IDS

Chapter 5

Network & Security

Gildas Avoine

INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
RENNES

SUMMARY OF CHAPTER 5

- Classification
- Network IDS
- Host IDS
- Conclusion

CLASSIFICATION

- Classification
- Network IDS
- Host IDS
- Conclusion

Generalities

- Protection is needed, but looking out and defending is better.
- Do not wait for the symptoms of an attack before reacting.
- Intrusion Detection Systems (IDS) analyze:
  - Network traffic (Network IDS, NIDS).
  - Events on servers (Host IDS, HIDS).
- Analysis can be done in real-time or off-line.

Classification

	Real-time analysis	Off-line Analysis
Network IDS	Traffic Capture and Analysis	Log and Configuration Analysis
Host IDS	Syscall and Registry Inspector	System Log Analysis

NETWORK IDS

- Classification
- Network IDS
- Host IDS
- Conclusion

Network IDS

- Consist of a sniffer and a traffic inspector.
- Predefined rules applied to the sniffed packets.
- Protocols in any communication layer can be considered.
- When a packet activates a rule, an action is performed.
    - Log the event.
    - Trigger an alarm: SMS, mail, web interface, etc.
    - Reset a connection or reconfigure the firewall.

Intrusion Prevention Systems: IPS

- An IPS is an IDS that reacts to an attack.
  - IP level: Filters the source IP address in the firewall (for a while).
  - TCP level: Sends a spoofed TCP reset packet to the destination to kill the connection.
  - Application level: “corrects” a web request to remove special characters.
- Beware of denial of service attacks.

IDS based on Traffic Characterization

- IDS carries out statistics on traffic.
- If a value goes beyond its usual limits, assume there is an attack.
- This system can recognize new attacks.
- It may also not recognize them... (false negatives).
- It sees attacks where there is no attack (false positives).
- The high false positive rate makes this type of IDS unpopular.

IDS based on Signatures

- The IDS has a database of known attack signatures.
  - E.g. Web request with URL of 2000 characters=buffer overflow
  - Signature collected thanks to honeypots.

- It does not recognize new attacks (must constantly be updated).

- False negatives.
  - Manual attacks can have variations that are not detected.
  - Signatures are sometimes too restrictive.

- False positives.
  - There is a priori no false positives, but...
  - IDS often does not know if an attempted attack was successful.
  - IDS does not know if the attack's target is vulnerable.

Snort: Signature-based (www.snort.org)

- Sniffer for Linux and Windows.
- “Signature, protocol and anomaly based inspection methods”.
- Snort analyzes traffic, for example in front of the firewall.
- Sends mails and/or updates the FW’s filtering rules.
- Huge signature database updated by users and developers.

Snort: Example of Signature

- log tcp any 80 − > any any
  - Means "Log TCP packets coming from any host, port 80, going to any host, any port".
- alert tcp any any − > 192.168.1.0/24 143 (content: "|90C8 C0FF FFFF|/bin/sh"; msg: "IMAP buffer overflow!";)
  - Means "Alert when receiving a packet from any host, any port to port 143 of a computer with IP address 192.168.1.0/24, when the packet contains the string '|90C8 C0FF FFFF|/bin/sh' ".

HOST IDS

- Classification
- Network IDS
- Host IDS
- Conclusion

Tripwire: Integrity-based Host IDS

- Tripwire is a typical example of a HIDS with a differed analysis.
- It creates a digital signature of all files and directories that should not be modified.
- The signatures cannot be modified by an attacker.
- It regularly compares files and signatures to detect any modifications.
- It generates an alarm when it detects a modification and can automatically restore the original version of the file.

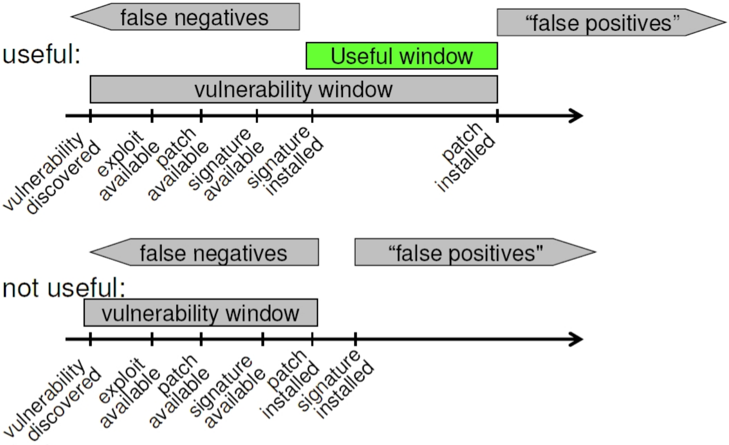
CONCLUSION

- Classification
- Network IDS
- Host IDS
- Conclusion

Conclusion

- IDS with characterization are not yet very efficient.
- IDS with signatures work well but:
  - Majority of the attacks for which we have the signature can be blocked by a firewall.
  - We should first prevent before trying to detect.
  - It is not sufficient to install an IDS, we must also know how to react to attacks and treat the daily quota of false positives.
  - Automatic reactions are usually not advisable due to DoS.
- Affording both of them provides a good in-depth security.
- IDS is typically located in front of the FW.
- IDS within the internal networks creates less frequent and more critical alarms.

Efficiency Window



References

- http://cosy.univ-reims.fr/~fnolot/Download/Cours/reseaux/m2pro/SESY0708/ids-ips.pdf
- http://dbprog.developpez.com/securite/ids/
- http://manual.snort.org