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

A Systems Security Case Study – From Research to Implementation

Keh Hong Guan
March 2003
GSEC version 1.4b, Option 2

Introduction

The maintenance and design of a security is always a challenge for a security administrator, especially if it is an existing infrastructure that was inherited from the previous administrator. The purpose of this paper is to discuss the methods and procedures used to evaluate the existing security infrastructure for security risk and enhanced the environment

Overview (Before)

A wholly subsidiary of my company (Company A), is a payment gateway/content provider for another sister company of ours (Company B), which is a mobile service provider. As a payment gateway/content provider, it is important to have a good security infrastructure. Sensitive data, such as credit card numbers flowing from the mobile service provider to the backend systems are at risk if not properly managed, e.g. financial institutions.

I was asked by the management of company A to evaluate the security risk hazard on the existing infrastructure, and implement strategies to enhance the security based on the risk found.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Background

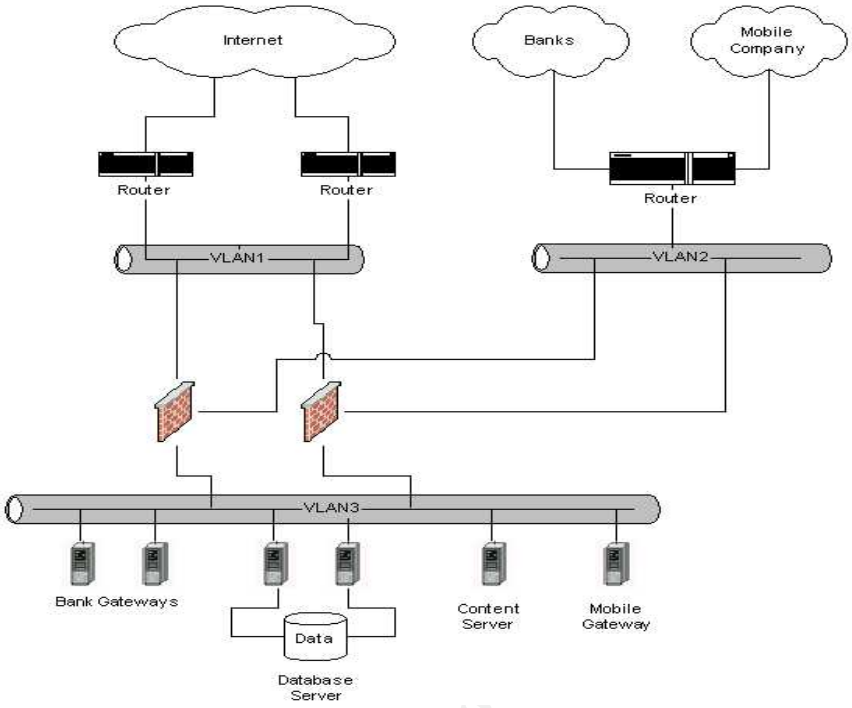

Figure 1

The existing network was a flat network as shown in Figure 1. Basically there are 4 categories of servers involved:

- **Mobile Gateway**. Running on Solaris platform with customize application, this server provides the data bridging from company B to various gateways listed as below, depending on the service the data carries

- **Content Server**. A Windows 2000 Server with Microsoft IIS service (FTP) and in-house windows based application hosts non-critical information, e.g. movie schedule, currency exchange, etc. Data which are stored here are either gathered thru the Internet by the in-house application or provided by third-party via FTP. The data are also pumped into the database server for other services used.

- **Bank Gateway**. A Windows 2000 Advanced Server running Microsoft IIS service (WWW), Microsoft Messaging Queue (MSMQ), and in-house windows based application hosts as a gateway to banks. Messages forwarded by the Mobile Gateway to the IIS service will be processed by the ASP page and put into the MSMQ to be process by the in-house application, which will then be sent to the bank. A single bank gateway is connected to a single bank only.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- **Database Server**. A pair of servers running on Windows 2000 Advanced Server running as a Domain Controller (DC) with Microsoft Cluster Services (MSCS) installed provides Oracle database services under Oracle Failsafe Services. It hosts various database for storing information used by Content server and Bank Gateway.

