the weak link used to access critical company information and data. Further investigations and analysis using a honeypot showed that the man in the middle attacks could be used to locate and steal important banking credentials, personal information, email addresses, passwords, and usernames. Since the attacker acts as a standard controller of the system, it becomes difficult for the client or the bank to detect any anomaly (Ben-Eid, 2015). Another form that was detected through the careful analysis of the system was the session hijacking. In this case, the criminal strives to use the existing sessions and connection between different network devices to carry out their illicit operations (Gandhi et al., 2014). This form of fraud usually occurs when the HTTP used by the bank is not a secure protocol. In such instances, the cookies that are stored or exchanged during connection gives the attackers a chance to access systems and steal vital data. These are common forms of an attack that organization must strive to prevent. Failure to come up with a security system and prevention methods will result in significant losses for the organization and its clients.

While testing security networks, the issue of false negative and false positive results often come up. These issues deals with the accuracy of the system and must be taken into account when deciding on better safety solutions and protection mechanisms (Gandhi et al., 2014). A false negative result occurs when the tests or the system fails to identify a threat that exists (Tanenbaum & Wetherall, 2011). A false positive, on the other hand, occurs when the results detect a vulnerability that does not exist. In the present case, the analysis revealed that a wide range of factors could cause false negatives. For instance, the hiding or suppressing of headers can lead to such outcomes. Other common causes include the faking of header information by the firewall, changes in the system version numbers, and loading of new updates (Ben-Eid, 2015). False positive results, on the other hand, occurs when a configuration setting prevent the detection of vulnerability or when a patch is applied in a manner that does not change the system version number. These are just some of the instances that were identified during the analysis. It is important to state that both false adverse and false positive outcomes can lead to catastrophic failures. They may allow attackers to access the network without being detected by the IT team. Thus, there should be attempts to improve the vulnerability

assessment capabilities of a network or system.

Recommended Remediation Strategies

Businesses usually face dangerous and analogous situations that may affect their operations and the security of client information. For companies which operate in the financial sector, the identification and possible prevention of risks is a priority. Despite this being the case, there are organizations that are underprepared to deal with the threats emanating from the cyberspace (Ben-Eli, 2015). In the current world, the cyberspace has become a dominant platform that allows organizations to carry out their duties while also exposing them to the acts of crime. The outcome is a damage to the organization's reputation, profits margins, and competitive advantage. Therefore, there is a need to come up with measures and methods for cyber-attacks mitigation.

Based on the outcomes of the analysis that was done to the bank's system, this report makes four essential recommendations that can be used to mitigate cyber threats. First, the bank should optimize its information security and IT networks. When selecting a security system or protocol, the organization should look into the issues such as confidentiality, provenance, accountability, integrity, and availability (Tanenbaum & Wetherall, 2011). Secondly, the organization should consider IT security to be one of the primary components of the risk management methods. Third, the bank should identify a system that will allow it to engage in real-time tracking of traffic and gathering of intelligence.This technology will be of great importance in terms of protection against internal and external cyber threats. Finally, it is crucial to develop a multi-layered security system that consists of dual authentication, secure login, and firewalls.

Joint Net Defense Bulletin

For Immediate Release

Financial Institutions Letter

August 2018

In the last few years, the world has continued to embrace technology in various sectors and use it to carry out a wide range of tasks. Today, organizations rely on technology in their operations and efforts to meet the specific needs of customers. Others rely on various innovations to achieve their short term and long term business goals. However, technology can also be a double-edged sword with far-reaching positive and negative outcomes. Recent reports show that organization in the financial sector have been exposed to a wide range of threats coming from the cyberspace. These attacks are launched by individuals who are motivated by different factors such as financial gains and the desire to access personal client information and data. Irrespective of the nature of the attack, the outcomes are often catastrophic for the specific organization and the financial sector as a whole. It is for this reason that the security apparatus and agencies in the country are always working with organizations to identify and understand the threats. Moreover, the agencies help the organizations in developing mechanism and methods for thwarting the attacks.

The purpose of this joint statement is to help organizations operating in the financial sector to deal with some of the major threats that they face today. A recent investigation by the security experts revealed that the systems and networks used by some banks and financial organizations are prone to different kinds of attacks such as the man in the middle and session hijacking. These attacks can negatively affect the normal operations of the enterprise and compromise the confidentiality of customer data and information. Besides, it can adversely affect the competitive position of the enterprise in the market.

In recent years, the incidences of cyber attacks have gone up. In addition, the country has witnessed multiple cyber crimes that can cripple the financial sector when not managed. Therefore, there is a need to embrace interventions that will lead to a secure industry and to protect the organization and their clients from the acts of cybercriminals. Organizations operating in the financial sector must understand that they are vulnerable to different types of attacks. Furthermore, they must know their responsibility when it comes to protecting their systems, networks, and customers.

To this end, we recommend that bans should take the following measures to improve the security of their operations.

- Optimize its information security and IT networks in terms of confidentiality, provenance, accountability, integrity, and availability

- Make information technology security a priority area in the risk management efforts

- Engage in real-time tracking of traffic and gathering of intelligence

- Develop and implement a multi-layer security system

The above recommendations can help in reversing the trend that is currently being witnessed in organizations.

However, the management must work with the rest of the workforce to facilitate the successful implementation of the recommendations. Cyber threats are constantly evolving, and organization must remain proactive in the fight against the menace. Therefore, banks that find signs of such malicious acts and activities should report to the FBI through the field offices or CyWatch. All in all, the reports can be sent to the National Cybersecurity and Communications Integration Center so that the issues can be investigated and managed.