



security-assessment.com

Intrusion Detection

“this is not the packet you are looking for, move along”

About Security-Assessment.com

- Specialise in high quality Information Security services throughout the Asia Pacific region
- Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients
- We are committed to security research and development – Identifying & responsibly publishing vulnerabilities in public and private software
- We are an Endorsed Commonwealth Government of Australia supplier
- Sit on the Australian Government Attorney-General's Department Critical Infrastructure Project panel
- Certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs

Agenda

- Prologue
- Basic Concepts
- Intrusion Detection
- Intrusion Prevention
- Limitations

About Me

- Have had the experience of both running and attacking large scale IDS installations.
 - Thousands of sensors
 - Multiple sites
 - Millions of EOIs per day

Prologue

- Some things in here may seem obvious
- Looking at it as a complete system, braking it up into its components and discussing the vulnerabilities from the perspective of an attacker.

Basic Concepts

An IDS sensor captures traffic and compares it to a rule to generate an Event of Interest which is [hopefully] looked at by an analyst.

Event of Interest

An Event of Interest (EOI) is an output of the system that something may be wrong, different or require attention.

An EOI is not necessarily an attack

An attack doesn't necessarily generate an EOI

Alternatively an attack may be thousands of EOI

An EOI may trigger an active response

IDS – A little history

1st Generation: *Gee that's going to hurt !*

2nd Generation: *Gee that's going to hurt ! - Yep it sure did*

3rd Generation: *Gee that's going to hurt ! - better ask them to stop*

4th Generation: *Gee that's going to hurt ! - better tell them to stop*

5th Generation: *Gee that would have hurt !*

Intrusion Detection

- Two main types of Detection
 - Rule Based
 - Heuristic Based
- Two running modes
 - Real Time
 - Batch Mode
- Generates an EOI that an analyst must action

Intrusion Prevention (as a technology)

- Same as IDS, except with an active response
 - Sending reset (RST) packets
 - Control of other filtering devices (such as a Firewall)
 - Silently drop packet (sensor must be 'in-line')

Limitations

An IDS sensor captures traffic and compares it to a rule to generate an Event of Interest which is [hopefully] looked at by an analyst.

- Potential Limitations are when the IDS:
 - Captures traffic
 - Compares it to a rule
 - Generates an event
 - Someone performs manual analysis

Traffic Capture

- If your attack doesn't go past the IDS, it won't see it. Consider:
 - Network Design
 - Is the IDS only at the top of the network ?
 - Only on Production Hosts ?
 - Route around it ?
 - Hop around it ?

Traffic Capture

- Load Balancing
 - Send half the attack through a different leg.
- Redundant Sites
 - Does the hot site have an IDS too?
 - Is it kept up to date?
 - Is it looked at ? ever ?

Traffic Capture

- Traffic Load
 - Its easy to overload an IDS.
 - 'Stick'
 - Database
 - Packet loss

Traffic Capture

- Encryption
 - SSL. no seriously.
 - VPNs
 - Application level

However: sometimes the existence of a data stream can be enough.. like h4x0r.ru having an SSH (or similar) connection to / from really.important.host.company.com

Traffic Capture

- Confuse it
 - If it can't decode the protocol you are using, It wont (usually) block you.
 - Tell it lies
 - Encode your attack
 - Fragmentation etc.

Rules

- Rules are often not very good
- Commercial Vendors do not disclose them
- You can only write a rule for a known attack
- Generic rules are often easily bypassed

When the Rule is known (eg Snort)

- See what the rule is detecting
 - port ?
 - header data ?
 - string (eg name of exploit)
 - etc
- Find what it is and change it in the attack

Heuristic Rules

Heuristic rules are still rules, they are just automatically generated.

- You must know the network well
- Most networks are under constant attack
- Outage / Change windows

Event of Interest (IPS)

Intrusion prevention systems can actively respond to an EOI

- look for resets (and their TTL value)
- consider traffic load
- is availability or confidentiality more important ?
 - Island the IPS sensor
- In-line devices often fail open
 - overload the sensor

The Analyst

- Analysts come in several forms:
 - The Network / System Admin
 - Doesn't have the time to care. Unless you start to ring the bells of Hell you'll be fine.
 - The Security Admin
 - Old / simple attacks will be picked up, but you can get away with things if you choose your timing well.
 - The full time Security Administrator – 24/7 environment.
 - Usually asleep, playing X-box or out getting food

The Security Analyst.

- An Analyst will have so many attacks and potential attacks to look at, it's all about prioritising. To do this, the Security Analyst will be looking for the following:
 - Evidence of active targeting
 - Identification of history
 - Identification of technique
 - Identification of intent
 - Level of knowledge of the attacker
 - Individual or group of attackers

If you can trick the analyst into ignoring you, (often called an 'exception') you will be able to continue unhindered.
(Exceptions can be created by src, dst, or EOI.)

To Recap..

- It's not just about the technology
- There are many points of vulnerability to consider
- Only one part of the system needs to fail
- It is difficult, but it can be done

Thank you

Questions ..?

Contact me :

Declan.ingram @ security-assessment.com