Cisco: Intrusion Prevention System (IPS / IDS)

Introduction

Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are security mechanisms for monitoring network traffic and detecting potential attacks. A basic version of IPS/IDS can be deployed on Cisco routers without the need for external equipment.

- **IDS** - A system that detects threats (informs, does not block).
- **IPS** - a system that detects and blocks threats.

Cisco enables IPS/IDS to be implemented directly in the IOS using built-in signatures and appropriate policies.

Requirements

- Cisco IOS with support for IPS functions
- Access to IPS signatures (`.pkg` file).
- Flash memory with adequate space
- Enabling the service and configuring the relevant policies.

IPS configuration in inline mode

1 Enabling inspections

```
conf t
ip ips name moj_ips
```

2 Load IPS signatures

The signatures must be downloaded and uploaded to the router (from TFTP or locally). Example:

```
ip ips signature-definition
 load tftp://192.168.1.100/IOS-Sxxx.pkg
```

3. enabling IPS on interfaces

An IPS policy must be assigned on the interfaces:

```
interface FastEthernet0/0
 ip ips moj_ips in
```

```
 exit

interface Serial0/0
 ip ips moj_ips out
 exit
```

4. configuration of alerts and logging

```
ip ips notify log
ip ips notify sdee
```

In addition, if the router has logging capabilities:

```
logging buffered 51200 debugging
```

Modes of operation

- **inline (IPS)** - packets are analysed and can be blocked before reaching their destination.
- **promiscuous (IDS)** - packets are only analysed and reported (requires SPAN/mirroring).

Integration with Snort (open source IDS)

Snort is a popular, free IDS/IPS system that can be configured to analyse traffic flowing through a router.

A. Installation of Snort

On a Linux system (e.g. Ubuntu/Debian):

```
sudo apt update
sudo apt install snort
```

B. Snort configuration for traffic analysis

1. **Sniffer (monitoring) mode:**

```
sudo snort -i eth0 -A console -c /etc/snort/snort.conf
```

2. **Set the router interface to SPAN/monitor mode** (If you are using GNS3, do „port mirroring” on the interface):

```
monitor session 1 source interface FastEthernet0/0
monitor session 1 destination interface FastEthernet0/1
```

3. **Connect Snort** to the SPAN destination port (e.g. `FastEthernet0/1`).

C. Create your own signatures

Snort signatures are stored in `.rules` files. Example of a rule:

```
alert tcp any any -> any 80 (msg:"HTTP access detected"; sid:1000001;
rev:1;)
```

Place your own rules in the `/etc/snort/rules/local.rules` directory and enable them in the configuration file.

Automatic signature download for Snort

The most convenient way to update Snort rules is to use the tool **PulledPork**.

A. Installation of PulledPork

On a Linux system:

```
sudo apt install pulledpork
```

Or download from the repository:

```
git clone https://github.com/shirkdog/pulledpork.git
```

B. PulledPork configuration

Edit the `pulledpork.conf` configuration file:

```
rule_url=https://www.snort.org/reg-rules/snortrules-snapshot-29120.tar.gz|sn
ortrules-snapshot.tar.gz|oinkcode
oinkcode=TWÓJ_KOD_OINK
snort_path=/usr/sbin/snort
config_path=/etc/snort/snort.conf
rule_path=/etc/snort/rules/snort.rules
local_rules=/etc/snort/rules/local.rules
sid_msg=/etc/snort/sid-msg.map
```

> To obtain the `oinkcode`, register at. https://www.snort.org/

C. Starting the update

```
sudo ./pulledpork.pl -c /etc/pulledpork/pulledpork.conf -l
```

Can be added to `cron` to update daily.

D. Check for loaded rules

```
sudo snort -T -c /etc/snort/snort.conf
```

Applications

- Edge protection in small networks.
- Access monitoring and control in campus networks.
- Integration with security policies (ACLs, CBAC, ZBF).
- Detection of known exploits and attacks (Snort).

Summary

IPS/IDS on a Cisco router is an effective, albeit limited, solution for detecting and preventing attacks. When combined with a tool such as **Snort** i **PulledPork**, the administrator gains the ability to implement up-to-date rules that detect the latest threats.