Whisper

Whisper is a intrusion detection system that uses signature based detection to determine known attacks on a system, anomaly based detection to determine unknown attacks on the system, and IP address blacklisting detection to determine unknown IP addresses that have visited the system.

How Whisper works

Whisper will work in three aspects;

- IP address blacklisting
  - Whisper has the ability to parse IP addresses outside of the known IP range of the network and will check each IP address against multiple blacklists to determine if the provided IP address is "bad" or "good". If a "bad" IP address is determined it will be blocked by the host and logged into a database for future analysis. This will work in the following aspect:
    - Know range is 10.0.1.1-10.0.1.255
    - IP address 198.56.78.23 vists 10.0.1.56
    - Whisper detects visited IP address and performs blacklisting check leveraging ipvoid
    - IP address is detected as 5/12 blacklists
    - Whisper bans the IP address and continues
- Signature based detection
  - Whisper has the ability to detect malicious attempts against a database of known malware signatures, if a signature is seen on the system Whisper will determine the system as "compromised" send and alert to the IT team, boot the user off the network, and shutdown the system. How this will work is as follows:
    - Whisper scans local computer TA678945 for known malware signatures
    - Signature 17ed9e156874afe00c127419e2d5dea7 is detected on the system
    - Whisper verifies that the detection is not a false positive
    - Whisper alerts the user with a notification, sends an alert to the IT team, boots the system off the network, and shuts down the system for further analysis
- Anomaly based detection
  - Whisper will be trained to determine the usual routine of a system, if the routine does not go as normally detected, Whisper will run both an IP address check and a signature based check to determine if there is a false positive, otherwise it will alert the user, boot them off the network, and shut down the system. How this will work:
    - Whisper has a given model of the basic understanding of the daily routine of the system

- Whisper detects that daily the user visits 67 websites and uses Photoshop for 6 hours between 8-5pm, Monday through Friday and once every other week on Sunday
- On Saturday at 3:56am Whisper detects a user login and file access
- A verification that nobody is on that system is sent to the IT team
- If the verification is not responded to in 30 minutes, or is responded to with a keyword (like "no") Whisper will cut the network connection to the system and shutdown the computer