



IT Risk – CVSS and Beyond

Alain Mayer
CTO, RedSeal

IT Risk Management is Everywhere

- **NIST**
 - **CVSS: Prioritized Risk**
 - **800-30: Risk Management Guide for IT Systems**
- **Almost all security vendors have offering for IT Risk**
 - **McAfee Risk Advisor**
 - **Symantec Risk and Compliance**
 - **RSA Risk Management**
 - **Qualys IT Security Risk and Compliance**





Prioritized Risk: When the environmental score is computed, the vulnerability now becomes contextual. That is, **vulnerability scores are now representative of the actual risk to an organization**. Users know how important a given vulnerability is in relation to other vulnerabilities.

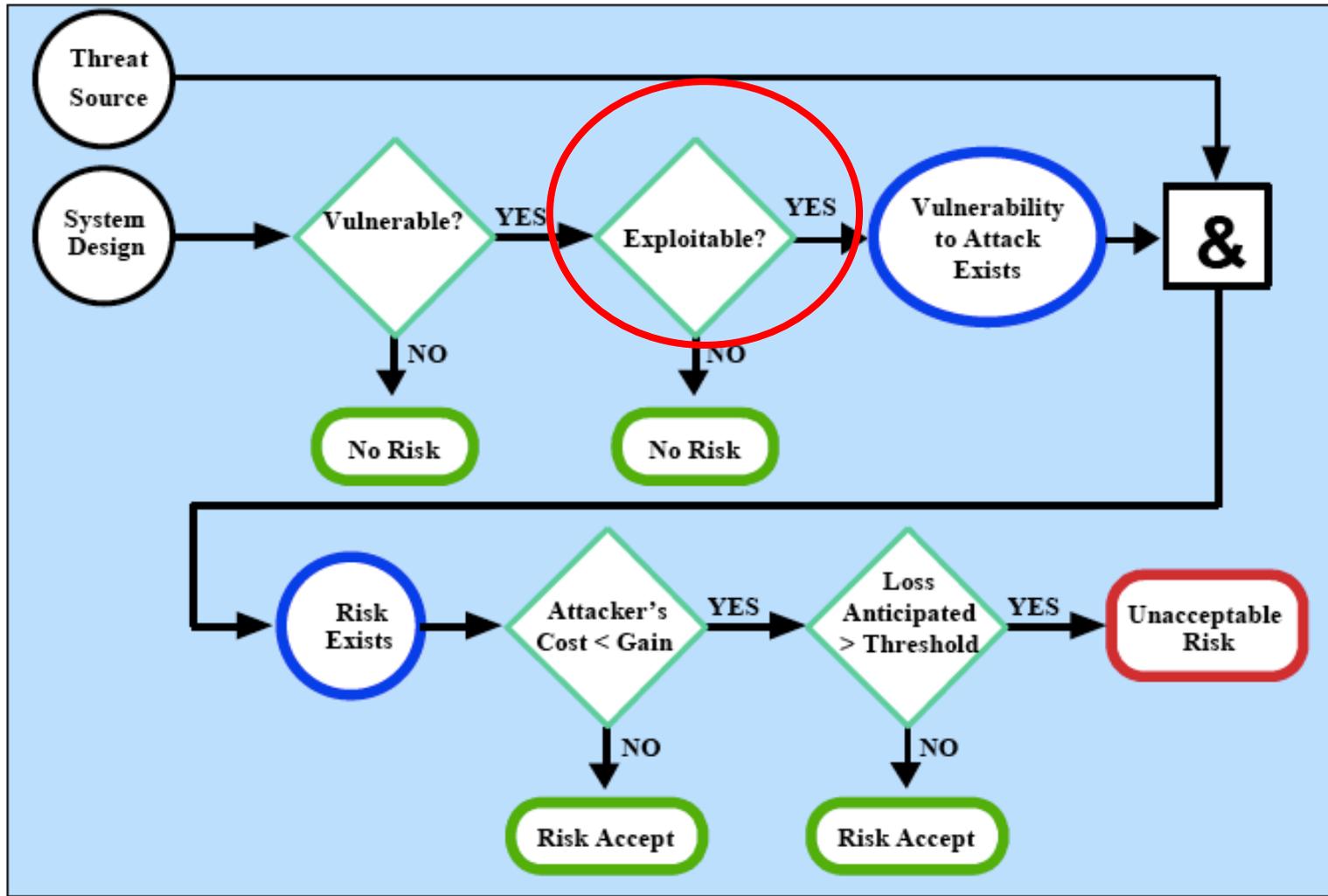


Figure 4-1. Risk Mitigation Action Points

Risk-based on Attack Graph

Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]

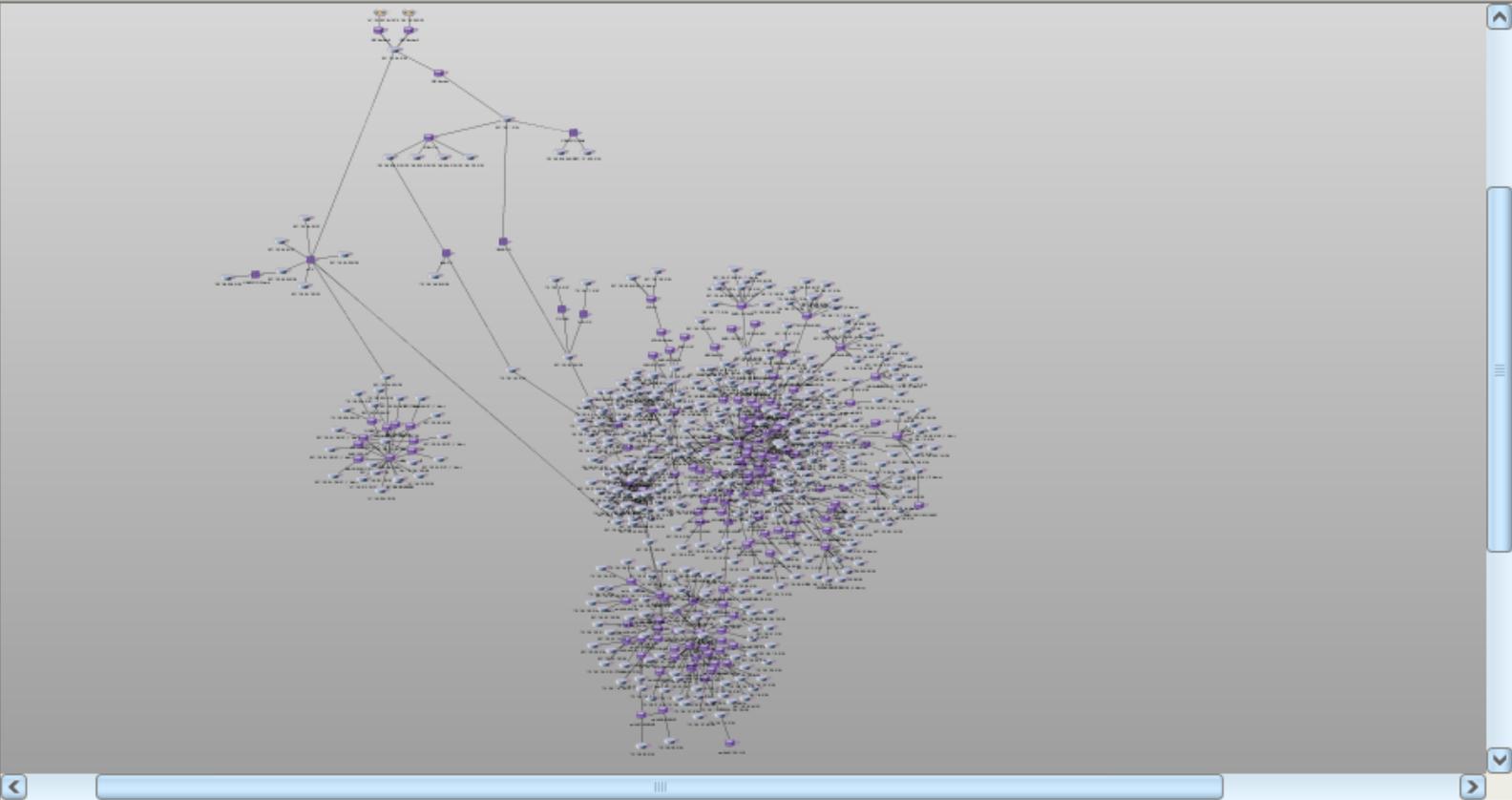
File Edit View Tools Help

Home Risk Threats Inventory Reports

Subnets < > Threats From Threats To 16% Layout Export

Find

- Unmapped
- 10.224.128.0/24
- 10.224.129.0/24
- 10.224.131.0/24
- 12.126.143.200/30
- 147.146.72.32/30
- 147.146.197.76/30
- 147.146.205.76/30
- 147.146.213.76/30
- 147.146.221.76/30
