A Review of Network Security Threats

Amritpal Singh Gill

Pursing B. Tech., Department of Information Technology

Amritsar College of Engineering & Technology

Er. Parambir Singh

Assistant Professor, Department of Information Technology

Amritsar College of Engineering & Technology

Abstract

Protection is the significant part in the computer technology. The main objective of network security is to secure from threats. This research investigates different security threats which are used to corrupt or insecure a system. To access the database and fetch any important information either within the organization or from different organization threats are used. In the latest couple of years threats are expanding fastly in the industry. The Consequence of individual threats range far, some alter the integrity or confidentiality while others affect the availability of a system. This paper illustrate different types of security threats and also study of its harshness for awareness, so that a common person can easily understand different types of security threats.The different ways for sending a threat to a network such as unauthorized person attacks to gain access to a network, having intention to smash or corrupt the data.

1.Introduction

Security threats disturbs the network and systems,any application or software thatcan corrupt our system we call it security threat. There are various types of security threats which can affect the security of the system through which unauthorized person or organization can illegally access private important data. These threats are so harmful that even they can blast your computer by changing power rating, can delete your data.

Figure 1.[6]

There are method to defend network security threat but no one can guaranteed a secured network.The guarantee to secure network is when the system is off. In this research security threats are classified and described. The main motive of this research is to spotlight various

types of security threats so that every person should be aware of these threats and prevent the threats to happen in their system.

2. Types of Attack

Classes of attack might include passive monitoring of communications, active network 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. A system must be able to limit damage and recover rapidly when attacks occur.

There are many 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.

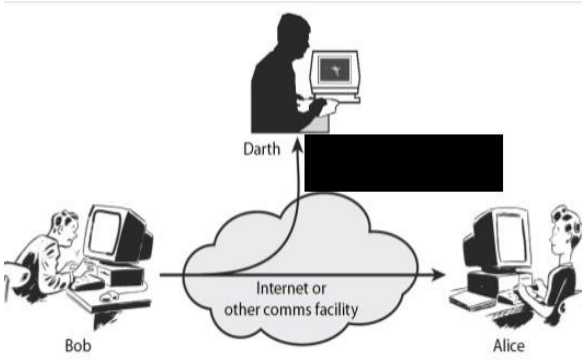

Figure 2.[7]

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

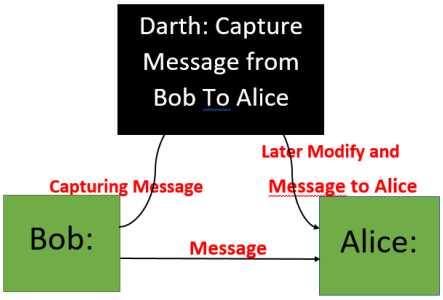

Figure 3

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

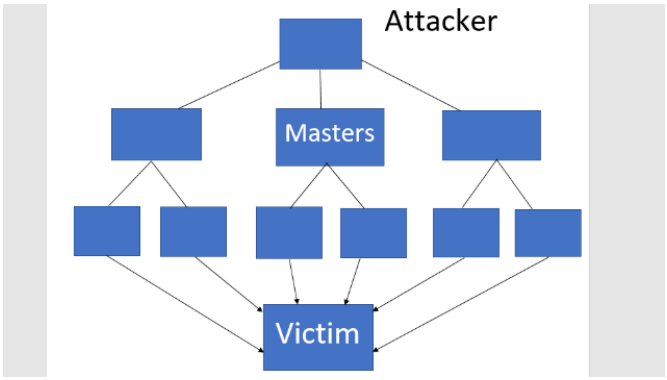

Figure 4.

A distributed attack requires that the adversary introduce code, such as a Trojan horse or backdoor 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 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) Man-in-Middle Attack

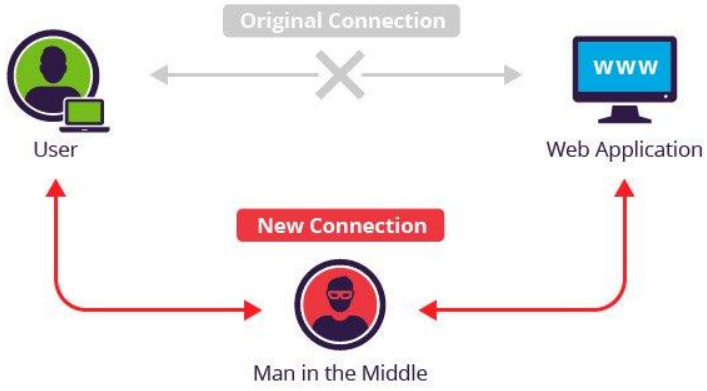

Figure 5. [8]

As the name indicates, there will be a man in between two persons actively tracing the information and controlling the communication transparently. In this attack, the person will be unaware about the attacker and provide all information thinking that communication is going on with the original party. The attacker can then inject new information or modify the information. This allows the attacker to read, delete, modify the data, corrupt the system, inject viruses etc...

