Crossref Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

Analysis of Decreased IP Forwarding Rate Attack on an Enterprise Network

[1] Osa, E & [2] Konyeha, S
[1]Department of Electrical / Electronics, University of Benin, Benin City, Benin City, Edo State
[2]Department of Computer Science, University of Benin, Benin City, Edo State
E-mail: susan.konyeha@uniben.edu
Phone: +2348060826547

ABSTRACT

Effects of Infect and Decrease IP Forwarding Rate by an attacking workstation and subsequent Scan and Clean scenario is compared to safe network configuration by adding the Routers attack in the simulation. The Riverbed Modeler Academic Edition 17.5 designing and evaluating network output. A comparison of two cases is deemed in this article. The first scenario is configured as an attack on the routers, while the second scenario is modelled as a stable and usable topology of the network. The performance is analysed based on the Client Database Entry Response time, Cyber traffic received, Infected Device Count and IP Processing Delay. The attack on the routers is demonstrated by the dramatic increase in the DB entry response time of the users, the existence of infected device counts and the spikes in the IP Processing Delay.

Keywords: Database, Router, Cyber traffic, Network, Configuration, IP Forwarding.

Journal Reference Format:
Osa, E and Konyeha, S (2020): Analysis of Decreased IP Forwarding Rate Attack on a Routed Network. Behavioural Informatics, Digital Humanities & Development Journal Vol 6. No. 1. Pp 67-68. Available online at behaviouralinformaticsjournal.info; https://www.isteams.net/behavioralinformaticsjournal http://dx.doi.org/10.22624/AIMS/BHI/V6N2P6

1. INTRODUCTION

OPNET (Optimised Network Engineering tool) now known as Riverbed Modeler, was launched in 1987 as the first commercially available communication network modelling platform (Sally F., 2020;OPNET, 2004).OPNET is considered to be extremely useful due to its ability to emulate a wide variety of networking technologies. It also allows the entire network to be modelled, including its routers, switches, protocols, servers and the specific applications they support. As a simulation language geared towards communications, OPNET has the advantage of having direct access to the source code and an easy to use front end. OPNET models consist of three primary model layers, namely the process layer, node layer and network layer, respectively.

The ability to create process models using finite state machines facilitates a modular approach, because the complex networks can be broken down into individual states and each state can be described and implemented individually. OPNET may typically perform three key functions such as modeling, simulating and analyzing. It offers a very simple but detailed graphical modeling framework i.e. creating all kinds of protocol models (Jyoti, Debonita and Shovon, 2013). IP Forwarding rate refers to the number of network packets which the network equipment (switch or router) may handle. The rate of forwarding is measured in packets per second (pps) (Zeifman, 2016).

1.1 Significance of Study

Simulation software is perfect for experimenting with this kind of research to escape the difficulty and needless costs of constructing a physical network environment and to use the time effectively (Guo, Xiang, and Wang, 2007). Riverbed Modeler Academic Version can be used to show that routers are compromised and IP forwarding rate attacks decreased.

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

The study is carried out to show the effects the above attack will have on routers in particular and the enterprise network in general. Such information could prove vital in deploying network topologies as well as proactive cybersecurity solutions.

2. REVIEW OF RELEVANT LITERATURE

The Internet's main functionality (and any other data communication network) is to facilitate the communication between end-systems. The Internet has thus acted as a platform for many attacks in which malicious users obtained unauthorized access to end-systems for hacking, surveillance, etc. Apart from such attacks targeting access to end-system data, there are also denial-of - service attacks aimed at making end-systems temporarily inaccessible (Chasaki, Wu and Wolf, 2011). Cybercrimes or misconducts on the Internet refers to the misuse of the Internet. It is a crime committed over a network with the use of a computer or related devices. Cybercrimes includes the use of goods or services that are illegal or commonly considered a criminal offence. The system is either a victim, or a weapon used in any crime committed online, i.e. the Internet. Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue and Spiegel (2012) describe a cyber-attack as any action taken to disrupt the functions of a computer system or network for political or national security, or to impede the effective governance of any country.

2.1 Enterprise Network

An enterprise network is the backbone for making communications simpler for a company and linking computers and devices through departments. Typically an Enterprise Network environment is designed to enable data access and analytics insight. Routers are network-wide devices which link multiple networks. They relay data from one system into another. They also connect internet devices over networks. Additional features can be placed in routers to improve ease of use or protection (Extreme Networks, 2020).

2.2 Cybercrime and Cybersecurity

Cybercrime and cyber-security are problems that an integrated world finds hard to distinguish. This is stressed by the fact that the 2010 UN General Assembly resolution on cybersecurity addresses cybercrime as a major threat (UNGA, 2010). A cyber-attack is a malicious and deliberate attempt by a person or organization to access another individual or organization's information system. The attacker usually seeks some form of benefit from disrupting the network of the victim. Cyberattacks regularly strike companies. Cybersecurity has become a major concern for managers and directors across the financial, healthcare, education, and government sectors. Because of flaws in cybersecurity, many organizations have been attacked by hackers or have been the victims of data breaches. The consequences of these accidents can be expensive and disruptive to companies when cybersecurity breaches occur (Consolidated Technologies Inc., 2017). The Forbes magazine forecast global cybersecurity spending at $101 billion in 2018, and hitting $170 billion by 2020. It is clear that spending alone will not curb the hackers' threat and their malware deployed. The basics of how to protect the organization and lay down core principles governing daily operations are required (LaBrie, 2018).

2.3 Router Infection

Cryptojacking detections of malware rose by 459 percent over the first half of 2018. Routers play an important part in this, with up to 415,000 computers infected with cryptomining malware in 2018 worldwide (Townsend K., 2019). Security researchers witnessed a major router attack in which threat actors inserted CoinHive to mine for Monero on more than 170,000 computers. By leveraging a critical flaw in MikroTik routers, attackers gathered sensitive information from targeted devices (Bonderud D., 2018). VPNFilter is called a malware that attacks a range of routers and is capable of knocking out infected devices and make them accessible. It has the ability to spy on traffic which is routed through the system. VPNFilter is considered to have the ability to infect businesses and small office / home office routers (Symantec Security Response, 2018).

Crossref
Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

3. RESEARCH METHODOLOGY

3.1 Research Design

In this experiment the OPNET Riverbed Modeler Academic Edition version 17.5 was used to run simulations in the network. The network simulates different users in different subnets accessing the Database Server. Routers R1, R3 and R5 are gateway routers connecting the green, white and red subnets respectively while R2 is a common router connecting all subnets to the Database Server. The network testbed is shown in Figure 1:

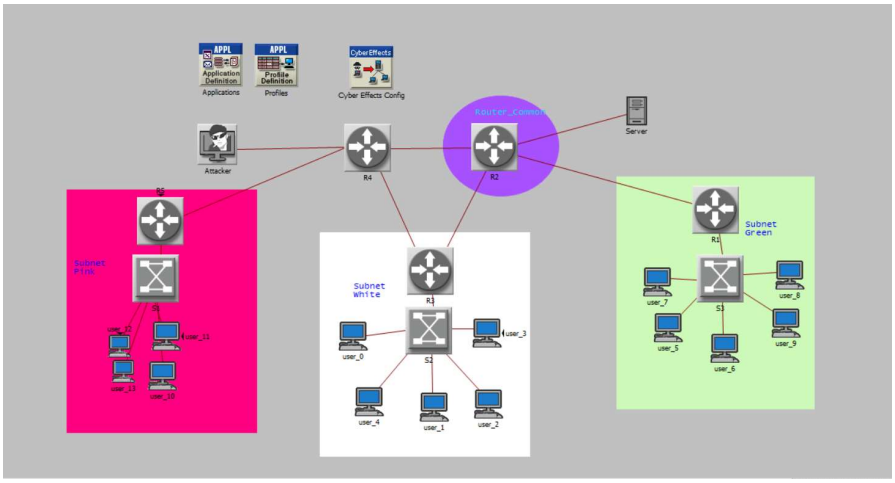

Figure 1. Network Testbed.

3.2 Attack Scenario

In this scenario the Cyber Effects Config. Node has the Script and Attack defined to alter the router IP rate. Four profiles are defined (one for each router) with the attacks happening in two phases, Phase one (P1) and Phase two (P2). The attack structure is similar for all routers.

In Phase one, the script “Infect and Decrease IP FwD rate 99.9%” is sent .This script first infects the router and then decreases its forwarding rate by 99.9%.

In Phase two, the script “Scan and Clean” is sent after 500 seconds to nullify the changes made by P1 and return the IP Forwarding rate to its original value.

3.3 Configuration Setting

For applications definition, the applications configured on this object are: Database Access (Heavy and Light), Email (Heavy and Light) and File Transfer (Heavy). For profile definition, there were three profiles configured in this object namely: Engineer, researcher and E-commerce Customer. For the Attacker, the cyber effects by the attacker consists of four profiles which are configured as shown in Figure 2.

Crossref
Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

Figure 2. Attacker Cyber Effects Profile.

3.4 Data Collection

Cyber Effects Config. Node. Data was collected from four cyber attack profiles configured as shown in Figures 3 to Figure 6.

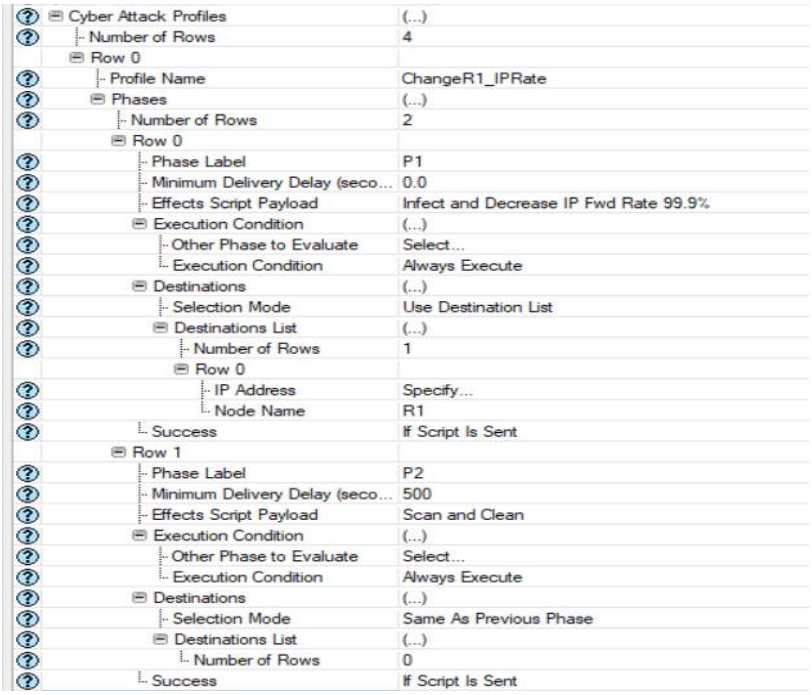

Figure 3. Attack Profile on Router 1.