- 157.130.227.64/30
- 167.107.34.60/30
- 170.108.1.0/24
- 170.108.2.0/24
- 170.108.3.0/24
- 170.108.4.0/26
- 170.108.5.0/24
- 170.108.6.0/24
- 170.108.12.0/24
- 170.108.13.0/26
- 170.108.16.0/27
- 170.108.17.0/27
- 170.108.20.0/24



Related Tasks

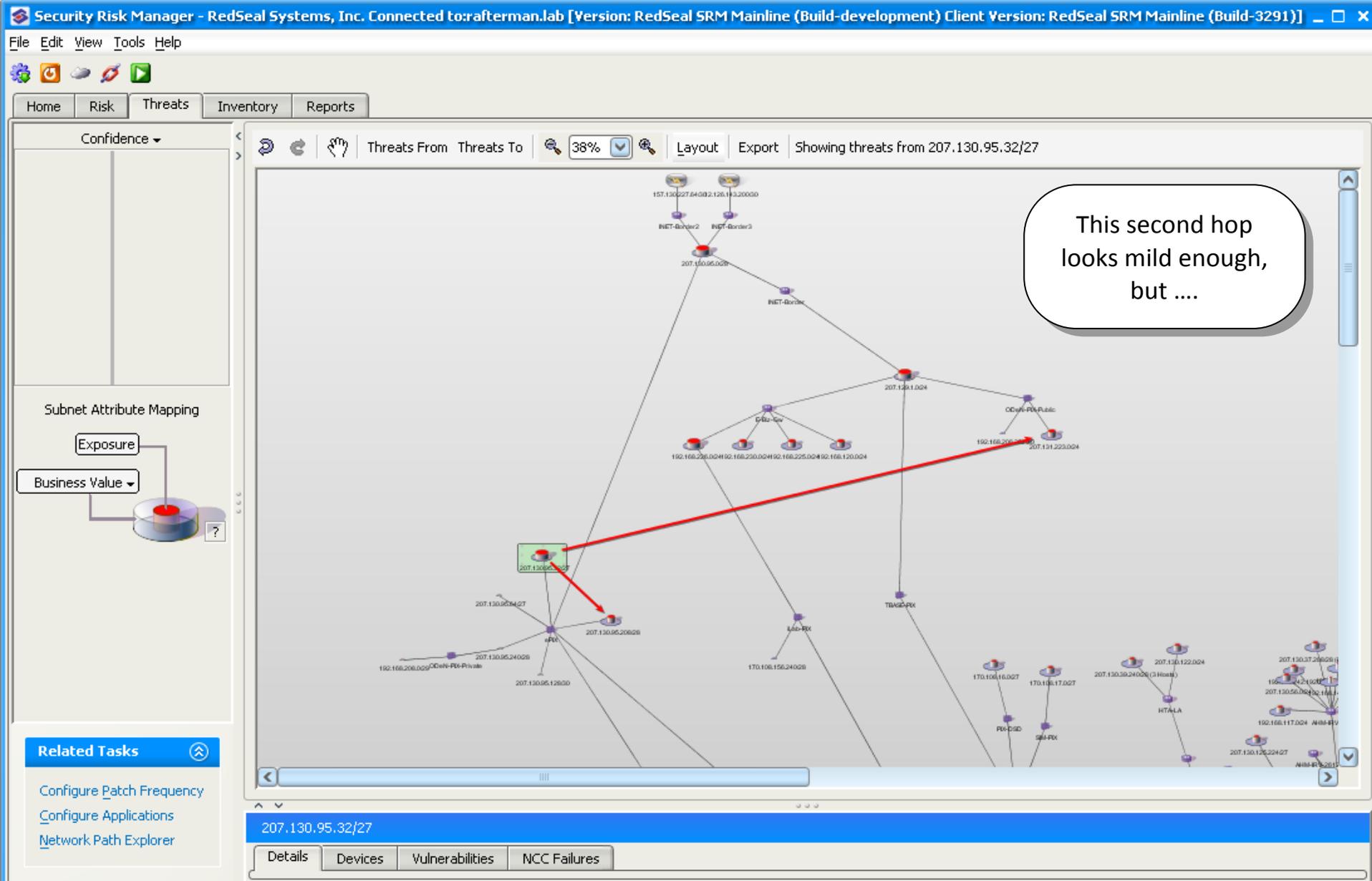
- Schedule Data Collection
- Configure Applications
- Network Path Explorer

