Plus971

NIDS/HIDS

horizontal line

11JULY **20**23

# NETWORK BASED INTRUSION DETECTION SYSTEM (NIDS)

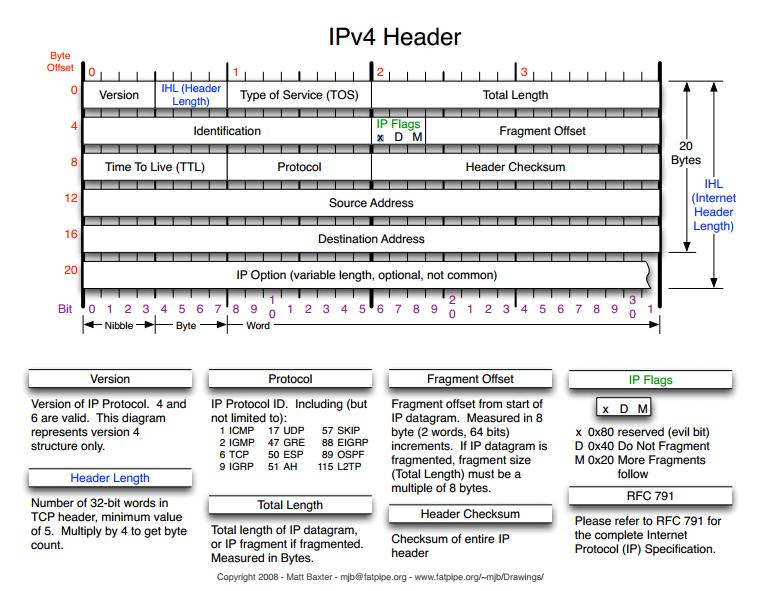
## What is it?:

NIDS is software that helps an organization identify suspicious/malicious activity within their network infrastructure (Servers, Employee PC’s,...) using a mixture of signature and anomaly based detection methods NIDS can detect anomalies activities in the network, the packet is then flagged as (H,M or L) and brought to the dashboard where the analyst takes further action.

## Installation steps:

1. After a machine has been selected, install NIDS software.
2. Connect the NIDS machine to a port on the switch and port forward all traffic to the internet onto that port.
3. select another port to act as the machine's IP address where the NIDS dashboard can be reached by other machines in the network.
4. Port Mirroring:

## How packets are flagged:

* **Signature based detection:** Every packet that travels through the network has a signature that NIDS compares network packets against a database of known malicious packet signatures and alerts the admins by flagging the packet and displaying the necessary information on the dashboard.
* **Traffic anomaly detection:** When NIDS is first setup it takes a baseline for network activity in the given scenario by monitoring and analyzing traffic, any significant deviation from this baseline can be seen as an anomaly and will be flagged and brought to an analyst's attention. For instance a DDos attack will raise the amount of network traffic in a significant way and this will raise flags.
* **Protocol Analysis:** NIDS also checks if each packet follows the correct structure and header format for a given protocol if the format/violates protocol specifications is incorrect the packet is flagged. An example would be if the evil bit in a packet header is set to 1 then the packet will be flagged. - bad example, change later.
* **Pattern Matching:** NIDS can use pattern matching techniques to identify patterns within packets that may indicate malicious activity and flag them.
* **Heuristic Analysis:** Heuristic algorithms can be used to identify malicious behavior in the network by looking for patterns of packet transmissions that may indicate a coming attack but don't necessarily have a known malicious signature.
* **Statistical Analysis:** statistical models can be used to identify network traffic patterns and properties of packets, properties such as packet size, protocol usage e.g. 200 ssh requests to a given computer. These properties can be indicators of abnormal activity and can be proactively flagged.
* **Reputation-Based Analysis:** NIDS can also keep a list of known malicious IP Addresses and any packets arriving from that site can be flagged as malicious.

## What happens after a packet is flagged:

1. Alert Generation: When a packet os flagged the admin/SoC team is notified via the NIDS Dashboard and relevant information is displayed, such as:
   1. IP Addresses
   2. Port numbers
   3. Timestamps
   4. Details about the detected anomaly
2. Alert Prioritization and Analysis: The alert along with its logs are then looked at by SoC analysts/Admins and based on the severity and relevance to the organization's security policies it is dealt with accordingly.
3. Investigation and Response: after receiving the alert the Soc team initiates the investigation to determine the nature of the alert(false positive?) and the scope of it(Severity) if action is needed then response procedures are followed to mitigate risk,
4. Validation and False positive analysis: if the packet is a false positive then the team looks into the packets data and verifies if the packet is malicious or not and determines why it was flagged, was it a faulty rule/misconfiguration?
5. Response actions: based on the severity and nature of the alarm the security team can take the following steps:
   1. Block source IP address
   2. Adjusting firewall rules
   3. Quarantining or isolating affected systems
   4. Deploying patches or updates
   5. Taking steps dictated by the circumstances
6. Reporting and Documentation: During the whole process every event is logged in the form of documentation of flagged packets, investigations conducted, actions taken, lessons learned, etc. this will act as a reference should the incident or something similar occur again.

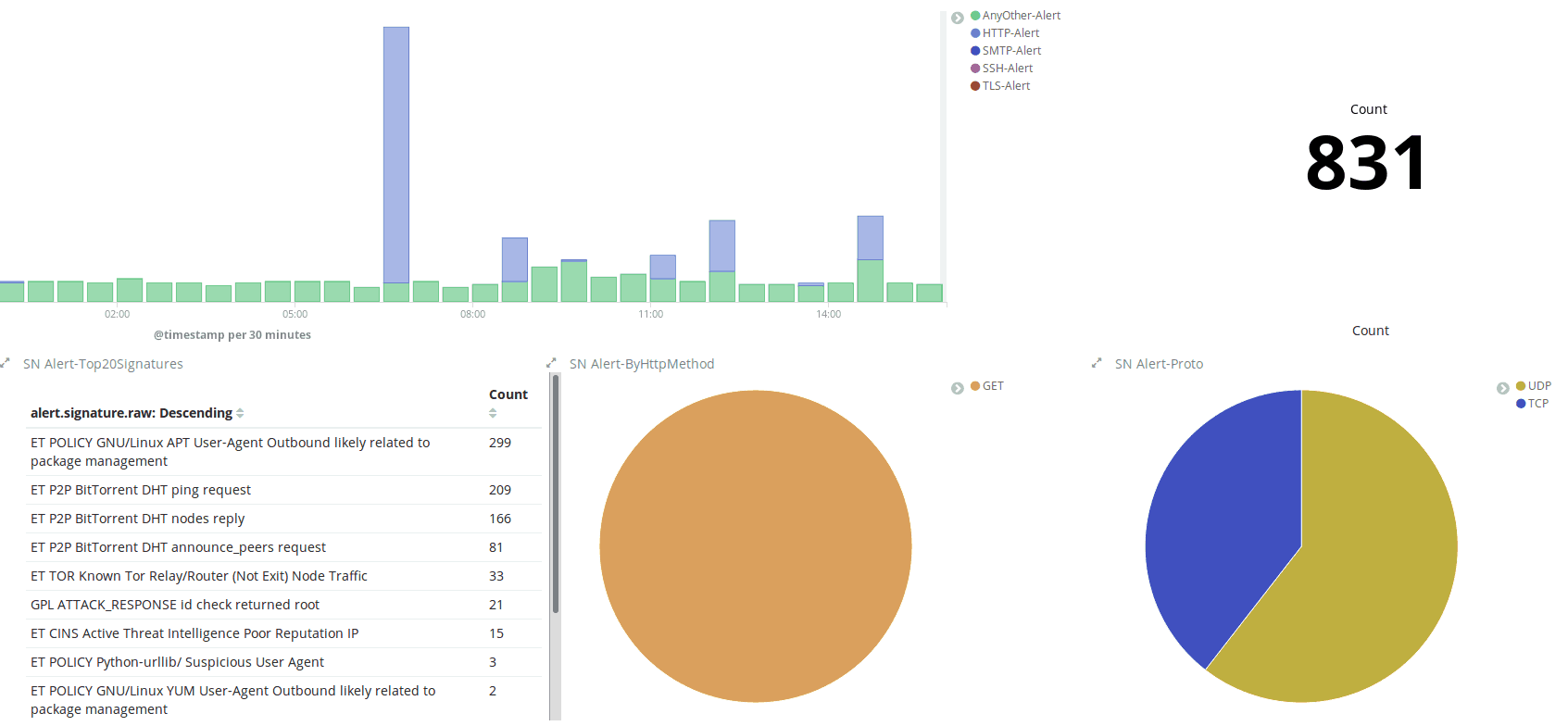
## Advantages of NIDS:

