Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

An Empirical study on Network security threats and Solutions

Arvinder Kaur [1], Harpreet Kaur [1], Er. Baldeep Singh[2]
[1] PG student of Computer Sciences Application
[2] Assistant Professor,
SBBSU, Punjab, India

Abstract:- **Network security is a major part of a network that needs to be maintained because information is being passed between computers and is very vulnerable to attack. There are several types of threats to the computer that can harm our secret information. To recover their information there are different solution develop by various scholars. In this paper we will discuss on a several security threats and its solutions.**

Keywords:-**Network security, Threats, Attack.**

1. Introduction

Computer network may be defined as collection of computer and peripherals which are connected together some communication medium. It is basically inter connection of various computers for the purpose of resource sharing. In computer network networked computing devices exchange data with each other using data link. The connection establishes between either wireless media or cable media. It enables computer communicate with each other and to share commands data and hardware and software resources.
Computers network basically built from two components hardware and software. Both components have their own vulnerabilities [1] and risks. They explain some threats and solutions.
Types of Threats:-
Hardware Threats
Software Threats

2. Hardware Threats

Hardware threats:-Hardware threats are easy to detect in comparison with software threats. These threats [2] can harm both devices and data. Hardware threats need physical access which makes it difficult option for Hackers. Hardware[3] Threats is a common cause of data problems are Power can fail, electronics age, you can mistype there are accidents of all kinds.
There are some solutions of Hardware threats:-
2.1. Physical Threat
2.2. Electrical Threat
2.3. Environmental Threat
2.4. Maintenance Threat

Physical Threat:-Physical threats are occur improper installation, selecting wrong components, lack of knowledge, unsecure or less secure network components are main problems of physical threats. There are mainly two types of physical threats.
a. Accidently
b. Intentionally
There are some solutions of Physical threat
2.1.1. Always Purchase branded and genuine components.
2.1.2. Hire experienced and knowledgeable technical staff.

Electrical Threat:-Any Electrical power failure that may be voltage fluctuation can cause hardware threat.
There are some solutions of Electrical Threats:-
2.2.1. Use UPS (Uninterruptible Power Supply) for critical network resources.
2.2.2. Use RPS (Redundant power supplies) for critical network.

Environment Threat:-Threats are occur Extreme weather conditions (such as moisture, very high and low temperature) can also network devices.
There are some solutions of Environmental Hardware Threats
2.3.1. Always maintain room temperature and humidity level between these parameters.
2.3.2. Protect a network devices away from direct sun light and heavy winds.

Maintenance Threat:-These threats are occurred improper disaster planning trigger the maintenance. It includes lack of spare parts, poor cabling, on components. There are some solutions of Hardware Threat:-
All components are clearly label
Cabling equipment in racks securely
Always maintain a sufficient stock of critical spare parts for emergency use.

3. Software threats and solutions

Software threats[4] are harmful pieces of computer code and application that can damage your computer and steal your financial and personal information. Software threats can generally problem or an attack by one or more types of malware program.
Security threat involves three goals:-
3.1. Confidentiality
3.2. Integrity
3.3. Availability

Confidentiality: - This goal defines how we keep our data private from eavesdropping[5]. Valuable information or sensitive data must be protected from unauthorized access. Packet capturing and Replying are the example of threats for this goal. Data encryption is used to achieve this goal.

Integrity: - This goal defines how we avoid our data from being altered. We can match data from original source through using Hashing[6]. Data hashing is used to take the

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

fingerprint of data.
Availability: - This goal defines how we keep available data to our genuine users. It means information must be available to all authorized during their needs. DoS (Denial of service attacks) is the example threat for this goal.

4. Type of Network Security Attack

4.1. Passive Attack
4.2. Active Attack
4.3. Insider Attack
4.4. Password Attack
4.5. .Packet Capturing attack
4.6. Denial of service attacks

Passive Attack:-passive attack is indirect attack. The attacked host is completely unaware about this; hence it is called Passive attack. Attacker is try to observe the host.
Active Attack:-Active attack from the word active, it is clear that is nothing but direct Attack.
In this case the attack one get aware of attack.
Insider Attack:-According to a survey more than 70% attacks are insider. They are divided in two parts; intentionally and accidentally. In intentionally attack is damage network infrastructure or data. Intentionally attacks are done by frustrated employees for money or revenge. In accidentally attack, damages are done by the lack of knowledge and carelessness.
Password Attack:-In this attack are Adversary tries to login with guessed password. Two methods are use for this attack are Brute force[9] and dictionary attack[10]. The Brute force attack is tries to all possible combination of all word. In dictionary method are Adversary tries with word list of potential password.
Packet capturing Attack:-Packet capturing attack is part of passive attack. In this attack an attacker are use to packets capture software which software are captures all packets from wires.
Denial of Service Attacks:- DoS[7] attack is a series of attacks. It refers to the unavailability of resource which blocked or degraded by an attacker. This attack an adversary tires to misuse the legitimate services. Several networking are available for troubleshooting[8]. Attackers are use this troubleshooting for evil purpose. For example ping command is used to test the connectivity between two hosts. An adversary can use this command to continuously ping a host with oversized packets. In such a situation target host will be too busy in replying (of ping) that it will not be able run other services.

Use genuine software and keep it up to date.
Avoid pirated software as they may contain virus and worms.
Use difficult password.
Disable unnecessary services

5. Conclusion

As information travels with in the network and outsider of it, it faces various threats of interception and interference by third party intruders. So, keeping this data secure a network is undertaken with three main objectives i.e confidentiality, integrity, availability with the specified solutions in this paper .We can protect our information from hardware and software threats that can be harm our information.

References

[1] "Term:Vulnerability". fismapedia.org
[2] Internet Engineering Task Force RFC 2828 Internet Security Glossary.
[3] J. Clark, S. Leblanc, S. Knight, Compromise through USB-based Hardware Trojan device, Future Generation Computer Systems (2010) (In Press).
[4] "Check Point Unveils 'Software-Defined Protection' Security Architecture"
[5]"eavesdrop". Online Etymology Dictionary..
[6] "Hash Functions". cse.yorku.ca. September 22, 2003. Retrieved November 1, 2012. the djb2 algorithm (k=33) was first reported by dan bernstein many years ago in comp.lang.c.
[7] "Understanding Denial-of-Service Attacks"
[8] "Troubleshooting at your fingertips" by Nils Conrad Persson. "Electronics Servicing
[9] "ElcomSoft uses NVIDIA GPUs to Speed up WPA/WPA2 Brute-force Attack". ZDNet
[10] Jeff Atwood. "Dictionary Attacks 101".