Table of Contents

Introduction:

1.An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

2.Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

3.A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

4.The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS).

5.A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS.

6.It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based

detection (detecting deviations from a model of “good” traffic, which often relies on machine learning).

Comparison with firewalls:

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

Limitations:

1.Noise can severely limit an intrusion detection system’s effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.

2.Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to newer strategies.

3.For signature-based IDSs there will be lag between a new threat discovery and its signature being applied to the IDS. During this lag time the IDS will be unable to identify the threat.

Evasion techniques:

There are a number of techniques which attackers are using, the following are considered

‘simple’ measures which can be taken to evade IDS:

1.Fragmentation:

By sending fragmented packets, the attacker will be under the radar and can easily bypass the detection system’s ability to detect the attack signature.

2.Avoiding defaults:

The TCP port utilised by a protocol does not always provide an indication to the protocol which is being transported. For example, an IDS may expect to detect a trojan on port 12345. If an attacker had reconfigured it to use a different port the IDS may not be able to detect the presence of the trojan.

3.Address spoofing/proxying:

Attackers can increase the difficulty of the ability of Security Administrators to determine the source of the attack by using poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server then it makes it very difficult for IDS to detect the origin of the attack.

4.Pattern change evasion:

IDSs generally rely on ‘pattern matching’ to detect an attack. By changing the data used in the attack slightly, it may be possible to evade detection. For example, an IMAP server may be vulnerable to a buffer overflow, and an IDS is able to detect the attack signature of 10 common attack tools. By modifying the payload sent by the tool, so that it does not resemble the data that the IDS expects, it may be possible to evade detection.

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
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