Risk Analysis

Risk analysis on current situation is important to identify the threats or vulnerabilities. A check on the existing infrastructure lets me conclude that a lot of problems exist in the system in terms of architecture design and security standpoint exists. Specifically:

- **Single Point of Failure (SPOF)**. There are multiple occurrences of single point of failures in the architecture at the network and system level. At the network level, all connections except to the Internet terminate at a single and shared router. All network VLANs are created on a single switch only with no redundancy path. At the system level, certain servers like the bank gateway have only a unit that will communicate with a single bank. Another point to mention that all of the servers have only one network connection.

- **Minimal security protection**. As seen in the network diagram above, the only protection to all the servers are a pair of firewall, which interconnects the network to the mobile service provider, Internet, and banks. If attackers have compromised the firewall, the whole network will be in jeopardy.

Based on the analysis report, the management decided to revamp the entire infrastructure to align with the current business strategy. Certain constrains have been brought up by the management of company A regarding the newly design architecture:

- **Minimal impact on availability**. The management stressed out that no outrage would occur.

- **Budget constrain**. The budget allocated for this exercise was minimal because the management did not foresee purchasing additional equipment.

Implementation Stage (During)

The implementation of the new infrastructure design was separated into 3 stages to reduced downtime and also easier to recover if problem occurs.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Stage 1: Redesign network

The first stage of the implementation is to restructure the network equipments and servers to a better security environment in addition to remove single point of failures for each component.

One of the SPOF that we eliminated was the connection to the banks and mobile service provider as shown in Figure 2. By implementing a second router, it removes the single point of failure for network connectivity to both the parties in case of hardware failure or bandwidth flood caused by attacks (E.g. DoS or other attacks).

