



GARNET

Graphical Attack graph and Reachability Network Evaluation Tool*

Leevar Williams, Richard Lippmann, Kyle Ingols

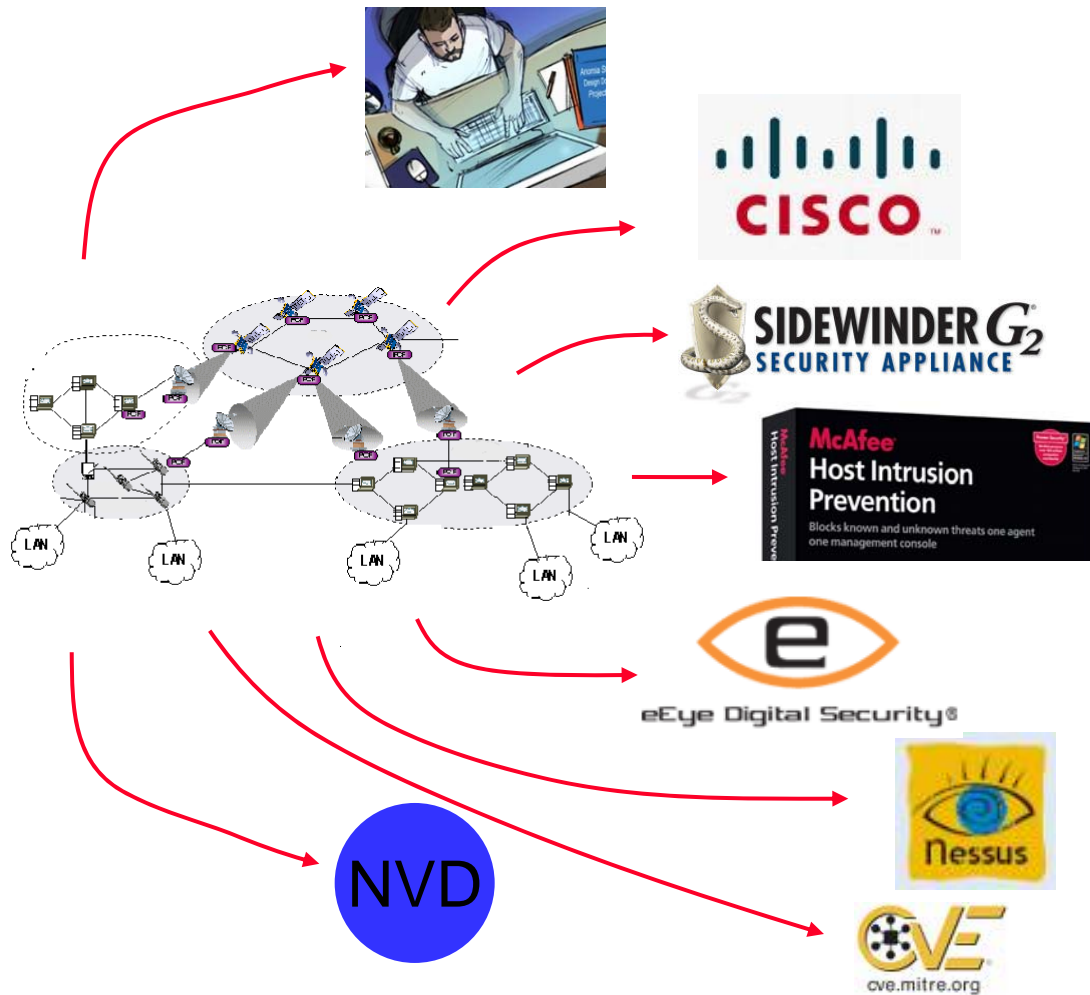
MIT Lincoln Laboratory

15 September 2008

MIT Lincoln Laboratory



A Defender's Primary Advantage is Detailed Network Knowledge – This Needs to Be Used Effectively!

