Global Scientific JOURNALS

GSJ: Volume 10, Issue 11, November 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

A FRAMEWORK ON CYBERCRIME AND RAPID DEVELOPMENT FOR PRIVATE INSTITUTIONS BASED ON FORENSIC METHODS TO ANALYZE DATA FLOW

NGENZI Patrick
Department of Information Technology
Graduate School
Kigali – Rwanda
pattyzon@hotmail.com

And

Sanja Michael Mutongwa
Academic & Research
University of Kigali
Kigali – Rwanda
sanja_michael@yahoo.com / msanja@uok.ac.rw

ABSTRACT

The wide spread of the use of computer and the rise of internet led to advent of cybercrime. The first cases of cybercrime were seen in 1980's in the USA and eventually spread all around the World, especially in developed countries (Peter Sommer, 2004). During this period, the number of computer related crimes increased, and different governments and organizations started to set up laws and strategies to eradicate these crimes. The general objective of this research is to extend a forensic framework to prevent and fight cybercrime in private institutions in Rwanda. The data gathering instruments included structured questionnaires and document review. The study has the following specific objectives: to investigate the effects of digital evidence on rapid development in private institutions; to examine the forensic methods used to prevent cybercrime within private institutions; to analyze forensic tools used by private institutions to fight cybercrime; and to develop a framework on cybercrime and rapid development for private institutions. The target population was the Liquid Intelligent Technologies employers and employees of Kigali, Rwanda. Researcher will gather data from this population, data that would contribute to answering the research questions. In this context, the population of this study included Liquid Intelligent Technologies (LIT) staffs and employees, LIT Stakeholders, LIT Operations Managers and LIT Customers. Researcher will gather data from this target population, data that was collected by answering the research questionnaire. The size of the population was 300 employees. The sample size of 171 respondents was drawn from the target population. The findings revealed that shows that (54.39%) of the respondents were female and 45.61% of the respondents were female. The great number of respondents (52.05%) were between 0 and 5 years of experience. The results indicated that 7.01% of respondents were Data Analysts, 8.19% were IT Managers, 12.86% were Communication Engineers, and 22.81% were Network Engineers, 27.49% were Field Engineers, and 21.64% were Operations Engineers; and finally, 52.63% of respondents had bachelor

level of education. Different components and devices were used in this study including computers, firewall, switches, routers, and network servers. The ping command was used to test a connection between one computer and another. For example, we used ping command to test inter-vlan connectivity through the firewall. As the result, the computers from different networks or vlans have communicated successfully without any signal loss. This was due to the configuration of the firewall so that it may be able to filter information being transmitted across different networks. Researcher consulted experts opinions and publications on this subject and compiled a model simulation with Cisco Packet Tracer 8.1.1 for laying a cybercrime framework that can be used to prevent cybercrimes by filtering packets flow especially from outside networks. The researcher has shown how the research contributed to the existing knowledge for the new ideas generated during this study. The research has recommended different personnel including future researchers, network administrators, network end users and the University of Kigali.

Keywords: *Cybercrime; Forensic Methods; Data Flow; CyberSecurity*

1. Introduction

The wide spread of the use of computer and the rise of internet led to advent of cybercrime. The first cases of cybercrime were seen in 1980's in the USA and eventually spread all around the World, especially in developed countries (Peter Sommer, 2004). During this period, the number of computer related crimes increased and different governments and organizations started to set up laws and strategies to eradicate these crimes. As indicated by Rwanda Investigation Bureau (2019), at least 113 cases of cybercrime, of which 64 were committed in the City of Kigali, were recorded in 2018 leaving many counting losses. Cybercrimes committed using technology such as computer, internet, telephone and any other type of information technology tools has led to an economic loss to the country amounting to Rwf 6 billion in 2018. In 2020 cybercrimes increased by 72 per cent during the Covid-19 lockdown imposed countrywide. As a result, a considerable amount of money was stolen by cybercriminals who took advantage that nowadays most of services are administered while relying more than ever on computer systems, mobile devices, and the Internet (NKUSI Fred, 2020).

Due to the rapid development of technology, especially the wide spread of many digital devices using internet and cheap electronic data capturing devices easily available to everyone, digital forensic skills are undoubtedly going to play an increasingly pivotal role in the resolution of serious cybercrimes. Given the investments made by the Government of Rwanda in the ICT infrastructure to support its economic development goals, it is imperative that infrastructure be resilient and secure against cyber threats (MYICT, 2015). Although there have been significant efforts and government interventions to address cyber security challenges through various institutions, there is a lack of adequate strong institutional framework to coordinate cyber security initiatives with an integrated approach as to fully realize cyber security strategic objectives. This includes ICT Policy and regulatory functions, consumer protection, matters of national interest and data security, regulation of electronic certification service providers, obligations of certification authorities, computer misuse, cyber-crime, and protection of personal information.

2. Literature review

According to Paternoster (2017), cybercrime has developed into involvement for public code and has been investigated by the use of crime theories, situational factors, and individual factors. Moreover, the internet does not stand alone to give internet connection for a laptop so, it is useful to see the different device connected to the internet to deliver and acquire data like cyber threats and cellular objects .Nowadays the trends in information and communication technologies have raised the speed of personal information exchange, storage, share, and processing to remarkable level.

Technologies and communications are rapidly changing in modern times causing ever changing concepts of

crime and criminality to adapt to an online world. The prevalence of technologies and the internet has radically changed the way we live, communicate, travel, share information, transfer funds, work and do business (Viano, 2017). To begin discussing cybercrime, victimization online and use of cybercrime prevention methods it is crucial to understand how cyberspace emerged, extent of cyberspace and how it is regulated.

2.1 Cybercrime

Cybercrime is expressed as a horrible committed contrary to a group of individual or individual by the help of new technology for instance chat room, email, internet with the crime decide of helpfully producing emotional harm, physical and mental (Oluga et al., 2014).

Figure 1: Cybercrime (Oluga, 2014)

There is a huge number of cyber-crimes exists all over the world will catch a top-level to obtain money in an unauthorized way. Whilst the relationship between crime and technology is not known, the studies suggest that crime is transposed since the 1990s, gaining new directions and establishing an array of recent obstacle and aids on policing (Brown, 2015). The characteristics of online criminal activity mean the capability criminals have needed an international reach in investigating illicit intrusions into digital networks to collect information, demolish websites or perform distributed retraction of service attacks (Clough, 2015).

2.2 Phishing

Social media phishing is the primary selection among the cybercriminals and they can be used in many forms of crimes such as espionage, unlawful activities and cyberbullying.

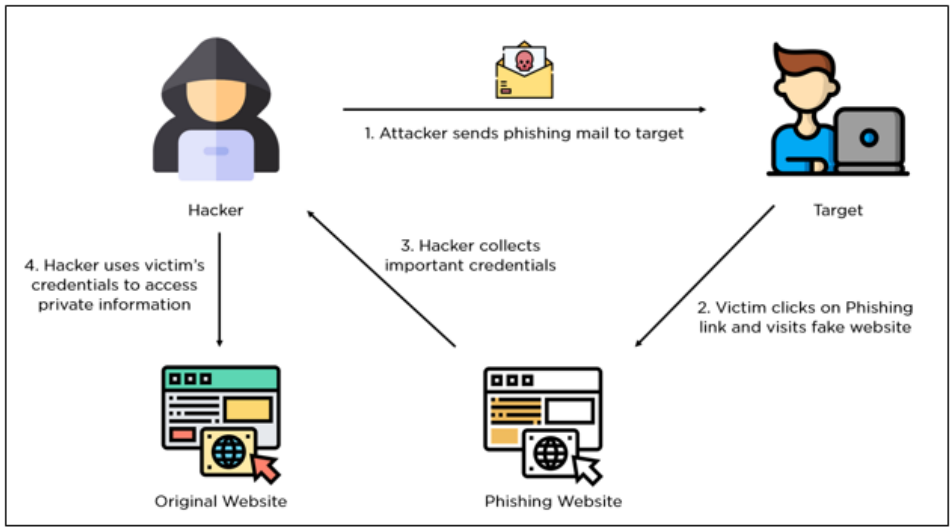

Figure 2: Phishing (Omar, 2013)

2.3 Forms of cybercrimes

Online identity theft

Online identity theft is the major common cybercrime. It is used to access into somebody else's personality or identity unsolicited to the users for fraud or steal money. This type of cybercrime the cyber-criminal use social media to get exact users information.

Cyber-criminal used a various method like malware, phishing, hacking, ransomware, fake online profiles picture to deceive someone personality or personal information of the target (Norden, 2013). The information accessed by criminals served to commit crime or fraud and used to by some illegitimate good as well as illegal activities.

