Global Information Assurance Certification Paper

GIAC Enterprises – Security Of a Windows 2000 Network Infrastructure

Securing Windows
GCWN Practical Assignment
Version 3.1 – Option 1
By Barrie Rody

Table of Contents

Assignment Introduction

This paper is to outline the Windows 2000 Infrastructure at a fictional company, GIAC Enterprises. It will outline the security procedures used to secure a Windows 2000 based network. It will include two diagrams: one of the network infrastructure and one of the Active Directory structure. There is a general overview of the company as well as an overview of the network infrastructure of the company. The Active Directory structure of the company will be explained. The various group policies used throughout the Active Directory will be outlined and explained. Additional security requirements such as web server security will also be covered. Finally, there is a short section on disaster recovery.

1. GIAC Enterprises Introduction

Gadgets, Inventive And Creative (GIAC) Enterprises is a company that develops and markets household gadgets. These gadgets are the kind typically found on late-night infomercials. Due to the highly competitive nature of the market, security is extremely important.

GIAC does not manufacture the gadgets that it creates, as it out-sources the manufacturing to keep from dealing with the overhead necessary in maintaining manufacturing plants. The company's focus is dedicated to inventing and then marketing the products.

The company has 2 locations, the head office and a remote location for the Research and Development (R&D) department.

The Head Office location consists of the following departments:

1. Sales / Marketing – 100 people
    a. The Sales portion of this team is responsible for taking phone-in orders for the products. The majority of orders are placed over the phone. They are also responsible for checking the web-based orders to assure that they are correct before the orders are processed.
    b. The Marketing portion of this team is responsible for creating the various ad campaigns to market the products.
2. Finance – 10 people
    a. The Finance department is responsible for typical finance jobs such as payroll and expense claims.
3. Executives / Administration – 10 people
    a. This group consists of the CEO, Vice-Presidents, Human Resources and the Office Manager.
4. Information Technology (IT) – 6 people
    a. The IT department is responsible for maintaining the computer and network infrastructure for the company. At the Head Office location there is one Network Engineer, two Systems Administrators and three Desktop Support Specialists. Despite being in different

locations, the Network Engineers share what work they can and are, as a team, responsible for the network infrastructure. The same holds true for the Systems Administrators. This is a little more difficult for the Desktop Support Specialists, as they typically need to be in the same physical location to do their job. Therefore the Desktop Support Specialists are responsible for the desktops that are located in the same office that they are currently working. There is a rotation schedule so that all members of IT have the opportunity to rotate between the two office locations.

The R&D location consists of the following departments:

1. Research and Development (R&D) – 50 people
    a. The R&D department is responsible for inventing new products and improving old ones. This includes everything from the conception of the idea to preparing the exact specifications for products to be sent out to manufacturing. The gadget business is highly competitive, so security is important within this group.
2. IT – 4 people
    a. The IT department is responsible for maintaining the computer and network infrastructure for the company. At the remote R&D location there is one Network Engineer, one Systems Administrator and 2 Desktop Support Specialists.

The R&D location has its own members of the IT department onsite, but they are still considered members of the company-wide IT department.

2. Network Design

The network hardware is all Cisco equipment that is maintained by the network engineers that are part of the IT Department. The actual network equipment is beyond the scope of this paper; therefore it is not discussed in detail. It will not be specified in the physical architecture diagram.

The servers are all Dell equipment running Windows 2000 Server with Service Pack 2, except the two SQL Servers. The SQL Servers are running Windows 2000 Advanced Server with Service Pack 2 and SQL Server 2000 with Service Pack 2. The Exchange servers are Exchange 2000 Service Pack 2. The Web Servers are using IIS 5. The client machines (desktops and laptops) are all running Windows 2000 Professional Service Pack 2.
Relevant hot-fixes are applied only after careful research and testing on the test network.

