GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

GIAC/GCWN Practical

Version 3.1 Option 1

© SANS Institute 2000 - 2002, Author retains full rights.

A Secure Windows 2000 Infrastructure

David Hed – International Attendee
September 15, 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ABOUT THE REPORT 4

DESCRIPTION OF GIAC ENTERPRISES 5

About business -segment and history 5
Summary on infrastructure 5
Summary on organization 5
DEPARTMENTS AND THEIR LOCATIONS 6
Research and Development 6
Quality Assurance and Deployment group 6
Sales and Marketing 6
Finance and Human Relations 6
Helpdesk and IT -support 7
FUTURE PLANS 7

NETWORK DESIGN AND D IAGRAM 8

SECURITY ZONES AND "PHYSICAL TRUSTS" 9
SecZone1 9
SecZone2 9
SecZone3 10
SecZone4 10
SecZone5 10
SecZone6a 10
SecZone6b 10
SecZone7 11

INFRASTRUCTURE COMPO NENTS 12

Communication Backbone Infrastructure 12
Firewalls 12
Webservers 12
Databases 13
Proxies, Loadbalancers and reverse proxies 13
Backup 13
Additional Local Systems 13
External DNS and Mail Architecture 14
Internal DNS and Mail Architecture 14
Antivirus systems 14
Other support systems 15
REMOTE OFFICES 16

ACTIVE DIRECTORY DESIGN AND DIAGRAM 17

PHYSICAL DESIGN 18
Domain controller architecture 18
FSMO Role architecture 18
Network Administration and Support 19
Print server architecture 19
DHCP architecture 20
Sites 20
Naming Standard and DNS architecture 21
Hardware cer tification 22

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

LOGICAL DESIGN (FORE ST, DOMAINS) 23

OUs 25
Design reasoning for OU structure 25
GENERAL USER OUS 26
Finance and Human Relations 26
IT-support 26
Quality Assurance and Deployment 26
Sales and Marketing and the sub -OUs 26
AMSTERDAM DOMAIN OU STRUCTURE 26

GROUP POLICY AND OTH ER SECURITY 27

DOMAIN POLICY 30
Password Policy 30
Account Lockout Policy 31
Kerberos Policy 31
Audit Policy 32
User Rights Policy 33
OTHER GPO SETTINGS AND POLICIES 35
Security Options Policy 35
Varning Banner 37
User rights assignment Policy for IT -support 38
Security Options Policy for IT -support 39
Developer Debug Policy 39
Laptop Cache Logon Policy 39

ADDITIONAL INFORMATI ON ABOUT THE SYSTEMS , AND MORE 40

LOGSERVER 40
GUEST ACCOUNT LOCKOUT 40
SECURITY ROLES IN USE BY GIAC 40
OPEN PORTS ON DOMAIN CONTROLLERS 42
UDP Ports for Domain Controller 42
TCP Ports for Domain Controller 42
UNNECESSARY SERVICES 43
Windows 2000 unsafe services 43
Required services for IIS 44
"May be required" services for IIS 44
ACCESS CONTROL MECHANISMS IN WINDOWS 2000 45
INFORMATION ON TRAVERSING OF FOLDERS 46
USAGE OF EFS 47
IPSEC ON INTERNAL NETWORKS 47
HOTFIXES AMONG OTHER UPDATES 47
VERIFICATION OF BACKUPS 47
DOCUMENTATION AND ROUTINES 47
EDUCATION 48

SOURCES 49

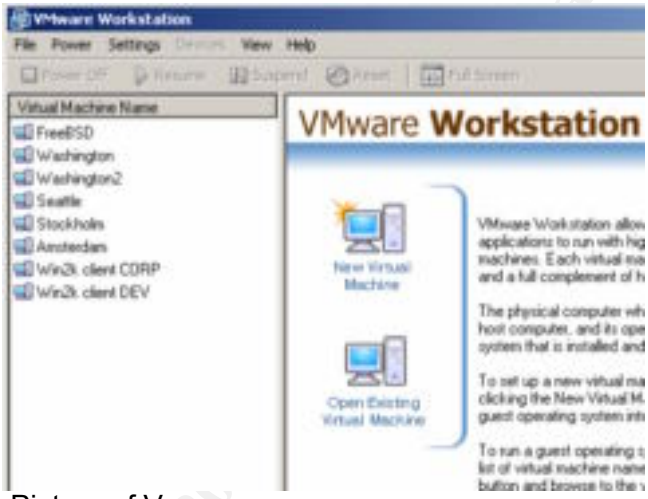
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

About the report

Be advised that s pelling error, grammar errors and other language limitation may be unwillingly included in the report. English is not the writer's primary language. The Formatting is 25mm (a little less then 1 inch from each side) and Arial12 has been used throughout the report. Differences between the domains are discussed, although the primary focus is on corp.giac.com.

All settings and machines where actually installed during creation of this document. The tool used was VMWare3.1.1 and using host -only-mode on a laptop with 512Mb RAM (domain controllers had to settle for 96Mb and not all active at the same time). I do recommend other students of GCWN to try this solution for flexibility and to be able to carry your fictional enterprise in a backpack!



Picture of Vmware

All images are either snapshots from VMWare sessions or created by myself in Visio or ms-paint.

Effort has been made not to cut and paste rehashes of best practice documents in this report and to exempli fy some as implementation. As the writer is not paid by words, all texts do in some way relate to the design and additional padding text are tried to be kept at a minimum with a reference included as source to why this judgement was made.

Some brands have been named and their products are under their copyright, some products has been made up such as AppGuard that shouldn't be mistaken for products with similar names. This document is not a study document for parts of MCSE. It is taken for granted that you understand the parts within and outside of Active Directory.

The company is actually purely fictional. And most importantly, no electrons were harmed in the creation of this document.

Enjoy!

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Description of GIAC Enterprises

About business-segment and history

GIAC Enterprises an American company, primary an e -business. Primary business focus on helping people back to normal life after fortune cookies making them into luck seekers, GIAC also has fortune cookie production from earlier stages but are focusing on helping online users with a software portal to self -help. Interactive study guides availble online and research reports on why so many people have failed as luck-seekers are availble on the www.giac.com systems. The Amsterdam office is growing at a tremendous rate and perhaps it is time to document that branch by other workers within GIAC...

Summary on infrastructure

GIAC Enterprises has rebuilt the IT -infrastructure from the ground using Windows 2000 and do not have many legacy applications to tak e into consideration. This means that all migration from Windows9x/WindowsNT is complete.

Summary on organization

GIAC Enterprises is currently placed in four locations, Washington (HQ), Seattle, Stockholm and Amsterdam (Research and Development main offi ce). There are roughly 50 persons working in Stockholm and Seattle, 100 people in Amsterdam and 200 in the HQ making the total number of people roughly 500, making GIAC large enough to plan AD in a good way and have supporting infrastructural components in place.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Departments and their locations

Research and Development

All research is being "out-contracted" within the company to Amsterdam. Where they for some strange reason has alot of creative ideas that help GIAC Enterprises keep ahead of its competition. The Amsterdam office takes care of its own infrastructure. The developed material is transported over VPN to SecZone3 (explained in more detail in the next segment). There it is placed on a fileserver/dropbox for Quality Assurance. This department is not discussed at full-length within the report.

Quality Assurance and Deployment group

The Quality Assurance and Deployment group is a department in Washington. The QAD is answering directly under management are the QADs. They work to make sure that the code from Amsterdam lives up to expectations and that every function is properly documented. All programs are staged in the isolated lab before production (SecZone7 explained later).

A small group also exist under QAD that takes care of auditing and security incidents, they work closely with IT-support but answer to management.

Sales and Marketing

Sales people exist in all offices except Amsterdam, the majority of the people does however work in Washington. They work together with the IT-support department for continously updating the websites. Their primary working area is to continue the searching for potential clients and keeping existing ones happy.

Finance and Human Relations

GIAC Enterprises continues to grow rapidly and the Finance and Human Relations department handles all administrative tasks except for sales reports. All persons under this department are placed in Washington

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Helpdesk and IT-support

All infrastructure are taken care off within this group. Local contractors has some service tasks for remote offices. But the IT-support group are responsible for keeping the systems functional and secured.

As an enterprise decision together with management is to aim for a standard to primary use Windows systems where people work with/at. Some UNIX servers are kept for support and infrastructural systems.

The helpdesk and IT-support personnel are mainly focused in Stockholm and Washington, Seattle has only a minimum semi-employed helpdesk staff that helps users and changes toners and similar activities. The Stockholm office works to overlap the Washington office timewise so that people working in out of office hours and costumers calling in can get proffesional support instead of a voice mail. All IT-security staff are placed in Washington, some accounts with delegated rights are created for Stockholm and Seattle. The support structure is that all incoming calls and other ways of contact is taken care of and registered by helpdesk, if they are unable to help then the problem get escalated through level2 and finaly leve3. When its out of office hours important clients and internal staff can reach support by navigating through a tele-voice system.

