3. The Sensor Platform

The most important non-human component of the NSM is the Sensor.

> The sensor is a combination of hardware and software used to perform collection, detection and analysis.

A sensor might perform the following actions:

- Collection
- Collect PCAP
- Collect Netflow
- Generate PSTR Data from PCAP Data
- Generate Throughput Graphs from Netflow Data
- Detection
- Perform Signature-Based Detection
- Perform Anomaly-Based Detection
- Perform Reputation-Based Detection
- Use Canary Honeypots for Detection
- Detect Usage of Known-Bad PKI Credentials with a Custom Tool
- Detect PDF Files with Potentially Malicious Strings with a Custom Tool
- Analysis
- Provide Tools for Packet Analysis
- Provide Tools for Review of Snort Alerts
- Provide Tools for Netflow Analysis

NSM Data Types

Overview of the primary NSM data types that are collected for detection and analysis.

Full Packet Capture (FPC) Data

FPC data provides a full accounting for every data packet transmitted between two endpoints. The most common form of FPC data is `PCAP`.

Session Data

The summary of the communication between two network devices.

Statistical Data

The organization, analysis, interpretation, and presentation of other types of data.

Packet String (PSTR) Data

Is derived from FPC data, and exists as an intermediate data form between FPC data and session data.

Log Data

Raw log files generated from devices, systems, or applications.

Alert Data

When a detection tool locates an anomaly within any of the data it is configured to examine, the notification it generates is referred to as alert data.

Sensor Type

Collection-Only

A collection-only sensor simply logs collected data such as FPC and session data to disk.

Half-Cycle

Performs all of the functions of a collection-only sensor, with the addition of performing detection tasks. It logs data, and runs a NIDS, such as Snort, either in real time, or in near real time, from data stored in disk. When analysis must occur, data is pulled back to another device rather than the analysis being performed on the sensor itself. Most common sensor.

Full Cycle Detection

Collection, detection, and analysis are all performed on the sensor. Half cycle sensors are much preferred, and these are normally deployed in small companies. Half cycle sensors are much safer, because data is not managed directly from within the sensor.

Sensor Hardware

When deploying a sensor, server-grade hardware must be utilized.

To determine the characteristics of the hardware used, we can use a laptop, workstation, or spare server to perform the test.

Once the sensor has been placed on the network, you will utilize either a SPAN port or a network tap to get traffic to the device.

CPU

An easy way to begin planning for your sensor deployment is to map the number of cores required on the system to the tools being deployed.

Memory

Use a motherboard with additional memory slots, so that you can expand them later if needed.

Hard Disk Storage

Effectively planning for storage needs requires you to determine the placement of your sensor and the types of traffic you will be collecting and generating with the sensor.

Steps to calculate storage:

- *Step 1*: Calculate Traffic Collected
- *Step 2*: Determine a Feasible Retention Period for Each Data Type
- *Step 3*: Add Sensor Role Modifiers

Network Interfaces

The most important hardware component in the sensor, because the NIC (Network Interface Card) is responsible for collecting the data used for all three phases of the NSM Cycle.

A sensor should always have a minimum of two NICs. One NIC should be used for accessing the server, either for administration or analysis purposes. The other NIC should be dedicated to collection tasks.

In order to Gauge exactly what throughput you will need for your collection NIC, you should perform an assessment of the traffic you will be collecting.

The most important aggregate numbers are:

- Peak to Peak traffic (Measured in Mbps)
- Average bandwidth (throughput) per day (Measured in Mbps)

Traffic is bi-directional! A 1 Gbps connection has a maximum throughput of 2 Gbps - 1 Gbps TX and 1 Gbps RX.

Load Balancing: Socket Buffer Requirements

Traditional GNU/Linux network sockets are inefficient for network capture and analysis, so use `FP_Ring`, a tool that makes network flow stay in user space, instead of going from kernel to user space.

SPAN Ports vs. Network Taps

A SPAN port is the simplest way to get packets to your sensor because it utilizes preexisting hardware. A SPAN port is a function of an enterprise-level switch that allows you to mirror one or more physical switch ports to another port.

Use of a SPAN port to capture traffic.

A tap is a passive hardware device that is connected between two endpoints, and mirrors their traffic to another port designed for monitoring.

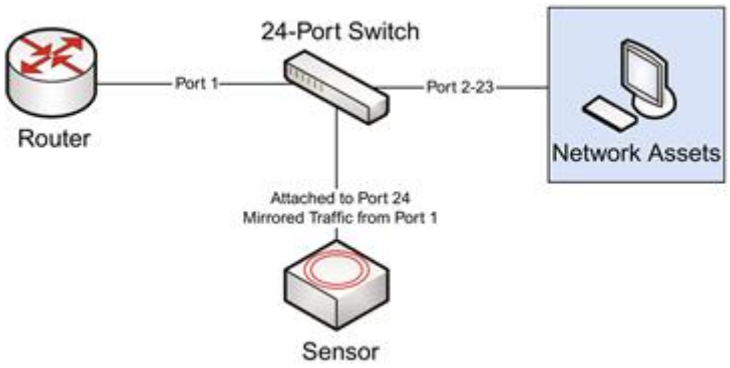

Figure 1: SPAN Port

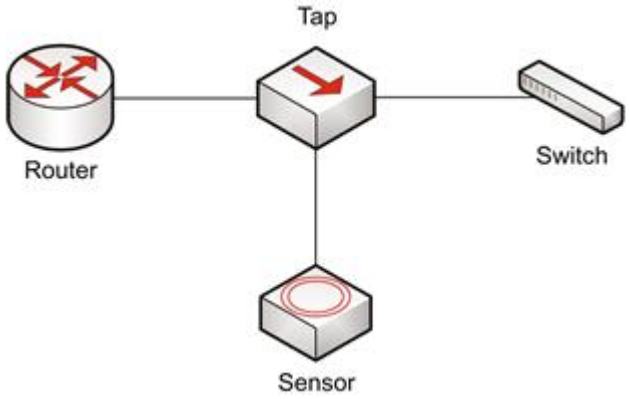

Figure 2: TAP

Bonding Interfaces

To make things easier, if you are monitoring two interfaces with the same sensor, bond them together to create a virtual interface. This way, both logs will be merged, and the information gathering process will be easier.

Sensor Operating System

While the particular flavor you choose may not matter, it is very important that you use something `*nix` based. There are a variety of reasons for this, but the most prevalent is that most of the tools designed for collection, detection, and analysis are built to work specifically on these platforms

Sensor Placement

This placement determines what data you will be able to capture, what detection ability you will have in relation to that data, and the extent of your analysis.

Utilize the proper resources

Speak with the networking department to find out the best location of the sensor. If there is no network diagram, create one.

Network Ingress/Egress Points

In the ideal case, and when the appropriate resources are available, a sensor should be placed at each distinct ingress/egress point into the network including Internet gateways, traditional VPNs, and partner links.

In the network diagram, there are sensors at each ingress/egress point.

1. At the corporate network edge
2. At the research network edge
3. At the ingress point from a business partner network
4. At the edge of the wireless network

Any malicious activity occurring in the network will communicate with the external network. If you are monitoring every place at which this may happen, you are assured to intercept the packet.

Visibility of Internal IP Addresses

It is critical that your collected data serves an analytic purpose. Always ensure you are on the right side of the routing device.

On scenario A, the sensor will only see the external IP of the internal router, because it masks it's internal devices IP. In scenario B, as the sensor is inside the internal router, it will be able to identify what specific device the exploit is being executed on.

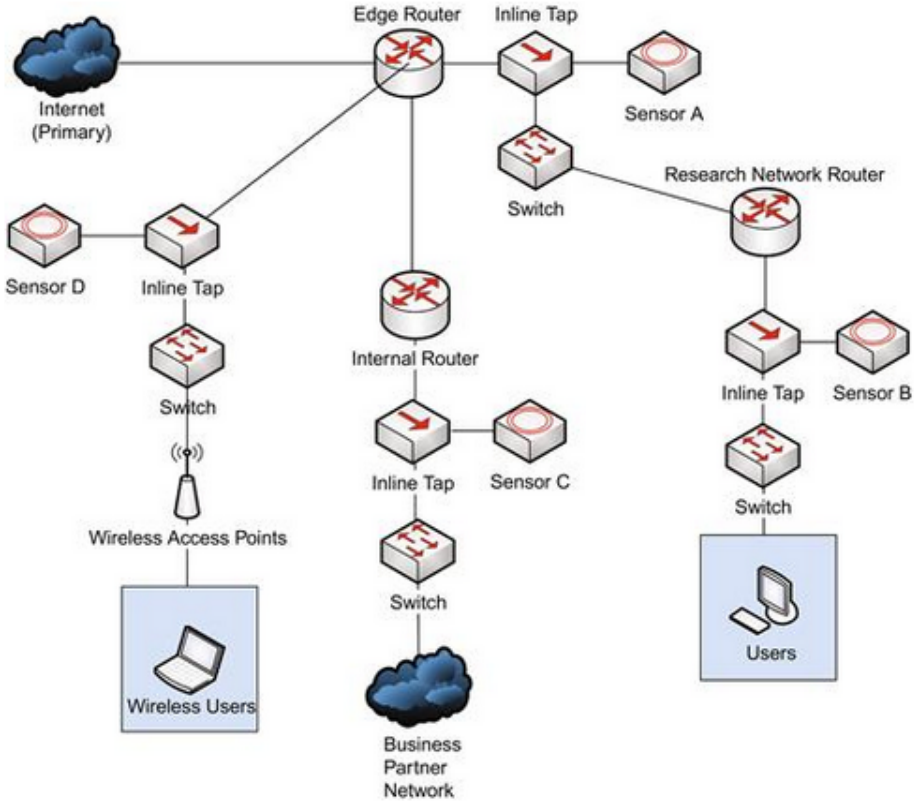

Figure 3: Network Ingress/Egress Points

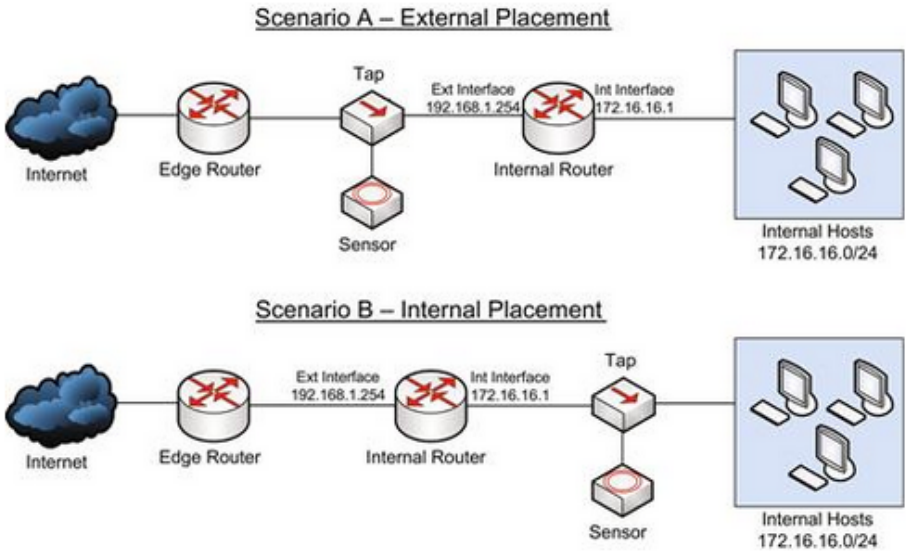

Figure 4: Scenarios

Proximity to Critical Assets

If you have budget limitations, you have to monitor from the most critical devices outwards. Ensuring these critical devices are being monitored.

Creating Sensor Visibility Diagrams

The ultimate goal of the sensor visibility diagram is for an analyst to be able to quickly assess what assets a particular sensor protects, and what assets fall out of that scope.

A basic network visibility diagram should contain at least these components.

- High-level logical view of the network
- All routing devices, proxies, or gateways that affect the flow of traffic.
- External/Internal IP addresses of routing devices, proxies, and gateways.
- Workstations, servers or other devices – these should be displayed in groupings and not individually, unless they are particularly critical devices
- IP address ranges for workstation, server, and device groupings
- All NSM sensors, and appropriately placed boxes/areas that define the hosts the sensor is responsible for protecting.

Securing the Sensor

The sensor contains a lot of very sensitive information, that is stored in packet captures, and network statistics. It's security should be paramount.

Operating System and Software Updates

Ensure regular updates to the OS. If the sensor is not connected to the Internet, configure a satellite server for it to download the updates from.

Operating System Hardening

Configure your sensor to meet hardening standards such as:

- Center of Internet Security (CIS) standard
- NSA Security Guide for Operating Systems
- HIPPA
- NERC

Limit Internet Access

Normally, sensors shouldn't have Internet access. When the sensor has to download malware signatures, configure it to point to a external server of your control to obtain it's updates.

Minimal Software Installation

Only necessary software be installed on the sensor. Use a minimal OS and install only the required hardware to perform the necessary tasks.

Under no circumstances should the compiler be left on this system, as it provides an additional tool for an attacker to use against your network should the sensor be compromised. Instead, compile the sensor in another computer and push the compiled sensor to the machine.

VLAN Segmentation

Most sensors should have at least two network connections. The first interface is used for the collection of network data, while the second will be used for the administration of the sensor, typically via SSH

Host-Based IDS

It is necessary to install some form of host-based intrusion detection system (HIDS)

Free HIDS:

- OSSEC
- AIDE

The HIDS software should send logs to another computer on the network, as if the sensor is compromised, these logs can be deleted, and the administrator never find out the sensor has been compromised.

Two-Factor Authentication

Important to secure the sensor, as if it's compromised, further attack orchestration can be carried out.

Network-Based IDS

Subject the sensor to the same NIDS detection used for the rest of the network.

Mirror the administration interface's network traffic to the monitoring interface.

Create a Snort rule that alert if the sensor communicates with devices that it is not allowed to.