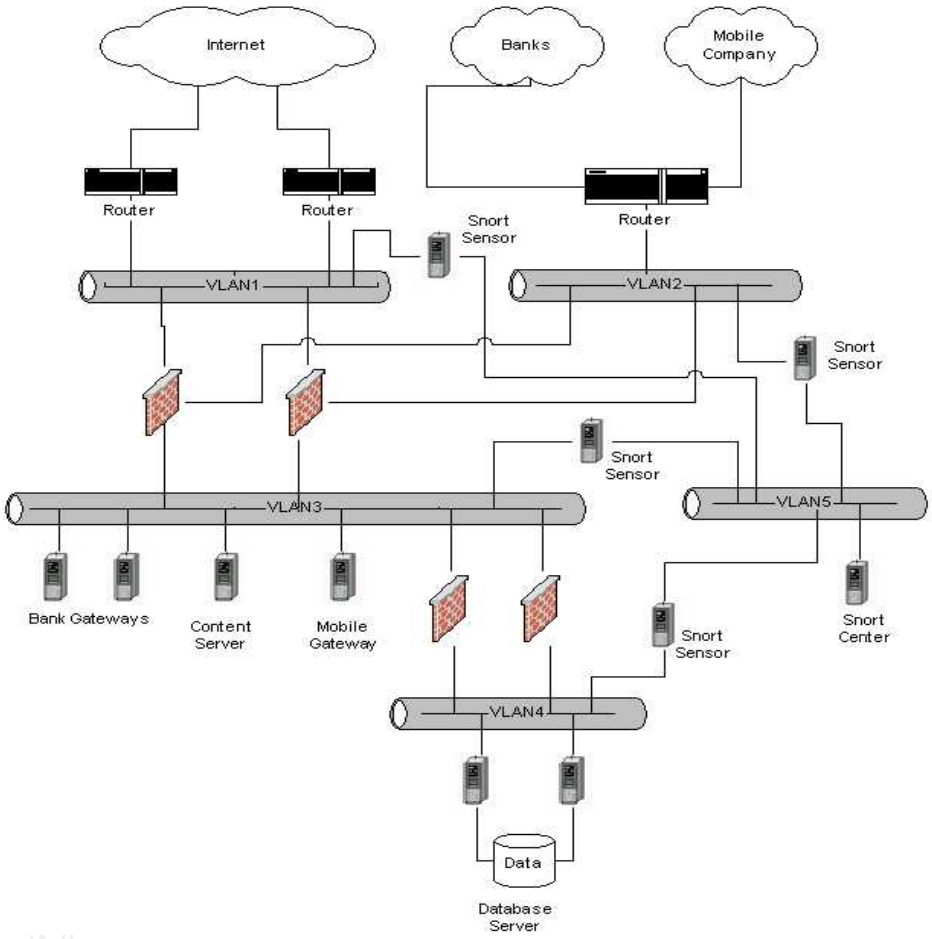

Figure 2

As for systems, we installed a second Network Adapter (NIC) to each server and configure Adapter Fault Tolerance (AFT) on both the Network Adapter using Intel's Advanced Network Services. By implementing this configuration, the system will provide a redundancy path for each server. This will reduced the downtime and increase availability.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A new VLAN (VLAN4) is created on the switch to cater the Database Server, which I found was quite insecure if located on the same network as the rest of the server (VLAN3) as it contains sensitive data. Deployment of a new set of firewall was also done for communications between VLAN3 and VLAN4 to restrict unauthorized access to the database server. NetScreen firewall was chosen because of 2 reasons:

1. **Budget constrain**. We evaluated a number of firewalls on the market, such as CheckPoint appliance-based firewall, NetScreen, and Cisco PIX firewall. I found that NetScreen would be a better choice based on the performance, the price, and also because it suites the current environment that the company has.

2. **Different vendor**. The current perimeter firewall that exists on the network was a CheckPoint appliance-based firewall. By using a different firewall, it can prolong time for attackers to access to the network behind the firewall because the vulnerability will be different than the perimeter firewall, e.g. vulnerabilities found in CheckPoint might not be a threat for NetScreen firewall.

Restriction of intranet network communications to VLAN3 has been place by terminating to the new firewall deployed. The original design does not have any security in-place and full access was given to everyone in the intranet network. With the new design, access control can be placed to prevent unauthorized access to the servers.

Stage 2: Secure individual components

The next stage is to secure each individual network equipments and servers. Although the network design has been changed to provide a better environment, it doesn't mean that network equipments and servers are vulnerability-free and secure from attacks. Lets look into each component in the network:

Perimeter Routers

All perimeter routers selected were Cisco routers running on the current version of IOS Release 12.2(16). Updates on the Cisco IOS software should be done when a new version is released to resolve vulnerabilities found on the previous version. In addition, new features are also included in some of the software released e.g. IPv6 feature was supported on IOS Release 12.0(21).

Other steps that I took to secure the perimeter routers are as follow:

- **Access Control List (ACL)**. Using an access control list (ACL), I restricted network flow in and out of the network by allowing required protocols, IP addresses and ports, and that deny everything else. I've also included all private IP address block like 0.0.0.0/8, 10.0.0.0/8,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

169.254.0.0/16, 172.16.0.0/20, and 192.168.0.0/16 from external (or known as untrusted network) because all these addresses are private addresses.

- **Disable unwanted services**. A standard Cisco router configuration has a number of unwanted services running by default. By allowing those services to run, an attacker can exploit the router by using the vulnerability of the services. Below are the services that I disabled on all the perimeter routers in my environment (commands are in brackets):
    - TCP small services (*no service tcp-small-servers* & *no service udp-small-servers*)
    - Cisco Discovery Protocol (CDP) (*no cdp run*)
    - Finger (*no service finger*)
    - HTTP server (*no ip http server*)
    - BootP server (*no ip bootp server*)
    - SNMP (*no snmp-server*)

- **Secure interfaces**. All interfaces on routers can be configured to be more secure using certain commands available thru the Configuration Interface mode (commands are in brackets):
    - Disable IP-directed broadcasts at router to prevent Smurf attacks (*no ip directed-broadcast*)
    - Shutdown unwanted interfaces (*shutdown*)

- **Enable access password with MD5-based algorithm**. By issuing the command *enable secret [password]* in the Configuration Interface mode, the console password will be encrypted with MD5-based algorithm. Although this command is issued, password will still be displayed on the configuration file when you display it. Issuing *service password-encryption* will keep passerby from reading the password when the configuration file is open.