Crossref
Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

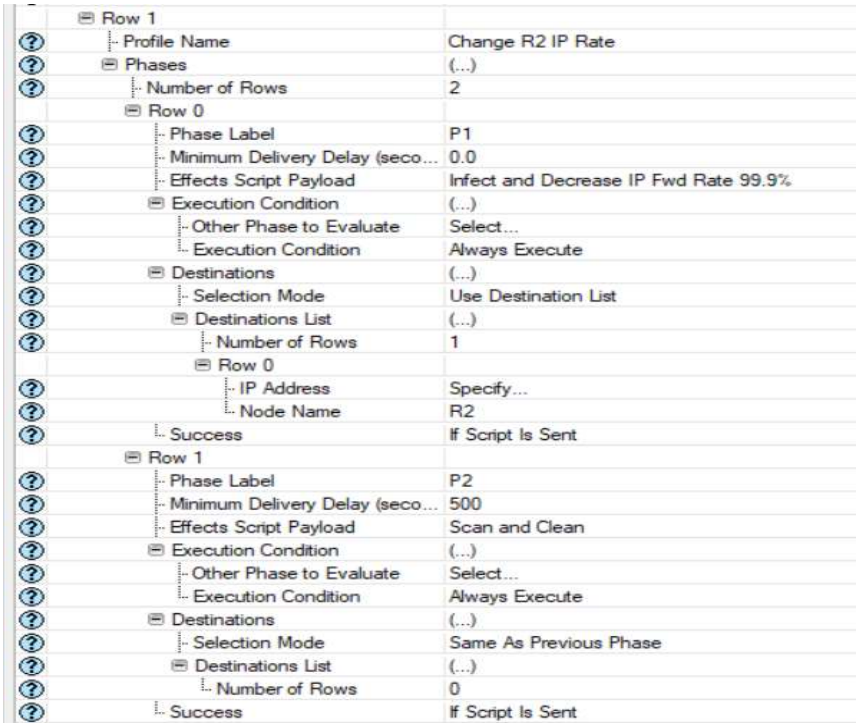

Figure 4. Attack Profile on Router 2.

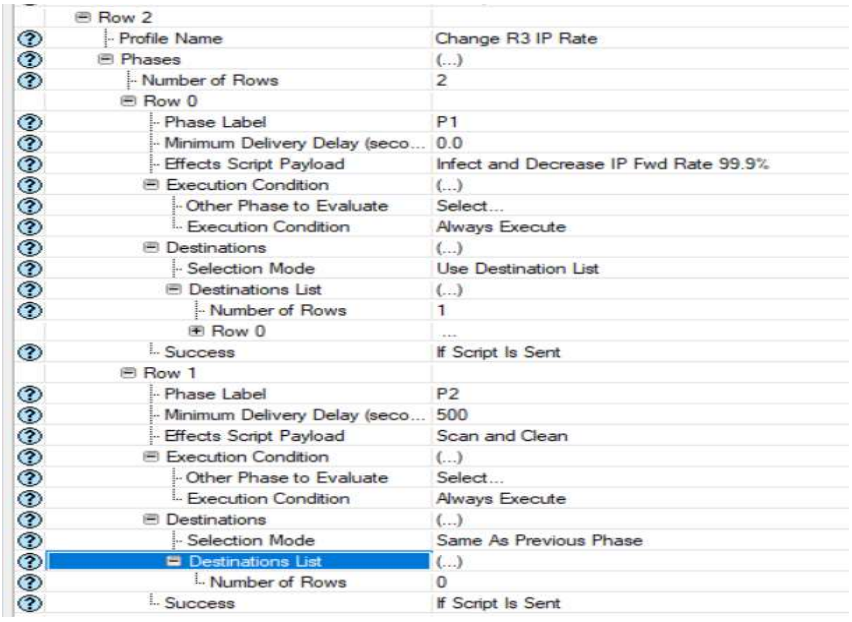

Figure 5. Attack Profile on Router 3.

Crossref
Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

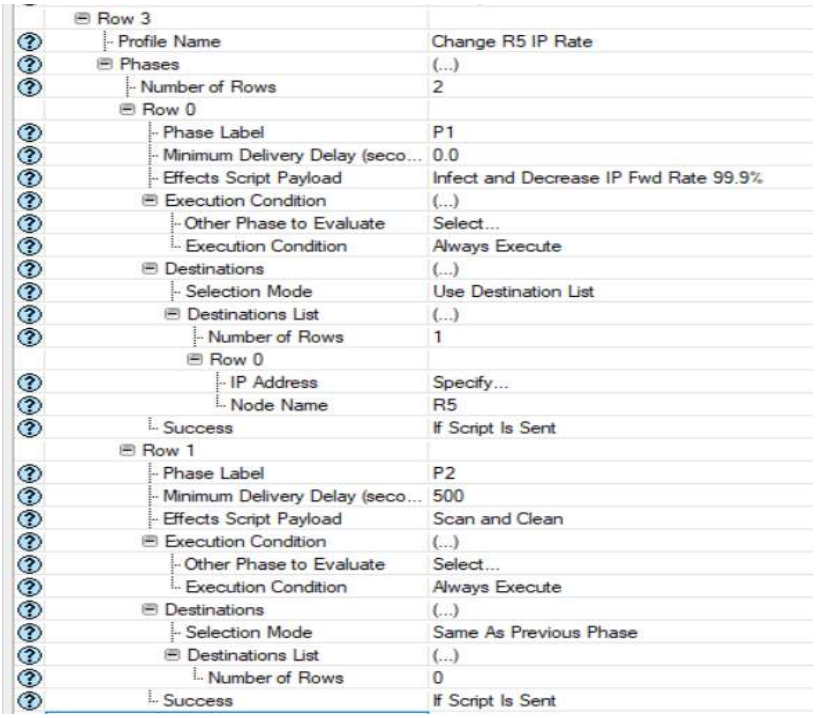

Figure 6. Attack Profile on Router 5.

The cyber Remedy Profile is configured as shown in Figure 7.

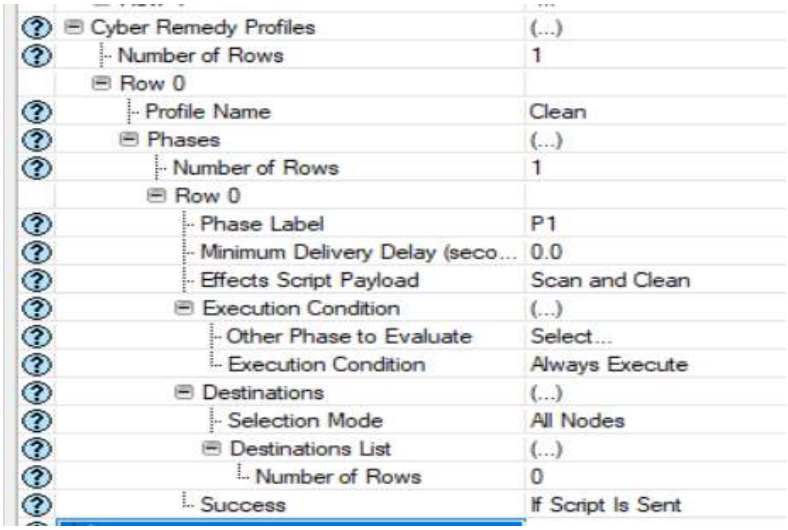

Figure 7. Cyber Remedy Profile.

Crossref
Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

All routers except R4 (which has no Cyber Effect capability) have the Cyber Effects configured with an infection probability rate of 100%. For the server, the application service is configured to Database Access (Heavy) while the Cyber Effects is configured with infection probability of 100%. All workstations are set to the Engineer Profile. The healthy network scenario simulates a network without cyberattack but just normal IP traffic.

To configure this scenario, all attack definitions in the respective objects above were removed while all other definitions were retained. The simulation was set to run for 60 minutes and the value per statistic was set to 100.

4. DATA ANALYSIS AND DISCUSSION OF RESULT

4.1 Results

Four statistics were collected which include: Cyber Effects Traffic Received, Client DB Entry Response Time, Cyber Effect Infected Devices Count and IP Processing Delay.

Figures 8-11 display the results for the attack scenario, while figures 12-15 display the results for the healthy network scenario as represented below.

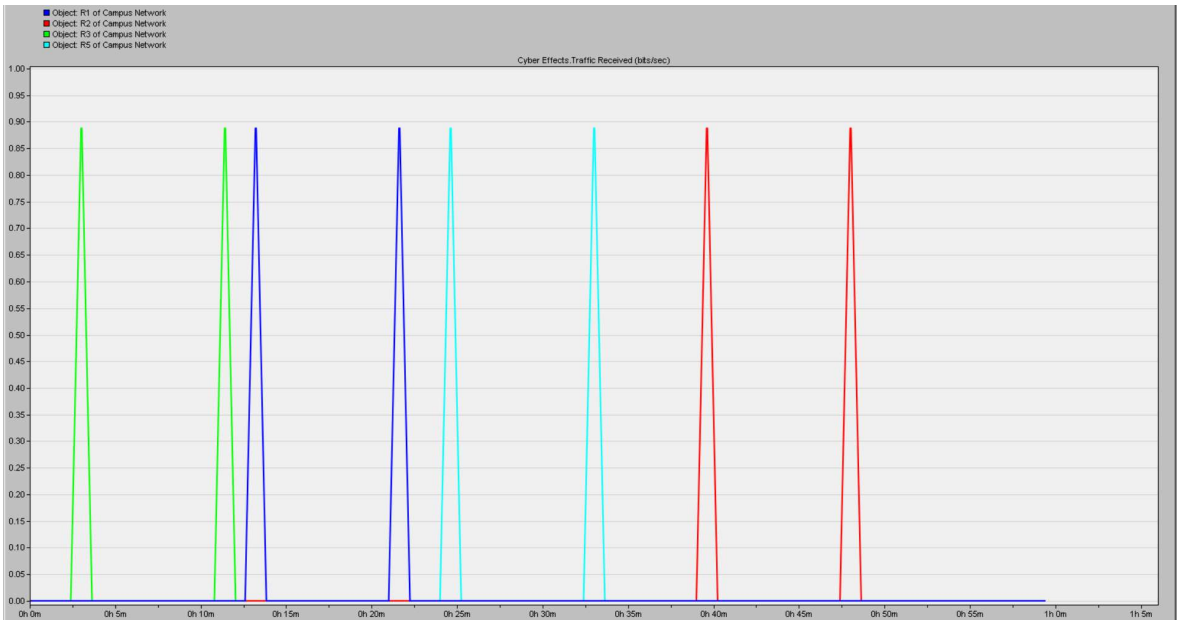

Figure 8. Cyber Traffic Received by Infected Routers.

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

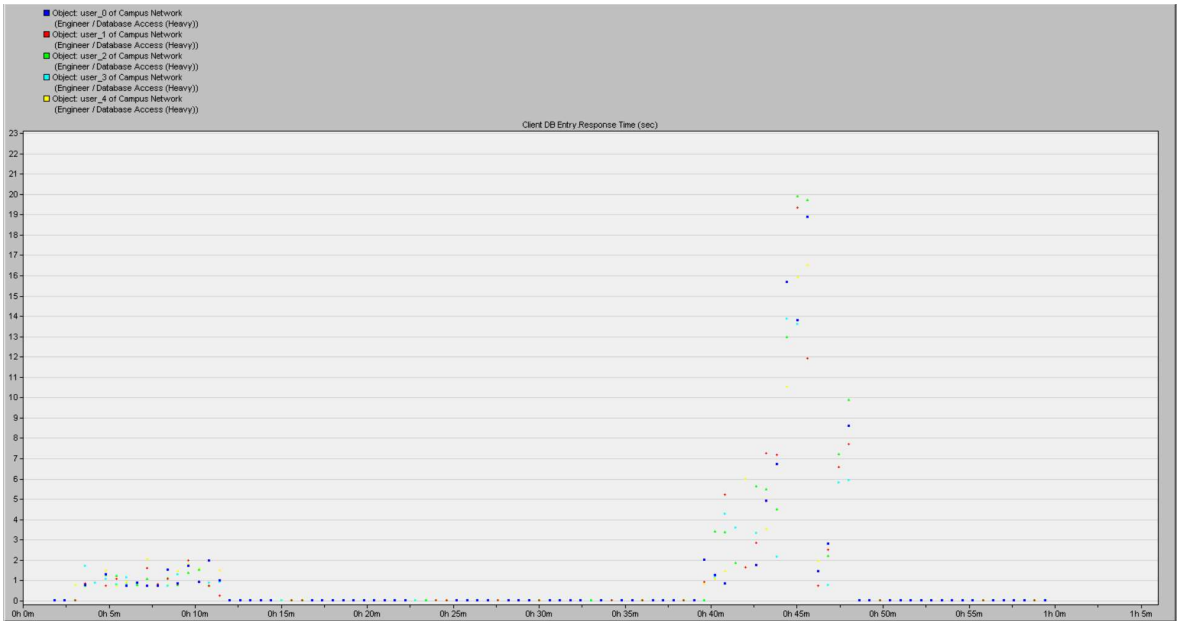

Figure 9. Database Entry Response Time for users in Subnet White.

