Reassemble or GTFO

- Getting
- The
- Fragments
- Out

finux@finux.co.uk

Arron Finnon - 17th November 2011 -Deepsec

”Intrusion Detection Systems (IDS for short) main purpose is to monitor systems for signs of intrusion or malicious use. An IDS can either be protecting a single host, this is known as Host-based Intrusion Detection System HIDS, or protecting a network, this is known as Network-based Intrusion Detection System NIDS.”

” @stevelord: @f1nux the 90s just called, they want their frag, flag and source port tricks back #everythingoldisnewagain ”

https://twitter.com/#!/stevelord/status/1280290241727815 69

The worrying thing, Mr. Lord isn't too far from the truth

It goes a long way in showing these issues are inherit and can not be simply “coded out”.

whois finux

- Attack Researcher of iDappcom
  - We specialise in auditing IDS/IPS have some awesome tools for it.
  - I research established, new and emerging evasion techniques and strategies.
  - I also investigate network threats with the aim of seeing how security devices fair against them
- I podcast and speak far too much

Get in contact

- finux@finux.co.uk
  - Feel free to drop me an email. I can give you some links to some awesome stuff.
- @f1nux
- www.finux.co.uk
- www.idappcom.com

Today's Outcome

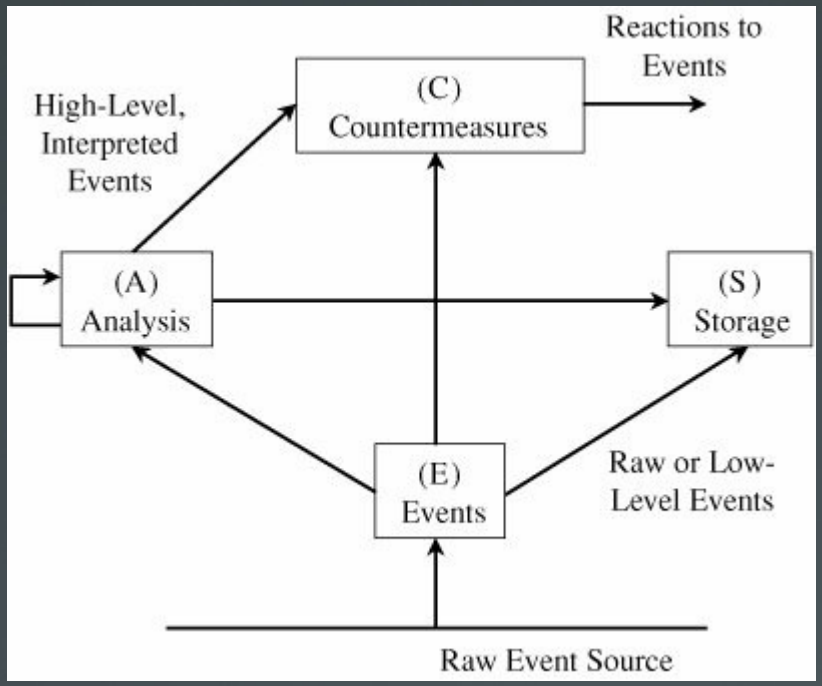
- You should have a basic understanding of how IDSes work
- You should have a basic understanding on the challenges faced by an IDS
- You should understand how an attacker could use these issues/challenges to evade detection