* Real time alerts: when NIDS identifies a threat it is immediately brought to the admin.security teams attention via the dashboard thus facilitating swift action to minimize the “damage”.
* It Can correlate attacks against multiple hosts
* It does not affect the performance of the host/Employee’s machine
* Compliance and regulation: NIDS can help organizations acquire certification and meet compliance requirements for regulations as it monitors the network for unauthorized access, preventing data leaks etc…
* Scalability: NIDS is a scalable system that can grow as the organization grows, NIDS machines can be placed in key points in the networks to avoid congestion or bottlenecks in the network resulting in slower speeds.
* Integration: NIDS can easily integrate with other security tools and systems such as firewall, IPS Systems and SIEM tools.

## Disadvantages of NIDS:

* False Positives: NIDS can often produce false positive alerts that can create multiple alerts to legitimate but unusual traffic, they can be triggered by network complexity, more traffic than usual etc… These false positives can create a distraction for the SoC team and draw attention away from an actual attack.
* False Negatives: The system can also produce false negatives letting malicious packets through, this occurs due to out of date malicious signature definitions or if the actor finds another way to bypass detection.
* Encrypted traffic: Encrypted traffic makes it difficult to check the packet for malicious intent and while there do exist ways to decrypt and check the data this adds additional complexity and performance overhead.
* Performance Impact: Inspection of all the packets in a highly congested network introduces more performance overhead as essentially every packet needs to be checked and this takes time. A way of thinking about this is adding a stop signal in a highly congested road. NIDS also takes up a decent amount of computational resources and organizations need to be considerate of the NIDS machine’s hardware requirements.
* Blind Spots: NIDS operates by placing a machine in key parts of a network that can leave blind spots in the network that attackers can infiltrate without being detected.
* Limited Application layer visibility: NIDS has limited visibility in the application layer of a packet and thus cant prevent application level attacks such as sql injection which occur at application level. A web application firewall(WAF) is needed for protection against these types of attacks.
* Network complexity: as the size of an organization's network infrastructure grows so will the level of expertise required to set up the NIDS machines in the network as policies would need to be modified.