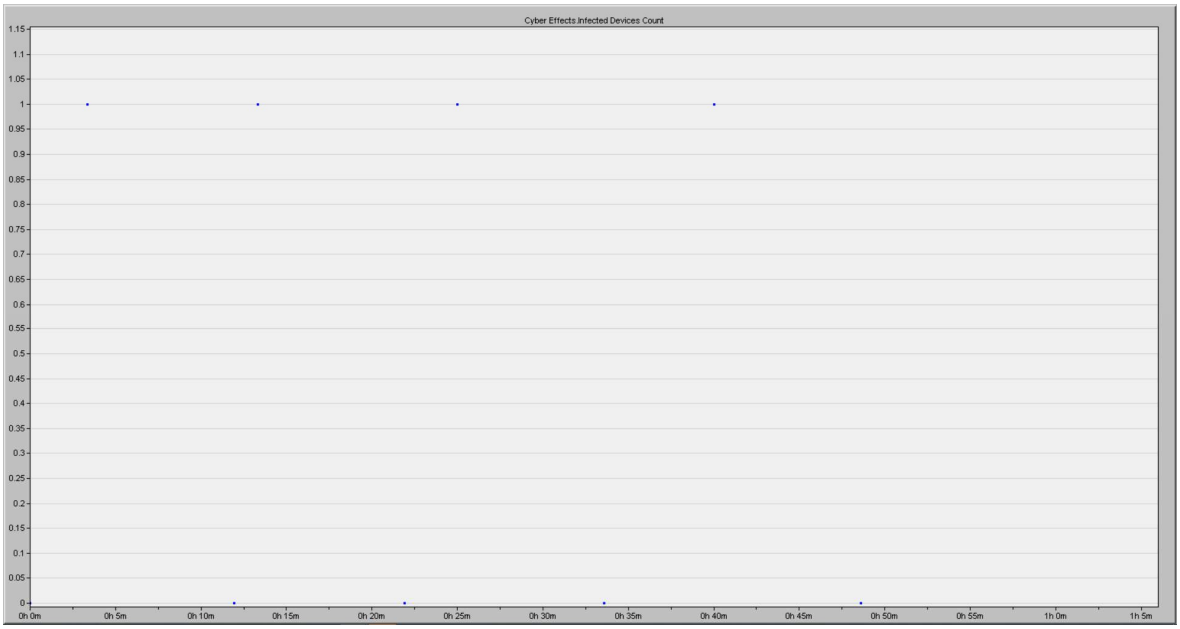

Figure 10. Infected Device Count

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

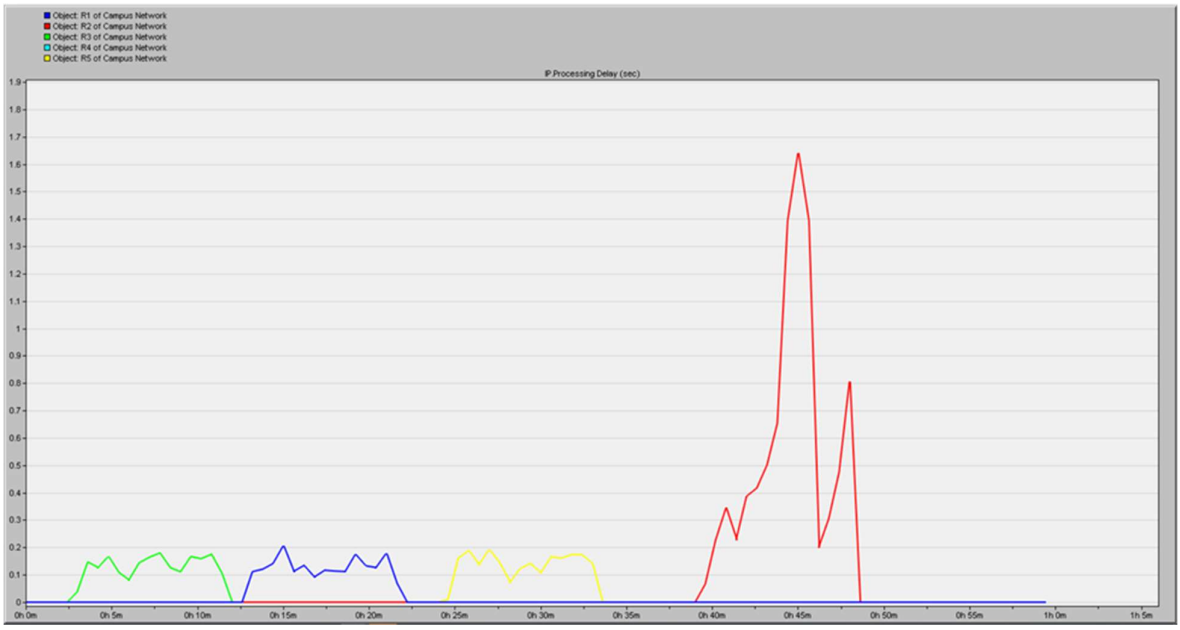

Figure 11. IP Processing Delay of Infected Routers.

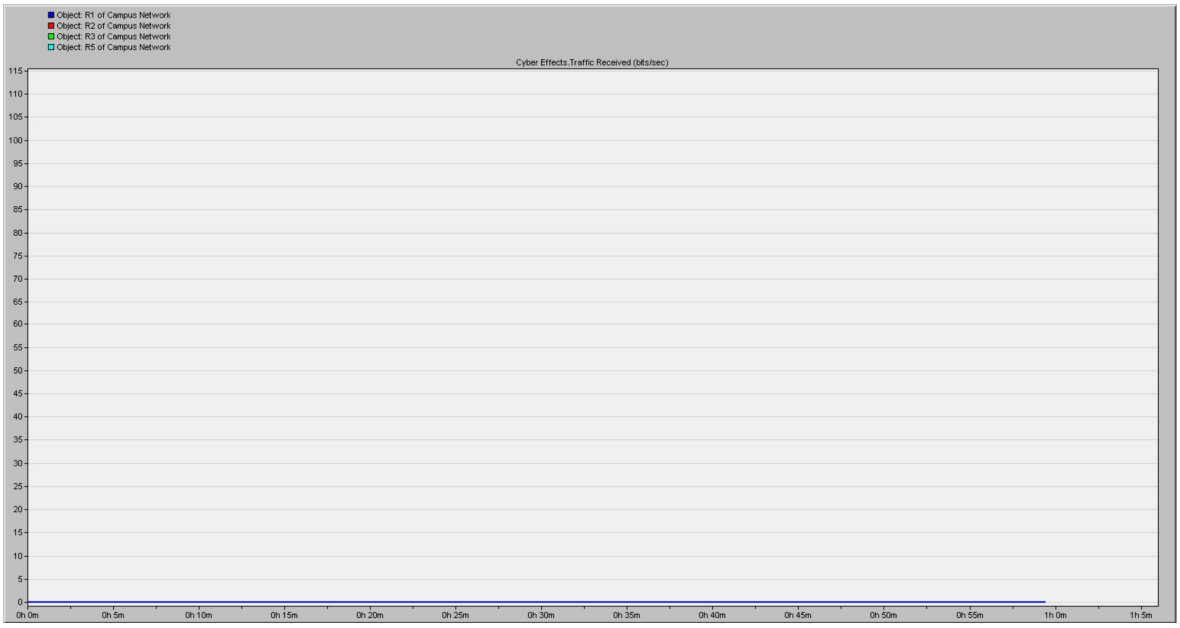

Figure 12. Cyber Traffic Received by Routers.

