International Journal of scientific research and management (IJSRM)
\||*Volume*||*3*||*Issue*||*5*||*Pages*|| *2794-2796*||*2015*||
Website: www.ijsrm.in ISSN (e): 2321-3418

Network Security: Attacks, Tools and Techniques

***Vandna*[1], *Dr. Ritu Sindhu*[2]**
[1] ***Department of Computer Science Engineering,*** *SGT Institute of Engineering & Technology, Gurgaon*
[2] *Associate Professor, CSE Department, SGT Institute of Engineering & Technology, Gurgaon*

ABSTRACT

Network security is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue.

There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network.

Keywords- Network Security, Threats, Cryptography, Ping

INTRODUCTION

The security of network is a big issue for security administrators because network is growing day by day. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues [1]. Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator [2]. Each and every client who is working on the internet wants security of information but sometimes he or she do not know that someone else may be a intruder is collecting the information. Information is an asset that must be protected [3]. Network security is the process by which digital information assets are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability.

To secure the information and the entire network system, one specific methodology is required which can be capable of providing the complete security solutions.

II.BASIC TYPES OF ATTACKS

Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc.

A. Security Threats

There are a number of security threats that can be the cause of a network security attack. Main security threats are denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares, unauthorized access to the network resources and data, accidental deletion of the files and the uncontrolled internet access.

B. Virus Attack

A computer virus is a small program or an executable code that when executed and replicated, perform different unwanted and harmful functions for a computer and a network. Viruses can destroy your hard disks and processors, consume memory at a very large scale and destroy the overall performance of a computer or network. A Trojan is a malicious code that performs harmful actions but it cannot be replicated. Trojan can destroy systems' critical data. A computer worm is a program that replicates to all network and destroy useful data. The viruses, malware, adware and Trojan horses can be prevented if you have an updated antivirus program with the latest pattern files.

C. Unauthorized Access

Access to the network resources and data should be allowed only to the authorized persons. Every shared folder and resources in your network should have been accessed only by the authorized persons and should also be scanned and monitored regularly.

D. Information Theft and cryptography attacks

Another threat to a network is to loss of the important information and this loss can be prevented, if you good encryption methods such as 128 bit security or 256 bit security encryption methods. In this way, your data when transferred through FTP programs, can be encrypted and can't be read or use.

E. Unauthorized application installations

Another virus and security attack prevention method is to install only the authorized software applications to our network server and your all client computers. Nobody should be allowed to install any kind of program which can cause security threats such as songs or video programs, codec, gaming software or other web based applications.

F. Application Level Attacks

The attacker exploits the weakness in the application layer for example, security weakness in the web server, or in faulty controls in the filtering of an input on the server side.Examples include malicious software attack (viruses, Trojans, etc.), web server attacks, and SQL injection.

III. BASIC SECURITY TIPS

This basic Network Security useful security tips and methods to secure your network such as installing a update antivirus program, email scanning programs, network monitoring tools, internet access policy and other security prevention methods. Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers [4, 5]. Network security is a very important aspect of a computer network. Minor security vulnerability can result in a heavy loss of the critical data of your server and other client computers. Keeping the computer as well as network secure, is the big responsibility of the network administrator and the security specialists. There are lot of security measures and prevention methods which I will discuss in this section. Typically a computer network can be attacked by a number of ways such as virus attacks, unauthorized access, cryptography attacks and a number of other security threats. Regularly scan all the network devices, emails, open ports, server and client computers. It's the responsibility of the network administrators to check and deploy the missing security patches in all the network computers. They should also remove the unnecessary network shares, user's accounts, wireless access points and restrict the access to the network users.

A. Turn Off Ping Service

The primary purpose of a ping request is to identify hosts that are currently active. As such, it is often used as part of reconnaissance activity preceding a larger, more coordinated attack. By removing a remote user's ability to receive a response from a ping request, you are more likely to be passed over by unattended scans or from "script kiddies," who generally will look for an easier target. Note that this does not actually protect you from an attack, but will make you
far less likely to become a target.For disable ping outside from your public IP:
for that, the icmpconfig would be the following:

```
icmp deny any echo outside
icmp permit any outside
```

echo requests get dropped,
but all the other icmp types are still allowed.

B. Close unused ports

Ports let the outside world communicate with your computer. Think of a port as a door: when the door is open, anyone can get inside. A closed port keeps your computer safe from unwanted outside communication. In security parlance, the term open port is used to mean a TCP or UDP port number that is configured to accept packets. There are various ports and maximum are by default open in our computer like FTP, TELNET, UDP, SMTP, FTP etc. In general we need only some port like FTP, HTTP etc. If someone wants to enter in our network or system they used these types of open ports. So if not necessary close unused ports. Malicious hackers (or crackers) commonly use port scanning software to find which ports are "open" (unfiltered) in a given computer, and whether or not an actual service is listening on that port. In contrast, a port which rejects connections or ignores all packets directed at it is called a "closed port" [6]. Ports can be "closed" through the use of a firewall.

C. Bind IP To MAC Address

We know that MAC address is unique number which cannot be changed. We can make a list of IP address used in our network and then bind those IP addresses to the particular systems MAC address. After doing this activity no one can use out sider system or laptop in your system
Command for mac binding -:
For example fastethernet port 1

```
Switch# config terminal
Switch (config) # interface fastethernet 0/1
Switch (config-if) # switchport mode access
Switch (config-if) # switchport port -security
Switch (config-if) # switchport port-security violation restrict
Switch (config-if) # switchport port-security mac-binding
Switch (config) press ctrl+z
Switch # write press enter
```

D. Use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack by someone attempting to break into or compromise a system. IDSs use traffic analysis and advanced algorithms to determine if a probe has been conducted. Many IDSs are designed to address increased requirements for security visibility, denial of -service (DoS) protection, anti-hacking detection, and e -commerce business defences. An Intrusion Prevention System (IPS) can take the work of the IDS one step further, by taking immediate action that does not require human intervention, as IDS alarms are generated based on a predefined set of rules.

IV. CONCLUSION

There are a number of ways, which guarantee for the safety and security of your network. Perform regular network security testing. Don’t provide more or unwanted access to any network user. Must have an updated antivirus program. Operating system should be regularly updated. If you have windows based operating system you can update it from the Microsoft website. Keep inventory of your network resources such as devices and software applications. Turn off your computer when you are away and don’t leave your computer unattended. Put a strong network and system administrator password. Use a switched network, so that you can identify the problem very quickly.

REFERENCES

[1] Akin T.,"Hardening Cisco Routers," O’Reilly & Associates, 2002.

[2] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317 - 323.

[3] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology, 2004.

[4]Chen S., Iyer R., and Whisnant K., " Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.

[5] 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

[6] Pcmag.com encyclopedia term

.