

1. Progression of Packet Filtering

- 1.1. Firewalls
- 1.2. Stateful inspection
- 1.3. Deep packet inspection
- 1.4. UTM or Next Gen firewalls
- 1.5. Application layer firewalls
- 1.6. IPS and signature based filtering

2. Intrusion Detection and Analysis

- 2.1. Protocol analysis
 - 2.1.1.Examples
 - 2.1.1.1. TCPdump
 - 2.1.1.2. Wireshark
- 2.2. Flow analysis
 - 2.2.1.sFlow
 - 2.2.2.NetFlow
 - 2.2.3.JFlow
- 2.3. Network Behavior Anomaly Detection (NBAD)
- 2.4. IDS/IPS

3. Concepts of IDS and IPS

- 3.1. All About the Hosts
 - 3.1.1.IDS: emulating expected behavior from a host
 - 3.1.2.Why IDS and hosts may respond differently
- 3.2. Host based vs Network based
 - 3.2.1.Where the agent/sensor resides
 - 3.2.2.Options for enforcement
 - 3.2.3.Layer 7
 - 3.2.4.Encrypted traffic visible in HIDS/HIPS
 - 3.2.5.Ability to detect distributed attacks with NIPS
- 3.3. Use of Protocol Analysis in IDS/IPS
 - 3.3.1. Not all IPS/IDS engines are full protocol analyzers. Some products rely on simple pattern recognition techniques to look for known attack patterns. While this can be sufficient in many cases, it creates an overall weakness in the detection capabilities. Since many vulnerabilities have dozens or even hundreds of exploit variants, pattern recognition-based IPS/IDS engines can be evaded. For example, some pattern recognition engines require hundreds of different signatures (or patterns) to protect against a single vulnerability. This is because they must have a different pattern for each exploit variant. Protocol analysis-based products can often block exploits with a single signature that monitors for the specific vulnerability in the network communications.
- 3.4. Detection methods of IDS and IPS
 - 3.4.1.Behavior based
 - 3.4.2.Signature based
- 3.5. IPS as enforcement and correction
 - 3.5.1.IPS methods for stopping attacks
 - 3.5.2.IPS methods for correcting packets
 - 3.5.3.IPS and ability to see layer 7

4. Use cases for IDS and IPS

- 4.1. Use cases for IDS
 - 4.1.1. When availability is more important than security
 - 4.1.2. Honeypots or systems to trap malicious attackers, need data for prosecution
 - 4.1.3. Watching outbound traffic for compliance violations
 - 4.1.4. Monitoring networks you do not own or have authority to 'modify'
 - 4.1.5. Silent or transparent monitoring (no IP address on IDS, no alert that traffic was dropped)
- 4.2. Use cases for IPS
 - 4.2.1. Enforcement
 - 4.2.2. Malformed packet correction
 - 4.2.3. Addressing known attacks

5. Attacks and Countermeasures

- 5.1. Insertion
- 5.2. Evasion
- 5.3. Denial of Service
- 5.4. Protocol Attacks
- 5.5. Application Attacks
- 5.6. Attacking IDS versus IPS Systems**

6. Vendor and Technology Comparisons

- 6.1. IBM
- 6.2. McAfee
- 6.3. Cisco
- 6.4. Juniper
- 6.5. Sourcefire IPS
- 6.6. Snort