ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Improvement of Overall Network Security Using Routers

M.Nagalakshmi
Assistant Professor,
RITW, Hyderabad.

K.V.Ramani
Assistant Professor,
RITW, Hyderabad.

Abstract:

As the internet grows and computer networks become larger and superior, network security has become one of the most significant factors to consider. Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. In this paper a design and implementation of a network security model was presented, using routers gateways and firewall. This paper also examines network security weakness in router and firewall network devices, type of threats and responses to those threats, and the method to prevent the attacks and hackers to access the network.

Keywords:

Network Security, Routers, Firewalls and Network management.

Introduction:

In today's era, almost every single organisation uses a computer and has a computer network to send, receive and store information. Whether it's sending emails, storing documents, or serving information through a web server, it is very important to focus on security, especially if your network contains sensitive, confidential and personal information. Network security affects many organisations, whether they are large, small, or government organisations. If network security is breached an intruder can do all sorts of harm. That is why people need to be aware of and to be educated about network security and how to secure their computer and network. Systems are required to be updated regularly as new security flaws are discovered. Without being up to date, it makes it easy for a hacker to gain unauthorized access to the system.

Breaches of confidentiality:

Each business will identify with the need to keep certain critical information private from competitor eyes. Data destruction: Data is a very valuable commodity for individuals and enterprises alike. It is a testament to its importance when the proliferation of backup technology available today is considered. Destruction of data can severely cripple the victim concerned.

Data manipulation:

A system break-in may be easily detectable, as some hackers tend to leave tokens of their accomplishment. However, data manipulation is a more insidious threat than that. Data values can be changed and, while that may not seem to be a serious concern, the significance becomes immediately apparent when financial information is in question.There are many more potential threats that can cripple a system.

Security Attacks:

Not only do you have to focus on security, you also have to be aware of the types of security attacks that can happen on your computer network. Before we go on to discuss about the types of security attacks, an attacker may aim to do one of the following:

Interruption – Interruption is an attack on availability such as a denial of service attack (or DOS). An interruption attacks' aim is to make resources unavailable. Not to long ago, WordPress.com, a popular Blog Hosting Site was faced with a DOS attack taking down the servers so the service was unavailable to its users.

Interception – Interception is an attack to gain unauthorised access to a system. It can be simple eavesdropping on communication such as packet sniffing or just copying of information

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Modification – Modification is an attack that tampers with a resource. Its aim is to modify information that is being communicated with two or more parties. An example of a modification attack could be sending information that was meant to go to one party but directing it to another.

Fabrication – A Fabrication attack is also known as counterfeiting. It bypasses authenticity checks, and essential is mimicking or impersonating information. This sort of attack usually inserts new information, or records extra information on a file. It is mainly used to gain access to data or a service.

Keeping the above in mind, there are two main types of attacks whose aim is to compromise the security of a network – passive attack and an active attack.

Passive Attack:

A passive attack can be split into two types. The first type of passive attack is to simply monitor the transmission between two parties and to capture information that is sent and received. The attacker does not intend to interrupt the service, or cause an effect, but to only read the information.The second type of attack is a traffic analysis. If information is encrypted, it will be more difficult to read the information being sent and received, but the attacker simply observers the information, and tries to make sense out of it; or to simply determine the identity and location of the two communicating parties.A passive attack is usually harder to detect as there is little impact to the information communicated.

Active Attack:

On the other hand, an active attack aim is to cause disruption, and it is usually easily recognised. Unlike a passive attack, an active attack modifies information or interrupts a service. There are four types of an active attack:

Masquerade – To pretend to be someone else. This could be logging in with a different user account to gain extra privileges. For example, a user of a system steals the System Administrators username and password to be able to pretend that they are them.

Reply – To capture information to send it, or a copy it elsewhere

Modification – To alter the information being sent or received
Denial of service – To cause a disruption to the network

Even though a passive attack doesn't sound harmful, it is just as bad as an activate attack, if not worse.

Security Services:

Security services is a service that provides a system with a specific kind of protection. The X.800 OSI Security Architecture defines 6 major security service categories, that once a system satisfies these 6 categories, the system is X.800 compliant.

Confidentiality – Protects data from being read or accessed by unauthorised personnel

Authentication – Ensures that no one can impersonate someone to be legitimately authorised to access a services they should not access.

Integrity – Ensures data cannot be alternated and messages that are sent and received have not been read, duplicated, modified or replayed to another party.

Non-repudiation – Prevents the sender or receiver from denying the transmission of a sent or received message. The sender and receiver are to be able prove that they sent or did not send or received a message

Access control – Limits and control access to certain system applications to certain users

Availability – Ensures the service is only available to legitimated users and not available to users who do not have access to the application

Focus of implementation of Network Security:

Deter – To educate people and discourage people to break into systems for illegal and malicious reasons
Prevent – To put in place measures to prevent unauthorised access. This can be authorising uses with

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

special access, encrypting communication, and updating security systems.