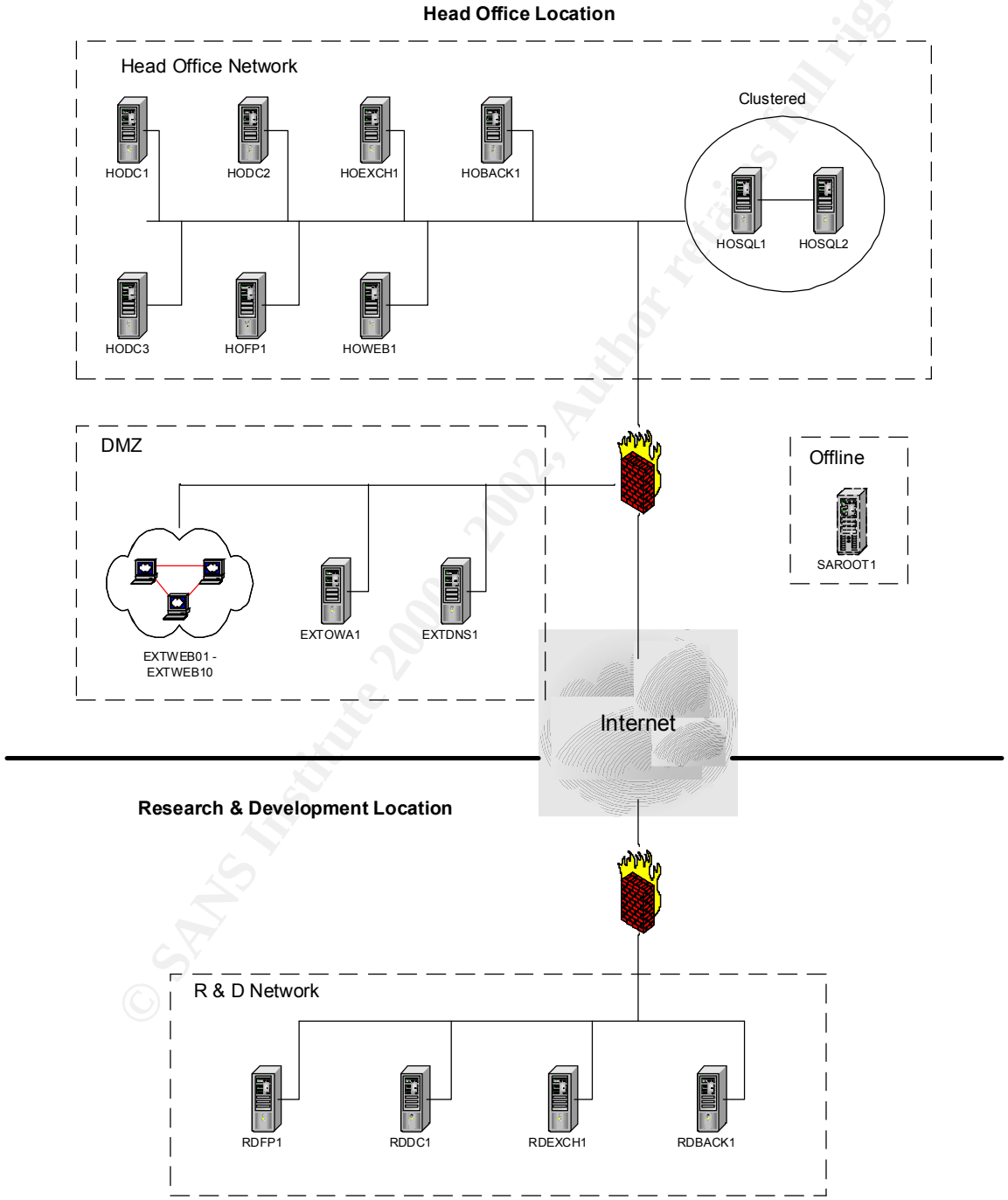
The Test Network is completely independent of the production network and will be discussed later.

All servers, including the test network servers are contained in locked, air-conditioned servers rooms. The doors to these rooms have a keycard entry

system and only those that need access to do their jobs will have access to the server rooms.

2.1 Physical Architecture Diagram

The networking hardware, except the firewalls, is not included in the diagram as it is out of the scope of this paper.



2.2 IP Infrastructure

All servers are configured with static IP addresses. All workstations are configured to use DHCP. Since the operating systems on the network are exclusively Windows 2000, there is no need to run WINS. There will be a total of four subnets for the network, two for each site. Each site will have one subnet for servers and one for clients. This is not counting the DMZ which will, of course, be on its own subnet.

2.2.1 DNS

The external DNS namespace (giac.com) is maintained in the DMZ on one Windows 2000 server. The server is not part of the Active Directory Domain. The DNS zone in the DMZ will be manually configured and then it will be configured to not allow any dynamic or unsecured updates. It will only be updated manually.

The internal DNS namespace (win2k.giac.com) is maintained with an Active Directory integrated zone on all domain controllers. By using Active Directory integrated zones we gain the following benefits:

1. Multi-Master Replication – Any client can register with any DNS server and the DNS records for that client will be replicated to all other DNS servers. This is far better than all clients registering with the single Primary DNS server and then doing zone transfers out to all Secondary servers.
2. Incremental Zone Transfers – When records are replicated out to the other DNS servers, only changed records are replicated, not the entire zone database.
3. Fault Tolerance – Since all DNS servers are considered equals and can all receive updates, there is no single point of failure as long as you have more than one DNS server.
4. Improved Security – DNS records, as with all Active Directory objects, can have their own access control lists. Also, the zone can be setup to only accept secure updates, meaning that clients would need to log into the Active Directory domain before they could register themselves with DNS.

2.2.2 DHCP

DHCP will be running on two domain controllers at the head office site (HODC1, HODC2) and one domain controller at the R&D site (RDDC1). There will be one scope per site that will correspond to the subnet that the clients will use. The two domain controllers in the head office site will split their scopes in a 70/30 fashion. This means that one DHCP server will have a scope containing 70% of the IP addresses for the subnet and the other DHCP server will have 30% of the same subnet.

2.3 Server Descriptions

All servers will be Dell equipment running Windows 2000 Server, Service Pack 2. The model of each server will vary depending on its role. For example the File and Print Servers need more disk space than the domain controllers, therefore they will be configured with larger disks in a RAID-5 configuration.