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

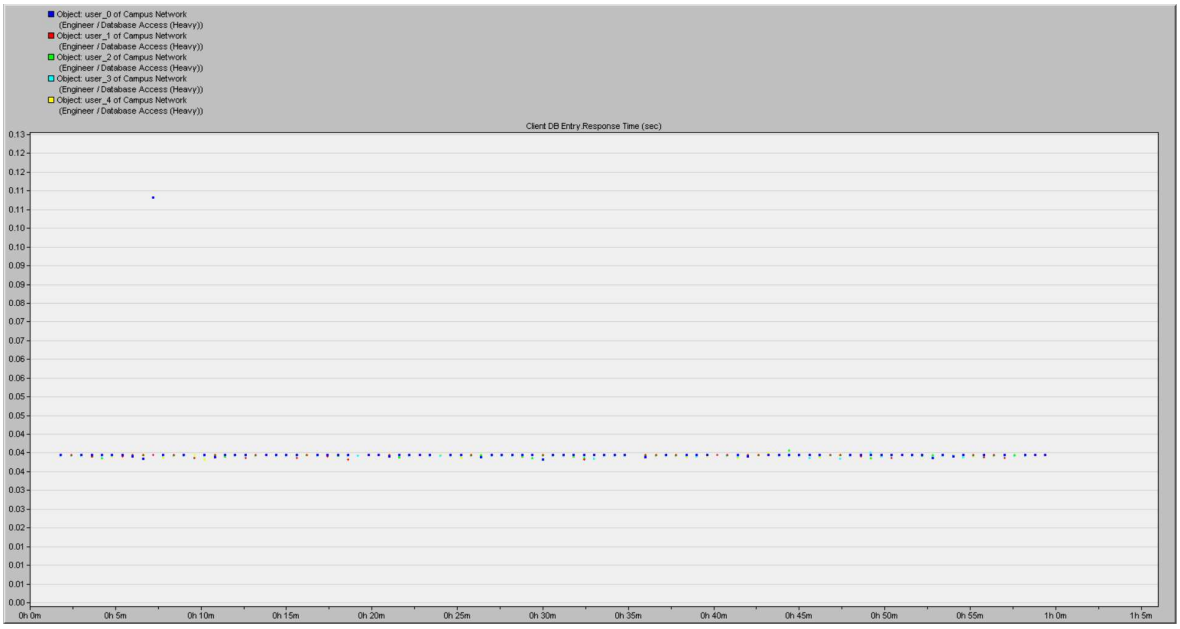

Figure 13. Database Entry Response Time for users in Subnet White.

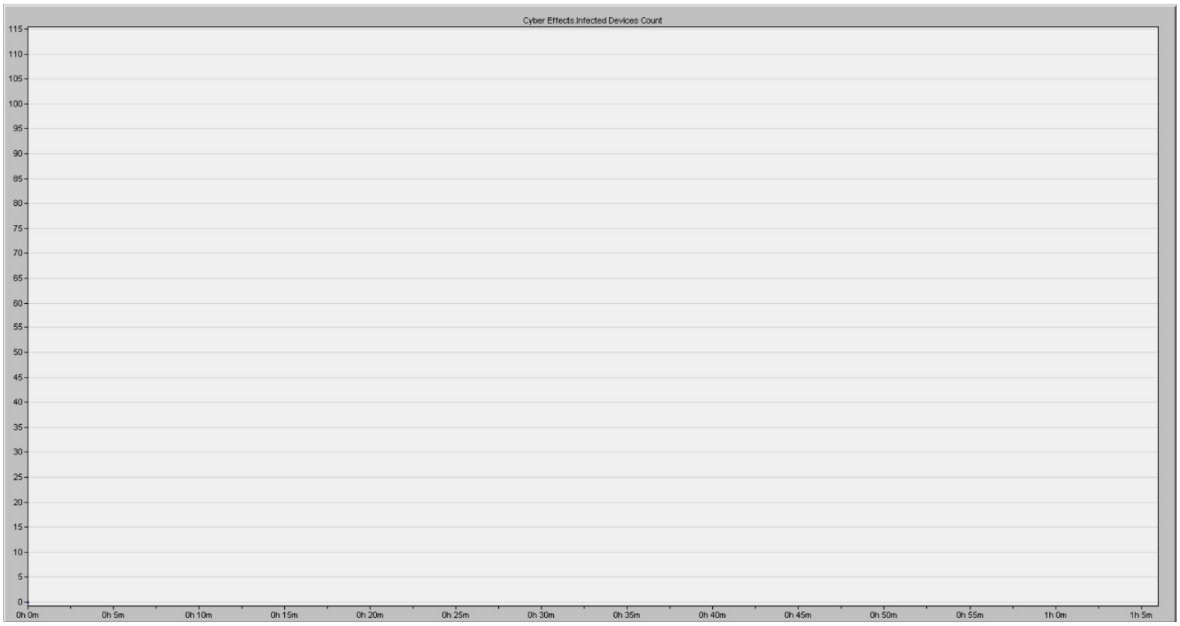

Figure 14. Infected Device Count

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 6, No 2, June, 2020

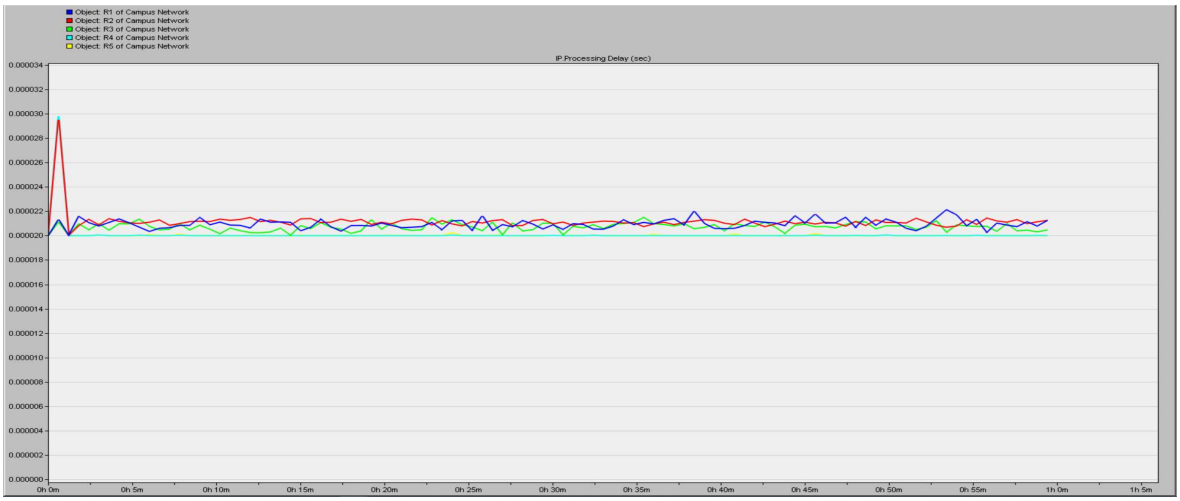

Figure 15. IP Processing Delay of Routers.

