Integrating Third-party Data Sources with the Network Mapping System

Christopher Gullo†, Domingo Colon*, Celeste Matarazzo*

†Rochester Institute of Technology
Computer Science
Rochester, NY

*Lawrence Livermore National Laboratory
Computation Directorate
Livermore, CA

Introduction

The deployment of NeMS can be expedited with initial target data, bypassing slow client information requests and inaccurate supplied addresses.

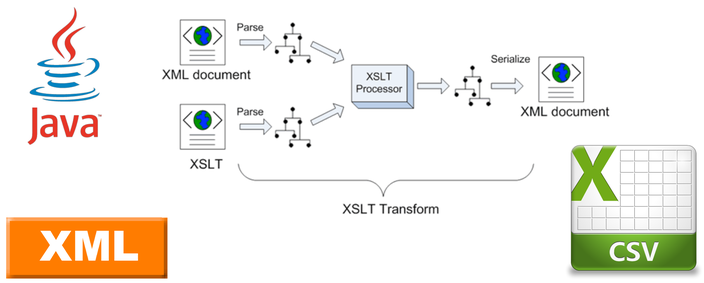
Network Mapping System (NeMS)

- NeMS is a software-based network characterization and discovery application.
- The final result of running NeMS is a map of the targeted network environment for information technology and security personnel to view and analyze.
- NeMS as a system uses two LLNL-developed software projects; the NeMS tool itself, and the Everest visualization system.
- This provides network security managers and information technology personnel with continuing network situational awareness.

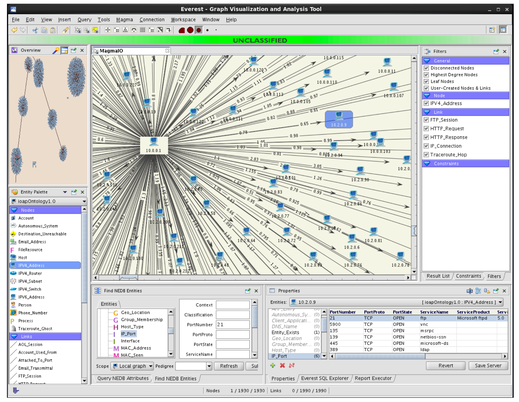
Tenable® Nessus®

- Nessus® is the industry's most widely-deployed vulnerability, configuration, and compliance tool.
- Data from Nessus® can be used to assist NeMS deployment.

Technologies



Project Overview



Integrating third-party data into NeMS allows access to initial data before deployment. This makes NeMS more efficient and more effective. Instead of scanning more of the network than necessary, which costs additional time and money, a more educated set of targets can be determined with this data.

When clients already use third-party systems daily, taking advantage of their data is a great benefit and a large improvement to the operation of NeMS.

Tenable® Nessus®, having been surveyed as one of the most popular third-party vulnerability scanners used, was chosen as the proof-of-concept data source.

Input Types

There are two types of NeMS inputs focused on in this project:

- IP address CIDR (Classless Inter-Domain Routing) ranges
- Target XML files

192.168.1.1/24

CIDR ranges will provide NeMS with a set of more specific areas to scan, providing a starting point for execution.

Target XML is the traditional data NeMS generates. These files will directly translate to NeMS and the Everest visualization system without scanning on its own.

Data Sources

With the goal of integrating third-party data sources with the Network Mapping System, it is easy to realize that there are a lot of sources to to choose from. Nessus'® data happens to be using XML (eXtensible Markup Language), so this format became the focus.

In working with Nessus'® XML, test data was requested and received in the comma-separated values (CSV) format, so this format also became a focus.

Knowing that future data sources will be important for NeMS' future, one of the project goals was towards implementing and maintaining modularity. This will allow future formats, more than the initial XML and CSV, to make their way into data for NeMS.

CIDR Ranges

Nessus® Data as an XML Source

Using XML XPath technology, single host IP addresses are extracted from the provided Nessus® data files and converted into appropriate CIDR ranges.

Nessus® Data as a CSV Source

Using the OpenCSV Java CSV parser, the list of IP addresses are gathered and condensed into appropriate CIDR ranges.

Target XML

Nessus® Data as an XML Source

Given an entire Nessus® data file (XML format with Tenable'®s own schema), the XML is read and subsequently parsed for re-building into NeMS' own schema as a Target XML file.

Nessus® Data as a CSV Source

With the Nessus® data exported into CSV format and parsed, Target XML files are created with each unique IP address found. Duplicate IP address simply update the existing Target XML created.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

IM Review and Release # LLNL-POST-658247