Network security monitoring essay

Law, Security

Emergency Network Security Monitoring

This refers to the collection, analysis, of indications and warnings to detect and respond to intrusions in a computer network during a crisis. All computer networks have vulnerabilities that both external and internal intruders are likely to attack. The threats may come over wired or wireless networks.

Network Security Monitoring uses indicators to detect threats to an organization’s security. Indicators are activities that show the intruder's intentions. Intrusion Detections Systems compile the indicators and forward them to an analyst. The analyst interprets the information, and if need be, gives a warning to the supervisor for corrective decision-making.

Decision makers use the information from the analysts to form a response. The response depends on the extent of the intrusion, the duration and timing of the intrusion, and the data accessed during the intrusion. The response should include shutting down the means of access the intruder used to access the system.

Evaluation Managed Security Monitoring Providers

Many service providers provide managed security monitoring services to network owners at a fee. The monitoring involves a day-to-day supervision of the network to detect intrusions and other malicious activities. Discussed below are several managed security-monitoring providers.

Symantec is a company based in Mountain View. Founded in 1982, it provides systems management, storage and security facilities to individuals and organizations. Concerning security monitoring, it provides real time monitoring in networks, applications and the endpoints. Symantec also offers intrusion prevention services on the endpoint, network and host. It offers predictable pricing that depends on the size of the enterprise and not the size and complexity of the network. It also prioritizes alerts so that decision makers can react suitably to the most dangerous threats.

Solutionary is a company that provides all day managed security services all over the globe. It uses a technology called Active Guard to monitor databases, networks, applications, and endpoints and produces a log file on demand or after a certain period. Solutionary also provides cloud-monitoring services.

Deploying an in-house NSM Solution

The first step in creating a customized NSM solution is to install firewalls to scan incoming and outgoing packets and filter out all the harmful data not blocked by the internet service provider. The analysts then install the sensors on the hubs to collect information about the traffic. Sensors also go to the proxy server to inspect information from the web and potentially recognize intruder’s data packets.

DMZ (Demilitarized Zone) switch is a security feature that separates the outside internet and the internal Local Area Network. The security analysts place a sensor on the SPAN port of the DMZ switch to scan incoming and outgoing traffic. To scan for traffic on the wireless networks, it is crucial to install sensors on the NIC cards and a firewall between the Wireless Access Point and the Internal Switch.

When an organization installs an in-house NSM solution, there is always the danger that a person will scan for unauthorized information leading to loss of customers' trust. For this reason, individuals should not act alone on the collected information. Instead, teams of analysts work to examine the collected information. This reduces the chances of an individual using collected information for personal gains.

Analyst Training Programs

- Weapon and tactics

In this program, the analyst studies the tools and techniques that attackers use to compromise a computer network, called offensive tools. The analyst also gains knowledge of the defensive tools that used in preventing, detecting, and reacting to intrusions. There exist many hacking tools available free on the internet used to gain access to a forbidden network and compromise its security. To prepare against these, the analyst should download these tools and perform test attacks in a controlled environment. They should learn how the intruder performs each phase of the attack. This should help them create suitable defenses to combat the offensive tools. These tools include Nemesis, Xprobe, Ettercap, among others.

The analysts should also download and learn how to use the freely available defensive tools in protecting their network against unwanted intrusion. These tools include Snort and Ethereal.

- Telecommunications

Telecommunications refers to communication over a distance. Analysts have to know how data packets move from one computer to another. They should understand the operations of the TCP /IP standard. They should also be capable of identifying the main types of packets, normal, suspicious and malicious. Analysts should also be able to create and troubleshoot a LAN network.

- System Administration

This is the operation and maintenance of computer systems. The analyst completely understands the organization's system in order to differentiate between normal and suspicious traffic. The analysts should focus on using as many operating systems as possible and learn how to use many applications in them. This gives them experience in the workings of the target system.

- Scripting and Programming

This deals with the ability to code instructions for the computer to execute towards a certain output. A person who can program is able to create customized tools to defend against a new offensive tool.

- Management and policy

These deals with the non-technical parts of security. The analyst should have up-to date training on legal constraints about the kind of data collected and stored by an organization. They also should understand the general business of the organization who's Network they are monitoring. This will enable them to recognize things that are out of the ordinary. The analysts should be capable of advising the top management of security issues.

References

Bejtlich, R. (2004). The Tao of Network Security Monitoring Beyond Intrusion Detection. Boston: Addison Wesley.

Spitzner, L. (2002). Honeypots: Tracking Hackers. Boston: Addison-Wesley.

Thomas A. Limoncelli, Limoncelli, T. A., & Hogan, C. (2001). The Practice of System and Network Administration. Boston: Addison-Wesley.