Network Security - Overview

Published on Sunday, December 27, 2015

Hi Folks,

We'll start with overview of network security today, relevant components of this topic will be covered in upcoming articles. Any doubts or suggestions- do use comments section!

==> This article is a part of PK Series (IT Officers)

What is Network Security?

Network Security is the protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to system. A simple example of network security is an anti-virus application that we use in our computers.

Kinds of security elements required are:

1. **Authentication** - process of reliably verifying the identity of someone by means of a password, smart card, bio metrics etc.

2. **Confidentiality** - Protecting information from being read or copied by anyone who is not explicitly authorized by owner of that information.

3. **Integrity** - Protecting information from being deleted or altered in any way without permission of the owner.

4. **Availability** - System should be accessible as and when the users want it. (*how would you study if bankexamstoday.com is down half the time*)

5. **Non Repudiation** - The ability of receiver of information to prove that sender actually did send that message.

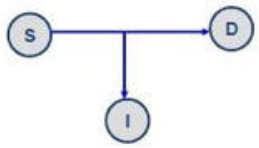
6. **Auditing** - The ability to record events that might have some security relevance. Audit trail may allow undo operations to help restore the system to previous good state.

Security Attacks

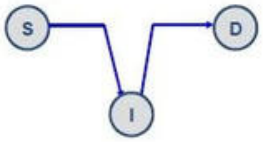
Any action that compromises the security of information is said to be a security attack. Below are discussed four types of attacks:

1. **Interruption** - attack on availability

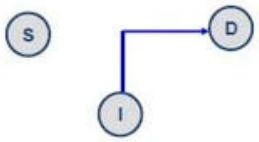
2. **Interception** - attack on confidentiality



3. **Modification** - attack on integrity



4. **Fabrication** - attack on authenticity



Passive and Active Attacks

1. **Passive Attack** - It is said to occur when an unauthorized entity obtains information that is being transmitted (eavesdropping). It is comparatively difficult to detect. Passive attacks can be of two types:
When the observer tries to know the content being transmitted.

When the observer tries to know the location, identity of users.

2. **Active Attack** - It is said to occur when an unauthorized entity modifies the original data stream or creates a false one. It can be further divided into four categories:
a) **Masquerade** - In this attack, one entity pretends to be a different entity.
b) **Replay** - In this data is captured passively and transmitted subsequently to produce an authorized effect.
c) **Modification** - In this, some portion of legitimate message is altered before it reached the intended recipient.
d) **Denial of Service** - It prevents the normal use of communication facilities. DoS attacks can be done at application layer or network layer specifically. In application layer attack, an attempt is made to overload the server by sending a large number of fake requests resulting into its failure. In network layer attack, an attempt is made to clog the connecting architecture i.e routers, switches, E.g - SYN flooding.

Security Tools

1. Cryptography (symmetric and asymmetric)
2. Firewalls and Proxies (Ipchains, Iptables)
3. TCP wrappers and UDP relayers
4. Authentication Modules
5. Kernel level security in Linux
6. Log files (/var/log/*)

We'll start with cryptography from next article onwards.

Quote of the day

If you want to shine like a sun, first burn like a sun. - *Late Shri A.P.J Abdul Kalam*