GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

DRAGON – An Intrusion Detection System

Introduction

How any other tool for Intrusion Detection, Dragon is a good cost-effective option. Dragon is a Network and Host IDS basically composed by these products: Dragon Sensor, Dragon Squire and Dragon Server. In this document, I will present some information about all components that composed Dragon.

Dragon

The Dragon solution includes three basic building blocks. These are Dragon Sensor, Dragon Squire and Dragon Server.

- Dragon Sensor is a network IDS that works on Linux and/or Unix. It monitors network packets for traffic that may indicate network misuse and/or abuse.

- Dragon Squire is a host based IDS. It monitors key system files for evidence of abuse and can also receive security information from routers and firewalls via SYSLOG or SNMP.

- Dragon Server manages data from all of the Dragon Sensor and Dragon Squire engines. Based on Linux it also provides several real times, forensic and trending web based interfaces for event analysis.

© SANS Institute 2000 - 2002, Author retains full rights.

Dragon Sensor

Dragon Sensor monitors live network packets and looks for signs of computer crime, network attacks, network misuse and anomalies. When it observes an event, the Dragon Sensor can send pages and e-mail messages, and then take action to stop the event and record it for future forensic analysis.

For signature selection, you can choose from over 1500 signatures. To be updated with new signatures go to https://63.210.52.6/. All Dragon events are categorized into suspicious, probe, attack, compromise, success, failure, virus, collection and maintenance groups. While other NIDS concentrate on attack and probe detection, the Dragon Sensor can usually collect enough evidence to indicate if an attack has succeeded or failed. These groupings are key to reducing false positives.

Dragon Squire

Dragon Squire is a host-based intrusion detection and firewall monitoring system that looks at system logs for evidence of malicious or suspicious application activity, and monitors key system files for evidence of tampering in real time. Dragon Squire has been tuned to prevent high load levels and minimize any negative system impact to a server's performance. Besides being an excellent system security tool, Dragon Squire can also analyze firewall logs, router events and just about anything that can speak SNMP or SYSLOG.

Dragon Squire's signature library includes suspicious events from a wide variety of operating systems. These events check for suspicious file transfers, denied login attempts, physical messages (like an Ethernet interface set to promiscuous mode) and system reboots. The library also includes security messages from many applications and services such as Secure Shell, Sendmail, Qmail, Bind and Apache Web servers.

Dragon Squire is a complement to the Dragon Sensor network IDS. There are many network attacks (such as web attacks sent over an SSL connection) which the Dragon Sensor (or any other NIDS) cannot observe. Correlating these host and network events (along with firewall information) is accomplished at the Dragon Server.

Dragon Server

It provides an engine management, event alerting, analysis and correlation. Dragon Server facilitates secure management of all Dragon Sensors and Dragon Squires. It also aggregates all alerts into one central database so that disparate attack information can be correlated. The Dragon Server includes a variety of reporting and analysis tools as well as the ability to customize alerts via e-mail, SNMP or SYSLOG messages.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Dragon Sensor Architecture

Dragon Sensor is a network packet based intrusion detection system. It collects network packets and analyzes them for a variety of suspicious activities. This suspicious activity may indicate network abuse, probes, intrusions or vulnerabilities. Dragon Sensor is highly configurable and extremely fast. Multiple Dragon Sensors can operate jointly to provide enterprise coverage of complex networks.

Dragon Sensor focuses on network performance and the collection of forensic evidence. A variety of analysis tools are included to process collected data. For example, these tools sort through the collected data and produce flat log files, summary information, activity graphs and rebuild network sessions for inspection.

Dragon Sensors take two configuration files named dragon.net and dragon.sigs which control what type of network traffic and event data is logged to the hard drive. The dragon.net file controls basic Sensor configuration, IP/TCP/UDP header anomalies, port scan/sweep detection, policy driven events (such as finding new web servers), filtering, SNMP alerting and protocol reconstruction. The dragon.sigs file specifies unique network patterns which may indicate probes, attacks and compromises and many other types of network abuse.