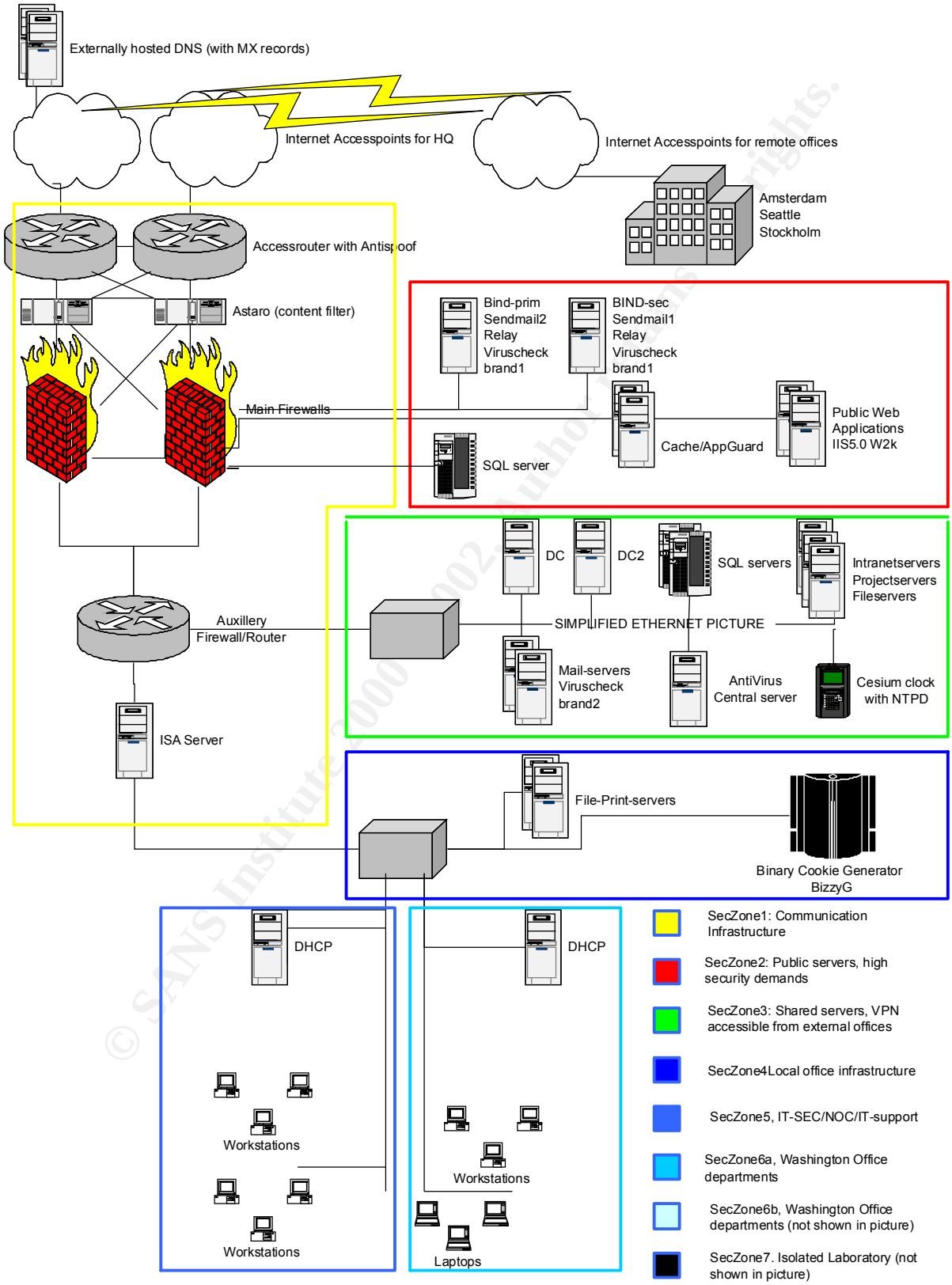
Future plans

There is hope within the organization that Windows 2000 will increase efficiency as well as offer better security. Plans are to expand the e-biz segment in Washington with the help from the development department in Amsterdam. Universal Groups will not be used because that is in my opinion a symbol of bad planning. The security strategy for the future is to continue to segment networks based on trust and thier administration. Further evolvement in the user roles are also taking place and more grannular design of GPOs.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Design and Diagram



Picture1: Network design and securityzones

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As the picture on the previous page shows the network layout is segmented on trusts and usage between networks.

Security zones and "physical trusts"

GIAC Enterprises has learned the hard way by starting new bransh offices that there is a need of documenting security zones. For enforcing policies at deployment it is important to follow the strategic recommendation from the IT -security group. Networks must be segmented into well defined containers with all dependencies to other systems verified and documented.

SecZone1

This SecZone includes Communication infrastructure together with an ISA -server used for employee access to the internet. These systems are the true coresystems with platinum service contracts. Spare powersupplies and ot her spare parts are on the shelves within the facilities so that a system is up and running without to much lost revenues in case of hardware failure. Systems are standard appliances mostly from CISCO and BSD-friendly vendors. The branch offices use standa rd i386 boxes with OpenBSD as their firewalls (not alot of rules and can be remotely managed from Washington). All systems with harddrives have SCSI -RAID1 and Redundant powersupplies as standard, this includes all production systems.

SecZone2

SecZone2 con tains the Public servers. These systems are accessible from the internet, these systems are patched through escalation from IT -sec department. All systems are highly secured and for information security issues considered to be hacked/lost already. These sy stems are very locked down, with the latest patches and hotfixes availble (after testing). These systems cannot communicate to the rest of the enterprise (mailservers/DNS servers are an exception for these services). Administration of these takes place on a separate network segment within the IT -support department. There are blocking rules in the firewalls to/from this segment that is very restricted to only include the specific services that is being offered.

ALL ACCESS FROM PUBLIC HOSTS CAN ONLY REACH SE CZONE2, this is firewalled and verified with regular portscans from the outside. (Please note that VPN-users are accepted to SecZone3), this also includes internal systems such as DNS

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SecZone3

SecZone2 contains the Internal Enterprise servers. These syst ems include the internal coresystems such as accounting systems, payroll -systems, manufacturing systems, CRM-systems, etc. These systems are accessible from the other branches through VPN, it is here all shared resources are placed, please notice it is "to tally" isolated from SecZone4. A dropbox for files from Amsterdam is placed in this seczone. It is the only machine that Amsterdam has access to within the production systems.

These are segmented from each other on VLANs and production zones. For image purposes and being out of scope for the report it is simplified in the picture.

SecZone4

The Local Infrastructure. Similar systems are also represented in the other sites (Seattle and Stockholm). These are only used by internal personnel and are not accessible from other offices, here are internal material stored. Its mostly fileservers and some database servers. At the main -HQ there is a big legacy fortune cookie machine that only is to be connected at fullmoon for generation of transaction feeds. These are replicated out to the database at SecZone2 by people with furry big beards. If it wasn't for this system GIAC wouldn't be the leading fortune cookie company in the world.

SecZone5

The internal NOC and supportpersonnel including the IT -security group wo rk work in a segment of their own. There doesn't exist any laptops that are members in the domain. Some communication technicians have their own with serial -cables and different clients. There also exist a separate management network not shown in the picture that is used for router and firewall configuration. IDS are also accessible from this network.

SecZone6a

There are some office segments that are built up by a switched environment between the buildings and floors. They are typically a internal C -net within the 192.168.x.x address-space. These segments has only got a DHCP -server as supportive system within the same broadcast domain (Note: No segments share the same broadcast domain and multicast functionality for installations is not yet deployed).

SecZone6b

Just another example zone of another office department in Washington.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SecZone7

An Isolated lab is a requirement to not disrupt production. Computers are built up here from backups of production servers and changes are performed on these machines. The purpose is dual. For starters you verify that backups are taken correctly and secondly you verify that changes will not affect the production environment in a bad way.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Infrastructure components

Communication Backbone Infrastructure

Displayed partly in SecZone1 in the picture. Connection to the internet with two separate feedings from different ISP's at the Washington site, these connections are routed with BGP as controlling protocoll. The traffic between locations is encrypted with VPN at the external gateway (OpenBSD and CISCO applicances). All outgoing and incoming corporate traffic such as mail are concentrated to Washington HQ. This excludes external web-browsing from remote offices. External VPN-users do however go through the enterprise firewalls to reach internal systems. The networks at the different locations are fully switched.

Amsterdam has a 2Mb line to Stockholm and Seattle is connected to Washington with a Burstable T3 with 8Mbs - 48Mbs. Stockholm and Washington are connected through the internet backbone with 155Mbit through a European ISP with 10Mbit guaranteed bandwidth. This bandwidth is enough to keep project and other shared files on the mainHQ systems.

