

# NeMS *(formally known as Net\_Mapper)*

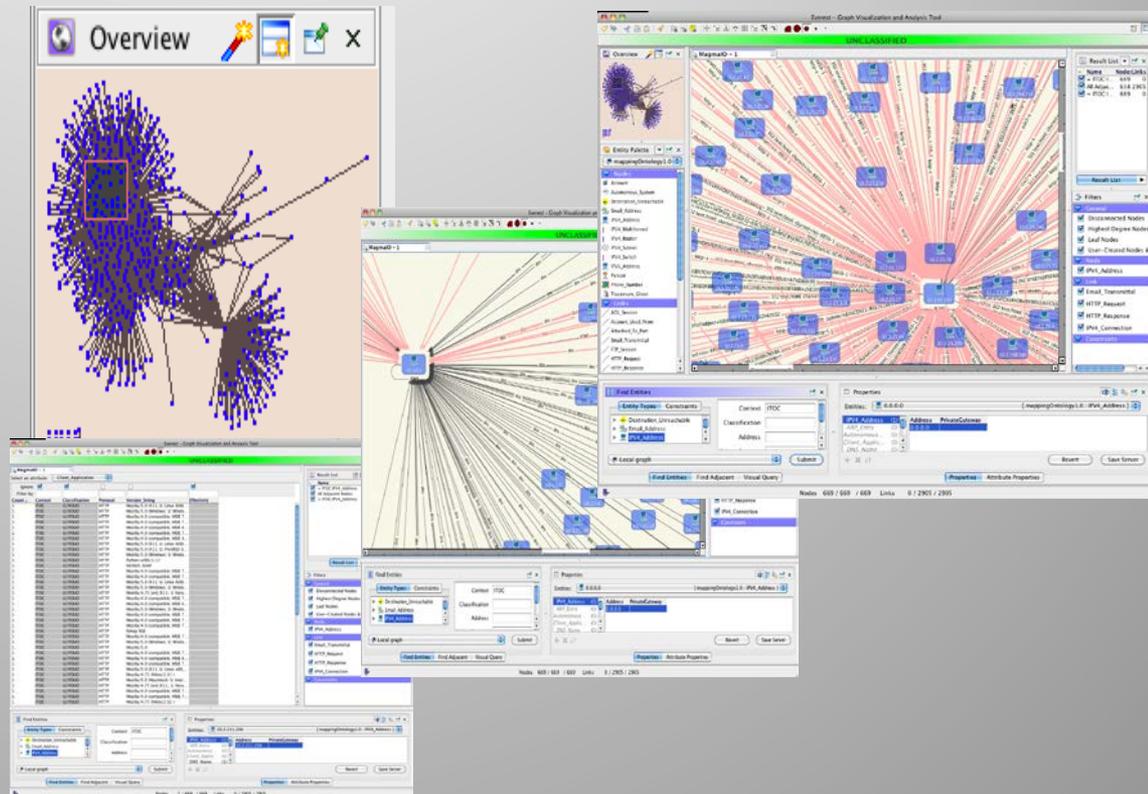
## Network Mapping and Discovery for Cybersecurity Situational Awareness



*Celeste Matarazzo and Domingo Colon*



This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344.  
Lawrence Livermore National Security, LLC



# How can you secure a network if you don't know what IT is?

- Computer networks are organic and complex
- Network Mapping provides a current snapshot of a network's structure and activity profile
- Network maps combine available data to provide a picture of HOW the network is actually being used
- Mapping operations discover ACTUAL network topology including routers, switches and end hosts services running on these devices
- Mapping discovers changes in a network

# Network Mapping System (NeMS)

- Software-based **network** characterization and discovery tool
- Constructs visual representations of computer network based on observed behavior
- Iterative analysis platform from which network security managers and information technology (IT) personnel can explore the findings of each mapping operation

# What's unique about Network Mapping System (NeMS)

- Network maps combine available active and passive data to provide a picture of how the network is actually being used
- Mapping conducted from any vantage point within a network, including multiple vantage points
- Flexible controls to enable the mapping operations to meet speed, load and security requirements (e.g., throttle)
- Validated in controlled environments (with ground truth) and in operational networks
  - **Found 100%** of hosts were identified **plus the unexpected discovery of an unknown external network connection**
  - Operational network measured load and found NO impact to performance

# Mapping results provide detailed characterizations of network environments

- Open ports
- Available services and version information
- Operating Systems
- Network Topology
  - Traceroute
  - Router Interfaces (SNMP)
  - Static Routes (SNMP)
- Passive Mapping techniques provide:
  - Host discovery
  - Host activity (transactions between nodes)
  - The content of communications

SNMP Results

Type	Val
sysLocation	Unknown
sysContact	root
sysDescr	Vyatta VC6.3-2011.07.21
sysServices	14
sysObjectID	.1.3.6.1.4.1.30803
sysName	vyatta

Operating Systems

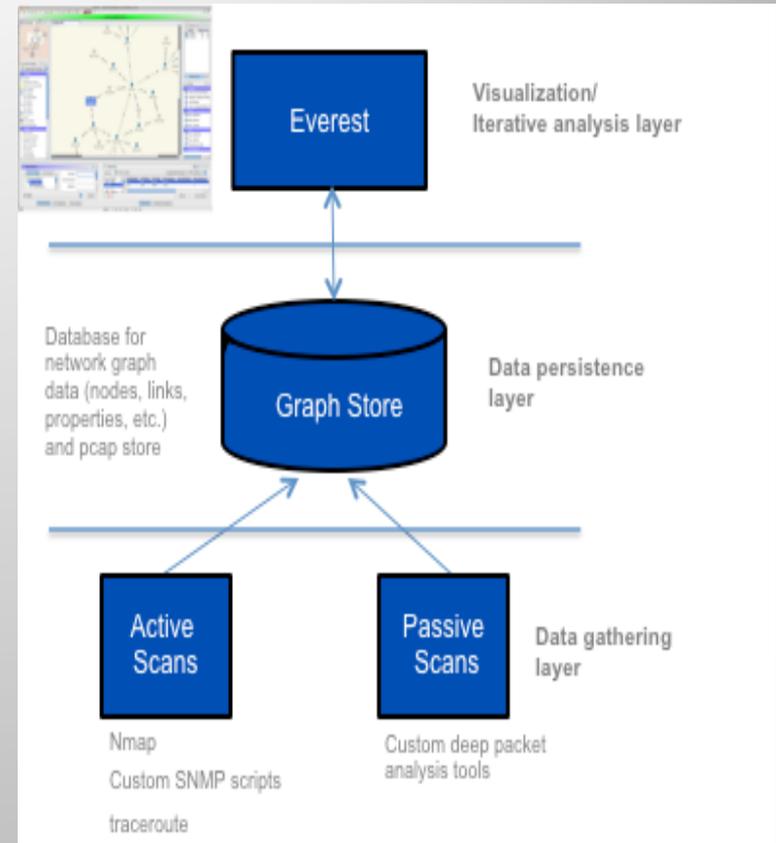
Context	Classification	OperatingSystemType	Confidence
Internet	U	Linux 2.6.17 - 2.6.28	100
Internet	U	Microsoft Windows Server 2008	100
Internet	U	Microsoft Windows 7	100
Internet	U	Microsoft Windows XP	100

Open Ports

The screenshot displays the Everest - Graph Visualization and Analysis Tool interface. The main window shows a network topology graph with nodes representing IP addresses and their connections. The interface includes several panes: Overview, Entity Palette, Result List, and Properties. The Properties pane is open for the entity 150.1.0.254, showing details such as PortNumber (21), PortProto (TCP), PortState (OPEN), ServiceName (snmp), and ServiceVersion (1). The Status bar at the bottom indicates 1 / 49 Nodes and 0 / 66 Links.

# LLNL NeMS - overview

- Software-based high-performance network characterization and discovery
- Combines intelligent network probes, passive traffic analysis and host discovery
- Constructs OBSERVED network topology and behavior including end hosts and services
- Mapping toolset provides iterative visualization and analysis environment to explore findings



Network Mapping Architecture

# Competitive Differentiation

- Configurable to minimize disruptions and impacts on the target operational network and to require minimal intervention by network security staff
- System has a modular structure that allows the easy addition of new capabilities
- Builds on 15 years of network analysis and high performance computing expertise
- Focuses on discovery of the network rather than compliance checking

# Contact Information

**Celeste Matarazzo**

**matarazzo1@llnl.gov**

**Domingo Colon**

**colon3@llnl.gov**

Webinar available:

[https://ipo.llnl.gov/?q=resources-entrepreneurs-technology\\_market\\_discovery](https://ipo.llnl.gov/?q=resources-entrepreneurs-technology_market_discovery)