iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44501

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Network Security and Cyber Security: A Review

Mrs. K. N. Rode[1], Ms. Shubhada Chandrakant Patil[2], Ms. Akshata Adinath Patil[3], Ms. Rutuja Pravin Dahotre[4]
[1, 2, 3, 4]*Sharad Institute of Technology College of Engineering, Yadrav-Ichalkaranji*

Abstract: ***Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. Now – a - days security measures works more importantly towards fulfilling the cutting edge demands of today's growing industries. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. In this paper Author has described the important measures and parameters regarding large industry/organizational requirements for establishing a secure network. Wi-Fi networks are very common in providing wireless network access to different resources and connecting various devices wirelessly. There are need of different requirements to handle Wi-Fi threats and network hacking attempts. This paper explores important security measures related to different network scenarios, so that a fully secured network environment could be established in an organization. Author also has discussed a case study to illustrate the minimal set of measures required for establishing network security in any organization.***
We will be analyzing a variety of cyber-attacks and different security methods. We aspire to create research into the subject area. This paper explores how cybercrime has become a serious threat in our lives and we are going to look at a few of the different security methods that are being used in this arena and their various weaknesses.

I. INTRODUCTION

Network security can be defined as protection of networks and their services from unauthorized alteration, destruction, or disclosure, and provision of assurance that the network performs in critical situations and have no harmful effects for neither user nor for employee . It also includes provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access.
Cyber security is generally the techniques set to protect the cyber environment of the user. This environment includes the user themselves, the devices, networks, applications, all software's etc. The main objective is to reduce the risk including cyber attacks. Cyber security is the branch of computer security related to internet. The main security objective is to project the device using various rules and to establish various measures against attack over the internet.

A. Network Security Attacks

Security attacks can be classified under the following categories:-

1) Attacks

This type of attacks includes attempts to break the system by using observed data. One of the example of the passive attack is plain text attacks, where both plain text and cipher text are already known to the attacker.

The attributes of passive attacks are as follows:
a) Interception: attacks confidentiality such as eavesdropping, "man-in-the-middle" attacks.
b) Traffic Analysis: attacks confidentiality, or anonymity. It can include trace back on a network, CRT radiation.

2) Active Attacks

This type of attack requires the attacker to send data to one or both of the parties, or block the data stream in one or both directions. The attributes of active attacks are as follows,
a) Interruption: attacks availability such as denial-of-service attacks.
b) Modification: attacks integrity.
c) Fabrication: attacks authenticity.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

B. Network Security Measures

Following measures are to be taken to secure the network :

1) A strong firewall and proxy to be used to keep unwanted people out.
2) A strong Antivirus software package and Internet Security Software package should be installed.
3) For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
4) When using a wireless connection, use a robust password.
5) Employees should be cautious about physical security.
6) Prepare a network analyzer or network monitor and use it when needed.
7) Implementation of physical security measures like closed circuit television for entry areas and restricted zones.
8) Security barriers to restrict the organization's perimeter.
9) Fire asphyxiators can be used for fire-sensitive areas like server rooms and security rooms.

C. Network Security Tools

Following tools are used to secure the network :

1) N-map Security Scanner is a free and open source utility for network exploration or security auditing.
2) Nessus is the best free network vulnerability scanner available.
3) Wire shark or Ethereal is an open source network protocol analyzer for UNIX and Windows.
4) Snort is light-weight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks.
5) Net Cat is a simple utility that reads and writes data across TCP or UDP network connections.
6) Kismet is a powerful wireless sniffer.

II. INTERNET SECURITY PRODUCTS

1) *Antivirus:* Antivirus software and internet security programs are able to project a programmable device from attack by detecting and eliminating the viruses. Antivirus software was used in the early years of internet but now with the development several free security applications are available on internet.
2) *Password Managers:* The password managers is a software application that is used to store and organize the passwords. Password managers usually store passwords encrypted, requiring the person to create a master password; a single, ideally a very strong password which allows the user access to their entire password database.
3) *Security Suits:* The security suits contains the suits of firewalls, anti-virus, anti-spyware and many more. They also gives the theft protection, portable storage device safety check, private internet browsing or make security related decisions and are free of charge.
4) *Security Tokens:* Some online sites offers the users the ability to use the six digit code which randomly changes after every 30-60 seconds on a security token. The keys on the token have built computations and manipulated numbers based on the current time built into the device. This means that after every thirty seconds there is only a certain sequence of numbers possible which would be correct to access to the online account.

III. SECURITY METHODS

A. Cryptography

1) The most widely used tool for securing information and services .
2) Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message .

