International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347:3878, Impact Factor (2014): 3.05

A Review on Network Security Threats and Solutions

Prakhar Golchha[1], Rajesh Deshmukh[2], Palak Lunia[3]

[1, 3]Final Year Engineering Students, Computer Science & Engineering Department, SSIPMT, Raipur, India
[2]Assistant Professor, Computer Science & Engineering Department, SSIPMT, Raipur, India

Abstract: ***Security is a fundamental component of every network design. When planning, building, and operating a network, you should understand the importance of a strong security policy. Network Security is a security policy that defines what people can and can't do with network components and resources. The fundamental purpose of a network security is to protect against attacks from the Internet. There are many different ways of attacking a network such as: Hacker/Cracker attacks whereby a remote Internet user attempts to gain access to a network, usually with the intention to destroy or copy data. The major attacks to network security are passive attack, active attack, distributed attack, insider attack, close: in attack, Phishing Attack, Hijack attack, Password attack etc. However a system must be able to limit damage and recover rapidly when attacks occur. So there are various solutions when any of above attacks occurs. Some of the common solutions of these attacks are firewalls, user account access controls and cryptography, Intrusion Detection Systems (IDSs), Network Address Translation (NAT), Stateful Packet Inspection etc. It is always said that "Prevention Is Better Than Cure" some most common preventions that can be taken to be secured are to keep your operating system updated and by using a reputable antivirus program. [1]***

Keywords: Threats, Trojan, Vulnerable, Sniffers, Botnets, virus, enclave, buffer overflow, protocol, Firewalls, Malicious, Phishing, Sniffers

1. Introduction

With an increasing amount of people getting connected to many networks, the security threats that cause very harm are increasing also. Network Security is a major part of any network that needs to be maintained because information is passing through or passed between many routers, computers etc and it is very vulnerable to attack.[2]

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and open networks have generated an increased need for network security and dynamic security policies.

The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks. As they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks. However, internal threats still exist.

Network security starts with authenticating, commonly with a username and a password. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti:virus software or an intrusion prevention system (IPS) helps to detect and inhibit the action of such malware. An anomaly:based intrusion detection system may also monitor the network like wires traffic and may be logged for audit purposes and for later high:level analysis. Communication between two hosts using a network may be encrypted to maintain privacy. With the development of large open networks, security threats have increased significantly in the past 20 years. So to get secured from these threats preventions should be taken before hand. However instead of closing the network from outside world there are some alternate solutions also to these network attacks. [7]

2. Types of Attack

Classes of attack might include passive monitoring of communications, active network attacks, close:in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation:states. A system must be able to limit damage and recover rapidly when attacks occur.

There are five types of attack:

1) Passive Attack

A **passive attack** monitors unencrypted traffic and looks for clear:text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

2) Active Attack

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These

attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

3) Distributed Attack

A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back: door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

4) Insider Attack

An **insider attack** involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

5) Close: in Attack

A **close: in attack** involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close: in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

One popular form of close in attack is **social engineering** in a social engineering attack; the attacker compromises the network or system through social interaction with a person, through an e:mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

6) Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e:mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

7) Hijack Attack

Hijack attack in a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.

8) Spoof Attack

Spoof attack in a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

9) Buffer Overflow

Buffer overflow a buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

10) Exploit attack

Exploit attack in this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

11) Password Attack

An attacker tries to crack the passwords stored in a network account database or a password: protected file. There are three major types of password attacks: a dictionary attack, a brute: force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute: force attack is when the attacker tries every possible combination of characters.

3. Security Threats

According to IT Security.com the following are ten of the biggest network threats:

1. Viruses and Worms: A virus is a malicious computer program or programming code that replicates by infecting files, installed software or removable media. Whereas a worm is a program or script that replicates itself and moves through a network, typically travelling by sending new copies of itself via email.

2. Trojan Horses: The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Some Trojans are designed to be more annoying than or they can cause serious damage by deleting files and destroying information on your system.

3. SPAM: Spam is any kind of unwanted online communication.

4. Phishing**:** Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

5. Packet Sniffers: Computer network administrators have used packet sniffers for years to monitor their networks and perform diagnostic tests or troubleshoot problems.

6. Maliciously Coded Websites: Malicious code is the term used to describe any code in any part of a software system that is intended to cause security breaches or damage to a system.

7. Password Attacks: Password attacks are the classic way to gain access to a computer system is to find out the password and log in.

8. Zombie Computers and Botnets : In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e:mail spam and launch denial:of:service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. [3]

4. Solution of Network Security

The recommendations to protect your company against Phishing and Spear Phishing include: [9]

1. Never open or download a file from an unsolicited email, even from someone you know (you can call or email the person to double check that it really came from them)
2. Keep your operating system updated
3. Use a reputable anti:virus program
4. Enable two factor authentication whenever available
5. Confirm the authenticity of a website prior to entering login credentials by looking for a reputable security trust mark
6. Look for HTTPS in the address bar when you enter any sensitive personal information on a website to make sure your data will be encrypted

4.1 Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

1. User account access controls and cryptography can protect systems files and data, respectively.
2. Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware: or software:based.
3. Intrusion Detection Systems (IDSs) are designed to detect network attacks in progress and assist in post:attack forensics, while audit trails and logs serve a similar function for individual systems.
4. "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter:attacks. In some special cases, a complete destruction of the compromised system is favoured, as it may happen that not all the compromised resources are detected.[4]

Preventing network attacks

There is also Denial of Service (DoS) and distributed DoS attacks resulting in loss of services such as email, Internet connectivity or causing servers to run almost at a standstill. A correctly configured firewall will prevent most attacks and may use a combination of the following processes to offer protection:

1. **Steal the network:** This is a process in which the firewall effectively 'hides' the protected network so that it does not appear on the Internet.
2. **Stateful Packet Inspection**: Stateful packet inspection technology analyses each packet as it travels through the firewall to make sure that it is legitimate and that the source and destination of each packet are valid.
3. **Network Address Translation (NAT):** NAT removes the IP addresses of computers behind the firewall and replaces them with a single public IP address.
4. **Closing unused ports:** Depending on the configuration of the firewall unused ports, often the subject of hacking attacks can be closed.[5]

Protection of Network from Cyber Attacks:

1. Install IDS/IPS with the ability to track floods (such as SYN, ICMP, etc.)
2. Install a firewall that has the ability to drop packets rather than have them reach the internal server. The nature of a web server is such that you will allow HTTP to the server from the Internet. You will need to monitor your server to know where to block traffic.
3. Have contact numbers for your ISP's emergency management team (or response team, or the team that is able to respond to such an event). You will need to contact them in order to prevent the attack from reaching your network's perimeter in the first place.
4. Ensure that HTTP opens session's time out at a reasonable time. When under attack, you wish to reduce this number.
5. Ensure that TCP also time out at a reasonable time.
6. Install a host:based firewall to prevent HTTP threads from spawning for attack packets.[6]

5. The Future of Network Security

Care taken about network security:

IT departments can no longer simply protect the network perimeter and call their network secure. Cloud services, mobile devices, remote workers and wireless networks are all expanding the network boundary beyond its traditional reach. And as networks become more complicated, IT departments are becoming more concerned with how they can effectively secure data. So phos and research company Vanson Bourne surveyed 571 IT decision makers worldwide to gain a deeper understanding of the impact of these changes to network security. And to discover which issues are causing IT teams the most grief, and how they plan on managing the expanding network perimeter.

6. Conclusion

- Network Security is a very broad field and being a Network Security manager is not an easy job. There are still threats such as password attacks that have no prevention.
- Many of the threats set out to get personal information.

- In some attacks**,** the attacker tries to break the security systems through stealth, viruses, worms, or Trojan horses.
- In attacks like phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank and thus fools the user and retrieves the information.

Computer and network technologies have intrinsic security weaknesses. These include protocol weaknesses, operating system weaknesses, and network equipment weaknesses. Common examples of technological weaknesses are: : HTTP, FTP, ICMP and other protocols are inherently insecure such as operating system security holes and problems.

Thus there are still some attacks which are not yet solved and some are going through researches and are hoped to be solved in mere future.

Reference

[1] http://computernetworkingnotes.com/network:security:access:lists:standards:and:extended/types:of:attack.html
[2] http://www.itsecurity.com/features/network:security:threats:011707
[3] http://www.itsecurity.com/features/network:security:threats:011707
[4] http://en.wikipedia.org/wiki/Computer_security
[5] http://fastnet.co.uk/help:and:support/troubleshooting:knowledge/knowledge:base/network/779.html
[6] http://www.sophos.com/en:us/security:news:trends/security:trends/how:to:protect:your:network:from:cyber:attacks.aspx