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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Cynthia Williams
Course: Security Essentials Level One
Title: Security Mechanism of Intrusion Detection System: RealSecure

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

Security Mechanism of Intrusion Detection System: RealSecure

Businesses have lost productivity and millions of dollars for not having a secure network. A variety security products such as firewalls, scanners to conduct vulnerability assessment, and intrusion detection systems are available for businesses to use to protect their internet from attackers. Although all these tools serve a purpose in protecting the internet, my focus will be on the importance of intrusion detection systems, especially RealSecure.

Firewall products are echoed throughout the Information Technology Industry as excellent security tools for businesses to use to ward off attackers from penetrating their network. Firewalls allow authorized users into the network and lock out unwanted or unauthorized users. But, can firewalls do the job alone? I don't think so. Firewalls can not protect the network from malicious activities happening inside the network. For example, a firewall cannot protect the network from disgruntle or incompetent employees who wants to do harm to their company's network. What happens if a system administrator has been fired from job and still able to access the network because of root privileges? He or she has access to user IDs, passwords, users and systems files and directories. Then, there are your attackers who can get through firewalls by coming through modems and routers, or as a result of bad firewall configuration. He or she can cause denial of service, create a virus in the system, steal legitimate login IDs and passwords, for instance. Although businesses do not want to admit it because of embarrassment, these instances have happened. Millions of dollars have been lost as a result of these attacks. Therefore, firewalls alone cannot stop all attacks, especially attacks occurring inside the network.

Additional safeguards are needed to protect the network. Internet scanners used to conduct risk assessments provide a different twist in protecting the network. Businesses can conduct vulnerability assessment to look for vulnerabilities in their network and correct them before an attacker finds them and causes havoc to the network. This tool which consists of a database of known signature attacks is tried out against a network. This tool generally features vulnerability fixes as well as other countermeasures. Internet Security System internet scanner, for example, consists of over 700 known signature attacks. It looks for vulnerabilities and present fixes across several platforms. Scanners as vulnerability assessments can detect security vulnerabilities in areas such as passwords, misconfigured software, server buffer overflow, and open ports, for example.

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

The third security device I'll address in detail is the intrusion detection system, especially RealSecure. The purpose of an intrusion detection system is to build usage patterns of a normal system and triggers an alert when abnormal patterns or anomalous activities are detected. Intrusion detection systems can consist of three segments.

Intrusion detection system can be host-based product. In this case, intrusion detection system can reside on hosts, workstations, or servers. It monitors operating systems and audit logs on Window NT and UNIX. If evidence of anomalous activities are detected security administrator is notified. Host-based products can audit system activities down to its minute level. It can detect changes in system files, can tell you who is accessing files and what kind of files are being accessed. It can tell you when users login and out of workstations. If an attacker tries to install potential malicious codes such as the viruses and software such as back doors they can be detected using known signature attacks.

An IDS can also be a network-based product. In this instance, an IDS performs real-time monitoring of network traffic. It looks at package headers traveling across the network to looking for attacks. It can look into packets and reveal malicious code such as backdoor attacks. It can detect denial of service attacks, buffer overflow, viruses, system of configuration changes, for example. The selling point of a network-based IDS is that it monitors traffic in real time, response to attacks in progress, and provides fast notification to security administrators, which can prevent serious damages from occurring to the network.

The third type of IDS is called hybrid. IDS as a hybrid includes both host -and network-based product, and features a risk assessment component. This I learned from a previous security class. Internet Security Systems' RealSecure falls in this category. Although ISS Internet Scanner is not a component of RealSecure, it is a product of ISS and can be purchased with RealSecure. ISS Internet Scanner will be discussed briefly.

This now brings me to the intrusion detection system I specifically want to discuss, and that is RealSecure. RealSecure is the first integrated network- and host-based intrusion detection and response system in the Information Technology industry. What I like about RealSecure is that it consists of the three comprehensive security segments which include: the RealSecure Manager; RealSecure Engine, which is now called Real Secure OS; RealSecure Agent which is now called RealSecure Network Sensor. I will briefly discuss, RealSecure Server Sensor, a new critical component of RealSecure, that just recently hit the market.

RealSecure Network Sensor operates on devoted workstations looking for abnormal usage patterns or anomalous activities. It also sends a response alerting sites of abnormal activities. RealSecure Sensor watches packet traffic traveling over the network looking for attack signatures, which is an indication that an intrusion is underway. If the network sensor detects unauthorized activity, it canbe configured

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

to terminate the connection, send email or pager alert to system administrator of an attacks or possible attacks. This tool allows reconfiguration of firewalls or other user-definable actions. It also can send an alarm to the RealSecure Manager, which I will discuss shortly or a "third-party console for administrative follow-up and review."

RealSecure OS is a host-based product that complements the RealSecure Network Sensor. The sensor provides information not available in real-time environment. Each sensor is installed on a workstation or host and examines logs looking for attacks, and analyzing whether the attack was successful or not. RealSecure OS can be configured to prevent further attacks by terminating user processes and suspending user accounts. It also can send alarms, log events, sent traps, send-emails, and execute user–define actions.

