IDS Signatures

etutorials.org/Networking/Router+firewall+security/Part+VII+Detecting+and+Preventing+Attacks/Chapter+16.+Intrusion-Detection+System/IDS+Signatures/

Cisco IDS network-based solutions are signature-based. Basically, a signature is a rule that examines a packet or series of packets for certain contents, such as matches on packet header or data payload information. Signatures are the heart of the Cisco network-based IDS solution. This section focuses on signatures and their implementation.

TIP

It is important to point out that it is not necessarily the number of signatures that makes an IDS signature-based solution good. Instead, it is the flexibility of the signatures in detecting an attack. For example, in one IDS solution, it might take three separate signatures to detect three separate attacks; in a different solution, a single signature might be capable of detecting all three attacks. Flexibility in signatures, as well as the ability to create your own signatures, should be more of a concern when choosing a signature-based IDS solution.

Signature Implementations

Signatures come in two implementations:

- Context? Examines the packet header for a match
- Content? Examines the packet contents for a match

Context signatures examine only the packet header information when looking for a match. This information can include the IP address fields; the IP protocol field; IP options; IP fragment parameters; IP, TCP, and UDP checksums; IP and TCP port numbers; TCP flags, ICMP message types; and others.

Content signatures, on the other hand, look inside the payload of a packet as well as the packet headers. As an example, many web server attacks send malformed or specific URLs that are contained in application data. As another example, one sendmail reconnaissance attack looks for EXPN and VRFY commands in the application data (this is covered in the Cisco 3103 signature).

Signature Structures

Besides coming in two implementations, signatures support one of two structures:

- Atomic? Examines a single packet for a match
- Composite? Examines a stream of packets for a match

An example of a signature that uses an atomic structure is one that examines a TCP segment header for both the SYN and FIN flags. Because this information is contained in the TCP header, and because this is contained in one IP packet, only one packet must be examined to determine whether there is a match.

Some types of attacks, however, are spread across many packets and possibly many connections. A composite structured signature has the sensor examine a stream of packets for a match. An example of a composite signature is one that looks at a series of fragments from the same connection and determines whether the fragments are overlapping (this would be an obvious attack because a real fragmented packet can be reassembled, whereas overlapping fragments cannot).

Basic Classification

In general, there are four basic categories of signatures:

- Informational (benign)? These signatures trigger on normal network activity, such as ICMP echo requests and the opening or closing of TCP or UDP connections.
- Reconnaissance? These signatures trigger on attacks that uncover resources and hosts that are reachable, as well as any possible vulnerabilities that they might contain. Examples of reconnaissance attacks include ping sweeps, DNS queries, and port scanning.
- Access? These signatures trigger on access attacks, which include unauthorized access, unauthorized escalation of privileges, and access to protected or sensitive data. Some examples of access attacks include Back Orifice, a Unicode attack against the Microsoft IIS, and NetBus.
- DoS? These signatures trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash. Examples of DoS attacks include TCP SYN floods, the Ping of Death, Smurf, Fraggle, Trinoo, and Tribe Flood Network.

Cisco Signature Categories

In implementing signatures, Cisco divided the classification of signatures into eight categories, shown in Table 16-1.

Table 16-1. Cisco Signature Classification Categories

Signature Series	Description
1000	Signatures on IP header rules, which include IP options, IP fragments, and bad or invalid IP packets
2000	Signatures on ICMP packets, which include ICMP attacks, ping sweeps, and ICMP traffic records
3000	Signatures on attacks using TCP, including TCP host sweeps, TCP SYN floods, TCP port scans, TCP session hijacking, TCP traffic records, TCP applications, e-mail attacks, NetBIOS attacks, and legacy web attacks
4000	Signatures on attacks using UDP, including UDP port scans, UDP applications, and UDP traffic records
5000	Signatures on web server and browser attacks using HTTP
6000	Signatures on cross-protocol (multiple-protocol) attacks, including distributed DoS (DDoS) attacks, DNS attacks, Loki attacks, authentication attacks, and RPC attacks
8000	Signatures that look for string matches in TCP sessions/applications
10,000	Signatures that trigger on an ACL violation on a Cisco router (match on a deny statement)