INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 7, Issue 3 - V7I3-1891)
Available online at: https://www.ijariit.com

# Secure organization networking

*Vishnu Rai*
raivishnu1013@gmail.com
*Maharaja Agrasen Institute of Technology, New Delhi*

*Puneet*
puneetkashyap58@gmail.com
*Maharaja Agrasen Institute of Technology, New Delhi*

*Dr. Amita Goel*
amitagoel@mait.ac.in
*Maharaja Agrasen Institute of Technology, New Delhi*

*Vasudha Bahl*
vasudhabahl@mait.ac.in
*Maharaja Agrasen Institute of Technology, New Delhi*

*Nidhi Sengar*
nidhisengar@mait.ac.in
*Maharaja Agrasen Institute of Technology, New Delhi*

## ABSTRACT

***Perhaps the greatest concern companies have in doing business over the Internet is the security risk. Hackers, denial-of-service (DoS) attacks, fraud, and even cyber-terrorism are very real dangers. In addition, you'll wonder the way to guarantee the performance and reliability of your Internet-based services. Or, you'll not be sure that you simply have the resources and support needed to deploy and manage eCommerce services and processes. The good news is that a sound network infrastructure can address these issues. At the inspiration of strong e-commerce, infrastructures are routers and switches. An integrated approach to routing and switching lets all workers—even those at different sites— have equivalent access to business applications, unified communications, and videoconferencing as their colleagues at headquarters. This project helps you grow your network over time, adding features and functionality as you would like them while ensuring complete investment protection. All workers—even those in distant locations—have the same access to business applications, unified communications, and videoconferencing as their colleagues at headquarter thanks to an integrative approach to routing and switching.***

***Keywords:*** *Networking, Denial-of-Service (DoS), Routing, and Switching*

## 1. INTRODUCTION

There is a huge incline in the processes and works done by computer and internet in the world. Therefore, it is very important that we have a secure network which can be kept in a check at all times in any organisation. There is a constant increase in the use of electronic devices and internet in today's world.

Everyone nowadays uses technology and internet in one way or other, for one reason and other. The internet use has an enormous escalation and it's not turning back any time soon. We all know that if we are using internet, we aren't just accessing the info available on internet we are being susceptible to our data being erupted or attacked. Another thing with internet is that it changes continuously and sometimes dangerously stop these vulnerabilities and we need to keep our systems at a check. Also, as we all know that we are all heading towards a time where major organisations will be shifting a lot of their work to work from home and therefore most of the attacks are going to be on personal computers and thus the necessity to secure the private computers are going to be quite ever.

Perhaps the best concern companies have in doing business over the web is that the security risk. Hackers, denial-of-service (DoS) attacks, fraud, and even cyber-terrorism are very real dangers. In addition, you'll wonder the way to guarantee the performance and reliability of your Internet-based services. Or, you'll not be sure that you simply have the resources and support needed to deploy and manage e-commerce services and processes.

The good news is that a sound network infrastructure can address of these issues. At the inspiration of a strong e-commerce infrastructure are the routers and switches.

An integrated approach to routing and switching let's all workers—even those at different sites—have an equivalent access to business applications, unified communications, and videoconferencing as their colleagues at headquarters.

This project lets you grow your network over time, adding features and functionality as you need them while ensuring

complete investment protection. An added advantage of this integrated approach is that your IT personnel can centrally manage the network from headquarters, which keeps staffing counts low.

## 2. LITERATURE REVIEW

In my research I found different types of cyberattacks – big and small, infamous and unfamous orthodox and unorthodox, organisational and personal, carried out by whitehats, blackhats and greyhats, some of them were even carried out for fun. Following are some attacks which i feel shall be brought into notice for the higher understanding of this report. Also, i might wish to bring into the notice that i'm not the primary to write down about these incidents and that they are published at tons of places.

