Activity # 7 - Network Security Solutions

Started: Nov 25 at 6pm

Quiz Instructions

You will learn about Network Security Tools.

This will lock questions after answering.

Question 2 1 pts

Intrusion Detection System (IDS)

What is IDS?

An Intrusion Detection System (IDS) is hardware or software used to detect security breaches and attacks by monitoring a network or host.

Types of IDS

There are many different types of IDS products:

Network Intrusion Detection System (NIDS)

Network Intrusion Detection System (NIDS) is used to detect whether there is traffic suitable for attacker behavior by passing all traffic on the network through it. When abnormal behavior is observed in the traffic, an alert can be generated and the administrator can be informed.

Host Intrusion Detection System (HIDS)

The Host Intrusion Detection System (HIDS) works on a specific host in the network. It tries to detect malicious activities by examining all network packets coming to this device and all network packets going from this device. Detected malicious behaviors are reported to the administrator as an alert.

Protocol-Based Intrusion Detection System (PIDS)

A protocol-Based Intrusion Detection System (PIDS) is a type of IDS that examines the traffic between a server and a client in a protocol-specific way.

Application Protocol-based Intrusion Detection System (APIDS)

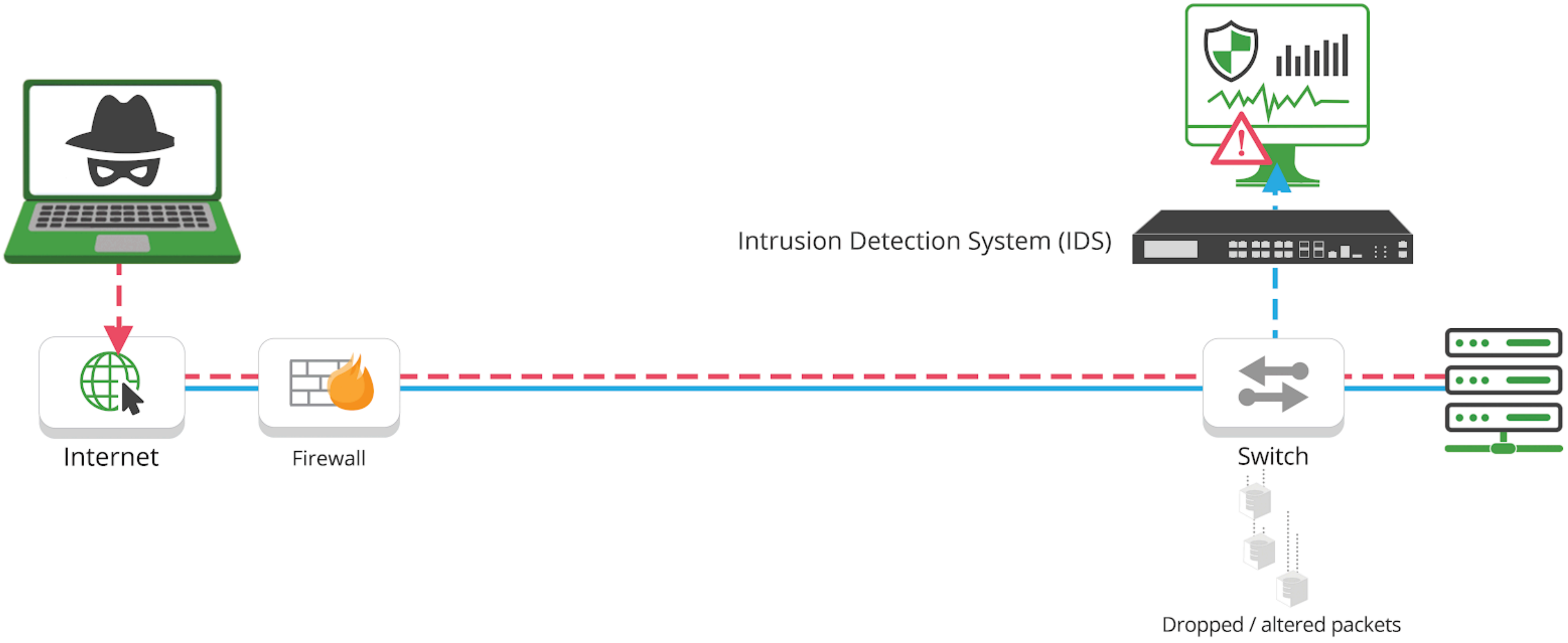
An Application Protocol-Based Intrusion Detection System (APIDS) is a type of IDS that tries to detect security breaches by monitoring communication in application-specific protocols.

Hybrid Intrusion Detection System

A hybrid Intrusion Detection System is a type of IDS in which two or more violation detection approaches are used together.

Functions of IDS

- Detecting security breaches according to the detection methods used by the IDS product is the main task of the IDS product.
- When IDS detects a security breach, the administrator is informed, and/or this information is sent to the Logs .