Spam

Spam is a message that involves hateful links. The spammer can deliver wide unnecessary messages extremely posting varies links on the social media account in the form of advertisement or poster by false identification and it is considered as the major violation of Facebook by Facebook help Centre. There are various kinds of spam technique-click-jacking technique in this technique of the spam the attackers used a link that advice the users to click on the link which contains another page and deliver link that targets the victim. This method permits the attackers to commit the crime on social media by a single click.

Stealing confidential information

Cybercriminal can steal the necessary information during the data is transfer between social media called Facebook and third party requests. Third part requests can be served to harvest sound between the users within no consent. Confirming security of monetary authorizations might be threatening since submissions are the third event.

3. METHODOLOGY

Research Design; Study population; Sample size; Data collection tools

3.1 Research Design

Researcher consulted secondary data and experts publications on the subject being studied. Literature to consult was obtained from tangible and/or non-tangible media and Internet media in the form of journals, e-

books and other materials relevant to cybercrime frameworks and model development to find out how to bridge the gap identified in current model.

3.2 Study population

The target population was the Liquid Intelligent Technologies employers and employees of Kigali, Rwanda. In this context, the population of this study included Liquid Intelligent Technologies (LIT) staffs and employees, LIT Stakeholders, LIT Operations Managers and LIT Customers. Researcher gathered data from this target population, data that was collected by answering the research questionnaire. The size of the population was 300 employees.

3.3 Sample size

The sample is done in from knowledge gained to represent the entire target under study (Cohen et al., 2011). Sampling is the action of selecting the quantity of observations to include in a statistical sample. The sample size of 171 respondents was drawn from the target population

3.4 Tools for data collection

Data collection involves gathering of data using defined techniques in order to answer the pre-determined research question of the study (Sam, 2012). Researcher used questionnaire as an instrument consisting of questions for the purpose of gathering information from respondents. Researcher used questionnaire because the study concerned with variables that could not be observed such as views, opinions, perceptions, and feelings of the respondents.

4. ANALYSIS AND FINDINGS

4.1 Components for model design

Routers

Routers were used to manage the transfer of data through these networks. Routers join individual computer networks together to make up the internet, transferring information and providing the digital directions that allow computers to connect to each other anywhere in the world.

Network firewall

Network firewall was used to ensure that no one is able to connect to the home router. The router will have a variety of management services running on it such as the website that is used to configure the router among other services. Because the router is connected to the public Internet, we don't want anyone being able to connect to the router and make any changes on it from the public Internet.

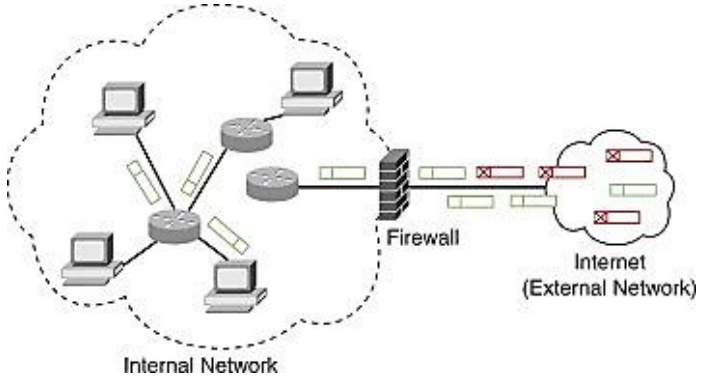

Figure 3: Network firewall

Network switch

Network switches were used to connect devices in a network to each other, and allows them to 'talk' by exchanging data packets. Switches can be hardware devices that manage physical networks, as well as software-based virtual devices.

4.2 Model implementation

Without having the firewall in place, an attacker could attempt to break into the router, and if they were successful, they would then be able to reconfigure the router to allow themselves access to one or more of the computers or devices on the home network.

