Vision Statement

Team Name: MAN^2

Project Sponsor: NAVAIR-PIPELINES

Project Name: NOMADS

Members:

Nick Arenberg - narenberg@ucsb.edu (Team Lead)
Nick Mattair - nmattair@ucsb.edu (Scribe)
Andy Ho - andyho@ucsb.edu
Matthew Chen - matthewchen@ucsb.edu
Max Medearis - m_medearis@ucsb.edu

Background

The Problem

Cybersecurity is more important than ever. With the frequency of cyberattacks increasing, it is necessary to ensure that networks that are thought to be secure have no leakage. Even if network transmissions are secure, attacks could be siphoning vital data through faulty software or hardware on an endpoint. However, manually gathering information on every endpoint device on a network is time-consuming and expensive. It wastes valuable security resources. Plus, if a security audit misses a threat, it would either exist for adversaries to exploit or require another expensive audit to root out. In short, human security teams are too slow and unreliable to perform detailed security audits of large networks. Human teams are valuable for analysis and response, so using them for that purpose is highly inefficient. Some automated solutions exist for detecting some of these vulnerabilities. However, existing solutions like Red Seal don't quite meet the specifications required by the Navy.

Why is this important?

The need for a low-cost, quick, and accurate security audit application is clear. In this increasingly online and interconnected world, and with the rise of the Internet of Things, being able to spot and shut down potential security threats is vital. Especially when it comes to matters of security and national defense, like those that would be handled on Navy networks. Instead of dedicating valuable manpower to manually check every endpoint, a software that could automate the process would not only increase security, but allow for the allocation of resources to other, more pressing areas.

Existing Solutions

Red Seal

https://www.redseal.net/#home

Endpoint Detection and Response (EDR) Platforms

https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compared/
https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

Palo Alto Networks Cortex XDR

https://www.paloaltonetworks.com/cortex/endpoint-protection

Each of the above options does its own version of endpoint detection and response. Generally, that includes constant monitoring of endpoint devices, alert triage, incident response capabilities, and data analytics to identify threats.

Project Goals

Outcome

With this project, we will create an application that continuously monitors a network to determine the hardware and software installed on each endpoint. This data will be checked against a ledger of known software to locate any irregularities or issues. It will be presented to users in an easily consumed manner. Users will be able to see a network graph and view reports from potential threats with detailed information on each specific endpoint and their flagged activities.

Milestones

1. Identify all endpoints on network
2. Determine hardware and software on each machine
3. Check against approved software database/if any software is out of data
4. Continuously monitor/React to changes
5. Visualize network graph
6. Visualize alerts/irregularities
7. Generate comprehensive report

Implementation Technologies

- Python

    - Some GUI framework (PyQt, Tkinter, etc.)
        - https://towardsdatascience.com/top-10-python-gui-frameworks-for-developers-adca32fbe6fc
    - Network graphing libraries: NetworkX and/or PyVis
- Electron might be a nice(r) way to make a GUI
    - https://www.electronjs.org