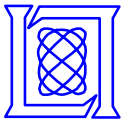


Specify Asset Values
and Adversary

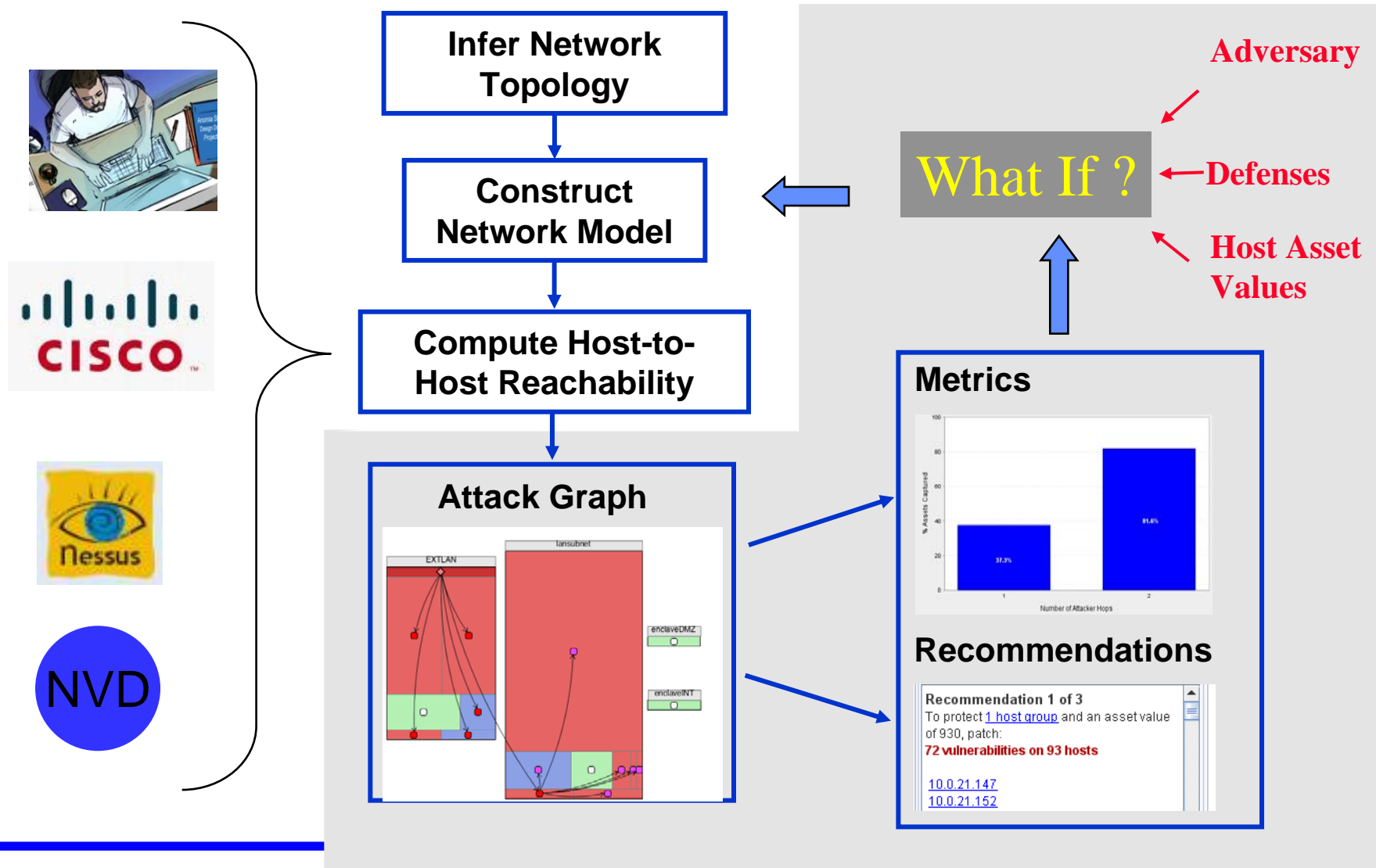
Define Network
Topology
and Filtering Rules

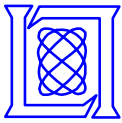
Discover
Vulnerabilities

Define Vulnerability
Requirements/Effects

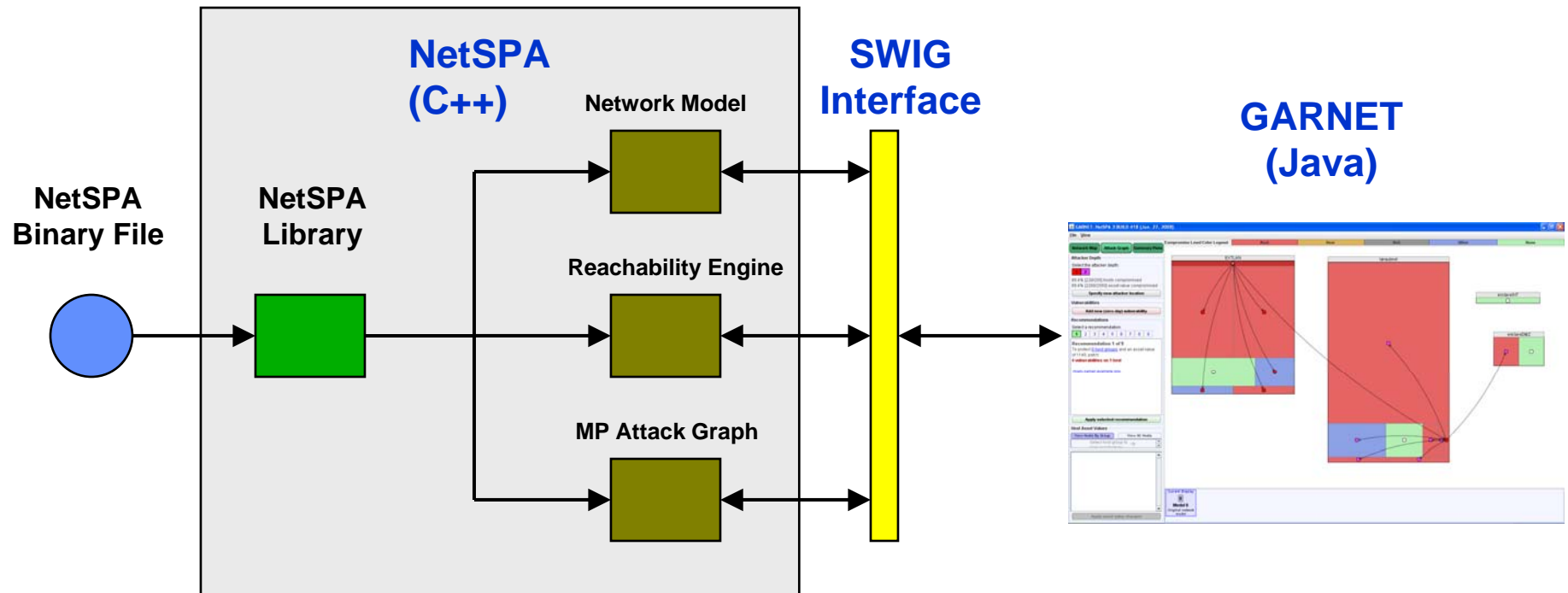


A Tool Named NetSPA Integrates This Data and Supports “What If” Experiments

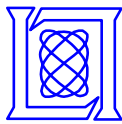




GARNET Uses NetSPA to Provide Rapid Interactive Response



- **GARNET** is implemented in Java using Swing
- NetSPA loads binary network model and produces C objects for data access
- Java and C code communicate using SWIG Toolkit



A Heuristic Evaluation Greatly Improved GARNET's Ease of Use

- Five participants evaluated 9 networks with the initial GUI and provided recommendations using protocols developed by (Nielsen and Molich, 1990; Nielsen 1994)

Original

The original GUI interface features a top navigation bar with three tabs: "Network Map", "Attack Graph", and "Summary Plots". The "Attack Graph" tab is selected. Below the tabs, the "Attacker Depth" section includes a "Select the attacker depth:" label and two buttons labeled "1" and "2". It displays statistics: "89.7% [227/253] hosts compromised" and "89.7% [2270/2530] asset value compromised". The "Recommendations" section has a "Select a recommendation:" label and a row of buttons from "1" to "9", with "1" selected. A green checkmark icon and the text "Apply Selected Recommendation" are present. Below this, "Recommendation 1 of 9" is shown, detailing protection for 9 host groups and an asset value of 1130, with 4 vulnerabilities on 1 host. The "Exploitable Vulnerabilities" section contains a "Select host group to view exploitable vulnerabilities" label with a right-pointing arrow and a "+ Add a new (zero-day) vulnerability..." button. At the bottom, there is a "Display Controls" button and a "Network Information and Filters" label.

Revised

The revised GUI interface features a top navigation bar with three tabs: "Network Map", "Attack Graph", and "Summary Plots". The "Attack Graph" tab is selected. Below the tabs, the "Attacker Depth" section includes a "Select the attacker depth:" label and two buttons labeled "1" and "2". It displays statistics: "89.8% [228/254] hosts compromised" and "89.8% [2280/2540] asset value compromised". A "Specify new attacker location" button is added below. The "Vulnerabilities" section has an "Add new (zero-day) vulnerability" button. The "Recommendations" section has a "Select a recommendation:" label and a row of buttons from "1" to "10", with "1" selected. Below this, "Recommendation 1 of 11" is shown, detailing protection for 7 host groups and an asset value of 1140, with 4 vulnerabilities on 1 host. An "Apply selected recommendation" button is added below. The "Host Asset Values" section has "View Hosts By Group" and "View All Hosts" buttons. Below this, there is a "Select host group to view asset values" label with a right-pointing arrow and an "Apply asset value changes" button at the bottom.

- 20 Major Changes
- All “What-If” controls unified in Attack Graph Panel
- All network details placed in Network Map Panel

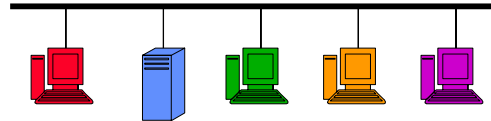


Security Compared by Determining Adversary Cost to Achieve Goals

- Emulate MORDA (Mission Oriented Risk and Design Analysis) procedures

- **Need to model**

- System (Network)



- Adversary goal



- Defenses

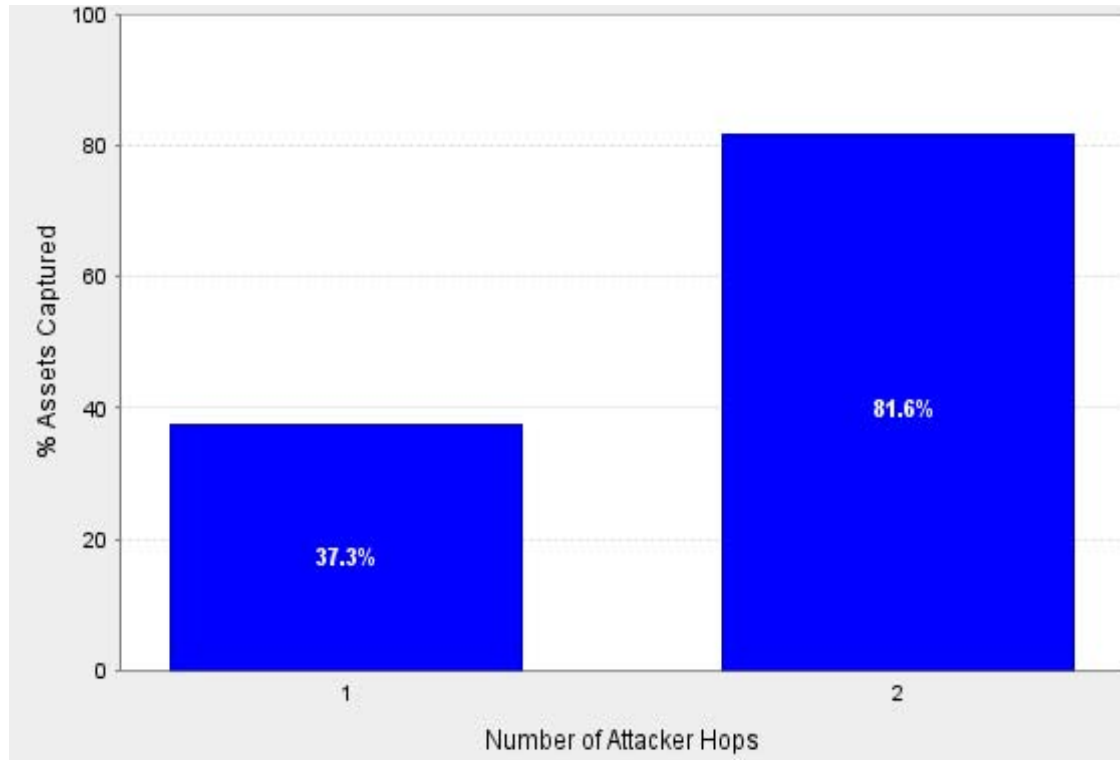


- Adversary

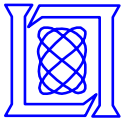




We Currently Assess Adversary Cost Using Three Different Metrics



- Number of hops to reach assets
- Number of unique exploits that are required
- Cumulative CVSS attack complexity