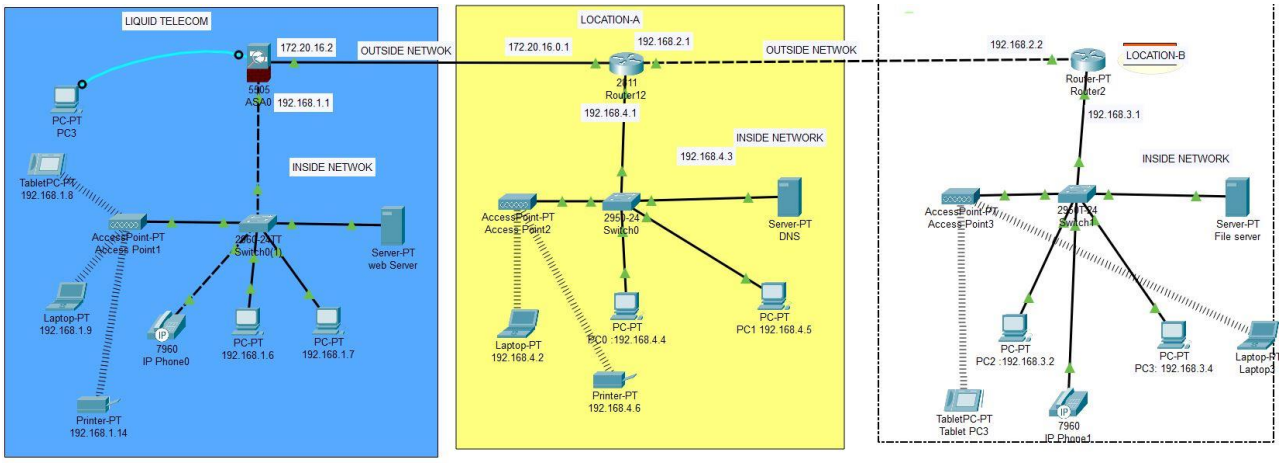

Figure 4: Design model of a cybercrime framework

4.3 Model testing

Using Packet tracer simulation at the testing phase of this model, networking devices were added to the network such as computers, switches, servers, routers and firewall. With internet connection, researcher tested the connectivity between devices. The figure below ping results whereby it indicated zero loss of packets, with that being observe, we conclude that the connection is established from LAN network to external network.

The figure below shows the ping results whereby it indicated zero loss of packets, with that being observe, we conclude that the connection is established from LAN network to external network.

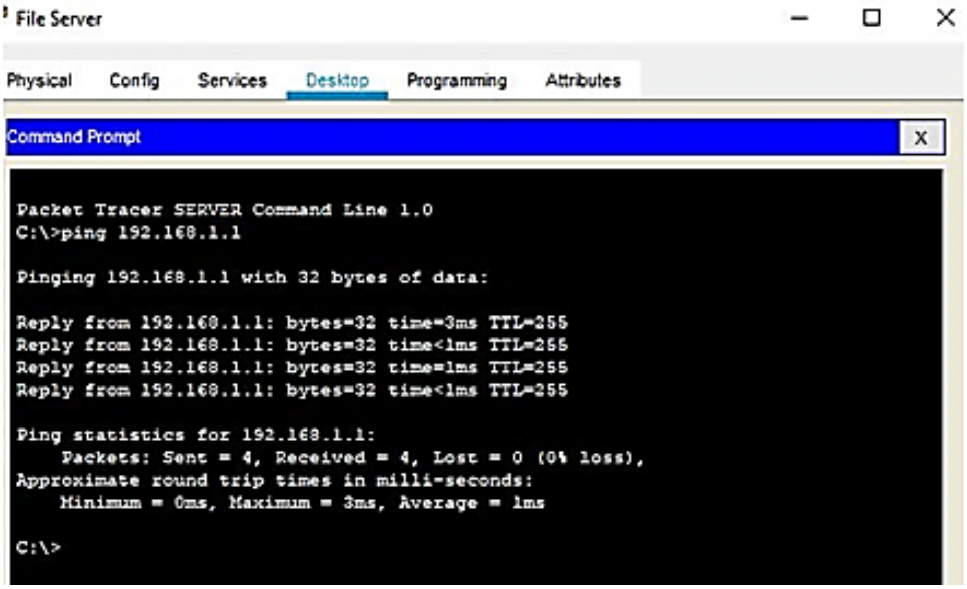

Figure 5: Connectivity testing 1

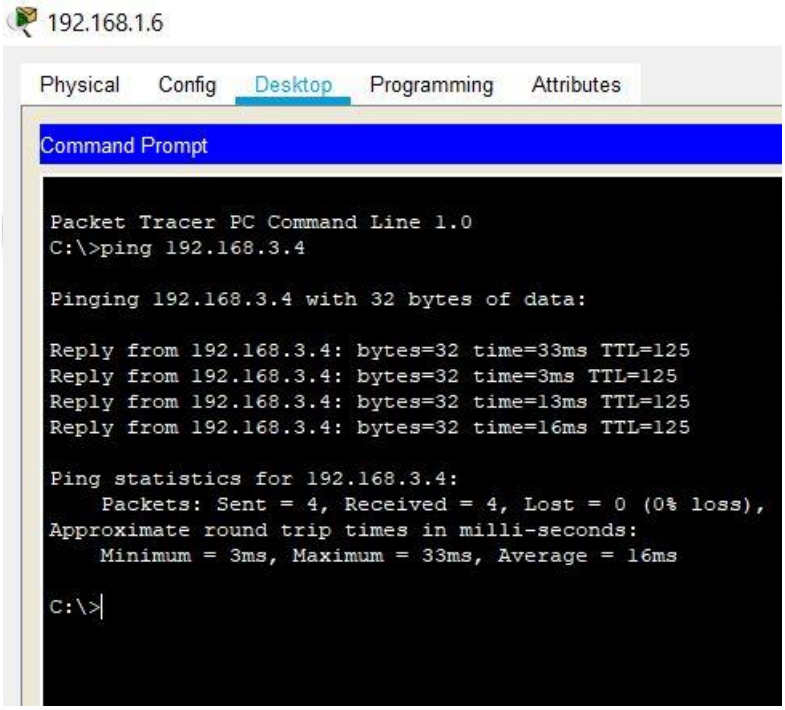

Figure 6: Connectivity testing 2

A ping command was used to test a connection between one computer and another. For example, we used ping command to test inter-vlan connectivity through the firewall. As the result, the computers from different networks or vlans have communicated successfully without any signal loss. This was due to the configuration of the firewall so that it may be able to filter information being transmitted across different networks.

5. Conclusion

The drive of this research was to develop a framework on cybercrime and rapid development for private institutions based on forensic methods to analyze data flow. During this research, different methods and techniques have been employed to collect and analyze data. Data used in this research were gathered from the selected samples including 102 Liquid Intelligent Technologies (LIT) staffs and employees, 11 LIT Stakeholders, 29 LIT Operations Managers and 29 LIT Customers through self-administered questionnaires. Basing on the total population at Liquid Intelligent Technologies of 300, Slovin's formula was employed to stem the sample size of 171.

This study was a success in terms of achieving objectives that was set at the beginning of this journey; objectives including but not limited to studying technologies and models currently being used for cybersecurity, and designing a cybercrime framework model. Researcher consulted experts opinions and publications on this subject and compiled a model simulation with Cisco Packet Tracer 8.1.1 for laying a cybercrime framework that can be used to prevent cybercrimes by filtering packets flow especially from outside networks. The researcher has shown how the research contributed to the existing knowledge for the new ideas generated during this study. The data gathering instruments included structured questionnaires and document review. The research has recommended different personnel including future researchers, network administrators, network end users and the University of Kigali.

REFRENCES

[1] Brown, C. (2015). Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55 -119.

[2] Clough, J. (2015). Understanding information disclosure behaviors in Australian Facebook users. Journal

[3] Maple, C., Short, E., and Brown, A. (2015). Predicting overt and cyber stalking perpetration by male and female college students. Journal of Interpersonal Violence, 27, 2183-2207.

[4] Mohay, G. M. (2003). Computer and intrusion forensics: Artech House.

[5] Nguyen, H. (2019). Cybersecurity governance framework in Vietnam : state of play, progress and future prospects. Governance Systems for Cybersecurity / Vietnam Science, 86–98.

[6] Nkusi Fred, "Why the rise of cybercrime in coronavirus pandemic?" in The New Times, of August 04, 2020.

[7] Oluga, A., Agana, H.C, and Inyiama, B. (2014). Cybercrime detection and control using the cyber user identification model. International Journal of Computer Science and Information Technology and Security, 5, 354–368.

[8] Omar, M., and Sad, Al. (2013). Threats and anti-threats strategies for social networking websites. International Journal of Computer Networks and Communications, 5, 5361.

[9] Peter Sommer (2004), "The future for the policing of cybercrime". Computer Fraud & Security.

[10] Tow, P., and Dell, J. (2010). Understanding information disclosure behaviours in Australian Facebook users. Journal of Information Technology, 25, 126- 136.

[11] Viano, E. C. (2017). Cybercrime, Organized Crime, and Societal Responses. Springer, Cham.