

Topological Vulnerability Analysis

Predicting all possible paths of vulnerability

Overview

Cyber security is a global issue of growing importance. Cyber espionage can affect technical, military, political and economic interests anywhere. Attacks are no longer direct – they are increasingly sophisticated and stealthy. Cyber security is mission critical.

Network security concerns are highly interdependent; each machine's susceptibility to attack depends critically on vulnerabilities and connectivity across the network. To protect critical networks, management must understand not only individual system vulnerabilities, but also their interdependencies.

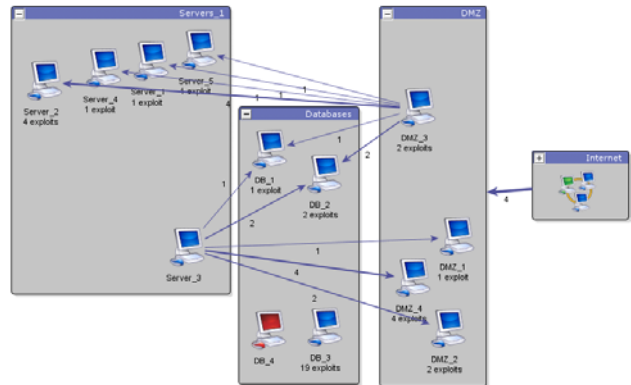
The Problem

Configurations may change, but vulnerabilities evolve and mutate. Currently, network administrators must rely on labor-intensive processes for tracking network configurations and vulnerabilities, which requires a great deal of expertise and is error prone because of the complexity, volume, and frequent changes in security data and network configurations. The organization of networks and the interdependencies of vulnerabilities are so complex as to make traditional vulnerability analysis inadequate.

The Right Tool

Gathering information is just the first step. Network vulnerability scanners have become common tools to help network administrators discover and patch security holes on enterprise networks. Analysis of vulnerability reports can be accomplished with reasonable effort on smaller networks. However, analysis of larger networks is much more difficult because of the size and the potential for error. Depending on the extent of a security breach and the data that has been compromised, errors in vulnerability analysis have the potential to be costly.

Are you using the right tool for the right job?

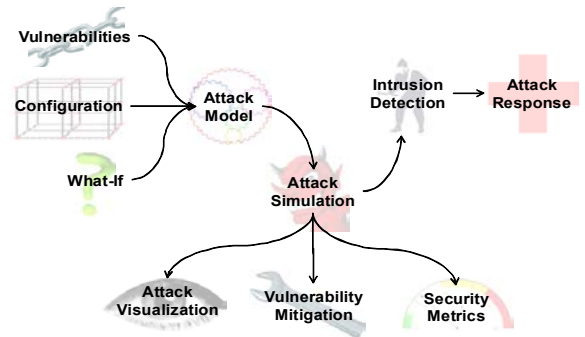


The Next Step

Network vulnerability scanners have created a new problem - how to manage, interpret, and visualize the data contained in vulnerability reports. Thus, the success of vulnerability scanning technology has created a need for software to aid in network vulnerability analysis. Topological Vulnerability Analysis (TVA) via the CAULDRON tool is the next step in decision support.

The Solution

CAULDRON takes the “heavy lifting” and complexity out of improving enterprise security by providing next generation technology to run on demand. Using integrated updated data sets, IT management can now **predict all possible paths of vulnerability** within your enterprise.



Building upon data already gathered, CAULDRON correlates and creates visual representations of all vulnerabilities. CAULDRON will create a “punch list” of prioritized vulnerabilities to fix and/or harden. Apply resources more judiciously.

Our TVA approach provides a unique new capability, transforming raw security data into a roadmap that lets one proactively prepare for attacks, manage vulnerability risks, and have real-time situational awareness.

CAULDRON supports both offensive (e.g., penetration testing) and defensive (e.g., network hardening) applications. The mapping of attack paths through a network via TVA provides a concrete understanding of how individual and combined vulnerabilities impact overall network security.

CAULDRON places vulnerabilities and their protective measures within the context of overall network security by modeling their interdependencies via attack graphs. The analysis of attack graphs provides alternative sets of protective measures that guarantee safety of critical systems. Through this unique new capability, administrators are able to determine the best sets of protective measures that should be applied in their environment.

name	preconditions	postconditions
bt_MozillaSuiteAndFirefox XPInstallJavaScript ObjectInstanceValidation	<p>preconditions</p> <ul style="list-style-type: none"> access <ul style="list-style-type: none"> access execute machine attack connection <ul style="list-style-type: none"> from attack to victim vuln <ul style="list-style-type: none"> vid bugtraq.13232 external_ids 	<p>postconditions</p> <ul style="list-style-type: none"> access <ul style="list-style-type: none"> access execute machine victim privilege <ul style="list-style-type: none"> privilege user machine victim

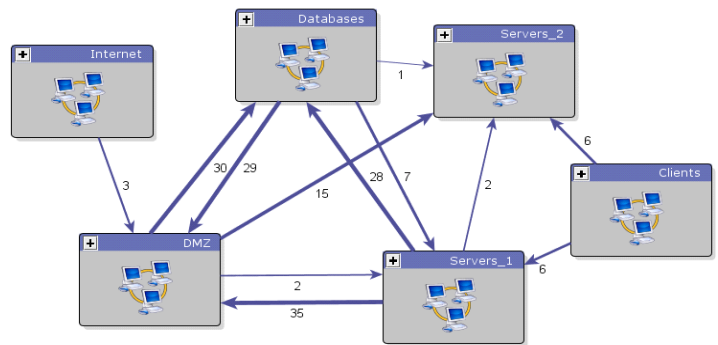
CAULDRON automates the analysis of vulnerability reports allowing administrators to better assess their network security posture. By displaying the results of analysis in the form of an attack graph, all known attack paths from an attacker to a target are succinctly depicted, and a response strategy can be more easily created. Detailed high priority specifics are a click away.

From models of the network vulnerabilities and potential attacker exploits, CAULDRON discovers attack paths (organized as graphs) that convey the impact of individual and combined vulnerabilities on overall security. Immediately use sophisticated attack graph visualizations, with high-level overviews and detail drilldown. Decision support capabilities let analysts make optimal tradeoffs between safety and availability, and show how to best apply limited security resources.

CAULDRON has the ability to create “what if” scenarios as it relates to enterprise security. This means management can simulate attacks and solutions for overall effectiveness – while saving time and related costs.

Background

CAULDRON was created by The Center for Secure Information Systems (CSIS) - housed in the Volgenau School of Information Technology and Engineering at George Mason University. Established in 1990, CSIS is the first academic center in security at a U.S. university. One of the nation’s premier security research organizations, it is also a charter NSA Center of Academic Excellence in Information Assurance Education. CSIS maintains a dedicated full-time team of scientists and engineers with a wide range of expertise, including vulnerability analysis, network attack modeling, intrusion detection, penetration testing and related areas.



Contact ProInfo at 301 237 0007 or johnrw@proinfomd.com for more information.

