Global Information Assurance Certification Paper

Security Plan for GIAC Enterprises

By Dennis Depp

GCNT Practical Assignment (v. 3.0)

Executive Summary

GIAC is a small privately held company of approximately 800 personnel. This is a security plan for the internal network of GIAC and starts at the GIAC firewall. The prize gem of GIAC is their Research and Development team, which is considered one of the best R & D teams in the online fortune cookie sayings business. Because of the highly competitive and cutthroat nature of the online fortune cookie saying business, GIAC's CIO wants the highest possible security for the R&D section to include, if possible, encryption of the network traffic between machines. Within the fortune cookie saying business, it is not uncommon for sales and marketing staff to switch jobs between companies. For this reason, network traffic between non R&D computers needs to be monitored.

The GIAC network consists of a user enclave and a hardened enclave. All externally initiated traffic will terminate in the hardened enclave. This area currently contains the external web server, the email gateway and the externally accessible DNS server. This area is separated from the Internet and the user enclave by a firewall. The user enclave is separated into two areas, a main user enclave and the R&D enclave. These areas are separated using a router. The different mission of these two groups of users creates different security needs. A separate address space for each of these groups makes it easier to implement IP security (IPSec) filters for these areas. The computers and users in these areas are also split into different Organizational Units within Active Directory. This provides an easier method for managing the security posture for these groups.

The organizational structure of Active Directory is configured based on security boundaries and reflects the need for increased security in the R&D section. Organizational Units separate the R&D section from the rest of the user network. This allows for the separate security needs of these computers and users to be managed with Group Policy objects. An OU will also be established for the externally accessible servers, the web server and the email gateway. Security of each of these two areas will be heightened thru the use of IPSec filters. IPSec filters within GIAC depend on the location of the servers and their purpose. Domain controllers will have an IPSec filter that is not location dependent. Servers within the hardened enclave will have an IPSec filter based on the functions performed by the server. File and Printer servers and workstations will have IPSec filters based on their location.

This document will discuss the network design, the Active Directory structure and specific steps taken to ensure the integrity of this system. The security steps will include group policy object configuration, IPSec rules and configuration and other security steps that are used to secure this network.

Network Design

We begin our security configuration with a discussion of the GIAC Enterprises network. GIAC Enterprises network is isolated from the Internet via a firewall. A diagram is provided at figure 1. The firewall segments the network into a hardened enclave for machines that require access from the Internet and a user enclave for everything else. In the hardened enclave are the external web server and the email gateway. Both the external web server and the email gateway are placed in the hardened enclave because they allow unsolicited traffic from the Internet. Both these servers must allow this traffic to perform their primary function.

The external web server is running Windows 2000, with IIS 5, Service Pack 2 , Internet Explorer 6.0 and the following hotfixes:

Q252795	Q276471	Q285156	Q258851	Q292435	Q296185
Q298012	Q299553	Q299687	Q299796	Q301625	Q302755
Q303984	Q307353	Q313675	rbupdate		

The web server is configured with 2 – 18 GB drives mirrored with a hardware RAID controller. This drive contains the Windows system files and the IIS log files. This drive is formatted with NTFS. The data drives consist of 3 – 18 GB drive configured with hardware RAID 5. RAID 5 was chosen because of its increased performance during reads. This drive is also formatted with NTFS. GIAC decided to update this server to Internet Explorer 6.0 because the version that ships with NT 2000, Internet Explorer 5.0 is no longer supported or tested for vulnerabilities by Microsoft. As a result, hotfixes are no longer created for version 5.0. Since this is an initial installation, Internet Explorer 6.0 was chosen in hopes that another upgrade of Internet Explorer will not be needed to stay within Microsoft's support cycle. This server will not be kept up to date with the latest version of Internet Explorer. However, security hotfixes will continue to be applied to this machine, as they are made available and tested by GIAC staff. Event Log Manager (ELM) version 2.2 is installed on this machine to monitor the event logs and send updates to a centralized repository. ELM is configured to notify the systems administration team for various events. IPSec policy on this computer allows any communication on ports 80 and 443. All non-http traffic must be from the user enclave and it must be digitally signed or the packet is dropped. The IPSec policies will be discussed in greater detail later in this document.

The email gateway is running Windows 2000 with Microsoft SMTP service, Service Pack 2 and the following hotfixes:

Q252795	Q276471	Q285156	Q258851	Q292435	Q296185
Q298012	Q299553	Q299687	Q299796	Q302775	Q303984
Q307353	Q313675	rbupdate			

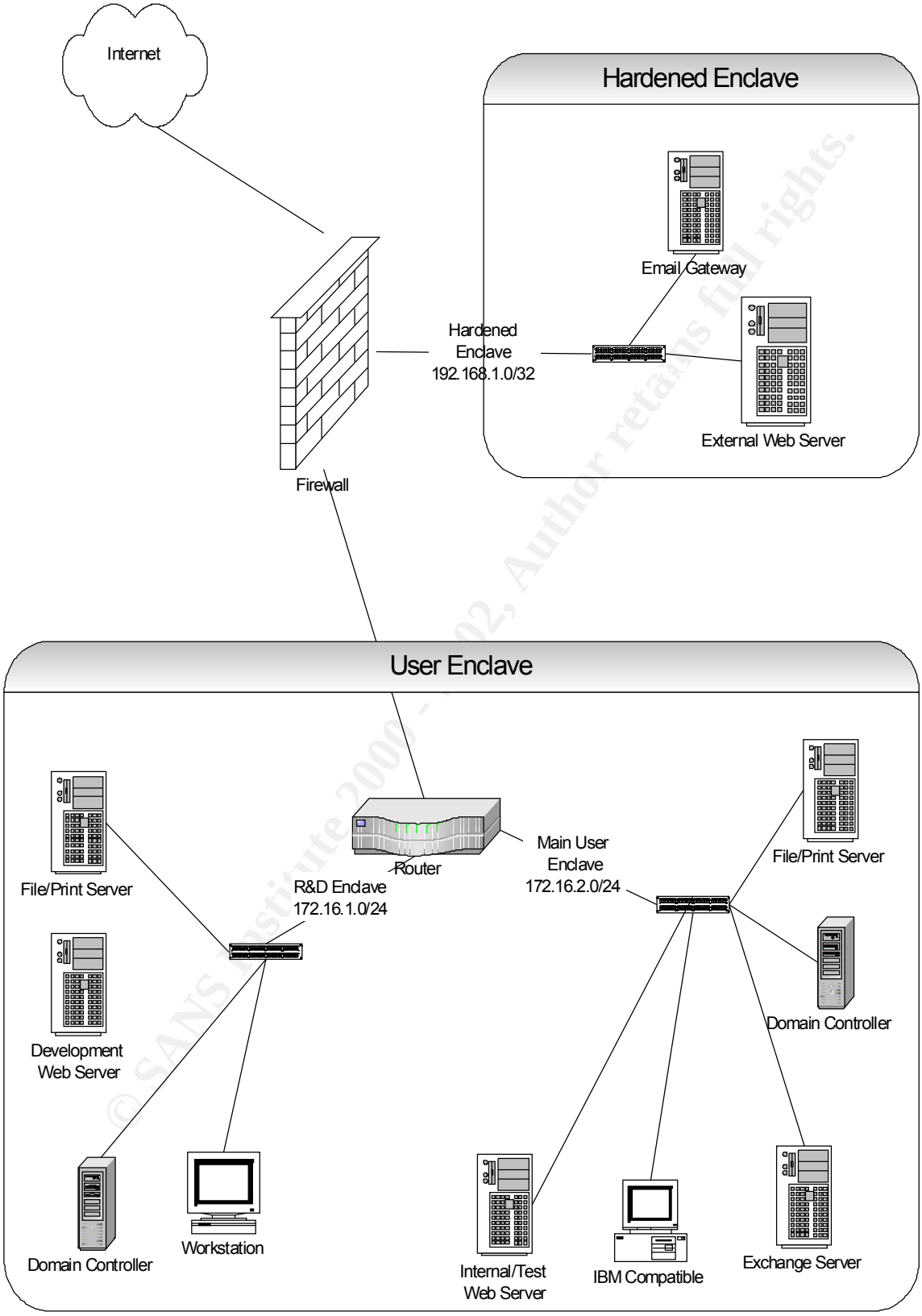

Figure 1 GIAC Enterprises Network

This server is configured with 2 - 18 GB drives mirrored using a hardware RAID controller and formatted with NTFS. This server has an IPSec policy that allows all communication on port 25. All non-port 25 traffic must be digitally signed and must come from the user enclave. Traffic between this server and the Exchange server is required to be digitally signed. As with the external web server, Internet Explorer 6.0 and ELM 2.2 are installed on this machine.

The User enclave is split into two separate areas by a router. The two areas are the main user enclave and the R&D enclave. These areas each use a private IP address space. The areas are separated because of additional security requirements in the R&D enclave. Within the R&D enclave will be the workstations for the members of the R&D group. There will also be one domain controller and a file and print server for the R&D group. The domain controller is running Windows 2000 service pack 2 and Internet Explorer 6.0 with the following hotfixes:

Q252795	Q276471	Q285156	Q258851	Q292435	Q296185
Q298012	Q299553	Q299687	Q299796	Q301625	Q302755
Q303984	Q307353	Q313675	rbupdate		

This server is configured with 1-18 GB drives mirrored with hardware RAID and 3-18 GB drives configured as RAID 5. The mirrored drives contain the system files and the Active Directory log files. The RAID 5 drives contain the Active Directory database files. Both of these drives are formatted with NTFS. The Active Directory database files are placed on the RAID drive because of the enhanced performance during reads. The domain controller is running DNS with Active Directory integrated zones. A domain controller is placed here to allow R&D users to continue working when there are problems with the router. This machine is also running ELM 2.2

The file and print server is placed here, as only R&D users will be allowed to access this file server. It is running Windows 2000 service pack 2 with Internet Explorer 6.0 and the following hotfixes:

Q252795	Q276471	Q285156	Q258851	Q292435	Q296185
Q298012	Q299553	Q299687	Q299796	Q302755	Q303984
Q307353	Q313675	rbupdate			

This server is configured with 2-18 GB drives mirrored with Hardware RAID. The data drives are 4-36 GB drives configured as RAID5. Both drive are formatted using NTFS. ELM 2.2 is installed and running on this machine.

One of the main functions of the R&D group is to update and deploy new technology in the sale of online fortune cookie sayings. To assist with this function, a development web server resides in this domain. Its configuration is the same as the external web server except all traffic to and from this machine, including http and https traffic must be encrypted. This and all the servers within this enclave are configured to require IPSec encryption.

A second domain controller, an Exchange server, internal web server, a test web server and a file and print server all reside in the main user enclave. The second domain controller is configured identical to the server in the R&D enclave. The internal web server is configured like the external web server with the exception that all traffic to and from this server must be digitally signed. The file and print server is configured similar to the file and print server in the R&D enclave with the exception that traffic to this server can be digitally signed instead of encrypted. The Exchange server is configured with 2-18 GB drives mirrored using hardware RAID for the operating system, 2-36 GB drives mirrored using hardware RAID for the Exchange log files and 5-72GB drives configured using hardware RAID for the Exchange information stores. All of these drives are formatted with NTFS. This machine is running Windows 2000 with Internet Explorer 6.0 and service pack 2. It is also running Exchange 2000 with Exchange service pack 2 and ELM version 2.2. The Exchange server has the following hotfixes installed:

Q252795	Q276471	Q285156	Q258851	Q292435	Q296185
Q298012	Q299553	Q299687	Q299796	Q302755	Q303984
Q307353	Q313675	rbupdate			

The domain controller is placed in this enclave to allow users to continue work in the event of a router outage. It also provides redundancy for the Active Directory database. The Exchange email server sits in the user enclave, as this is the location of the user base. Although email needs to communicate with the Internet, this is done through the email gateway in the hardened enclave. This server only accepts email from the gateway and forwards all outgoing email to the email gateway. The internal web server is used in house only and never accepts communication from the Internet. For this reason, it is placed in the user enclave. Because personnel from R&D and Sales & Marketing need access to this web server, it is placed in the Main User Enclave.

Active Directory Design

The Active Directory for GIAC Enterprises consists of a single domain, GIAC.NET. This is the simplest structure to organize and meets all of GIAC Enterprises needs. There are three main Organizational Units within the GIAC.NET domain: Hardened Enclave, Main User Enclave and R&D Enclave. Within each of these OU's are sub-organizational units. A diagram is provided at figure 2. Under the Hardened enclave there is a separate OU for Web servers and Email gateways. While this structure seems trivial considering GIAC only has one Web server and one email gateway. As GIAC grows, they expect to add additional web servers perhaps in a cluster or load balancing fashion, and they hope to add an additional email gateway for fault tolerance.

The R&D Enclave OU will have sub-OU's for servers, workstations, groups and users. The Main User Enclave OU will have sub OU's for servers, workstations, groups and users. This setup aligns the GIAC.NET domain along lines that correspond to security boundaries. The Hardened Enclave has specific security needs because machines in this area interact with the Internet as their main function. Because of this interaction, special

care needs to be taken to ensure hackers do not compromise these machines. In the event these machines are compromised, notification is made immediately to the Systems Administrator. By using sub-OUs, machines with common functionality are grouped together. Currently there is only one machine in each of the sub-OUs in the Hardened Enclave. Placing the computers in a domain global group and assigning permissions to the respective group policies could also have accomplished this as well. However, as additional computers are added to the Hardened Enclave OU, it would require an additional step of assigning the computer to a group that may have been overlooked. By making sub-OUs, it allows for a more seamless expansion. Although there is a security risk of making these servers in the Hardened Enclave members of the GIAC domain, the ability to secure communications using IPSec with Kerberos authentication and the management capabilities of group policy objects made these risks acceptable.

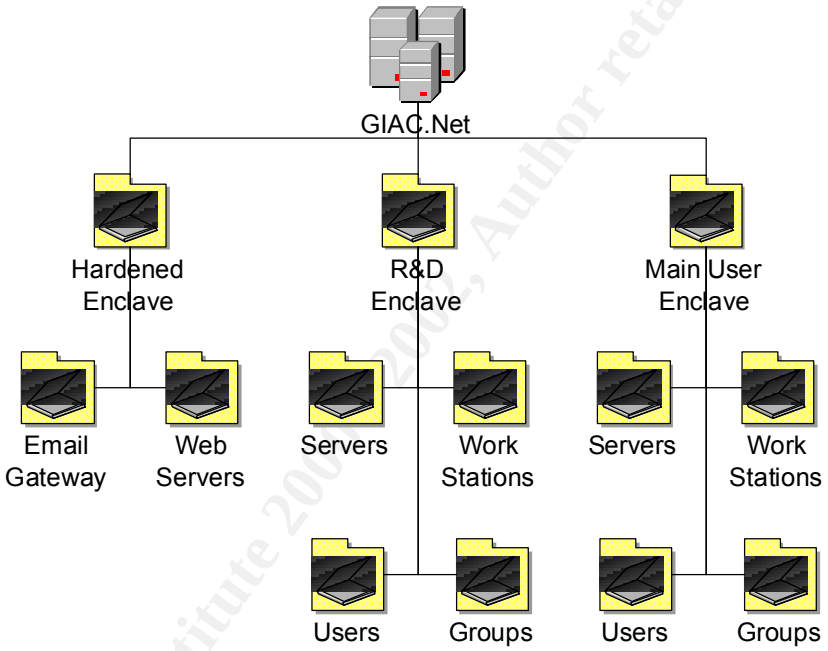

Figure 2 GIAC Enterprises Active Directory

The remaining two groups are also setup along security boundaries. The R&D Enclave OU has more stringent security concerns because this is the heart and sole of GIAC Enterprises. Should these servers be compromised or the data stolen, GIAC would suffer severe loss of profitability. The servers and workstations are separated to allow separate group policies and IPSec policies to be applied. Again this could have been accomplished though the use of permissions on the group policies, but this structure is cleaner and provides fewer opportunities for error. The users between the two groups are split to allow for distributed delegation of user accounts. Staff within the R&D enclave will manage users in the R&D Enclave OU. While R&D staff will also manage the groups, this is a different set of staff than those who manage the user accounts.

The Main User Enclave is another security boundary. While the information on these computers is important and needs to be protected, it is not as vital to the success of GIAC

Enterprises. For example, some could compromise the HR data and post the salaries of GIAC staff. This would be embarrassing and would cause problems for GIAC enterprises, but it would not be of the same magnitude of someone stealing GIAC's secrets for providing online fortune cookie saying. In this enclave, GIAC is reaching a balance between ensuring hackers cannot gain access to GIAC systems while also monitoring employee activity to protect from an employee attempting to steal information.

Group Policies

One of the great benefits of Windows 2000 is the ability to configure a vast array of computer settings available through the use of Group Policy Objects. Group Policy Objects are NT 4.0 Poledit on steroids! Through the use of Group Policy Objects, GIAC can set the security configuration for each of the various organizational units. Also management of these group policy objects can be delegated. This will be an important feature as the GIAC domain grows.

GIAC has defined group policies for several OUs within the GIAC domain. We will take a look at the various security settings that are defined and how these changes differ between the OUs. A large portion of GIAC's group policies is based on IPSec. While these IPSec policies are applied through the use of Group Policies, they will be defined is a separate section of this document.

Default Domain Policy

The following settings are included in the Default Domain Policy:

Password Policy:
- History 15 passwords
- Minimum age 2 days
- Maximum age 90 days
- Minimum password length 8 characters.
- Passwords must meet complexity requirements
- Disable Store passwords using reversible encryption.

Password history of fifteen passwords and minimum age of two days makes it difficult for users to reuse a password, as they would have to wait thirty days to reuse a password. The password complexity requirements require at least one from three of the four following areas, uppercase, lowercase, number and special character.

Account Policies
- Account Lockout Duration 0 Minutes
- Account lockout threshold – 3 failed attempts
- Reset account after 30 minutes

Account lockout duration of 0 locks out the account until an administrator unlocks it. The granularity of Active Directory makes it easy to delegate this task to helpdesk personnel. By requiring IT support to unlock the account, IT support personnel can verify the user was trying to access the account not some hacker trying a brute force attack. Account lock threshold of 3 failed attempts gives users a second and third chance to ensure they typed the password correctly and to ensure the caps lock is not on. By resetting the account after 30 minutes allows the users to make mistakes again when they return from lunch. This setting does allow a hacker to attempt a slow attempt to brute force attempt the password. The user could guess 2 passwords every 30 minutes without the account being locked out. However, this would only give the hacker 8640 guesses before the Maximum Password age would be reached. Still, the security event log should be checked regularly for such attempts.

Local Policies

Audit account logon events - Success/Failure
Audit account management - Success/Failure
Audit directory service access - Failure
Audit logon events - Success/Failure
Audit object access - Success/Failure
Audit policy change - Success/Failure
Audit privilege use - Success/Failure
Audit process tracking - none
Audit system events – Failure

Auditing logon successes and failures helps to detect random password hacks and stolen password break-ins. Audits for account management, policy change, and privilege use checks for misuse of privileges in the case of success and failure indicates someone attempts tasks they are not authorized. Audits for object access should only be initiated on sensitive files to ensure only the proper personnel access these files. GIAC audits all files stored on the R&D files server due to their sensitive nature.

Security Options

Additional Restrictions for anonymous connections – No access without explicit anonymous credentials.

Allow system to be shut down without having to log on – Disabled
Audit use of Backup and Restore privilege – Enabled
Digitally sign client communications (always) - Enabled
Digitally sign Server communications (always) - Enabled
Do not display last user name in logon screen

Lan Manager Authentication level – Send NTLMv2 response only\refuse LM & NTLM

Message text for user attempting to logon - “Unauthorized access to this computer is prohibited. If you do not have authorization to use GIAC computer systems leave NOW! All activity will be monitored.”

Message title for users attempting to logon – “Attention!”
Number of previous logons to cache – 0

Rename administrator account – Cookies
Rename guest account - Giac
Restrict CD-ROM access to locally logged-on user only – Enabled
Restrict floppy access to locally logged-on user only - Enabled
Secure channel: Digitally encrypt secure channel data (when possible) – not defined
Secure channel: Digitally sign secure channel data (when possible) - enabled
Secure channel: Require strong (Windows 2000 or later) session key – enabled
Send unencrypted password when connecting to third party SMB server - disabled
Smart Card Removal – Lock Workstation
Unsigned driver installation – Warn
Unsigned non-driver installation – warn

Additional restrictions for anonymous connections prevents hackers from gaining valuable information about users and shares, i.e. getting a listing of available shares and available usernames on a given machine. The requirement to digitally sign client and server communications ensures only members of the domain will be communicating within the user enclave. The secure channel communications require signed data when possible. Within the user enclave this should be always. We set Digitally encrypt secure channel data (when possible) to not defined. GIAC wants to be able to monitor traffic in the main user enclave. Encrypting data when possible would make it more difficult to monitor internal traffic. By not displaying the last username, we prevent someone with physical access from finding out who was last logged onto a computer. The setting to ensure NTLMv2 response only should not be needed as only Windows 2000 workstations and servers are on this network and these machines use Kerberos authentication instead of NTLM. However, this setting protects against the use of poor NTLM v.1 credentials to be used if a down level client is somehow connected to the network. While changing the name of the Administrator and guest accounts is only a speed bump to a hacker, it is hoped this will slow them down enough for our intrusion detection system to find their mischief.

Event Logs:
Maximum log size 10MB for each log.
Restrict Guest Access to each log
Retention Method – as needed for each log.

10 MB size for each log provides enough space to store several days' worth of files with out loosing data. Restricting guest access to logs ensures only authorized personnel can see the logs. The retention method is set to "as needed" to ensure data is not lost if the log files fill up. "Shutdown the computer when the security log is full" is not defined as this gives a hacker an opportunity for a denial of service attack. Instead Event Log Manager is utilized to ensure event logs are centrally collected for servers and critical machines.

System Services.
DNS client - Disabled
NetMeeting Remote Desktop sharing - Disabled
NTLM Provider – Disabled
Internet Connection Sharing – Disabled
TCP/IP NetBIOS helper - Disabled
Telnet – Disabled

In addition to being disabled, the permissions on these services will be set to Administrators and System – Full Control and the Interactive group – Read. The DNS client service provides client level caching of DNS names. This is not needed in the GIAC domain and has been disabled. GIAC does not want users to be able to access their desktops remotely. By disabling the NTLM service, down level clients cannot access shares within the GIAC domain. Because GIAC is running all Windows 2000, TCP/IP NetBIOS helper is not needed. Telnet is a security risk because it sends passwords in clear text. Why Microsoft added this to Windows 2000 is a mystery. Maybe in 5 years Microsoft will include an SSH service!

IPSec Policies
The IPSec policies for this and all group policy will be discussed in a separate section.

Administrative Templates
Windows Components
Netmeeting
Disable remote Desktop Sharing – Enabled
Internet Explorer
Disable Automatic Install of Internet Explorer Components
Disable Periodic check for Internet Explorer software updates
Disable software update shell notifications on program launch

Although the NetMeeting Remote Desktop Sharing service is set to disable, this is added protection so users will not be sharing their desktops. The IT group has set the default Internet Explorer Components that it allows to be installed on the desktop. Changes to this policy must be made using the approved configuration control process. Microsoft has a poor track record concerning security fixes and product updates. For this reason, the GIAC IT department will test and approved all fixes and updates for Microsoft products. Products and updates will be pushed out using the software package distribution within Group Policies.

System
Run these programs at user logon – Disabled
Disable the run once list – enabled
Disable legacy run list – enabled
Group Policy
Disable background refresh of Group Policy – Disabled

The first three settings in this list prevent unauthorized programs from running on workstations. This is a favorite spot for hackers to plant Trojans. By disabling the run one list, the legacy run list and run this programs at user logon, a hackers path to planting Trojans on GIAC computers is reduced. By disabling the disable background refresh of Group Policy (Note the use of double negatives ARRGGG!) group policies are refreshed even when a current user is logged on.

Network
Network and Dial-up connections (All)
Prohibit configuration of connection sharing – enabled

By enabling this policy, the sharing tab from the properties dialog box of a LAN connection and the Internet Connection Sharing page from the network connection wizard are removed.

Printers
Web-Based Printing – Disabled

This prevents servers from hosting web based printing.

User
Windows Settings
Internet Explorer maintenance
Authenticode Settings – Enable trusted publisher lockdown

This setting prevents users from always trusting a given certificate. The only trusted certificates are imported using Import current Authenticode Security Information. This reduces the threat of a "rogue" certificate being issued incorrectly. If you recall, this happened between Verisign and Microsoft a few months back.

Default Domain Controllers Policy

All of the settings that are applied in the Default Domain Policy are also applied in any other OU policy within the GIAC domain unless the policy is specifically block. Because of this, all of the settings in the Default Domain Policy will be applied to the domain controllers. The only settings we need to set in the Default Domain Controller Policy are settings that either change or are not configured in the Default Domain Policy.

Restricted Groups
Enterprise Admins – No members.
Schema Admins – No members.

By making the Enterprise Administrators and Schema Administrators restricted groups with no members, casual mistakes requiring Enterprise Administrator or Schema Administrator privileges are avoided. These changes can have very serious consequences

and may not be reversible without an authoritative restore. Before changes are made that require a schema administrator or enterprise administrator privileges, first, a domain administrator will need to add the appropriate account to the proper group. Adding members to these groups is audited and the audit logs are reviewed closely for such activity. In order to enhance performance, under the properties of this policy, the "Disable User Configuration settings" box is checked.

R&D Enclave Group Policy

Because of the highly sensitive nature of the business conducted within the R&D enclave, a more stringent set of security is required.

Local Policies
Security Options
Allow system to be shut down without having to log on – Disabled

Allowing systems to be shut down without logging on is disabled by default on Windows 2000 servers. This will also apply this setting to the workstations in the R&D Enclave.

Administrative Template
Network
Offline Files
Enables – Disabled

By disabling offline files, GIAC ensures that no server files are cached on the users workstations.

Hardened Enclave Web Servers OU

Under the Hardened Enclave Web Servers Group Policy, the following additional services settings will be made.

Alerter – Disabled
ClipBook – Disabled
Computer Browser – Disabled
DHCP Client – Disabled
Distributed File System – Disabled
Distributed Link Tracking Client – Disabled
Distributed Link Tracking Server – Disabled
Distributed Transaction Coordination – Disabled
DNS Client – Disabled
Fax Service – Disabled
File Replication Services – Disabled
Indexing Service – Disabled
Internet Connection Sharing – Disabled
License Logging Service – Disabled

Messenger – Disabled
NetMeeting Remote Desktop Sharing – Disabled
Network DDE – Disabled
Network DDE DSDM – Disabled
Print Spooler – Disabled
QoS RSVP – Disabled
Remote Access Auto Connection Manager – Disabled
Remote Access Connection Manager – Disabled
Removable Storage – Disabled
Task Scheduler – Disabled
TCP/IP NetBIOS Helper Service – Disabled
Telephony – Disabled
Telnet – Disabled

These services are not needed on the Web server. Furthermore the permissions on each of these services is set to Administrators and System – Full Control and the interactive group set to read.

Event Logs:
Maximum log size 50000MB for security log
Retention Method – Overwrite events older than 15 days for security log.

Under Security Settings, File System the following settings will be made;

D:\webs\www.giac.net\root D:\webs\www.giac.net\scr D:\webs\www.giac.net\images	Full Control: Administrators System	Read: Everyone
D:\webs\www.giac.net\exedll	Full Control: Administrators System	Traverse Folder / Execute Files: Everyone
%systemroot%\inetsrv\metabase.bin %systemroot%\inetsrv\metaback	Full Control: Administrators System	
%systemroot%\System32\Logfiles	Full Control: Administrators System	Read: Operators Authors
D:\	Full control: Administrator System	
%systemroot%\system32\Inetsrv\httpext.dll	No Access: Everyone	

Authors are not given permissions to create files on the production web site. Instead, once the files have been tested and approved, they are moved over in a scheduled update. This simplifies the permissions on the production server.

The following Audit setting will be made under Security Settings, File System:

%systemroot%\system32\logfiles – Audit Everyone group failed and success for all NTFS actions.
C:\ - Audit Everyone group failures for all NTFS actions and successes for Create Files / Write Data, Create Folders /Append Data, Delete subfolders and files, Delete, Change Permissions and Take Ownership.
D:\ - Audit Everyone group failures for all NTFS actions and successes for Create Files / Write Data, Create Folders /Append Data, Delete subfolders and files, Delete, Change Permissions and Take Ownership.
%systemroot%\inetsrv\metabase.bin – Audit failed and success NTFS access.
%systemroot%\inetsrv\metaback – Audit failed and success NTFS access.
%systemroot%\system32\tools – Audit all access.

Hardened Enclave Mail Servers OU

Under the Hardened Enclave Mail Servers Group Policy, the following additional services settings will be made.

Alerter – Disabled
ClipBook – Disabled
Computer Browser – Disabled
DHCP Client – Disabled
Distributed File System – Disabled
Distributed Link Tracking Client – Disabled
Distributed Link Tracking Server – Disabled
Distributed Transaction Coordination – Disabled
DNS Client – Disabled
Fax Service – Disabled
File Replication Services – Disabled
Indexing Service – Disabled
Internet Connection Sharing – Disabled
License Logging Service – Disabled
Messenger – Disabled
NetMeeting Remote Desktop Sharing – Disabled
Network DDE – Disabled
Network DDE DSDM – Disabled
Print Spooler – Disabled
QoS RSVP – Disabled
Remote Access Auto Connection Manager – Disabled
Remote Access Connection Manager – Disabled
Removable Storage – Disabled

Task Scheduler – Disabled
TCP/IP NetBIOS Helper Service – Disabled
Telephony – Disabled
Telnet – Disabled
Windows Management Instrumentation – Disabled
Windows Management Instrumentation Driver Extensions – Disabled

These services are not needed on the mail gateway. Furthermore the permissions on each of these services is set to Administrators and System – Full Control and the interactive group set to read.

Event Logs:
Maximum log size 50000MB for security log
Retention Method – Overwrite events older than 15 days for security log.

The following Audit setting will be made under Security Settings, File System:

C:\ - Audit Everyone group failures for all NTFS actions and successes for Create Files / Write Data, Create Folders /Append Data, Delete subfolders and files, Delete, Change Permissions and Take Ownership.
%systemroot%\system32\tools – Audit all access.

IPSec Policies

Within the GIAC domain, several IP filter lists and filter actions have been set up. The filter lists are:

1) All IP Traffic – this filter list acts on any IP traffic coming to or from the machines IP address
2) Hardened Enclave – this filter list acts on all IP traffic in the hardened enclave, IP addresses of 172.17.0.0/24
3) Main User Enclave – this filter list acts on all IP traffic in the main user enclave, IP addresses of 172.16.0.0/24.
4) R&D Enclave – This filter list acts on all IP traffic in the R&D enclave IP addresses of 172.17.0.0/24
5) SMTP traffic (25) – this filter list acts on all IP traffic on port 25.
6) Web traffic (80 & 443) – this filter list acts on all IP traffic on ports 80 (http) and 443 (https)
7) Internal Web Traffic – this filter list acts on all IP traffic on ports 80 and 443 that is with the R&D subnet and the Main User subnet

The following filter actions have been created:

1) Block – this action blocks all traffic to the machine.
2) Permit – this action allows the traffic to flow to the machine without any encryption of digital signatures.

3) Require Digital Signatures – this action requires digital signatures on all traffic to and from the machine. The security methods do not allow unsecured communication with non-IPSec aware computers and do not accept unsecured communication. The negotiated security in order of preference for these actions are:

AH integrity	ESP confidential	ESP Integrity	Key Lifetime
SHA1	None	None	0/0
MD5	None	None	0/0

4) Require Encryption – this action requires 3DES encryption on all traffic to and from the machine. The security methods do not allow unsecured communication with non-IPSec aware computers and do not accept unsecured communication. The negotiated security in order of preference for these actions are:

AH integrity	ESP confidential	ESP Integrity	Key Lifetime
None	3DES	SHA1	100000/900
None	3DES	MD5	100000/900

5) Require either encryption or signature – this action requires either 3DES encryption or digital signature on all traffic to and from the machine. The security methods do not allow unsecured communication with non-IPSec aware computers and do not accept unsecured communication. The negotiated security in order of preference for these action are:

AH integrity	ESP confidential	ESP Integrity	Key Lifetime
None	3DES	SHA1	100000/900
None	3DES	MD5	100000/900
SHA1	None	None	0/0
MD5	None	None	0/0

These filter lists and filter actions are combined to form the IP Security Policies for the different group policies. IPSec policy rules are applied from most specific to least specific. Also, only the last IPSec policy applied to a computer takes effect. This means only the IPSec policy within the last group policy is applied.

Default Domain Policy

The IPSec policy for the Default Domain Policy is called the Default IPSec Policy and combines the following filters and actions in the order they will be applied. This policy utilizes Kerberos for the authentication method.

1) R&D Enclave – Require Digital Signature
2) Main User Enclave – Require Digital Signature
3) Hardened Enclave – Require Digital Signature
4) All IP Traffic – Permit

This policy requires any traffic within the GIAC domain, either from the hardened enclave or the user enclave, to be digitally signed while allowing normal traffic to and from the Internet. By digitally signing traffic, all traffic from 172.16.0.0/24, 172.16.0.0/24 or 192.168.1.0/32 must be a member of the GIAC domain. This is because GIAC does not trust any additional Kerberos realms and Kerberos is the only authentication method used for this policy. The digital signatures of this policy ensure local communication is only with domain members. Because the traffic is digitally signed and not encrypted, the traffic can still be monitored. This policy will be in effect for the workstations in the Main User Enclave OU.

R&D Enclave Policy

The R&D enclave OU has needs for a more stringent IPSec policy. This policy, named R&D enclave, utilizes Kerberos as the authentication method and combines the following filters and actions:

1) R&D Enclave – Require Encryption
2) Main User Enclave – Require either Encryption or Digital Signature
3) Hardened Enclave – Require Digital Signature
4) All IP Traffic – permit

By requiring digital signatures within the R&D enclave, GIAC ensures all traffic between the R&D enclave workstations and the R&D enclave servers is encrypted. This traffic is only readable by the machines that participate in the communication. This meets GIAC's goal of encrypting the traffic within the R&D enclave.

R&D Enclave Servers Policy

The IPSec policy applied through the R&D enclave OU is not sufficient for the servers with the R&D Enclave. Another IPSec policy is created, R&D Enclave Servers, for this purpose. This policy again utilizes Kerberos as the authentication method and combines the following filters and actions:

1) R&D Enclave – Require Encryption
2) Main User Enclave – Require Encryption
3) All IP Traffic – Block

Rule 1 provides encrypted traffic within the R&D Enclave per GIAC directives. While clients from the Main User Enclave should not be communicating with the servers in the R&D Enclave, the servers still need to communicate with the Domain Controllers in Main User Enclave address space. By requiring this traffic to be encrypted, the workstations, which can only do digital signature with the R&D Enclave addresses, cannot communicate with the R&D servers. Finally the R&D servers have no reason to communicate with the Internet or the machines in the Hardened Enclave, thus this traffic is blocked. This creates some problems for users within the Main User Enclave that have

a need to access the servers within the R&D enclave. GIAC is planning to implement an RRAS server to provide an internal VPN capability, but because of cost and time involved this was not included in this initial security plan.

Main User Enclave Policy

The servers within the Main User Enclave OU will have a different IPSec policy applied through GPO than the Default IPSec Policy. This policy, Main User Server policy, utilizes Kerberos as the authentication method and combines the following filters and actions in the order they will be applied:

1) R&D Enclave – Require either Encryption or Digital Signature
2) Main User Enclave – Require either Encryption or Digital Signature
3) Hardened Enclave – Require Digital Signature
4) All IP Traffic – block

This policy allows the servers in the Main User Enclave to communicate with the workstations in the R&D enclave. Traffic between these machines is encrypted. Traffic within the Main User Enclave is digitally signed to allow monitoring of the packets. The servers need to communicate with the Hardened Enclave to allow the automatic updates of the web pages, which occurs nightly. Finally, all Internet traffic is block to ensure these machines do not communicate with the Internet.

Hardened Enclave Web Policy

The Hardened Enclave has no IPSec policy at the OU level, but it does have specific policies for it sub-OU's. The External Web Servers IPSec policy is applied to the Web Servers sub-OU in the Hardened Enclave. This policy utilizes Kerberos authentication and implements filters in the following order:

1) Internal Web Traffic – Require Digital Signature
2) Web traffic (80 & 443) – permit
3) Main User Enclave – Require Digital Signature
4) Hardened Enclave – Require Digital Signature
5) All IP Traffic – Block

By requiring traffic between the External web server and internal workstations to be digitally signed, GIAC moving toward all communication between internal clients will be digitally signed. Hence they can concentrate on outside traffic simply by eliminating traffic on the IPSec ports, TCP 50 and 51 and Kerberos port, 88. The rule for internal web traffic is applied before the Internet web traffic because this rule is more specific.

Hardened Enclave Email Gateway Policy

Also within the Hardened Enclave is Email Gateway OU. The GPO for this OU applies the Mail Gateway IPSec policy. This policy utilizes Kerberos authentication and implements filters in the following order:

1) Internal SMTP traffic – Require Digital Signature
2) SMTP traffic (25) – Permit
3) Main User Enclave – Require Digital Signature
4) Hardened Enclave – Require Digital Signature
5) All IP Traffic – block

The internal SMTP traffic should only be between the Exchange server and the email gateway. Any other SMTP traffic is suspicious and should be investigated. Because the email gateway receives mail from the Internet, traffic on port 25 is set to permit. Any traffic between the Main User Enclave and the Hardened Enclave, as well as traffic within the Hardened Enclave must be digitally signed.

Domain Controllers Policy

The IPSec policy that is applied to the domain controllers is called Domain Controllers IPSec Policy. This policy utilizes Kerberos authentication and implements filters in the following order:

1) R&D Enclave – Require either Encryption or Digital Signature
2) Main User Enclave – Require Digital Signature
3) Hardened Enclave – Require Digital Signature
4) All IP Traffic – Block

This policy requires Digital Signature or Encryption to all Domain Controllers. This works to implement GIAC Enterprises policy of internal traffic should be signed or encrypted. All traffic to and from the Internet is blocked, as these machines should not be connected to the Internet. NOTE: With this policy, it is not possible to join new computers to the domain. In order to join the domain, the IPSec policy Domain Controllers Join Domain, must be applied to the Domain Controller in the Main User Enclave. This policy utilizes Kerberos authentication and implements filters in the following order:

1) R&D Enclave – Requires either Encryption or Digital Signature
2) Main User Enclave – Permit
3) Hardened Enclave – Require Digital Signature
4) All IP Traffic – Block

This maintains IPSec security between the R&D Enclave and the Hardened Enclave. This requires all computers to be on the Main User Enclave subnet when they join the domain. NOTE: Per Microsoft Knowledge Base article Q254949, Microsoft does not support using IPSec between domain member and domain controllers. This is because it is not possible for non-domain computers to get the initial IPSec policy. However, by

loosening the policy while the computer joins the domain, this short fall is circumvented. All computers must be in the subnet of the Main User Enclave. Once the computer joins the domain, it is possible to move the computer to a different subnet.

Non-Group Policy Security Settings

Some settings cannot be easily set through the use of group policies. The following 7 registry settings are set to harden the TCP/IP stack and make it more resilient. These changes will make the TCP/IP stack more resilient when under a SYN flood attack, prevent Windows 2000 from changing TCP/IP settings when it receives certain types of packets, and protect against name release attacks. These and other registry settings are set in a harden.reg file. This file is then delivered to the workstations using group policy via startup scripts. Because the startup scripts are run every time the computer reboots, these settings will continually be reapplied.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: Reg_DWORD
Value: SynAttackProtect = 2
This key provides protection against SYN attacks by causing TCP to time out more quickly if it appears there is a SYN-Attack in progress.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: REG_DWORD
Value: EnableDeadGWDetect = 0
This key prevents Windows from switching gateways.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: REG_DWORD
Value: EnablePMTUDiscovery = 0
This sets the MTU to 576 bytes for all connections not on the local subnet. This prevents an attacker from forcing the MTU to a small number and over working the TCP/IP stack.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: REG_DWORD
Value: KeepAliveTime = 300,000
Changes the frequency TCP sends a keep-alive packet to verify an idle connection is still valid. This changes the value to 5 minutes from the default 2 hours.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
Type: REG_DWORD
Value: EnableICMPRedirects = 0

Prevents Windows 2000 from altering its route table in response to ICMP redirect messages.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\
Type: REG_DWORD
Value: NoNameReleaseOnDemand = 0
Provides protection against name-release attacks.

Key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<interface>\
Type: REG_DWORD
Value: PerformRouterDiscovery = 0
Prevents incorrect router advertisements.

It is desirable to have all communication between domain controllers to be either encrypted or signed using IPSec policy. Ideally this would include the authentication process using Kerberos. The default release of Windows 2000 did not allow Kerberos traffic to be protected using IPSec. In Service Pack 1, Microsoft fixed this oversight. (See Microsoft Knowlegebase article Q254728) In order for Kerberos traffic to be protected, the following registry entry must be made. This entry must be made on each domain controller. This registry change has been packaged in a file called IPSecKerberos.reg and is manually changed on the domain controllers using the registry file. With this entry, Kerberos traffic between domain controllers can use IPSec; however, there will still be a few packets sent during the boot process that will not be protected using IPSec.

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC\
Type: REG_DWORD
Value: NoDefaultExempt=1
This value secures Kerberos traffic between domain controllers using IPSec.
Q254728

Security configuration for external Web server

The most vulnerable system in the GIAC network is the external web server. By design, this system allows unsolicited traffic on http port 80. Microsoft has distributed patches to fix many bugs in IIS since it inception. The recent worms that have specifically attacked IIS such as Nimbda and Code Red have made the security of IIS appear to be lacking. However, in both of these cases these worms exploited vulnerabilities that were already fixed by Microsoft. Furthermore, by taking care during the setup and configuration of IIS, these worms could have been avoided even if the Microsoft supplied patches had not been applied. This next section will highlight the steps taken to secure GIAC's external web server.

The system files will be installed on drive C. During the setup of IIS, the inetpub directory will be installed on drive D. Both of these drives are configured with NTFS. During the installation of the web server, the system files were installed in the C:\Web directory instead of the C:\Winnt directory. During the setup of Windows 2000, Indexing Server was not installed. Options for the Internet Information Service (IIS) are as follows:

- Common files
- Internet Information Services Snap-in
- SMTP Service
- World Wide Web Server

After the installation completes, the files in C:\Web\web\printers, C:\Web\system32\Inetsrv\iisadmpwd, D:\inetpub\AdminScripts, and C:\program files\Common files\system\msadc folders are removed. C:\Web\web\printers contains the files for Internet Printing, which is not needed on this server. While the D:\inetpub\AdminScripts folder has some valuable scripts, they should not remain on the server. Instead they can be placed on a CDROM and carried to the machine when necessary. The msadc files removes support for Remote Data Services.
We need to setup the file structure for our web server. Create a folder on the D drive called Webs\www.giac.net. Under this folder, create the following sub folders:

- \root
- \scr
- \exedll
- \images

Use the IIS snap-in to move the default web site to d:\webs\www.giac.net\root. Create virtual directories under the www.giac.net web root for inc, scr, exe, and images. The IIS permission on the root and images folder are set to read with the execute permissions set to "None." The root folder and its sub folders will only contain static .html pages. The images folder and its sub folders will contain any graphics that are needed on the site. The scr folder is for storing script files such as .asp, .stm, .shtm, .shtml, .pl etc. The IIS permissions on the /scr folder is set to none and execute permissions are set to scripts only. On the /exedll folder, the IIS permissions are set to none and the execute permissions are set to scripts and executables. This folder is for storing .exe and .dll files.

By default Windows 2000 turns on NetBIOS over TCP/IP. GIAC's 100% Windows 2000 system has no need for NetBios over TCP/IP. Furthermore, our web server has no need or any protocols other than TCP/IP. Luckily, Windows 2000 provides an easy way to turn off NetBIOS over TCP/IP. We disabled NetBIOS over TCP/IP by selecting Start, Control Panel, Network and Dial-up Settings. Select the local area network setting, the properties button, Internet Protocol (TCP/IP) and the properties button. Click on the advanced button. Select the WINS tab and select the radio button for Disable NetBIOS over TCP/IP.

Remote Data Services (RDS) allows IIS web servers to act as a front end to a database. This functionality is not needed at GIAC and needs to be turned off. Earlier in this paper we addressed two of the three items needed to remove this functionality, removing the /MSADC virtual folder and deleting the files in the C:\program files\common files\system\msadc directory. One additional step that needs to be taken is to delete the HKLM\system\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch value using regedt32. This eliminates RDS support for IIS.

From within the IIS snap-in under Web Site Properties, bind the web site to 192.168.1.10, not to all assigned. This ensures the web server is only listening on a particular IP address instead of listening to all assigned IP addresses.

By default, the IUSR_WWW is a member of the guest group. This can allow the IUSR_WWW account access to some resources where it should not be allowed access. To prevent this, remove the IUSR_WWW from the guest group.

From the IIS snap-in, in the www.giac.net web site properties, the Home Directory Tab and the configuration button, remove all extensions except the .asp extension. Select the .asp entry and select edit. Change the extension from .asp to .htm. Have the developers use the .htm extension for their asp pages instead of .asp. Under the Verbs select the Limit to radio button and ensure only GET, POST appear in this list. Ensure that the Check that file exists box is checked. Select the App Options tab and uncheck the Enable parent paths box. Go to the properties for the inc, exe and images folders. Select the configuration button and remove the extension for .htm. This hides the fact that you are using .asp pages as the urls look like they are static web pages. By removing the remaining extensions, we eliminate several possible avenues of attack.

Two potentially dangerous dll files are scrrun.dll and Wshom.dll. Scrrun.dll allows wsh script access to files system objects. By having this dll registered on the web server, a hacker could potentially upload a wsh script file in a web page and gain access to data on the web server's hard drive. The second dll, wshom.dll is needed for Windows Scripting host to run. Because these are not utilized in the web environment at GIAC, these files should be unregistered with the following commands:

```
Regsvr32 scrrun.dll /u
Regsvr32 wshom.dll /u
```

There are two changes we need to make set in the Metabase. Because the GIAC web server does not utilize server side include files, the following Metabase value is set.

```
Key:  /LM/W3SVC
Type:  REG_DWORD
Value: SSIExecDisable=1
User Type: File
```

This value is set with the following command:

Cscript.exe adsutil.vbs set w3svc/SSIExecDisable true

Also, by default the IP address of the web server appears in the content-location field of the header. This IP address is the internal address of the server. This can give a hacker information about GIAC's internal IP setup. To avoid releasing this information, the following Metabase value is set.

Key: /LM/W3SVC
Type: Dword
Value: UseHostName = 1
User Type: Server

This value is set using adsutil.vbs with the following command line:

Cscript.exe adsutil.vbs set w3svc/UseHostName True

Many of the commands needed to manage the web server can also be of great use to a hacker when trying to gain access to the system. In order to prevent their misuse, the following files have been move to a new folder, C:\Web\system32\tools:

ARP.EXE	ISSYNC.EXE	REGINI.EXE
AT.EXE	MSIEXEC.EXE	REGSVR32.EXE
ATSVC.EXE	NBTSTAT.EXE	RECES.EXE
ATTRIB.EXE	NET.EXE	ROUTE.EXE
CACLS.EXE	NET1.EXE	RSH.EXE
CLIPSRV.EXE	NETSH.EXE	RUNAS.EXE
CMD.EXE	NETSTAT.EXE	RUNONCE.EXE
COMMAND.COM	NSLOOKUP.EXE	SYSEDIT.EXE
CSCRIPT.EXE	POING.EXE	SYSKEY.EXE
DEBUG.EXE	POLEDIT.EXE	TELNET.EXE
EDIT.EXE	POSIX.EXE	TFTP.EXE
EDLIN.EXE	QBASIC.EXE	TRACERT.EXE
FINGER.EXE	QFECHECK.EXE	TSKILL.EXE
FTP.EXE	RCP.EXE	WSCRIPT.EXE
HYPERTRM.EXE	REGEDIT.EXE	XCOPY.EXE
IPCONFIG.EXE	REGEDT32.EXE	

Auditing of these files has been setup using the web server group policy.

Once the web server was completely setup, the following command was run:

Sfc.exe /scannow

This command updates the \dllcache folder with all the changes and modifications made when applying Service Packs and hotfixes. Once these changes are made, if any of the files protected are modified or deleted, Windows File Protection (WFP) will check the file against its catalog files that are stored in %systemroot%\sytem32\catroot and replace the files from the %systemroot%\system32\dllcache. WFP also creates an Event ID 64002 in the system event log. These events are monitored and immediate notification is made to the systems administrator when 64002 events occur. Finally we install URLSCAN from Microsoft. URLSCAN will scan url requests before they are passed onto the web server. Microsoft provides a default urlscan.ini file to configure URLSCAN. The following changes are made to the urlscan.ini file:

```
UseAllowExtension=1
AllowHighBitCharacters=0
```

UseAllowExtension changes the default to only permit .asp, .htm, .html, .txt, .jpg, .jpeg, .gif files. We add one additional file to this list, .pdf. The AllowHighBitCharaters denies sending UTF8 or MBCS characters be sent to the web server.

Now that the external web server is setup, we need to setup two additional web servers. The first server is the Test server that is setup in the Main User Enclave. It will mirror the external server as exactly as possible. Some NTFS directory and file permissions will be loosened slightly to allow for easier access to place files on this server. To accomplish this, a web administrators group is created in Active Directory. This web administrators group will be given write and delete access to all files in the d:\webs\www.giac.net directory. Final testing of any changes to the web server will be tested here prior to moving being move to the production web server.

The second web server that is setup will also mirror the configuration of the external web server with the modified permissions stated above. This server will be in the R&D enclave and will be used to develop new services and products within the online fortune cookie business that will be move onto the test server and into production if they pass the rigorous testing required to ensure they meet GIAC's security requirements. On these two servers, we have two reasons to setup the security. The first is to protect these machines from internal hackers, and the second is to ensure the web applications being developed will work as designed on the production server. By having these servers, especially the test server match the test server match the security configuration of the production server, GIAC ensures the applications will work in the production environment.

Email Gateway Configuration

The email gateway server that is setup in the Hardened Enclave needs to be hardened to prevent against attacks. In addition to hardening the TCP/IP stack which is done on all the computers in the domain, we want to move potentially dangerous command to the %systemroot%\system32\tools directory. The commands we will be moving are:

ARP.EXE	ISSYNC.EXE	REGINI.EXE
AT.EXE	MSIEXEC.EXE	REGSVR32.EXE
ATSVC.EXE	NBTSTAT.EXE	RECES.EXE
ATTRIB.EXE	NET.EXE	ROUTE.EXE
CACLS.EXE	NET1.EXE	RSH.EXE
CLIPSRV.EXE	NETSH.EXE	RUNAS.EXE
CMD.EXE	NETSTAT.EXE	RUNONCE.EXE
COMMAND.COM	NSLOOKUP.EXE	SYSEDIT.EXE
CSCRIPT.EXE	POING.EXE	SYSKEY.EXE
DEBUG.EXE	POLEDIT.EXE	TELNET.EXE
EDIT.EXE	POSIX.EXE	TFTP.EXE
EDLIN.EXE	QBASIC.EXE	TRACERT.EXE
FINGER.EXE	QFECHECK.EXE	TSKILL.EXE
FTP.EXE	RCP.EXE	WSCRIPT.EXE
HYPERTRM.EXE	REGEDIT.EXE	XCOPY.EXE
IPCONFIG.EXE	REGEDT32.EXE	

Auditing of these files has been setup using the web server group policy.

After the email gateway was completely setup, the following command was run:

Sfc.exe /scannow

This is the same process we used on the external web server to update the \dllcache directory.

As part of regular maintenance for servers in the GIAC, domain sfc.exe /scannow is run once a month. On the servers in the hardened enclave, the full path for the sfc.exe file must be supplied since %systemroot%\system32\tools is not part of the path. Also a visual basic script, hfnetcheck.vbs, is run nightly. This script runs the hfnetchk program from Microsoft, parses the output and sends a report via email to the systems administrator. This report is run on each of the servers and domain controllers in the GIAC domain. While this is not the primary means used to ensure the production servers are up to date on service packs, it provides a good backup method to ensure no servers are overlooked when applying hotfixes.

As this document was going to press, Microsoft released a security rollup package for Windows 2000. (See Microsoft Technet article http://www.microsoft.com/technet/security/news/w2ksrp1.asp) This new package will replace 15 of the current hotfixes that are needed when securing a new install of Windows 2000. The remaining hotfix, Q313675, is a security rollup for Internet Explorer 6.0. The Security Rollup package is currently being test on GIAC's test network and will be deployed once it passes integration testing. This demonstrates the need for constant diligence to remain current with security patches and fixes.

References:

Microsoft Paper: *Security Consideration for Network Attack*
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/website/dosrv.asp

Microsoft Knowledgebase article Q254728
http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q254728

Olsen, Gary L. Windows 2000 Active Directory Design & Deployment United States of America: New Riders Publishing, 2001

Kurtz, George; McClure, Stuart; Scambray, Joel Hacking Exposed Network Security Secrets & Solutions Berkley, California: Osborne/McGraw-Hill, 1999

Fossen, Jason et. al. Securing Internet Information Server 5.0 SANS Institute

Microsoft, *Windows 2000 Security Rollup Package 1 Now available*,
http://www.microsoft.com/technet/security/news/w2ksrp1.asp