University of Southampton
School of Electronics and Computer Science

COMP3210
Network Monitoring

and the Return of the Googly-eyed Laptops

Topics

- Network Monitoring
- Intrusion Detection
- Intrusion Protection

Graeme Bragg
gmb@ecs.soton.ac.uk
Electronics & Computer Science
University of Southampton

How do You Know a Breach Has Happened?

University of Southampton
School of Electronics and Computer Science

- When your company is in the news?
- When your systems are locked?
- When all your data is gone?
- When your customers complain that your website gave them malware?

- This is all after the damage has been done.
- You need to know before, this is where monitoring can help…

Things You Might Want to Monitor

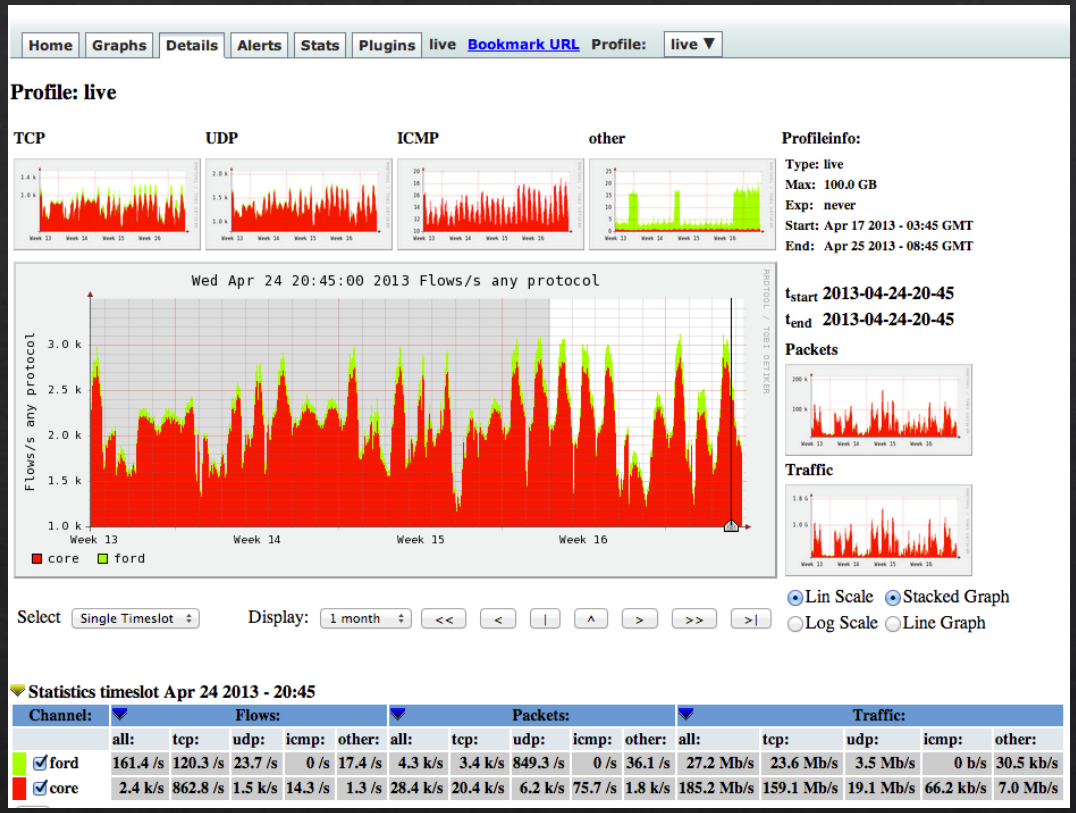
University of Southampton
School of Electronics and Computer Science

- A whole host of metrics that can be monitored to indicate security breaches or just a poorly network:
  - Traffic metadata
  - Traffic payloads
  - ARP/NDP tables
  - Routes
  - Switch port utilisation
  - Firewall logs
  - DNS entries & queries

Network Flow Monitoring

University of Southampton
School of Electronics and Computer Science

- A way to collect *metadata* about traffic for analysis:
  - IP source & destination
  - Protocol(s) and port
  - Packets count and data total
- Can record details of all packets, or just a sample
- A few options:
  - Argus was the first (1984) and still going as an open source project
  - Cisco Netflow (1996) is the most well known
  - sFlow is the industry standard.



Is Metadata Useful?

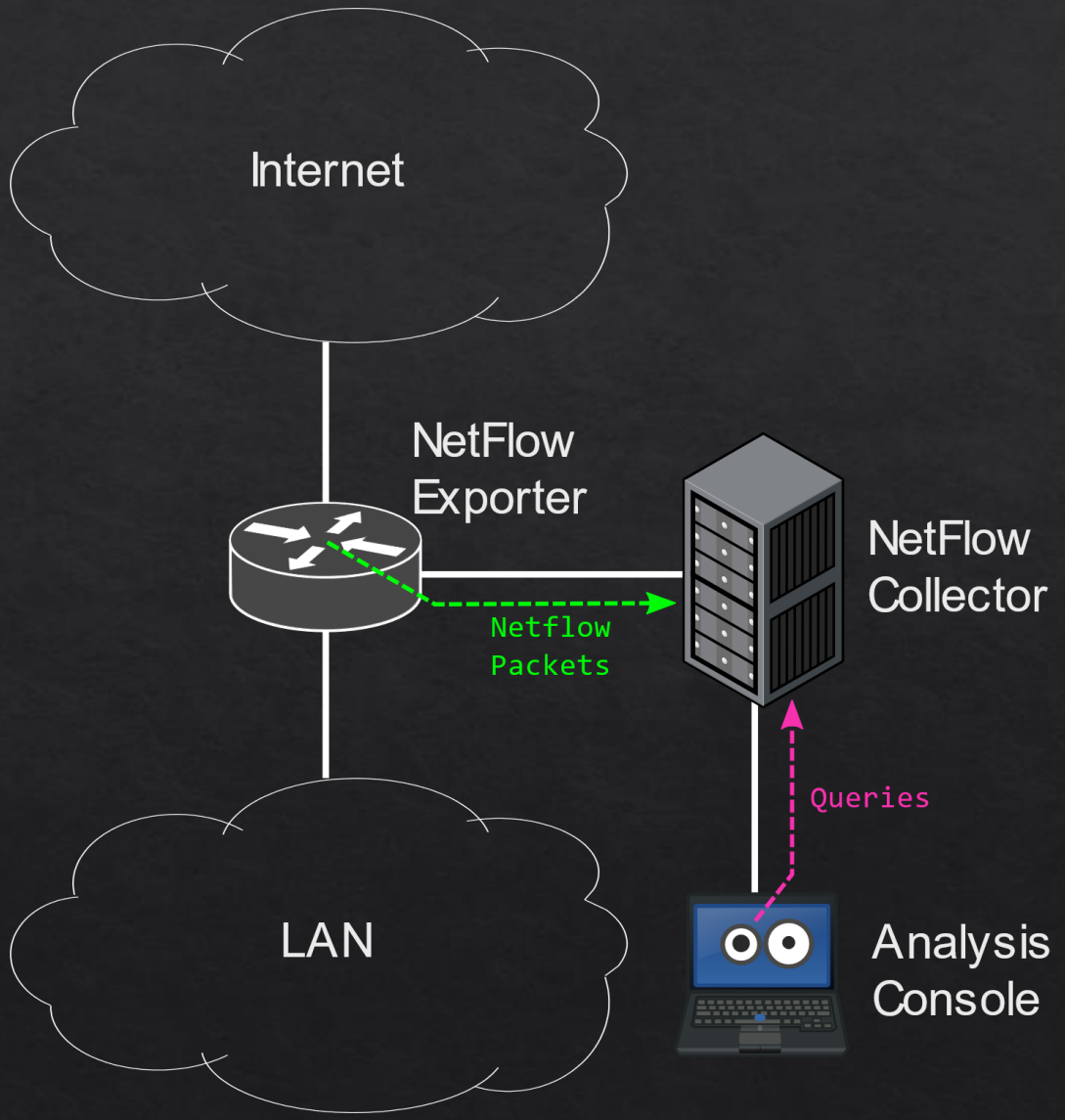
University of Southampton
School of Electronics and Computer Science

- Network flow monitoring can help you spot anomalies with appropriate tools. e.g.:
  - Build a profile of good/normal traffic
  - Spot out-of-profile or known-bad traffic
  - You could do this manually, but automation is good
    - e.g. Cisco Netflow
- Helpful after an attack for finding any other compromised systems
- Can also be useful for network capacity monitoring

NetFlow

University of Southampton
School of Electronics and Computer Science

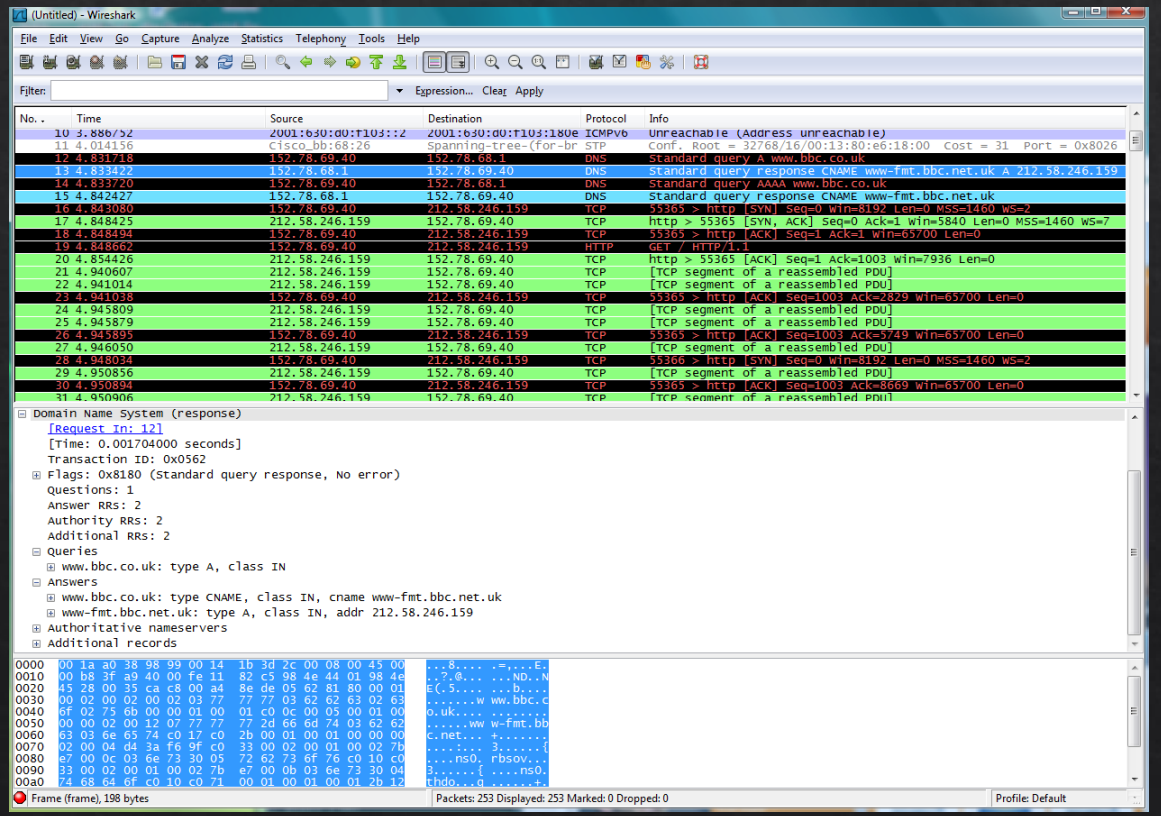
- A three-component system
  - Flow Exporter: A device that records network flows it sees (e.g. a switch, router or dedicated probe) and forwards data to a Flow Collector
  - Flow Collector: stores and pre-processes data sourced from one or more Flow Exporters.
  - Analysis: Performs analysis (and visualisation) of flow data stored in a Flow Collector



Packet Capture

University of Southampton
School of Electronics and Computer Science

- A step beyond network flow monitoring: Capture ***all*** network traffic and payload data for analysis
- Gives ***a lot*** of insight but:
  - It takes up a lot of space
  - Processing it can take a lot of resources
  - Potential privacy issues
- Plenty of tools
  - tcpdump
  - Wireshark/pcap
  - Various commercial offerings