Importance of IDS for Security

IDS is a product developed to detect malicious behavior. It can be said that security is lacking in a network without IDS. Because IDS is one of the products that has reached a certain technological maturity. Due to its task, it is very important to detect security breaches. It is recommended to be used with other security products rather than alone. Since the IDS product does not have the ability to take action, it will be more effective to use it with a security product that has the ability to take additional action.

Some popular IDS products used in the cybersecurity industry are as follows:

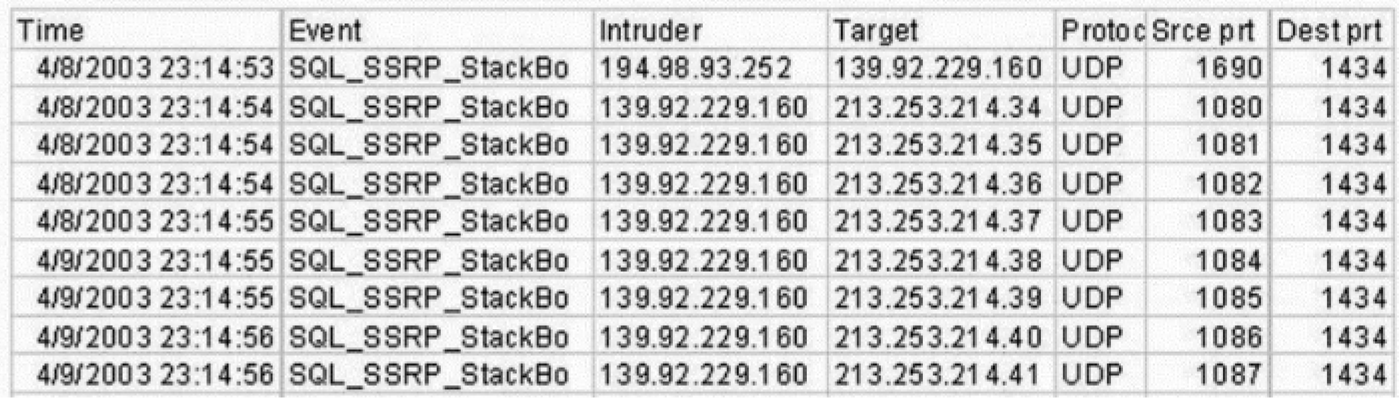
- **Zeek/Bro**
- **Snort**
- **Suricata**
- **Fail2Ban**

- **OSSEC**

What log sources does the IDS have?

During its operation, IDS detects security violations according to previously established rules. Therefore, it is very important how much the written rule defines the attack. If the written rule cannot detect the attack or detects the normal behavior as an anomaly, the rule should be changed or the incoming alerts should be reviewed by the analyst. Among the IDS logs examined by the analyst, there is information in the network packets regarding the security breach.

Sample of Logs in IDS *(This is not a standard log, it varies to different vendors):*



Time	Event	Intruder	Target	Protoc	Srce prt	Dest prt
4/8/2003 23:14:53	SQL_SSRP_StackBo	194.98.93.252	139.92.229.160	UDP	1690	1434
4/8/2003 23:14:54	SQL_SSRP_StackBo	139.92.229.160	213.253.214.34	UDP	1080	1434
4/8/2003 23:14:54	SQL_SSRP_StackBo	139.92.229.160	213.253.214.35	UDP	1081	1434
4/8/2003 23:14:54	SQL_SSRP_StackBo	139.92.229.160	213.253.214.36	UDP	1082	1434
4/8/2003 23:14:55	SQL_SSRP_StackBo	139.92.229.160	213.253.214.37	UDP	1083	1434
4/9/2003 23:14:55	SQL_SSRP_StackBo	139.92.229.160	213.253.214.38	UDP	1084	1434
4/9/2003 23:14:55	SQL_SSRP_StackBo	139.92.229.160	213.253.214.39	UDP	1085	1434
4/9/2003 23:14:56	SQL_SSRP_StackBo	139.92.229.160	213.253.214.40	UDP	1086	1434
4/9/2003 23:14:56	SQL_SSRP_StackBo	139.92.229.160	213.253.214.41	UDP	1087	1434

Physical Location of the IDS Device

The location of the IDS device in the network may vary depending on which type of IDS it is. For example, a NIDS-type device must pass all packets coming into the network over it. Therefore, it is more suitable to be positioned close to the network devices that provide access to the external network. A HIDS-type device, on the other hand, should be positioned close to the host in the network because it only examines the network packets coming to and leaving a certain host.

Q # 1

AnimoSpace Support

How many of the following are tools in the IDS type?

1. Snort
2. Volatility
3. OllyDbg
4. Suricata
5. Zeek/Bro
6. REMnux

Answer Format: X

Sample Answer: 7

6

Next ▸

Quiz saved at 6:01pm Submit Quiz