4.2 Analysis of Result

The Cyber Traffic Received by Infected Routers (which also reflects the traffic delivered by the attacker) is represented in Fig 8. There are two spikes to each router. The first spike represents the Attack script while the second spike represents the Scan and Clean script. As shown the attack on R1 occurs at 800 seconds, R2 at 2400 seconds, R3 at 200 seconds and R5 at 1500 seconds which are the respective attack Start Times configured. The Scan and Clean operation occurs 500 seconds after each of the attacks. Figure 9. shows the rise in response time for users in the white subnet due to attack. The first rise is due to the attack on R3 and it subsides 500 seconds later. The second rise which is greater is due to the attack on R2. This rise is very high due to the high traffic on R2 which is the router connecting all nodes to the Database server. Similar trends are observed for the green and red subnets (not shown because of brevity).

Figure 10 shows that one device each is infected at 200, 800, 500 and 2400 seconds respectively which corresponds to routers R3, R1, R5 and R2 respectively. Figure 11 represents the Delay in IP processing for routers R1, R2, R3 and R5 which is due to the decrease in IP Forwarding Times. However there is a shift in result paradigm as reflected in figures 12, 13, 14and 15. Figure 12 shows that there is no attack traffic received by any of the routers. This is because the infect and decrease IP Forwarding rate script was not configured. Figures 13 shows a steady Database Response time for users in the white subnet (a condition which holds same for all subnets) as against the output of Fig. 9. This shows that when there is no attack, the response time remains steady. Figure 14, shows zero infected devices count since no router was infected while Figure 15 shows an almost constant IP Processing Delay. This is because there was no Infect and Decrease IP Forwarding Rate attack.

5. CONCLUSION

This simulation experiment was carried out to analyze the effect of Infect and Decrease IP Forwarding Rate attack on a Routed Network. A Scan and Clean remedy was implemented after each attack. The results demonstrate the Cyber Attack Effect, the Remedy Effect and the impacts they have on the network performance. This work provides an insight into how The Decrease in IP Forwarding Rate attack affects router performance in a network. This knowledge is useful to Network Engineers and Cybersecurity experts in implementing their solutions, as well as other relevant stakeholders.

REFERENCES

1. Banerjee J.S., Goswami D. and Nandi S., 2014, OPNET: A New Paradigm for Simulation of Advanced Communication Systems. International Journal of Management and Technical Research. 1. 319-328.
2. Bonderud D., 2018. Massive Router Attack Injects CoinHive Malware Using Winbox Bug. SecurityIntelligence.com.
3. Chasaki D., Wu Q. and Wolf T., 2011. Attacks on Network Infrastructure, In 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN) (pp. 1-8).IEEE.
4. Cisco.com 2020, What Are the Most Common Cyber Attacks? [online] Available: www.cisco.com.
5. Consolidated Technologies Inc., 2017, Enterprise Cybersecurity. [Online] Available: https://consoltech.com/blog/enterprise-cybersecurity.
6. Extreme Networks, 2020, What is an Enterprise Network Made Of? [online] Available: www.extremenetworks.com.
7. Guo J., Xiang W., and Wang S., 2007, "Reinforce Networking Theory with OPNET Simulation," Journal of Information Technology Education. Vol.6 pp 215-226.
8. Hathaway O.A., Crootof R., Perdue W and Levitz P. (2012) "The Law of Cyber-attack". California Law Review.Vol.100, Issue 4. Pp. 817-886.
9. IDG (2013) "Cyber Crime, Hacking and Malware". An Annual Publication.
10. Jyoti S.B., Debonita G. And Shovon N., 2013, OPNET: A New Paradigm for Simulation of Advanced Communication Systems. International Conference on Contemporary Challenges in Management, Technology and Social Sciences at M.G. Institute of Management and Technology, Lucknow. April 5th-6th, 2014.
11. LaBrie G., 2018.The Five Core Principles of Modern Enterprise Cybersecurity (Part1) [Online] Available: https://blog.wei.com.
12. OPNET Technologies, Inc. 2004. "OPNET Modeller", [Online] Available: http://www.opnet.com/products/modeler/home.html.
13. Sally F., 2020. Network Simulators. [Online] Available: http://www.icir.org/models/simulators.html.
14. Symantec Security Response, 2018, VPNFilter: New Router Malware with Destructive Capabilities.,[Online] Available: https://Symantec-enterprise-blogs.security.com/blogs.
15. Townsend K., 2019, Routers: a vulnerable opening to your home and personal data. [Online] Available: https://blog.avast.com.
16. UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.
17. Zeifman I., 2016, Can You Handle 300 Mpps? Forwarding Rate vs Throughput Rate – The DDoS Perspective [Online] Available: https://www.imperva.com.