So what is an IDS

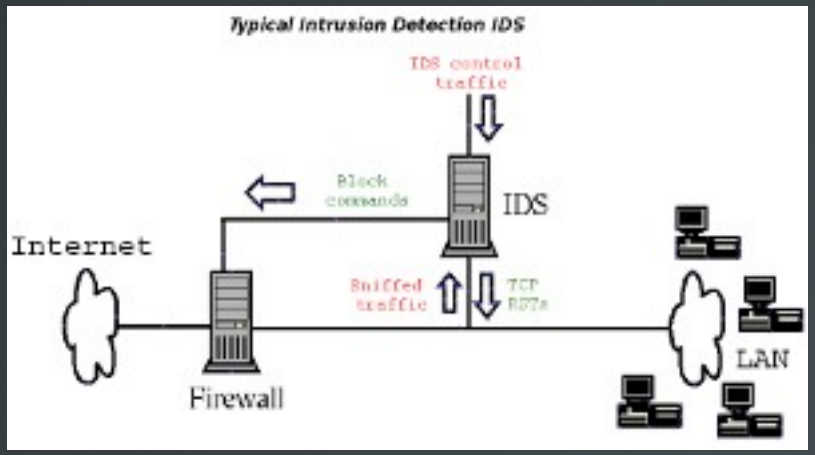
The reality of these Detection Systems is they analyse data to determine if a threat is in play. HIDS use a multitude of system information to basis its analysis on, such as logs, system events, connection states and so on. However due to it's somewhat introverted nature it has little prospective on events occurring on the network. The opposite can be said for NIDS, it's only source of information to base it's analysis on is data being transmitted over the network. NIDSes are unaware of what is happening on a host, and HIDSes are unaware of what is happening on the network.

What is CIDF?

- Common
- Intrusion
- Detection
- Framework

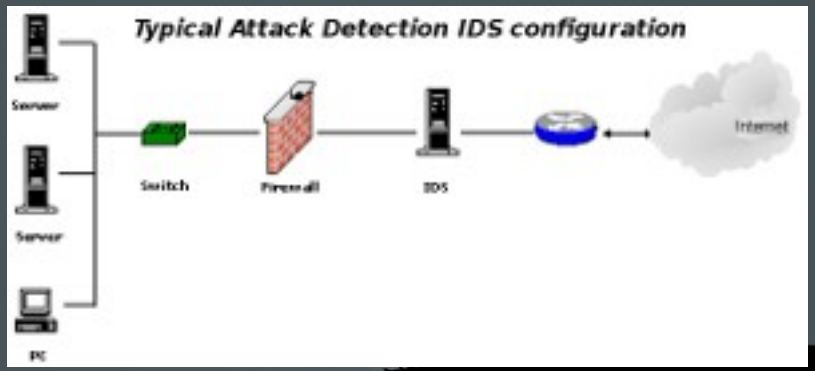


Typical Deployment



Typical Network IDS being deployed to detect intrusions. Its placement enables it to watch the LAN for issues

Typical Network IDS being deployed to detect attacks against the network. Its placement is before a firewall.



Host Vs Network

- Host Intrusion Detection Systems
  - HIDS use a multitude of ”system” information to basis its analysis on
  - somewhat introverted nature it has little prospective on events occurring on the network
- Network Intrusion Detection Systems
  - Only source of information to base it's analysis on is data being transmitted over the network
  - NIDS are unaware of HOST issues

Issues faced by IDSes

- Ambiguous RFC's
- Inconstancies in implementations
- Lack of system resources
- Lack of data to analysis
- Protocols
  - Some are easy to workout in a single packet
    - UDP port 53 ????
  - Some are not
    - TCP port 135 ????

So what's the point

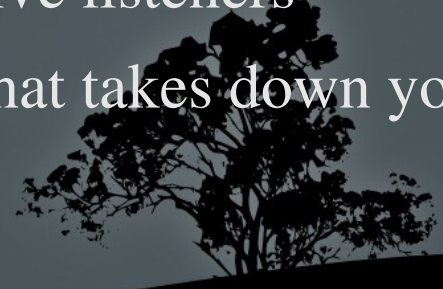
- Well surprisingly vendors tend to oversell IDSes abilities
  - Stops all known attacks
  - Anti-APT, Anti-LulzSec, will SAVE your company
- The thing is they DON'T talk about detection rates
  - If I sucked that bad I wouldn't want to go there too
- They DO talk about throughput
  - Doesn't help the device owner though
  - Blinky lights tell you its ON, doesn't tell you if its effective

Some simple evasions

- Signature Matching
  - AAAAAAAAAAAAAAAAAAAAAAAAA
  - Snort rule for detecting shellcode
  - Oh yeah, that's because all h@x0r5 use A's for their buffers
- HTTP Compression
  - GZIP'd and CHUNKED transfer encoded
  - IDS has no way of knowing what and when the payload will stop.