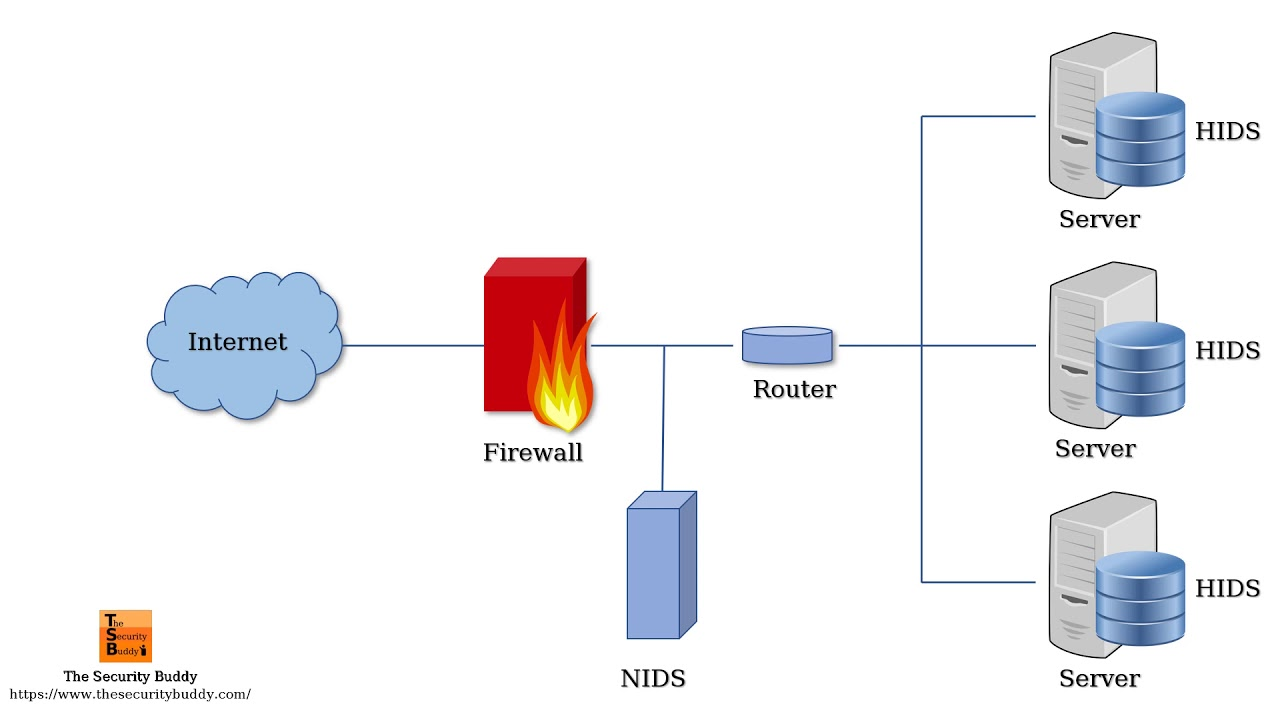
## Example NIDS Software

* Snort - open source, widely used, highly customizable, large community that updates rule sets continually.
* Suricata - designed for high speed networks, supports multi threading and is known for its robust rule language and support for new protocols.
* zeek(formerly bro) - open source, detailed insights into network activity useful for intrusion detection and incident response.

*- Suricata Dashboard Example*

# HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

## What is HIDS?

It is a security tool designed to monitor and protect individual host devices or end point devices from unauthorized access, malicious activities and other security breaches, HIDS operates at the host level for that machine and uses various techniques to detect suspicious behavior. Unlike NIDS, HIDS focuses on a machine's internal activity.

HIDS can also be deployed as an agent based solution deployed across a network to monitor multiple machines centrally and can complement other security features such as firewalls, AV software, NIDS, etc…

## Primary Functions Of HIDS

### System file integrity monitoring:

HIDS checks all files in the system for any unauthorized modifications, tampering or changes by comparing the current state of the file system against a known baseline or a cryptographic checksum to detect anomalies.

### Log Analysis:

HIDS inspects the following logs to detect anomalies System Logs, Application Logs, Audit Logs. It uses these logs to look for anomalies, abnormal patterns and specific event indicators to detect malicious activity.

### Registry Monitoring:

The system registry contains important configuration information and settings that if tampered with can allow a malicious actor to take control of the entire system gaining them access to stored passwords, documents, etc… and so HIDS looks for changes that could indicate malicious intent.

### Users and Process Monitoring:

HIDS monitors users as multiple login attempts, privilege escalations, etc… can be indicators of malicious activity. HIDS also checks running processes as an application that seems legit on the front can spawn many sub processes in the background that have malicious intent (for instance an offline app such as notepad transmitting data to another computer outside the network). RAM can also be checked by the HIDS to detect any unauthorized tampering with the pages in RAM that can cause trouble

### Malware Detection:

HIDS scans the host for known malware signatures, suspicious file behaviors, or indicators of compromise that can alert the HIDS(for instance if a word document when opened spawns 20 processes). HIDS can detect Malware, backdoors, trojans, etc…

### Real Time Alerting:

When the HIDS detects an event or activity that matches a predefined rules or signatures, it generates alerts or triggers alarms to notify the sys admins/ security team.

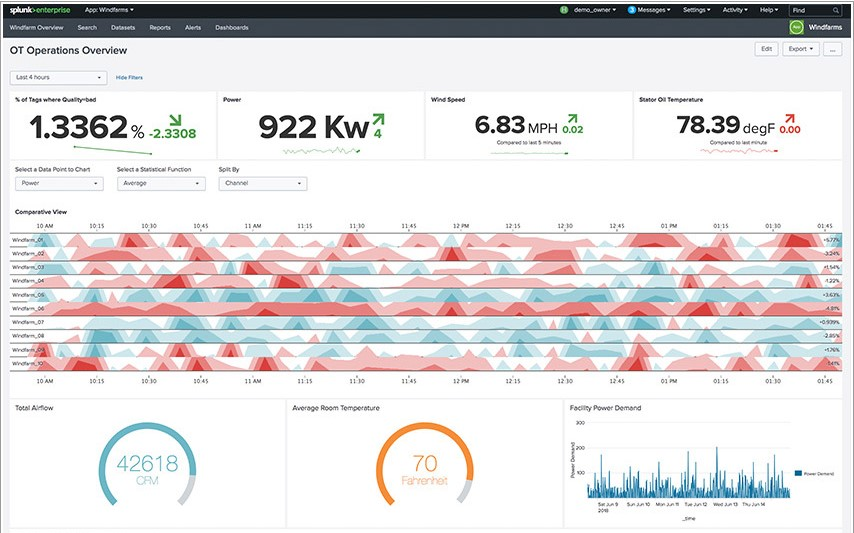
## Logs in Event Viewer

### What is it?

Every machine has an event manager that records/logs all interaction with the machine such as:

