Network Penetration and Testing in a Rural Banking Environment in Ghana

1st Wellington Amponsah,
dept of Computer Science and Engineering
Shaheed Udham Singh College of Engineering and Technology Tangori
Mohali, India

2nd Simon Amonovi
dept of Electrical and Engineering
Koforidua Technical University
Koforidua, Ghana

3rd Kwabena Gyeke-Lartey
Dept. of Computer Science
KNUST, Kumasi

4th Taiwo E. Ajagunsegun
Dept. of CSE
Shaheed Udham Singh College of Engineering and Technology Tangori
Mohali, India

Abstract:- Ghana's Banking sector has seen much improvement and this is evidence by the establishment of Commercial Banks, Rural and Community Banks and Savings and Loans. Cyber-threats and the measures necessary to counter them in the Banking industry are the major security issue of the hour that the bank is facing. Information security issue is vital and more critical when it wants to implement and apply IT into its operations. Penetration and testing uses and techniques those hackers employ in penetrating the network system to verify presence of vulnerabilities in the network. This research demonstrates how to perform and identify the security strength and reveal the vulnerabilities, and possible exploits in the security of the internal network and misconfiguration of firewall of the Bank using penetration testing.

Keywords:- *Network Security, Cyber Security, Penetration And Testing, Virtual Private Network.*

I. INTRODUCTION

The Banking sector of the country has witnessed much improvement. This improvement has brought the numerous commercial Banks, Rural and Community Banks (RCBs) and Savings and Loans. The Rural and Community Banks (RCBs) were first established in Ghana in 1976 to provide banking services to the rural population to provide credit to small-scale farmers and businesses and also support development projects in the rural communities. The RCB Banks are locally owned and managed [1]. In 1981 about 30 existing RCBs formed the Association of Rural Banks (ARB) to serve as a networking forum and as a network of institutions sharing a common mission, the ARB promoted and represented the RCBs and also provided training services to member RCBs [1]. [1][2]The Rural and Community Banks are supervised by the clearing ARB Apex Bank under the regulation of the Bank of Ghana, which owns shares in the Banks. According to [3] the country currently has 144 Rural and Community Banks across the country with their respective branches spread across the country. [4][5] Rural Bank is a unit bank which is a limited liability under the Ghana Company's Act which can be defined as rural financial institution/cooperative/ community bank which is to mobilize savings that provide customized financial services to rural communities within its area of operation.

Technology has become the main driving tool for our national development and now applied in all forms of our lives. This technology is applied in the financial field, health sector, educational sector, etc. Data protection and providing security to data is one of the major challenges facing the industry. In the Banking industries network and data security is one of the challenges affecting the industry.

Ghana is now maturing in the field of cyber security and this has been described by World Bank in collaboration with the Global Cyber Security Capacity Centre (GCSCC) as being at the formative level. A finding from the assessment is evidenced in the implementation of a number of initiatives including the formal adoption of a National Cyber Security Policy & Strategy (NCSPS) in 2016, and the National Cybersecurity Institutional Framework (NCIF). In addition, a National Cybersecurity Advisor was appointed to coordinate cybersecurity issues in government and across non-governmental sectors.

The use of the internet in Ghana is experiencing huge patronage. It is now being used in most of our institutions to enhance operations of their activities and service provision. In the Ghanaian banking industry, Information technology has now been recognized as the life wire of the Banks since it simplifies and supports the performance which has made it very demanding of the Banks to adopt in full Information Technology in her operation for customer satisfactions and the reputation and performance the financial market. And this demands for a high network and information security in the banking services to protect and secures its systems to maintain information vital to its operations.

II. PROBLEM STATEMENT

Information security issue is vital and more critical when it wants to implement and apply IT into its operations. The demand for the application of information communication and technology in the banks is to create more business and ease of operations. Inadequate security measures and insecure network of the Bank affect the beliefs of customers and their ability and wiliness to transact any kind of transaction or business with the Bank. And it is a major threat to the growth of the banks in the country as a whole. The security of customer information is very vital information that is treated as a valuable. Hackers with information about the network of the Bank, staff information and even customer information can perform many transactions in the name of these staff and customers. Some information which can be stolen includes their date of birth, social security number, tax identification numbers, address, staff login details, etc.