The horrible truth

- Lots of IDSes only inspect the 1st xx amount of bytes. Normally about 300 or so.
  - Why on earth would you do that
    - Throughput, processing takes time!
    - I can send lots of junk mwhahaha
- Inherently IDSes tend to “fail-open”
  - There is a few reasons why
    - For starters they tend to be passive listeners
    - Who wants to be the company that takes down your bank over an error



Attacking NIDSes

The process of taking an unordered sequence of packets, and reconstructing them is called ”reassembly”

This is only x1 of many techniques that can be used

Of course many IDSes don't fair well in reassembly at all. Snort is a great example of this

Attacking how an IDS interprets a data stream

Sniggers*

Insertion Attacks

You have lost your inner-child if you are not sniggering at that statement!

The aim is;

To trick the IDS into accepting packets that the end-point will reject

.i.e. you have inserted data into its processing/reassembly

****Insertion attacks disrupt stream reassembly by adding packets to the stream sequence numbers***

example

GET /cgi-bin/phf? HTTP/1.1

Pretty easy to detect, a simple signature could be written!

GET /cgi-bin/**p**leasedontdetect**t**h**i**s**f**orme

Something as simple as; if the IDS is not checking IP checksum's, then the end-point is likely to reject them .i.e. the stuff in the red

Pretty much a guaranteed to be dropped going over the internet. Unlikely to be effective locally though. However an attacker could “insert” packets for reassembly

Evasions

The aim is;

That the end-point will accept packets that the IDS rejects

The ”accuracy” of the IDS has been defeated

Whole streams could go by unchecked!

We have “evaded” IDS reassembly

example

DF Flag

Do not Fragment Flag could be used in a situation where the end-point MTU (Maximum Transmission Unit) is larger than the IDS's MTU

TCB

Transmission Control Block in essence is a data structure that keeps information relevant to a TCP connection

TCP sequencing is an important factor!

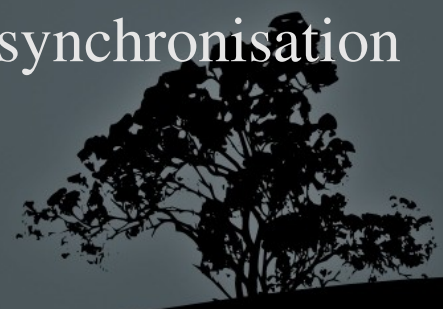
The TCB Issue

- How does an IDS reorder unordered stream?
  - The same was as any other TCP implementation
    - Sequence Number's
- So when does the IDS initiate a TCB?
  - Bloody good question!

You've guessed it, make a mistake here and your bad guy could well be in the clear.

Where to start

- 3 Way Handshake == SYN SYN/ACK ACK
  - Totally susceptible to evasion attacks
  - Miss the 3WH and your IDS is desynchronised from the data stream.
  - This is NOT good!!!!
- Take sequence from traffic
  - Totally susceptible to insertion attacks
  - Establish rouge TCB's and occupy resources
  - Can potentially recover from desynchronisation



Reassembly Attacks

- Reality x2 different looking streams within x1
  - These attacks are the fine line between interpretation of the streams by IDSes and End-Points
- Insertion Vs Evasion
  - Both can have devastating effects on an IDS
- Network Protocol inconsistencies
  - Can happen at TCP as well as IP
  - Example overlapping fragments

Overlapping Fragments

- Windows
  - Always favours the old data in over lapping fragments
- Unix
  - Always favours new data in over lapping fragments
- There are more than ”TWO” IP implementations
  - They all have different ways of dealing with it
- Lets not talk about flags and overlapping
  - :-/

Summary

- IDS/IPS cannot stop all known attacks now never mind unknown ones.
  - Will vendors please stop promising the earth #KthxBai
- IDS/IPS doesn't need to be like a web server!
  - It needs to be like ALL the web servers EVAR!
- You can only analysis what you understand
  - Data/Information is king
- Deep Packet Inspection
  - O'rly

Questions

- If your not too bored with this
  - I have some reading material
  - It is interesting to me
    - More likely works as a replacement for Night Nurse for you though.