Analyze Network Security Using Escalating Adversary Models

1. Script User

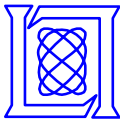
- Has an exploit for all known vulnerabilities

2. Single Zero-Day

- Able to create a zero-day exploit for the one application server on this network that provides the most access

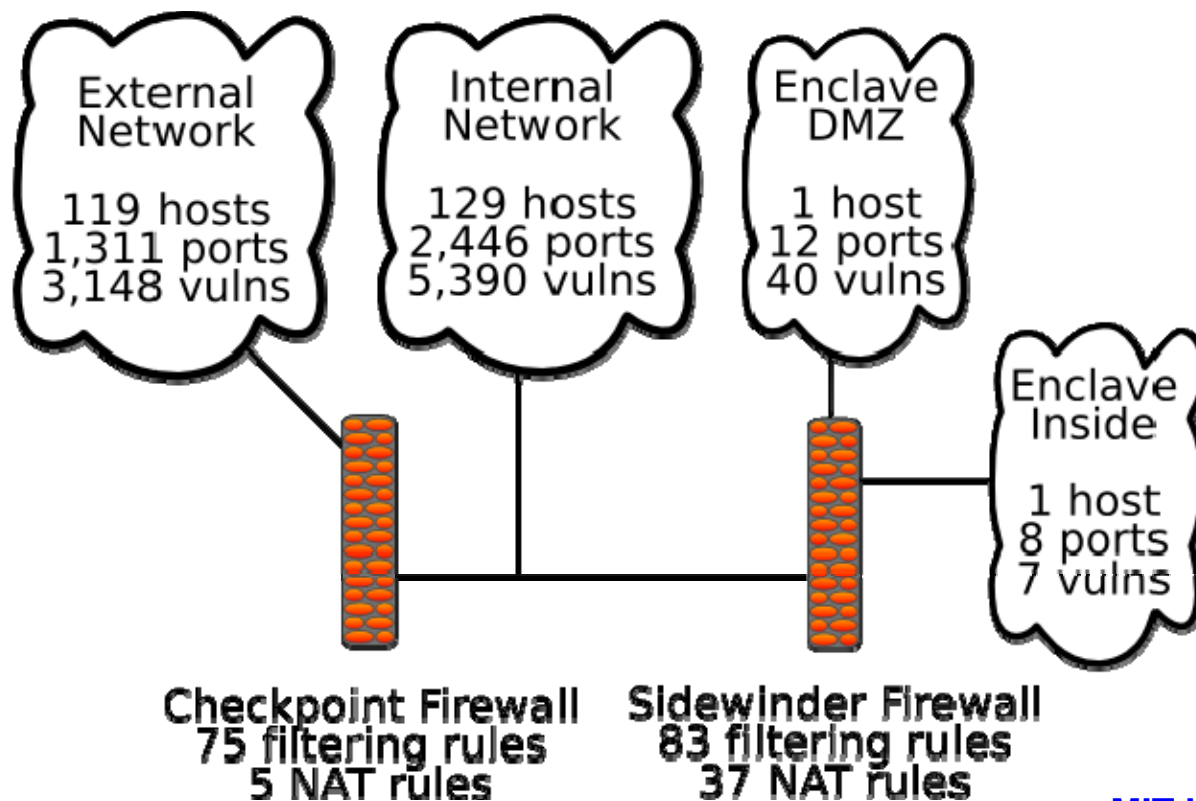
3. Comprehensive-Zero Day

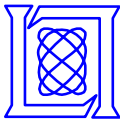
- Able to create a zero-day exploit for all application servers on this network
- Any host that can be reached can be compromised



Example Network

- Anonymized data from real, field test network



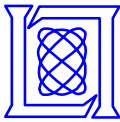


Demonstration: Loaded Network

The screenshot displays the GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008) interface. The main window shows a network map with two subnets, 'lansubnet' and 'EXTLAN', both colored green. A legend at the top indicates compromise levels: Root (red), User (yellow), DoS (grey), Other (blue), and None (green). The 'lansubnet' and 'EXTLAN' subnets are connected to 'enclaveINT' and 'enclaveDMZ' respectively. The left sidebar contains several sections:

- Subnet Reachability:** A dropdown menu is set to 'EXTLAN'. There are radio buttons for 'Show Incoming Reachability' and 'Show Outgoing Reachability', and a button for 'Hide All Reachability Links'.
- Network Information:** A section titled 'Entire Network' showing 'Total Asset Value: 2550', '255 hosts in 4 subnets, 4 host groups', and '363 unique vulnerabilities'. Below this are tabs for 'Hosts' and 'Vulnerabilities'.
- Hosts List:** A list of IP addresses from 10.0.21.147 to 10.0.21.165.
- Host Details:** A detailed view for IP 10.0.21.147, showing 'Subnet: EXTLAN', 'IP: 10.0.21.147', 'Compromise Level: N/A', and 'Asset Value: 10'. It also lists '0 exploitable vulnerabilities' and '15 additional vulnerabilities' with links to CVE and Nessus identifiers.