Cyber-threats and the measures necessary to counter them in the Banking industry are the major security issue of the hour that the bank is facing. This is because there have been a number of attacks on the various networks in the various Banks which are done in an organized and in a very dangerous way and this calls for a serious attention and considerations.

Priority and attention have not been given to security of the information system of the bank. Hacking attacks on Bank's network in Ghana recent days has increased drastically in a very sophisticated manner. The attacks on the bank's information system have become more frequent in a well-organized and a more dangerous way. Protecting the digital assets of the bank has not been a priority or concern and the access of this information by hackers will affect the reputations and also compromises intellectual property of the Bank.

This is because ports on the network have been left open since they really on firewalls or have no knowledge about the various ports that are opened on the network. These ports that are opened are being scanned by hackers and also exploits for vulnerabilities which are the means of locating and identifying specific weaknesses in the network of the bank and services that are being run. The Bank becomes vulnerable to hacking because they do not employ secure information security systems, as well as intrusion and detection systems to protect their data.

IT staff of the bank have no knowledge or background in security and few checks of the various vacancies declared by the banks in the country only requested for people with BSc/HND Computer science, IT, MIS, MBA background. None of the RCBs has a staff dedicated to cyber security or network security to handle security issues of the bank.

Technologies are constantly evolving and growing, at a rate that is so rapid that one can have a difficult time keeping up. Antivirus that is aimed at protecting one computer is often found to be out of date. Most of the RCBs use free and outdated VPN.

III. OBJECTIVE

This research is to show how to perform and identify the security strength and reveal the vulnerabilities, loopholes and the possible exploits in the security of the internal network and misconfiguration of firewall of the Bank using penetration testing techniques approach. This will enable identify security flaws, to understand the level of risk and vulnerabilities and exploits to secure the network. To obtain important data from intruders such as hackers, who may have unauthorized access to the application and exploit the network to access sensitive information if any kind of vulnerability is identified. It is to also provide evidence for the support to increase investments in the security personnel and technology.

IV. ABOUT THE AKUAPEM RURAL BANK

Akuapem Rural Bank was established in 1980 for helping the rural dwellers. The Bank was awarded 64th position in the Ghana Investment Promotion Centre (GIPC) Ghana club 100 awards. The bank also won the maiden Association of Rural banks awards for the best Eastern region RCB. The goal of the Bank is to become the best Rural Bank in Ghana and has its corporate values Honesty, responsibility, dependability, and motivation. As part of government policy, the Bank has the main data center at Apex Bank. However, the bank also has its own internal Data center which is linked to the main data center at Apex Bank. The Bank has an application called Jboss services deployed on its server and other branches. The Bank's data center is connected to the Apex Bank data center through Wide Area Network and the communication channel is through Multiple Layer Switching (MPLS) radio and Very Small Aperture Terminal (VSAT). The Bank uses wireless communication across all the offices and its surroundings. Customer can access online account balances by the use of U-connect application we can be downloaded from google play store. Bank does most of the network and system security with regards to storage and WAN. The SUSU application is developed by the bank. The network is connecting through Comsys Ghana as ISP to Apex Bank. Comsys provide Data communication and internet communication. The Data center connects to Apex for its banking application and other auxiliaries' product whiles the internet connects to the outside world.

V. LIMITATION OF THE STUDIY

As part of this research, the objective is to present how network penetration testing of the Bank can be done. The penetration testing procedure shall not involve attacking the Bank's network structure and security system. This is only to help IT staff to be able to understand and undertake penetration and testing of the network in a banking environment. It will help obtain knowledge to secure the network of the bank and to adopt network penetration and testing approach to identify vulnerabilities in the system.

VI. NETWORK SECURITY

[6]It is the monitoring of network and preventing unauthorized use of network resources. The security tasks are managed by the network administrator. These include policies and practices which are adopted to prevent and monitor unauthorized access to the network, misuse of network resources and their modification, denial of a computer service on the network and network-accessible resource. It protects the usability and integrity of your network and data. Network security includes both the hardware and the software technologies.

Effective network security manages access to the network and targets a variety of threats and stops them from entering or spreading on the network. Network security combines multiple layers of defenses at the entry point to the network and in the network. Each of the layers implements policies and controls. It provides Authorized users with access to the network resource and block malicious actors from carrying out exploits and threats.