Detect – To become aware of a security breaches. This could be setting up logs to record who has accessed items or used the system

Correct – To implement a fix to the flaw discovered in a system. If someone has breached the security of the system, implement measures to prevent it from happening again

Router:

A router is a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A router uses a combination of hardware and software to "route" data from its source to its destination. A router can be configured to route data packets from different network protocols, like TCP/IP, IPX/SPX, and AppleTalk. Click the following link to learn more about routers.

Routers segment large networks into logical segments called subnets. The division of the network is based on the Layer 3 addressing system, like IP addresses. If the Network Layer (Layer 3) Data packet (IP Datagram) is addressed to another device on the local subnet, the packet does not cross the router and create a traffic congestion problem in another network. If data is addressed to a computer outside the subnet, the router forwards the data to the addressed network. Thus routing of network data helps conserve network bandwidth.

Routers are the first line of defense for your netwprk and they must be configured to pass only traffic that is authorized by the network administrators. Thus a router can function as a firewall if it's configured properly.

Firewall:

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network.

GATEWAY LEVEL SECURITY IN COMPUTER NETWORKS:

India has earned itself a reputation of an IT superpower. Internet Service Providers (ISPs) of India has played a seminal role in accomplishing this status. Today, ISPs across over the country are synonymous with excellent Infrastructure and Statutory support. ISPs are providing Data Communication services including Value Added services to IT/IT Enabled Services (ITES) related industries.The objective of the project is to filter traffic associated with specific lists of URL passing through the Internet Gateway as per the DoT's (Department of Telecom) mandate. Regularly ISPs are receiving Blocking Instructions from DoT to block certain websites at ISP level which is mandatory.

In most of cases, ISPs are receiving blocking instructions to block specific content in a particular domain. By blocking through the IP address is not an effective solution to block the URL's as it would block the access to the entire domain instead of blocking required content in the domain. In such a case, ISPs are not complying with the DoT mandate due to lack of blocking mechanism at the Gateway Level.Network-based URL filtering (NUF) is one of the most widely used tools for detecting and stopping malicious and unwanted web traffic, like preventing anonymous websites as per the instructions of Department of Telecommunications (DoT) at the Gateway level.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

However, currently the conventional techniques still suffer from high bandwidth consumption and high latency issues due to millions of URL analysis requests to the network servers per day. A model of Gateway Level URL filter is proposed to address this issue. In the gateways of NUF is used to cache the analysis results from the network server to accelerate web traffic, alleviate the server load, and reduce bandwidth consumption of the entire NUF service. Analysis and trace-based experiments are employed to explore the properties and evaluate its performance in NUF. The results show that the proposed scheme typically eliminates at least 90% of memory requirements as compared to a general hashing table solution.In ISP, enterprise, and other networks, URL filtering is widely used to prevent users to access unwanted and malicious web sites. Several service and device providers like Fortigate, Juniper, Cisco, Websense, Checkpoint etc provide network-based URL filtering (NUF) as a solution to classify, monitor, and control web traffic. NUF provides two important benefits over gateway-based URL filtering which analyzes the URLs by simply comparing them with the local database in a gateway and updating the database continuously.

However, a service provider of NUF reported that they receive over 100 million requests for URL categorization per day. The bandwidth consumption amongst the gateways and network servers is therefore the key factor of the capacity and the maintenance cost of the service. Furthermore, waiting for the response from the network server indeed introduces processing delay to web traffic. In our preliminary tests, the average network latency from our laboratory to three network servers of a service provider is between 100 to 500 ms. This motivates us to design an efficient model for NUF to reduce the bandwidth cost between the gateways and networkservers, while accelerate the processing time in the gateways of NUF. The first idea is the local caching of URL analysis results in the gateways. The second idea is to use a hashing structure as the data representation of local caching.A wide range of techniques have been proposed for enhancing web applications, like web access security, URL forwarding and lookup engine, and web proxy caching. Web content filtering is one of popular approaches to provide web access security. The key function of this method is the classification on web pages.It provides a hierarchical structure for classifying a large collection of web content.

In the works of different machine-learning-based methods are used to perform web content filtering. Although those methods provide accurate filtering results, it seems to take too much time to process each web page by multiple intelligent techniques. In contrast, Network URL Filter and Gateway Level URL Filter are more appropriate for ISP, enterprise, and other networks.

Conclusion:

This paper deals with and discusses the security weakness in router and firewall configuration system and risks when connected to the Internet .Also this paper presented the tips and recommendations to achieve a best security and to protect the network from vulnerabilities, threats, and attacks by applying the security configurations on router and firewall.

References:

[1]National Communications System, Public Switched Network Security Assessment Guidelines, National Communications System publication, 2000.
[2] Swanson Marianne and Federal Computer Security Program Managers' Forum Working .
[3] Group, Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18, 1998.
[4] Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, FEBRUARY 2004.
[5] Rybaczyk P., "Cisco Router Troubleshooting Handbook ", M&T Books, 2000.
[6] Jo S., "Security Engine Management of Router based on Security Policy," proceedings of world academy of science, engineering and technology, volume 10, ISSN 1307-688, 2005.
[7] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009,
[8] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," Proc. Information Security Conf. (ISC '07), vol. 4779, pp. 189-202, 2007.
[9] Adi Shamir, "Identity-based cryptosystems and signature schemes". In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.