Network Security Tutorial

By: Mohammed Almulla

Introduction

Network security is huge configuration that is designed to protect CIA triad of computer network. The CIA triad means confidentiality, Integrity, and availability. Before going deep to network security lets introduce first cyber security.

Cyber Security

Cyber security is understanding, managing, controlling, and mitigating risk to an organization's critical assets. So, you need to ask about the assets (valuable objects) in an organization that if a risk effect on, it will cost the organization too much. In other words, you must know what you are protect, then you must implement security. The most important thing in security is that you must define risk because it is the heart of security.

$$Risk = Threats \times Vulnerabilities$$

The risk is the probability of loss, threat is the potential of harm, and vulnerability is the weakness that allow the threat to evident itself against an organization.

Motivation of Attackers

It is important to know what motives the threats or attackers. By knowing what motives them then we can build a security system. As follows what motives the attackers:

1- Attackers like to count the number of systems they compromise

2- Attackers could revenge of an organization, many of them could be insiders

3- Attackers that their goal is to steal finances

4- Attackers that espionage on an organization then sold the secrets of that organization to another party.

Hackers

A hacker is anyone who attempts to gain access to unauthorized resources. They are people that attack systems and networks without permission, collect secret data, crash systems, etc. There are two types of hackers:

- Beginners: They use tools and techniques available on the internet.
- Professionals: They use tools in the internet or they develop their own tools, and they use their own strong knowledge of: TCP/IP protocols, cryptography, networking, etc.

There are only 10% professional hackers, while there are many dangerous hackers that are called cyber-criminals. Also, many hackers been disappeared, killed, or in jail. Many also become official hackers that recruited by governments, or many are recruited by criminal organizations.

Dark Web & Deep Web

Deep web is part of the world wide web (www) that have a hidden IP address, and to access it you need a specific browser such as Tor. While the dark web or Darknet is a small piece of deep web that have encrypted websites and a hidden IP address. The dark web is more dangerous than the deep web because it contains illegal websites, black markets, etc. While deep web contains websites not indexed with search engines we use such as Google, Yahoo, etc. An example on deep web websites is hidden wikis, net banking, medical records, etc.

Intrusion Detection & Prevention Systems (IDPS)

Intrusion detection system is a system that detect intrusions in a system. Intrusions like malicious activities or unauthorized access to the system by an attacker. It is like an alarm to alert the admins if any malicious activity begins to the system to provide countermeasures. It is set of techniques and methods that are used to detect suspicious or malicious activities in the network or system.

While Intrusion detection system is only detecting intrusions, Intrusion detection and prevention system is detecting plus prevent and response to the malicious activity. The intrusion detection and prevention system is sending alerts with try to make action such as block or deny the malicious or hosts traffic to prevent the system from the malicious activity.

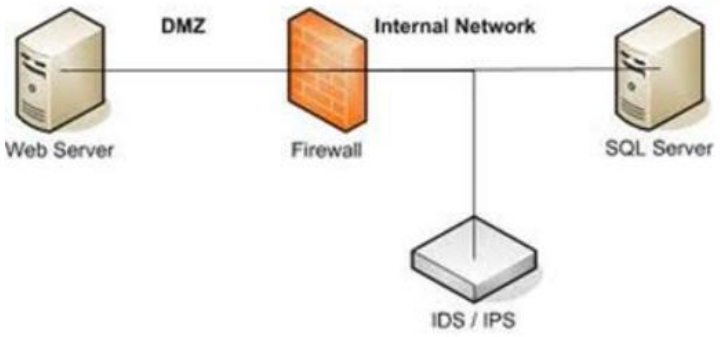
The goals of IDPS are as follows:

- Alert the admins if a malicious activity begins and try to prevent or minimize damage
- Must assess large volumes of network traffic
- Must record its findings in log to examine past activity
- Must detect and record unauthorized access without compromise to be an evidence
- Must respond immediately
- Must protect itself and the system to be inaccessible to an attacker

IDPS & Firewalls

IDPS can work in parallel with firewalls. The firewall protects an organization from outside attacks. Also, the firewall is good in filtering incoming and outgoing packets

traffic. But, flooding the firewall with an accepted packets will be going to crash it. The IDS detects if someone is trying to get inside the network or trying to access internal systems.



IDPS Categories

Firstly, there are three primary detection methodologies as follows:

1. Anomaly Detection: It detect both network and computer intrusions and misuse by monitoring system such as CPU over utilization, Hard disk continuous activity, and user logins and files transferring. We use anomaly detection when we concerned about network misuse in an organization or to monitor all email traffic, web usage, and FTP servers.
2. Signature Detection: also known as misuse-based or knowledge-based detection. It is that the network engineers code the signature for any attack that they research about it, then they made a database from these signatures. Finally, the IDPS compare between any packet enters the network with the signatures stored in the database. If any packet be like any signatures, it will activate the alarm and response system. Else, it will let the packet pass. Also, the signatures must be updated to maintain IDPS effectiveness. An example on signature detection is an email with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware. The weakness of signature detection that is not keeping state information (Stateless).

