Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.235 – 237

AN OVERVIEW OF NETWORK SECURITY- ITS TYPES AND TECHNIQUES

NISHU SETHI

Gurgaon, India

NETWORK:
An interconnected computers or devices which share the hardware and software resources for millions of users. Each of these networks are being given a unique address referred to as Internet Protocol(IP)Address which is numerically defined and Structured as A:B:C:D, where A,B,C,D are defined in the range from 0-255. A,B,C represents the network address and D defines the address of the computer or the device on user end. Networks are present everywhere in your life.

SECURITY:
Security is defined as the safe state which is free from the risks. It is the process to protect or safeguard your data from others. It is a survey of dependence, limited facilities and searching the right balance among all the players in the preoccupation to make everything work ideally.

Types of Security:

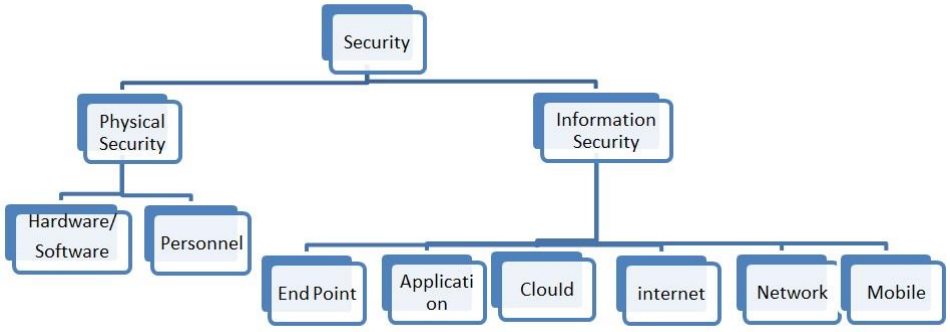

Fig: Types of Security

Physical security:
Physical security is the protection of data, hardware, personnel, software, and networks from physical actions, which can damage an organization. It includes terrorism, fire, natural disasters, theft etc.
Information security:
Infosec protects the information from the threats to achieve confidentiality, Integrity and Availability. It includes Application Security, Cloud Security, End point Security, Internet Security, Mobile Security, Network Security.

NETWORK SECURITY
Network security means the protection of network and data including hardware and software technologies from the threats. Most common threats include worms, spyware, Trojan horses, viruses, zero hour attack, Denial of Service attack, data interception and identity theft. Network Security works on multiple layers of Security.
Steps to protect Network from attacks:

1. **Analysis**: The detailed requirements of the network and the threats that could imply on that are collected and are being analysed to determine the existing system
2. **Implementation**: Once the analysis is being done now it is ready to implement a network security system that provides protection and has sufficient authorization policies.
3. **Testing**: When the security system is implemented it is used to perform tests on various types of threats using a large no of test cases to make sure that all of the features are working correctly and are completely protecting the network against any threats.
4. **Modify**: After Testing is performed the results will reveal the shortcomings of your system and where it can be changed to increase the efficiency of the security system.

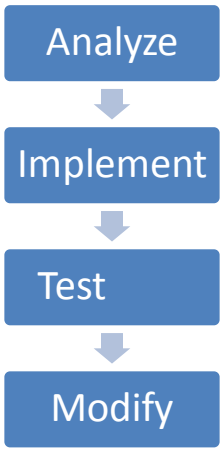

Fig: Steps to protect Network

Techniques for Network Security:
Network Scanning: These are fast and can efficiently scan the hosts, depending on the number of hosts available in the network. They are highly automated and are available with many freeware tools for which it requires expertise to interpret the results. Also these techniques are not so costly.

Vulnerability Scanning: This type of technique is used to identify the known vulnerabilities i.e. the surface vulnerability and could provide advice on removing those discovered vulnerabilities. Also these are easy to run and available in high costs.

Penetration Testing: Penetration Testing verifies the vulnerabilities which are beyond the surface vulnerability level and are repeatedly exploited to gain greater efficiency, where the vulnerabilities are not theoretical. It is very time consuming process because all the hosts available on large or medium sized networks are tested individually. This could be dangerous if handled by inexperienced testers.

Password Cracking: This technique is used to quickly find the password of the user or the network, and can clearly show the strength of the password to be cracked. But few organizations do not support this type of technique due to and have restricted the proxy sites for avoiding hacking.

Log Reviews: this type of technique acts as the source of data which provides the excellent information based on the existing records, which makes the task tedious to manually review and automated tools do not work perfectly for these because they can filter the vital data.

File Integrity Checkers

Virus Detectors

War Dialing

War Driving

