International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 9 ǁ 2021 ǁ PP. 57-59

An Outline for Network Security

Dr. Shivraj V. Patil
Department of Information Technology
Rajarshi Shahu Mahavidyalaya, (Autonomous)
Latur (Maharashtra)

Abstract
The computer networks are used to performance statements and interactions among offices and personals. The networks are comprised of nodes, which are node terminals i.e. single computer, and one or more servers. They are connected by transmission media, some of which are private and others which are open to the public. The example of a network system that is open to society access is the Internet, but many private networks also use publicly-accessible communications. Nowadays, most company's server computers can be accessed by their employees whether in their offices over a private interactions network, or from their homes. Network security involves all activities that organizations, enterprises, and institutions take on to protect the value and continuing usability of assets and the integrity and continuity of operations. An effective network security policy requires identifying threats and then selecting the most successful set of tools to fight them.

Keywords*: Network Security Measures, Unauthorized Entry, Network Threats, Network Attacks, Network Security Management*

Date of Submission: 09-09-2021 Date of acceptance: 24-09-2021

I. Introduction to Network security measures

Maintaining Network security is a broad subject means securing our network from unauthorized entity or Mal ware. The unauthorized entity may modify the information or accessing the network through remote computer may harm the network. Following are some network security measures.

1.1 Availability :

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

1.2 Integrity:

Integrity guarantees the identity of the messages when they are transmitted

1.3 Confidentiality :

Confidentiality means that certain information is only accessible to those who have been authorized to access it.

1.4 Authenticity :

Authenticity is essentially assurance that participants in communication are genuine and not impersonators.

1.5 Non repudiation :

Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message.

1.6 Authorization:

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. [1]

II. Network Threats

Network threats are expert persons who are eager to make use of the security weakness of a network in order to impose costly damage. They can achieve this by using various attacking tools in the market. These attackers have a variety of names depending on what they do as shown in the following list.

2.1 Hacker –This is an individual who attempt to get illegal access to network resources with bad intentions. But however, in early days a hacker was known to be a good computer programmer.

2.2 Cracker – This is a person who tries to gain illegal access to network resources for malicious intentions.

2.3 Spammer – individual who sends bulk of unwanted emails of which may content a virus in an attachment planned harm your computer or to take information from your computer and forward by email to the spammer.

2.4 Phishers – This person by email or other means trap persons into getting personal information such as credit card number or password. They usually cover up as trusted persons.

III. Physical Threats

3.1 Hardware threats can be explanatory by securing sensitive devices in lock where only legal persons can have access. Use of security cameras to monitor access to devices.
3.2 Environmental threats like high temperatures can be avoid by using air conditioners for server rooms.
3.3 Electrical threats may be managed by using UPS. In addition to UPS, use of generator to provide instant power if electrical power is permanently out for some reason.

IV. Network Attacks

There are four groups of network attacks namely:
1. Reconnaissance attack
2. Access attack
3. Denial of service attack
4. Malicious code attack

4.1 Reconnaissance Attack

This attack is also called as information collecting attack. In this, the attacker uses a variety of tools to get valuable information. After information collecting such username and password, the attacker can then launch a brave attack.
'Network engineer tools' by Solarwinds is a good kit for reconnaissance attack. It has all necessary tools for reconnaissance attack. Some tools used in reconnaissance attack involve the following:
• Packet sniffers - for capturing and analyzing packets
A network sniffers monitor's data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called "network probes" or "snoops," sniffers examine network traffic, making a copy of the data but without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels including Ethernet frames. Years ago, sniffers were tools used exclusively by professional network engineers. Nowadays, however, they are also popular with Internet hackers and people just curious about networking. Several sniffer software applications are available on the Web for download. [2]
• Ping sweep - for identifying running computers on the network
• Port scan - to identify open UDP (user datagram protocol) or TCP (Transmission control protocol) ports on target computer
• Internet information queries using WHOIS to get information about domain ownership.

4.2 Access Attack

In this type of attack, the attacker uses tools like hacks and scripts to get access to computers, servers, routers or resources that he is not allowed. He does by cracking the user id and password. This attack is divided as password attack, trust exploitation, port redirection or man in the middle attack.

4.3 Denial of Service (Dos) attack

Dos attack is an attack type that overcomes the resources of targeted device, for example a router, the router cannot render it's require services. DOS attack has different forms as Ping of Death, Syn flood & Email bomb.

