Graduation Project

Snort-Based IDS

Real-Time Network Threat Detection

BobXploit

Think Like a Hacker, Protect Like a Pro

By BobXploit

Think Like A hacker protect Like A Pro

Special Thanks

Anibus Security Group

ANUBIS
CYBER SECURITY TEAM

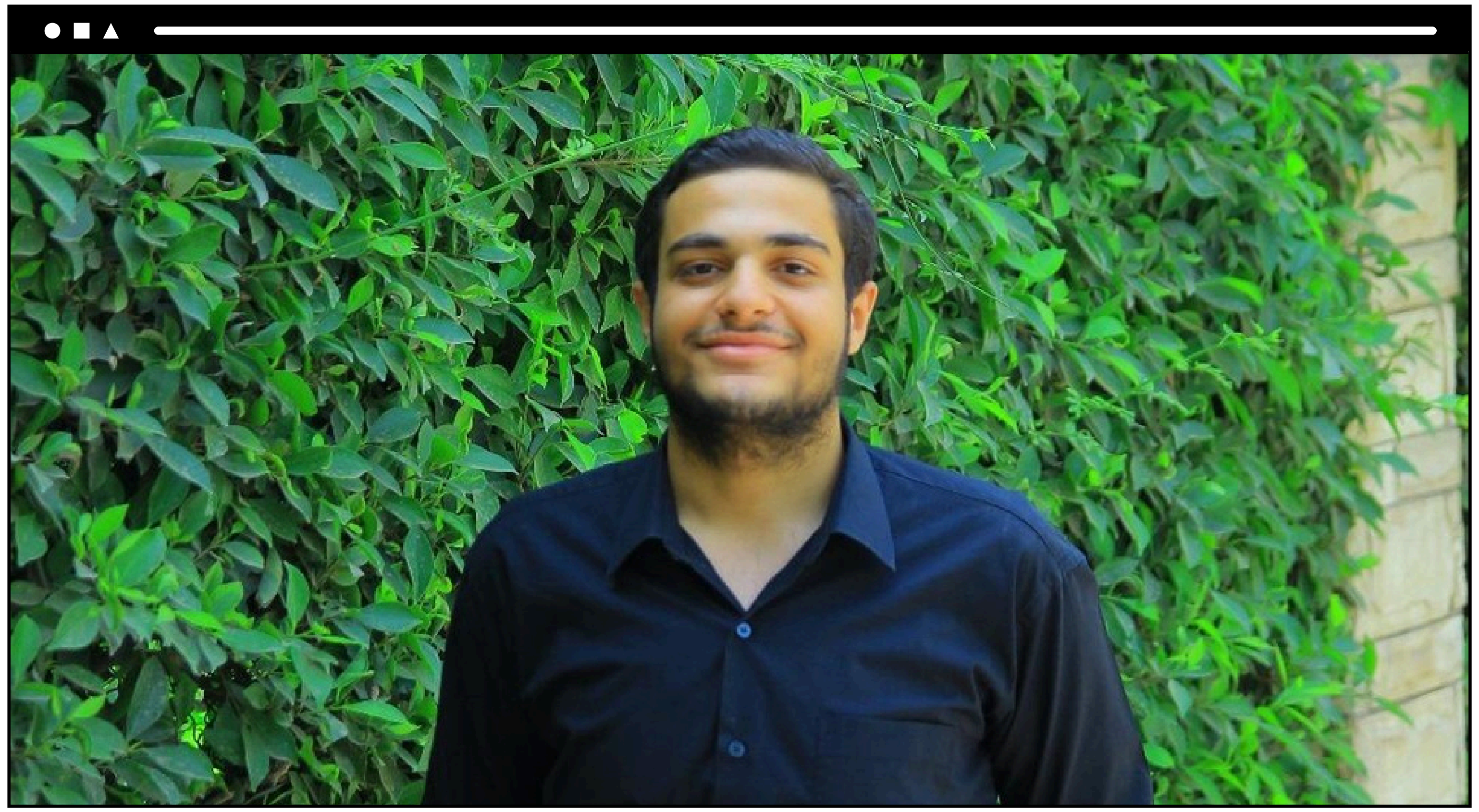
Eng / Mahmoud Ramadan

Eng / Ahmed Abaza

```
┌──(rootⓀkali)-[/home/BobXploit]
└─# whoami
```

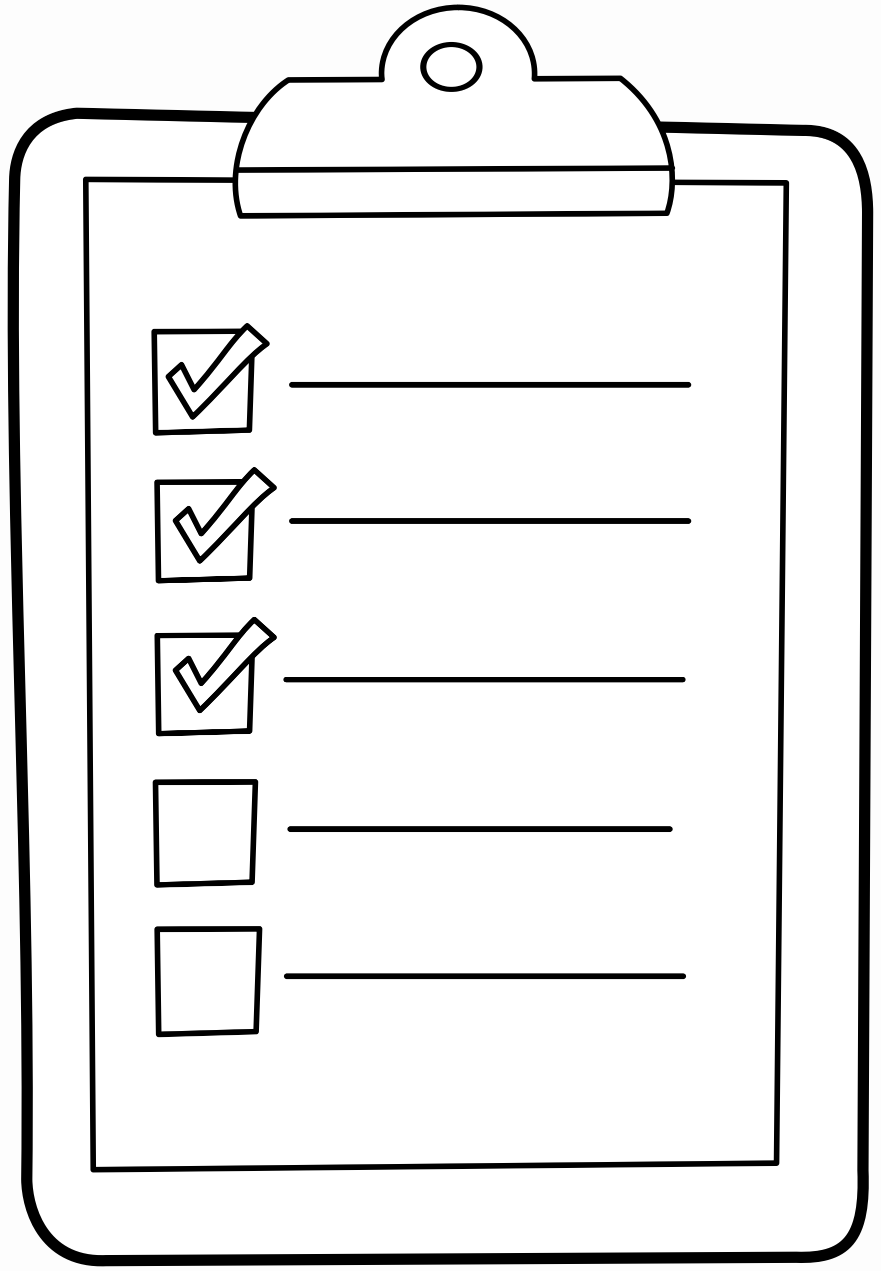
Abanoub Ehab (BobXploit)

- **Cyber Security student @ GDG CIC (Google Developer Group)**
- **Cyber Security Member @ MSP (Microsoft Student Partners)**
- **CTF Player & Top 5% @ try hack me (Microsoft Student Partners)**



Overview

Project Idea – "Why I Built"	01
Introduction	02
What is Snort?	03
Project Architecture	04
Practical Demo	05
Resources	06



1. Project Idea – "Why I Built"

Problem: Networks today are under constant attack — from

- **malware**,
- **port scanning**,
- **brute-force attempts**.

Objective: Build and demonstrate a working Intrusion Detection System using Snort that can detect malicious activities in **real time.**

Scope:

- Install and configure Snort
- Create and test detection rules
- Demonstrate how Snort can alert on suspicious traffic

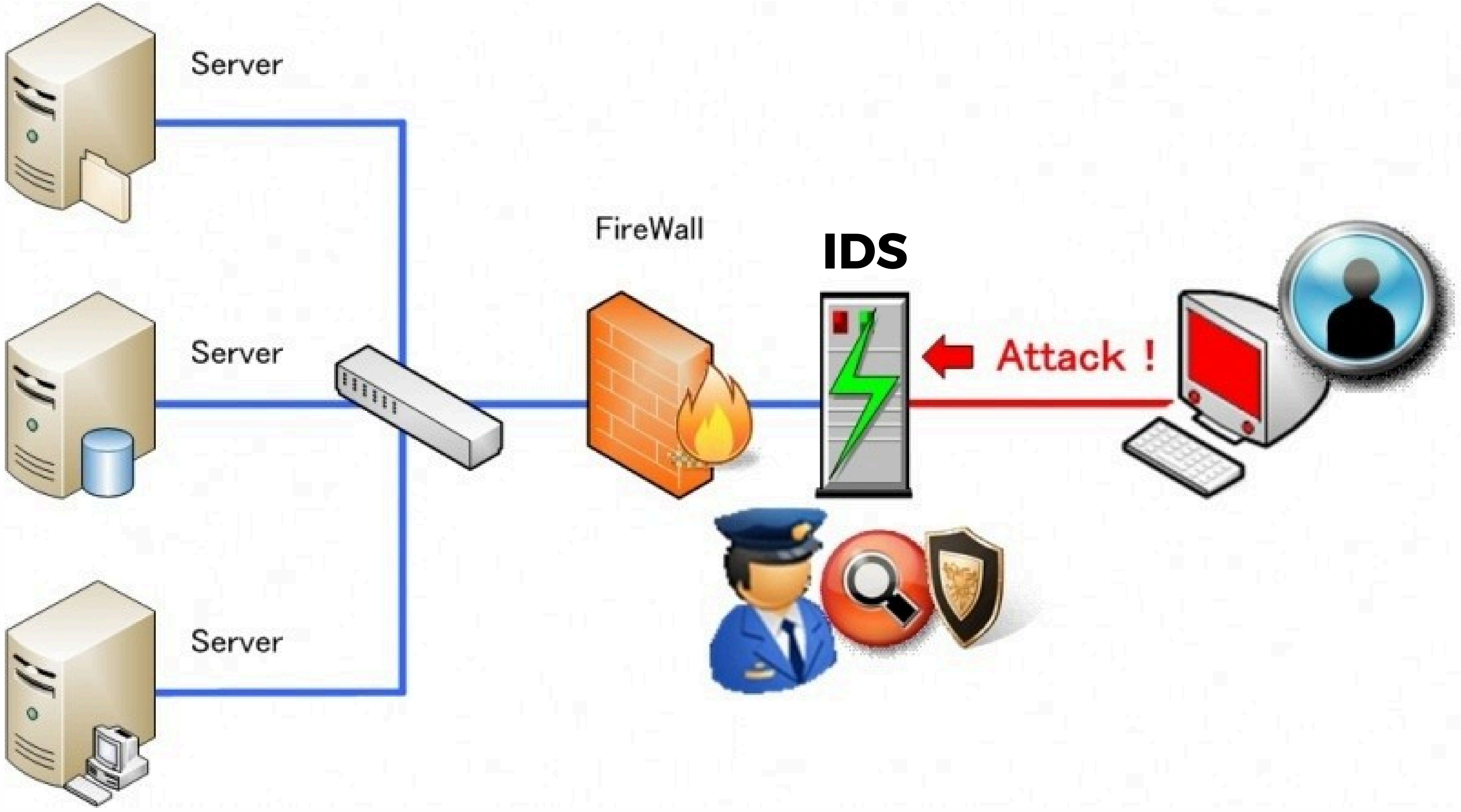
Goal: Show that Snort can be used to enhance the security of small-to-medium networks using free, open-source tools

2.Introduction

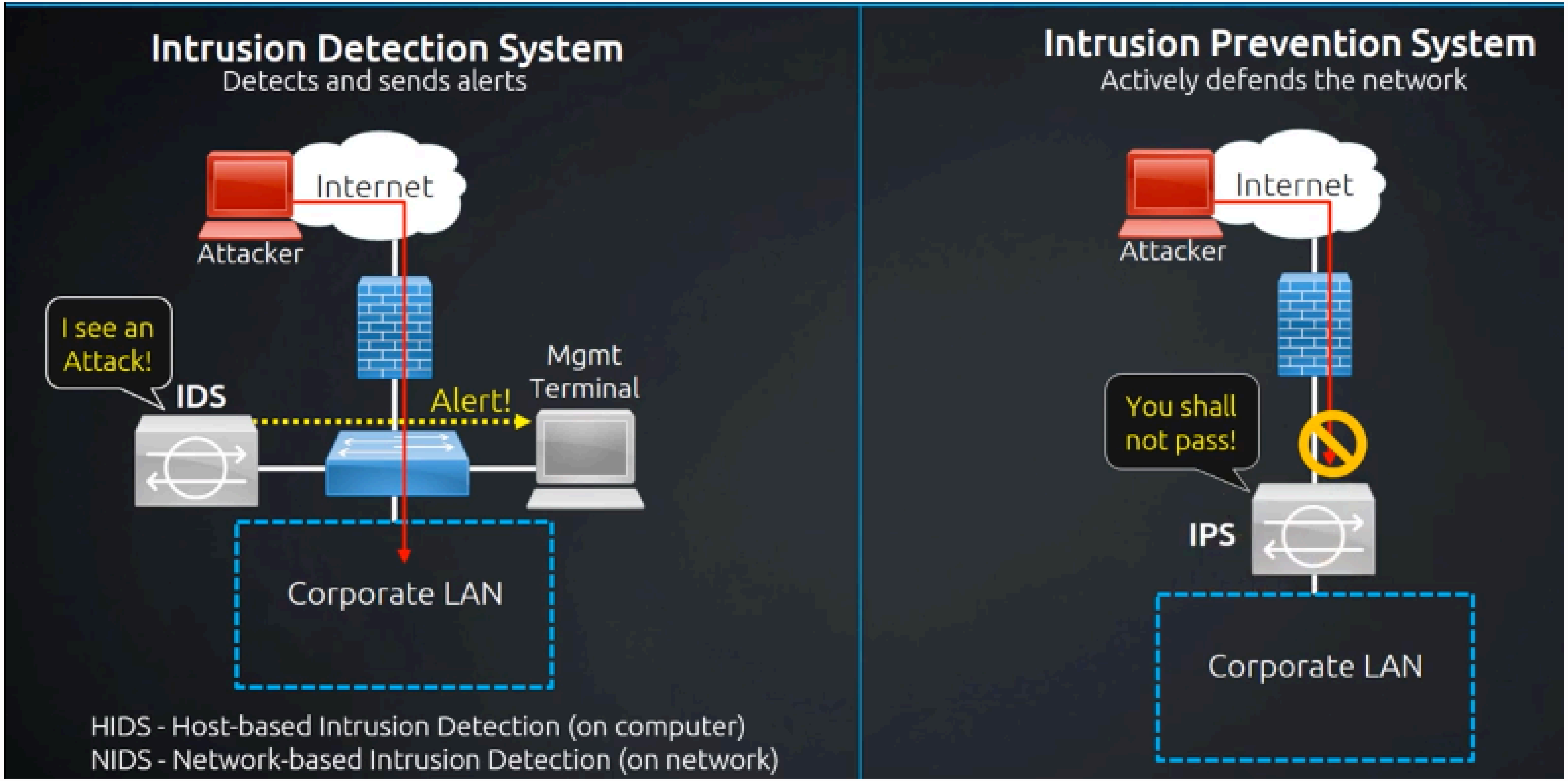
- What is Network Security?
- What is an IDS?
- IDS vs IPS
- Importance of real-time detection

2.What is an IDS?

IDS Is Stands for (**Intrusion Detection System)**



IDS vs IPS


Intrusion Detection System
Detects and sends alerts
Internet
Attacker
I see an Attack!
IDS
Alert!
Mgmt Terminal
Corporate LAN
HIDS - Host-based Intrusion Detection (on computer)
NIDS - Network-based Intrusion Detection (on network)
Intrusion Prevention System
Actively defends the network
Internet
Attacker
You shall not pass!
IPS
Corporate LAN

By BobXploit **Think Like A hacker protect Like A Pro**

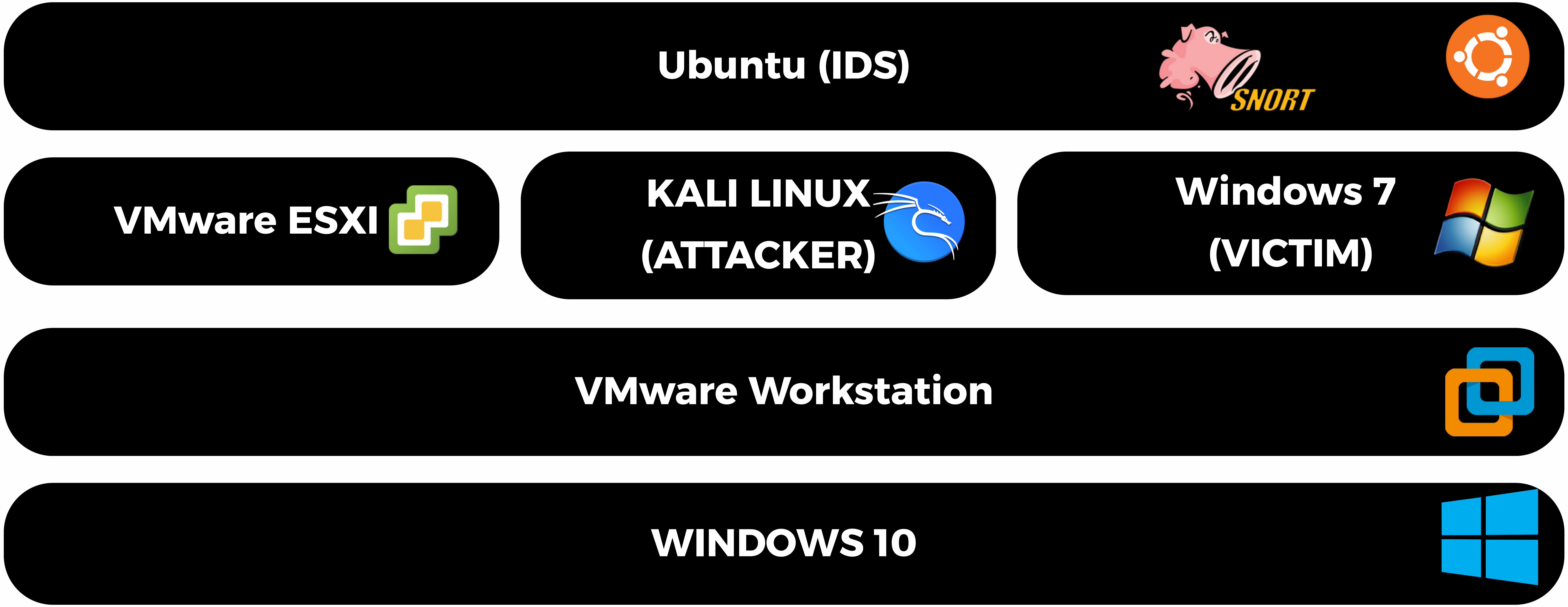
Importance of real-time detection

- **Minimizes Damage**
- **Reduces Response Time**
- **Protects Sensitive Data**

What is Snort?

snort is a popular **free** and **open-source IDS/IPS system** that is used to perform traffic/protocol analysis, content matching and can be used to detect and prevent various attacks based on predefined rules.