2.3.1 Domain Controllers

The three main domain controllers (HODC1, HODC2, RDDC1) will all be running on identical hardware. The Active Directory roles of these computers will be discussed later.

Dell PowerEdge 1650	
RAM	1 GB 133MHz SDRAM
Processor	2 x Intel Pentium III 1.4GHz, w/512k cache
Hard Disks	2 x 18 GB 10k RPM in a RAID 1 mirror set
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team

HODC1 is also an Issuing Certificate Server, having been issued a certificate from the Stand-Alone Root Certificate Server SAROOT1. SAROOT1 will be discussed below. The certificates that HODC1 will be issuing are for use in the VPNs that are used to tunnel from the DMZ to the corporate network. These will be discussed later.

The third domain controller in the head office (HODC3) will be running on a lesser server with an IDE drive configuration. This will be done to allow for an easy backup through a disk image utility and easy creation of a test network with an identical Active Directory setup. As the third domain controller, it will be easy to temporarily pull HODC3 offline and run Norton Ghost to take a backup of the system. This will be further explained in the Disaster Recovery section. Using this Ghost image and an identically configured server, it will be easy to create a test network from scratch that has identical AD information to our production network. This will be further explained in the section outlining the test network.

Dell PowerEdge 350	
RAM	1 GB 133MHz SDRAM
Processor	1 x Intel Pentium III 850MHz, w/256k cache
Hard Disks	1 x 20 GB IDE hard drive
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team

Since the third DC is for backup purposes only, it will not run DHCP and will not be allowed to authenticate clients, but it will still maintain an AD Integrated DNS zone for win2k.giac.com. To prevent HODC3 from authenticating clients some

changes will need to be made to the DNS SRV records for HODC3. By setting the Priority of the SRV records of HODC3 to something higher than that for HODC1 and HODC2, then it will not be allowed to authenticate users unless the first two domain controllers are unreachable.

2.3.2 File and Print Servers

There will be one File and Print Server per site (HOFP1, RDFP1). Disk space is far more important on these machines, so they will be configured with larger disks in a RAID-5 configuration. They will serve no functions other than to provide file space and to host the printers for clients in their respective sites.

Dell PowerEdge 2650	
RAM	2 GB SDRAM
Processor	2 x Intel Xeon 2.0GHz, w/512k cache
Hard Disks	5 x 36 GB 10k RPM in a RAID-5 array for 144GB of usable space
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team

2.3.3 Exchange Servers

There are two Exchange Servers, HOEXCH1 in the head office and RDEXCH1 at the R&D location. There is an Exchange front-end server used for Outlook Web Access, EXTOWA1, but that will be discussed with the IIS servers as it also runs IIS. There are also two Exchange Servers for the Test Network. Their hardware is identical to the two production servers. They will be discussed under the Test Network description below.

Dell PowerEdge 2650	
RAM	2 GB SDRAM
Processor	2 x Intel Xeon 2.0GHz, w/512k cache
Hard Disks	5 x 36 GB 10k RPM in a RAID-5 array for 144GB of usable space
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team

2.3.4 Backup Servers

There will be one Backup Server per site (HOBACK1, RDBACK1). These machines will be dedicating to backing up the other servers. They will serve no other functions.

Dell PowerEdge 2650	
RAM	1 GB SDRAM

Processor	1 x Intel Xeon 2.0GHz, w/512k cache
Hard Disks	2 x 18 GB 10k RPM in a RAID 1 mirror set
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team
Tape Backup	Spectralogic Treefrog with 2 drives

The backup server for the head office (HOBACK1) location will also have one extra 10/100 NIC for use in connecting to the test network. The NIC team connected to the production network and the single NIC connected to the test network will never be permitted to be connected at the same time. When moving the server from production to test, the network cables going to the adaptive team will be disconnected and then the cable for the test network will be plugged in.

2.3.5 IIS Servers

There are 12 web servers total. EXTWEB01 – EXTWEB10 and EXTOWA1 are in the DMZ. HOWEB1 is installed within the head office network. The Web Servers, both internal and external, are configured with identical hardware.

Dell PowerEdge 1650	
RAM	2 GB SDRAM
Processor	1 x Intel Xeon 2.0GHz, w/512k cache
Hard Disks	2 x 18 GB 10k RPM in a RAID 1 mirror set
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team

EXTOWA1 is dedicated to being a front-end server for Exchange 2000 and hosts Outlook Web Access (OWA). This allows GIAC employees to access their mail and calendars from anywhere on the web. Security is maintained by using a VPN between EXTOWA1 and the two domain controllers that it must use to authenticate the OWA users. This will be discussed further in the Additional Security Section.

The external web servers (EXTWEB01 – EXTWEB10) are installed behind a hardware load balancer. The web servers in the DMZ are used to host the company's e-commerce site. They connect to the SQL server that is installed within the head office network. They also use a VPN to connect to servers inside the corporate network, but this time to the SQL servers.

The internal server (HOWEB1) is used to maintain the company's Intranet site.

2.3.6 SQL Server

There are two SQL Servers (HOSQL1, HOSQL2). They are the centerpieces of the company's e-commerce initiative. While e-commerce isn't the most important aspect of the company, it is still important that these servers stay working. As such, they are configured in a cluster and have high hardware demands.

