Metrics Suite for Enterprise-Level Attack Graph Analysis

Homeland Security
Science and Technology

Cyber Security Division
2012 Principal Investigators' Meeting

October 11, 2012

Sushil Jajodia (PI), Steven Noel (co-PI)
Metrics Suite for Enterprise-Level Attack Graph Analysis
Center for Secure Information Systems, George Mason University
[jajodia, snoel]@gmu.edu
703-993-2029

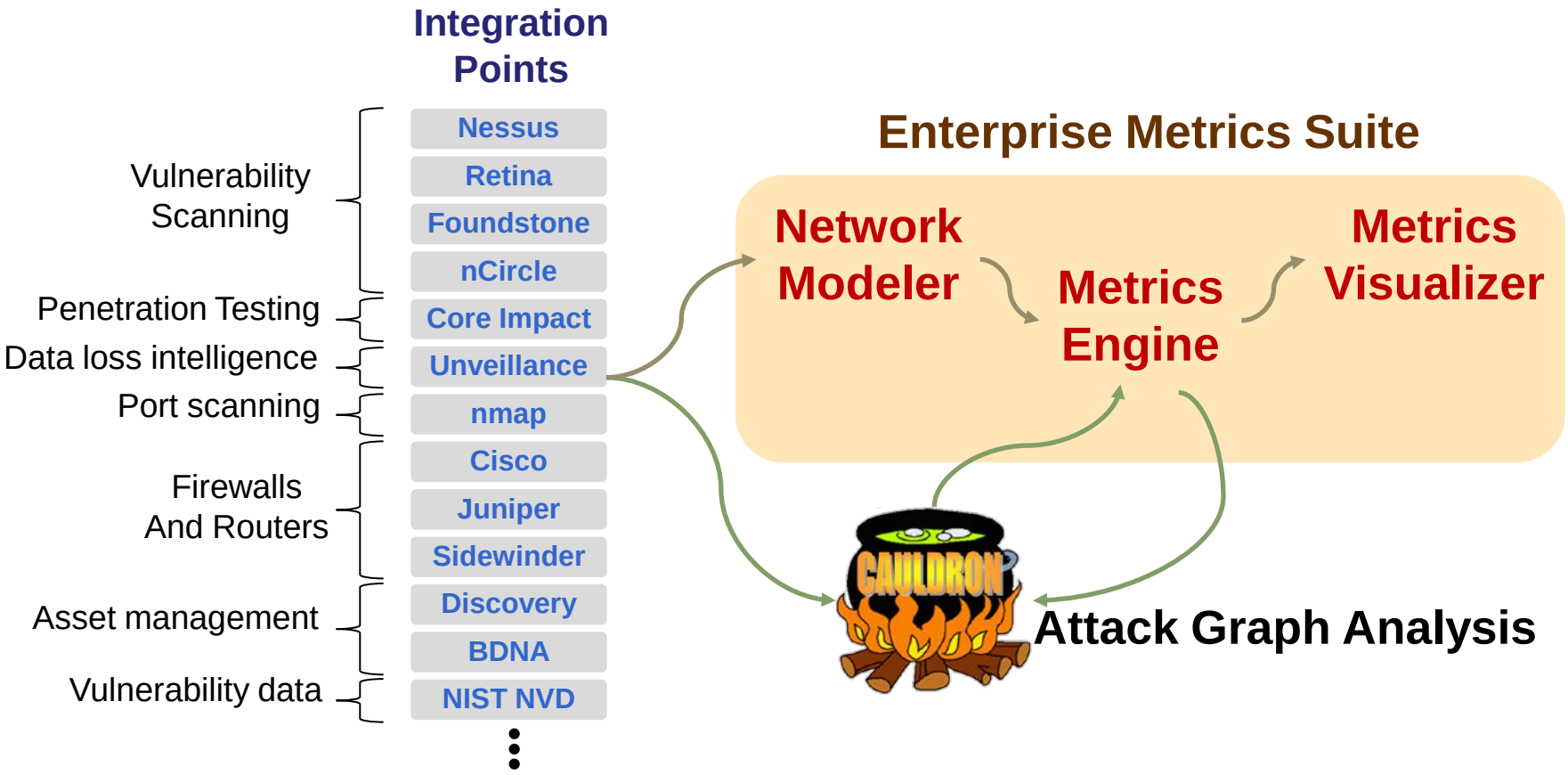
Introduction

- TTA #2 (Enterprise-Level Security Metrics), Type III
- GMU Center for Secure Information Systems
  - Top national research and academic security center
  - 10+ years developing TVA technology
  - 20+ TVA-related publications, 700+ citations
  - 5 TVA-related patents, others pending
- Applied Visions, Inc.
  - Experts in data visualization
  - Interactive visualizations of attack graph metrics
- ProInfo, Inc.
  - Lead commercialization efforts in Cauldron
  - Strategic vision for Cauldron rollout
  - Support customer engagements

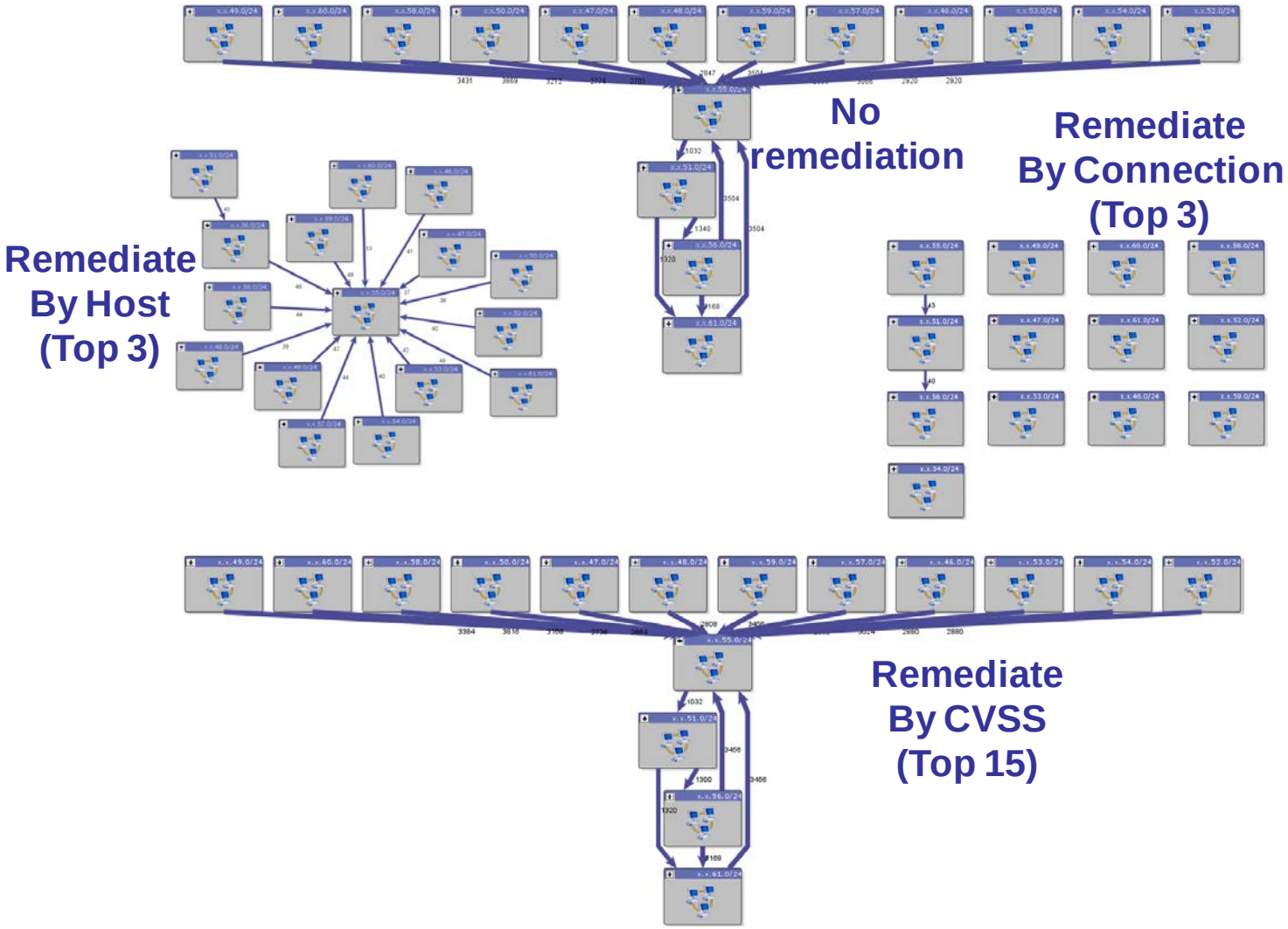
Project Goals

- Suite of metrics for measuring enterprise cyber security risk
- Based on multi-step attack vulnerability throughout the network
- Complementary metrics for measuring different aspects of enterprise security
- Based on applicable standards (CVE, CVSS, etc.)
- Interactive visualizations showing how security evolves over time
- Integration with Cauldron attack graph tool

System Architecture



Motivating Example



Challenges

- Understand impact of combined vulnerabilities and policies on security posture
  - Prioritize critical problems
  - Compare options for risk mitigation
  - Measure improvement or degradation of security over time
- Build comprehensive and accurate models of networks, vulnerabilities, and risk factors
- Apply meaningful metrics that inform decisions in complex environments

Metrics Capabilities

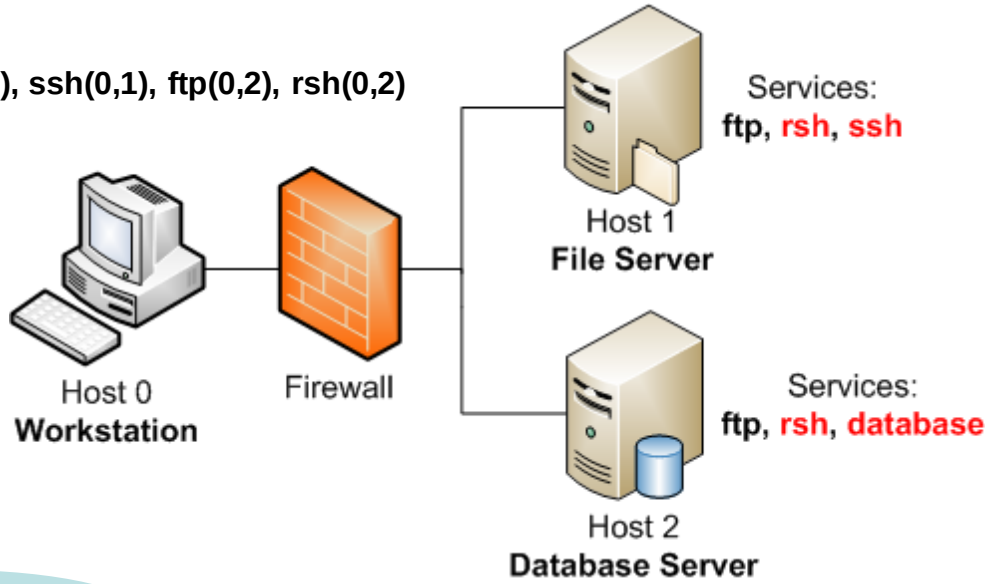
- Isolated network data and events
  - Hosts, vulnerabilities, firewall rules, IDS events, etc. without context
- Attack graph elements
  - Isolated data correlated and placed in context of layered defenses
- Attack graph logic and structure
  - Impact of threats throughout network, how likely an attack will succeed
- Attack graph predictive analysis
  - What-if scenarios, zero-day vulnerabilities

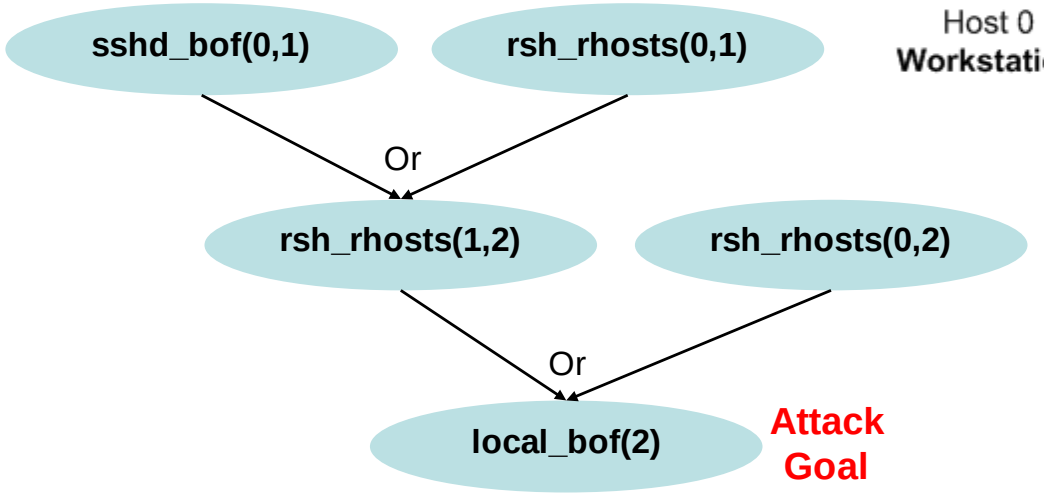
Sample Metrics

- *Vulnerability-Exploitability-Attackability*
  - Measures host vulnerability, exploitation likelihood, and ratio of actual to potential number of attack paths
  - Attack graphs as collections of single-step attacks
- *Attack Likelihood*
  - How likely an attack scenario will succeed
  - Overall attack risk based on attack graph logical relationships
- *CVSS Interdependency*
  - Analyzes interdependencies of CVSS base metrics for vulnerabilities
  - In context of attack path sequences
- *k-Zero-Day Safety*
  - Ability of network to survive exploitation of zero-day vulnerabilities
  - Favors layered attack defenses and heterogeneous platforms

Small Example

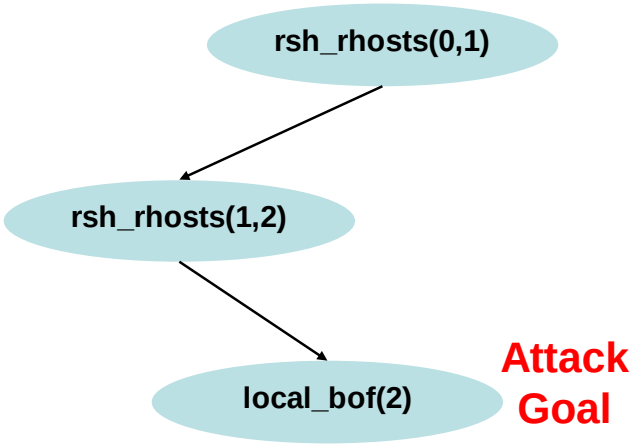
Firewall Policy
- **Allow ftp(0,1), rsh(0,1), ssh(0,1), ftp(0,2), rsh(0,2)**
- **Deny all other**



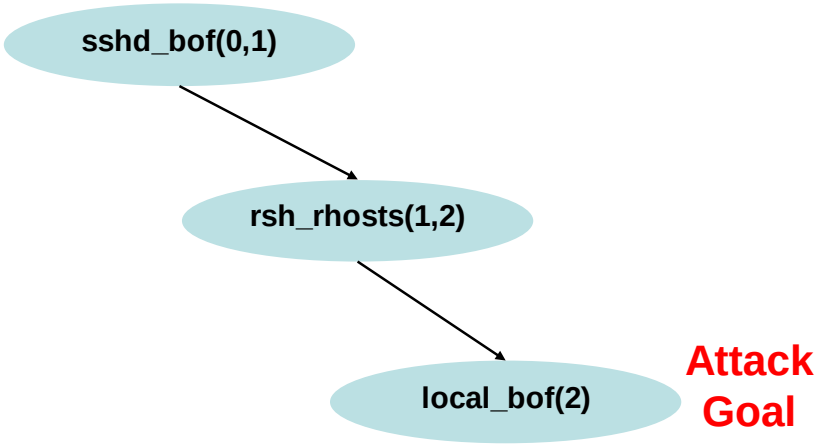


Options to Compare

Option 1: block ssh(0,1) and rsh(0,2) in firewall



Option 2: block rsh(0,1) and rsh(0,2) in firewall

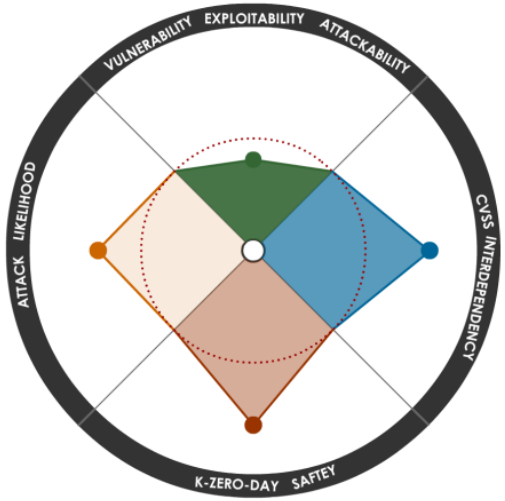


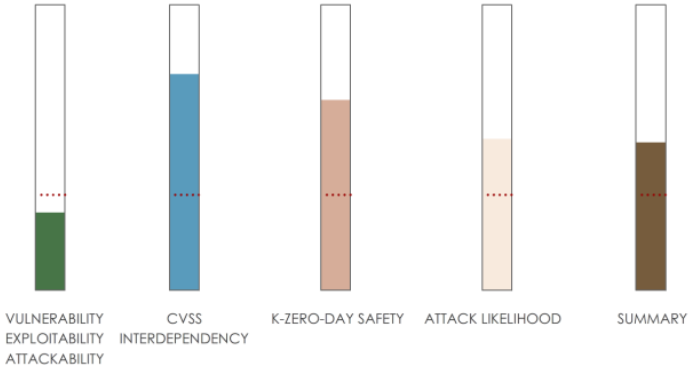
Option 3: Patch vulnerabilities, no change to firewall
Option 4: Patch vulnerabilities, change firewall per Option 1
Option 5: Patch vulnerabilities, change firewall per Option 2

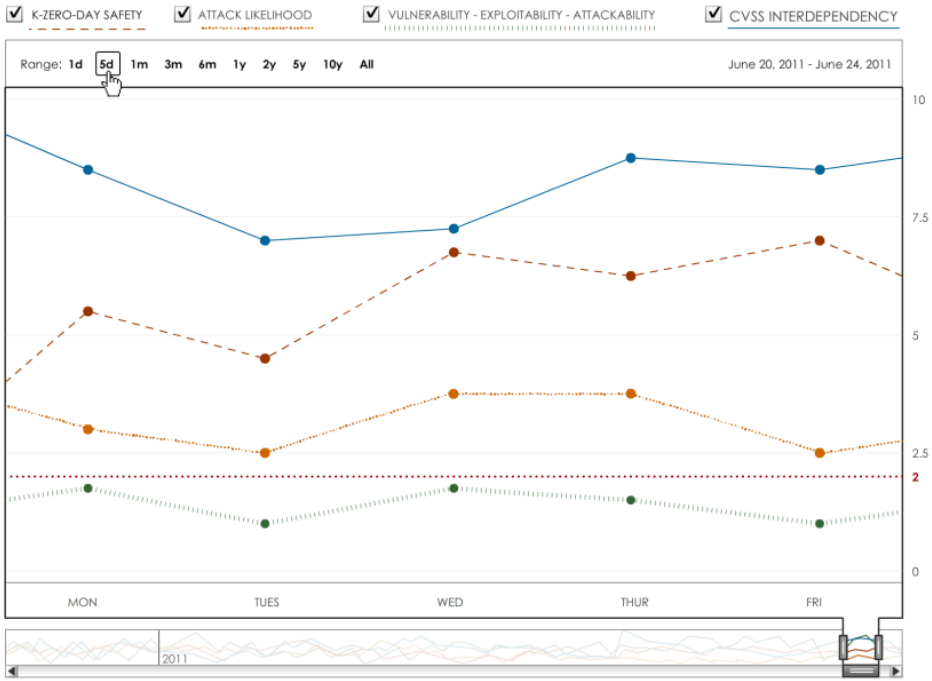
Comparison Results

Network Configuration	VEA	Attack Likelihood	CVSS Interdependency	*k* Zero Day
Initial	8.70	4.60	7.64	10
Option 1	8.23	4.37	7.27	10
Option 2	8.36	3.45	5.74	10
Option 3 (Initial patched)	0.0	0.0	0.0	5
Option 4 (Option 1 patched)	0.0	0.0	0.0	5
Option 5 (Option 2 patched)	0.0	0.0	0.0	3.33
Initial / Option 2	1.04	1.3	1.3	1

Metrics Visualization



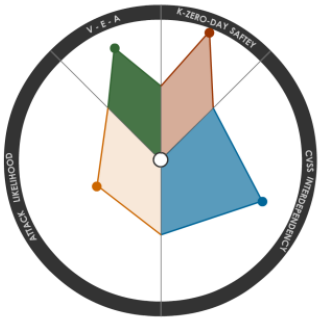




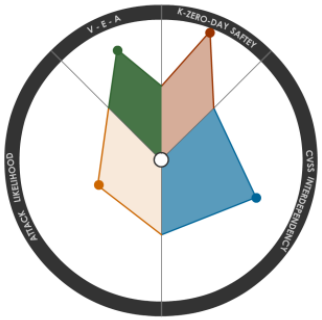
Visually Comparing Options

Homeland Security
Science and Technology

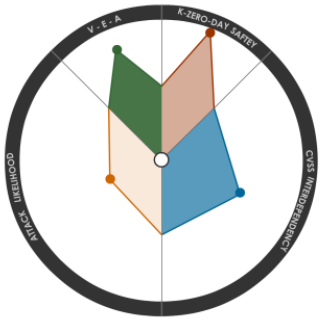
Initial



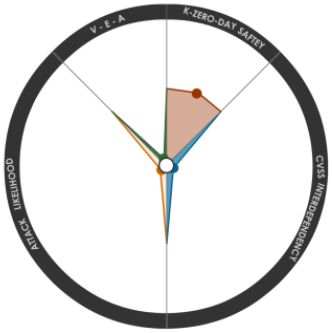
Option 1



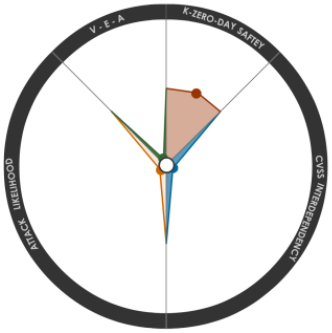
Option 2



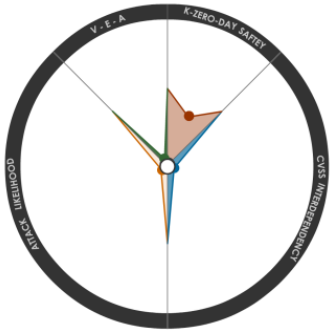
Option 3



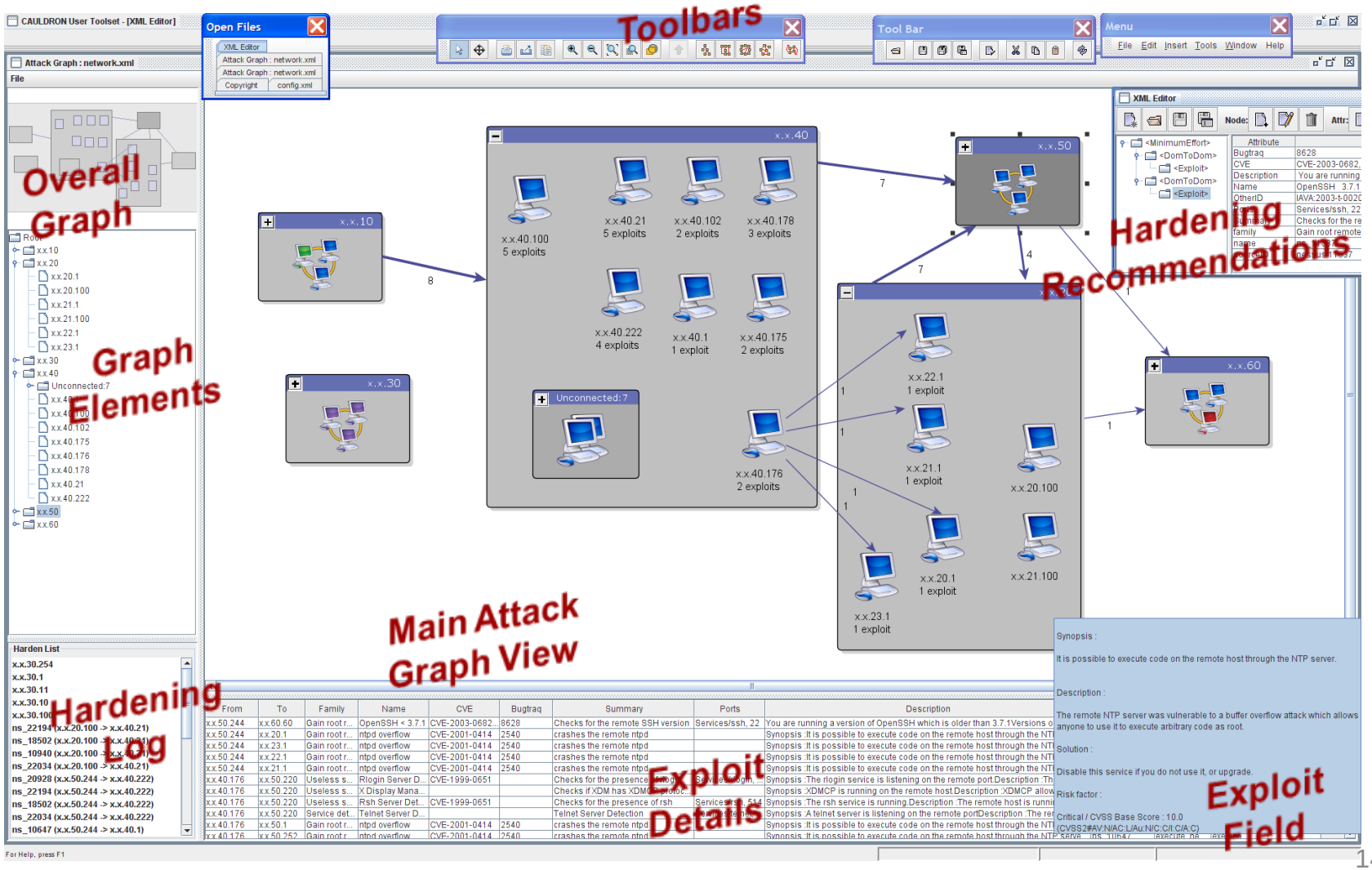
Option 4



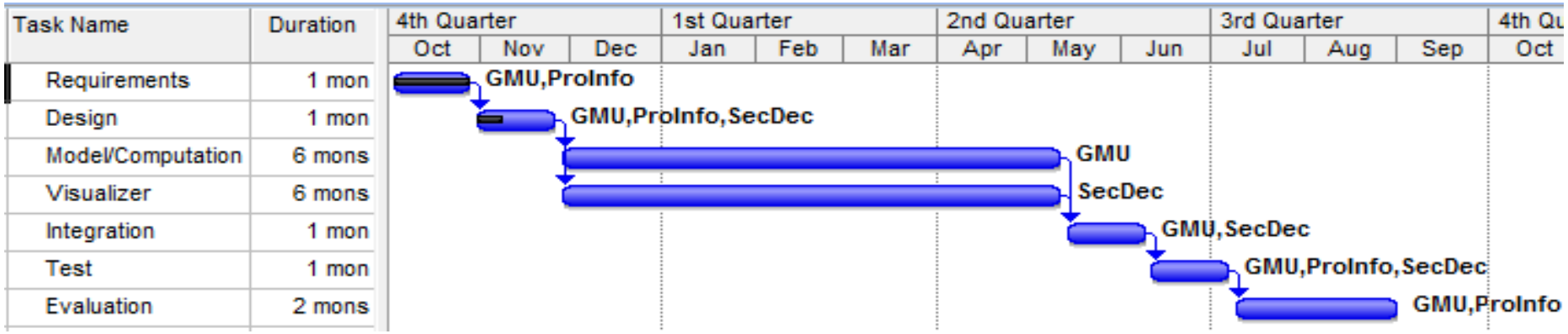
Option 5



Cauldron Dashboard



Schedule and Deliverables

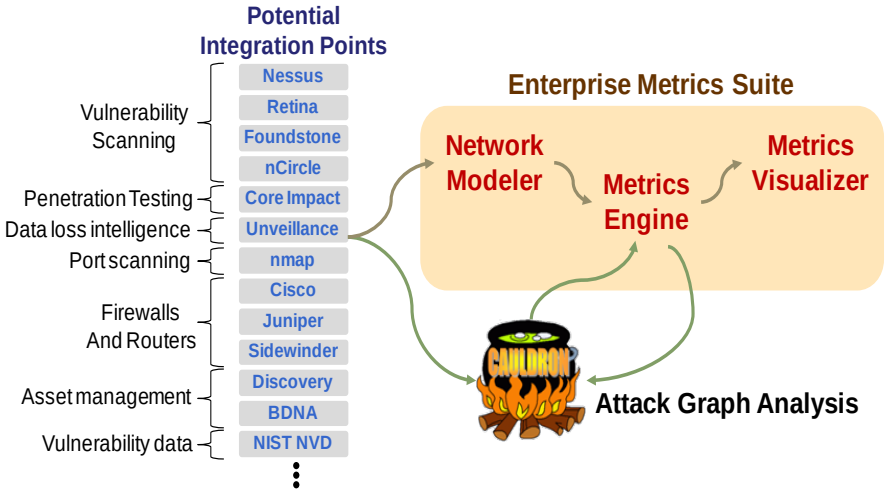


- Project Reviews (kickoff, mid-year, end of year), interim meetings via video/telephone/web
- Software implementation and associated documentation
- Monthly status reports
- Final Report (requirements, design, interfaces, test results, lessons learned, etc.)

Transition Plan

- Cauldron commercialization through Mason Tech Transfer (GMIP) and ProInfo/CyVision partnership
- Cauldron deployed in a variety of customer settings
- Significant IP, protected by patents and copyrights
- Available under GSA scheduling
- Marketing through direct sales and a network of resellers, strategic partners, and OEM relationships
- Strategic partners for services and complementary technologies
- Strategy: Identify early adopters for new metrics capabilities combined with Cauldron, delivering mission-critical requirements for situational awareness, common operating picture, and visualization

Metrics Suite for Enterprise-Level Attack Graph Analysis



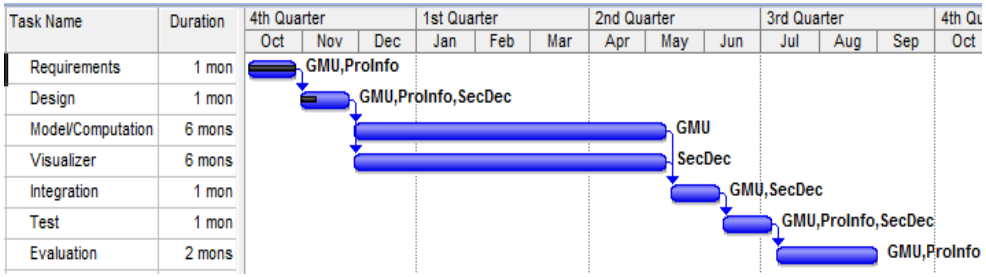
OPERATIONAL CAPABILITY

- Suite of metrics for enterprise network security risks.
- Based on network-wide model of multi-step attack vulnerability.
- Complementary metrics for measuring different aspects of enterprise security.
- Integrates seamlessly with Cauldron attack graph tool.

TECHNICAL APPROACH

- Model network attack vulnerability, populate from scan tools, firewalls, and other data sources.
- Correlate model with known cyber attack vulnerabilities and environmental metadata, apply network access policy rules.
- Based on assumed threat sources and mission-critical assets, compute network-wide metrics that measure security for the entire enterprise.
- Visualize for trending and comparative analysis.

SCHEDULE & CONTACT INFO.



Principal Investigator:
Sushil Jajodia
Center for Secure Information Systems
George Mason University
jajodia@gmu.edu

Subcontractors:
Applied Visions, Inc. (Secure Decisions Division)
ProInfo, Inc.