B. Firewalls

A firewall is simply a group of components that collectively form a barrier between two networks. There are three basic types of firewalls:-

1) *Application Gateways:* This is the first firewall and is some times also known as proxy gateways as shown in figure 1. These are made up of bastion hosts so they do act as a proxy server. This software runs at the Application Layer of the ISO/OSI Reference Model. Clients behind the firewall must be categorized & prioritized in order to avail the Internet services. This is been the most secure, because it doesn't allow anything to pass by default, but it also need to have the programs written and turned on in order to start the traffic passing.

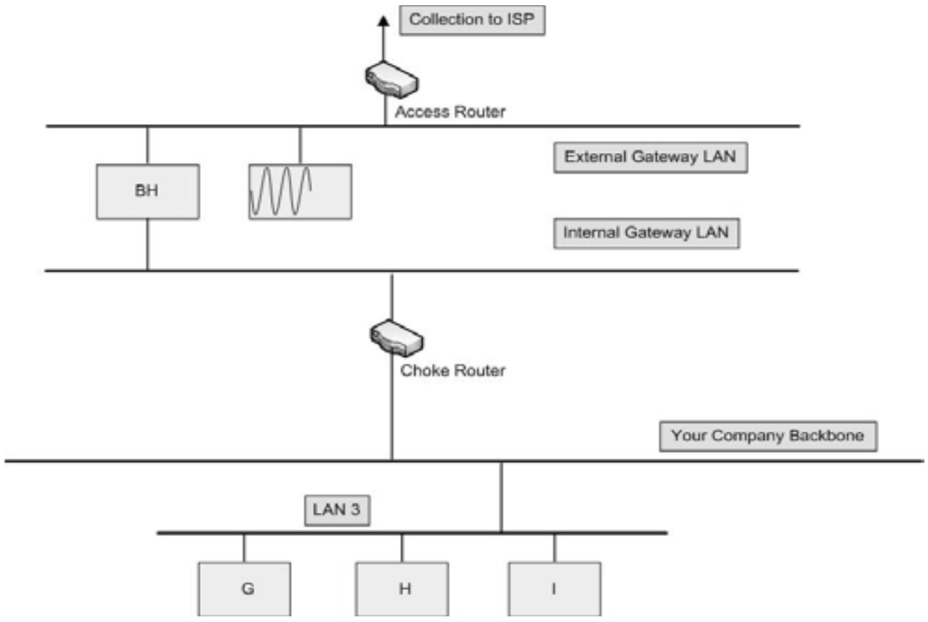


Figure 1: A sample application gateway

2) *Packet Filtering:* Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent through it, without any restrictions as shown in figure 2. ACL's is a method to define what sorts of access is allowed for the outside world to have to access internal network, and vice versa. This is less complex than an application gateway, because the feature of access control is performed at a lower ISO/OSI layer. Due to low complexity and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. There are problems with this method; thought TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, use layers of packet filters are must in order to localize the traffic.

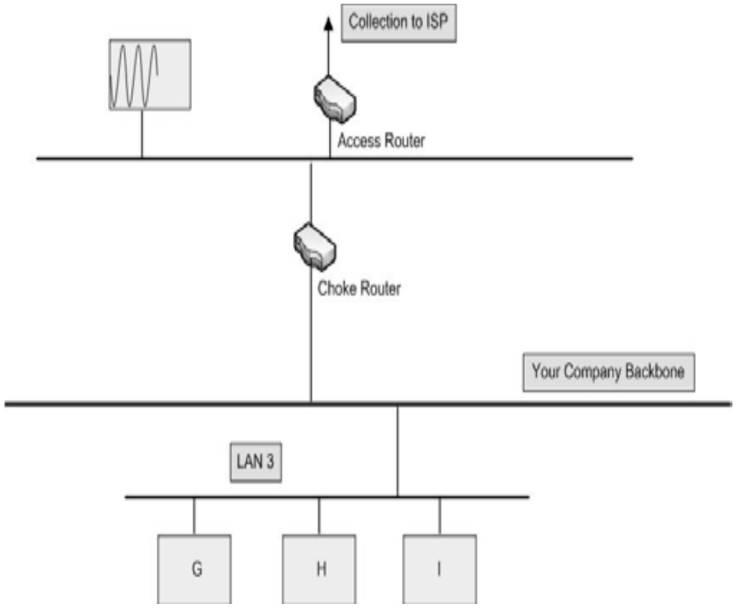


Figure 2: A sample packet filtering gateway

It can differentiate between a packet that came from the Internet and one that came from our internal network.
Also It can be identified which network the packet came from with certainty, but it can't get more specific than that.

3) *Hybrid Systems:* In an attempt to combine the security feature of the application layer gateways with the flexibility and speed of packet filtering, some developers have created systems that use the principles of both. In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed Uses of packet filtering and application layer proxies are the other possible ways. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

IV. FUTURE WORK

Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance. Reactive security will no longer work.