Project Architecture



Ubuntu (IDS)

SNORT

VMware ESXI

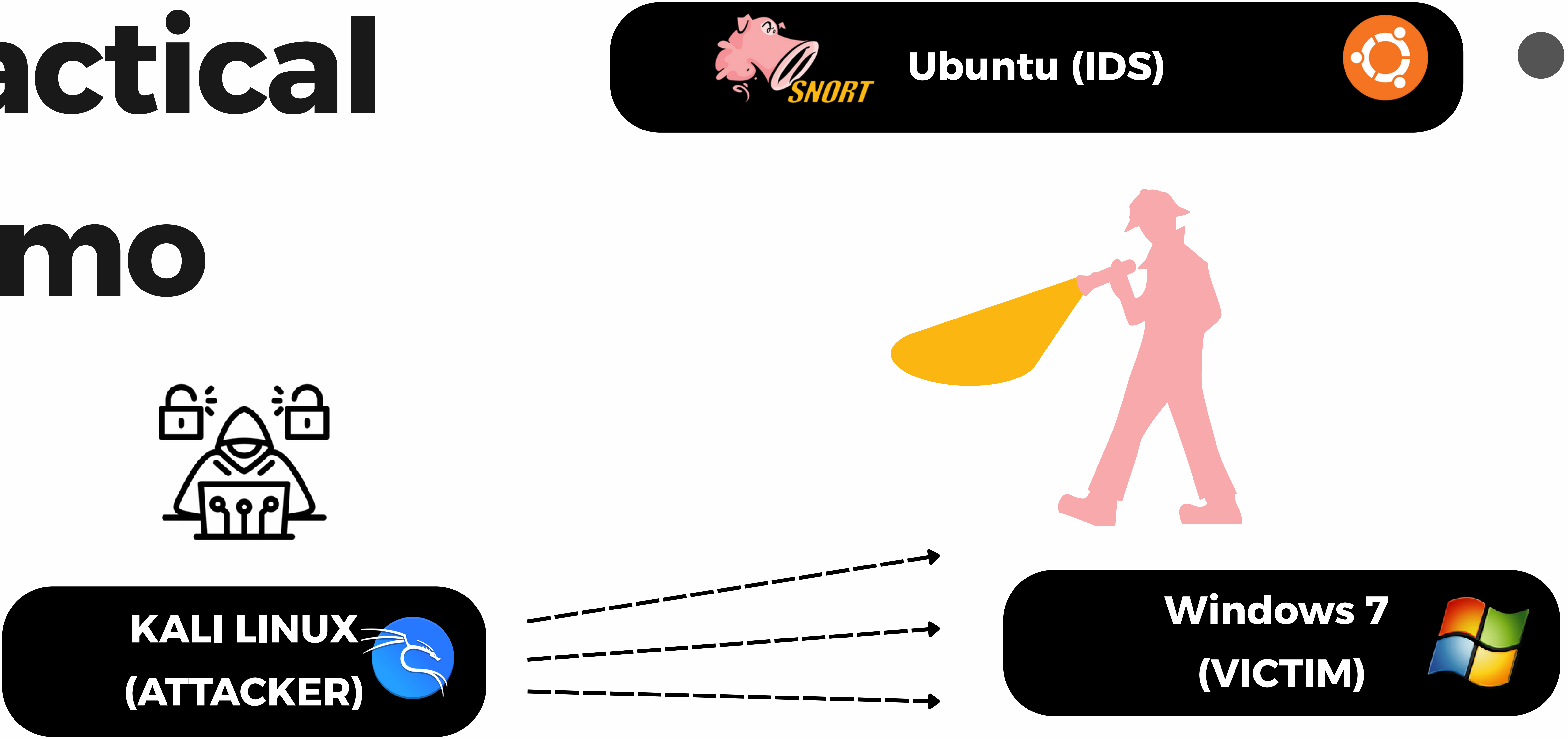
KALI LINUX (ATTACKER)

Windows 7 (VICTIM)

VMware Workstation

WINDOWS 10

Practical Demo



Ubuntu (IDS)

KALI LINUX (ATTACKER)

Windows 7 (VICTIM)

Recourses:

- Snort Playlist @hackersploit
- Blue machine @Try_Hack_Me
- Ubuntu ISO @ubuntu.com
- Snort Rules @snopy.org

THANK YOU

By BobXploit

Think Like A hacker protect Like A Pro