At the bottom left, a 'Current Display' box shows a '0' and the text 'Model 0 Original network model'.



Demonstration: Rearranged Network

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Network Map Attack Graph Summary Plots

Subnet Reachability

Select a subnet:

lansubnet

Show Incoming Reachability

Show Outgoing Reachability

Hide All Reachability Links

Network Information

Entire Network

Total Asset Value: 2550

255 hosts in 4 subnets, 4 host groups

363 unique vulnerabilities

Hosts Vulnerabilities

10.0.21.147

10.0.21.152

10.0.21.153

10.0.21.154

10.0.21.156

10.0.21.160

10.0.21.161

10.0.21.165

10.0.21.147

Subnet: EXTLAN

IP: 10.0.21.147

Compromise Level: N/A

Asset Value: 10

0 exploitable vulnerabilities

15 additional vulnerabilities

CAN-1999-0635 on port 7

CAN-2003-0661 on port 137

CVE-1999-0103 on ports 7, 13, 17, 19

NESSUS-10150 on port 137

NESSUS-10394 on port 445

NESSUS-10397 on port 445

NESSUS-10736 on port 135

NESSUS-10859 on port 445

NESSUS-10860 on port 445

NESSUS-10914 on port 445

NESSUS-10915 on port 445

NESSUS-10916 on port 445

Comromise Level Color Legend

Root User DoS Other None

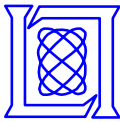
EXTLAN lansubnet enclaveINT enclaveDMZ

Current Display

0

Model 0

Original network model



Demonstration: Attacker Start Select

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Network Map Attack Graph Summary Plots

Attacker Depth

Attacker Location (click subnet to select):
EXTLAN

Attacker IP Range (optional):

OK Cancel

Vulnerabilities

Add new (zero-day) vulnerability

Recommendations

No available recommendations

Apply selected recommendation

Host Asset Values

View Hosts By Group View All Hosts

Host Name	Asset Value
10.0.0.117	E-1.0

Apply asset value changes

Compromise Level Color Legend

Root User DoS Other None

EXTLAN

iansubnet

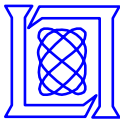
enclaveINT

enclaveDMZ

Current Display

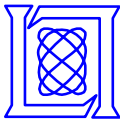
Model 0

Original network model



Demonstration: Attack Result





Demonstration: Attack, Step One

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Comromise Level Color Legend: Root (Red), User (Yellow), DoS (Grey), Other (Blue), None (Green)

Network Map Attack Graph Summary Plots

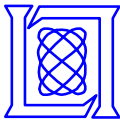
Attacker Depth
Select the attacker depth:
1 2
40.8% [104/255] hosts compromised
40.8% [1040/2550] asset value compromised
Specify new attacker location

Vulnerabilities
Add new (zero-day) vulnerability

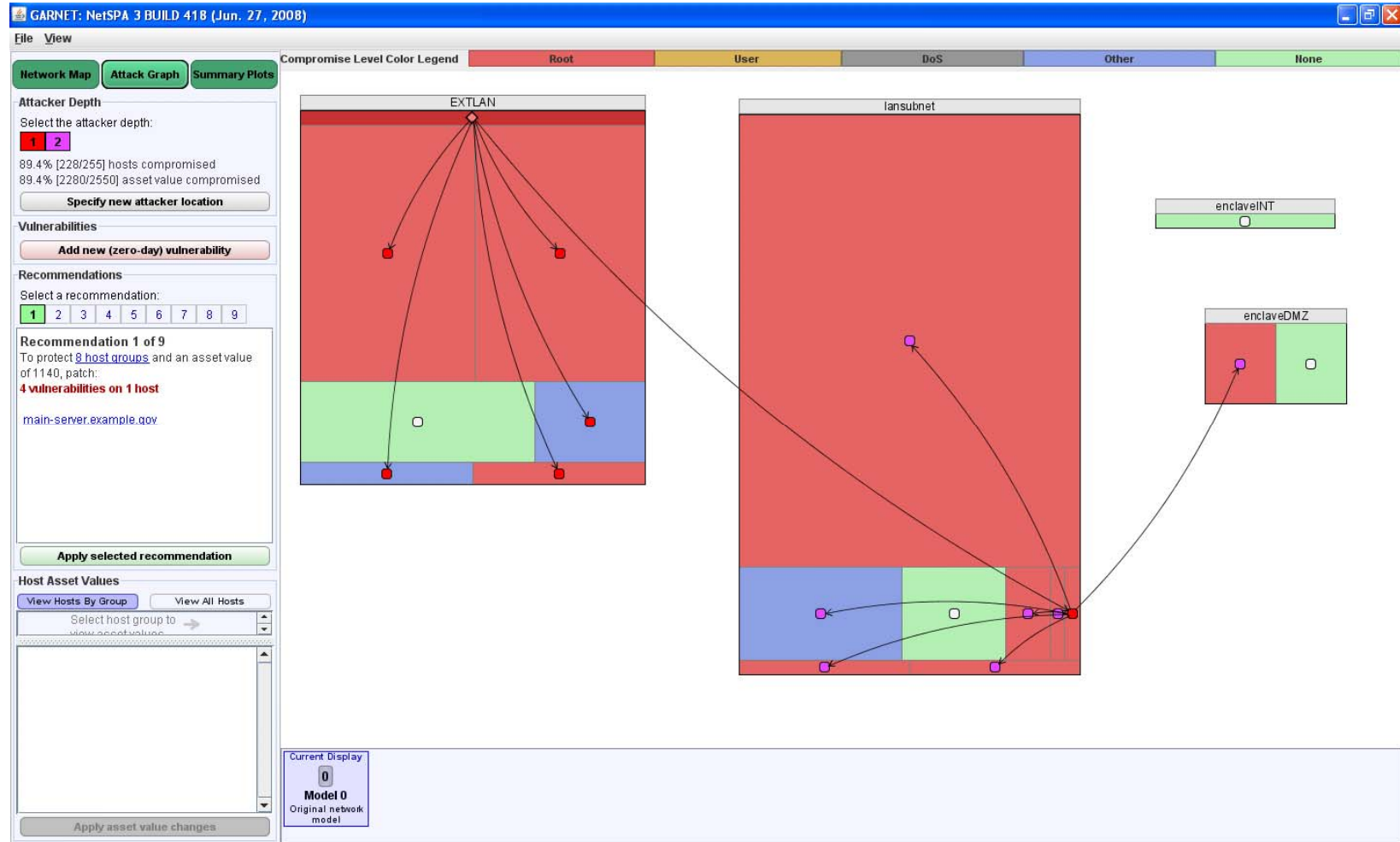
Recommendations
Select a recommendation:
1 2 3 4 5 6 7 8 9
Recommendation 1 of 9
To protect 8 host groups and an asset value of 1140, patch:
4 vulnerabilities on 1 host
main-server.example.gov
Apply selected recommendation

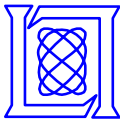
Host Asset Values
View Hosts By Group View All Hosts
Select host group to view asset value
Apply asset value changes

Current Display: 0 Model 0 Original network model



Demonstration: Attack, Step Two





Demonstration: Stepping-Stone

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Comromise Level Color Legend: Root (Red), User (Yellow), DoS (Grey), Other (Blue), None (Green)

Network Map Attack Graph Summary Plots

Attacker Depth
Select the attacker depth:
1 2
89.4% [228/255] hosts compromised
89.4% [2280/2550] asset value compromised
Specify new attacker location

Vulnerabilities
Add new (zero-day) vulnerability

Recommendations
Select a recommendation:
1 2 3 4 5 6 7 8 9
Recommendation 1 of 9
To protect 8 host groups and an asset value of 1140, patch:
4 vulnerabilities on 1 host
main-server.example.gov
Apply selected recommendation

Host Asset Values
View Hosts By Group View All Hosts
Select host group to view asset value
Apply asset value changes

Current Display: 0 Model 0 Original network model

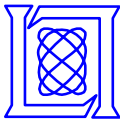
EXTLAN

lansubnet

enclaveINT

enclaveDMZ

Host Group 14
Access Level: Root
1 host
79 unique vulnerabilities



Demonstration: Reachability Trace

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Comromise Level Color Legend: Root (Red), User (Yellow), DoS (Grey), Other (Blue), None (Green)

Network Map Attack Graph Summary Plots

Subnet Reachability

Select a subnet: EXTLAN

Show Incoming Reachability
 Show Outgoing Reachability

Hide All Reachability Links

Network Information

Entire Network

Total Asset Value: 2550
255 hosts in 4 subnets, 18 host groups
363 unique vulnerabilities

Hosts Vulnerabilities

ls6
main-server.example.gov
mars5
martha.example.gov
mcescher.example.gov
mercury.example.gov
miles2000
milesadmin

NESSUS-11405 on port 32867
NESSUS-11418 on port 32805

78 open ports

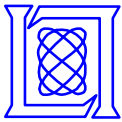
Trace attacker path to this host on port:
25 Trace

Path from attacker on EXTLAN to main-server.example.gov:
10.0.234.40 -> 10.1.60.115:25/tcp
START at link 0 "EXTLAN" with address 10.0.
TRAVERSING unfiltered group 0
ARRIVE intf 5 "autogenerated: internallan-ext
ALLOWED via rule 143 (seq. 7) "7: "
REDIRECT via rule 40 (seq. 1) "1: "10.0.234.40
ROUTED via rule 43 (seq. 1) "Generic all-to-all
ARRIVE intf 4 "ares-l.example.gov @ 10.1.0.10
ALLOWED via rule 20 (seq. 1) "Generic outbo
TRAVERSING unfiltered group 3
ARRIVE intf 132 "main-server.example.gov @
PACKET ACCEPTED on port ID# 1519 ""; 10.0.2

enclaveINT

enclaveDMZ

Current Display: Model 0 Original network model



Demonstration: Recommendation Used

The screenshot displays the GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008) interface. The main window shows a network map with three subnets: EXTLAN, lansubnet, and enclaveINT/enclaveDMZ. A compromise level color legend at the top indicates: Root (Red), User (Yellow), DoS (Grey), Other (Blue), and None (Green). The EXTLAN subnet is primarily red, indicating a high level of compromise. The lansubnet and enclaveINT/enclaveDMZ subnets are primarily green, indicating no compromise. A recommendation is applied to the EXTLAN subnet, showing 72 vulnerabilities on 93 hosts. The interface also includes a sidebar with controls for Attacker Depth, Vulnerabilities, Recommendations, and Host Asset Values. A progress bar at the bottom shows the transition from Model 0 (Original network model) to Model 1 (Modified version of Model 0).

