NOMADS

Navy Operational Machine Auditing Development Suite
Team MAN^2

Nick Arenberg  Matthew Chen  Andy Ho  Nick Mattair  Max Medearis

Mentors: Mike Cloud, Kevin Burk
Project Background

The Problem

- Cybercrime presents a clear danger to any organization
- Leaky networks can cause a lot of damage if they are exploited
- Large organizations need automation to cover all devices
- Human security teams are better utilized for analysis than data collection
Project Background

Issues with Existing Solutions

- Many, many endpoint detection and response tools
- What is the problem?
  - Expensive
  - Non-specialized
  - Time-intensive
  - Large footprint
  - Third-party
- Manual data collection is too slow
NOMADS

An automated, low-cost, small-footprint network auditor and visualizer.
How it Works (FP2)

Fetch
- Collect Data From Hosts
  - Host Discovery Scan
  - Network Audit

Process
- Create Insights, Find Liabilities
  - Approved Program Search
  - Neighbor Graph Generation

Present
- Share Insights with Ease
  - Interactive Network Topology Diagram
  - Visual Network Summary
Project Technologies

Fetch, Process
- Ansible/ansible-runner
- **Nmap**, Ncat, Paramiko
- Windows Remote Management
- Python

Present
- Flask
- Microsoft Visio
- Vis.js
- Vue
Demo
Conclusion

NOMADS Benefits

- Expedites process of manually compiling hardware and software lists for large networks
- Notifies administrators of questionable programs and computers
- Provides multiple visualization methods for report generation and easy understanding of issues
- Exports into numerous formats
- Fast, cheap, scalable, and easy
Conclusion

Applications of NOMADS

● Naval Air Warfare Center Weapons Division (NAWCWD)
● Naval Surface Warfare Center

Future Work

● Advanced software filtering features
● Continuous network monitoring
● Increased diagrams customizability
Special Thanks

NAVAIR
- Mike Cloud
- Kevin Burk
- Angelique Zamarron
- Doug Bradley

UCSB
- Chandra Krintz
- Jianwen Su
- Mason Corey

Any Questions?