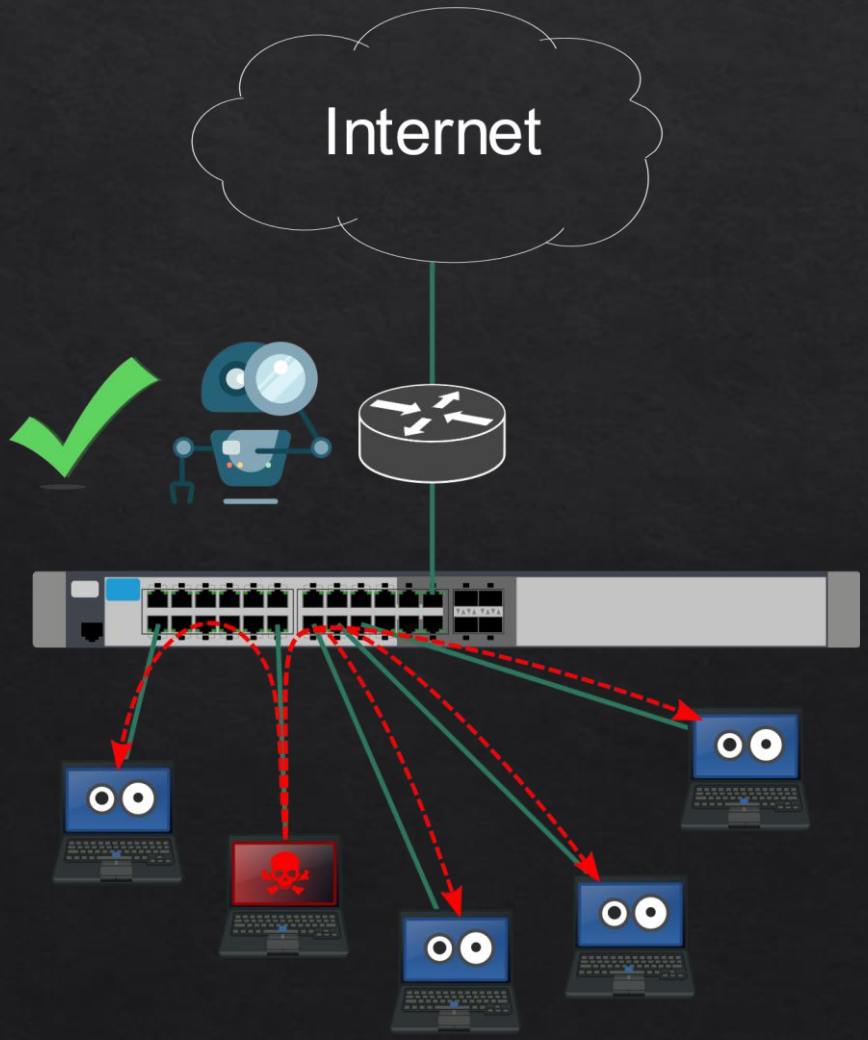


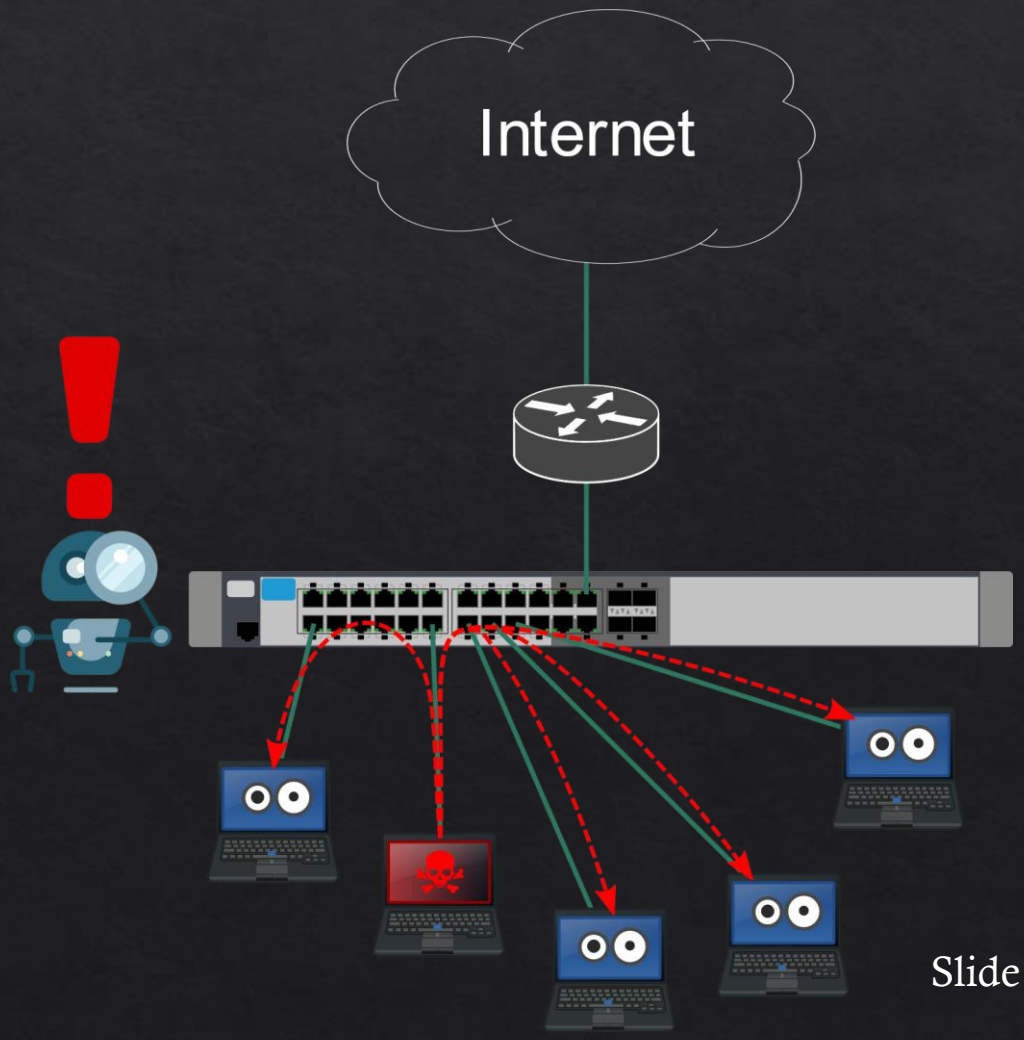
Where You Monitor is Important

University of Southampton
School of Electronics and Computer Science

Monitoring at the edge misses local problems

Monitoring more locally generates a lot more data



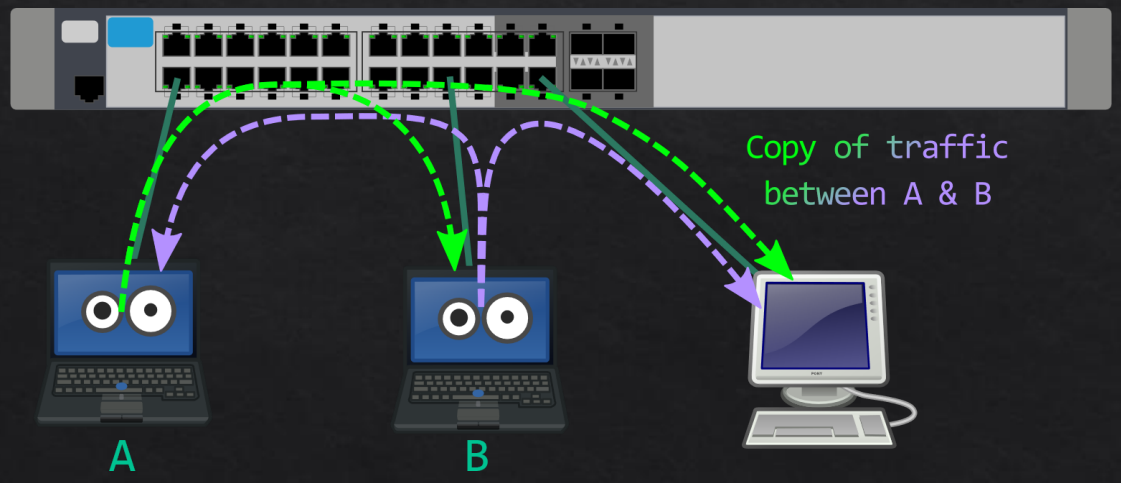


How do you Sniff?

University of Southampton
School of Electronics and Computer Science

- To sniff packets, you need to actually see them.
- In packet-switched networks, packets are only sent to relevant hosts.
- So how do we monitor traffic?

Switch mirror ports



Network Tap

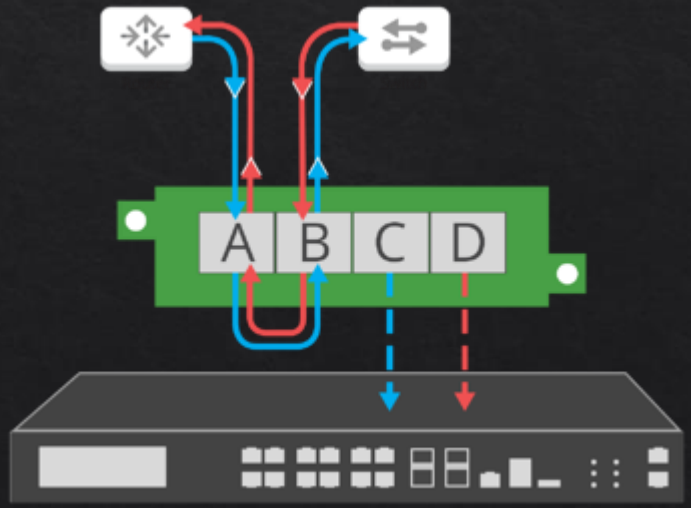


Image reproduced from https://www.garlandtechnology.com/breakout-passive-fiber-copper-network-tap

ARP/NDP Tables

University of Southampton
School of Electronics and Computer Science

- A client access port should have one (or maybe a small number of) MAC/EUI-64 address(es) associated with it

- Signs you might have an issue:
  - If you *suddenly* get a lot of MAC/EUI-64 addresses appearing on a single port
  - If you *suddenly* have a single MAC/EUI-64 address appearing on multiple ports
  - If you have "important" MAC/EUI-64 addresses appearing where they aren't meant to be

```
Saber# show mac address-table all
  Port   VLAN ID   MAC Address
  10     1         00:03:7f:ff:ff:ff
  3      1         00:30:93:14:04:cf
  2      1         24:5e:be:68:7e:15
  10     1         38:f9:d3:8d:d9:cc
  10     1         58:2f:40:d0:ec:82
  10     1         82:66:fd:1b:94:dd
  10     1         98:0d:67:fc:e2:37
  9      1         98:be:94:5a:18:c0
  9      200       98:be:94:5a:18:c0
  9      600       98:be:94:5a:18:c0
  9      4         98:be:94:5a:18:c0
  2      1         9c:93:4e:6d:95:bd
  10     1         9c:9c:1f:8d:e3:2b
  10     1         9e:59:fb:1e:9c:b1
  10     600       a0:f3:c1:c4:59:4d
  10     1         b6:8d:7c:0c:f1:2b
  10     1         b8:27:eb:19:61:53
  10     1         b8:27:eb:ce:ab:41
  CPU    1         bc:cf:4f:e0:66:52
  10     1         c0:06:c3:6f:89:5c
  2      1         d8:ec:e5:7d:b8:74
  10     1         dc:2c:6e:29:66:3f
  10     1         e4:95:6e:40:63:71
  10     1         e4:f4:c6:8c:23:7f
  5      1         ec:b1:d7:65:56:d8
  10     1         fa:73:b0:d9:4b:62
  10     4         fa:73:b1:32:8d:18
  10     1         fc:a6:67:74:40:a7
```

Automated Monitoring Tools

University of Southampton
School of Electronics and Computer Science

- Manually looking at logs, terminal dumps and packet captures is tedious and error-prone
- Plenty of tools to that aggregate data from data sources to automate monitoring. e.g.:
  - LibreNMS
  - zabbix
  - Prometheus
  - AKiPS
  - PRTG
  - Solarwinds

Image reproduced from https://www.zabbix.com/whats_new_4_0

Intrusion Detection

University of Southampton
School of Electronics and Computer Science

- An Intrusion Detection System goes even further and automatically monitors a network for malicious activity or policy violations
- Automatic notification/alerting of potential problems
- Various types:
  - Network IDS monitors network traffic
    - i.e. sniffing
  - Host IDS runs locally on a computer

How does IDS work?

University of Southampton
School of Electronics and Computer Science

- Matching traffic and packets against rules
  - Signature database (e.g. known exploits, SQL injection strings etc.)
  - Reputation/blacklists (e.g. botnet C&C servers)
  - Protocol anomalies
  - Traffic anomalies
- The challenge
  - False positives: Identifying legitimate behaviour as an attack
  - False negatives: Failing to identify an attack
  - Tuning is important
  - Which is worse?

Intrusion Prevention

University of Southampton
School of Electronics and Computer Science

- Takes IDS one step further and automatically responds to detected problems

- Various potential responses to detected problems:
  - Block problem traffic
  - Block suspected user accounts
  - Segregate compromised hosts
  - Trigger an incident response process
  - Increase level of network monitoring

IDS/IDP Tools

University of Southampton
School of Electronics and Computer Science

- There are many different tools out there ranging from open source to proprietary
- There are several free and open source projects:
  - Snort http://www.snort.org
  - Suricatta https://suricata.io/
  - Zeek https://zeek.org/

Detail by Signatures

Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	3	WEB-MISC Multiple Products excessive HTTP 304 Not Modified responses exploit attempt [sid 16008] [url technet.microsoft.com/en-us/security/bulletin/ms07-027] [cve 2007-6239] [cve 2007-0947]	869	4	13	Summary
2	1	WEB-CLIENT Adobe Director file file mmap overflow attempt [sid 17204] [cve 2010-2870]	1	1	1	Summary
3	1	FILE-PDF EmbeddedFile contained within a PDF [sid 23250]	4	1	4	Summary
4	3	FILE-IDENTIFY Portable Executable binary file magic detected [sid 15306]	7	1	4	Summary
5	3	FILE-IDENTIFY Ultimate Packer for Executables/UPX v0.62-v1.22 packed file magic detected [sid 16435] [url www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx] [url upx.sourceforge.net]	7	1	4	Summary
6	1	FILE-PDF EmbeddedFile contained within a PDF [sid 23041]	6	1	2	Summary
7	3	INDICATOR-OBFUSCATION eval gzinflate base64_decode call - likely malicious [sid 23113] [url vrt-blog.snort.org/2012/06/web-shell-poses-as-gif.html] [url labs.snort.org/docs/23113.txt]	8	1	7	Summary
8	1	WEB-PHP Wordpress timthumb.php theme remote file include attack attempt [sid 19653] [url code.google.com/p/timthumb/issues/detail?id=212] [bugtraq 47374]	605	37	5	Summary

Benefits of an IDS/IPS

University of Southampton
School of Electronics and Computer Science

- *Automatically* detect (and potentially prevent) attacks not stopped by other measures
- Handle incompetence…
- Log information, allow auditing
  - Record information about specific events
- Identify problems with security policies
- Document existing threats
- Deter violations
- Produce reports

Limitations of an IDS/IPS

University of Southampton
School of Electronics and Computer Science

- Configuration and maintenance
  - Is someone monitoring the system?
- Performance issues
- False positive/false negative balance
- Not great against newly published attacks
- Less effective against targeted attacks
- Growing advanced evasion techniques (AET)
- Don't rely on them!
  - They are a useful tool but can't compensate for holes in security
  - But many people rely on them for protection

Darknets and Honeypots

University of Southampton
School of Electronics and Computer Science

- Darknets: Using unused IP address space to monitor for unexpected network activity
- Honeypots: Specific decoy systems set up to allow an attack and observe (and respond)
  - Divert the attacker from the critical systems
  - Collect information about the attacker and their methods
  - Encourage the attacker to stay long enough to document/respond
- Trap and trace: Honeypot and an alarm
  - Legal issues: Enticement (legal) versus entrapment (not)!