Computer Security

System Monitoring

Presented by:
Larisa Perman
Yevgeniy Gershteyn

03/20/2003

Sources

- http://www.computer.org/students/looking/2002fall/2.pdf
- http://www.spectorsoft.com/

Overview

- Introduction
- Monitoring System Security by New Mexico Tech
- Spector Pro for Windows by SpectorSoft
- Conclusion: How Neural methods can be used for analyzing results of the recorded data

Introduction

- Information system security is a growing concern since computer systems worldwide are becoming increasingly vulnerable due to the rapid increase in connectivity and accessibility that has resulted in more-frequent intrusions, misuses, and attacks.
- In order to determine system security risk, system monitoring should be used to screen users activities (log and usage files).
- The neural networks can be trained with minimized, abstracted user logs for realtime detection of attacks and misuses.

Monitoring System Security

- This system was designed at New Mexico Institute of Technology
- Uses neural networks for misuse and anomaly detection of information systems that include both Unix/Linux processors and web servers.
- Provides real-time monitoring (the neural network based tool runs in real-time or near real-time).
- Cost-effective approach (highly effective in detecting true attacks and minimizing false alarms after proper "tuning").

Anomaly Detection vs. Misuse Detection

- Anomaly detection looks for differences in normal usage behavior of everything from standard running programs, to user behavior.
  - Highly difficult to customize system to system, or even user to user.
  - Discovers new problems (attack methods).
  - Irregular behavior may be counted as attack.
- Misuse detection looks primarily for recognized patterns of attack.
  - Simpler to process and locate.
  - Tends to fail when new attack method are discovered and implemented.

Serial vs. Association Patterns

- In a serial pattern time comes into play, as the features it looks for must be done in a somewhat sequential order.
  - For example: if w and if then x, and if then y, then z. {IF w then x then y THEN z} not equal to {IF y then x then w THEN z}.
- In an Association pattern it is no particular order, but simply is a collection of incidents.
  - If w and x and y, then z is the same as if w and y and x, then z.

7

Information Structure

- For the purpose of training neural networks, the data must be constructed in pairs of input/output
- The input data is taken from several system log files for each user to be processed by a set of rules to form the input for a back-propagation neural network.
- The output is a single value between 1 and 5 that indicates the likelihood that an intrusion has occurred.

8

Input Information (1)

Linux/Unix command (c1-c3) and operating system (c4)

c1	Weight	Each command in the system is assigned by a weight ranging 1-10, where 10 is the highest suspicious command. (*rm ** is higher then *rm filename*)
c2	Average Weight	The average weight of the commands (shows the level of the users intensity to committing an intrusion)
c3	Highest Weight	The weight of the most dangerous command the user has done (used to check if user has violated their access privileges)
c4	Authen-tication Failures	Measures login permission information

9

Input Information (2)

HTTP (h1-h3)

h1	Page Accesses	The number of times a user (IP address) has accessed the system. A measure of intensity.
h2	Page Failures	The number of times a page was not found, access in a restricted location was attempted, ect.
h3	Activities Average Weight	The averaged weight of the activity of the user, and meant to be a preliminary indication of the user's intentions to their current actions. This can also be used to differentiate between a user who accidentally does something that can be considered an attack.

10

Input Information (3)

Fingerprints (or Attack Scenario Patterns)

f1	Number of patterns located	A simple counter value that indicates how many rules were triggered. Rule: *If page x has been accessed a large amount within a small amount of time by the same user, then a pattern has been found.*
f2	Average fingerprint value Weight	An averaged weight of the fingerprints that the rules have located. A measure of intensity.
f3	Highest fingerprint value	The highest value within the rule patterns. A measure of attack likelihood.

11

Attack Fingerprint

- A serial or association pattern that is important in noticing that system security has been violated or in the processes of being violated.
- Example of the difference between a serial and an associative rule:
  - Serial: IF user_x has used the command finger on user_y, and then user_y shows a high degree of failed logins, THEN a pattern has been located with a security level of SL8.
  - Associative: IF (user_x is using su – , or using su root, or accessing restricted files) and user_x is not on the root list, THEN a pattern has been located with a security level of SL10.

12

Output Information

Suspiciousness

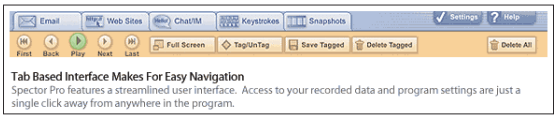
s1	Suspiciousness value	A single value that assigns the user to one of the suspicious levels: LOW – typical user; MEDIUM – review of user activity is needed; HIGH – user activity is suspicious and must be reviewed. ALERT1 – immediate system alert ALERT2 – problematic user such as novice user

NOTE:The single output of the neural network is the Suspiciousness Score.

13

Spector Pro

- Spector Pro is one of the existed applications for System Monitoring for Windows.
- Spector Pro is used for recording every detail of PC and Internet activity for home, office or school.



Tab Based Interface Makes For Easy Navigation
Spector Pro features a streamlined user interface. Access to your recorded data and program settings are just a single click away from anywhere in the program.

14

Spector Pro Features

- Email recording
- Chat and Instant Message recording
- Web Site recording
- Keystroke recording
- VCR-like snapshot recording
- Keyword Detection

All tools record simultaneously, secretly saving the data to a hidden location on the PC.

15

Additional Features

- Scheduled Recording
- Record by User ID
- Keep Recorded Information Hidden
  - Stealth Mode
  - Hot Key Access
  - Password Protection
- Using Spector in a Network

16

Conclusion

- Collected information can be used in neural network model to automate settings for users
- The network has to be trained with enough examples of the monitoring process
- Results can be used to modify user's restriction policy (or to create user's restrictions dynamically based on his/her activities)
- Further step: create a set of rules for each security level

17