Vulnerability scanning data

An effective way to find security holes is to examine infrastructure from the attacker’s point of view. Vulnerability scans probe an organization’s network for known software defects that provide entry points for external agents. Systems often keep network services running by default, even when they aren’t required for a particular server. These running, unmonitored services are a common means of external attack, as they may not be patched with the latest OS security updates.

Broadscale vulnerability scans can reveal security holes that could be leveraged to access an entire enterprise network. They show data about open ports and IP addresses that can be used by malicious agents to gain entry to a particular system or entire network. In the Common Information Model, vulnerability scanning data is typically mapped to the Vulnerabilities data model.

Application

When your Splunk deployment is ingesting vulnerability scanning data, you can use it to accomplish security and compliance use cases, such as the following:

- Monitoring NIST SP 800-53 rev5 control families
- Detecting Supernova web shell malware
- Reconstructing a website defacement

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with vulnerability scanning data.

- Tripwire IP360 Add-on for Splunk