NETWORK INTRUSION DETECTION SYSTEM

Utsav(20bcar0265)
Jasbir(20bcar0111)

28th March, 2022

—

Network IDS

—

Dr. Ajay Shriram Kushwaha

ABSTRACT

Intrusion Detection System (IDS) has recently become very famous as a key part of system defense. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. Pattern matching algorithm is usually used in intrusion detection system. During the detection process, the efficiency of pattern matching algorithm determines the performance of the intrusion detection system.

keyword: Intrusion Detection, Network Based

INTRODUCTION

Intrusion detection is defined as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions. The need for effective intrusion detection mechanism for computer systems was recommended by Denning and Neumann in order to find reasons for intrusion detection within a secure computing framework.

A host-based IDSs monitor activities associated with a particular host, while network-based ones operate on network data flows. The most common approaches to ID are statistical anomaly detection and pattern-matching detection.

Any set of actions that compromises the Confidentiality, Integrity, or Availability of Computer Resource is a type of Intrusion.

TYPES OF INTRUDERS

Masqueraders: unauthorized user who penetrates a system exploiting a legitimate user's account. (Outsider)

Misfeasor: a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuse his or her privileges. (Insider)

Clandestine user: an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. (Outsider/Insider)

CONSEQUENCES OF INTRUSION

- Read Privileged Data
- Perform Unauthorized Changes to Data
- Disrupt the flow of system

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

- ✓ NIDS resides on a computer or application connected to a segment of an organization's network and passively scan the traffic of the network.
- ✓ In NIDS, Sensors are located at choke points in network knows as Demilitarized Zone or DMZ.

NIDS FUNCTIONALITY

Sniffing:

Inspects the incoming traffic.

Protocol Awareness:

Protocol Reassembly & Normalization.

Alerting:

Send Email / Log Events.

MODES OF DETECTION

1. Signature-based Method:

   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) are not known.

2. Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

TYPES OF NETWORK INTRUSION DETECTION SYSTEM (NIDS)

Commercial:

- SolarWinds Security Event Manager (SEM)
- McAfee Network Security Platform (NSP)

Open Source:

- Snort
- Suricata
- Zeek (Bro)

NIDS EXAMPLE

Snort: Snort is probably the most well-known and popular IDS in existence. Its extremely large fan base has led to its rule formats being accepted as a widely-used standard, and many other Intrusion Detection and Prevention Systems are built to be compatible with it. Since Snort is open-source, it can be downloaded and deployed for free and is backed by Cisco.

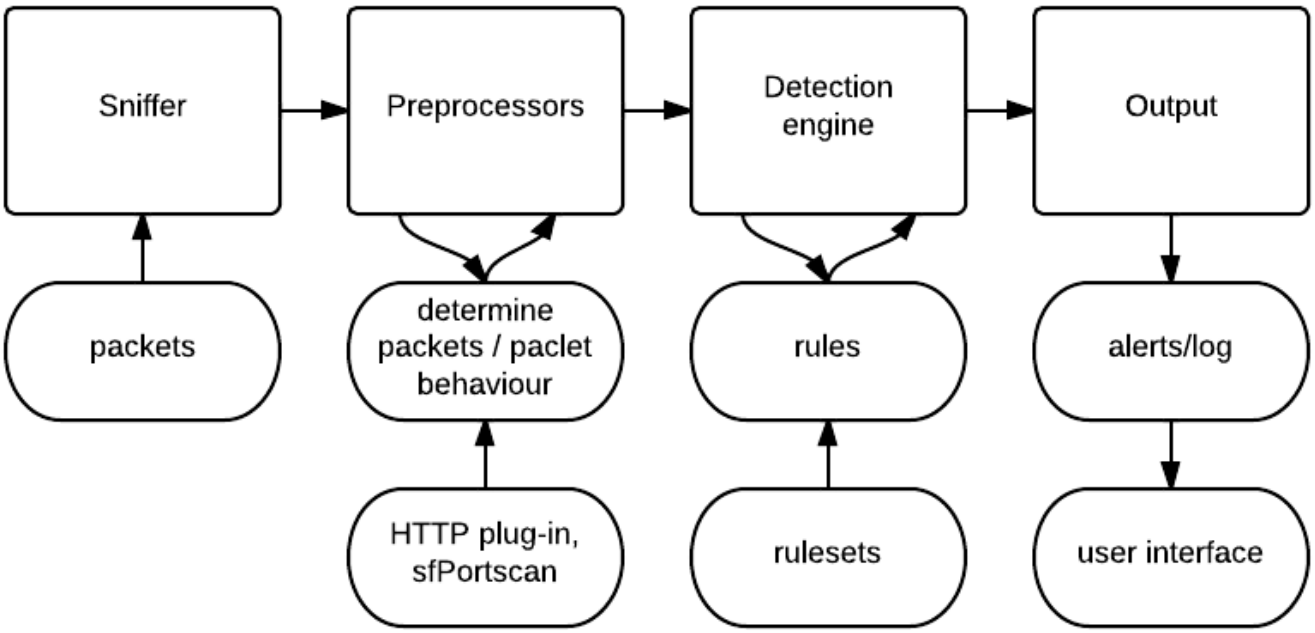
Pros:

- Usable on all operating systems
- Large library of pre-built detection rules
- Deep visibility into network traffic

Cons:

- Unstable updates

Snort Architecture:



Suricata: Suricata is designed to be a competitor to Snort. It is compatible with Snort file formats, rules, etc. and is also a free option. It includes features not available in Snort, such as performing network traffic analysis at the application level (which enables detection of malicious content spread over multiple packets).

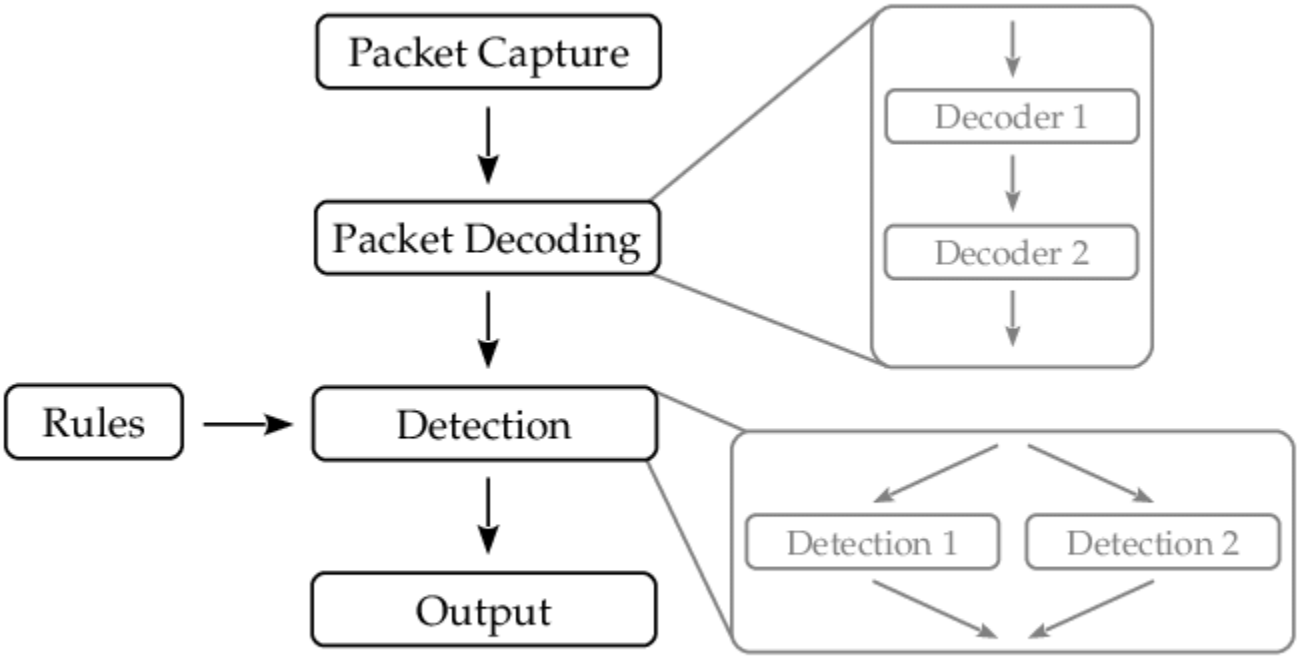
Pros:

- Open source
- Data collection at application layer
- Deep network traffic visibility
- Integration with a number of third-party tools
- Lua scripting support
- User-friendly interface
- Parallel processing with GPU support

Cons:

- Processor-heavy

Suricata Architecture:



Zeek: Zeek, formerly known as Bro, is an extremely powerful NIDS. Zeek's built-in scripting support enables a great deal of customization and customized automated responses to identified threats.

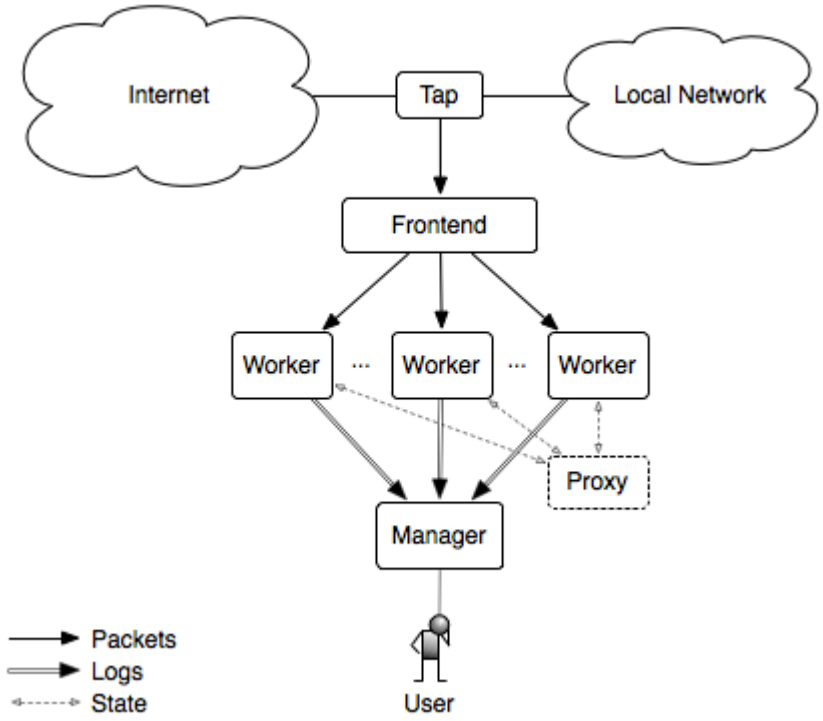
Pros:

- Open source
- Runs on MacOS and *nix systems
- Deep visibility into network traffic
- Integrated traffic logging
- Tasks enable customized automation

Cons:

- Steep learning curve

Zeek Architecture:



COMPARISON OF IDS WITH FIREWALLS

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

SPECIAL NOTE ON IDS COMPARED TO IPS

An IDS is reactive in nature. It only monitors and sends alerts of suspect activity. In contrast, an IPS will not only alert but can also take action to mitigate the problem. So, if the functionality of an IPS to take corrective actions is not required, why spend the money to implement an IPS? The answer to this stems from the concept of palatable risk. An IPS solution provides the capability for corrective actions to be taken before a system administrator has the opportunity to respond, which can be desirable during an active attack against systems. Without human intervention, it is possible to cause a Type I error (or false positive) and block legitimate traffic from legitimate customers. Certain types of attack are clearly articulated and can easily be effectively blocked with an IPS.

CONCLUSION

Intrusion detection system can be used for monitoring file system for changes. It is helpful in detecting what changes are made to the system after an attack. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. We intend to avoid the access and keep track of the intruder's attempts and intentions. Such a system can make a big addition to the security in today's world to avoid different kinds of attacks (CryptoLocker, WannaCry, other Ransomware attacks) happening around.