APPLICATION AND SIGNATURE - BASED IDS

Application-Based IDS

A refinement of the host-based IDS is the application-based IDS (App IDS). Whereas the HIDS examines a single system for file modification, the application-based IDS examines an application for abnormal events. It usually does this examination by looking at the. files created by the application and looking for anomalous occurrences such as users exceeding their authorization, invalid file executions, or other activities that would indicate that there is a problem in the normal interaction between the users, the application, and the data. By tracking the interaction between users and applications, the App IDS is able to trace specific activity back to individual users. One unique advantage of the App IDS is its ability to view encrypted data. Since the App IDS interfaces with data as it is processed by an application, and any encrypted data that enters an application is decrypted by the application itself, an App IDS does not need to become involved in the decryption process. This allows an App IDS to examine the encryption/decryption process and identity any potential anomalies in data handling or user access.

According to the Missouri State Information Infrastructure Protection Agency, "application-based IDS may be configured to intercept the following types of requests and use them in combinations and sequences to constitute an application's normal behavior:

File System (file read or write)

Network (packet events at the driver (NDIS) or transport (TDI) level)

Configuration (read or write to the registry on Windows)

Execution Space (write to memory not owned by the requesting application; for example, attempts to inject a shared library DLL into another process) "8

Advantages and Disadvantages of App IDSs: The following is a summary, taken from Bace and Mell. of the advantages and disadvantages of App IDSs:

Advantages:

1. An App IDS is aware of specific users and can observe the interaction between the Application and the user. This allows the App IDS to attribute unauthorized activities to specific and known users.
2. An App IDS is able to operate even when incoming data is encrypted since it is able to operate at the point in the process when the data has been decrypted by applications and has not been re-encrypted for storage.

Disadvantages:

1. App IDSs may be more susceptible to attack than other IDS approaches, since applications are often less well protecte7:Ciha; network and first as components.
2. App IDSs are less capable of detecting software tampering and may be taken in by Trojan Horse code or other forms of spoofing, It is usually recommended that App IDS be used in combination with "HIDS and NIDS.9

Signature-Based IDS

The preceding sections described where the IDS system should be placed for the purpose of monitoring a network, a host, 0r an application Another important differentiation among IDSs is based on detection methods-in other words, on how the IDS should make decisions about intrusion activity. Two detection methods dominate: the signature-based approach and the

statistical-anomaly approach. A signature-based IDS (sometimes called a knowledge-based IDS) examines data traffic in search of patterns that match known signatures-that is, preconfigured, predetermined attack patterns. Signature-based IDS technology is widely used because many attacks have clear and distinct signatures, for example: (I) foot printing and fingerprinting activities, described in detail earlier in this chapter, have an attack pattern that Includes the use of ICMP, DNS querying, and e-mail routing analysis; (2) exploits involve a specific attack sequence designed to take advantage of a vulnerability to gain access to a system; (3) denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, during which the attacker tries to prevent the normal usage of a system, entail overloading the system with requests so that the system's ability to process them efficiently is compromised/disrupted and it begins denying services to authorized users.10

The problem with the signature-based approach is that as new attack strategies are identified the IDS's database of signatures must be continually updated. Failure to keep this database current can allow attacks that use new strategies to succeed. An IDS that uses signature-based methods works in ways much like most antivirus software. In fact, antivirus software is often classified as a form of signature-based IDS. This is why experts tell users that if they don't keep their antivirus software updated, it will nor work as effectively. Another weakness of the signature-based method is the time frame over which attacks occur. If attackers are purposefully slow and methodical, they may slip undetected through this type of IDS because their actions will not match those of their signatures, which often include the time allowed between steps in the attack. The only way for a signature-based IDS to resolve this vulnerability is for it to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

,