The Dragon Sensor basically logs to the hard drive because the component of the Dragon Sensor/Squire/Server architecture which enables enterprise communication is a client/server program named Dragon Rider. For a Dragon Sensor being managed from a Dragon Server, a Dragon Rider Client program would be placed onto the Dragon Sensor. The Dragon Rider Client program watches all new event information being added to the Sensor's event log and sends new events to the Dragon Server. If the Server has new configuration information, the Dragon Rider Client will receive it and then restart the Sensor with the new configurations.

The only other file that is required by Dragon Sensor at start up is a 'key' file. This file, named dragon.key, performs license management. The dragon.key file is tied to a specific set of Dragon functions. These are Dragon Sensor, Dragon Squire and Dragon Server. A key file will contain one or more hostnames which have been authorized to become a Sensor, Squire or Server. All software can be installed on the same system, but the key has to reflect that.

A Dragon Sensor can be configured to be 100% stand-alone. That is, a Sensor can be deployed such that no IP stacks on any of it's network interfaces exist. In this case, the box must be managed from the physical console, or through a remote terminal server. In many cases, Sensors are deployed with one interface utilizing an IP stack, or two interfaces with only one IP stack. On any open network interface, it is highly recommended to secure the operating system before installing the Dragon Sensor. Assuming that the box will only be administered by a small number of people, the focus should be on disabling remote services such as Sendmail and Telnet. If tight host based security is desired for the Dragon Sensor platform, consider deploying OpenBSD.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Dragon Squire Architecture

Dragon Squire is a Host-Based IDS (HIDS) that can be run standalone or fully integrated into the Dragon Server architecture. Events can either be stored locally on the HIDS machine or forwarded to the Dragon Server and reported via the Dragon Fire interface. In either configuration Dragon Squire can generate SNMP traps for designated events. When storing the events locally, a set of the Dragon command line tools is stored on the machine to provide reporting and analysis capabilities.

Squire's capabilities include the following:

FILE CHANGE MONITORING

Files can be defined in the Dragon Squire configuration file (dsquire.net) by specifying a name of a file and the full pathname to the file. For each defined file, many attributes can be monitored like: MD5 Hash Values, File Permissions, File User Ownership, File Group Ownership, Inode Values, File Deletion, Truncated Files, Growing Files and Modification Time Changes
These file definitions help to comprise a security policy for each Dragon Squire. Security policies can be maintained via the Dragon Server web interface.

SIGNATURE PROCESSING

The contents of log files can be scanned to alarm if specified signature patterns occur. This is configured by specifying a FILE_FORMAT describing the record layout for a defined file and then defining signatures that pattern match within the FILE_FORMAT. The dsquire.net file contains the list of files to be monitored and their log formats, and the dsquire.sigs file contains a list of signatures which are to be applied to each file.

SERVICE MONITORING

On Linux platforms, specific TCP and UDP services can be monitored to generate events as services are started or existing services are terminated. The 'proc' file system is monitored for notification of network service starts and terminations.

SNMP MONITORING

Dragon Squire can also listen to a stream of SNMP traps from a variety of devices. The SNMP traps may be from firewalls, from routers or from any other type of device which can generate a trap. Signatures can be written for application to the received SNMP traps. This allows Dragon Squire agents to monitor a variety of network devices.

Dragon Squire operates with the Dragon Server through the use of the Dragon Rider Client which operates in a 'diskless' mode. By diskless, we mean that as long as the network connection to the Dragon Server is present, detected events flow immediately to the Dragon Server.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Dragon Server Architecture

The Dragon Server is the "hub" of all enterprise security operations for the entire Dragon products. It can control many Dragon Sensors and Dragon Squire engines. It receives information from them and presents the information for alerting and analysis to Dragon administrators. The Server is also the focal point for all configuration management of each engine. When administrators change an engine configuration, the Dragon Server will push the policy out to the modified Dragon engine.

The major features of Dragon Server are:

Centralized Network IDS, Host IDS, Firewall and Network Monitoring

The Dragon Server brings event centralization to the both the Dragon Sensor and Dragon Squire products. Since Dragon Squire can monitor log feeds from many major firewall vendors and several major network components (such as routers and DNS servers), correlation of security events across all of these platforms provides a complete security picture.