So, as in our example if an attacker modified the malware to be “freepics2.exe” a signature looking for “freepics.exe” would not match it, due to not having it in the database and it does not take the state information for the malware to know it later. Most IDPS are based on signature detection.

3. Stateful Protocol Analysis: As it is known the stateful protocol analysis keeps the state information of any packet enters the network. It uses the same method as signature detection adding to it keeping state information of a packet. When IDPS receives a packet, it compares between entries of the packet in the state table for the connection between the host and remote computer. The state table contains record of connections between computers that includes source IP and port, destination IP and port, and the protocol it used. Also, IDPS needs to maintain state information for the entire length of the attack, which is called the event horizon. It involves many approaches:
    a. Traffic Rate Monitoring
    b. Protocol State Tracking (Stateful packet filtering)
    c. Dynamic Application layer protocol analysis: Identify applications not using standard ports
    d. IP packet reassembly: Reassemble fragmented IP packets to prevent fragments from passing through to the internal network

There is another detection method, but its disadvantages exceed the advantages for it. It is known as heuristics that is an algorithm to detect suspicious traffic. It could be used in recognizing potential email-based attacks.

There are two types of IDPS as follows:

1. Network-based IDS (NIDS): the packets are analyzed while they are flowing through the network by a sensor. A sensor is hardware or software that monitors network traffic in real time. We position NIDS behind the firewall and before the LAN, between the firewall and the DMZ, or on any network segment.
2. Host-based IDS (HIDS): the IDS examines packets on each individual machine or host. In host-based configurations, an IDPS installed on a single host computer has its agent built in to the IDPS software.
3. Hybrid IDPS: combines the capabilities of an HIDPS and NIDPS for more flexibility and security.

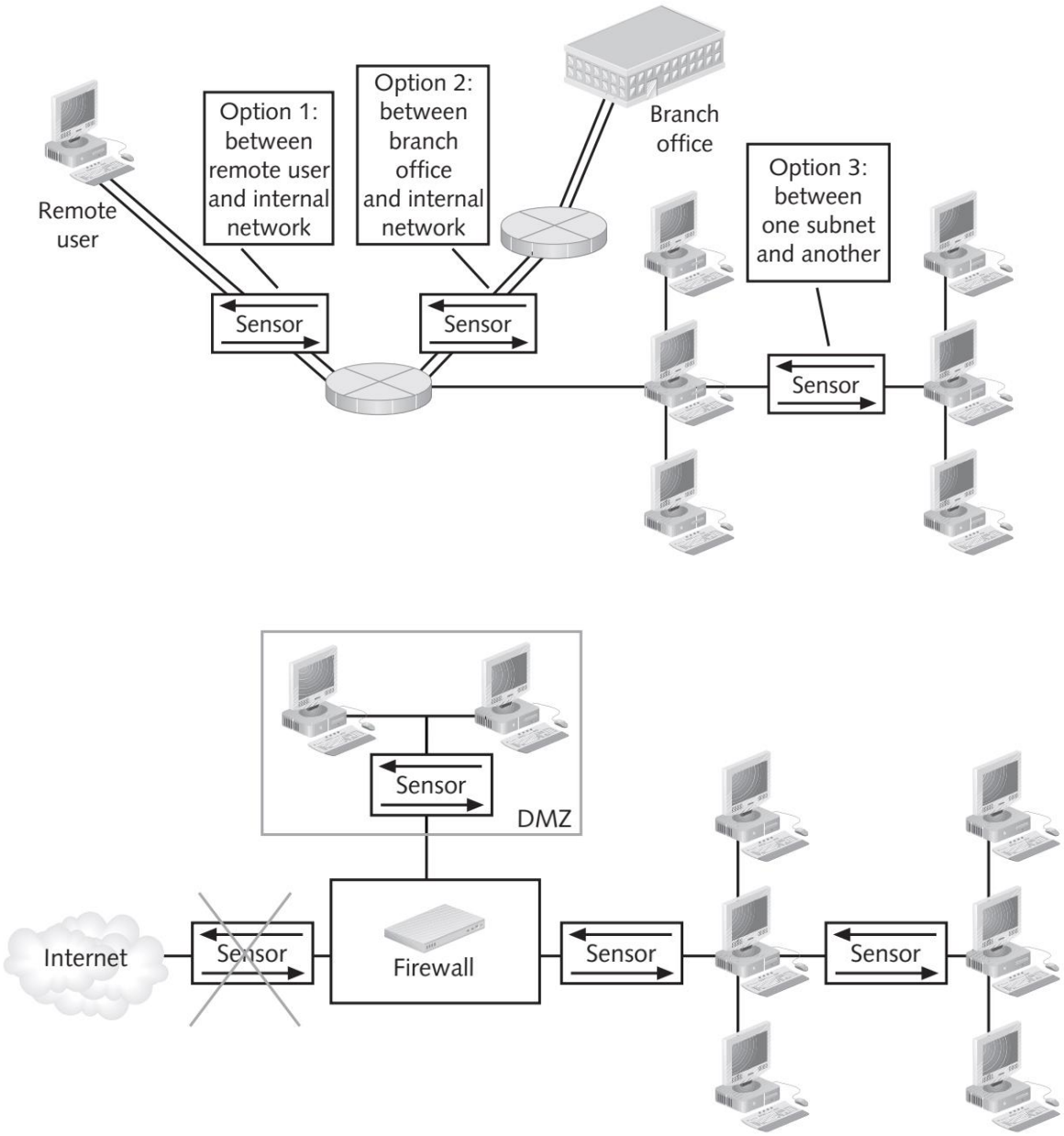
Furthermore, IDPS systems have two types as follows:

1. Passive System: the IDS detects the potential attacks, logs the information, and signals an alert
2. Reactive System: the IDS responds to the suspicious activity by logging off a user or by reprogramming the Firewall to block network traffic from any suspected malicious source (The Intrusion Prevention system job)

Where to put IDS system (sensor) on the network?

IDSs can be put in any place in the network and in any high-value host or server where traffic will be analyzed for detecting intrusions. The number of IDSs depends on many factors: The size of the network, Staffing limitation, and financial. In the most case, for each single network segment, an IDS sensor is recommended. In all sides of the firewall, it recommended to put network-based IDS (NIDS). And in high-value host and servers it

recommended to put Host-based IDS (HIDS). The sensors or agent data they gather log data and store it in a central repository called IDPS management server.



Why we need IDS if we have a firewall?

As we say before, firewalls just filter incoming and outgoing traffic without any attempt to detect attacks. It does not protect our networks and hosts from many types of attacks: IDS detect attacks against network that Firewalls are not able to see. For example, Denial of Service (DoS) attacks. Another major problem that firewalls are present only on the boundary of your network. Around 80% of attacks are due to hacking from the inside

network, where firewalls have no presences at all. A Firewall at the perimeter of the network sees nothing going on inside.

Denial of Service (DoS) attack

It is by fake TCP traffic to flood the target hosts. It floods the target host by SYN packets, then the host will send SYN+ACK and wait for an ACK, but the attacker will send another SYN, and another till the system slow the service and crash, due to the memory buffer will become full. It also known as half open connection. Most IDS will recognize and report DoS attacks.

The main reasons for adding IDS for your Firewall are:

- Catches attacks that the Firewalls allow and cannot detect (such as attacks on the web servers itself, where the firewall has no real action).
- Catches attempts that fail, especially failing attempts to gain access to a service.
- Catches insider hacking, and malicious activity from inside the network.

Questions to ask for IDS vendor:

- What does it cost?
- What's the cost of signature updates and product's maintenance?
- How many signatures does the system support?
- What intrusion response features does the product have?
    - Block hosts, protocols (ICMP, TCP, UDP), services/ports (http, smtp, ftp,…)
    - Talk to the Firewall/router/switch to update their ACLs or filter rules,…

Types of attacks detected by IDSs:

1. Denial of Service (DoS): DoS attacks are designed to bring down a network, a server, or a software by flooding it with large amounts of traffic. This is generally accomplished by sending a high volume of useless packets such as SYN or PING. Most IDSs will recognize and report these attacks.
2. Exploits: The attacker tries to exploit possible holes in the target host, device or software. The attacker may start checking for login accounts with easily guessable passwords.
3. Reconnaissance: Reconnaissance (discovery) step is a step that comes before an attack and consists into collecting information about the target networks or hosts. Reconnaissance activities perform usually: TCP and UDP port scanning, Ping sweeps (Ping Scanning), Tracerouting, etc.
4. Misuse: Activity indicates that someone is attempting to violate the corporate policy.

IDSs Benefits

IDSs allow centralized and ease-of-use intrusion management for many different networks. When an event is activated, different actions can be configured to run, such as: Sending email to the system administrator, Network shutdown, Server shutdown, Updating ACLs in router and switch, and Updating Firewall rules.

IDSs Shortcoming

An IDS is by no means the complete security solution, as it has many significant shortcomings:

- Since IDS relies on attack signatures, so IDS should have the most updated collection of attack signatures: This is near impossible since new vulnerabilities are found daily.
- IDS can do nothing for some types of attacks, such as Virus attacks.

References & Useful Resources

- Network Security 2, UAE University, Dr. Zouheir Altrabelsi slides
- Guide to network defense and countermeasures by Randy Weaver, Dawn Weaver, Dean Farwood