It was the year 1999. Jonathan James was only 15 at the time, but what he accomplished that year earned him a place in the hacker's hall of fame. James had infiltrated a US Department of Defence division's systems and planted a "backdoor" on its servers. He was able to intercept hundreds of official emails from government entities, including emails revealing usernames and passwords for various military computers, as a result of this. James was able to steal a piece of NASA software using stolen information, costing the space exploration organisation $41,000 in lost time while systems were shut down for three weeks. “The software [worth $1.7 million] supported the International Space Station's physical environment, including heating and cooling within the lebensraum,” according to NASA. James was apprehended later, but due to his youth, he received a short punishment. After being accused of colluding with some other hackers to obtain credit card numbers, he committed suicide in 2008. In his suicide letter, James refuted the claim.

Kevin Poulsen is famous for hacking into the Los Angeles telephone system in order to win a Ferrari in a radio contest. The 102nd caller received a Porsche 944 S2 from LA KIIS FM. Poulsen ensured his success by seizing control of the phone system and effectively blocking incoming calls to the radio station's phone number. He won the Porsche, but the police caught up with him, and he received a five-year sentence. Poulsen went on to become the senior editor of Wired News, the It security journal.

These were examples of attacks on corporations and companies but now lets have a look at few personal attacks about which this report is majorly concerned about as we all know this ongoing pandamic (COIVD-19) has shown us that the world can consider shifting to work from home which will ensure the bringing of personal computers into the firing lines of hackers and other cybercriminals.

The most common personal attack is that the denial of service attack (DoS attack). In this attack the attacker once access a personal computer or device can perform operations like sniffing.

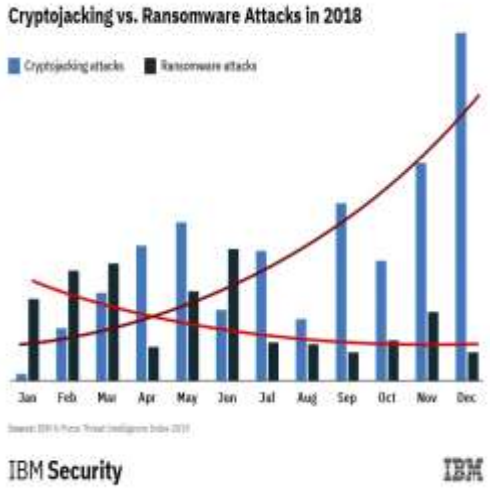
Also must be mentioned is that cyberattackers can very easily turn on webcams and mic of any device.

Man in the middle is also an attack worth mentioning as it is one the favourite attack of the cyberattackers as it gives them full access to any device on the network.

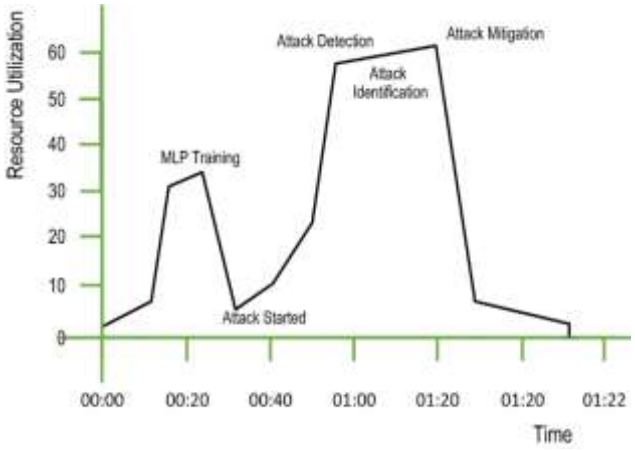
Also some extent to be noticed is that this report won’t be covering anything about public knowledge attacks like worms and viruses .