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Network Map Attack Graph Summary Plots

Attacker Depth
Select the attacker depth:
1
0.0% [0/255] hosts compromised
0.0% [0/2550] asset value compromised
Specify new attacker location

Vulnerabilities
Add new (zero-day) vulnerability

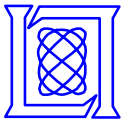
Recommendations
Select a recommendation:
1 2 3
Recommendation 1 of 3
To protect 1 host group and an asset value of 930, patch:
72 vulnerabilities on 93 hosts
10.0.21.147
10.0.21.152
10.0.21.153
10.0.21.156
10.0.21.160
10.0.21.165
Apply selected recommendation

Host Asset Values
View Hosts By Group View All Hosts
Select host group to view asset values
Apply asset value changes

Comprise Level Color Legend
Root User DoS Other None

EXTLAN lansubnet enclaveINT enclaveDMZ

Model 0 Original network model
Model 1 Modified version of Model 0
Current Display



Demonstration: Recommendation Used

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Comprise Level Color Legend: Root (Red), User (Yellow), DoS (Grey), Other (Blue), None (Green)

Network Map | Attack Graph | Summary Plots

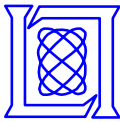
Attacker Depth
Select the attacker depth:
1
40.8% [104/255] hosts compromised
40.8% [1040/2550] asset value compromised
Specify new attacker location

Vulnerabilities
Add new (zero-day) vulnerability

Recommendations
Select a recommendation:
1 | 2 | 3
Recommendation 1 of 3
To protect 1 host group and an asset value of 930, patch:
72 vulnerabilities on 93 hosts
10.0.21.147
10.0.21.152
10.0.21.153
10.0.21.156
10.0.21.160
10.0.21.165
Apply selected recommendation

Host Asset Values
View Hosts By Group | View All Hosts
Select host group to view asset values
Apply asset value changes

Model 0 Original network model
Model 1 Modified version of Model 0 (Current Display)



Demonstration: Zero-Day Adversary

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Comromise Level Color Legend: Root (Red), User (Yellow), DoS (Grey), Other (Blue), None (Green)

Network Map Attack Graph Summary Plots

Attacker Depth
Select the attacker depth:
1
40.8% [104/255] hosts compromised
40.8% [1040/2550] asset value compromised
Specify new attacker location

Vulnerabilities
Add new (zero-day) vulnerability

Recommendations
Select a recommendation:
1 2 3
Recommendation 1 of 3
To protect 1 host group and an asset value of 930, patch:
72 vulnerabilities on 93 hosts
10.0.21.147
10.0.21.152
10.0.21.153
10.0.21.156
10.0.21.160
10.0.21.165
Apply selected recommendation

Host Asset Values
View Hosts By Group View All Hosts
Select host group to view asset values

Model 0 Original network model
Model 1 Modified version of Model 0 (Current Display)

Network Map showing EXTLAN and Iansubnet subnets. A dialog box titled "Add New Vulnerability" is open, displaying a table of applications and their impacts.

Application	Occurrences	Impact
Generic 10000/tcp app	6	--
Generic 10001/tcp app	1	--
Generic 01001/tcp app	34	--
Generic 01002/tcp app	1	--
Generic 01006/udp app	1	--
Generic 10080/udp app	1	--
Generic 10082/tcp app	1	--
Generic 01009/tcp app	1	--
Generic 01016/udp app	1	--
Generic 01018/tcp app	1	--
Generic 01019/tcp app	1	--
Generic 01022/udp app	1	--



Demonstration: Zero-Day Adversary Select Worst-Case Zero-Day Application

GARNET: NetSPA 3 BUILD 418 (Jun. 27, 2008)

File View

Comprise Level Color Legend: Root (Red), User (Yellow), DoS (Grey), Other (Blue), None (Green)

Network Map Attack Graph Summary Plots

Attacker Depth
Select the attacker depth:
1
40.8% [104/255] hosts compromised
40.8% [1040/2550] asset value compromised
Specify new attacker location

Vulnerabilities
Add new (zero-day) vulnerability

Recommendations
Select a recommendation:
1 2 3
Recommendation 1 of 3
To protect 1 host group and an asset value of 930, patch:
72 vulnerabilities on 93 hosts
10.0.21.147
10.0.21.152
10.0.21.153
10.0.21.156
10.0.21.160
10.0.21.165
Apply selected recommendation

Host Asset Values
View Hosts By Group View All Hosts
Select host group to view asset values

Apply asset value changes

EXTLAN iansubnet

enclaveINT

enclaveDMZ

Add New Vulnerability
Use this dialog to evaluate the impact of hypothetical zero-day flaws in one or more applications on the network.
Pick one or more:

Application	Occurrences	Impact
Generic 00022/tcp app	96	1220
Generic 00025/tcp app	48	1160
Generic 00123/udp app	91	50
Generic 00135/tcp app	92	40
Generic 00137/udp app	100	40
Generic 00139/tcp app	106	40
Generic 01025/tcp app	56	30
Generic 00023/tcp app	65	30
Generic 00021/tcp app	58	20
Generic 01024/tcp app	4	10
Generic 01029/tcp app	6	10
Generic 00011/tcp app	100	10

Compute Impacts 41%

OK Cancel

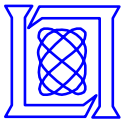
Model 0 Original network model

Current Display Model 1 Modified version of Model 0



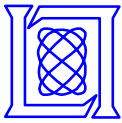
Demonstration: Zero-Day Adversary Using Port 22/tcp