Dell PowerEdge 6650	
RAM	8 GB DDR SDRAM
Processor	4 x Intel Xeon 1.5GHz, w/512k cache
Hard Disks	5 x 36 GB 10k RPM in a RAID-5 array for 144GB of usable space
Network Adapters	2 x Onboard 10/100 NICs configured in an Adaptive Load Balancing Team

2.3.7 Root Certificate Server

There is only one Root Certificate Server SAROOT1. It is not a member of the Active Directory domain nor is it connected to the network in any way. It was brought online to issue a certificate to HODC1 and then brought offline again. It does not require much in the way of hardware and is therefore run on a desktop class machine. Once offline, SAROOT1 is locked in the server room and kept powered down.

2.3.8 External DNS / Mail Relay Server

There is one server in the DMZ that serves two purposes. The server is named EXTDNS1. It handles the external DNS zone, giac.com and it acts as a Mail Relay Server. It can handle these two jobs, as there is little throughput on both counts.

Dell PowerEdge 1650	
RAM	2 GB SDRAM
Processor	1 x Intel Xeon 2.0GHz, w/512k cache
Hard Disks	2 x 18 GB 10k RPM in a RAID 1 mirror set
Network Adapters	1 x Onboard 10/100 NIC

2.4 Test Network Description

A Test Network or "sandbox" is extremely important to have in any network. It allows you to test hot fixes, service packs, new versions of software and configuration changes in a controlled environment separate from the production network. The Test Network at GIAC is built to mirror the production network as closely as possible. In fact, it is created by using an image of HODC3, so that it's Active Directory is identical to that of the production network. The domain and all of the servers have the same name as their production counterparts.

The backup server for the head office location (HOBACK1) will be used to restore the backups of the production servers onto the test servers. This will

create a test network that resembles the production network as closely as possible.

The Test Network has its own switch so that it can remain completely independent of the production network.

The Test Network is easily built by following the procedure below:

1. Take HODC3 offline and take a Ghost image of it, returning HODC3 to production when done.
2. Using an identically configured server, install the image onto it.
3. Install DHCP on the new HODC3.
4. Using NTDSUTIL.EXE transfer all FSMO roles to HODC3 and remove the other DCs from Active Directory.

Since this procedure is so quick and easy, the Test Network is usually recreated quarterly in order to keep it as close as possible to the production network. It can also be recreated quickly on-demand when needed.

2.4.1 Test Domain Controller

As mentioned above, the domain controller has the same hardware configuration as HODC3. If there is a requirement for more domain controllers, other desktops can be easily installed from scratch and DCPROMO'd to be DCs on the Test Network.

2.4.2 Test Application Servers

There are two servers that are dedicated to the test network. The application server hardware for the test network is the same as the production Exchange Servers. This serves two purposes. It allows us to easily build the test network by restoring the production Exchange Servers onto the test network servers and in the case of a disaster; we have 2 spare machines that can quickly be converted to production status as Exchange Servers. It is not as important to have standby SQL servers like this as the production SQL servers are clustered anyway. The Application Server hardware can be used to test for SQL server patches and upgrades as well.

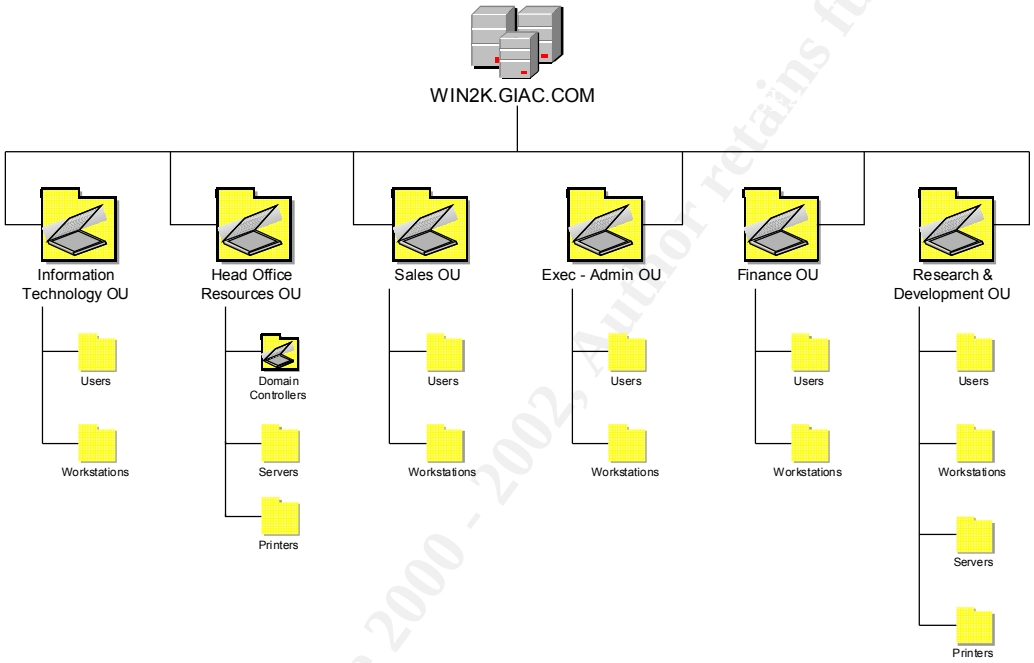
2.5 Remote Access

There are two methods of remote access for employees of GIAC Enterprises, dialing directly to the company and through VPN over the Internet. Hardware devices, including a RADIUS server and SecurID cards, provide these services.

3. Active Directory Design

Active Directory is the cornerstone of the Windows 2000 domain at GIAC Enterprises. For GIAC it is the primary reason for using Windows 2000. The benefits of using Group Policy alone are enough of a reason to use Windows 2000 and Active Directory.

3.1 Active Directory Structure Diagram



3.2 Operations Master Roles

In Active Directory, there are a number of roles that domain controllers can fulfill. Some of them are known as Flexible Single Master Operations (FSMO) roles.

3.2.1 PDC Emulator Master

This role is primarily for backward compatibility with systems that predate Active Directory. This role is not relevant at GIAC environment as all systems are running Windows 2000. This role is assigned to the first domain controller brought up in a domain. That is HODC1.

3.2.2 RID Master

The RID Master is responsible for handing out Relative Identifiers to domain controllers. There is one per domain. At GIAC HODC1 is the RID Master for the domain.

3.2.3 Infrastructure Master

The Infrastructure Master is responsible for making sure that Active Directory data references between domains remain current. There is one per domain. At GIAC HODC1 is the Infrastructure Master for the domain.

3.2.4 Schema Master

The Schema Master is responsible for hosting the read / write version of the Active Directory schema. All changes to the schema must go through the Schema Master. There is one Schema Master per forest. HODC2 is the Schema Master of the GIAC forest.

3.2.5 Domain Naming Master

The Domain Naming Master is responsible for maintaining the consistency of the domain naming structure, as well as registering new domains within the forest. There can only be one Domain Naming Master per forest. It is also recommended that the same server act as the Schema Master and Domain Naming Master. Therefore, HODC2 is also the Domain Naming Master for the GIAC forest.

3.2.6 Global Catalog Server

The Global Catalog contains some of the most commonly needed data from Active Directory across all domains in the forest. It is primarily useful in multi-domain environments, but is still necessary in single domain environments, such as that at GIAC. It is recommended to have one Global catalog server per site. Since there are two sites, two Global Catalog servers (HODC2 and RDDC1) are needed. HODC2 was chosen over HODC1 because it is recommended to separate the Global Catalog from the Infrastructure Master role.

3.3 Organizational Unit Descriptions

There is somewhat of a hybrid structure at GIAC Enterprises in that the Active Directory Organizational Units are not divided strictly by department, geography or purpose, but sometimes a combination of them. The majority of the OU's are divided by department. In the case of the Head Office Resource OU, it is separate due to geography and purpose rather than department. The R&D OU encompasses the R&D department plus all of the resources stored at the R&D location. This works because the remote location is only R&D resources and personnel, with the exception of the few IT personnel that work at the remote location. Those IT personnel are contained in the IT OU with everyone else in IT. Some of the OU's exist to facilitate better control of security and permissions through group policy. Others exist simply to separate the different departments.

Since the entire IT department is responsible for supporting the entire company, there is no delegation of administration by OU, but it is possible for the future. It is even being considered for the R&D department to have its own dedicated IT department.

3.3.1 IT OU

The IT OU simply collects the users and workstations that are part of the IT department into one OU, with sub-containers for the users and computers. Since the IT department could need different permissions than any other department, it is important that there be a separate OU for it. This makes having an IT specific group policy quite easy.

3.3.2 Sales / Marketing OU

The Sales / Marketing OU simply collects the users and workstations that are part of the Sales / Marketing department into one OU, with sub-containers for the users and computers.

3.3.3 Finance OU

The Finance OU simply collects the users and workstations that are part of the Finance department into one OU, with sub-containers for the users and computers.

3.3.4 Executive / Administrative OU

The Exec / Admin OU simply collects the users and workstations that are part of the Exec / Admin department into one OU, with sub-containers for the users and computers.

3.3.5 R & D OU

The R&D OU has sub-containers for the users, and computers for in the R&D department. It also has sub-containers for the servers and printers that are at the remote location. It is important to have the R&D department segregated out as the work that they are doing is very sensitive and extra security measures are necessary to secure their resources.

3.3.6 Head Office Resources OU

The Head Office Resources OU is used to group together the sub-containers for the domain controllers for the entire domain, and the servers and printers located in the head office.

4. Group Policy

Below will be outlined the various group policies that will be implemented at GIAC Enterprises. The majority of the security settings will match those recommended by the National Security Agency. There will, however, be some deviation from the NSA recommendations, to better match the requirements of GIAC Enterprises.

All users have a drive mapped to their home directory. Each department has a drive mapped to the folder for their respective departments. This is done in the logon script that is applied using group policy. Each OU has its own independent logon script for this purpose.

Note: Any setting not explicitly discussed in this paper is left at the default.

4.1 Domain Group Policy

The Domain Group Policy object is used for policies that will affect the entire domain. This is where account policies such as password policies are set.

4.1.1 Password Policy

Password policies are essential for any good security plan. GIAC has implemented a policy that is fairly strict, due to the sensitive nature of some of the work being done. It is important that the policy be strong, but not overly intrusive. Password policies that inconvenience the users too much have their own problems because users will simply write down their passwords on pieces of paper and keep them at their desks. This has the effect of being less secure than having a bit more relaxed password policy.
Enforce password history – 20 passwords remembered
Maximum password age – 90 days
Minimum password age – 1 day
Minimum password length – 12 characters
Passwords must meet complexity requirements – Enabled
Store passwords using reversible encryption for all users in the domain – Disabled
The above settings require users to change their passwords at least every 90 days. The passwords must be at least 12 characters long and must meet the Microsoft complexity requirements.

4.1.2 Account Lockout Policy

Lockout policies are also important as they help slow down brute force password guessing attempts. Here again, it is important to not go too far when creating a policy. It is possible that making this policy too unforgiving could lead to a denial of service (DoS) problem. For example, setting the lockout threshold to zero makes a locked account stay locked until manually unlocked by an administrator.

This initially sounds like a good idea, but is an easy target for a DoS attack as long as the attacker has knowledge of some usernames to lockout.
Account lockout duration – 30 minutes

- This setting indicates that once an account is locked, it will stay locked until 30 minutes have passed. The account will then be automatically unlocked.

Account lockout threshold – 5 invalid logon attempts
Reset account lockout counter after – 30 minutes

- This setting and the one before it work together. These settings indicate that if there are 5 incorrect logon attempts within 30 minutes, the account will be locked. 30 minutes after the last invalid attempt, if the account has not been locked, the counter will be reset to zero.

4.1.3 Kerberos Policy

The Kerberos Policy is considered secure enough at the default settings.

4.1.4 Local Policies \ Security Options

There are a few Security Options settings that will be set at GIAC.

Additional restrictions for anonymous connections – This setting was first tested to ascertain that the most secure setting would work. The most secure setting is "No access without explicit anonymous permissions". Since GIAC only has one domain (therefore no trusts), the GIAC domain is in native mode and all of the applications work when this is configured to the most secure setting, it has been set to "No access without explicit anonymous permissions".
Message text for users attempting to log on – The legal notice is outlined below:

> This system is for the use of authorized GIAC Enterprises employees, consultants and temporaries only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, systems personnel may provide the evidence obtained from such monitoring to law enforcement officials. All systems should be used in conjunction with GIAC Enterprises policies and not used in ways that are disruptive, offensive or disparaging to others.

Message title for users attempting to log on – "Warning: Use of this system is restricted and monitored."
Disable CTRL + ALT + DEL requirement for logon – Disabled

- This setting is disabled, so that in the event that a user has the knowledge and privileges to change this setting on their local machine, it will be overwritten by the domain policy on the next policy refresh.

Do not display last user name in logon screen – Enabled
LAN Manager Authentication Level – Send NTLMv2 response only \ refuse LM & NTLM
Prompt user to change password before expiration – 14 days
Recovery Console: Allow automatic administrative logon – Disabled
Rename guest account – "doesnotwork"

- The guest account is disabled anyway, but GIAC has chosen to rename it domain-wide to possibly prevent some future abuse of this account.

Send unencrypted password to connect to third-party SMB servers – Disabled
Strengthen default permissions of global system objects (e.g. Symbolic Links) – Enabled
Unsigned driver installation behavior – Warn but allow installation
Unsigned non-driver installation behavior – Warn but allow installation

4.1.5 Event Log Settings

It is important to have enough room in the logs that when an event occurs, the relevant information is still in the logs and has not been overwritten. GIAC has chosen a log size that allows for a great deal of information, but yet is still manageable and easy to use when needed.
GIAC has also chosen to restrict guest access to all logs. While not strictly necessary to restrict guest and null logons from accessing the logs, there is no reason to leave this open.
Maximum application log size – 10240 Kilobytes
Maximum security log size – 40960 Kilobytes
Maximum system log size – 10240 Kilobytes
Restrict guest access to application log – Enabled
Restrict guest access to security log – Enabled
Restrict guest access to system log – Enabled

4.1.6 Display Settings

It is important that when users leave their desk that they lock their workstations. Since it is possible for users to forget this, GIAC has chosen to enforce a screen-saver policy. It does not eliminate the problem of unlocked workstations being left unattended, but it minimizes the amount of time that unattended workstations will stay unlocked.

Activate screen saver – Enabled
Password protect the screen saver – Enabled
Screen saver timeout – 600 seconds (10 minutes)

4.2 Domain Controller Group Policy

Since the majority of important settings are configured at the Domain level, there are only a few settings that need to be configured for the Domain Controllers.

4.2.1 Local Policies \ Audit Policy

Auditing of domain controllers and other servers is important for tracking down potential exploit attempts. It can enable an administrator to determine what holes are being attacked and who the potential attackers are by seeing who was logged on during the attack. It will also show what users are repeatedly trying to overstep their privileges. This allows management to have discussions with the "curious" users if it becomes a problem.

Audit account logon events – Success, Failure
Audit account management – Success, Failure
Audit directory service access – Failure
Audit logon events – Success, Failure
Audit object access – Failure
Audit policy change – Success, Failure
Audit privilege use – Failure
Audit system events – Success, Failure

4.2.2 Local Policies \ Security Options

Allow Server Operators to schedule tasks (domain controllers only) – Disabled

Allow system to be shut down without having to log on – Disabled.

- Without this setting configured, it is possible for someone with physical access to the servers to create a denial of service situation by shutting the servers down. All GIAC servers are situated in secured server rooms, but any extra security is always nice.

Clear virtual memory pagefile when system shuts down – Enabled

4.3 IT OU Group Policy

Most of the restrictions that are placed on other departments using group policy are either unnecessary or unwanted for the IT department. Some of the settings would make troubleshooting more difficult. Therefore a group policy for IT is not defined.

4.4 Sales / Marketing OU Group Policy

4.4.1 Windows Explorer Settings

Since GIAC maps all network drives in logon scripts and would like to minimize the peer-to-peer file sharing, there are some settings that need to be configured for certain OU's containing users. The setting is not configured for the IT OU

since IT users might need this ability during the course of their work, for example in troubleshooting.
No "Computers Near Me" in My Network Places – Enabled
No "Entire Network" in My Network Places – Enabled

4.5 Finance OU Group Policy

4.5.1 Windows Explorer Settings

Since GIAC maps all network drives in logon scripts and would like to minimize the peer-to-peer file sharing, there are some settings that need to be configured for certain OU's containing users.
No "Computers Near Me" in My Network Places – Enabled
No "Entire Network" in My Network Places – Enabled

4.6 Executive / Administrative OU Group Policy

4.6.1 Windows Explorer Settings

Since GIAC maps all network drives in logon scripts and would like to minimize the peer-to-peer file sharing, there are some settings that need to be configured for certain OU's containing users. The setting is not configured for the IT OU since IT users might need this ability during the course of their work, for example in troubleshooting.
No "Computers Near Me" in My Network Places – Enabled
No "Entire Network" in My Network Places – Enabled

4.7 R&D OU Group Policy

4.7.1 Local Policies \ Audit Policy

In the case of GIAC, auditing is also important for all machines within the R&D OU. In this OU are servers and workstations of the researchers. While auditing is most important on the servers, it would still be nice to have the auditing on the researchers workstations.
Audit account logon events – Success, Failure
Audit account management – Success, Failure
Audit directory service access – Failure
Audit logon events – Success, Failure
Audit object access – Failure
Audit policy change – Success, Failure
Audit privilege use – Failure
Audit system events – Success, Failure

4.7.2 Local Policies \ Security Options

Allow Server Operators to schedule tasks (domain controllers only) – Disabled

Allow system to be shut down without having to log on – Disabled.
Clear virtual memory pagefile when system shuts down – Enabled
Rename administrator password – giacrdsecure

- This will be set to a particular username for the R&D computers. GIAC has decided to set this at the OU level so that the R&D OU can have a different administrator username from the Head Office Resources OU. This is done strictly for granularity, so that this username can be changed independently of that used elsewhere.

4.8 Head Office Resource OU Group Policy

4.8.1 Local Policies \ Audit Policy

This OU contains the servers (all but the domain controllers and DMZ servers) at the head office location. GIAC would like to have auditing on all of these servers.
Audit account logon events – Success, Failure
Audit account management – Success, Failure
Audit directory service access – Failure
Audit logon events – Success, Failure
Audit object access – Failure
Audit policy change – Success, Failure
Audit privilege use – Failure
Audit system events – Success, Failure

4.8.2 Local Policies \ Security Options

Allow system to be shut down without having to log on – Disabled.
Clear virtual memory pagefile when system shuts down – Enabled
Rename administrator password – hosafeuser

- This will be set to a particular username for the Head Office servers. GIAC has decided to set this at the OU level so that the Head Office Resources OU can have a different administrator username from the R&D OU. This is done strictly for granularity, so that this username can be changed independently of that used elsewhere.

5. Additional Security

Group Policy is a large step forward in the world of Windows security, but there is more to address when planning a secure network infrastructure. Some of the issues that will be discussed below include, securing the IIS servers sitting in the DMZ, securing the VPN connections that run through the firewall between the DMZ and the main corporate site, necessary periodic maintenance and documentation control.

5.1 IIS Server Security

This section will primarily discuss the IIS servers that are contained in the DMZ as they are the most important servers to secure. The intranet server within the

head office network will also be secured, but to a lesser extent since it is not accessible from the Internet.

The security recommendations of the National Security Agency were followed quite closely here. Some of the recommendations are listed below:

- All servers are in a secured location.
- All of the IIS servers in the DMZ are standalone servers, not members of any domains. Since there are only 10 IIS servers in the DMZ, it was decided that it was unnecessary to create a new domain in the DMZ.
- TCP/IP is the only protocol stack running on the servers.
- SMTP, FTP and NNTP are not required and are therefore not installed.
- Other relevant services that are not needed are set to disabled. These include Net Logon, Print Spooler, Remote Registry Service, Server Service and Workstation Service. This is just an abbreviated list.
- Since anonymous access to the web servers will be necessary, the IUSR_*computername* accounts cannot be disabled, but they will be secured.
    a. The User Cannot Change Password and Password Never Expires settings are checked.
    b. The user rights to access the server from the network and to log on as a batch job have been removed from the accounts.
    c. The IUSR_*computername* accounts have been added to the locally created WebPeople local groups on their respective servers. They have also been removed from all other groups.
- Since only members of IT that would have Administrative privileges on the servers anyway will be looking after the web servers, it is not necessary to follow the NSA guidelines and create a WebAdmins group.
- NTFS permissions for the Guests and Everyone groups are removed from the Inetpub directory and all child directories.
- A new directory structure was created to host the actual web files. The NTFS permissions were also secured by removing the Guests and Everyone groups. The file permissions will be configured as recommended by the NSA. This includes separating the files into different directories by content type and setting only the permissions necessary to access that type. For example the folder containing images only requires read access, but the folder containing scripts requires read and execute.
- The IIS samples, help files and admin scripts have all been removed from the servers. The administration websites is also not necessary and has been removed.
- Internet printing has been disabled completely as it is entirely unnecessary for these servers.
- Unused ISAPI extensions are unmapped and unused ISAPI filters are deleted.
- IPSec will be configured on the web servers to allow for the VPN tunnel between the IIS servers in the DMZ and the SQL servers in the corporate

network. It will also be configured to drop traffic that tries to use ports other than those allowed past the IPSec filter.
- Secure Socket Layer (SSL) is used to encrypt the data transmitted between the web servers and the customer during the registration and order process.

5.2 VPN Between Head Office and DMZ

There will be two main uses for the VPN setup. The Exchange front-end server needs secure communication between itself and the domain controllers and Exchange back-end server for Outlook Web Access. The web servers need secure communication with the SQL servers to record transactions.

The involved servers will be issued certificates from HODC1. IPSec policies will be used to ensure that all information that travels through the firewall will be secured.

5.3 Periodic Security Maintenance

Vigilance is vitally important in maintaining a secure network. All administrators will be responsible for staying current with the world of Windows security. Subscribing to relevant news lists, such as that provided by the SANS Institute will help with this. Security knowledge and certification will be kept current by attending relevant training courses.

Service Packs and hot-fixes are extremely important to maintaining security, but they can sometimes contain bugs. It is important that all service packs and hot-fixes be tested on the test network as completely as possible before they will be deployed to production servers. Only those that are necessary in the GIAC environment will be deployed.

There will be maintenance windows every two weeks on Saturday night to complete any necessary maintenance work and to apply any service packs and hot-fixes that are deemed tested and necessary. Obviously the web servers in the DMZ cannot be brought down in this fashion. Since the web servers are configured to load-share, they can be updated one at a time as needed.

5.4 Documentation Control

Documentation is essential in any network and security of the information contained in network documentation is important. The information contained in normal network documentation could be quite helpful to an attacker and quite damaging to a network. Because of this, the network documentation at GIAC is treated as some of the most secure data at the company.

All documents are stored online encrypted and in secure directories on the file server. A copy of this data is kept encrypted on a CD, which is stored in an

offline location together with the backup tapes. This information would be invaluable during a disaster recovery situation.

Documentation is required to be reviewed quarterly. At that time a new CD of the encrypted documentation will be made and sent offsite.

Since the passwords for the domain administrator, all local administrators and all service accounts require strong passwords and are required to be changed every 90 days, they would be difficult to remember; therefore they will need to be stored in a secure location. There will be an encrypted text file as part of the network documentation that contains a password list file.

6. Disaster Recovery

Disaster Recovery is one of those things that are planned for extensively, but it is hoped that it will never be necessary.

All servers in the production network are backed up weekly with a full backup and then nightly with a differential backup. The weekly full backups are kept offsite in a secure location for one year before they are returned and the tapes reused.

Once per month, or more often if Active Directory has changed significantly, HODC3 is brought offline and booted from a floppy disk. A Ghost image of this machine is taken and burnt to a CD. This CD is sent out to a secure location offsite with the backup tapes. This image will allow for a rapid recovery of our Active Directory domain as well as its uses in building the Test Network as discussed previously.

Disaster recovery documentation will be tested quarterly. This will be done by completing practice scenarios on the test network. A rotation will be established so that all administrators will have an opportunity to become familiar with the procedures and have hands-on experience recovering the network.

Bibliography

1. Fossen, Jason "Securing Windows" SANS Course Material

2. Minasi, Mark, et al. "Mastering Windows 2000 Server Third Edition", Sybex 2001

3. Chacon, Michael, et al. "MCSE: Accelerated Windows 2000 Study Guide", Sybex 2000

4. Heldman, Bill "MCSE: Windows 2000 Network Infrastructure Design Study Guide", Sybex 2000

5. Microsoft Corporation "Windows 2000 Group Policy", URL - http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp

6. National Security Agency "Security Recommendation Guides", URL – http://nsa1.www.conxion.com

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**