Firewall

The new network architecture features 2 types of appliance-based firewall, a pair of them running CheckPoint and another pair is a NetScreen firewall.

On the CheckPoint appliance-based firewall rules, allow only outbound on port 80 to the Internet and port 21 for inbound from the Internet for Content Server. As for Bank Gateways, allow port 80 for inbound from Company B and port 80 for outbound to banks. Port 80 is the only inbound port allowed from Company B to the Mobile Gateway.

Rules on the NetScreen firewall are much simpler. The only rules that configured on NetScreen firewall are allow port 1521 on inbound for Content Server and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Mobile Gateway to the Database Server, and any ports on inbound port for certain machines in the intranet network to VLAN3 and VLAN4.

Servers (General)

Securing Mobile Gateway (Solaris)

Due to the nature of the Mobiel Gateway, I can't do any much of hardening the machine because of the implementation of the software installed by vendor which I've totally have no idea how the mechanism work, and also no proper documentation left by the previous enginner who left the company.

Certain basic steps have been done to the extend of my knowledge on the system:

- **Apply Service Packs**. Applying service packs recommend by SUNSolve homepage on the gateway will protect it from known vulnerabilities.

- **Disable unnessesary services**. Non-used services like FTP, TFTP, and printer services are disabled on the system.

- **Miscellaneous security fixes**. There are a few fixes that can be done to secure the Solaris operating system:
    - Set the TCP initial sequence number generation parameters by inserting this command in /etc/default/inetinit: **TCP_STRONG_ISS=2**.
    - Set the following setting to protect against buffer overflow attacks in /etc/system:
      set noexec_user_stack = 1
      set noexec_user_stacklog = 1
    - Restrict root logins to console only by inserting the following into /etc/default: **CONSOLE=/dev/console**

Securing Windows-based Servers

There are a lot of baseline guides on hardening a Windows-based servers (Windows NT4 & Windows 2000) on the Internet. Based on all these guidelines, below are the checklists that I've applied to all the Windows-based servers in the network:

- **Install the latest Service Packs and Post Service Packs**. The current Service Pack version for Windows 2000 is Service Pack 3. Up to the current time, there are at least 22 post Service Packs available on Microsoft Security Bulletin for download to resolve security vulnerabilities, program fixes and enhancements.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- **Install latest Internet Explorer**. Although servers are not supposed to be used as a browsing, certain libraries in Internet Explorer are used in the customized application. The current version of Internet Explorer available on Microsoft is Internet Explorer 6 SP1. The current Hotfix for Internet Explorer is under Microsoft Support Knowledge Base Article ID 810847 and 813951.

- **Configure Audit Policy**. Audit Policy logs every event happening in the system over time. Events that can be logged includes event performed by users and also attempts by unauthorized network users trying to penetrate the system either by console or thru network. By installation default, no audit policies are installed. Below are the settings that I've set to be monitored via the Local Security Policy (Start->Settings->Control Panel->Administrative Tools->Local Security Policy):
    - Audit Account Logon Events: **Success and Failure**
    - Audit Account Management: **Success and Failure**
    - Audit Logon Events: **Success and Failure**
    - Audit Object Access: **Failure**
    - Audit Policy Change: **Failure**
    - Audit Privilege Use: **Failure**
    - Audit System Events: **Success and Failure**

- **Event Log Settings**. When you enable Audit Policy, all event logging will be place in the Event Log. Installation default the size for each Event Log is 512K, which is insufficient to log events in long term. Below are the ideal settings for each Event Log:
    - Maximum log size: **100MB**
    - Log Retention Method: **"Overwrite Events as Needed"**

  There is also a registry entry to restrict Guest to access to the event logs.
    - For Application Event Log:
      Key:
      HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application
      Value Name: **RestrictGuestAccess**
      Data Type: **REG_DWORD (DWORD Value)**
      Value Data: **1 (Enable restriction)**