The RealSecure Manager is delivered with the RealSecure Network Sensor and RealSecure OS. It's a management console that monitors and report the activities of the RealSecure OS and RealSecure Network sensor. The report provides security assessment of the network and can be administered from a single location. It is also "available as a plug-in module for a variety of network and system management environments."

The new RealSecure Sever Sensor I mentioned earlier is a combination of host- and network- based intrusion detection system. It resides specifically on the server. It audit kernel-level logs, examine applications, and monitor inbound/outbound network traffic. It can detect and block intrusion before they reach the operating system or application. This product can provide protection across an encrypted and high-speed network traffic. This product allows organizations to create their on blocking rules authorizing users assess to server or entrance through the firewall. A component incorporated in this product called SecureLogic minimize false positives by analyzing possible attacks between the time of the occurrence and when alarms are generated.

RealSecure can monitor a wide range of networks such as ethernet, fast ethernet, and token ring, for example. It provides one of the widest ranges of attack pattern recognition. It can monitor windows network and TCP/IP traffic. It can monitor traffic providing security coverage without delaying network traffic stream. It can detect e-mail, web and probing attacks, FTP and popular service exploits, and unauthorized network traffic, for example. It provides a comprehensive easy to read reports where you do not have to be a security administrator expert to read it. "It provides around-the-clock surveillance looking for attacks and responding to suspicious activity. It can intercept and respond to internal or external host and network abuse before systems are compromised "or damage is done. In a real-time situation, it can respond to network attacks by session termination and firewall reconfiguration.

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

ISS allows the flexibility of purchasing either the host or the network-based product or both segments at a discount. The cost of RealSecure as of March 2000 was $8,995.00. This is not too expensive if you are securing a large network. Purchasing only the hosts can be a lot more expensive if you are securing large network. Discounts are also provided if your organization already using one of its products. RealSecure Server Sensor cost $900. However, customers using RealSecure OS Sensor can purchase product at a discount of $225 per sensor.

What I like about RealSecure is that it is one of the most comprehensive IDS security tools available in the IT industry. Because it's both a network- and host-based product it provides added security protection avoiding serious damage or attacks to the network. With RealSecure Sever Sensor on the market, ISS has taken itself the next level of monitoring inbound/outbound network traffic to and from the server at multiple levels.

Although not endorsement by National Security Agency, RealSecure is on its Intrusion Detection Inventory List. NW Fusion Magazine named RealSecure as the product of the year in 1998. Network World reported that RealSecure had over 50% of the intrusion detection market in 1998. But more impressive, ISS received the Codie award in 1999 for RealSecure -- the best network intrusion software. This is one of the highest honor possible in the software industry where IT professionals are recognized by their peers.

The levels of security tools chosen by an establishment depends greatly on the organization's budget, security policy, the classification level of data on the network. Nevertheless, there are cheaper products available that one can purchase to protect their network. One thing most security professionals will agree to is that there must be many levels of defense to protect the confidentiality, integrity and availability of information on the network. I selected RealSecure because of the protection if provides to the network. Another reason I selected this product is because of all the accolades it has received from the IT industry in general. Plus, my agency and I use the ISS scanner to conduct vulnerability assessments and RealSecure looks for the same vulnerabilities.

Reference:

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

Internet Security System, Intrusion Detection System (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/ (12 October 2000)

Internet Security System, Intrusion Detection: RealSecure Manager (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_manager/ (12 October 2000)

Internet Security System, Intrusion Detection: RealSecure Manager (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_networksensor/ (12 October 2000)

Internet Security System, Intrusion Detection: RealSecure Network Sensor (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_networksensor/ (12 October 2000)

Internet Security System, Intrusion Detection: RealSecure Network Sensor (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_networksensor/ (12 October 2000)

Internet Security System, Intrusion Detection: RealSecure OS Sensor (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_ossensor/ (12 October 2000)

Internet Security System, Intrusion Detection: RealSecure OS Sensor (1994-2000). URL: http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_serversensor/ (12 October 2000)

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

Internet Security System, Intrusion Detection: RealSecure OS Sensor (1994-2000). URL: http://www.iss.net/cgi-bin/dbt-display.exe/db_data/press_rel/release/101100285.plt (12 October 2000)

Software Information Industry Association, 1999 Codie Award Best Network Security Product: ISS RealSecure. (2000) URL: http://www.siia.net/ (click on upcoming events, then click on Winner Circle" at buttom right hand corner of the page) (13 October 2000)

Henderson, Tom, "RealSecure: Looking For Trouble." Network Magazine.Com (10 October 1998). URL: http://www.networkmagazine.com/article/NMG20000509S0028 (15 October 2000)

Messmer, Ellen. "ISS To Give Managers That RealSeure Feeling." Network World Fusion. (02 July 1999). URL: http://www.nwfusion.com/news/1999/0702iss.html (11 October 2000)

Messmer, Ellen. Getting The Drop On Network Intruders." Network World Fusion. (4 October 1999). URL: http://www.nwfusion.com/reviews/1004trends.html?nf (11 October 2000)

Messmer, Ellen. Intrustion Detection: A Matter of Taste." Network World Fusion (27 September 1999). URL: http://www.nwfusion.com/buzz99/buzzintel2.html?nf (11 Oct 2000)

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