Encrypted Event Centralization

All Dragon Squire and Dragon Sensor engines can have their events centralized to the Dragon Server. This process is accomplished through the use of a single BLOWFISH encrypted TCP connection. BLOWFISH is an extremely fast encryption algorithm. Filters can be placed at each Dragon engine such that only certain types of event data get forwarded to the Server.

Engine Management

All Dragon engines can be managed individually or in groups. This makes management of large numbers of engines very easy. Also, all management is accomplished through a web interface which can be secured with any SSL web server.

Custom Signature Management

The Dragon Server maintains several databases of known malicious network traffic. Dragon Server administrators can write their own signatures and create their own custom signature libraries. All signature management is accomplished through a web interface and hooks are in place to link to online resources from CERT, Bugtraq and the CVE project.

Live Signature Updates

Enterasys constantly monitors a variety of online security resources and quickly writes Dragon Sensor and Dragon Squire signatures when new security threats are published. Enterasys also conducts a variety of R&D efforts to produce entire libraries of signatures which attempt to detect new varieties of misuse. Any Dragon customer who has purchased a Dragon Sensor license can subscribe their server to automatically download new signatures from Enterasys.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Dragon Server Web Components

Dragon Server Web Interface

This web server interface is dedicated to management of the Dragon engine configurations and will also monitor the performance of the engines as well. It is based on a combination of CGI-BIN PERL scripts and works with the Apache web server. Security can be enhanced by using an SSL version of the Apache web server.

Dragon Fire

The Dragon Fire interface is also a set of CGI-BIN PERL scripts which can analyze events collected at the Dragon Server. All analysis is performed on each day's logs. Suspicious events can be correlated, sessions can be replayed and many other forms of analysis are available as well.

Sorcerer

The Sorcerer application is a trending tool. It requires an SQL database to perform long term storage of Dragon events. The web server interface to Sorcerer is also a set of CGI-BIN PERL scripts which perform database queries to display trending information. The database can be kept entirely on a separate system which may increase performance.

Alarmtool

The Alarmtool is used to send SNMP traps, SMTP emails, SMTP pages, SYSLOG messages, or execute commands based on a policy. The policy is defined through a custom web interface which generates a configuration file. The 'alarmtool' program receives events at the Dragon Server and then alerts the Dragon dministrators.

Dragon Console

Because Dragon Server databases can grow to extremely large sizes, using the Dragon Fire interface can become very slow. The Dragon Console allows Dragon administrators to analyze events as they occur in real time. Several web interfaces, similar to Dragon Fire, exist to help organize the recent events and make a variety of displays in real time. No event detail, such as packet payload, is available, but up to 2,000,000 events can be stored in memory at one time. For large networks, this may be 2-5 days of typical event traffic. For small networks, this could be several months worth of traffic.

© SANS Institute 2000 - 2002, Author retains full rights.

Conclusions

Security is possible, using the most up to date tools that are available, to protect against virtually every type of threat that is currently known about. Unfortunately, new threats and security holes in some software package or another are being discovered on a daily basis.

It is important in any environment to know what types of threats you might be facing. Be aware of any potential security holes in your system, and take care to prevent attacks against these.

The Dragon tools and signatures are regularly updated to include information about new threats as they are discovered, however it is important to keep up to date with the latest version of these files.

References

1. Dragon Intrusion Detection
   http://www.enterasys.com/ids/

2. Intrusion Detection, Theory and Practice by David "Del" Elson, March 27, 2000
   http://www.securityfocus.com/frames/index.html?focus=ids

3. Ron Gula, Why Dragon ?, 1999
   http://www.securitywizards.com/intro.htm

4. Documentation for Dragon Sensor
   https://63.210.52.6/sensor/index.html

5. Documentation for Dragon Squire
   https://63.210.52.6/squire/index.html

6. Documentation for Dragon Server
   https://63.210.52.6/server/index.html

© SANS Institute 2000 - 2002, Author retains full rights.