    - For Security Event Log:
      Key:
      HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security
      Value Name: **RestrictGuestAccess**
      Data Type: **REG_DWORD (DWORD Value)**
      Value Data: **1 (Enable restriction)**

    - For System Event Log:
      Key:
      HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Value Name: **RestrictGuestAccess**
Data Type: **REG_DWORD (DWORD Value)**
Value Data: **1 (Enable restriction)**

- **Configure Security Settings**. Security settings for each server are configured via the Local Security Policy Editor. There are some settings that are useful for protecting the server from unauthorized access.
    - Additional Restriction for Anonymous Connections: **"No Access Without Explicit Anonymous Permissions"**
      This option is to prevent Null User account to access the server.

    - Allow System to be Shut Down Without Having to Log On: **Disable**
      By default, Windows 2000 Server and Advanced Server will have this option disable. It is to prevent shut down of the server without logging in.

    - Clear Virtual Memory Pagefile When System Shuts Down: **Enable**
      This option is to ensure that any sensitive information stored in the pagefile will be overwritten as the machine shuts down.

    - Prevent Users from Installing Printer Drivers: **Enable**
      When printer drivers are installed, the printer drivers will have privilege mode on the operating system and allows the drivers to accomplish tasks that are beyond the user's capability. If the printer drivers are actually "Trojan horse" printer drivers, then it will allow the operating system to execute the malicious code without restriction.

    - Rename Administrator Account: **"Rename to other than Administrator"**
      Attackers usually will use common account names to access to the systems. By changing the name, it will delay the attackers from accessing the system because it will take time for them to find out the actual account name

    - Rename Guest Account: **"Rename to other than Guest"**
      Unlike other accounts, Guest are disabled by default. This account is only used to allow unauthenticated users to the system.

    - Restrict CD-ROM Access to Locally Logged-On User Only: **Enable**
      Enabling this option will only allow locally logged on users to access the CD-ROM.

    - Restrict Floppy Access to Locally Logged-On User Only: **Enable**
      Enabling this option will only allow locally logged on users to access the floppy drive.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- **Disable unnecessary services running on system**. Most of the services on Windows are not necessary to be run to perform tasks. As Microsoft stated on their website, the more services that is running on your system, the more entry points that may be available for malicious attacks. The guideline that I followed for disabling the unnecessary services on the Content Server and Bank Gateways is listed on Microsoft Support Knowledge Base Article ID 189271.

- **Harden the TCP/IP stack**. Microsoft released some recommended registry settings to harden Windows NT/2000 system to defend against Denial of Service (DoS) attacks. Below are the registry settings that correspond to it:

  Registry Key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  - EnableDeadGWDetect (DWORD) = "**0**"
  - EnableICMPRedirect (DWORD) = "**0**"
  - EnablePMTUDiscovery (DWORD) = "**0**"
  - KeepAliveTime (DWORD) = **Decimal value "300,000"**
  - NoNameReleaseOnDemand (DWORD) = "**1**"
  - PerformRouterDiscovery (DWORD) = "**0**"
  - SynAttackProtect (DWORD) = "**2**"

Stage 3: Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is considered essential equipment for a good security environment. It provides additional layer of protection to the environment. There are 2 types of IDS, a Network IDS and a host IDS. NIDS provides real-time monitoring, and detection of attacks on the network by inspecting the traffic. HIDS provides real-time monitoring, detection, and prevention to security breaches for servers, applications and data.

A few free and commercial NIDS and HIDS products were evaluated by myself and another colleague to test the capabilities of each product and how well it suites the environment. After extensive testing, we decided that Snort will be our choice of NIDS due to our budget restriction, easy to manage, and also the quick updates on their rule signatures.

Due to the environment that all the VLANs are created on a switch, monitoring ports was created on each VLAN with all the traffics mirrored to the port for the NIDS sensors to work. A new VLAN (VLAN5) was created where a server (SnortCenter), which will be the central snort configuration file, and sensor logs consolidation, will be hosted. All the snort sensors, which has 2 NIC cards, will have 1 of them connected to each VLAN without any IP address configured and the other NIC card will be connected to VLAN5 to communicate with the SnortCenter.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Post-Implementation (After)

Assessment was done with a series of tests using various tools to validate how effective is the new architecture compared to the previous one. Various tools are used is because not all tools are prefect and with different features of testing methods. Testing on the new architecture from security standpoint involves penetration from outside and also from inside the network.