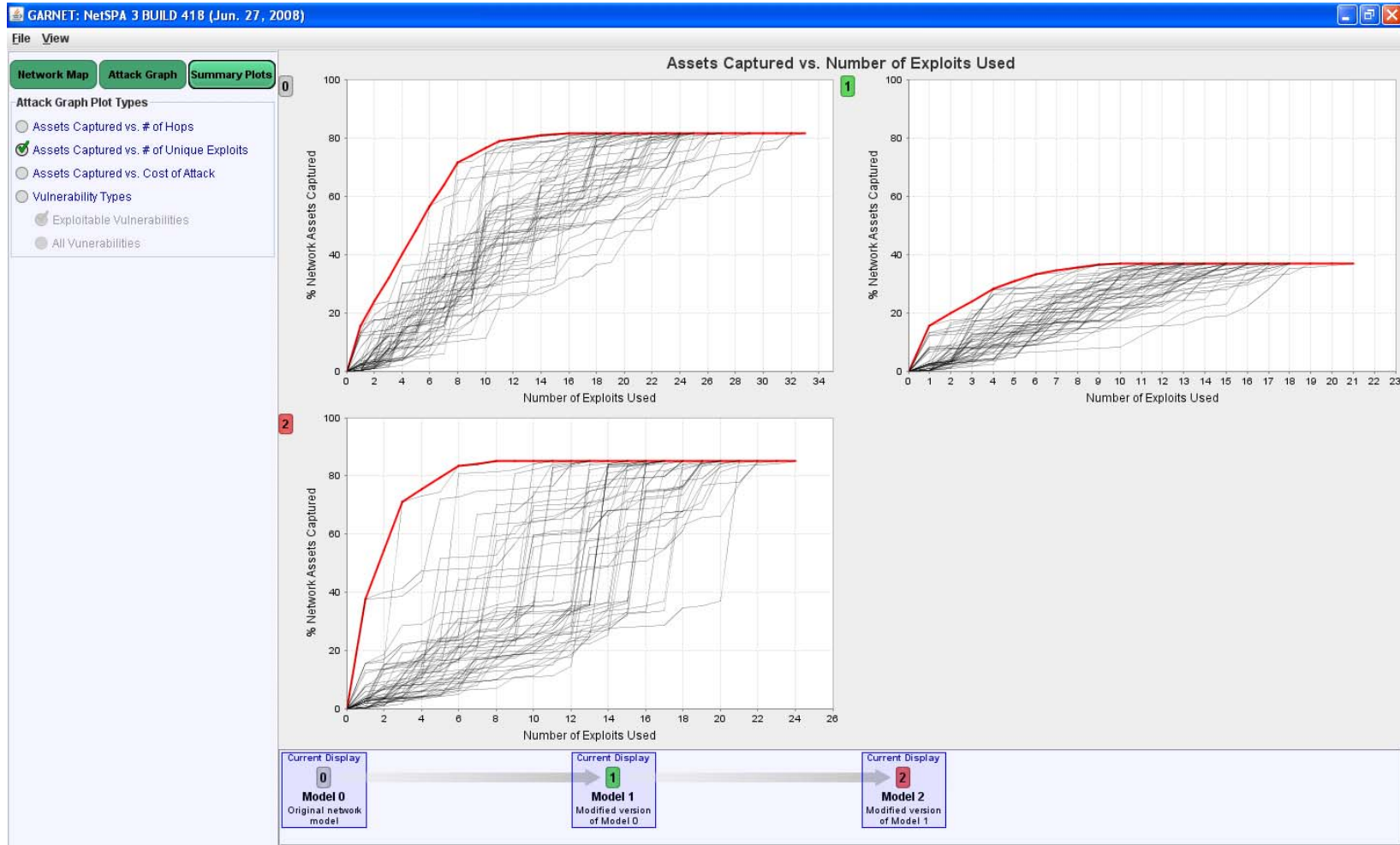


Demonstration: Assets Capture Versus Hops





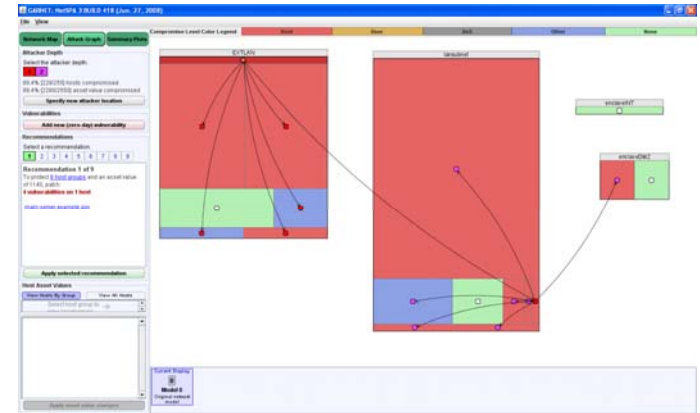
Demonstration: Assets Captures Versus Unique Exploits Required

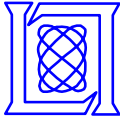




GARNET Summary

- **Rapid Interactive response**
- **Easy to use and intuitive GUI**
- **Supports “What-If” experiments**
- **Computes and displays ...**
 - Recommendations
 - Security metrics (attacker effort)
 - Host-to-host reachability
 - Attack graphs





Future Work

- **Adversary model**
 - Visualize client-side attacks
 - Import and use data on trust relationships
- **Extend Countermeasure Models**
 - Intrusion prevention systems
 - Proxy firewalls
- **Efficiently model endpoint or host-based firewalls**
- **Display physical/logical network topology including firewalls, routers, and switches**