Chapter 1 - The practice of Applied Network Security Monitoring

The main focus areas of Information Security are:

- *Protect*: Securing the system to prevent exploitation and intrusion from occurring.
- *Detect:* Detecting compromises that are actively occurring or have previously occurred.
- *Respond:* Response after the compromise has occurred.
- *Sustain:* Management of people, processes and technology associated with the CND (Computer Network Defense).

Key NSM Terms

- *Asset:* Anything within your organization that has value
- *Threat:* A party with the capabilities and intentions to exploit a vulnerability in an asset.
  - *Structured threat*: Utilizes formal tactics and procedures and has clearly defined objectives
  - *Unstructured threat:* Lacks the motivation, skill, strategy, or experience of a structured threat.
- *Vulnerability:* Software, Hardware, or procedural weakness that may provide an attacker the ability to gain unauthorized access to a network asset.
- *Exploit:* Method by which a vulnerability is attacked.
- *Risk:* The possibility that a threat will exploit a vulnerability.
- *Anomaly:* Observable occurrence in a system or network that is considered out of the ordinary.
- *Incident:* A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Intrusion detection

- Is a component of modern NSM.
- It had a set of similar characteristics:
  - *Vulnerability-centric defense*
  - *Detection in favor of collection*
  - *Mostly Signature-based*
  - *Attempts to Fully Automate Analysis*

Network Security Monitoring

The majority of NSM is dedicated to Detect in an effort to better Respond. On occasions, this may include elements of other areas, like deception or degradation (Honeypots)

Characteristics

- *Prevention eventually fails:* Eventually, a motivated hacker will find the way to get in. Shifting the mindset to be prepared for detection and response once the hacker has entered is the best way to respond to threats.
- *Focus on collection:* But collect only necessary data, as otherwise, the analyst will have data overload and won't be able to perform correct decisions. Also, the system won't scale properly if too many data is collected.
- *Cyclical Process:* collection should feed detection, detection should feed analysis, and analysis should feed back into collection.
- *Threat-centric defense:* Focus on the "Who" and "Why", to be able to infer what is going to be attacked.

Vulnerability-centric vs. Threat-centric defense

Vulnerability-centric	Threat-centric
Relies on prevention	Knows that prevention eventually fails
Focus on detection	Focus on collection
Assumes universal view of all threats	Knows that threats use different tools, tactics, and procedures
Analyzes every attack in a vacuum	Combines intelligence from every attack
Heavy reliance on signature-based detection	Utilizes all-source data
Minimal ability to detect unknown threats	Stronger ability to detect adversarial activities beyond known signatures
Linear process	Cyclical process

The NSM Cycle: Collection, Detection, and Analysis

Collection

Collection occurs with a combination of hardware and software that are used to generate, organize, and store data for NSM detection and analysis. The most common categories of NSM data include Full Content Data, Session Data, Statistical Data, Packet String Data, and Alert Data.

Common Collection Tasks:

- Defining where the largest amount of risk exists in the organization
- Identifying threats to organizational goals
- Identifying relevant data sources

- Refining collection portions of data sources
- Configuring SPAN ports to collect packet data
- Building SAN storage for log retention
- Configuring data collection hardware and software

Detection

Detection is the process by which collected data is examined and alerts are generated based upon observed events and data that are unexpected. This results in the generation of alert data. There are two main sub-genres, Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS)

Analysis

It occurs when a human interprets and investigates alert data.

There are multiple ways the analysis can be performed:

- Packet analysis
- Network forensics
- Host forensics
- Malware analysis

Challenges to NSM

- No standardization
- No Professional talent
- Costly

Defining the Analyst

The Analyst determines whether the alert is a false positive or requires further investigation.

Critical skills

Baseline skills (All of them required for a decent NSM analyst)

- Threat-centric Security, NSM, and the NSM Cycle
- TCP/IP Protocols
- Common Application Layer Protocols
- Packet Analysis
- Windows Architecture
- Linux Architecture
- Basic Data Parsing (BASH, Grep, SED, AWK, etc)
- IDS Usage (Snort, Suricata)
- Indicators of compromise and IDS Signature Tuning
- Open Source Intelligence Gathering

- Basic Analytic Diagnostic Method
- Basic Malware Analysis

Specializations (At least one, 3 perfect)

- *Offensive tactics:* Penetration testing and security assessments.
- *Defensive tactics:* Requires conceptualizing new development tools and analytic methods.
- *Programming:* BASH, Python, Java, C/C++
- *System Administration:* Involved in the collection process and moving data around for it to be ingested.
- *Malware Analysis:* Static and Dynamic malware analysis
- *Host-Based Forensics:* Gain information on a compromised host (File system forensics, memory forensics, incident timeline creation)

Classifying Analysts

Level 1 (L1) Analyst

- Possesses a reasonable grasp on several of the baseline skills listed previously, but will likely not have settled into any particular specialization.
- Reviews IDS alerts and performs analysis based upon their findings
- Most analysts fall in this classification

Level 2 (L2) Analyst

- Solid grasp on the majority of the baseline skills
- Selected specialization
- Mentor to L1

Level 3 (L3) Analyst

- Most senior
- Adept at all baselines and at least one specialty.
- No more analysis, but train other analysts.

Measuring Success

- should not measure the effectiveness of an NSM program by whether a compromise occurs, but rather, how effectively it is detected, analyzed, and escalated.
- Invest and empower the analysts.

Create a culture of learning

- NSM thrives on ingenuity and innovation, which are the products of motivation and education.

- Mantra: In every action an analyst takes, they should either be teaching or learning. No exceptions.

Emphasize teamwork Analysts who trust each other and genuinely enjoy spending time together are going to be much more effective at ensuring the incident is handled properly.

Provide Formalized Opportunities For Professional Growth Invest in Professional development, you are likely to keep your staff if you can provide opportunities for professional certifications, advancements in position, or migrations to management roles.

Encourage Superstars Challenge, provide opportunities, and instill responsibilities in them so that they feel empowered and feed their large ego.

Reward Success Let them know they are appreciated, and that they have made a difference.

Learn From Failures Do post-threat mitigation analysis, and maintain a positive environment.

Exercise Servant Leadership Servant leaders achieve results by giving priority to the needs of their colleagues.