Firewalls

First thing that happens with packets from the internet (and outgoing!) is that they are checked for spoofing and other faulty packets. As this is not a GCFW-practical I consider them out of scope and will refer to a best practice document instead[1]. Please also check the proxy section for the content filtering.

The main external corporate firewalls are of a known brand running BSD underneath. They segment up the different DMZ's and external communication with NAT. Both the external routers and main firewalls are redundant (systemwise).

The internal firewalls mainly used for routing purposes between the segments. These CISCO PIX do however act as auxillery firewalls. They provide an opening for shared resources to the stations/segments that are in need of accessing them.

At the remote offices the firewalls mainly exist as a gateway for IPSEC and Web-traffic.

Webservers

The main webserver is a IIS5 running on Windows 2000, it is located in SecZone2. It is duplicated and is load balanced through the Cache/Appguard boxes.

[1] Cisco Anti-Spoof Egress Filtering http://www.sans.org/dosstep/cisco_spoof.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In SecZone3 there is also a IIS5 server used for intranet notices and to provide webaccess to mailservers over VPN. Notice that Mail-servers and Webservers do not share the same DMZ.

All administrative traffic is encrypted over IPSEC-tunnels.

Databases

In SecZone2 there is a backend database for e-business. It is used to serve dynamic content to the webservers and the traffic between IIS and SQL servers is digitally signed. There also exist a collection of Database servers in the production segment (SecZone3). And at remote offices there are smaller db-servers for internal statistics and information exists to simplify the working environment for the users Amsterdam is also in charge of testing and giving certification approval of new hardware as well. The tests are performed in a isolated lab-environment. (lab-environments are out of scope for this report).

Proxies, Loadbalancers and reverse proxies

In SecZone2 there is a loadbalanced/redundant Cache/Application guard shielding the IIS5. The Appguards primary usage is to shield/filter what reaches the Public Web-server. All employee surfing is handled through the ISA Server. There is a custom user agent string in all deployed webbrowsers which is used to identify that it is only the regular web browser that access the internet. It is not a definite solution to limit other programs or people to access the internet. Malicious Code Filter, Predefined URL Filter, HTTP Privacy Filter and Virus Protection for SMTP is provided by the Astaro box. These machines does not provide any NAT and work transparently.

Backup

As for the HQ in Washington there is a Storage Area Network(SAN) with backups for the whole enterprise. Monthly backup tapes for secondary systems are transported to Washington. Amsterdam has its own infrastructure including backup routines. SAN-equipment is not included on the network image but is connected to some systems in SecZone3 and SecZone4. Note that the internet infrastructure in SecZone2 is NOT included in these backups. These systems have local DLT-drives.

Additional Local Systems

The different locations have firewalls, proxy servers, file-print servers and domain controllers(including dns) as supportive systems. The AD-relevant systems are discussed in greater detail in that section.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

External DNS and Mail Architecture

The external systems that communicate with other organizations are mostly based on Solaris, CISCO, BSD and Linux. As for mail servers the external ones are based on Solaris running Sendmail with a virus protection. The external DNS servers are based on Solaris and BIND. The primary external DNS is a fallback system for mail and a secondary mail server is the secondary DNS server. All administration takes place over SSH or IPSEC tunnels. To increase availability there also exist DNS servers that is colocated at totaly different segment and provider. There also exist a virus inspection on the Askaro box.

All e-mail transmitted within the enterprise is sent over VPN, external incoming and outgoing mail are sent through the relay servers at main HQ, where it is checked for viruses. (all mail that comes or leaves the enterprise are thereby checked twice on different brands of antivirus -control).

Each DMZ is inspected by extensive logging on each host and there are Network and Hostbased IDS-systems. All logs are concentrated and correlated at the main HQ. The main focus of this report is not the additional systems [Im certified for GCIA and consider it out of scope for this specifik report], the Network Diagram explains the layout of segments being watched. Well now when i mentioned it i cant let it go. Each segment that can be monitored is.Those who cant be spanned have passive taps attached to them. All interfaces are in “stealth mode” and management is on separate interfaces isolated from the regular infrastructure.

An important feature to mention is that all logfiles are stored on separate mirrored drives(RAID 1). This is primarily to reduce the risk of corruption and enhance system performance.

Internal DNS and Mail Architecture

In SecZone3 the internal mail-servers are placed. The systems are running Exchange Server and provide additional names for email-addresses. The user accounts in AD are not linked to e-mail addresses [a LDAP catalog handles these fields, they get replicated into AD as contact information, out of scope for this report since AD is the primary directory service]. This means that the User-ID is not the name used in e-mail addresses. These systems are also cleaning incoming and outgoing mail for viruses using a second brand in antivirus software (just as the firewalls are of different brands). All internal domain controllers have DNS running.

Antivirus systems

All clients have antivirus software deployed by GPO (Mandatory). The main policy server is placed in Washington and has slave servers placed in all offices. The main reason for this is to reduce bandwidth requirements for large updates. This is hereby limited to once per site instead of individual machines. Please note that there exist antivirus systems for incoming/outgoing mail.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Other support systems

The main HQ also has an inhouse cesium clock that is used as a reference within the organization over SNTP (Simple Network Time Protocol), the doomsday fortune cookies has previously had a bad trackrecord so timing is of extreme importance for GIAC Enterprises. The PDC emulator is used as an internal reference for clients and servers.

Future plans and architecural enhancements

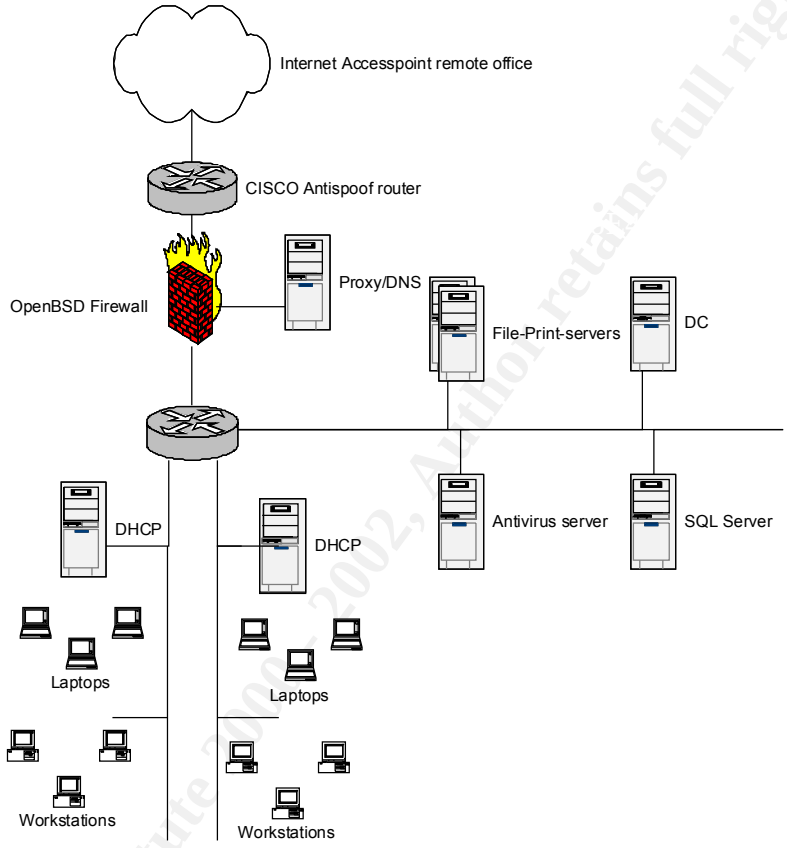
Plans are made for duplicating the www -infrastructure with more loadbalancers and placing additional internal databases in SecZon e2. To summarize these plans are that databases are moved upwards in the SecZones and on a DMZ if its own. All data access is thereby production data and NOT replicated data, these architectures are out of scope for this report but it is a trend that more and more companies will be forced to follow.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Remote Offices

Network design remote office Stockholm/Seattle/Amsterdam(simplified)



Picture2: Remote office network design

The remote offices are much more simple in thier layout then Washinton. As seen in the picture there is a separate leg for DNS on the firewall and a DMZ segment inside for internal projects and daily work.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Active Directory Design and Diagram

First lets explain the corporate domains that will be included in the documentation below.

All domain controllers are running in native mode [2], and the domains are active directory integrated.. Primarily to get rid of administrative limitations for computers groups or users, and to ensure that any WinNT computers will be placed in a domain of their own.

Both domains share the same Active directory Schema, the same Global Catalog and can therefore be said to be in the same forest, even though they do not share the same namespace (giac.com is not an active AD-domain). The use of Amsterdam domain is strictly for security reasons, not administrative. However the Amsterdam department has their own Administrators that take responsibility for the domain. Stockholm and Seattle are both controlled from the Washing ton HQ.

If you need to have separate domains for security reasons; they should not be linked to each other, or could be if they are created for replication reasons. Design is to be based on administrative requirements, not physical or organizational.

Webserver updates are managed from within the IT -support OU.

Some design consideration are taken from presentations on web -architecture from Microsoft[3]

Diagrams are shown in following pages (OUs and domains)

© SANS Institute 2000 - 2002, Author retains full rights.

[2] Mixed Mode vs. Native Mode http://www.winnetmag.com/Articles/Index.cfm?ArticleID=7156
[3] IIS as a Secure Web P ublishing Framework
http://www.microsoft.com/usa/presentations/Finnegan_Deml_SecuritySummitWest.ppt

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Physical Design

The network overview shows t he segmentation and it it based on levels of trust. For instance the internal systems are more trusting to each other than to/from other segments. Over VPN the physical design is not a limitation.

Domain controller architecture

There are four domain contr ollers within the main enterprise. There are two in Washington, while Stockholm and Seattle has only one each. The servers in Stockholm and Seattle are used to reduce replication, latency and congestion. If Stockholm or Seattle had been larger then a secon d domain controller would have been placed there for additional fault tolerance and load balancing. The internet infrastructure is often reliable. In the case of "internet being down" not alot of work can be done from the remote offices in any case since a lot of the project machines are placed there.

Amsterdam has two separate Domain Controllers and is not part of the main domain architecture.

All domain controllers are using high quality brand hardware with RAID5 SCSI disks. Testing has been made with ADSIZER from Microsoft and standard Pentium IV's with 2GB RAM is more then enough to handle the load. All cases are equipped with redundant power supplies and in Washington they are fed with separate powerlines from batteries at the basement. This is to p rovide extra time for the Diesel generators to get up and running. In Washington all core services including network devices are on this secondary powerfeed. All cables and other physical security is of good standard at all locations. All servers at other locations are on UPS within the server racks. For further inquiries about hardware architecture GIAC Enterprises will gladly give tours of our facilities. The brands and models for hardware devices are out of scope for this report.

All servers/domains are configured in native mode, being AD -integrated and is NOT Pre-Windows 2000 Compatible for security reasons such as Null user session vulnerabilities[4] § page 17.

FSMO Role architecture

Some rules for FSMO[5] placement[6]:

- The Infrastructure Master should no t be a Global Catalog server, and within the same site.

[4] Fossen, Jason. SANS track 5 book 5.1, SANS Institute, Page 17
[5] Active Directory FSMO Roles http://support.microsoft.com/default.aspx?scid=KB;EN -US;Q19713 2&
[6] Fossen, Jason. SANS track 5 book 5.1, SANS Institute, Page 38 -39

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- RID Master, PDC Emulator and Infrastructure master are only one per domain.
- The RID Master and PDC emulator should be the same Physical DC
- There is only one Schema master and one Domain Naming master in the enterprise and preferred to be on the same DC and this should be a Global Catalog Server.

To optimize the performance on Domain Controllers it is best to spread the roles by the rules stated above. A reminder of placement is that the Global Catalogs placed in Stockholm and Seattle are placed there to reduce replication and network latancy.

This means roughly that if load permits, and you only have access to two machines that you can place the FSMO roles as detailed below for Washington. Since no Pre-Windows2000 machines exist and since the Schema is not updated often(or at all) the following choice was made.

Washington
1. Global Catalog, Domain Naming Master, Schema Master
2.Infrastructure Master, PDC (+NTP), RID

The reason for placing the most critical servers all in Washington is based on administration and Washington being the largest office.

Stockholm
1.Global Catalog

Seattle
1. Global Catalog

Amsterdam
1.Global Catalog, Domain Naming Master, Schema Master
2.Infrastructure Master, PDC (+NTP), RID

Network Administration and Support

Nearly all Network Administration takes place from Washington, however the GIAC Enterprise has a contract with a Global Support team that takes care of hardware problems and assist when other IT-staff are unavailable. There are no RAS-systems or modems of any kind within the internal networks. All maintainance is performed through VPN or over the phone with a technician.

Print server architecture

Each location has 2 printservers that is overlapping each other for fault tolerance. In Amsterdam network resources are addressed when needed and there are no defined print servers in use.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DHCP architecture

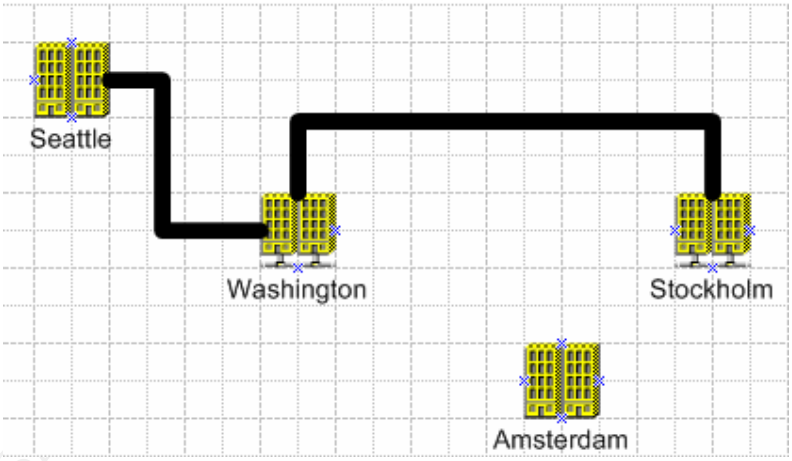
The importance and function of DHCP -servers shouldn't be neglected in planning. DHCP is a core service within the organization. Unlike DNS-servers that replicates all information, DHCP must be cluster aware or handle different scopes of IP -ranges. Suggested solution is to setup a two system cluster on each site.

Note: Important design factor is that no domain controller is a DHCP server. This is to prevent faulty updates within the Active Directory [7].

Suggestion is also to keep extensive logging activated as well as using the builtin feature for unauthorized DHCP server detection. Keep in mind that a DHCP local user group gets created for read access to the DHCP database and via the DHCP console at the time of DHCP setup.

Sites

The four different locations are sites and for corp.giac.com the replication between domain controllers is controlled from Washington which is the c entral when it comes to internet traffic. This means that it is uncommon for traffic to flow between Seattle and Stockholm. An important design factor is that if a site link to Washington should be down, the local resources and all accounts within the doma in are accessible because of the location of domain controllers in Seattle and Stockholm. Not illustrated in the picture is the updates of projects to servers placed in Washington from Amsterdam (but thats not AD -replication traffic).



Picture3: Sitelayout over the world between the offices for replication

Synchronization takes place outside office hours (for the remote offices). Manual updates can take place if there is an urgent need for updates.

[7] Fossen, Jason. SANS track 5 book 5.1, SANS Institute, Page 103

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Naming Standard and DNS architecture

The naming standard is build up as follows; Location 3 letter (ie Sea for Seattle), Building Letter plus number and floor number (ie R31 for Building R3 floor 1). Ending with the type of service its primary function is, along with a number starting at 1.

The four different locations will be named Was (Washington), Sea (Seattle), Sto (Stockholm), Ams (Amsterdam).

There are CNAMES/Alias for different services. For example a Intranet webserver in Seattle could be named SEAR31WEB1 with a alias name for http://intranet.Seattle.corp.giac.com/ . (or just http://intranet/ for people belonging to and logged in Seattle) This is used to help supportpersonnel as well as employees to quicker unders tand the location and to make searches more efficient/easy.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Every DNS entry are controlled by enterprise administrators and every change h as to come through them except for the ones that are dynamically updated. The internal DNS prefix is corp and Amsterdam has dev as its domain name. The choice of using separate namespaces is to have distinct borders between the different ”security areas”. This makes it three different security areas to admin.

*.corp.giac.com (Seattle, Washington and Stockholm)
*.dev.giac.com (Amsterdam)
[www and more].giac.com (external resources)

This means that the internal namespace is not resolvable from the Internet. The external DNS is running on Solaris and will therefore not be affected on the Windows 2000 architecture. If GIAC should be acquired or in any other way forced to change namespace then .NET will have functions for that [out of scope for this report].

As a security precaution the HQ external DNS are isolated from the internal networks. These external DNS servers only host information about the servers located on the DMZ's.

The domain controllers act as caching only system for forwarded requests from the internal network towards external resources (this includes the external corporate webpages and similar systems). This is used primary for further isolation and to simplify firewall configuration from the internal networks.

All DNS servers have been configured only to accept DNS queries that they have asked for (to prevent cache poisoning all Windows 2000 servers have been configured to only accept secure DNS updates) [8] The setting is within the advanced options for the DNS properties and the setting is named ”S ecure cache against pollution). An important part since the default configuration for Windows 2000 DNS is very naive.

Hardware certification

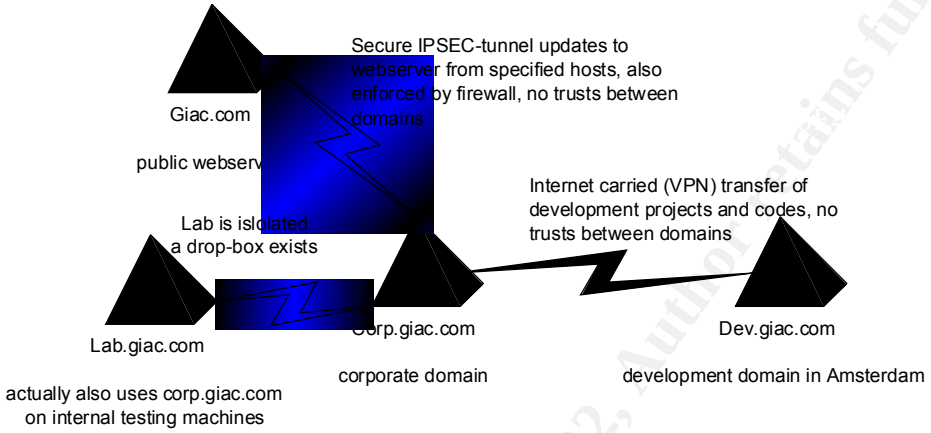
Amsterdam is also in charge of testing and giving certification approval of new hardware. The tests are performed in a isolated lab-environment. (lab-environments are out of scope for this report).

[8] How to Prevent DNS Cache Pollution http://support.microsoft.com/default.aspx?scid=KB;EN -US;Q241352&

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Logical Design (Forest, Domains)

Choice was also made to only share the name giac.com internally, there is NO trust between these domains. In a forest Domains are to exist for security boundaries, it was a risk GIAC wasn't willing to take for the DMZ enviroment.



Picture4: Active Directory, Domains and Trusts

The point of setting up separate forests is to provide isolation from the in ternet accessible systems. Meaning that the servers on the DMZ cannot authenticate themself and/or reach the internal systems limited by both administrative access lists and firewall policies. There are a limited number of people within the IT -support OU that have access to reach the external DMZ servers. Please note that all support personnel doesn't have access to all systems within the enterprise.

The absolute primary reason for making such isolations is security. GIAC cannot let a user in via unauthen ticated access (such as the internet through a IIS -server) to the internal networks. DMZs couldn't be part of the same administrative security boundaries. Mostly because of the administrative headache of restricting "everything" from these hosts. And since these systems shouldn't be able to access objects in the internal networks/zones then there is no real reason to keep them in the main corporate domain and/or forest. Of course this splitting of forests cause some administrative penalties but it is outwei ghed by the increase of security. Further the replication through the firewalls is limited as well because of the lack of domain controllers there and the non -usage of Universal groups anywhere in the other parts of the enterprise, primary to reduce the re plication on the WAN/VPN -links.

The AD-network consists of two real domains, one enterprise (corp.giac.com) and a separate for Research and Development (dev.giac.com). There also exist a grouping

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

of computers that handle the external communication. These systems are not AD-integrated.

A third domain lab.giac.com is mostly used for testing purposes. There is also a mirror of corp.giac.com in the laboration environment. And the forth for DMZ, that isn't a real AD-integrated domain, just some Windows 2000 servers and their support systems. Keep in mind that the term Forest is accurate even if it includes just one domain.

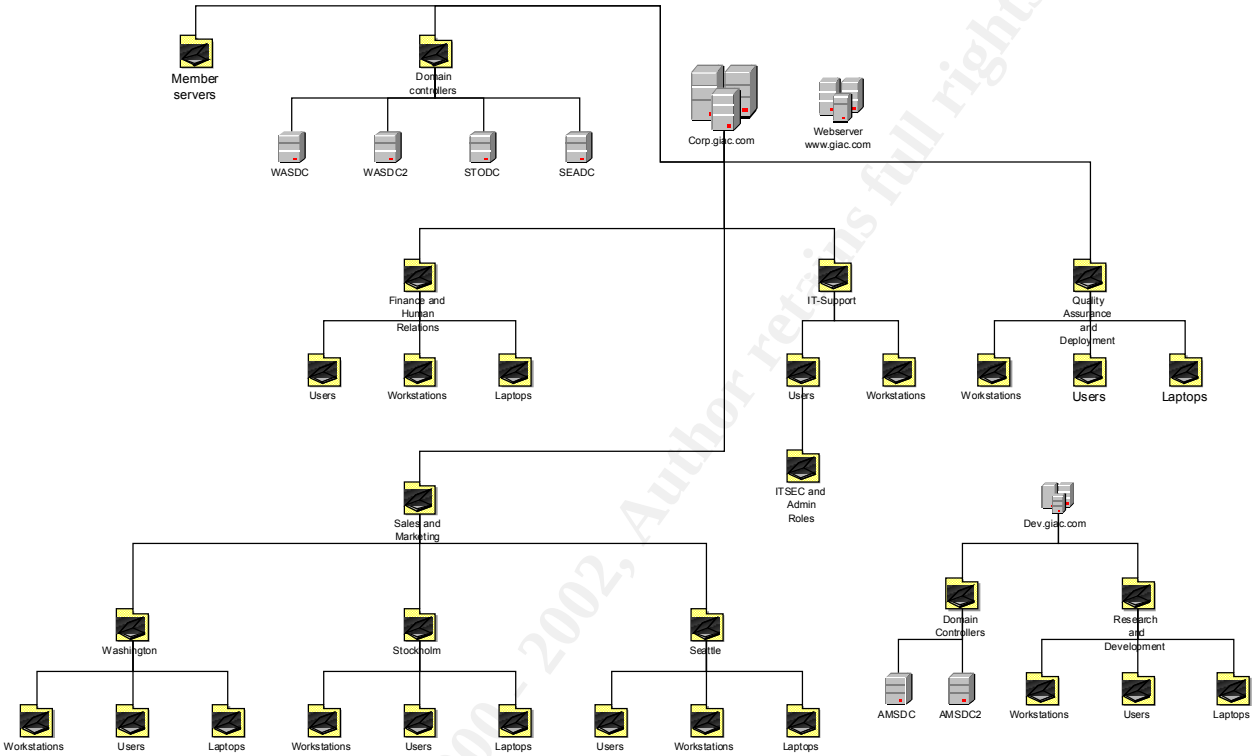
The administration is very simple in terms of complexity. All accounts within the Corporation networks are accessible and all resources are spread throughout the domain controllers. Which is imoportant out of a user perspective.

In the case of a compromised IIS-server it will not be able to affect corp.giac.com.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

OUs



Picture5: OU Layout and design

Design reasoning for OU structure

To minimize complexity the OUs are primary focused on user groups and thier computers. For the Sales and marketing OU there is a geographical structure with a "top-OU" for easy expansion. This also makes it easy for user grouping and deployment of GPOs.

Member Servers
This OU contains the servers used internally throughout the corp.giac.com domain. These servers share the server GPO -settings

Domain Controllers
The domain controllers, placed throughout the sites. All machines ha ve extensive logging and additional security settings, explained in the GPO segment.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

General User OUs

All User OUs contain both Workstation and Laptop OUs. This is to reduce complexity in the design without losing security or causing meaningless replica tion (such as making a separate OU structures for machines, resources and accounts/groups).

Finance and Human Relations

The most normal OU within Giac, primary only used for grouping purposes. This OU
also includes higher management.

IT-support

Note that no Laptop OU exist within this OU, this OU is the most complex within grouping and settings.

Quality Assurance and Deployment

This OU is primary used to group the office workers and give ability to perform administrative tasks.

Sales and Marketing and the sub-OUs

Please note that this OU is a branch of Sales offices, the impact of adding new offices throughout the globe such as new continents is minimal because of its flexible placement.

Amsterdam Domain OU structure

Amsterdam has a smaller structure primary to provide a easy solution, as all people in Amsterdam are developers or in some way members of development projects they share the same OU and are placed together with their machines as side OUs. There is not much administrative work with the Ams terdam office.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Group Policy and other Security

The administrator account is renamed on each site with adm in the end. So the built in adminaccount for Amsterdam could be named Amsadm, of course in reality it would be more complex, but the only reason f or changing is to show its a changed name, a cracker can/will find out the administrative account anyways. An account with the name administrator is created without any administrative rights and with an auditlog that is closely watched for potential intrud ers/mishaps. The disabled guest account is also changed to gst (ie Amsgst).

Administrative accounts are personal and the built in accounts are not used. Together with the Directory Service Restore Mode Administrator password they are stored in signed env elopes in a safe at a secret location near Washington. For the readers safety the actual location is considered out of scope for this report ; -)

GPO's is perhaps the most important to plan carefully and limit complexity in. Delegation will help the dail y administration, all changes must be tested thoroughly in the labs. Documentation is vital for keeping track of problems caused by changes.

All accounts throughout the domain are included in the domain -policy and are also used for dev.giac.com.

GPO's ar e enforced at startup time or at the time of login for a user. They also include control for Logoff/Shutdownscripts as well as for getting the system up and running.

Auditing is taken very seriously at GIAC Enterprises and separate access rights has been assigned. See more about section about Role -types of users.

GIAC does not create separate OU's for deploying different "physical groups" such as contractors or trainees. There will be separate Group Policy rights for these users. Effort has been ma de to reduce the number of GPO's.

A minimum for machine GPO has been determined to be three types of machines and a default domain policy.

- Default Domain Policy
- Domain Controller Policy
- Server Policy
- Workstation Policy

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Note: The IIS server is also hard ened with settings provided by templates but this is by hand not by GPO. SANS Institute already have some good papers on the subject [9]

Note: There exist a Developer Policy to give the ability to Debug systems

Security Templates are based on the work from NSA and some inspiration has been taken from NIST and recommendations from Insurance companies. After importing the renamed .inf files and refreshed scecli.dll with regsvr the work with the templates could be analyzed.

Verifying the result in Security Configuration and Analysis gives the following at the wasdc domain controller:

[9] Understanding IIS Vulnerabilities http://rr.sans.org/web/fix.php and the course books for track5

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Event Log used for all Windows 2000 systems:

Policy	Computer Setting
Maximum application log size	102400 kilobytes
Maximum security log size	409600 kilobytes
Maximum system log size	102400 kilobytes
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually
Shut down the computer when the security audit log is full	Enabled

The Event Log settings are pretty restricted, enforcing no guest access, no overwrites and shut down of system when the security audit log is full. The size is pretty large, although small enough to fit on a single CD if/when a computer needs to be reinstalled when it's not possible to dump them centrally. A central VB-script copies logs on specific hosts that are under audit or for random checks, and copies the rest to archive where they become encrypted. Also see text about logserver in the last segment.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DOMAIN POLICY

The Domain policy is the one being most restrictive and is based on NSA's w2k_domain_policy.inf. These settings are used for regular servers and workstations as well. Microsoft has more information about these settings and they are dicussed at depth there[10]

Password Policy

Password Policy	Setting	Reasoning
Enforce password history	24 passwords remembered	This is the maximum supported by Windows2000
Maximum password age	100 days	Three months should be enough, quarterly internal newsletters helps to remind people by having a little notice on this, 100 is set because of a margin for vacations and distribution problems of the "GIAC Quarterly"
Minimum password age	1 Days	Default from NSA, keeps the user from rotating passwords within the same day
Minimum password length	8 characters	This is lowered for making people NOT writing down the passwords near the computers
Password must meet complexity Requirements	Enabled	Makes password to be based three types of ascii: Upper case, Lower case, Digits, Nonalphanumeric and other basic controls[11].
Store Passwords using reversible encryption	Disabled	DISABLED! Could expose the passwords

The password policy is strict but has a "low" minimum password length, this is made by choice and all users are advised to choose as long passwords as they can remember. The relative low number of eight is for people not having that good memory and making these users NOT writing them down close to the computer.

Although my personal opinion is that external exposed systems (networkwise) are actually better off with a long password and a post -it note within physical reach (locked in a safe).

[10] Securing Servers Based on Role http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secops04.asp

[11] Passwords co mplexity requirements http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/504.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Account Lockout Policy

Account Lockout Policy	Setting	Reasoning
Account lockout duration	960 minutes	16hours making sure that if someone tries a break in after office hours the account lockout will be enforced until the next working hour. And if there are 10 post -it notes its only a 50% chance of the intruder getting in…
Account lockout threshold	5 invalid logon attempts	5 invalid logon attempts
Reset account lockout counter after	960 minutes	This is the time before the counter resets, it is as restrictive as the Duration

As the Reasoning text implies it should be hard for a intruder to gain access, this causes some incidents to be handled. The policy also hel ps people not to type down the wrong password. Five attempts is for people having around 3 accounts in their heads, and offering them a chance to fail on them once or twice. If an account should be locked out staff need to contact helpdesk.

Kerberos Policy[12]

Kerberos Policy	Setting	Reasoning (default NSA settings)
Enforce user logon restrictions	Enabled	
Maximum lifetime for service ticket	600 minutes	
Maximum lifetime for user ticket	10 hours	
Maximum lifetime for user ticket renewal	7 days	
Maximum tolerance for computer clock synchronization	5 minutes	

This is left at its default, mainly for performance reasons and that some articles imply that it shouldn't be altered without a good reason.

[12] Kerberos Policies http://support.microsoft.com/default.aspx?scid=KB;EN -US;Q231849&

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Domain Controller Policy
(based on w2k_dc from NS A)

Audit Policy

Local Policies, Audit Policy	Computer Setting	Reasoning
Audit account logon events	Success, Failure	Full Audit
Audit account management	Success, Failure	Full Audit
Audit directory service access	Failure // No auditing for Server policy	Keeps track of bad attempts. Not relevant for regular server or clients (No Auditing)
Audit logon events	Success, Failure	Full Audit
Audit object access	Failure	Keeps track of bad attempts
Audit policy change	Success, Failure	Full Audit
Audit privileg e use	Failure	Keeps track of bad attempts
Audit process tracking	No auditing	Not vital
Audit system events	Success, Failure	Full Audit

Green is for changes compared to DC/Servers/Workstations
Red is for changes from the GPOs, supplied by NSA

Pretty massive audit causing alot of logs to be centralized. Logs are correlated with IDS and Application Logs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

User Rights Policy

Local Policies, User Rights Assignment	Computer Setting
Access this computer from the network	Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS // Administrators, Users for Server Policy // Users, Administrators for Workstation policy
Act as part of the operating system	
Add workstations to domain	
Back up files and directories	Administrators
Bypass traverse chec king	Authenticated Users // Users for Server and Workstation Policy
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	
Enable computer and user accounts to be trusted for delegation	Administrators // Not defined with Workstation Policy
Force shutdown from a remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	
Log on as a service	
Log on locally	Administrators // Users, Administrators for Workstation policy
Manage auditing and security log	LogAdministrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Users, Administrators for Workstation policy
Replace a process level token	
Restore files and directories	BackupAdministrators
Shut down the system	Administrators // Users, Administrators for Workstation policy
Synchronize directory service da ta	
Take ownership of files or other objects	Administrators

Green is for changes compared to DC/Servers/Workstations
Red is for changes from the GPOs, supplied by NSA

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Noteworthy is that the managing of audits and security logs are granted to LogAdministrators and not Administrators. The setting for Debug isn't set, this is to prevent dumping the SAM -database (another GCWN -practical from Marcelo Weyne Romcy has more information on this subject) Also see section on addtional security for more info on Bypass traverse checking.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Other GPO settings and policies

Security Options Policy

Local Policies, Security Options	**Computer Setting**
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow Automatic Administrator Logon	Disabled
Allow server operators to schedule tasks (domain controllers only)	Disabled // This setting is "Not Defined" for Server policy
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires	Not defined
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Enabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Enabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Disable Media Autoplay	All Drives
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	See text below
Message title for users attempting to log on	Titlebar text is: GIAC Property, all usage is monitored!
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Rename administrator account	Not defined // This is done at installation time
Rename guest account	Not defined // This is done at installation time
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 or sign secure channel data (always)	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Secure system partition (for RISC platforms only)	Not defined
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock Workstation
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

Green is for changes compared to DC/Servers/Workstations
Red is for changes from the GPOs, supplied by NSA

Even if "Additional restrictions for anonymous connections" is standard by the NSA settings I would like to clarify its importance that its setting to "No access without explicit permissions" this makes a setting that all connections must have a valid/active account in the domain to gain access.

Server and Client communication is always signed, even though this causes some overhead. According to Microsoft up to 15% for signing and verifying each packet between servers. The reason for requirement of signing is to reduce the risk of MitM -attacks.

The LAN Manager Authentication Level is set to most restrictive and GIAC can get away with it by standardizing on Windows 2000 systems where this Authentication is needed.

Smart Cards are not yet deployed throughout the organization for Windows2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

machines, the GPO is already modified to handle such a enrollment for the removal behavior.

Varning Banner

GIAC SYSTEM

You are about to access a GIAC Enterprise System.
This equipment is to be used for work related tasks as described by your employer.

Unauthorized attempts to access or change information on these systems are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986.

GIAC Enterprises may monitor and audit the usage of systems.
All persons are hereby notified that use of this system constitutes consent to monitoring and auditing.

This warning banner has taken inspiration from NASAs IT -Security warning banner [13].

Although Department of Defense also has a good warning banner, this banner also implies that a authenticated and authorized employee may only use the system as described by the employer in a more clear stated text. The text is translated and modified for Dutch and Swedish as well. (out of scope for this report.)

[13] IT Security Warning Banner NASA IV&V Facility http://www.ivv.nasa.gov/ privacy/banner.shtml

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A note: Basic settings such as control panel and desktop settings are not discussed within this report. However worth noticing is that the dev.giac.com has a less restrictive policy for its users (developers).

Internet Explorer 6 is the standard web browser used for GIAC enterprises, it is rebuilt with IEAK.

The security zones have been changed around some to provide extra flexibility and security:

- Internet zone is defined for "semi-restricted" (read: not specifically trusted) sites, all scripting is turned off, no ActiveX or Java enabled. This zone is for the internet as a whole.
- Local Intranet is redefined to be sites of relevance for employees, some scripting are enabled. Sites that are included are the types of vendors and news agencies, this means that UNC-resolvable, localsites, and sites redirected by proxy are not included at all in this zone.
- Trusted Sites are redefined for official intranet-servers and partners.
- Restricted sites are locked down very hard and include spyware sites and affiliates with them, such as bonzo buddy, wild tangent, comet cursor and so on.

IT-security and admin Group Policy (for users in the IT-support OU)

Under Windows settings, Security Settings, Local Policies, User rights assignment

User rights assignment Policy for IT-support

Policy	Computer Setting
Access this computer from the network	Administrators
Debug programs	Administrators
Enable computer and user accounts to be trusted for delegation	Administrators
Log on locally	Administrators
Remove computer from docking station	Administrators
Shut down the system	Administrators

Also keep in mind that previous policy discussed also included separate roles for Backup and Audit/Log.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Under Windows settings, Security Settings, Local Policies, Security Options

Security Options Policy for IT -support

Policy	Computer Setting
Number of previous logons to cache (in case domain controller is not available)	10 logons

The GPO is created the types of user that can access the NOC's co mputers, and limiting others. It also gives the right for administrators to debug any forms off failures on the machine. An important policy that others may have learned the hard way is to include cached logons. All computers that this policy applies to ar e in a locked down area. This GPO is set with the no override option.

For the dev.giac.com domain there is some minor changes that are noteworthy:

All developers have the right to debug programs. Some settings such as removed control panels are not enforced. They are also in a higher degree local administrators on their own computers and are trained and educated regularly in computer security and the computers all lack floppydrives and cd -rom players. All communication is through the network and no c ode is to leave the building in source code format.

Developer Debug Policy

Policy	Computer Setting
Debug programs	Developers

For laptop users the option for Logons to cache is also in use, this is to provide extra flexibility for them.

Laptop Cache Logon Policy

Policy	Computer Setting
Number of previous logons to cache (in case domain controller is not available)	10 logons

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Additional information about the systems, and more

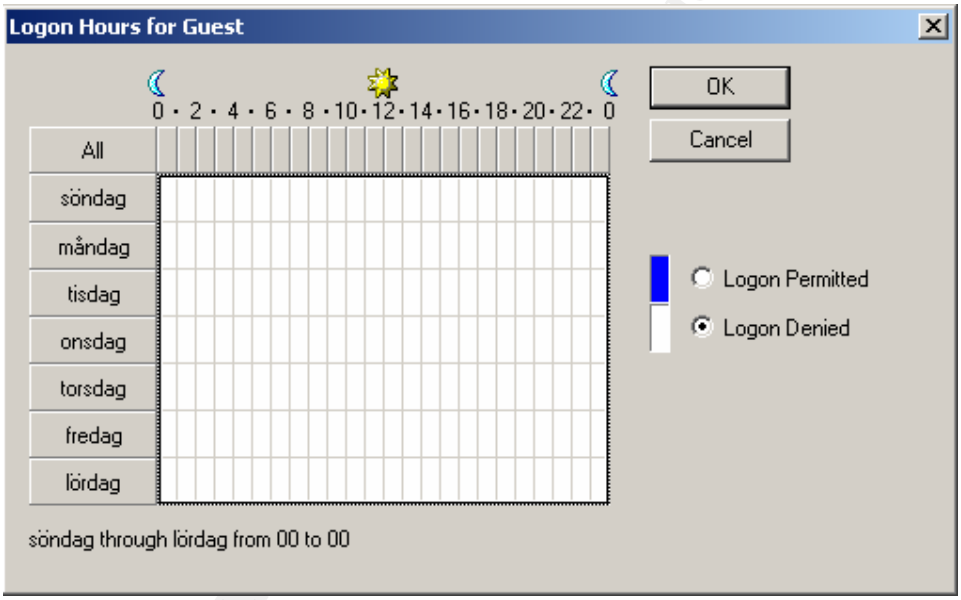
Some security issues has been discussed in the section for description of the GIAC Enterprise

Logserver

The logserver in used to rotate the logs to is configured not to allow access to itself from the network. All post-administration is taken care of over KVM -switches from the IT-security auditors. SANS Institute have a good d ocument on the subject [14]

Guest account lockout

As additional security for not compromising the whole architecture with a faulty click on the mouse. The guest account is also locked out with GPO so that no available hours to log in exist, no stations that u ser may use and no rights on any file systems. [Sorry for the Swedish within the bitmap]



Picture6: Logon Denied for Guest account at all times

Security Roles in use by GIAC

There are generally speaking five types of authorization roles to a system:

Standard User: Staff, Contractors and Trainees
Power Users: IT-staff, strategic planners, Research and Development and some executives.
LogAdministrators: Staff responsible for information and logs on the system
BackupAdministrators: Staff responsible for re storing and and checking system integrity.

[14] Automated auditing http://www.sans.org/newlook/digests/auto_audit.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Administrators: IT-staff responsible for accounts and maintenance (Systemadministrators), for clients this role also includes helpdesk

The primary reason for separating the Admin -roles is to separate access who handles logs and who handles accounts (of course a system administrator could violate rights by changing his own accounts, that would be present in a non -violatile log).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Open ports on domain controllers

To be able to successfully implement IPSEC througho ut the organisation at a later stage it is important to document the ports in use, the following text is a rehash from existing papers[15] but i found it important to include.

UDP Ports for Domain Controller

88/UDP (User Datagram Protocol) -- Kerberos
137/UDP -- NetBIOS Name Server
138/UDP -- NetBIOS Datagram
389/UDP -- LDAP
1645/UDP -- IAS: Internet Authentication Service
1646/UDP -- IAS: Internet Authentication Service
1701/UDP -- L2TP
1723/UDP -- PPTP
1812/UDP -- IAS Internet Authentication Service
1813/UDP -- IAS Internet Authentication Service
(self note: high UDP-ports must be open for answers from UNIX DNS -servers)

TCP Ports for Domain Controller

21/TCP (Transmission Control Protocol) -- FTP
25/TCP -- SMTP
80/TCP -- HTTP
119/TCP -- NNTP
135/TCP -- RPC
139/TCP -- NetBIOS Session Services
443/TCP -- HTTPS
445/TCP -- SMB
464/TCP -- Kerberos Password V5
500/TCP -- ISAKMP
563/TCP -- SNEWS
593/TCP -- RPC over HTTP
636/TCP -- LDAP over SSL
1067/TCP -- Installation Bootstrap Service
1068/TCP -- Installation B ootstrap Service
3268/TCP -- Microsoft Global Catalog
3269/TCP -- Microsoft Global Catalog with LDAP/SSL
3389/TCP -- RDP

[15] Windows 2000 Domain Controller Default Ports
http://support.microsoft.com/default.aspx?scid=KB;EN -US;Q289241&

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Unnecessary services

For NT4 the following services should be turned off for a C2 -certification[16].

NT4 unnecessary services (for C2 -certification)
Computer Browser
Microsoft DNS Server
Netlogon
NTLM SSP
RPC Locator
RPC Service
TCP/IP NetBIOS Helper
Spooler
Server
WINS
Workstation
Event Log

Please note that for a C2 more steps has to be performed. For further information t he most informative link I found was http://www.boran.com/security/nt2.html (not listed as source, only a recommendation)

From Harpal Parmars Paper on GCNT [17] he lists the following services for Windows 2000

Windows 2000 unsafe services

Computer Browser
DHCP Client
DHCP Server
DNS Server
Fax Service
IIS Admin Service
Internet Authentication Service
Internet Connection Sharing
Intersite Messaging
Messenger
NetMeeting Remote Desktop Sharing
Print Spooler
Protected Storage
Remote Registry Service

[16] Microsoft Windows NT 4.0 C2 Configuration Checkl ist http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/c2config.asp

[17] Harpal Parmars GCNT Paper http://www.giac.org/practical/Harpal_Parmar_GCNT.doc

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Routing and Remote Access
RunAs Service
Simple Mail Transport Protocol (SMTP)
TCP/IP NetBIOS Helper Service
Telephony
Telnet
Terminal Services
Windows Internet Name Service (WINS)
World Wide Web Publishing Service

Microsoft lists the following services as required by IIS[18]

Required services for IIS

Event Log
IIS Admin Service
License Logging Service
MSDTC
Protected Storage
Remote Procedure Call (RPC) Service
Server
Windows NT Server or Windows NT Workstation
Windows NTLM Security Support Provider
Workstation
World Wide Web Publishing Service

"May be required" services for IIS

Certificate Authority (required in order to issue certificates)
Content Index (required if using Index Server)
FTP Publishing Service (required if using FTP service; it's highly recommended that FTP and Web services run on different servers)
NNTP Service (required if using NNTP Service)
Plug and Play (recommended, but not required)
Remote Access Services (required if you use dial-up access)
RPC Locator (required if doing remote administration)
Server Service (can be disabled, but required to run User Manager)
SMTP Service (required if using SMTP Service)
Telephony Service (required if access is by dial-up connection)
Uninterruptible Power Supply (UPS) (optional; but it is recommended that you use a UPS)
Workstation (optional; important if you have UNC virtual roots)

[18] Services Needed to Run a Secure IIS Computer http://support.microsoft.com/default.aspx?scid=kb;EN-US;q189271

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access Control Mechanisms in Windows 2000

The following subject are rewritings from Microsofts papers on the subject [19]. I just rewrote it out of curiosity.

Security in Active Direc tory is based on Access Control Lists (ACLs) on every object.

Security principals based on users, security groups (keep in mind that these are different from distribution groups), services and computers. Objects can be defined by being a file, process, e vent or anything else with a Security Decriptor.

There are two types of ACL; DACL(discretionary) and SACL(system) [20]. All objects are identified by their Security Identifier (their SID). Keep in mind that these SIDs are unique and should never be a refere nce to any other object [21]. The Security Descriptor String Format [22] consists of four main components:

O: Owner
G: Primary Group
D: DACL
S: SACL

The entry in an ACL is an Access Control Entry (ACE). An ACE contains the set of access rights and SIDs that iden tifies[23] the trustee for the rights allowed, denied and audited[24]. The trustee is the user/group/session to which ACE applies. Each ACE applies to one trustee.

Security Descriptors keeps the ACL for which rights that has been assigned to an object by what u sers, these are called discretionary access control lists (DACLs). Keep in mind that the use of NULL DACLs will grant all access to all users. The ACL is controlled by the owner of the object and specifies the access particular users or groups can have to the object. The reasoning behind this is to grant the absolut user the correct set off permissions while keeping general/unauthorized/unauthenticated users such as guest out.

SACLs are the ACLs that control the generation of audit logs, on attempts to acc ess objects. The SACLs are typically only in control by system administrators.

[19] Security http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28001191
[20] Security Descriptors http://msdn.microsoft.com/library/default.asp?url=/library/en -us/security/security/security _descriptors.asp
[21] Security Identifiers http://msdn.microsoft.com/library/default.asp?url=/library/en -us/security/security/security_identifiers_sids_.asp
[22] Security Descriptor String Format http://msdn.microsoft.com/library/default.asp?url=/library/en -us/security/security/security_descriptor_string_format.asp
[23] SID Strings http://msdn.microsoft.com/library/default.asp?url=/library/en -us/security/security/sid_strings.asp
[24] Access Control Entries http://msdn.microsoft.com/library/default.asp?url=/library/en -us/security/security/access_control_entries_aces_.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Information on Traversing of folders[25]

The link supplied as a footnote is not working, see below for google cache). I have included/modified parts of the text for Traverse Fol der Permissions. Basically just for being curious on why NSA haven't limited that option. Although GIAC has chosen that it is not worth the hassle.

> Traverse Folder permission allows or denies browsing of folders, the user cannot open the folder without proper access/authorization. The permissions can only be used for users not listed in the security policy with assigned user's "Bypass traverse checking" right. (Initial setting is "Everyone" group, so for all users).

Example of combinations on (h: \test\traverse).

Permission for "test" directory according to the table: Full permission for "traverse" and "1.txt" and "2.txt" files.

Menu start 1. h: \test\ 2. h:\test\traverse \
Command prompt 1. cd test 2. cd test \traverse
Command Prompt 1. type h: \test\1.txt 2. type h: \test\traverse \2.txt
(Denied - Using the Command.com - Invalid Directory, Using the cmd.com - Access is Denied)

Permission	**Bypass traverse checking. Defined**	**Bypass traverse checking. Not Defined**
Traverse Folder	1. Denied, 2. OK 1. OK, 2. OK 1. Denied, 2. OK	1. Denied, 2. OK 1. OK, 2. OK 1. Denied, 2. OK
List Folder	1. OK, 2. OK 1. Denied, 2. OK 1. OK, 2. OK	1. OK, 2. Denied 1. Denied, 2. Denied 1. Denied, 2. Denied
Traverse Folder + List Folder	1. OK, 2. OK 1. OK, 2. OK 1. OK, 2. OK	1. OK, 2. OK 1. OK, 2. OK 1. OK, 2. OK
No Permission	1. Denied, 2. OK 1. Denied, 2. OK 1. Denied, 2. OK	1. Denied, 2. Denied 1. Denied, 2. Denied 1. Denied, 2. Denied

Practically, you will encounter such cases not too much. On client computers this righ t assigning is not used, only administrators operate servers and the directories are easily shared for clients.

[25] Traverse Folder / Bypass traverse checking http://www.atlguide2000.com/eng/win2k/ntfs3.htm
http://216.239.39.100/search?q=cache:8Rt18o0tlm8C:www.atlguide2000.com/eng/win2k/ntfs3.htm+&hl=sv&ie=UTF-8

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

One OS, One Service
When and as often as resources/budget permits the usage of using dedicated machines for its duties, primary to get better security and also for ease of administration/documentation/dependencies.

Usage of EFS

EFS is used on specified folders and with the migration to WindowsXP, EFS will be used for Offline folders.

IPSEC on internal networks

As hardware accelerators inside t he NetworkInterfaces has become cheaper it is a suitable standard to encrypt traffic within the company.

Hotfixes among other updates

The distribution of hotfixes is not by standard available by GPO. According to Eric Schultze's presentation now availabl e online[26] you should create a .MSI package for the hotfix and distribute it over GPO software installation.

Verification of backups

Even though this is mentioned in the text, it is important to clarify that it is important to regularly verify that backups are taken correctly and that they are usable to restore computers.

Documentation and routines

Another part not solved by technical architectures and software solution is that the complexity of networking systems gets bigger and bigger. It is important to document plans and changes throughout the enterprise with proper documentation and routines. All computer systems and services should have their own documentation and it should be written well enough so that other people beside the system administrator hi mself/herself can get the system back online in the case of failure.

[26] How to keep up with Security Patches http://www.blackhat.com/presentations/win -usa-02/schultze - winsec02.ppt

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Education

Finally and definitely not least important; Education. It is very important for almost all personnel to educate themselves in how to work with computers in a secure way. All users are provided with a educational guide on how viruses work and how they can easily avoid them (example: do not open suspicious mail or attachments, do not take programs with you from home and such). The users can there after logon to a webserver where they perform a test of certification on their ability to use a computer within the enterprise.

For IT-personnel it is important to gain deeper knowledge and management encourages employees to go to IT -conferences such as SANS -conferences or vendor specific.

Thank you for your time reading this report!

/David Hed
IT Security Architect
GIAC Enterprises

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sources

Cisco Anti-Spoof Egress Filtering http://www.sans.org/dosstep/cisco_spoof.htm

How to Prevent DNS Cache Pollution http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q241352&

IIS as a Secure Web Publishing Framework

http://www.microsoft.com/usa/presentations/Finnegan_DemI_SecuritySummitWest.ppt

Passwords complexity requirements http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/504.asp

Kerberos Policies http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q231849&

IT Security Warning Banner NASA IV&V Facility http://www.ivv.nasa.gov/privacy/banner.shtml

Securing Servers Based on Role

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/se

cops04.asp

Windows 2000 Domain Controller Default Ports
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q289241&

Microsoft Windows NT 4.0 C2 Configuration Checklist

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/c2config.asp

Harpal Parmars GCNT Paper http://www.giac.org/practical/Harpal_Parmar_GCNT.doc

Services Needed to Run a Secure IIS Computer http://support.microsoft.com/default.aspx?scid=kb;EN-US;q189271

Access Control Lists

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/access_control_lists_acls_.asp

Security Identifiers

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_identifiers_sids_.asp

Security Descriptors

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_descriptors.asp

Security Descriptor String Format

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_descriptor_string_format.a

sp

Security http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28001191

Access Control Entries

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/access_control_entries_aces_.asp

Mixed Mode vs. Native Mode http://www.winnetmag.com/Articles/Index.cfm?ArticleID=7156

Active Directory FSMO Roles http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q197132&

Fossen, Jason. SANS track 5 book 5.1, SANS Institute

Automated auditing http://www.sans.org/newlook/digests/auto_audit.htm

Understanding IIS Vulnerabilities http://rr.sans.org/web/fix.php

Traverse Folder / Bypass traverse checking http://www.atlguide2000.com/eng/win2k/ntfs3.htm

How to keep up with Security Patches http://www.blackhat.com/presentations/win-usa-02/schultze-winsec02.ppt

SID Strings http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/sid_strings.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.