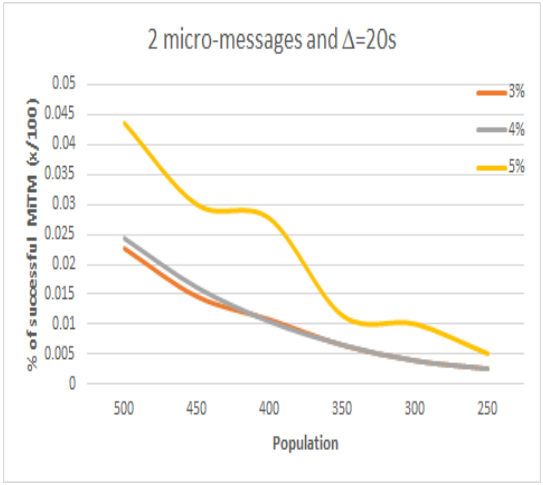
## 3. CONTENT

95 of security breaches are because of a human error or failing to notice the attacks and issues that are present in front of them. Some of the common issues overlooked by the users are DoS(Denial of service attack), Cryptojacking and Man in the middle (MITM). For the people who are new in Information Technology cryptojacking is hiding on someone’s personal computer and mining cryptocurrencies.




Also here are some statistics for MITM and DoS Attacks.




Percentage of successful MITM attacks. (a) Getting key information in 3 micro-messages; (b) Getting key information in 4 micro-messages; (c) Getting key information in 5 micro-messages.

From above statistics it's clear that we need to be very careful about our computer systems. There are a lot of people aware about the antiviruses and firewalls available to stop the viruses and worms that try to enter our system. However, there are not many people aware about the codes and commands to check for the security of their system and their network.

## 4. METHODOLOGY

"Secure Organisation Networking" has been created using a combination of some basic commands, routing commands, rip commands, EIGRP commands, OSPF commands, VLAN commands, trunking commands and VTP commands.

## 5. IMPLEMENTATION

Following devices have been used in the implementation of this project although the number of devices may vary from one organisation to another.

8 SERIAL CABLES
28 COPPER CROSS OVER
8 COPPER STRAIGHT THROUGH
8 ROUTERS
16 SWITCHES (LAYER 2)
1 MULTY LAYER SWITCH
28 PCs
CONSOLE CABLES

All of these devices have been used and connected virtually on CISCO packet tracer which is an easy-to-use networking simulation tool.

Also, apart from these devices the other major and defining part of the project is the protocols that have been used.

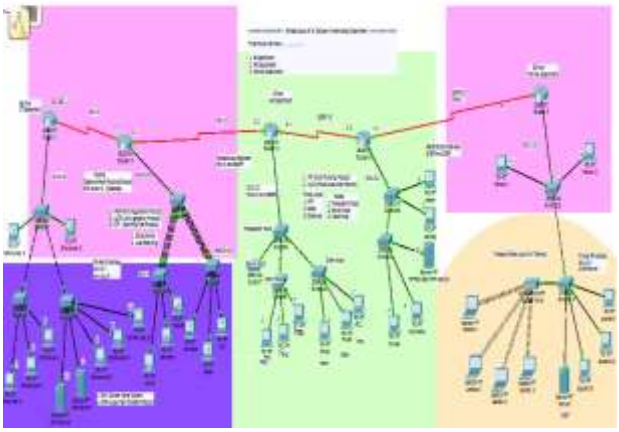
Following are the three important protocols that have been used for this project.

RIPV2
OSPF
EIGRP

These protocols are the soul of this project they make sure that the networking that has been done will be secure and will not have any bugs or errors.

## 6. OUTPUT AND RESULTS

Here is a snapshot of the virtual connection on CISCO packet tracer.



All the devices have been connected and are working properly.

## 7. REFERENCES

[1] Advanced System Checker Vishnu Rai, Dr. Amita Goel, Ms. Nidhi Sengar, Ms. Vasudha Bahl, Volume: 07 Issue: 11 | Nov 2020.

[2] Wayne Jansen and Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology, Special Publication 800-144, December 2011, 80 pages

[3] "Cloud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[4] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[5] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.