Abstract:

Computer security is fairly new and a developing field with a lot of holes in it. Since most computers are connected through the internet, malicious software can easily infect most computers in a matter of minutes. The Computer Security Research Lab aims to increase knowledge of computer security and make it better. Several key issues of computer security are explained along with objectives of the CSRL. Accompanied in this research study are computer security objectives in the CSRL, computer security tactics in the CSRL, the CSRL network setup, descriptions of honeypots, Snort (IDS Sensor) explanation, how to make sense of IDS sensor alerts, specifically using SnortALog, and explanations of the sorted data in the SnortALog report.

Get More Attention: To facilitate the data needs of our research, we must gain a lot of attention. To do this, we created a “virtual” network of honeypots using a honeypot software called HoneyD. With HoneyD, our virtual honeypot computers obtained real IP addresses, allowing them to be scanned and increase our server popularity.

Create Alerts: The Intrusion Detection System (IDS) Sensor we used to obtain security alerts on our network is called Snort. Snort analyzes network traffic with a set of predetermined rules and stores its alerts on a MySQL database when a security rule is broken.

Make sense of it all: Since Snort can create millions of alerts in a short amount of time, we are not able to manually analyze the data obtained from Snort.

CSRL Network Setup:

Servers: Linux Server with HoneyD and multiple web sites. Windows 2003 Server with HoneyD and multiple web sites.

Tap: The tap works like a splitter. It splits the network traffic between the servers and the “outside world” allowing the traffic to be routed undetected through the snort sensor. This allows the snort sensor to analyze the traffic without being detected by “Black-hats.”

What do Honeypots do?

Honeypots are bait computers. If someone is trying to access a honeypot computer, that only means one thing, there is an intruder. Honeypots can be real computers filled with data that appears to be credit card numbers or something worth taking. Some honeypots are created by software designed at simulating “real” computers. This is done by honeypot software by allocating unused IP addresses in the area and assigning them to honeypot computers. A black hat will then scan the internet for computers. The sophisticated thing about HoneyD, honeypot software, is that it will reply to requests as a “real” computer would.

What does Snort do?

Snort is an Intrusion Detection System aimed at alerting a user about malicious behavior lurking about, via e-mail or by storing the alerts on a database. Snort monitors the traffic in the computers Ethernet card. Snort is software and generates alerts based on previous malicious criteria saved as snort rules. These rules are not perfect. They may create false alarms or not detect intrusion at all.

SnortALog:

SnortALog is a program that takes snort log files as input and outputs a HTML report with pie charts, graphs, and sorted data tables. These reports are easy to read and help interpret snort alerts.

Popular Protocols: From three SnortALog reports generated using snort logs from three production machines in the CSRL, we found PIM being the most popular protocol consisting between 50% - 80% of event activity. The popularity of PIM is due to its ability to lead to more research. (PIM) = Protocol Independent Multicast.

Severity of Events: In another category of events labeled severity, we found 80% - 90% of the activity was of medium severity and 10% - 20% being categorized as low severity. We were perplexed as to not finding any high severity events.

Projects by Resources: In the number of events by hour category we found that during the summer months of captures data, suspicious behavior peaked at 6 am PST. We were also shocked when both Linux servers had almost identical graphs reflecting the number of events per hour. They varied from the Windows server. We concluded that maybe Linux machines get attacked selectively, or vice versa.

Projects by Destination: In the last category we will analyze, the Distribution of events by destination, we found our most dangerous data. 70% - 90% of suspicious activity had occurred in port 161. “Port 161 = Simple Network Management Protocol (SNMP) which provides a “machine-to-machine” facility allowing one computer to interact with another. This allows attackers to exploit computers.” [8] We concluded that Port 161 is a vulnerability and should be shut down immediately.

References:

[6] We concluded that Port 161 is a vulnerability and should be shut down immediately.

Computer Security Research Lab

Project funding title: “Information Fusion in Sensor-based Intrusion Detection Systems.”

Funded by: National Geospatial-Intelligence Agency

Goal: The goal is to establish a security laboratory, design a new model for information fusion in sensor based intrusion detection systems and analyze the behavior of the system in common applications.

Project Steps:

1. IP setup.
2. Secure Linux.
5. Setup servers.
6. Refine generated IDS algorithm.
7. Setup honey pot.
8. Incorporate GUI.

Computer Security Research Lab Objectives:

Obtain Data: Obtain data from snort alerts via allowing black hats to scan / attempt to compromise computer.

Analyze alerts: Distinguish between real alerts and false positives.

Improve Snort Rules: Improve IDS rules to reduce false positives and create new alerts that might have been missed previously.

Computer Security Tactics in CSRL

Get Attention: In order to obtain data, we must increase traffic to our servers. One way of doing this is to create dummy websites. Dummy websites offer services or entertainment to internet users which help gain attention.

SnortALog is used to make sense of IDS sensor alerts generated by Snort. Snort can create millions of alerts making it impossible for users to figure out what exactly is happening in the network traffic. SnortALog aims at making sense of all the snort alerts. SnortALog is a program that takes snort log files as input and outputs a HTML report with pie charts, graphs, and sorted data tables. These reports are easy to read and help interpret snort alerts.

SnortALog:

SnortALog is a program that takes snort log files as input and outputs a HTML report with pie charts, graphs, and sorted data tables. These reports are easy to read and help interpret snort alerts.

SnortALog:

SnortALog is a program that takes snort log files as input and outputs a HTML report with pie charts, graphs, and sorted data tables. These reports are easy to read and help interpret snort alerts.

SnortALog:

SnortALog is a program that takes snort log files as input and outputs a HTML report with pie charts, graphs, and sorted data tables. These reports are easy to read and help interpret snort alerts.