Edith Cowan University

IBM i2 solutions help university researchers catch a group of would-be hackers

Overview

The need

After successfully luring would be hackers into their Honeypot, the research team at ECU was faced with the daunting task of analyzing millions of lines of cyber data.

The solution

IBM i2 software helped the team consolidate and visualize this massive amount of disparate data to quickly uncover insightful patterns and trends.

The benefit

Professor Valli's team was able to save hundreds of hours of research. In one instance they turned what would have been a 30 hour project into a 30 minute task.

Edith Cowan University (ECU) is a large multi-campus institution serving communities in Western Australia and a significant cohort of international students.

Awarded university status in 1991, ECU has since developed innovative and practical courses across a wide range of disciplines, established a vibrant research culture and attracted a growing range of quality research partners and researchers, many working at the cutting edge of their fields.

One such researcher is Professor Craig Valli of ECU's School of Computer and Security Science. Recently, Professor Valli lead a team of researchers using Honeypots, decoy computer systems whose role is to deceive hackers into believing they are attacking a legitimate system, to study hackers attempting intrusions. Honeypots present potential hackers with attractive targets which appear to contain operating system vulnerabilities, while in reality logging each attempted intrusion into a database. Studying these logs involves analyzing hundreds of thousands to millions of lines of textual data.

Cyber analysis can involve millions of lines of data

Analyzing this volume of data is nothing new to many law enforcement users who routinely analyze tens of thousands of telephone records using IBM® i2® Analyst's Notebook® – a key component of IBM® i2® solutions – but the requirements for analyzing cyber security audit logs can often run into millions of records. Analyzing logs of this volume can potentially take hundreds of man hours and severely hinder the analysis process.

Solution Components

- IBM® i2® Analyst's Notebook®

"Analyst's Notebook takes hundreds of thousand or millions of lines of textual data and transforms it into a rich graphical story."

—Professor Craig Valli, Edith Cowan University School of Computer and Security Science

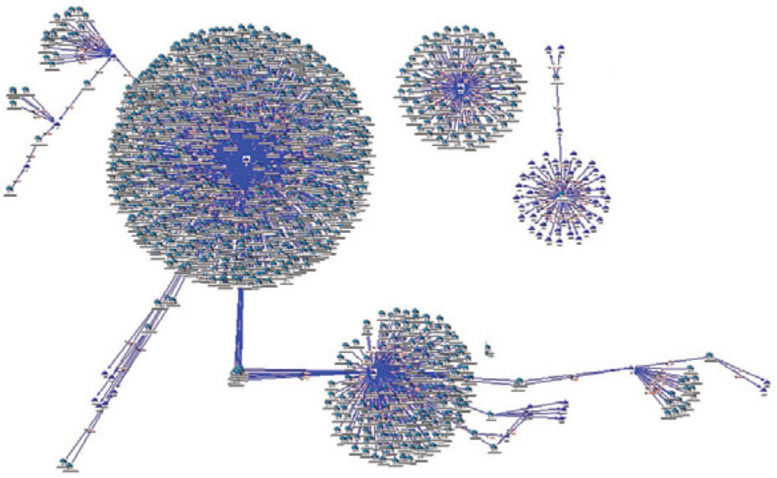

Figure 1: An Analyst's Notebook association chart showing the mapping of complex hacker networks and identifying their Command and Control nodes.

Visualization and search capabilities help uncover hidden patterns and trends

To solve this challenge, Professor Valli's team utilized new modules within Analyst's Notebook to quickly profile the resulting charts and identify signature patterns of suspected hackers. This did not necessarily mean looking for high volume attacks from known IP addresses, but rather analyzing more discrete data. The team looked for the more subtle patterns hidden within the larger clusters.

Standard search functionality such as Find Path, Find Linked and Find Clusters made it easier to identify and isolate the hackers. This allowed millions of records to be quickly grouped into more actionable clusters for more effective targeting.

Client Support Manager Tim Green provided the initial training for the ECU team. "The commonalities between transaction analysis of telephone billings and intrusion logs are strikingly similar – both are date and time stamped and have a source and destination. The techniques we use in law enforcement apply equally to Honeypot analysis. Once you understand the industry-specific requirements it was very easy to apply Analyst's Notebook to this analysis problem."

An analytical approach saves resources and time

The ECU team found that Analyst's Notebook also gave them significant resource savings in their data interpretation. Analyst's Notebook helped enable rapid analysis of the intrusion detection data. During an examination of the distributed denial of service (DDOS) attack, initial hand trace techniques resulted in over 30 hours of work. The same analysis performed using Analyst's Notebook took only 30 minutes to arrive at the same conclusion. When used in conjunction with other tools, the range of analysis available to computer forensics and IT security personnel was greatly extended.

Professor Valli concluded that "Analyst's Notebook is a valuable tool in our analysis arsenal and has saved literally hundreds of hours of work, allowing us to get on with understanding the problem situations presented by log files. The ability of Analyst's Notebook to handle disparate data types from a range of sources surrounding particular entities – which could include firewall logs, intrusion detection system logs, router log files and Honeypot log files – is of great value and hard to match. This allows us to establish an eagle-eye view of the situation which can be very difficult with other analysis tools. Analyst's Notebook even outperforms some dedicated network analysis scripts and tools in its ability to manipulate and interpret the data set."

> *"Analyst's Notebook is a valuable tool in our analysis arsenal and has saved literally hundreds of hours of work, allowing us to get on with understanding the problem situations presented by log files."*
>
> —Professor Craig Valli, Edith Cowan University School of Computer and Security Science

For more information

To learn more about IBM i2, please contact your IBM representative, or visit: **ibm.com**/i2software

To learn more about all of the IBM Smarter Cities solutions, visit: **ibm.com**/smartercities

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America

November 2012

The content in this document (including currency OR pricing references which exclude applicable taxes) is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.