# IDS Fundamentals:

## TYPES OF IDS:

## HOST INTRUSTION DETECTION SYSTEM (HIDS):

* This type of IDS solutions is installed individually on the hosts.
* Only detect the potential security threats associated with that host.
* Detailed visibility of the host’s activities.
* Resource-intensive and require management on each host.

**NETWORK INTRUSION DETECTION SYSTEM (NIDS):**

* Detect the potentially malicious activities within the whole network.
* Monitor network traffic of all hosts.
* Provide centralized view of all detections inside a whole network.

**DETECTION MODES:**

**SIGNATURE-BASED IDS:**

* Each attack has its own pattern, known as signature.
* IDS have their databases where signatures of known attacks are stored.
* Efficiency = Stronger database
* Unable to detect Zero-day attacks.
* E.g., Snort

**ANOMALY-BASED IDS:**

* Learn normal behavior of the network/system and performs detections if there are deviations from the normal behavior.
* Can also detect Zero-day attacks, due to the anomaly-based detection.
* May also generate false positives.
* Can reduce false positives by fine-tuning IDS.

**HYBRID IDS:**

* Combines both signature-based IDS and anomaly-based approaches.
* Use the database for known attacks and anomaly-based detection for Zero-day attacks

**IDS EXAMPLE: SNORT**

**MODES OF SNORT:**

**PACKET SNIFFER MODE:**

* Reads and displays packets without performing any analysis on them.
* It can be helpful in network monitoring and troubleshooting
* Allows to display the network traffic on console or output it in a file.

**PACKET LOGGING MODE:**

* This mode allows to log the network traffic as PCAP file.
* Includes all network traffic and any detections from it.
* Helpful in Forensic investigations.

**NETWORK INTRUSION DETECTION SYSTEM MODE:**

* It’s the primary mode on SNORT.
* Monitors traffic in real-time and apply rules files to identify any known attack patterns stored as signatures.
* If a match occurs, it generates an alert.

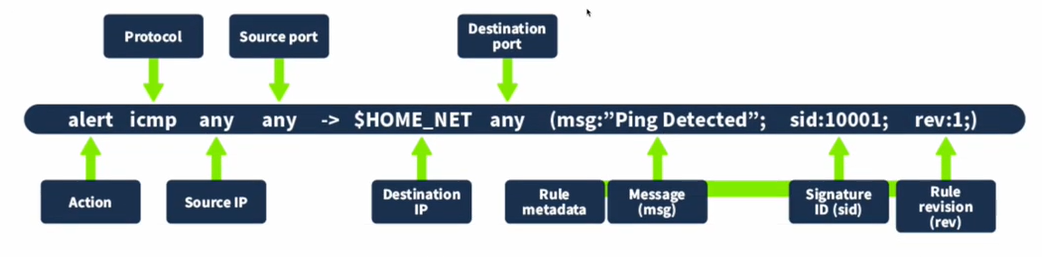
**SNORT DIRECTORY:**

* All the snort files are stored inside **/etc/snort** directory.
* Key file for Snort is its configuration file **snort.conf**
* In snort.conf we can specify which rule files to enable and which network range to monitor and enable other settings.
* Rule files are stored in **rules** folder.

**RULE FORMAT (HOW RULES ARE CREATED IN SNORT):**

There is a specific way of writhing rules.

This rule will detect ICMP packets coming from any IP address and port, reaching the home network to any port.

****

Details of this rule:

* **Action:** This specifies which action to take when the rule triggers. In this case, we have the action to “alert” when the traffic matches this rule.
* **Protocol:** Refers to the protocol that matches this rule. In this case, we use the protocol “ICMP”, which is used when we ping a host.
* **Source IP:** This determines the IP from which the traffic is originating. Since we want to detect traffic from any source IP, we set this as “any”.
* **Source port:** Determines the port from which the traffic is originating. Since we want to detect traffic from any source port, we set this as “any”.
* **Destination IP:**  Specifies the destination IP to which the matching traffic comes; it generates the alert. In this case, we used “$HOME\_NET”. This is a variable, and we defined its value as our whole network’s range in the Snort’s configuration file.
* **Destination port:** Specifies the port the traffic would reach. As we want to detect traffic coming to any port, we set it as “any”.
* **Rule metadata:** Every rule has some metadata. That is defined at the end of the rule in parentheses. The following are its components:
  + **Message (msg):** This describes the message to be displayed when the subject rule triggers. The message should indicate the type of activity detected. In this case, we used “Ping Detected”.
  + **Signature ID (sid):** Every rule has a unique identifier that differentiates it from the other rules. This identifier is called the signature ID (sid). In this case, we set the sid to “10001”.
  + **Rule revision (rev):** This sets the revision number of the rule. Every time the rule is modified, its revision number is incremented. This helps in tracking the changes to any rule.

# IDS LAB SETUP:

## Initial Setup:

## Virtual Box Installed Windows version 10 ISO (You can download it from the official site and can make a ready to use ISO file)

To fulfil both of these requirements you can watch this video:  
<https://youtu.be/XvZ45lsrG4A?si=4eenwasxmXUg9DGj>

**Then:**Install Wincap, you can download it from here:

[www.wincap.org/install/](http://www.wincap.org/install/)

After that install the npcap, you can download this one from here:  
[npcap.com](http://www.npcap.com)

Now in this Lab we will be installing the Snort’s installer for windows, download it and install it from here, for windows we will be using the snort’s 2.9\_19\_installer64.exe

[www.snort.org/downloads](http://www.snort.org/downloads)

Download and install it   
Install it on the default path, for future ease

After that create account on snort if already have one then sign in and download the community roles for the compatible version of windows we downloaded earlier.

At the moment In this scenario it will be:  
snortrules-snapshot-29111.

Now extract the rule folder you just downloaded and copy the rules and preproc\_rules folders and navigate to the Snort folder, if you did choose the

Default location then it will be C:\Snort

Now inside of the Snort folder past those folders and if asked select copy and replace.

Now will have to make some changes to the configuration file

Open the snort.conf inside of the Snort\etc

This is a long process so I am attaching the video link:  
<https://youtube.com/watch?v=e_KV3xivSnI&si=6J53b9D-qvbJLTph>

Now after all the steps its time to check:

Open the command prompt and navigate to the Snort\bin

You can use the dir command to see what’s in there:  
and after that you can use this command to check the version:

snort.exe -V

this will show the information about the current version installed on your setup

Then to check if our configurations went well, we can use this command to run a configuration checking test

Snort -T -c C:\Snort\etc\snort.conf

If you face any errors feel free to use the internet….

Then to run the Snort in sniffer mode we can use this command:

Snort -i <interface-number> -v

Sorry I forget to told earlier to check the interface-numbers configured we can use this command:

snort -W

make sure you’re in the Snort\bin directory on the command prompt.

And to exit the sniffer mode press ctrl + c.

Snort as IDS:

To run the snort as IDS we can use this command:

First make sure you are in the C:\Snort\bin directory

Then use this command:

Snort -i <interface-number> -c C:\Snort\etc\snort.conf -A console

End of the story this is just a basic guide do your own research and learn by hands on practice.

…Best Wishes…