Details Viewer

Analysis Current

The image displays a complex network attack graph within a software interface. The graph consists of numerous nodes, represented by small icons, interconnected by lines. The nodes are color-coded, with many appearing in shades of purple and blue, indicating different risk levels or states. The graph is organized into several distinct clusters or sub-networks, with some clusters being significantly larger and more densely connected than others. The interface includes a sidebar on the left with a list of subnets, a top navigation bar with tabs for Home, Risk, Threats, Inventory, and Reports, and a main toolbar with options for search, zoom, and layout. The status bar at the bottom indicates that the analysis is current.

Attack Graph: Security Risk Manifestation



Attack Graph: Security Risk Manifestation

Security Risk Manager - RedSeal Systems, Inc. Connected to:rafterman.lab [Version: RedSeal SRM Mainline (Build-development) Client Version: RedSeal SRM Mainline (Build-3291)]

File Edit View Tools Help

Home Risk Threats Inventory Reports

Confidence ▾

Threats From Threats To 🔍 21% 🔍 Layout Export Showing threats from 207.130.95.208/28

Subnet Attribute Mapping

Exposure

Business Value ▾

Related Tasks

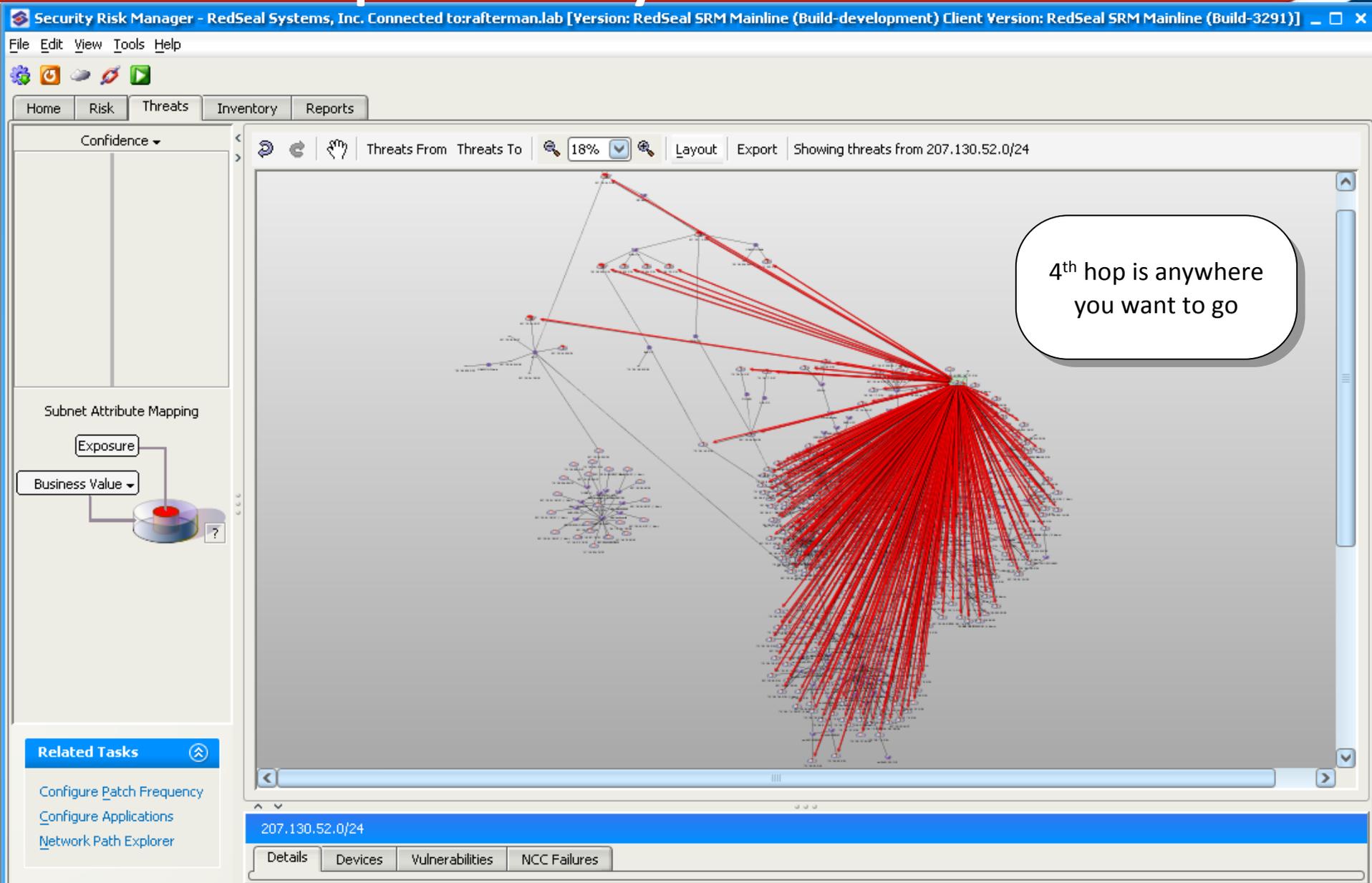
- Configure Patch Frequency
- Configure Applications
- Network Path Explorer

207.130.95.208/28

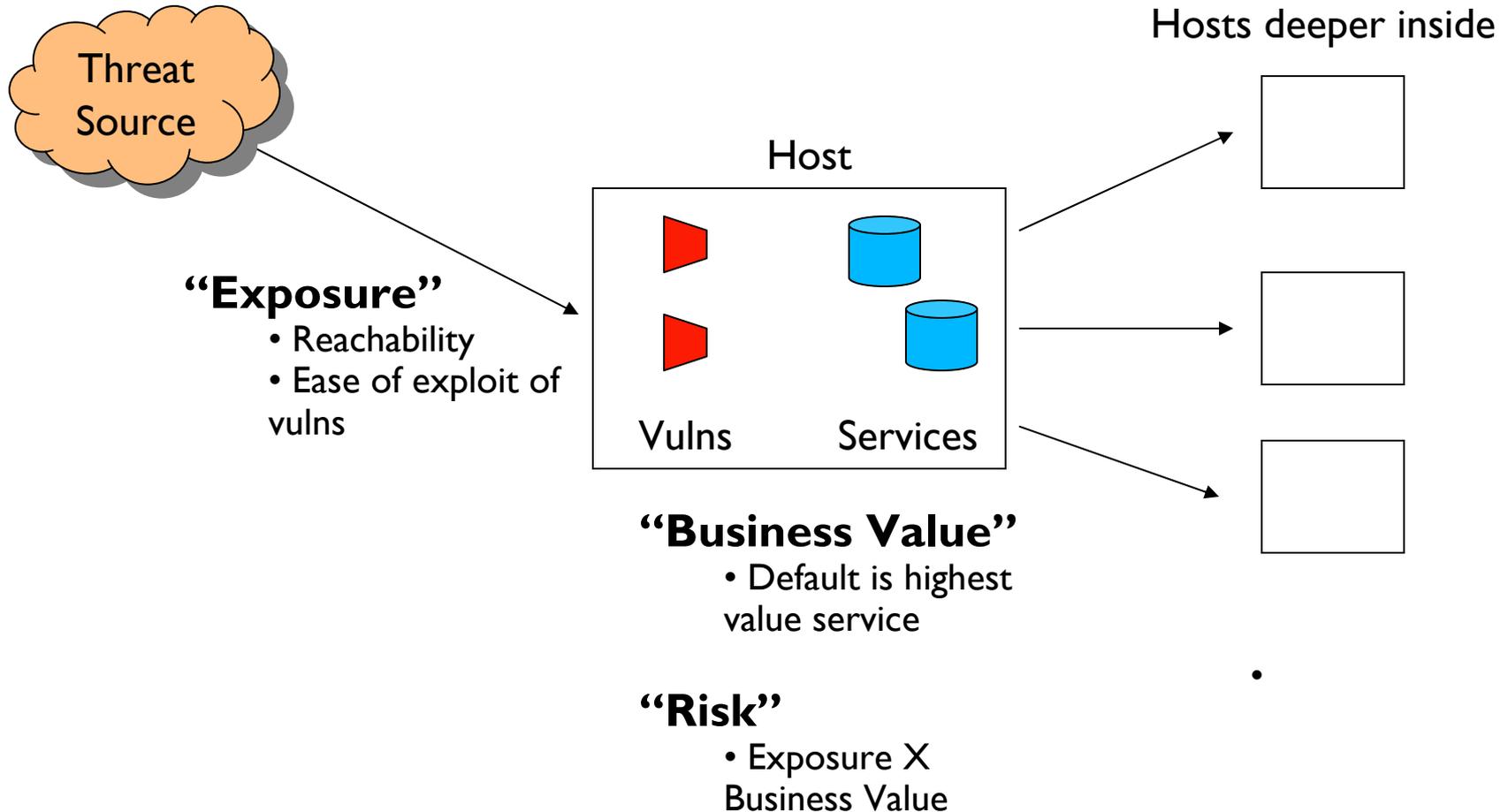
Details Devices Vulnerabilities NCC Failures

This (and only this) third hop breaks in!

Attack Graph: Security Risk Manifestation



Overview of the RedSeal Risk Metrics



Why is IT Risk Management Hard?

- **Security Silos**

- Rigidly patching only high-severity vulnerabilities might not remove vulnerabilities with biggest risk impact
- Firewall teams focused on enabling access for critical business systems

- **Drift Happens!!**

- Even the best designed network does not stay that way (and not many are carefully designed to start with)
- Frequent (sometimes daily) configuration changes eating away at the best intentions



Steps toward effective IT Risk Management

- Understand risk by analyzing data across every aspect of your **entire infrastructure**.
- **Discover and rank** vulnerabilities according to direct and indirect threat paths.
- **Coordinate the efforts** to patch, reconfigure, harden or re-architect based on fixing vulnerabilities that pose the highest risk first.
- **Instantly assess** how changes will affect risk.