TYPES OF ATTACKS

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

Different types of attacks are as follows:

1. Operating system attack
2. Application level attack
3. Shrink wrap code attack
4. Misconfiguration attack

1. Operating system attack: An operating system attack is done when the operating system in been installed at that time the hacker hacks it because the default setting of operating system is such that all its ports, nodes are open so the hacker can easily destroy our operating system or can easily get the information required.

2. Application layer attack: An application layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

1. Read, add, delete, or modify your data or operating system.

2. Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.

3. Introduce a sniffer program to analyse your network and gain information that can eventually be used to crash or to corrupt your systems and network.

4. Abnormally terminate your data applications or operating systems.

5. Disable other security controls to enable future attacks.

3. Shrink Wrap code attack: In shrink wrap code attack this takes the advantage of the built-in codes and scripts most off-the-shelf application come with. These scripts and code pieces are designed to make installation and administration easier but can lead to vulnerabilities if not managed properly.

4. Misconfiguration attack: In this attack it states that if you are not a smart administrator so you always make mistakes like forget to give permission to authorised person and then you bring new device in your organisation you just leave it as default so hacker can use default setting to access a device always set a password and user name as your organization name .Thus hacker can easily hack your all important information or also can destroy it easily.

Related Posts:

1. Security threats
2. Computer and cyber security
3. Introduction to network security

4. Intrusion detection tool
5. Categories of security assessments
6. Security terminologies and principals
7. Intoduction to intrusion
8. Intrusion detection tool
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer