Global Information Assurance Certification Paper

GIAC Enterprises Security Architecture Assignment 1

For

Level 2 GCFW

By
Corey White

TABLE OF CONTENTS

1.0 Introduction

The purpose of this document is to define the security architecture for GIAC Enterprises. The components that will be addressed in this policy are the firewall, routers and VPNs of the customers, suppliers, and the business partner of GIAC Enterprises.

1.1 Assignment 1 - Security Architecture (25 Points)

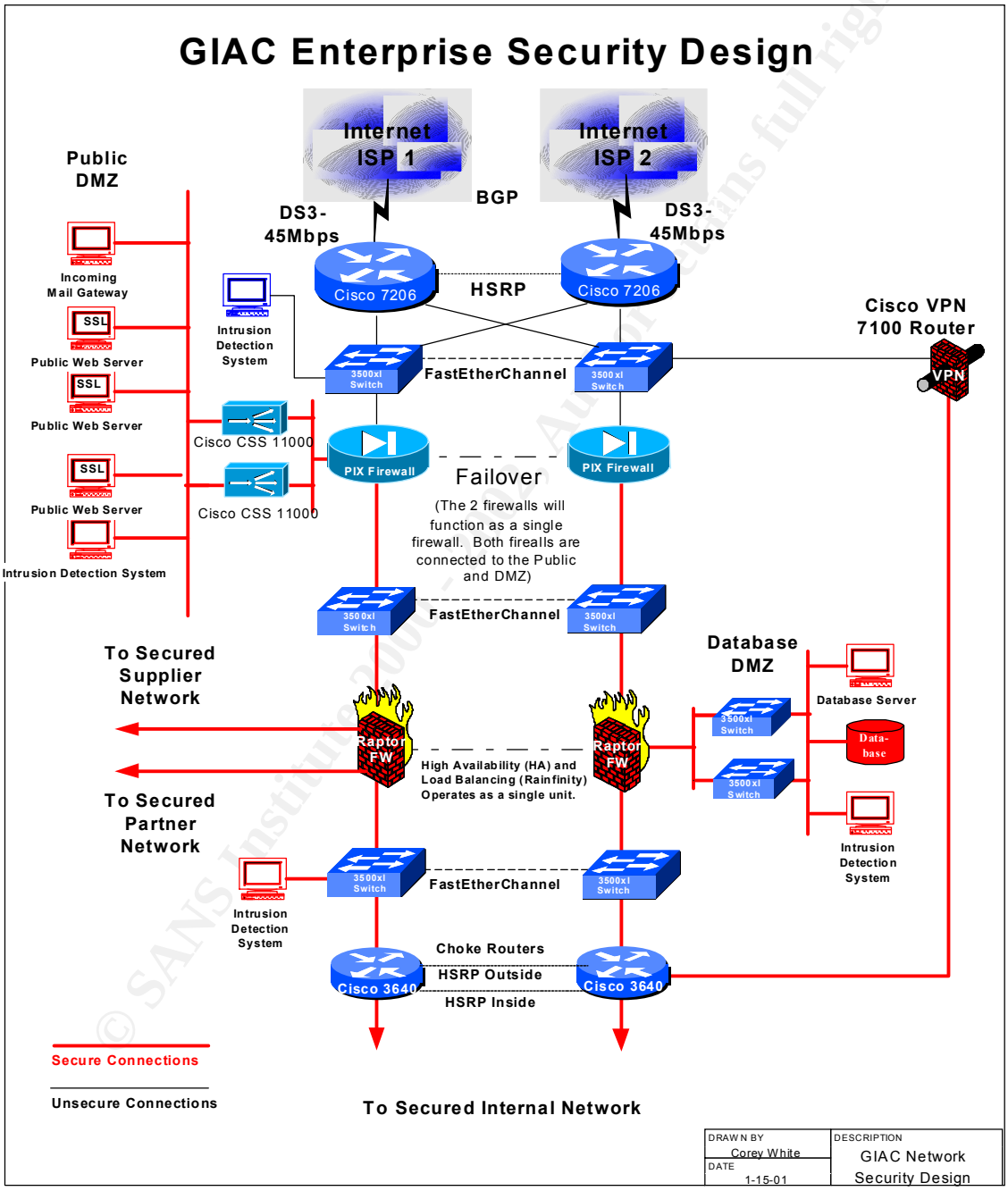
Define a security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component.

2.0 Security Architecture Customer Network



2.1 ISP Selection

Two ISP have been selected to add redundancy and to allow for BGP to be configured on the border routers. Each router has a connection to Internet at 45mbps. This provides a high-speed connection to the Internet allowing customers and VPN fast reliable connection to GIAC web servers and internal network.

2.2 Border Routers

The border routers consist of two Cisco 7206 routers configured w/ HSRP on the inside interfaces and BGP on the outside interfaces for redundancy. Redundancy must be configured on all border router interfaces. This protects GIAC against availability attacks and makes the network more resilient. The version of the software is below:

Platform	Release	Software Features
7200	12.1.5a	ENTERPRISE/FW/IDS IPSEC 56

2.3 Intrusion Detection Systems

Realsecure v5.0 by ISS has been chosen as the Intrusion Detection System for GIAC Enterprises. One IDS is located in front of the PIX firewall that detections attackers knocking on the door. There are other IDSs located on each of the secured DMZs and all network segment to track successful intrusions into GIAC's infrastructure.

2.4 Cisco 3500xl Switches

The Cisco 3500xl switches are configured with Fastetherchannel to provide greater bandwidth and redundancy. No IP address is configured on the switches because that makes them vulnerable to an attack. The version of the switch is c3500XL-c3h2s-mz-120.5-XW.bin

2.5 Cisco CSS 11000 (Load Balancers)

The CSS 11000 is a traffic load balancer that also provides an extra layer of security because there is no direct access to web server and also it load balances the traffic to the web servers.

2.6 Cisco 7100 VPN Router

The 7120 VPN routers provide the highest speed encryption to the internal network via the CiscoSecure VPN Client software. The latest version of the software can be found below.

Platform	Release	Software Features

7100	12.1.6	ENTERPRISE/FW/IDS IPSEC 56

2.7 Web Server

The web servers are running Windows 2000 service pack 1 configured with Secure Socket Layer. Internet Information Server 5.0 with the latest hot fixes and patches applied.

2.8 DNS Server

The DNS server is the primary DNS server for the Internet domain name GIAC.com. There are two secondary servers configured at both of GIAC's ISPs. The DNS server is configured using Windows 2000 service pack 1 with the latest hotfixes.

2.9 Cisco PIX Firewall

The Cisco PIX firewalls are configured with fail over for redundancy. The firewalls are configured to allow the Internet traffic only to access the Public DMZ traffic further into the network is denied. Traffic from the DMZ is allowed to the database DMZ but not to the Internal network or the supplier or the Business partner network. The PIX firewalls are running version pix531.bin of the PIX software.

2.10 Raptor Firewall

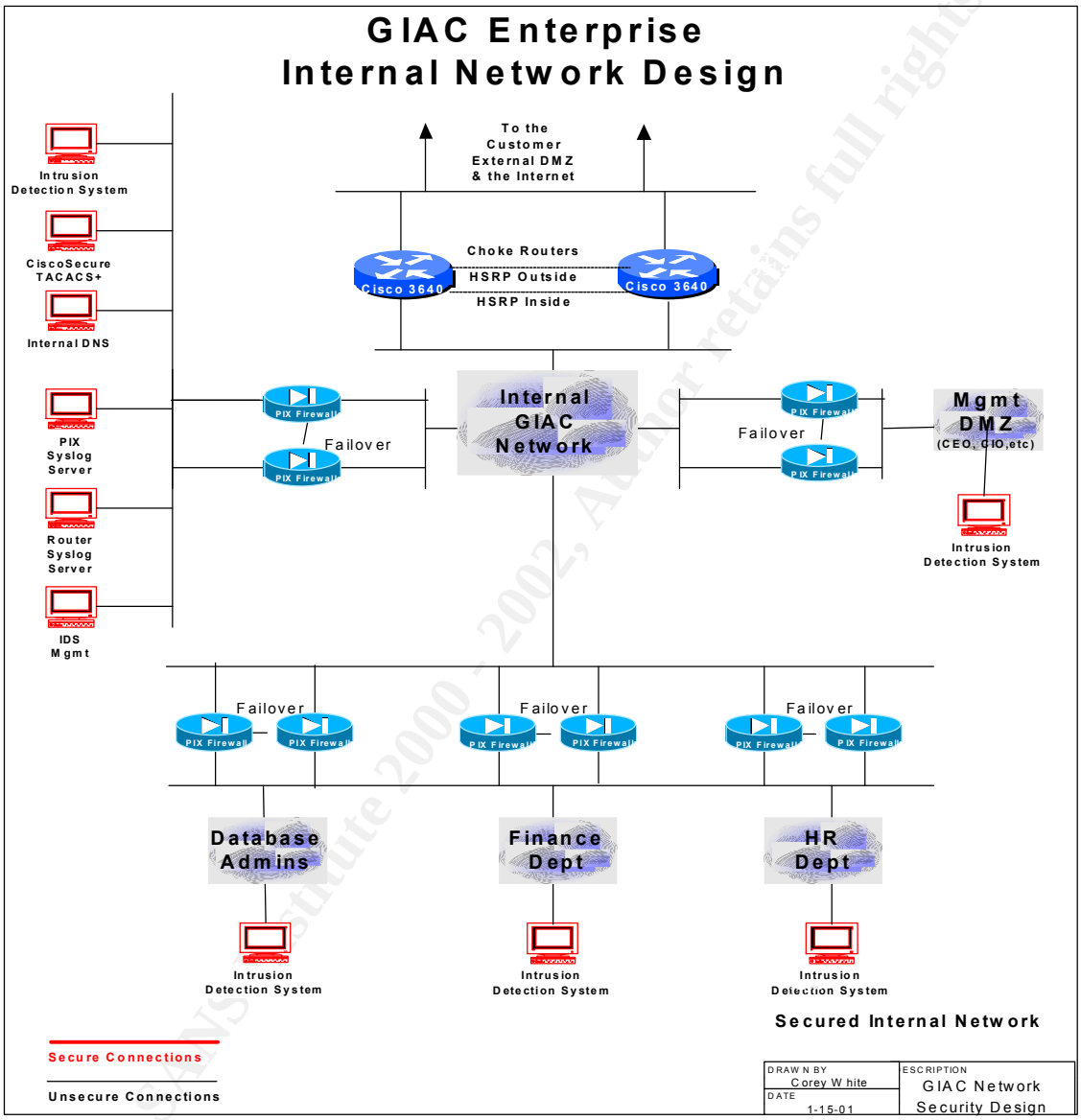
The Raptor Firewalls are running version 6.0 the latest version of the Raptor firewall. They are also configured with High availability and load balancing. The use of the second firewall on a different platform provides firewall differentiation thus further securing GIAC's infrastructure.

2.11 Cisco 3640 Routers

The Cisco 3640 routers are configured with HSRP on the outside and inside interfaces. These choke routers protect the internal network from the external infrastructure. The version of the software is shown in the table below:

Platform	Release	Software Features
3640	12.1.6	ENTERPRISE/FW/IDS PLUS IPSEC 56

3.0 Security Architecture Internal Network



3.1 PIX Firewalls

The Cisco PIX firewalls are configured with fail over for redundancy. The firewalls are configured to allow the Internet traffic only to access the Public DMZ traffic further into the network is denied. Traffic from the DMZ is allowed to the database DMZ but not to the Internal network or the supplier or the Business partner network. The PIX firewalls are running version pix531.bin of the PIX software.

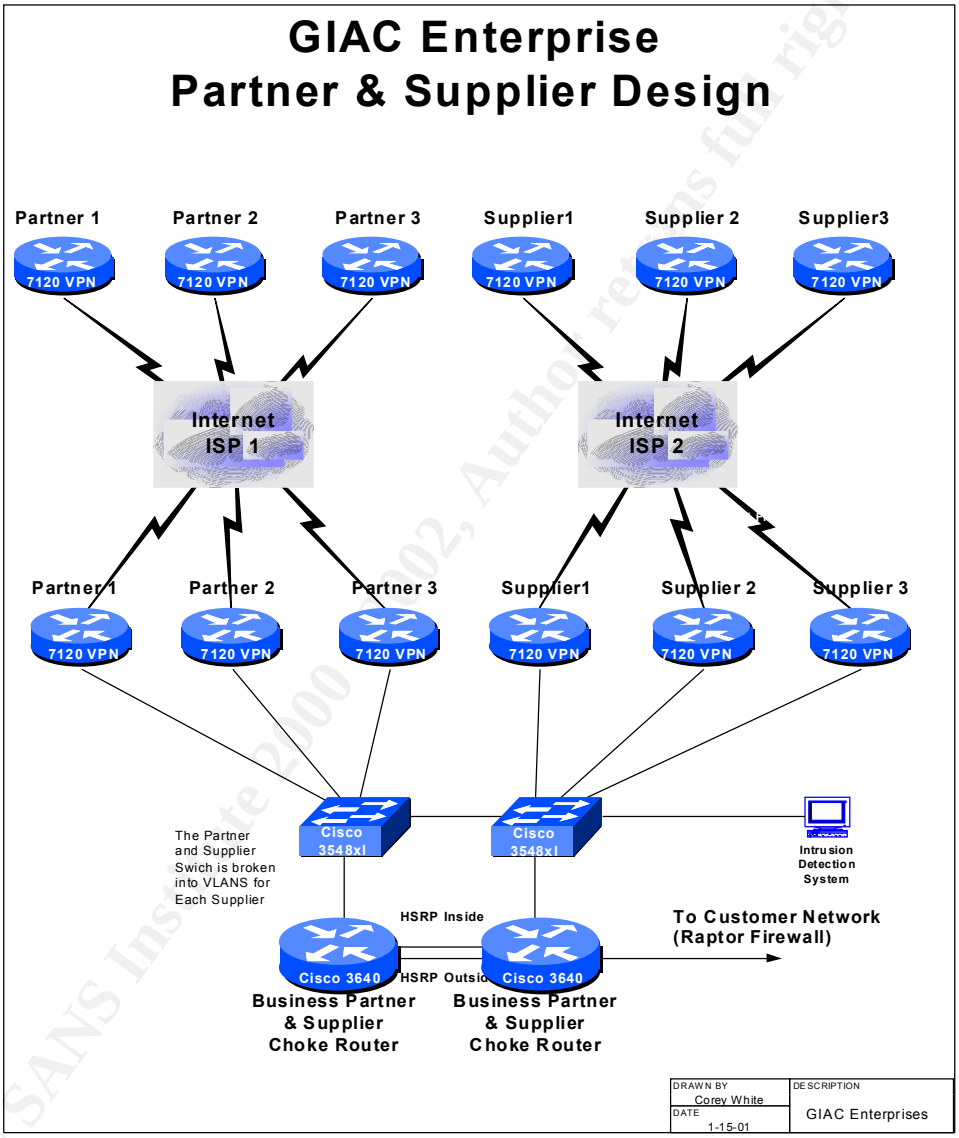
3.2 Syslog Servers

The Syslog server receives all the syslog servers to from the pix firewalls and the routers. The system administrator must monitor these logs regularly.

3.3 Cisco PIX Firewall

Internal firewalls are distributed separating the internal trusts of the Internal network. There is a management DMZ separated by PIX firewall that is configured only to allow desired traffic in or out. There is a HR, Finance, and Database DMZ. These firewalls protect the internal network from internal threats.

4.0 Security Architecture Suppliers and Business Partner Network



4.1 ISP Selection

Two ISPs are designed for the BP and supplier network. VPN routers are placed on both sides of the Internet connections. Encryption is used to protect the data that is transported over the public network.

4.2 7120 VPN Routers

The 7120 VPN routers provide the highest speed encryption to the business partner and suppliers. The latest version of the software can be found below.

Platform	Release	Software Features
7100	12.1.6	ENTERPRISE/FW/IDS IPSEC 56

4.3 Cisco 3548xl Switches

The Cisco 3500xl switches are configured with Fastetherchannel to provide greater bandwidth and redundancy. No IP address is configured on the switches because that makes them vulnerable to an attack. The version of the switch is c3500XL-c3h2s-mz-120.5-XW.bin

4.4 Cisco 3640 Routers

The Cisco 3640 routers are configured with HSRP on the outside and inside interfaces. These choke routers protect the internal network from the external infrastructure. The version of the software is shown in the table below:

Platform	Release	Software Features
3640	12.1.6	ENTERPRISE/FW/IDS PLUS IPSEC 56

GIAC Enterprises Security Policy Assignment 2

For

Level 2 GCFW

By
Corey White

5.0 Introduction

The purpose of this document is to define the security policy for GIAC Enterprises. The components that will be addressed in this policy are the firewall, routers and VPNs of the customers, suppliers, and the business partner of GIAC Enterprises.

5.1 Assignment 2 - Security Policy (25 Points)

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.

Any relevant information about the behavior of the service or protocol on the network.

The syntax of the ACL, filter, rule, etc.
A description of each of the parts of the filter.

An explanation of how to apply the filter.
If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
Explain how to test the ACL/filter/rule.
Be certain to point out any tips, tricks, or "gotchas".

6.0 Border Router

The border routers consist of two Cisco 7206 routers configured w/ HSRP on the inside interfaces and BGP on the outside interfaces for redundancy. Redundancy must be configured on all Border router interfaces. This protects GIAC against availability attacks.

The best security is to disable features and services that are turned on by default, but are not being used. In other words, if a router is not using something, turn it off. Enable only features that may aid in protecting the router or the networks behind the router. If a feature is needed, try to protect it as much as possible, using the protection mechanisms that the Cisco IOS provides. This is the approach that GIAC will take regarding router security.

The border router must be protected in a secured room with limited access therefore, physically securing the routers from being accessed by unauthorized individuals.

The following items must be adhered to when configuring a router at GIAC Enterprises:

- Passwords must be applied to the console port
- Passwords must be applied to all vty lines
- The routers must be configured to log to a minimal of two syslog servers
- The router must be configured to be monitored by snmp (HP OpenView)
- TACACS+ (CiscoSecure) must be configured on the border routers for AAA
- The router syslog messages must be monitored daily and any suspicious activity must be formally reported
- The session timeout on the routers must be set to 1 min and 30 seconds
- Service password encryption must be configured on the routers so that the passwords can not be seen in clear text
- SSH must be used to encrypt telnet session to routers
- Access list must be configured to only allow the networking subnet to access the borders routers
- No TCP/UDP small servers must be configured on the border routers
- Proxy arp must be disabled on all border routers

- CDP must be disabled on all border routers
- The border routers must be time synchronized with NTP configured
- Security banners must be configured on the border routers that state, "Unauthorized access is prohibited".

6.1 Access Control Lists (ACL)

Access control lists must be configured on the borders routers to limit access to the routers and into the internal network. The ACLs on the border routers serve as the first line of defense from the Internet. The following bullets detail the ACL configuration of the border routers that must be adhered to:

- All ports except 80, 443, 21, 123, 20, 53, 25, and 110 (TCP and UDP) must be denied by default on the border routers
- ICMP (Ping) is denied inbound in the internal network
- Access list must be configured on all inbound router interfaces
- Traffic inbound from the Internet using an internal IP address must be blocked
- Private RFC 1918 addresses must be blocked inbound on the border routers

7.0 Firewalls

The firewall infrastructure consists of multiple firewalls throughout the organization. The firewall types are Cisco PIX Firewalls and Raptor Firewalls. The different firewalls are deployed in case one of the firewall plat form becomes vulnerable to an attack or vulnerability chances are that the other firewall is not vulnerable to the same exploit, therefore still protecting the internal network from being attacked.

7.1 Primary Internet Firewalls

The primary Internet firewalls form a major part of the perimeter protection. The following documents the rule sets of the first layer of firewalls (PIX):

- Default deny all
- No traffic is allowed to originate from the Internet and the internal network
- If one component of the perimeter is compromised, it will not result in the compromise of the entire perimeter or the internal network
- Outgoing access list limited to ports 80, 53, 20, 21, 110, 25, and 443 must be applied to outgoing traffic
- Only inbound HTTP to the web servers and inbound SMTP to the mail gateway are allowed from the Internet.
- Changes to the firewall ruleset must be approved by the Information Security Department and must be accompanied by an approved business objective.
- Firewall log must be monitored daily

7.2 Business Partner Firewalls

The business partner firewalls consists of the VPN routers and the Raptor firewalls. The VPN routers connect to the business partner and suppliers. The traffic travels the Internet encrypted with authentication enabled on both ends of the connection. GIAC Enterprises own both routers on their site and routers on the business partner and suppliers site, therefore giving GIAC full control of their infrastructures and security.

7.2.1 Business Partner Firewall Rule Sets And VPN Routers

The business partner firewalls consists of the VPN routers and the Raptor firewalls.

- The VPN Routers must be configured with IPsec using Encapsulating security protocol (ESP). ESP provides encryption of the payload of the traffic.
- 3DES must be configured on all VPNs
- MD5 hashing algorithm must be configured to provide message integrity
- ISAKMP must be used for key management
- NAT Network Address Translation) must be used for communication to all business partners and suppliers. No internal host IP addresses should be revealed outside of the internal network.
- The raptor firewall must be configured to only allow the supplier and partners to the specific database they are allowed to access.

7.3 IPSEC Policy

The IPsec policy allies to the VPN routers and to the VPN client that access the internal network.

- The VPN Routers must be configured with Ipsec using Encapsulating security protocol (ESP). ESP provides encryption of the payload of the traffic.
- 3DES must be configured on all VPNs
- MD5 hashing algorithm must be configured to provide message integrity
- ISAKMP must be used for key management

8.0 Tutorial

8.1 How To Modify The Router ACLs

To modify a router's ACL it is important to use notepad to copy and make changes. First remove the access completely and paste it into notepad. Make the necessary changes to the ACL and paste it back. Making changes to the ACL while it is still on the router can be extremely dangerous and may cause the router ACL to function improperly.

8.2 What Order To Apply An Access List

Order is extremely important to access list on Cisco routers because they are read top down. If they are applied in the incorrect order your access may deny traffic that you want to be allowed. All access list have a default deny at the end of it that blocks all traffic that has not been previously specified. The deny rule is not visible. In many cases it should be added manually so that the administrator will see it and remember it is there.

ACLs should be implemented in the order in which they will be used first. You don't want your router to waste CPU cycles parsing through an access list to allow web traffic through when that is the most used line in the ACL. The most used lines in the ACL should be put on the top on the ACL.

8.3 Router Access List Annotated

access-list 2 permit X.X.X.X
THE ABOVE ACLS LIMITS TELNET ACCESS TO THIS ROUTERS TO DEVICES ON THE INTERNAL NETWORK ONLY

access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
THE ABOVE ACLS BLOCK ALL INBOUND RFC 1918 ADDRESSES WHICH SHOULD NOT BE ROUTABLE FROM THE INTERNET

access-list 101 permit tcp any eq www X.X.X.X 0.0.0.3
THE ABOVE ACLS PERMITS WEB TRAFFIC TO THE INTERNAL NETWORK

access-list 101 permit tcp any eq 443 X.X.X.X 0.0.0.3
THE ABOVE ACLS PERMITS SSL TRAFFIC TO THE INTERNAL NETWORK

access-list 101 permit tcp any eq ftp X.X.X.X 0.0.0.3
access-list 101 permit tcp any eq ftp-data X.X.X.X 0.0.0.3
THE ABOVE ACLS PERMITS FTP TRAFFIC TO THE INTERNAL NETWORK

access-list 101 permit tcp any eq telnet X.X.X.X 0.0.0.3
THE ABOVE ACLS PERMITS TELNET TRAFFIC TO THE INTERNAL NETWORK

access-list 101 permit tcp any eq smtp X.X.X.X 0.0.0.3
access-list 101 permit tcp any eq pop3 X.X.X.X 0.0.0.3

THE ABOVE ACLS PERMITS EMAIL TRAFFIC TO THE INTERNAL NETWORK

access-list 101 permit udp any eq ntp X.X.X.X 0.0.0.3
THE ABOVE ACLS PERMITS NTP TRAFFIC TO THE INTERNAL NETWORK

line vty 0
 access-class 2 in
THE ACCESS-CLASS COMMAND APPLIES THE ACCESS TO AN INTERFACE

 password 7 XXXXXXXXXXX
 login
line vty 1 4
 access-class 2 in
THE ACCESS-CLASS COMMAND APPLIES THE ACCESS TO AN INTERFACE

8.4 Testing the ACL Configuration

To test the access lists on a Cisco router use the "show access-list" command. This command shows the matches to your access list line by line.

The other way to test an ACL is to test your applications from end to end and see if they work or not. If they don't you know there is a problem with you access list.

The third and easiest to test and ACL it to configure logging on the routers and watch the logs to see what traffic is being denied by the firewall.

GIAC Enterprises Audit Your Security Architecture Assignment 3

For

Level 2 GCFW

By
Corey White

9.0 Introduction

The purpose of this document is to conduct a security assessment on GIAC Enterprise's border router and primary Internet firewalls. This assessment consists of planning, implementation of the assessment, and recommendations.

9.1 Assignment 3 - Audit Your Security Architecture (25 Points)

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Border Router and Primary Firewall described in Assignments 1 and 2. Your assignment is to:

Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

Implement the assessment. Validate that the Border Router and Primary Firewall are actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

10.0 Methodology

The methods that will be used to audit GIAC Enterprises border router and primary firewalls are documented. Interviews will be conducted at GIAC at three different levels.

Level 1 will consists of the network engineers that implement the policies stated in the security policy. As we all know everything is not implemented according to policy and policy is subject to interpretation.

Level 2 consists of officer in the Information Security Department to see what their understanding and interpretations of the security policies are.

Level 3 will be an IT manager to determine his dedication and understanding of the important of network security.

A copy of the firewall rule set and a copy of the router configuration will be obtained to validate the security implementations of the security policy. A physical audit of the firewall and border routers will be conducted.

Network scanning tools will be used to identify vulnerabilities in the firewalls and routers. These tools consist of a proprietary set of tools compiled for assessments. The results of these tools will be thoroughly documented in the final deliverable.

11.0 Cost and Resources

This assessment will be done in 40 hours (1 week). One resource has been identified to complete this task. The cost for this 1 resource is $300 per hour X 40 hours = $12,000.

12.0 Risks and Considerations

There are some minimal risk that the scanning tool could disable some production systems, there a written agreement must be signoff on by GIAC enterprises before any scanning can be conducted. There are other steps that are being taking to mitigate the risks. The steps are listed below:

- The GIAC Enterprises Helpdesk will be notified of what devices will be scanned and when so they can be monitored for any problems.
- All scans will be conducted after business hours between 7 PM and 7 AM, unless otherwise stated by GIAC staff.
- The scanning must be submitted and approved by GIAC Change Control Committee

13.0 Border Router and Firewall Audit

The border routers consist of two Cisco 7206 routers configured w/ HSRP on the inside interfaces and BGP on the outside interfaces for redundancy.

13.1 Border Router Security Policy Validation

Checking the configuration of the router against the security policy will validate the router's compliance to the policy.

13.2 Primary Internet Firewalls Audit Validation

The firewall configuration will be audited against the current security policy and against the current "best practices" in information security.

13.2.1 Tools and Commands

- AGNET Tools were used to conduct port scans against the border routers and firewall.
- AGNET Tools were also used to test the ability to ping and trace route into GIAC Enterprises
- NMAP will be used to determine if the routers are vulnerability to a TFTP download vulnerability. The command for this test is "nmap –sU –p69 –nvv Target IP"
- Solarwinds IP browser will be used to check the snmp community strings security
- Network vulnerability assessment tools like ISS Network Scanner will be used to scan the internal network, firewalls, and border routers.
- NMAP will be used to determine the firewall platform. Command = nmap –sS IP address
- Hping will be used to scan past the firewall. The following command will be used " Hping ip address –c2 –s –p80 –n
- The IOS versions on the router will be checked against the database at security focus for vulnerabilities.

14.0 Recommendations

The following sections describe the recommendations that are given to GIAC Enterprises at the end of the assessment.

14.1 Border Router and Primary Firewall Recommendations

Routers can be better managed by implementing the following:

- Description lines are not added to router ACLs. This is not required by the security policy and should be for change management.
- The "no ip unreachables is not configured on the router this allows someone to enumerate the router and the firewall.
- The router access list is not configured with the log parameter at end of each line. The command logs additional information about the ACL How many deny, allows, etc.
- The router is not configured with the command "no ip directed broadcast" to protect it from smurf attacks
- Policies should be developed that require frequent password changes, good password construction, and adequate documentation.
- All routers should be maintained at the same and most current IOS versions.
- All router configurations should be stored in a central and secured area. There should be a new version of a configuration file each time a change is required. The change should be made on the new file and then uploaded to the router.

- Authentication, Authorization and Accounting should be configured on all routers. User authentication and authorization will help protect GIAC network from being accessed by unauthorized users.
- Good management practices require that all similar equipment have the same, and if possible, the most recent IOS version. It is otherwise impossible to keep track of which version has what features or what patches.
  - Authentication provides a method of identifying users, including login and password dialog, response challenges, messaging support, and depending on the security protocol, encryption.
  - Authorization gives the method for a remote access control, including one-time authorization for each service per-user account list and profile, user group support and support of different protocols.

  - Accounting provides a method for collecting and sending security server information used for billing, auditing, and reporting. The information may include user identities, start and stop times, executed commands, number of packets and number of bytes. Accounting allows you to track the services users are accessing as well as the amount of network resources they are consuming.

- Configure the description field on ACLs with the name of the person performing the configuration, the date configured and the description of the line that is being configured to give an audit trial for future audits.
- Provide good configuration controls. Some area, such as a file server directory, should be set aside for the storage of all router configurations. There should be one directory that has the most current configuration file for each router and then another directory for past versions. This second directory should be adequately protected, not only from updating, but also from reading. Only a very select few should know the password. When changes are necessary, the file should be backed up, then edited and uploaded by a cut & paste operation when the administrator is telnet'd to the router. When proper router operation is confirmed, the new file should become the "current" version.
- One possibility for logging is to set up a standard syslog host to receive logging events. However, this does not offer an optimal level of granularity in redirecting log output nor managing individual hosts, applications, or events. It does, however, provide a central repository for important logging information.
- Another possibility many organizations have found more scalable and useful is to augment the logging facility with an event handler such as Seagate NerveCenter. Products such as NerveCenter provide rulesets, logic, and powerful programming syntax for directing incoming log entries, handling alerts and alarms, redirecting specific logging to a file or other server, running applications or scripts, or filtering repetitive alarms to a single alarm (very useful when tied to paging).

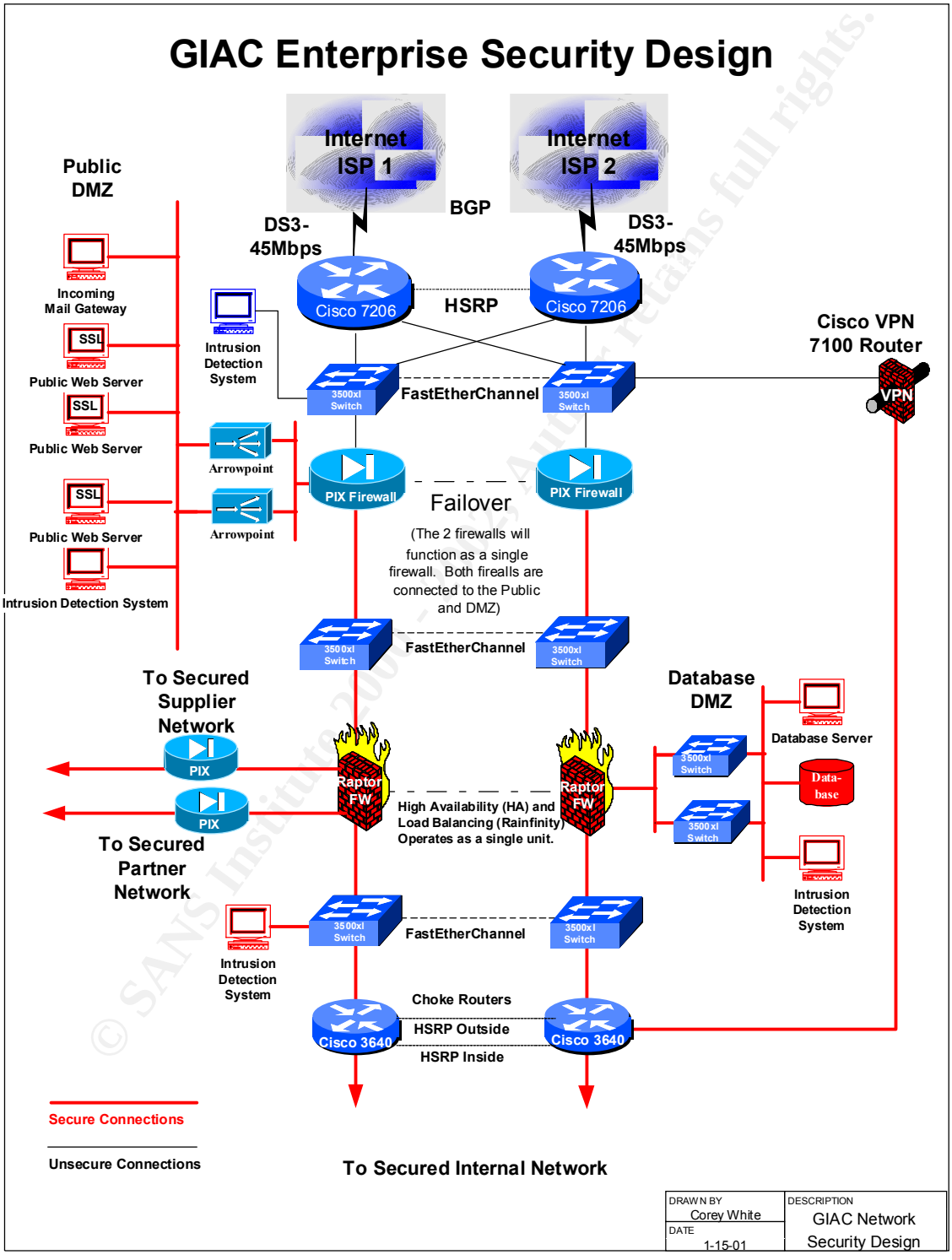
The following should be implemented to improve Network Management practices:

- Maintain a formal inventory of network components including serial numbers and the date the component was installed.
- Ensure that all network users are formally authorized to use the network. The security administrator should maintain files for access requests for all users of the network. The user, his/her immediate supervisor, and the owners of the data the user is authorized to access should sign the access requests.

- Check the network configuration regularly to ensure that all components attached to the network are authorized.
- Use NTP servers to ensure all routers and critical servers are time synchronized. Accurate time is especially important for authentication services and correct timestamps on log entries.
- Responsibility for conducting periodic risk analysis and security assessments should be formally assigned. The owner of the network is responsible for assigning responsibility for periodic risk analysis and security assessments of the network.
- Time periods between risk analysis or security assessments should commensurate with the sensitivity of data processed or maintained on the network. Since users on networks are able to install software and other mechanisms (e.g., dial-up) on their workstations, it is important that an assessment of the network be performed on an annual basis.
- Procedures should require a risk analysis or security assessment to be performed whenever significant changes to the network (e.g., physical facility, hardware, software, or communications) occur.
- Individuals responsible for network security and network administration should have the necessary experience and should receive formal training in order to be able to perform their duties.
- A plan should be developed to harden all GIAC routers. A router build document should put together with the procedure to harden a new router. This will ensure all routers are hardened the same.
- Configure login banners on all routers to deter unauthorized user from accessing the router.
- Ensure that Internet Control Message Protocol (ICMP) is blocked on all business partner connections.

14.2 Alternate Architecture

The alternate design below adds another set of firewalls between the business partners/ suppliers network and the customers network. This provides an extra layer of protection between both sides of the network.



GIAC Enterprises Design Under Fire Assignment 4

For

Level 2 GCFW

By
Corey White

TABLE OF CONTENTS

15.0 Introduction

The purpose of this document is to conduct a security assessment on GIAC Enterprise's border router and primary Internet firewalls. This assessment consists of planning, implementation of the assessment, and recommendations.

15.1 Assignment 4 - Design Under Fire (25 Points)

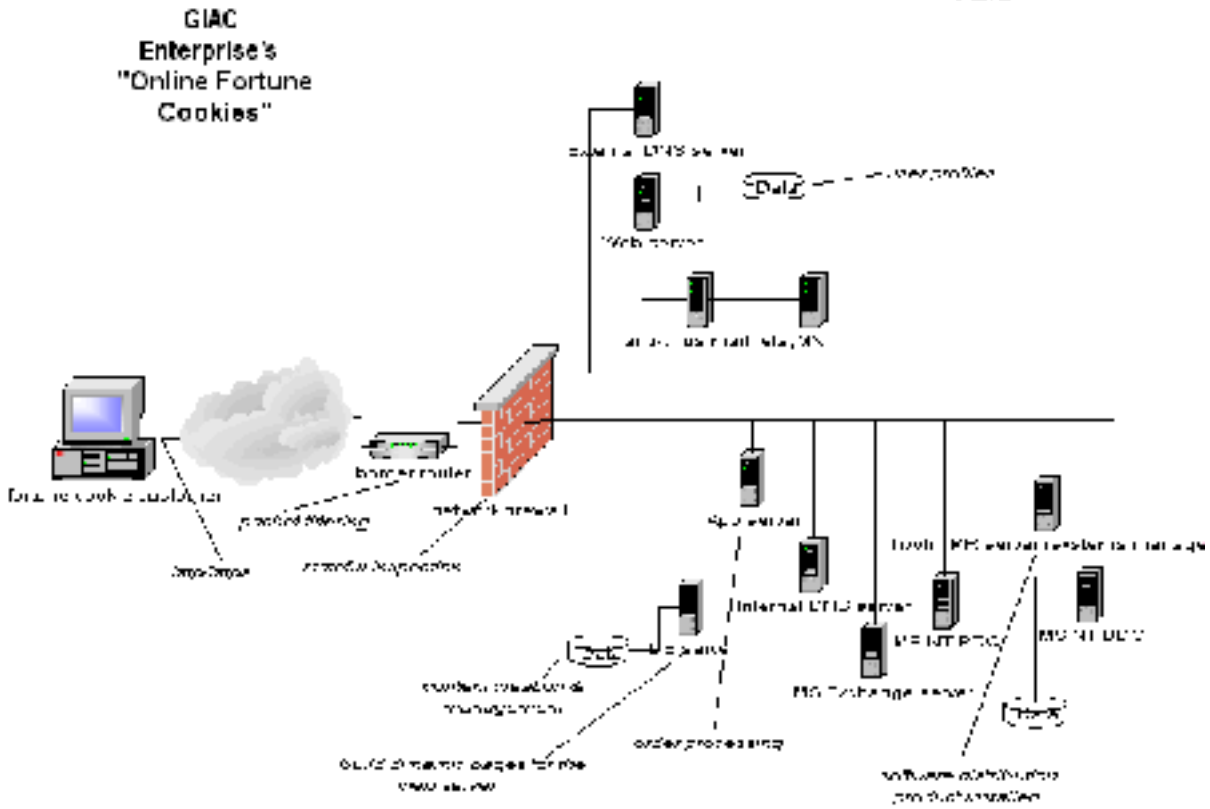
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

16.0 Design Under Fire

http://www.sans.org/y2k/practical/sinead_hanley_GCFW.doc



17.0 Objective 1 Firewall Attack

The design is using the Conseal Firewall which is not very known, therefore there are not many published vulnerabilities associated with this firewall. The problem with using this type of firewall is that it appears to be more of a personal firewall and not a network firewall as it is depicted in the diagram. Based upon the screen shots given the practical the firewall is running Windows 2000. It does not seem to have service pack 1 installed. There are multiple vulnerabilities that can be exploited on but I have chosen the one below:

http://www.microsoft.com/technet/security/bulletin/MS00-079.asp

This vulnerability will be allowed by the firewall because it is allowing port 80. I can build a packet with html mail and insert some code into the it run a Trojan giving me remote access into the firewall. The Trojan will be allowed out because it runs on port 80 and port 80 is allowed out through the firewall and the border router. Once I have remote control of the PC firewall I give myself administrator access, and slowly begin to compromise internal systems in seach of something interesting.

This vulnerability can easily be patched by monitoring the latest vulnerbilites and applying the necessary patches and hotfixes.

17.1 Objective Vulnerability

Microsoft Security Bulletin (MS00-079)
Patch Available for "HyperTerminal Buffer Overflow" Vulnerability

Originally posted: October 18, 2000

Summary
Microsoft has released a patch that eliminates a security vulnerability in the HyperTerminal application that ships with several Microsoft® operating systems. This vulnerability could, under certain circumstances, allow a malicious user to execute arbitrary code on another user's system.
Frequently asked questions regarding this vulnerability and the patch can be found at http://www.microsoft.com/technet/security/bulletin/fq00-079.asp

Issue
The HyperTerminal application is a utility that installs, by default, on all versions of Windows 98, 98SE, Windows ME, Windows NT, and Windows 2000. The product contains an unchecked buffer in a section of the code that processes Telnet URLs. If a user opened an HTML mail that contained a particularly malformed Telnet URL, it would result in a buffer overrun that could enable the creator of the mail to cause arbitrary code to run on the user's system. Please note

that, although a Telnet URL is involved in this vulnerability, there is no relationship between this vulnerability and the "Windows 2000 Telnet Client NTLM Authentication" vulnerability discussed in MS00-067.
HyperTerminal is the default Telnet client on Windows 98, 98SE and ME. However, it is not the default Telnet client on Windows 2000, and Windows 2000 users who have not taken steps to make it the default Telnet client would not be affected by the vulnerability.

Although HyperTerminal ships as part of several Microsoft products, it was developed by a third party – Hilgraeve, Inc. Additional information on the vulnerability and a patch for their full version product, HyperTerminal Private Edition, is available from their web site at www.hilgraeve.com

Affected Software Versions
Microsoft Windows 98 and Windows 98SE
Microsoft Windows Me
Microsoft Windows 2000
Patch Availability
Windows 98 and 98SE:
http://download.microsoft.com/download/win98/Update/12395/W98/EN-US/274548USA8.EXE
Windows Me:
http://download.microsoft.com/download/winme/Update/12395/WinMe/EN-US/274548USAM.EXE
Windows 2000 (can be applied to both Gold and Service Pack 1):
The Windows 2000 patch has been removed at this time. An updated patch is being developed and will be available shortly.
Note The above URLs may have been wrapped for readability.
Note Additional security patches are available at the Microsoft Download Center

More Information
Please see the following references for more information related to this issue.

Frequently Asked Questions: Microsoft Security Bulletin MS00-079, http://www.microsoft.com/technet/security/bulletin/fq00-079.asp
Microsoft Knowledge Base articles Q274548 (Win9x) and Q276471 (Win2K) discuss this issue and will be available soon.
A patch for HyperTerminal Private Edition (a for-purchase upgrade from the default client) is available from www.hilgraeve.com
Microsoft TechNet Security web site, http://www.microsoft.com/technet/security/default.asp
Obtaining Support on this Issue

This is a fully supported patch. Information on contacting Microsoft Product Support Services is available at http://support.microsoft.com/support/contact/default.asp.

Acknowledgments
Microsoft thanks Luciano Martins of USSR Labs (www.ussrback.com) for reporting this issue to us and working with us to protect customers.

Revisions
October 18, 2000: Bulletin Created.

18.0 Objective 2 Denial of Service Attack

The smurf attack is a very popular DoS attack. The smurf attack consists of a directed broadcast being sent ping request to a network devices that allows ping through. The attacker sends a spoofed ICMP packet to the broadcast address. The spoofed address makes it look like the packet came from the target system itself, therefore causing it to reply to itself. Using 50 other host configured to launch the same attack amplifies this attack making it flood the network devices it is directed at and causing it to ultimately go down.

The counter measure for this is to disable IP directed broadcast on the border routers or on your firewalls if using a form of UNIX. Other than the above listed solution there is no real way to address this problem. More information about this vulnerability can be found at the link below:

http://andrew2.andrew.cmu.edu/rfc/rfc2267.html

19.0 Objective 3 Internal System Attack

Based upon the design the target of my attack is a web server on the screened DMZ. It is a single point of failure if the server goes down then customers cab access the Web server and place orders which not good. The server is an IIS 5 server that is not patched. I have opted to use the Microsoft Security Bulletin (MS00-066) for "Malformed RPC Packet" Vulnerability. I chose the web server because it was the easiest target besides the DNS server and the mail server.

The hack is implemented by sending a malformed RPC packet to the server this causes a buffer overflow and brings down the server until it is rebooted.