1.Alert\Alarm

A signal suggesting that a system has been attacked.

2.Firewalls

The network security door. A firewall is not an IDS but their logs can provide valuable IDS information. A firewall works by blocking unwanted connections based on rules or criteria, such as source address, ports etc.

3.Appliance

Rather than install an IDS onto an existing system, ready built IDS appliances can be purchased which are usually rack mounted and only have to be plumbed into the network. Some examples of IDSs which are available as appliances are CaptIO, Cisco Secure IDS, OpenSnort, Dragon and SecureNetPro.

4.Attacks

Attacks can be considered attempts to penetrate a system or to circumvent a system's security in order to gain information, modify information or disrupt the intended functioning of the targeted network or system.

5.Evasion

Evasion is the process of carrying out an attack without an IDS successfully detecting the attack. The trick is making the IDS to see one thing and the target host another. One form of evasion is to set different time to live (TTL) values for different packets.

6.True Positive

A legitimate attack that triggers an IDS to produce an alarm.

7.False Positive

An event signaling an IDS to produce an alarm when no attack has taken place.

8.False Negative

A failure of an IDS to detect an actual attack.

9.True Negative

When no attack has taken place and no alrm is raised.

10.Noise

Data or interference that can trigger a false positive.

11.Alarm Filtering

The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks.

12.Attacker or Intruder

An entity who tries to find a way to gain an unauthorized access to information,inflict harm or engage in other malicious activities.

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool
10. Categories of security assessments
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