* connecting to port 22 for SSH ing from another computer,
* when a user logs in
* etc…

### Platform Specific event viewers:

* Windows - Windows Event Viewer, windows + R, then type “wventvwr”
* MacOS - can be viewed in the from the console app
* Linux - all log files are stored in the /var/log directory, applications for viewing the logs in a comprehensive way will need to be installed e.g. spunk

### Elements of a windows event log:

The windows log provides info about hardware and software events occurring in windows.

* Log name: name of the log to which events from different logging components will be written. Commonly logged for system, security and applications. Different types of log names are:
  + System log: contains info relevant to the system and its components, e.g. failure to load boot-start driver.
  + Application log: events related to a software, e.g powerpoint isn't loading
  + Security:logs related to safety. The event gets recorded during the audit process and includes e.g. failed and valid logins, file deletions, etc…
  + Setup:contains events that occur during the installation of the OS, on domain controllers this also contains logs related to active directory.
  + Forwarded Events:contains logs from other computers in the same network
  + Windows events are then categorized into 5 main types:
    - Information - app or service is going well
    - Warning - unimportant events hinting to a potential issue
    - Error - significant issue when a system cant function normally
    - Successful audit - records a valid attempt of audited security access for security log, such as a successful login attempt.
    - Failure audit - indicates the failure of audited security access under the security log, such as not being able to access a network drive
* Event date and time when the event occurred
* Task category: identifies the type of recorded event log, developers can define task categories for further levels of abstraction which can help narrow down the problem.
* Event ID: this is a windows id number that is unique
* Source: name of the program causing the event log
* Level: the security event level represents the level of severity they can be:
  + Information: indicates the event occurred without issue
  + Verbose: indicates the progress or success for an event
  + Warning: highlights a potential problem sysadmins should monitor
  + Error: Describes issues in the system or service that don’t require immediate troubleshooting and the service can still continue.
  + Critical: indicates significant issue in app or system that sysadmins should look at immediately.
* User: name of the user that was using the machine
* Computer: name of PC logging the event

## Advantages of HIDS:

* Zero day and unknown threat detection: HIDS can detect unusual patterns and flag them even if it doesn't recognize the activity as malicious.
* Compliance requirements: same as NIDS
* Forensic capabilities: Allows for forensic analysis to take place with ease as it records all interactions with the machine.

## Disadvantages of HIDS:

* Resource Intensive: HIDS can be resource intensive as they run on the machine they are protecting. This can lead to performance degradation.
* Managements and scalability: managing multiple hosts can be complex and time consuming especially as the organization scales.
* Limited scope: HIDS can only detect network based attacks to its own machine, it can't detect an attack on another computer in the network.
* false positives/negatives: like all IDS, HIDS can flag normal activities as malicious and vice versa this can lead to unnecessary alarms leading to wasted reconfiguration time.
* Dependance on host security: HIDS like all software can be tampered with, meaning if the host already has malware then the HIDS might become corrupted and non functional.
* Limited historical analysis:HIDS is bound by memory constraints and thus cant remember every type of attack signature that has ever occurred.

# SCENARIO

Organization name: RAK Academy(RAKA) school.

Security Measures: 1 NIDS, HIDS installed on every machine

Alert: HIDS on PC29 creates high level alert

What's happening?

The alert logs on PC29 suggest that the computer has downloaded a malicious file from the internet and this file has started up multiple threads of work in the background, NIDS then produces an alarm as multiple packets leave PC29 with a destination IP address in russia.

What happened?

A student was downloading a movie via utorrent and one of the seeders had injected malicious code in a segment which PC29 downloaded and when the student started playing the movie the file started other threads of execution in the background that were sending data to a russian IP.

What was done to fix IT?

A IT Admin went to the physical location of the pc and reading the HIDS killed the running processes and deleted the file off the computer.

A new rule was added to the NIDS ruleset blocking utorrent downloads and the russian IP was blacklisted.

And a rule to HIDS was added blacklisting utorrent packets from entering the machine.