6) Phishing Attack

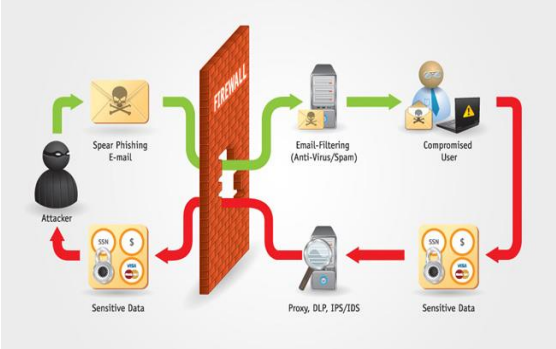

Figure 6. [9]

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 email 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

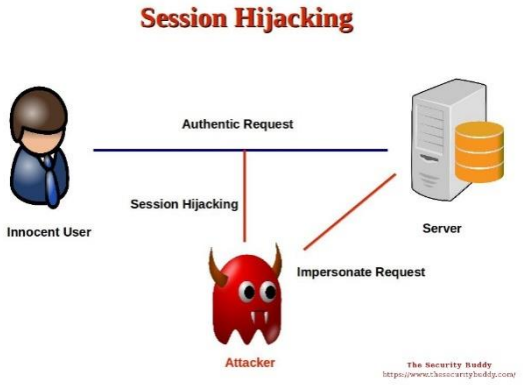

Figure 7. [10]

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

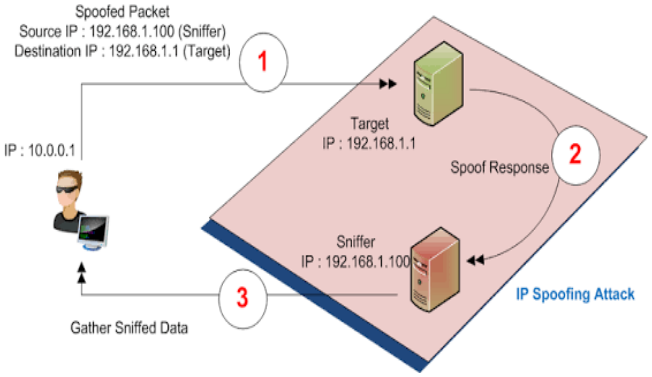

Figure 8. [11]

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

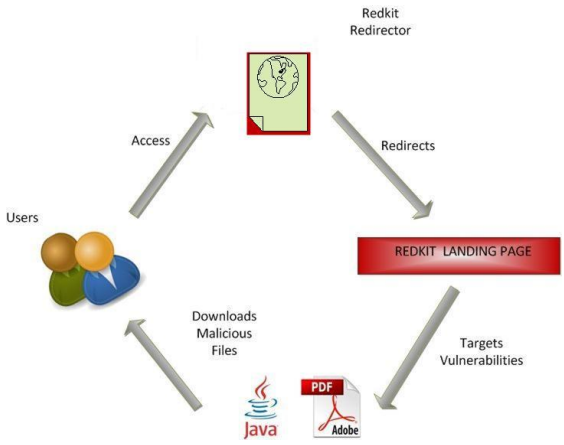

Figure 9. [12]

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

Figure 10. [13]

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. [1]

3. Security Threats

These are the common threats used in networks are:

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 theycan cause serious damage by deleting files and destroying information on your system.

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

4). 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.

5). Password Attacks:

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

6). 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 email 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. [2]

4. Solution of Network Security

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

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 antivirus 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 [3]

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.

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. [4]

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 hostbased firewall to prevent HTTP threads from spawning for attack packets.

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. [5]

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:thre ats:011707
[3]file:///G:/pdf/3-23-139087604528-31.pdf
[4]http://www.ijser.in/archives/v3i4/IJSER1567.pdf
[5]file:///G:/pdf/IIJCS-2017-04-13-6.pdf
[6]https://www.ophtek.com/the-biggest-it-security-threats-coming-in-2017/
[7]https://www.slideshare.net/ssibitamil/technical-seminar-on-security
[8]http://gotowebsecurity.com/phishing-attack-and-its-prevention/
[9]https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html
[10]https://www.thesecuritybuddy.com/malware-prevention/what-is-session-hijacking/
[11]https://greengravityhackers.wordpress.com/2018/04/14/spoofing-attack/
[12]https://securingtomorrow.mcafee.com/mcafee-labs/red-kit-an-emerging-exploit-pack/
[13]https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref