School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

# CYBR 171 T1 2023

## Ngā whakapūtanga o Te Haumaru rorohiko

## Cybersecurity Fundamentals

---

## Week 8

## Defending networks: Intrusion Detection and Honeypots

# Learning objectives

- PART 1:
  - What is an intrusion?
  - The main purpose of an intrusion detection system.
- PART 2:
  - Network versus host-based IDS.
  - Anomaly versus misuse-based detection.
  - Classification accuracy and tradeoffs.
- PART 3:
  - Honeypots for observing attackers.


# PART1: INTRUSION DETECTION SYSTEMS (IDS)

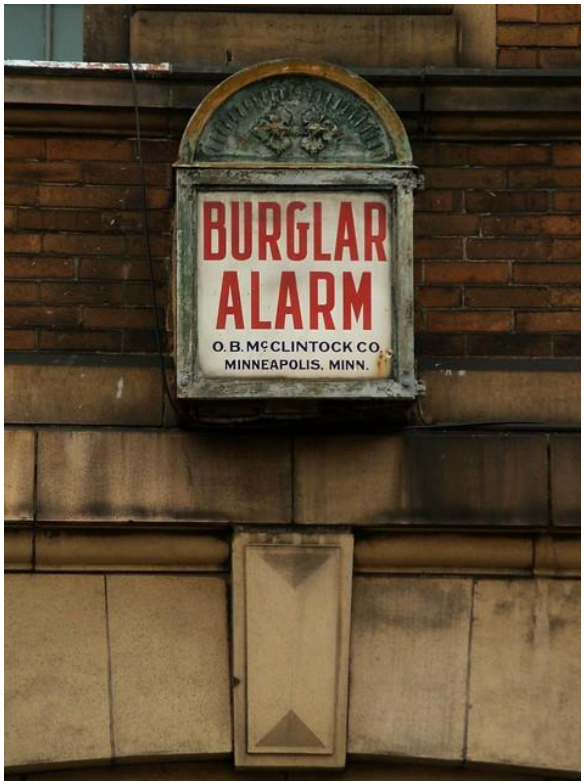
# When there is an attack

https://video.link/w/eSBl

# Intrusion detection in real life

**Monitors** system.
**Logs** suspicious activity.
**Alerts** administrator.

Software application
**or**
hardware appliance.




https://www.flickr.com/photos/takomabibelot/2134214940

# What is an intrusion?

- Intrusion includes:
  - Network scans
  - Suspected attacks
  - Misuse of network resources.

- Examples:
  - Brute forcing passwords.
  - Unauthorised programs.
  - Illegal file downloading.
  - Port scan for active services.


Real world example of car thief attempting to break into a car
https://pixabay.com/photos/car-burglary-thief-burglar-1590508/

# Example: Port scanning

Attackers want to find servers running on target machines.

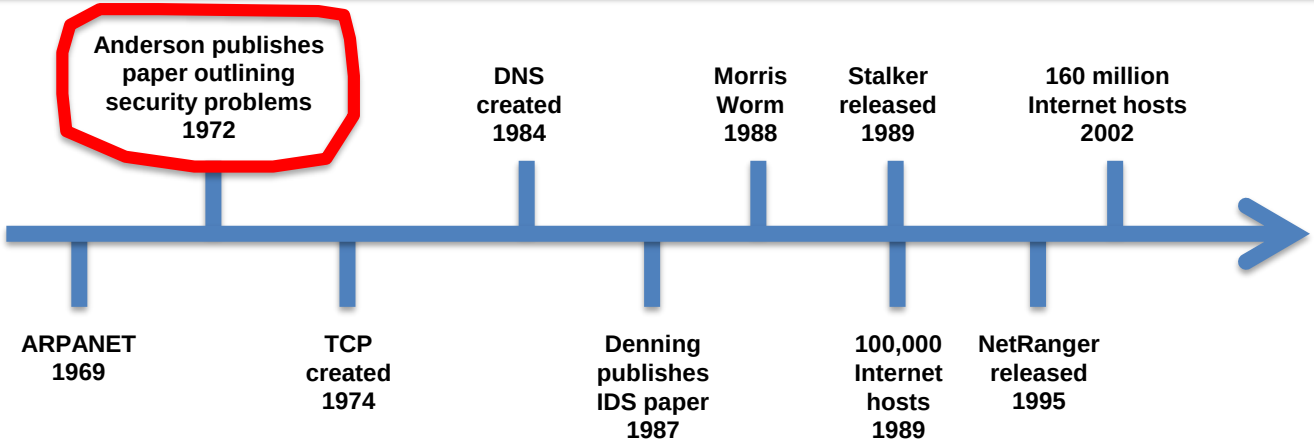
Attempt to connect to a range of ports.

Use information to exploit vulnerabilities.

Nmap is a popular tool.

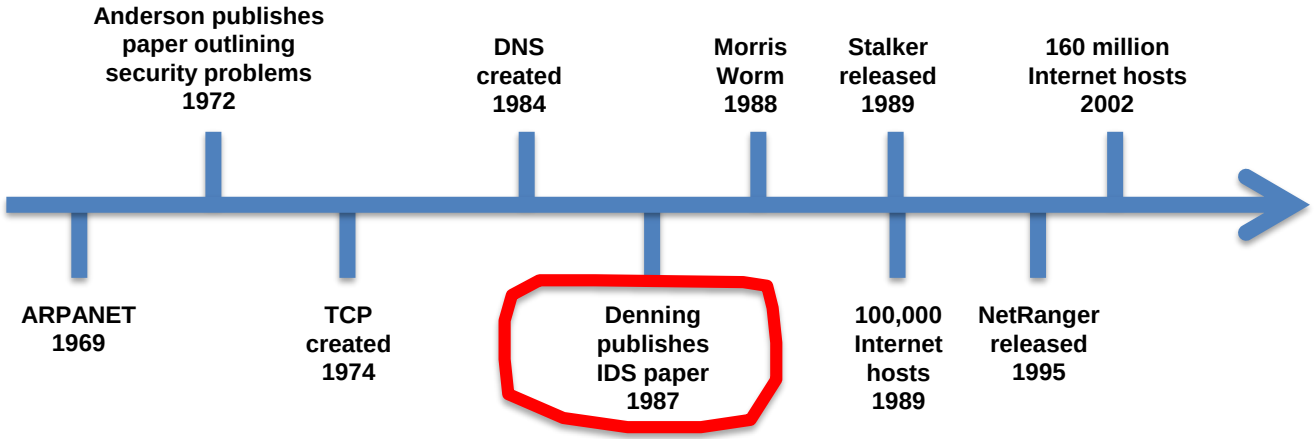
```
[root@darkstar ~]#
[root@darkstar ~]# nmap -PN sS -O Scanme.Nmap.Org

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
[root@darkstar ~]#
```

# A little history to show the evolution of IDS



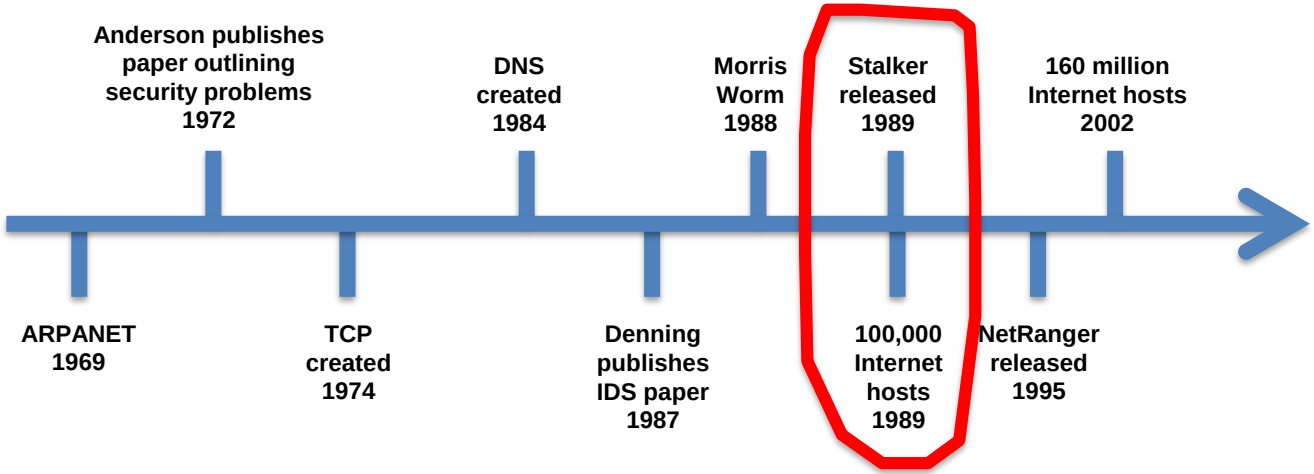

Anderson report in 1972 outlining vulnerabilities of computer systems to Trojan horses. Suggested using automated monitoring systems to look suspicious activity.

# A little history to show the evolution of IDS



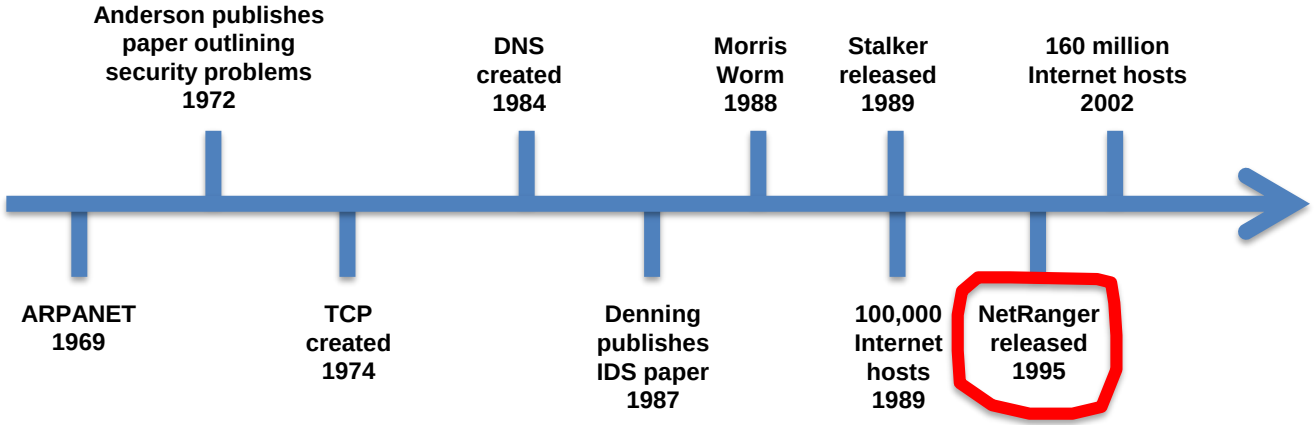

Dorothy and Peter Denning write first paper to define a model and architecture for such as system. Rule-based IDS.

# A little history to show the evolution of IDS



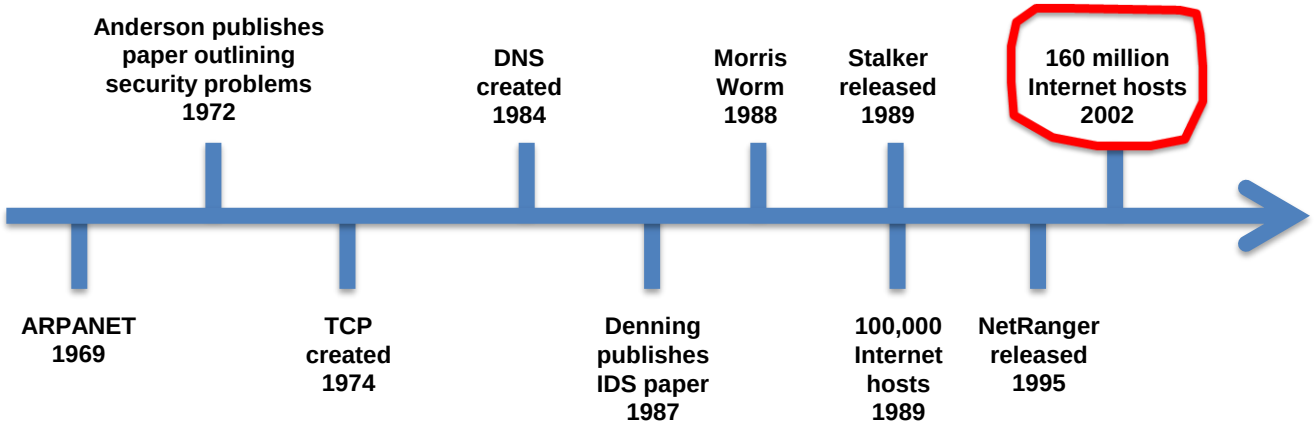

Stalker was first commercial implementation of IDS. **Host-based** comparing audit data with known patterns of suspicious activity.

# A little history to show the evolution of IDS

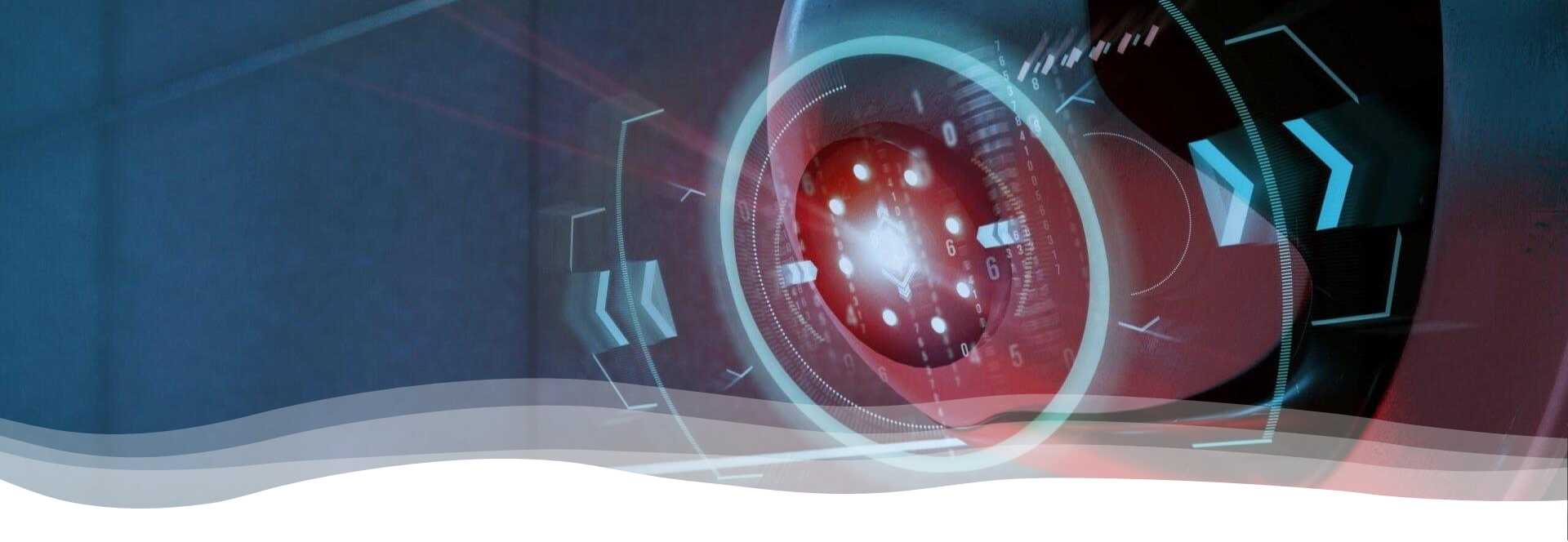



NetRanger was the first commercial IDS to monitor **network** activity

# A little history to show the evolution of IDS

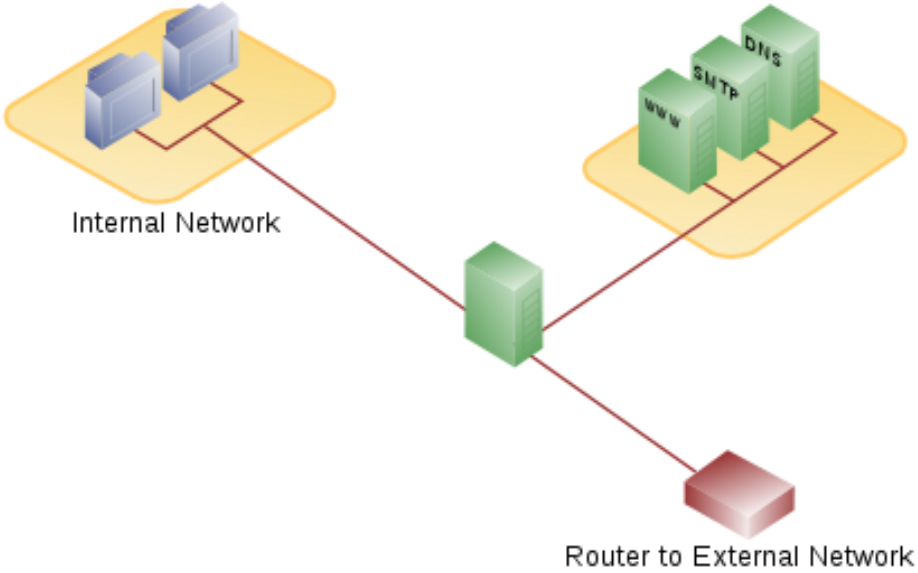



With the rise of the Internet, deploying an IDS became best practice



# PART 2: TYPES OF IDS AND DETECTION TECHNIQUES

# Network-based IDS (NIDS)




- Placed at strategic points in the network .
- Monitor network traffic to and from hosts.
- Won’t affect performance of hosts, doesn’t require installation on hosts simplifying deployment.

# Host-based IDS (HIDS)


- Run on individual hosts or devices.
- Usually a software agent.
- Monitor resources used by application – files, registry entries, memory, processes, network etc.
- Detects intrusions on the machine.
- ***Attacker will try and disable the HIDS once they get access to the host.***

# Passive versus reactive

- Intrusion detection can be **passive**:
  - Identifies intrusion.
  - Informs administrator.

- Also can be **reactive**:
  - Actively attempt to stop intrusion.
  - Block further data packets from source IP address.
  - **Intrusion prevention** or protection system (IPS)

https://pixabay.com/photos/cow-animal-livestock-fence-wooden-1990260/


https://pixabay.com/photos/electric-fence-fence-electric-2912014/

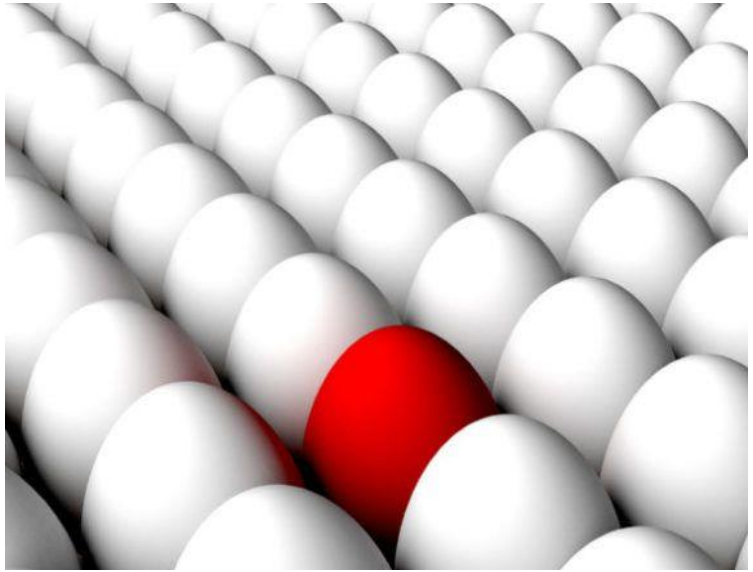
# Two main detection techniques

Anomaly detection

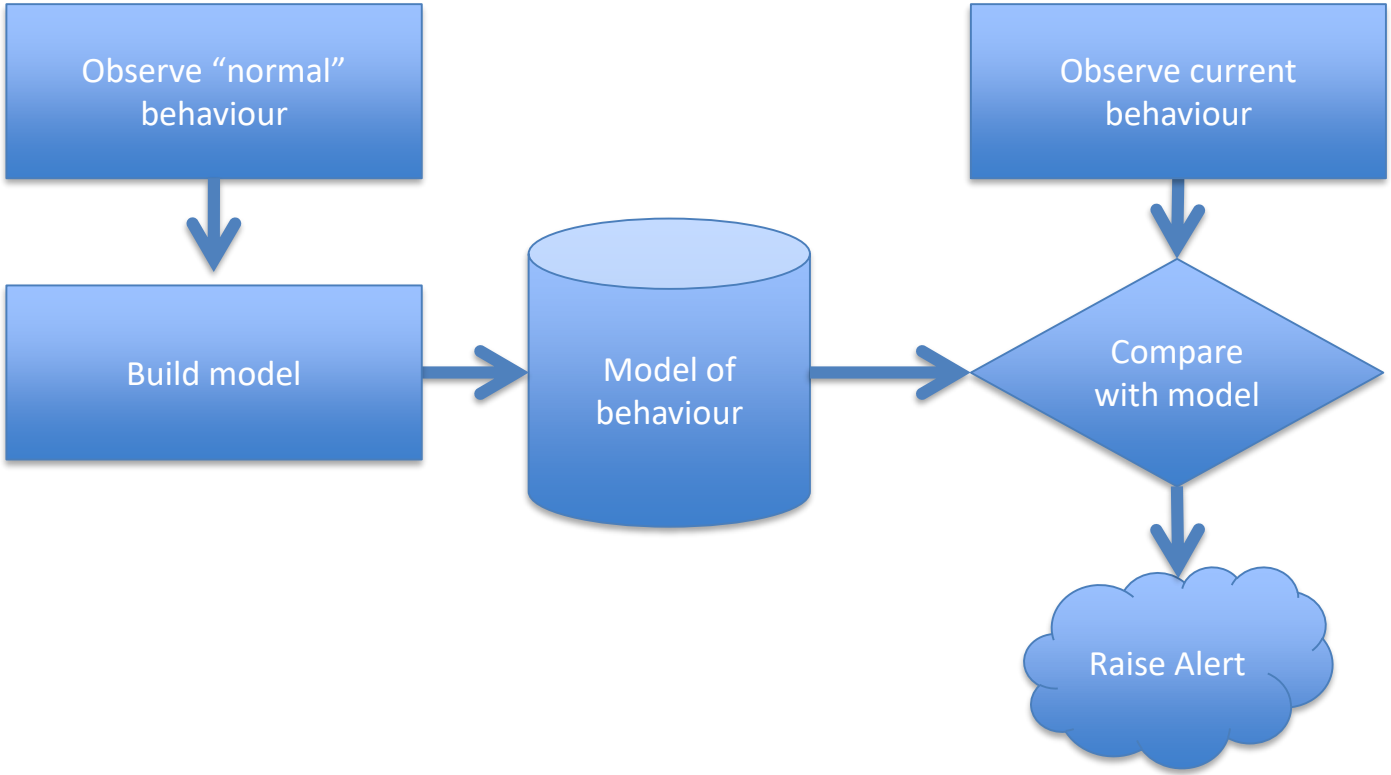
Misuse detection

# Anomaly detection

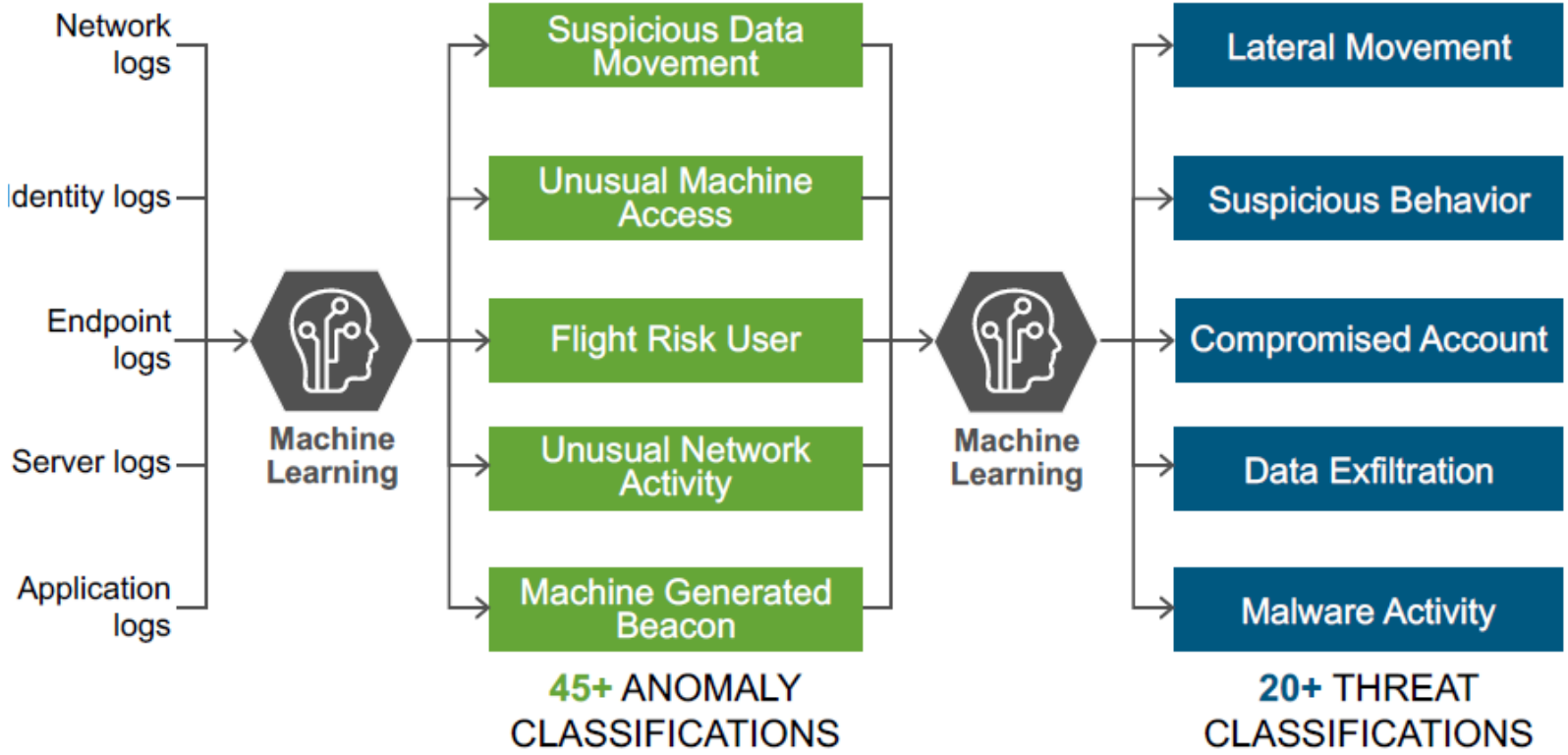
- Model of expected "**normal**" behaviour.
- Attacks are assumed to exhibit a different pattern.
- Able to detect unknown attacks.
- Example of "**normal**":
  - User logs on every weekday at 9:00 am.
  - Accesses supplier websites.
  - Logs off at 5:00 pm.
- Example of "**suspicious**":
  - User logs on at 3:00 am.
  - Installs new software.
- Weakness – potential for false alarms



# Anomaly detection



# Example: Splunk



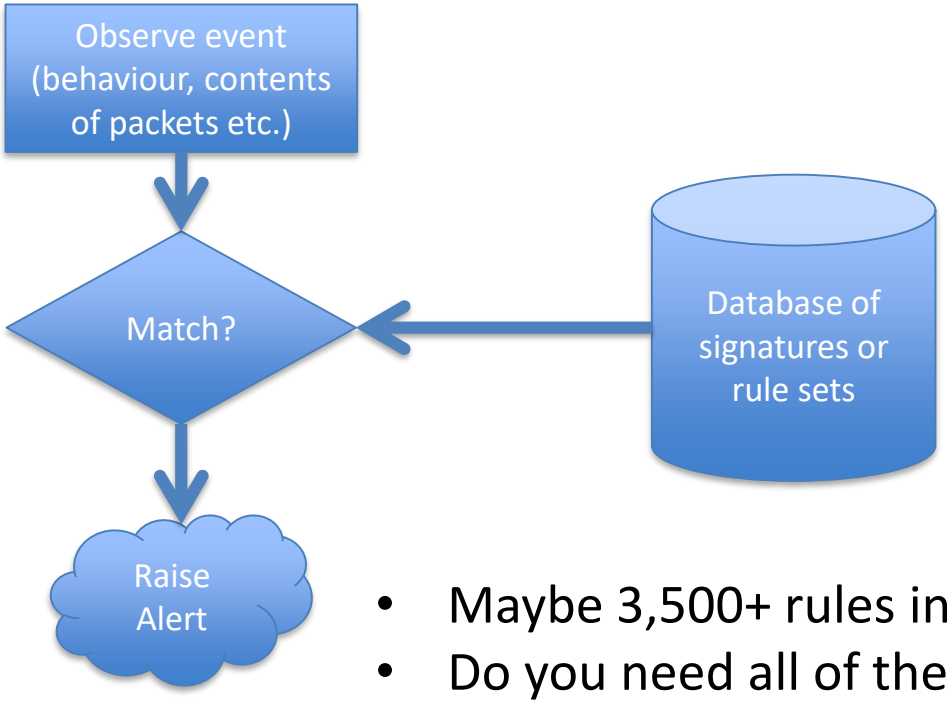

https://www.splunk.com/en_us/software/user-behavior-analytics.html

# Misuse detection

- Attack patterns of "**signatures**".
- Configured by an administrator.
- Identify user behaviour that matches.

- **Strength** – minimises occurrence of legitimate activity mis-identified.
- **Weakness** – only can identify known attacks and requires regular updates.

# Misuse or signature detection

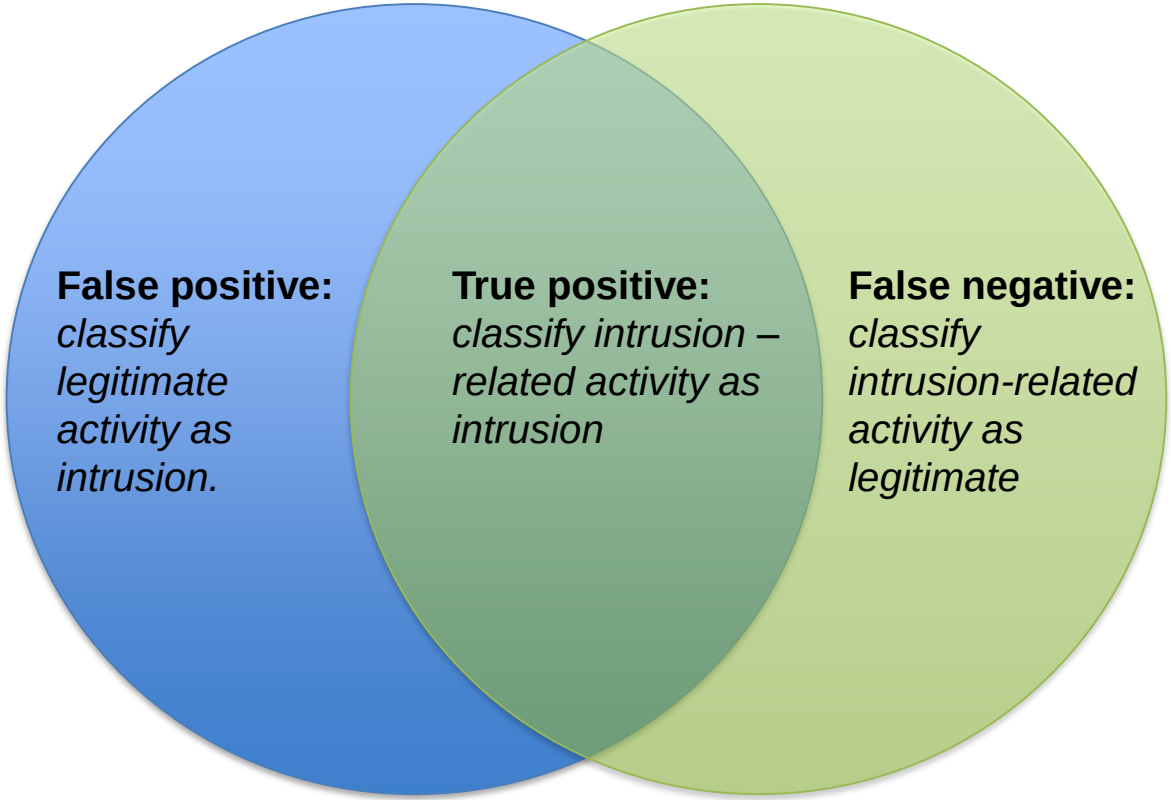



- Maybe 3,500+ rules in the database.
- Do you need all of them all of the time?
- Need to pick and choose.

# Example: SNORT


- Lightweight IDS system capable of performing real-time **traffic analysis** and **packet logging**
- Snort has three primary uses. It can be used as:
  1. a packet sniffer like tcpdump
  2. a packet logger (useful for network traffic debugging, etc)
  3. a full network intrusion detection system

# Classification accuracy



# Classification tradeoffs

- English WW2 radar installations wanted to distinguish between flocks of geese and bombers.
- More power = greater sensitivity at the cost of accuracy (higher false positives or negatives).
- Usually, can’t achieve both low false positives and false negatives.

# PART 3: HONEYPOTS

# Honeypots

- Used to study attacks or draw an attacker out.
- Computer or network appearing legitimate.
- Actually, a trap known as a honeypot.
- Monitor attacker behaviour with no risk to real assets.

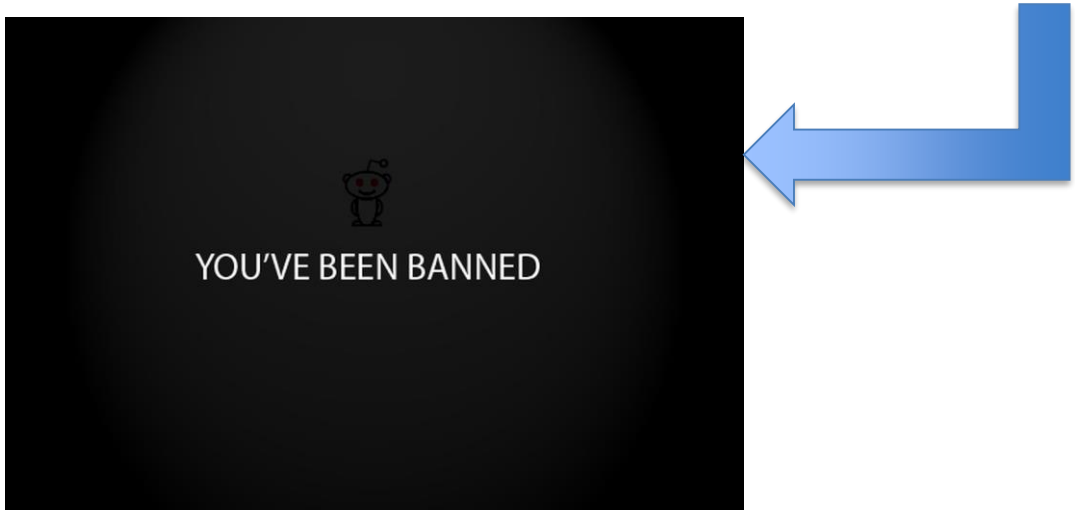
# Honeypots in real life

- Reddit is a forum for sharing news content or commentary.


- Subreddit /r/wallstreet:
  - Risky stock market gambling
  - Immature comedy
- Many people not there for trading, in particular minors who cannot be easily identified.

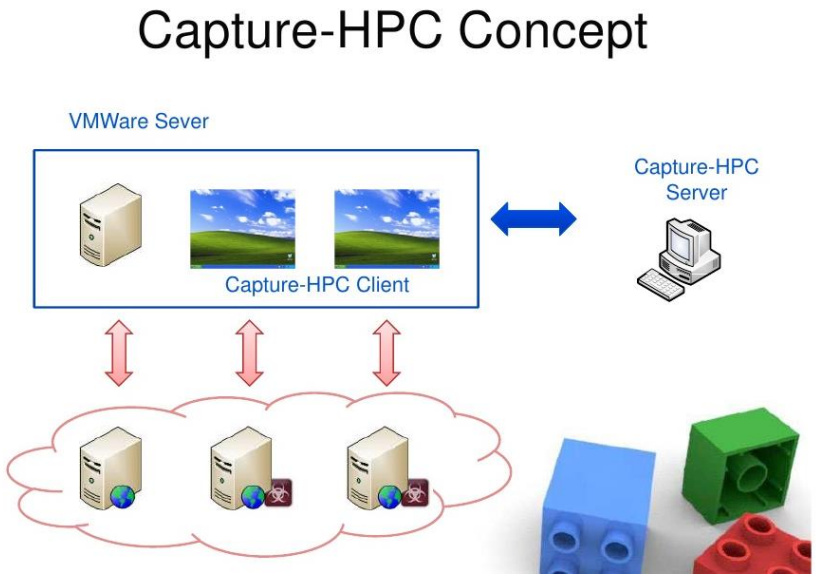
# Honeypots in real life

- Wildly popular moderator advertised special thread for those under 18
- Many minors signed up, revealing themselves.



# Honeypots at VUW

- PhD researcher Christian Seifert developed Capture-HPC.
- Used by Netherlands and Polish CERTs.
- More recently Junaid Haseeb PhD worked on IoT honeypots



# What’s up next

- **Thursday: Guest lecture Ben Creet**
- **Next week: Social engineering**