VII. CYBER SECURITY

[7]It is the process whereby you protect yourself online, as well as your entire online presence. The means of protecting yourself on the internet involve the installation of current and updated antivirus on the computers, the use of virtual private network (VPN). It also includes day-to-day activities as protecting your password, email details, passwords of users, amongst others. The essence of knowledge in cyber security is to protect the individuals in the bank, computers, networks, programs, and data from unauthorized access to banking information. Cyber security does not take a one-size-fit all approach. What works for one computer system may not necessarily provide full protection to another. Technologies are constantly evolving and growing, at a rate that is so rapid that one can have a difficult time keeping up. Antivirus software that may have protected an older computer that you had five years ago may not protect you adequately on the computer that you have now. An encryption program or VPN that promises to keep you safe online may leave you exposed to undetected threats, possibly those originating in other countries.

VIII. PENETRATION AND TESTING

Penetration testing refers to the testing of a network system, cyber system, or application to detect weaknesses that may be exploited by a malicious hacker. The term "penetration testing" refers to testing the security of a computer system and/or software application by attempting to compromise its security, and in particular the security of the underlying operating system and network component configurations. According to [ken] the de facto stewardship of penetration testing tools and processes by IT Security organizations is significant which has afforded IT Security people with the opportunity to test a computer and application's configurations from afar, as a sort of independent audit function. During penetration and Testing, one is essentially trying to gain access to a system without having any usernames or passwords or the credentials of the system and obtain vital inform. The aim is to see how easily it will be for one to obtain confidential information about an organization, and then increase the security of the network system or the information security system that is being tested. In simple words, penetration testing, also known as pen testing is the process of testing the network and other applications for vulnerabilities. The main purpose of this test is to secure the network or important data from outsiders like hackers, who can have unauthorized access to the application and exploit the network to access sensitive information if any kind of vulnerability is identified within it. Generally, vulnerabilities are introduced by accident during configuration of the network security, development and implementation of the system and applications. Common vulnerabilities include configuration errors, application bugs, and design errors. Testers use different sophisticated tools and advanced knowledge of IT to identify the behavior of an attacker, who penetrates the client's network and it's applications to obtain information and access to higher permissions without proper authorization. Penetration testing tools are used to identify standard vulnerabilities in the application. These tools will scan code to check whether there is any malicious code present in the system network by examining data encryption techniques and figuring out different hard-coded values like username and password.

A. Types Of Network Penetration and Testing

The type of a network penetration and test selection depend on the purpose and scope of the Bank. Whether Bank want to simulate an attack by their employees, a network administrator or external sources.

Generally, there are three different types of network penetration and testing. These are Black box, white box and grey box penetration and testing. In black-box penetration and testing, the pen tester is not provided with much information about the application he/she is going to test on the bank. The tester has a full responsibility collate information about the bank's network, system, and application running on the network.

White-box penetration and testing is where the tester is provided with all the required and necessary information by the bank concerning the network, implemented systems and applications, the type of operating system and their details. It is an attack by an internal source.

In grey box penetration testing, the tester will have the partial knowledge of the application or the network system and it can be considered as an attack by an external hacker, who had gained illegitimate access to the Bank's network infrastructure details. [10]The penetration tester is provided with information such as the hostnames, some selected internet protocol addresses and people that are allowed to connect to the Bank's network remotely. The Penetration Tester is given enough common information a normal user can know. It is the combination of both the white box testing and the black box testing approach during penetration testing. The Penetration Tester is provided some basic details of the target; however, internal workings and some other privileged information is still kept from the Penetration Tester. Real attackers tend to have some information about a target prior to engaging the target. Most attackers do not choose random targets. They are motivated and have usually interacted in some way with their target before attempting an attack. Gray box is an attractive choice approach for many conducting Penetration Tests because it mimics real-world approaches used by attackers and focuses more on vulnerabilities rather than reconnaissance.

B. How Penetration and Testing can be done

The process of penetration and testing follow a methodology that is accepted globally. In other to perform the penetration and testing on the Bank's network, the following steps should be adopted as explained below.