Therefore, organizations need to better understand what the future trends, risks, and threats are so that they can be better prepared to make their organizations as secure as possible.

Generally the network security system tools in the past were command line interface (CLI) based. It's only in this last few years that more and more computer and network administration task is done remotely through a web-based tool. Network system tools are very important no matter whether they are GUI or CUI, in today's heavily inter-connected era.

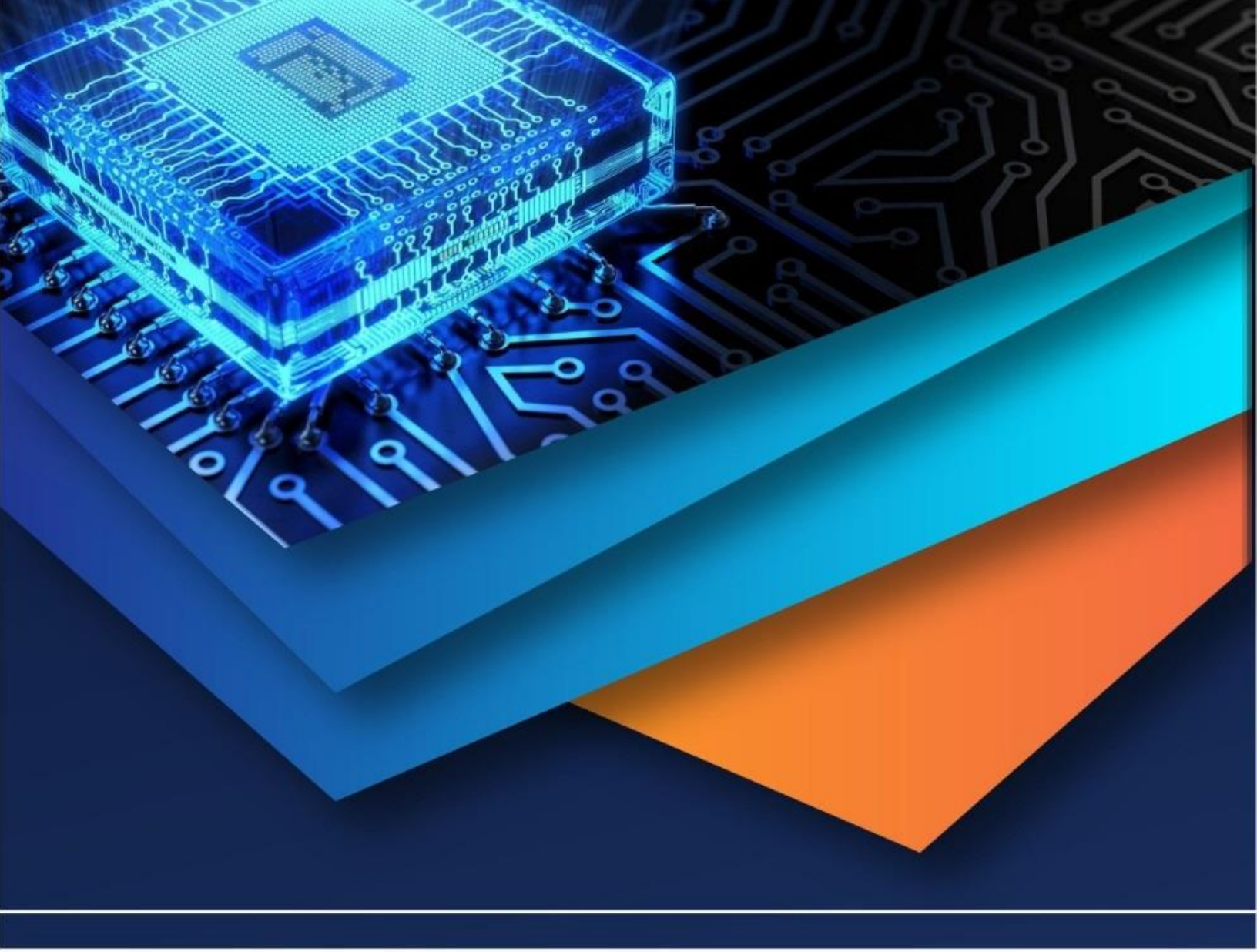
V. CONCLUSION

Network Security is an important concept that is gaining attention as more and more internet usage is increasing. The security threats and various protocols were analysed to maintain the network security. When an attack become sophisticated so does the technology becomes. Today biggest challenge is enforcing policies against these threats.

This paper is basically trying to tell about the various cyber-attacks and the various security methods that can used to prevent our device from getting attacked.

REFERENCE

[1] https://www.ijert.org/a-review-paper-on-cyber-security
[2] https://www.researchgate.net/publication/267691532_MODERN_NETWORK_SECURITY_ISSUES_AND_CHALLENGES



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY