Sentinel

Network Intrusion Detection System (NIDS)

DEFENDING OUR DIGITAL WAY OF LIFE

Lesson objectives

→ Gain a deeper understanding of **network attacks in practice**

→ Learn about **network intrusion detection systems**

→ **Prepare for building one yourself!**

What are the stages of a network attack?

Defining goals

What are the goals of the attack?

- 💣 Damage
- 🔒 Steal information
- 🤖 Possibly infect multiple computers to create a botnet.

Defining goals

Reconnaissance

- 🔎 Gathering information
  - To plan the attack strategy
  - Identify vulnerabilities, identify security measures
  - IP addresses, server versions…

Defining goals | Reconnaissance

Reconnaissance techniques

- ⚡ Active
  - Ping scan
  - Open ports
  - ARP (Address Resolution Protocol) scanning can be used once inside the network.

ARP
Address **R**esolution **P**rotocol

Defining goals → **Reconnaissance** →

Attack vectors

"How do we get in?"

- Analogy - robbing a real building:
  - "Inside man"
  - Steal a key
  - Breaking and entering

Defining goals → Reconnaissance → Attack vectors

Attack vectors - gaining access

- 🐟✉️ “Inside man”
  - Phishing - getting an insider to run a malware, or disclose secret information
- 🔑🥷🏿 Steal a key
  - Credential attacks
- 💥🔨Breaking and entering
  - Using vulnerabilities and exploits

Defining goals → Reconnaissance → Attack vectors

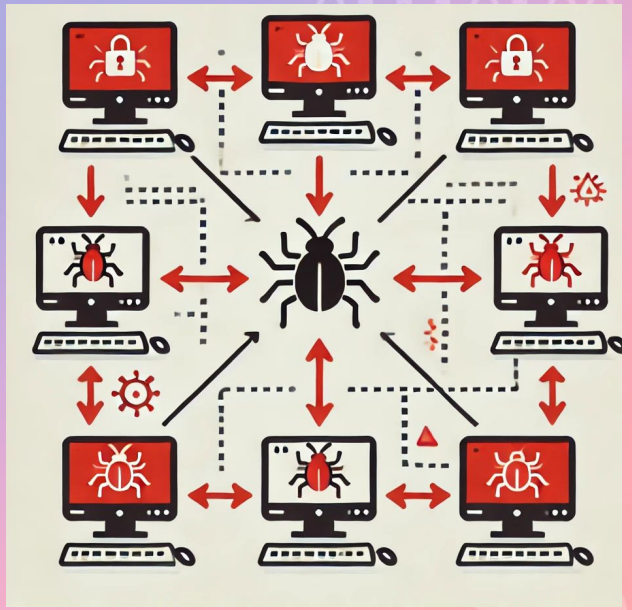
Example - Phishing

- Impersonating as a trusted entity
- Platform - email, Whatsapp, SMS, social media
- Tricking the user to download & execute a malware

Defining goals → Reconnaissance → Attack vectors

OK, we're inside! What's next?

- **Spreading**
  - 🔍 Discovery of internal network - scans (ping, arp, open ports), network captures
  - 🖥️➡️🖥️ Lateral movement (infecting more computers) - using stolen credentials, more phishing, or more exploits



Defining goals → Reconnaissance → Attack vectors → What's next?

OK, we're inside! What's next?

- **Command and Control (C2)**
  - 💬 How attackers maintain communication with malwares
  - Attackers use known protocols (DNS, HTTP) to avoid detection or rely on proprietary encrypted channels.
  - Or using proprietary encrypted channels

Defining goals → Reconnaissance → Attack vectors → **What's next?**

OK, we're inside! What's next?

- **Exfiltration**
  - 📄📁 Transfer of stolen data from the network to the attacker
  - Usually compressed and encrypted

Defining goals → Reconnaissance → Attack vectors → What's next?

How do we defend?

🤔

How do we defend?

🤔

Threat intelligence

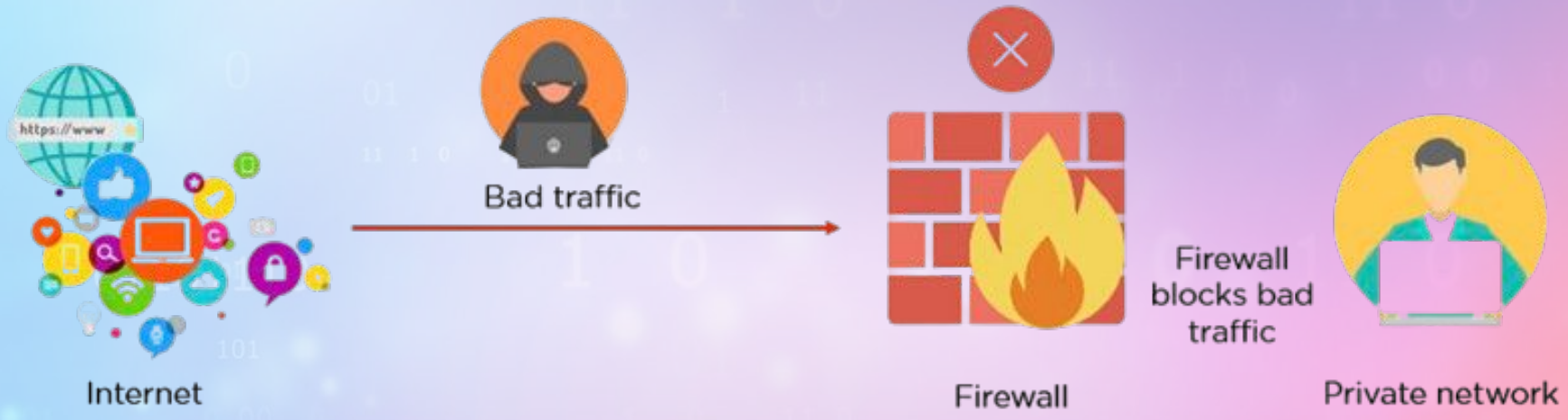
- How is crime prevented in the real world?
- Knowing tactics
  - If we know how robbers pick locks, we can build better locks
- Knowing the criminals
  - If we know what they look like, we can identify and catch them

Threat intelligence

- Similarly in cyber attacks
- Knowing tactics
  - Learn attack techniques to make adequate protections
- Knowing the criminals
  - Be able to identify known malware
  - Be able to identify known IPs, domains

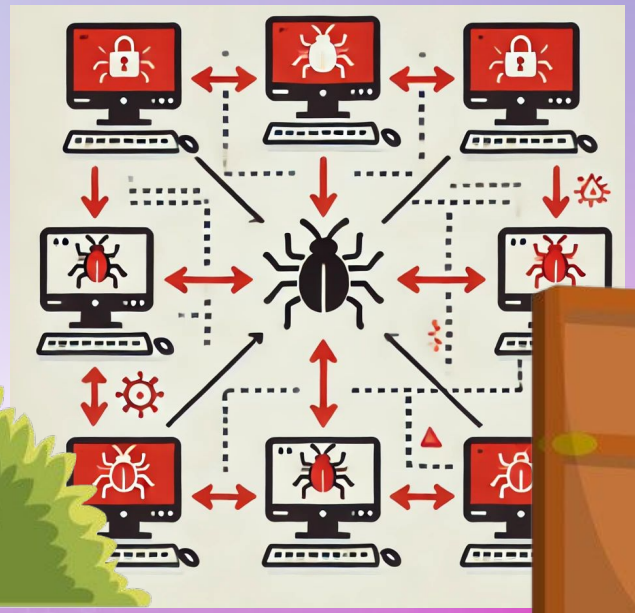
Defensive products

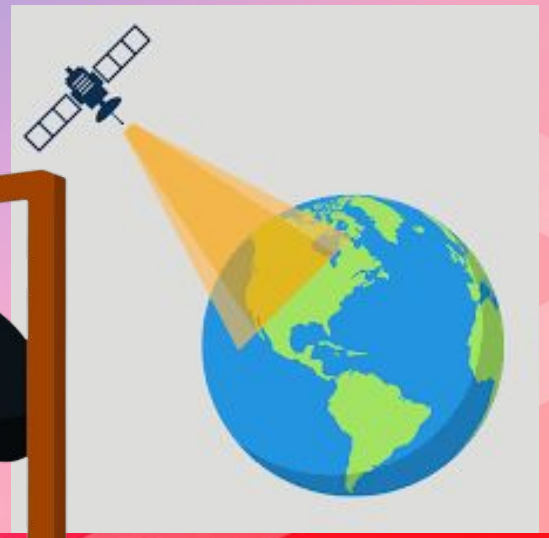
- Automation of what we mentioned
- A program that understands
  - Attack techniques
  - Recognizes malicious programs and addresses
- And more importantly - can detect them in real time



What to detect?

- Malicious actions
- Whether it's phishing, exploitation, brute-forcing, network scans…
- The more opportunities to catch attackers
  - The better!





User interface

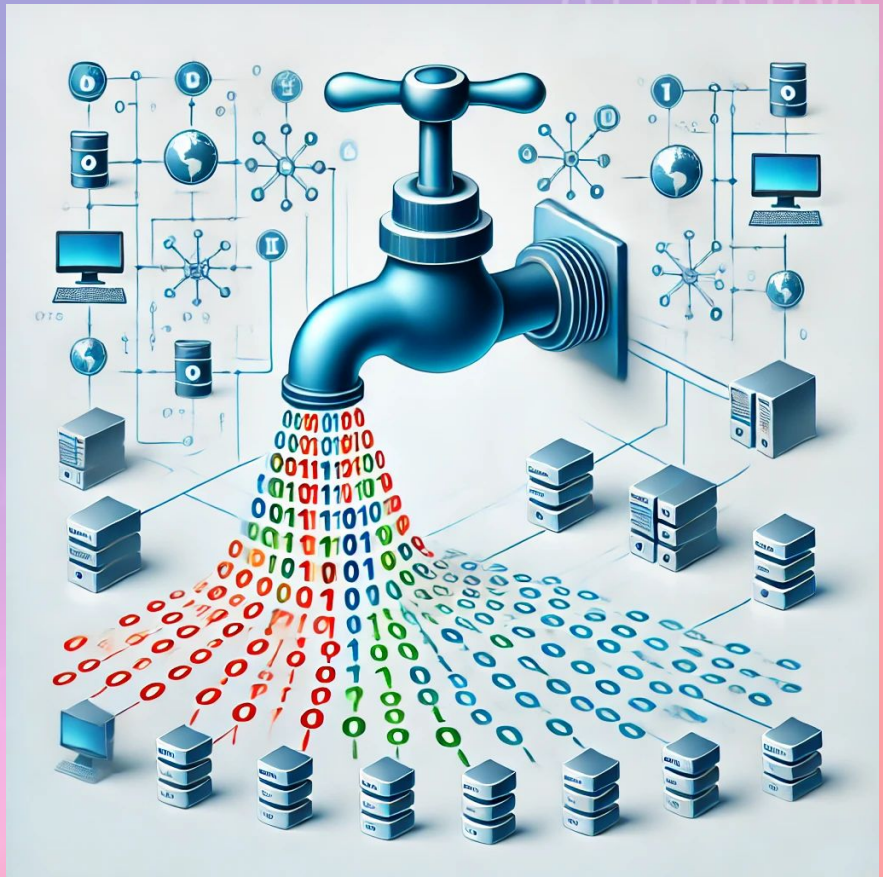
- Input
  - Definitions
  - Exceptions
- Output
  - Alerts

Basics of detection

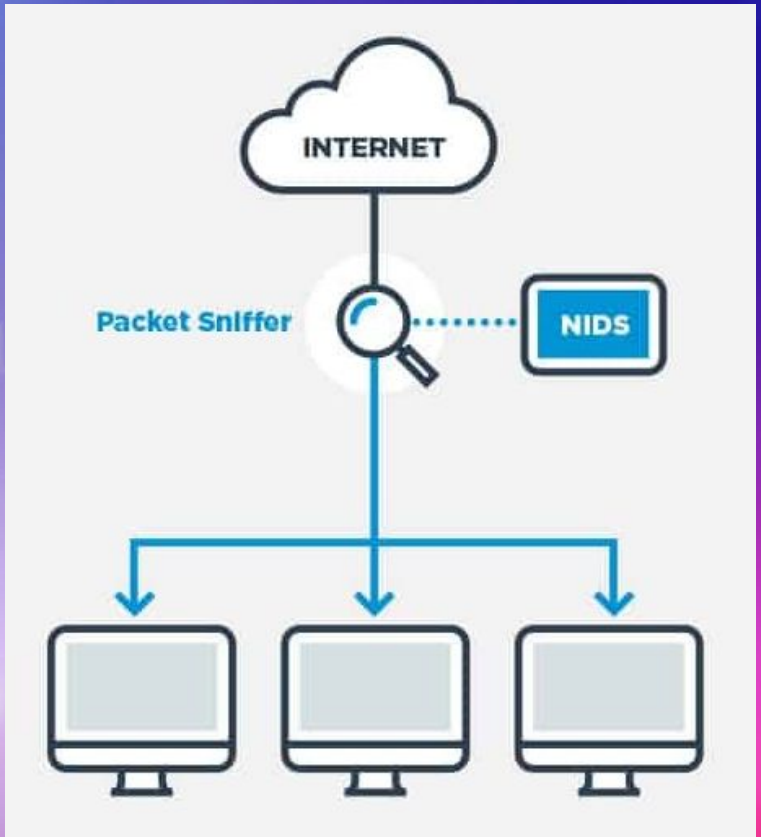
- Detection requires visibility
- Different products rely on different visibilities
  - Antivirus - access to filesystem
  - Endpoint Protection - access to operating system internals
  - Network Intrusion Detection System - access to network traffic

Network visibility

- Setting up an NIDS requires giving it network visibility
- The process is simple
  - Connect the NIDS to the router
  - Configure the router to mirror all traffic to the NIDS
  - Done!

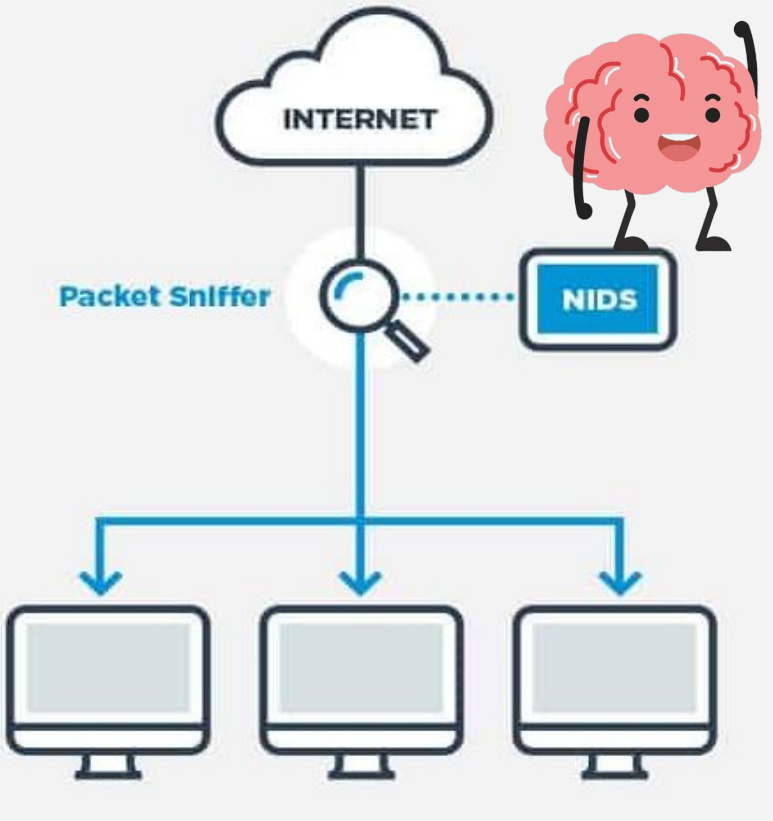


What kinds of malicious traffic could we detect?



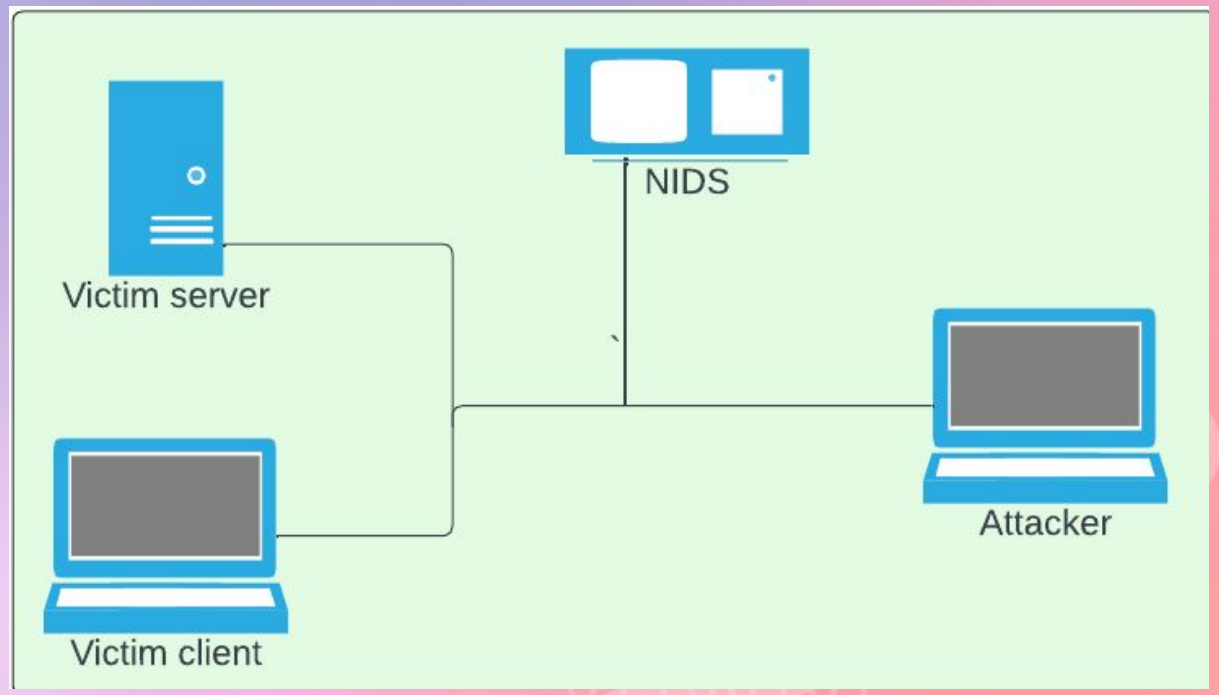
NIDS

- Designed to detect threats in network traffic
- Not necessarily to block or prevent - but to detect and notify
- Requires knowledge of known attack techniques / signatures
  - Specifically, how they look like in network traffic



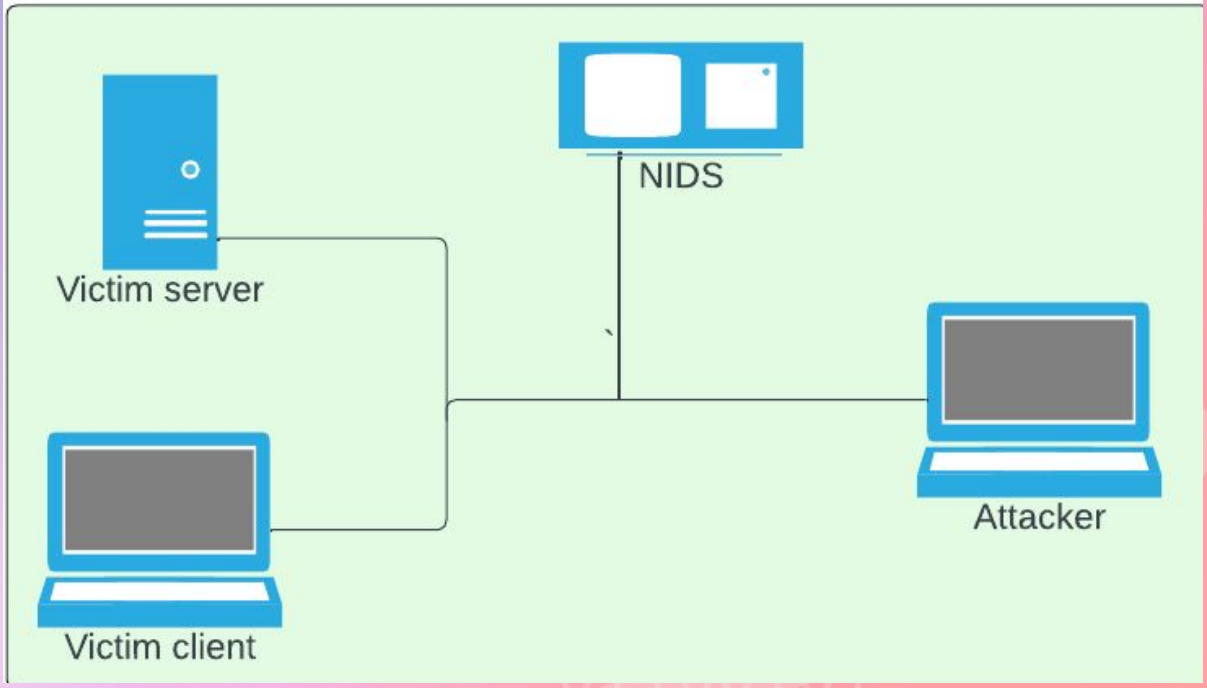
Workshop environment

- NIDS
  - Your workstation
  - Windows machine
- Attacker, client, server
  - The network to monitor
  - Attacks happen inside the network
- All traffic is mirrored to the NIDS

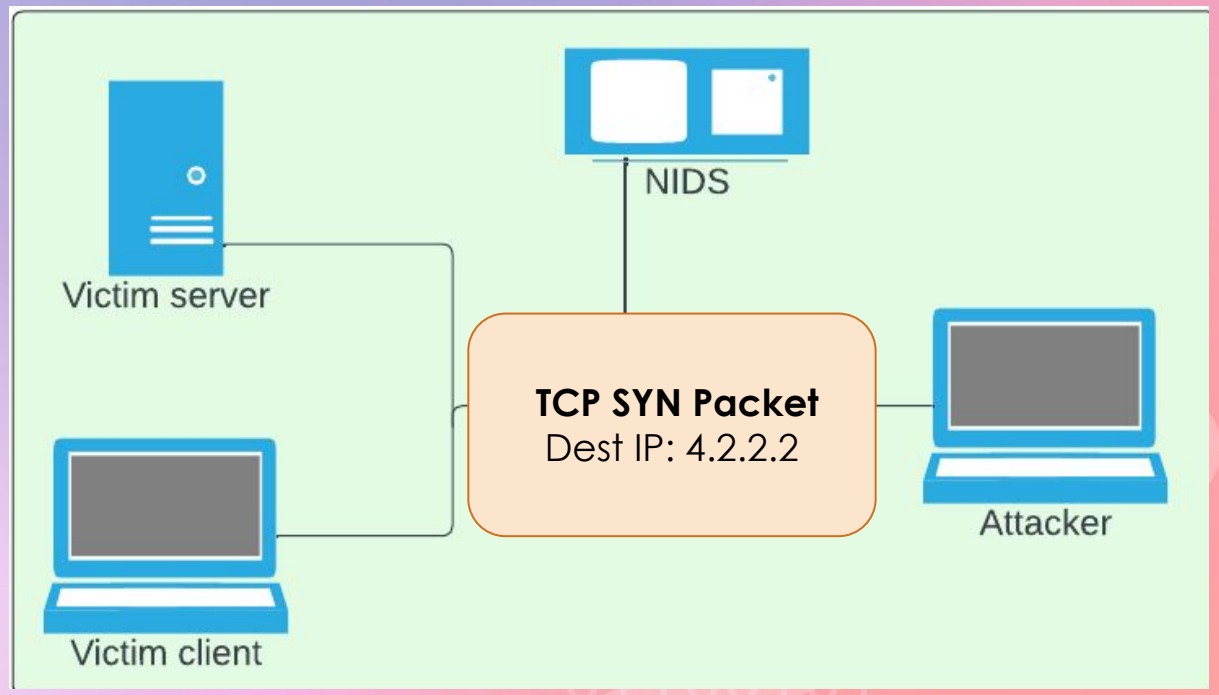


Attacks simulation

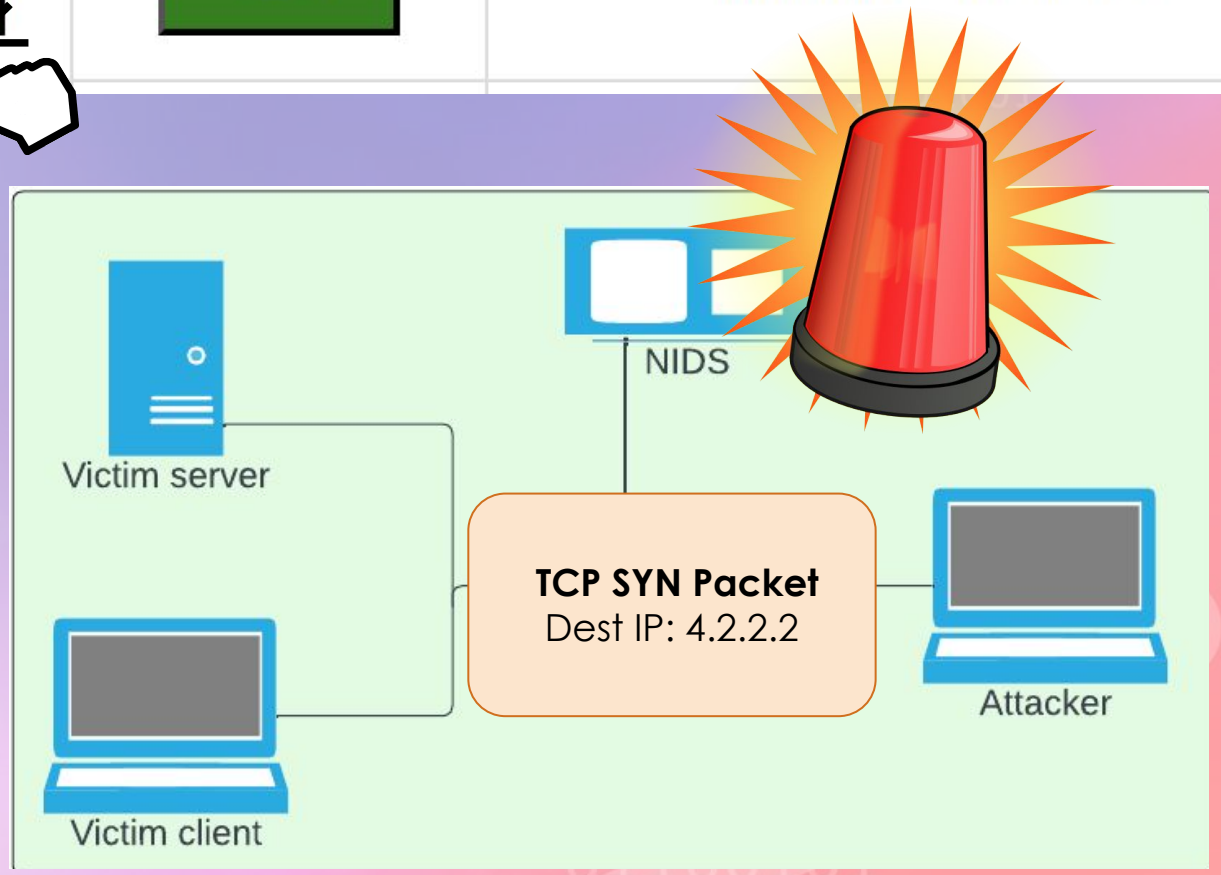
- Web interface for controlling simulations of malicious traffic
- Your NIDS should detect the malicious traffic



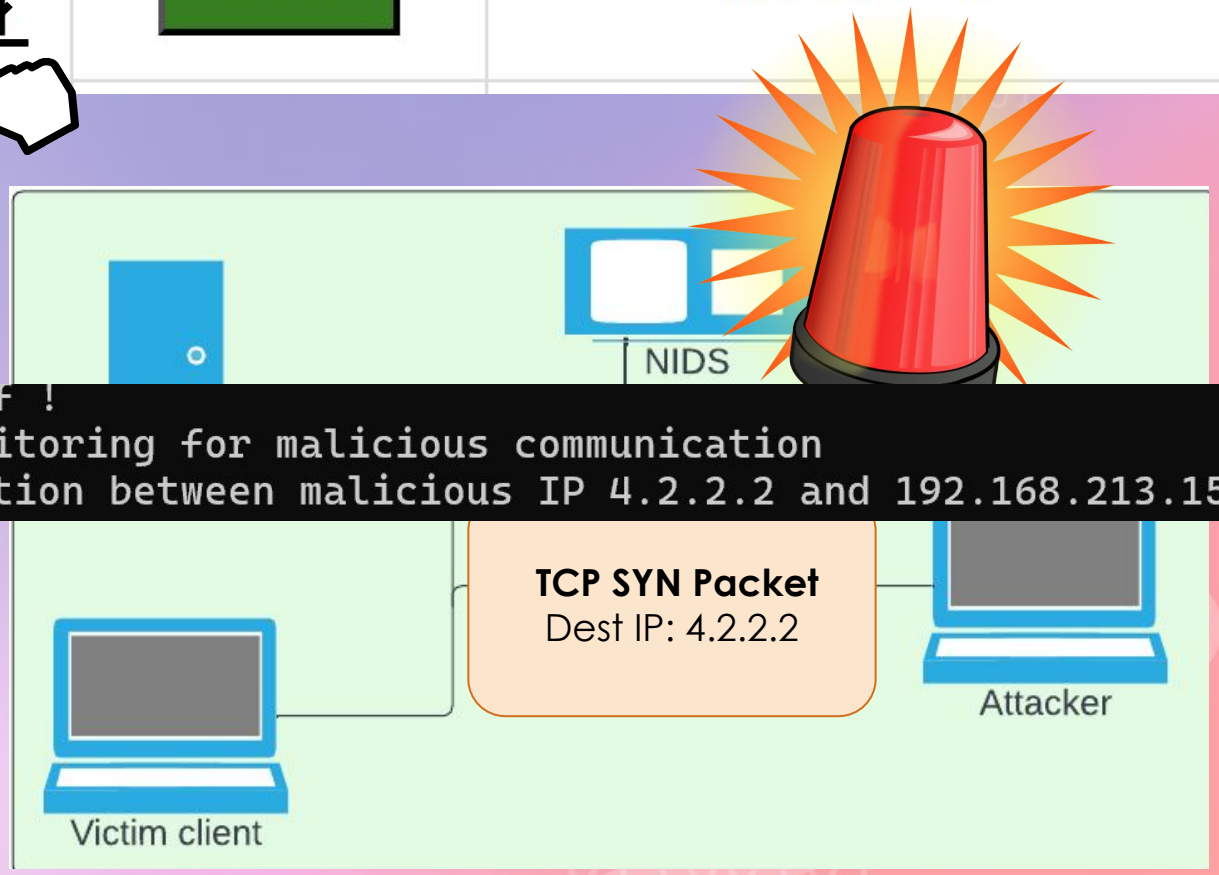
ID	Description	Malicious Trigger	Non-Malicious Trigger	Threat intelligence
1.1	Detect communication with a C2 server	Start	Start	Known C2 IP: 4.2.2.2



ID	Description	Malicious Trigger	Non-Malicious Trigger	Threat intelligence
1.1	Detect communication with a C2 server	Start	Start	Known C2 IP: 4.2.2.2



ID	Description	Malicious Trigger	Non-Malicious Trigger	Threat intelligence
1.1	Detect communication with a C2 server	Start	Start	Known C2 IP: 4.2.2.2




```
WARNING: Wireshark is installed, but cannot read manuf !
2024-11-21 19:28:57,428 - INFO - Starting NIDS... Monitoring for malicious communication
2024-11-21 19:29:03,966 - WARNING - *ALERT* Communication between malicious IP 4.2.2.2 and 192.168.213.154
```

Non-malicious triggers

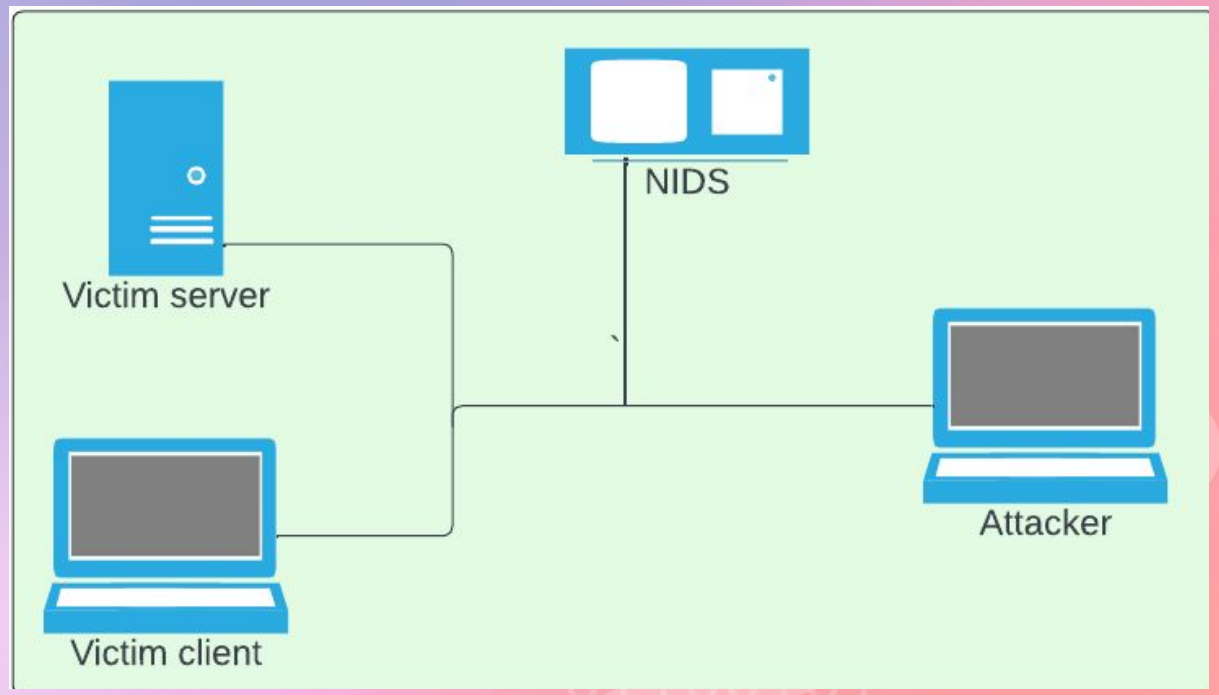
- To make sure your solution doesn't have **false positives**
- These should not generate alerts!

ID	Description	Malicious Trigger	Non-Malicious Trigger	Threat intelligence
1.1	Detect communication with a C2 server	Start	Start	Known C2 IP: 4.2.2.2

Simulation interfaces

- Attacker
  - http://192.168.x.x:5000
- Client
  - http://192.168.x.x:5001

- Remember to filter out ports 5000 and 5001!



How would you develop this?

- Python script
- Sniffing with scapy
- Inspecting each packet (using ‘prn’ argument)
- Adding specific detection code per level

Q&A