➢ *Reconnaissance*

The first stage in network penetration and testing is reconnaissance. This involves defining the scope and goal of the test, the systems to be addressed and the methods to be used in the process. [8]Reconnaissance defines the target environment based on the scope of work and once the target is identified, research is performed to gather intelligence on the target such as which ports are in use and the services being run. The network diagram, Internet Protocol Address, devices operating in network, applications, services and their version. It also exposes the security defense systems the Bank has implemented such as Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)

➢ *Scanning*

[9]Scanning is a method for bulk target assessment. To discover the live IP addresses in the network, to discover the open ports on the machines, to fingerprint the services and to detect the vulnerabilities which is done by the vulnerability scanners. [10]The fundamental goal of scanning is to identify potential targets for security holes and vulnerabilities of the target host or network. There are many tools that are available for scanning our network such as ncat, and nmap. The most popular scanning tool is network mapper which is called Nmap. The Nmap tool can be used in combination with other tools such as metasploit framework to determine the available ports, services, the services type and their version. Nmap is able to identify even if a host is alive or dead even if ICMP is completely down on the network Nmap is free in kali Linux and can also be used in windows. It is important to know that the type of scanning to perform determines the type of scanning such as scanning and bypassing firewalls will require

➢ *Identification of system vulnerabilities*

After the scanning of all available devices on the network is completed the pen tester undertakes vulnerability assessments which are to identify vulnerabilities in the system which can be exploited. [11] Vulnerability assessment is the process of identifying the vulnerabilities in a system which is conducted on behalf of the organization. Threats available in the system will be identified. [10] Vulnerability phase is started after some hosts are identified via nmap scans or other scanning tool after the reconnaissance. One of the best tools for vulnerability scanning is Nessus, Nikto, Metasploit and Open Vulnerability Assessment System (OpenVAS). It is an open-source vulnerability scanner which employs Nessus Attack Scripting Language (NASL). Finding the vulnerability allows the users to access complete information on the network

➢ *Reporting*

Writing a report and stating all important activities is final phase of penetration and testing. The findings are conveyed to the managers of the Banks in a very meaningful manner. The managers are made aware of the good things and the bad things and what has to be done to improve their security. This report must be in a clear language which a non-technical staff can easily understand. Kali Linux has several tools that are available to deliver information found during the penetration testing.

IX. CONCLUSION

It is recommended that the Bank runs a regular and consistent penetration and testing of the network security and relevant applications. The penetration and testing activity is to prevent hackers or intruders from tempering with information resources of the bank.

It is hereby conclude that, it is very necessary to ensure that information security breaches are detected as early as possible. Threats should be detected in a timely manner that will make the bank's network system robust to prevent hacker's attack. There must also be a quick and timely response which is to enable the Bank to prevent and mitigate the damages that may be caused by attackers of the system. This is to aid check how well the network is secured against extremely trained hackers who are attacking the network with determined stealth. This will enable the bank to train train their information security team to be proactive in the identification of attacks and the reaction to threat.

REFERENCES

[1]. GTsamenyi Matthew, and Shazard Uddin "the caes of rural banks in ghana: corperate Governance in Less Developed and Emerging Economie*s". Emerald Group Publishing. pp. 311 334. ISBN 978-1-84855-252-4

[2]. BAkwasi A. Boateng, Kennedy Annoh-Koranchie, andmEric Hayford "An Appraisal of rural and community banks in Ghana", www.iiste.org ISSN 2224-607X (Pper) ISSN 2225-0565 (online) Vol.6, No.6,2016

[3]. Bank of Ghana report , " List of rural banks". https://www.bog.gov.gh [Accessed: Januay, 2019 online]

[4]. Alok. Kumar, and Alimany Contte, "Financial and accounting manual for Rural banks," https://www.microfinancegateway.org/sites/ [Accessed: January,2019]

[5]. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6]. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7]. Waleed Al Shehri "A Survey On Security In Wireless Sensor Networks" International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.1, January 2017 DOI: 10.5121/ ijnsa. 2017.9103 25

[8]. Georgia Weidman "Penetration Testing: A hands-on introduction to hacking"

[9]. Chaitra N. Shivayogimath " An overview of network penetration testing". IJRET eISSN: 2319-1163 | pISSN: 2321-7308

[10]. Timothy P. Layton, Sr. "Penetration Studies–A Technical Overview". URL:http://www.sans.org/readingroom/whitepapers/testing/penetration-studies-technicaloverview-267

[11]. Vulnerability assasment www.en.wikipedia.org/wiki/Vulnerabilitya ssessment

[12]. Simon Parkinson and Andrews Crampton "Guide to Vulnerability Analysis for Computer Networks and Systems"