Tools that were chosen for this assessment risk were:

- **ISS Internet Scanner**. A well-known leading commercial security tool available on the market, ISS Internet Scanner is an integrated part of Internet Security Systems' security management platform. It provides comprehensive network vulnerability assessment on systems and network equipments for measuring online security risks.

- **Nessus**. Another security scanner on the market. Nessus is a leading open source security scanner that runs on a UNIX platform. Just like ISS Internet Scanner, it can scan various system platforms for vulnerabilities.

- **CIS Benchmark and Security tools**. Center of Internet Security (CIS) has extensive benchmark and security tools available for evaluating Windows NT/2000 machines, Linux, HP-UX and also Cisco routers. CIS Scoring Tools provided by CIS gives novice administrators a quick evaluation check on their systems to determine their security configuration and provides reports on actions that should be taken to further secure their systems.

- **Nmap**. Nmap or Network Mapper is an open source tool for network exploration or security auditing. It can determined open ports on a system, what operating system is it running and other characteristics using raw IP packets.

Results from the tools are positive. There were no vulnerabilities found on all the systems and network equipments. As for Nmap results, some of the systems have open ports, which were not used by the systems nor the applications. I've run a tool called TCPView from Sysinternals on the affected system to determine the process that uses the port and disable them.

Checklist was also used to audit all the systems and network equipments. Compilation of the checklist was based on the hardening guidelines generated by well-known bodies like SANS, NSA, and CIS.

Some misconfigured settings were detected during the inspection based on the checklist and were rectified immediately after consulting the developers on the impact on their application running in the system. A particular setting, which involves the setting for hardening TCP/IP stack in Windows system, keeps

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

generating errors on the event log. Although the checklist recommended the settings and also by the assessment tool, decision was made to retain the recommended setting and a report was made to Microsoft as a bug.

Although some concerned negative results generated by the tools above were ignored due to the design of the systems, the management were pleased with the results shown from the intensive changes of the infrastructure.

Conclusions

Security is an ongoing effort. While the management of company A has made a good start in protecting their company assets, further effort still needs to be taken, to prevent future unforeseen threats. Day-to-day security management is needed to ensure a safe and secure environment.

References

- Intel Corporation. "Advanced Networking Services – Teaming". URL: http://www.intel.com/support/network/adapter/ans/teaming.htm
- Cisco Systems, Inc. "Cisco - Internet Security Advisories". February 22, 2003. URL: http://www.cisco.com/warp/public/707/advisory.html
- CERT. "CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks". March 13, 2000. URL : http://www.cert.org/advisories/CA-1998-01.html
- Check Point Software Technologies Ltd. "Check Point Advisories". URL: http://www.checkpoint.com/securitycenter/advisories/index.html
- Center of Internet Security. "Solaris Benchmark". URL: https://www.cisecurity.org/tools2/solaris/SolarisBenchmark.pdf
- Sun Microsystems. "SUNSolve Home". URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=home
- Microsoft Corporation. "Microsoft Support Knowledge Base". URL: http://support.microsoft.com/default.aspx?scid=fh;[ln];kbhowto
- WinGuides. "Harden the TCP-IP Stack for Denial of Service Attacks (Windows 2000-XP) at Registry Guide for Windows". December 19, 2002. URL: http://www.winguides.com/registry/display.php/1237/
- Alphademon. "Implementing Snort 1.9.0 and SnortCenter on RedHat 8.0". December 16, 2002. URL: http://www.my-snort.org/modules.php?name=News&file=article&sid=25

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Center of Internet Security. “Benchmark and Scoring Tools”. URL: http://www.cisecurity.com/

- The National Security Agency. “Security Recommendation Guides”. March 5, 2003. URL: http://www.nsa.gov/snac/index.html

© SANS Institute 2003, Author retains full rights.