4.4 Malicious Code Attack

This is an attack on a computer either by a virus, worm or Trojan horse. The preceding paragraphs look at viruses, worms and Trojan horses.
A worm does not require human intervention to spread from infected an infected host to a new host. When a worm attacks a computer, it copies itself into the computer memory and then launches attack to another vulnerable host.
A virus unlike a worm, attaches itself to a file. It requires human interference to spread from one host to another.
A Trojan horse cover-up like a justifiable program.

V. Network security policy

Network safety consists of the policies accepted by the network administrator to secure the network and the network-accessi0ble resources from illegal access, and steady and nonstop observing and measurement of its efficiency combined together. A network safety plan is a general document that outlines rules for computer network access, determines how policies are compulsory and lays out some of the basic architecture of the company security environment. The document is typically numerous pages long and written by a group. It's a very complex document, meant to rule data access, use of passwords and encryption, email attachments etc. It states these rules for individuals or groups of individuals all through the company. Security plan should keep the malicious users out and also apply control over potential risky users within your organization. The first step in creating a policy is to understand what information and services are available, what the potential is for damage and whether any protection is already in place to stop abuse.

VI. Network security management

Safety Management for networks is different for all kinds of situations. A small network would only require basic safety while large network will require high maintenance and advanced software and hardware to avoid malicious attacks from hacking and spamming.

Some of the securities are as follows:-

- Strong firewall or Unified Threat Management System,
- Sturdy Antivirus software and Internet Security Software,
- For verification, use strong passwords and change it frequently,
- For wireless connection, use a strong password,
- Increase awareness about network security to employees,
- Use an optional network analyzer or network monitor and
- Security framework to mark the company's area.

Network safety consists of the necessities made in a basic computer network setup, plans accepted by the network administrator to keep the network and the network-accessible resources from illegal access, and nonstop monitoring and measurement of its efficiency. The terms network safety and info security are often used interchangeably, however network safety is generally taken as providing safety at the margins of an organization, keeping the unauthorized persons out. Network safety systems today are more effective, so the effort has moved to protecting resources from attack by people inside the business. One response to this insider threat in network safety is to categorize large networks, so that a worker would have to cross an internal boundary and be legitimate when they try to access confidential information. Information security is explicitly concerned with all aspects of protecting information resources, including network security. Network safety starts from validating any user, generally with a username and a password. With two factor authentication something you have is also, or with three factor authentication something you are is also used. Once authenticated, a stateful firewall applies access policies like what services are permissible to be accessed by the network users. Though effective to stop illegal access, this component fails to check potentially harmful content such as computer worms being transmitted over the network. An intrusion anticipation system helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system also monitors network traffic for doubtful content, unexpected traffic and other anomalies to protect the network.

VII. Other safety tools and their disadvantages

There are so many safety tools that are intended to detect system vulnerabilities, these tools have a number of disadvantages, such as-

- Network safety and monitoring is typically assigned to a single central security. The failure of this central security will cause to be the system unable to perform security and susceptible to attack.
- Host-based monitors and integrity checkers can be disabled and audit trails corrupted by intruders.
- As the size and density of the network increases, so does the computational load and data logging requirements placed on this central security.
- As new vulnerabilities are discovered and security advisories are issued, the test suites of these security tools quickly become outdated and new tests are often not available until the next software release.

This thesis outlines a test methodology and model security tool that attempts to overcome these limitations by using autonomous mobile agents.

VIII. Conclusion

Security Management for networks is different for all kinds of situations. A small network would only require basic security while large network will require high maintenance and advanced software and hardware to avoid malicious attacks from hacking and spamming.Network security consists of the necessities made in a basic computer network setup, plans accepted by the network administrator to keep the network and the network-accessible resources from illegal access, and nonstop monitoring and measurement of its efficiency. The terms network security and info security are often used interchangeably, however network security is generally taken as providing safety at the margins of an organization, keeping the unauthorized persons out.

References

[1]. http://www.metainfotech.com/solutions/network-security.php

[2]. R. Prajwala Rani, “Capturing the Data Packet by Setting the NIC Card in Promiscuous Mode”, International Journal of Engineering Sciences & Research Technology, 2(11): November, 2013