Global Information Assurance Certification Paper

SANS GIAC
GCNT Practical Assignment Version 3.0
Option # 1

A Secure Windows 2000 Infrastructure Design

Marcelo Weyne Romcy
February 12, 2002

Description of GIAC Enterprises

GIAC Enterprises is a Brazilian E-business start-up company that deals with on-line sales of fortune cookie sayings. The company received recent investments from a private equity Bank. These investments are being used for product development in Latin America. It has around 180 employees across a main office in Brazil (Sao Paulo) and 4 branch offices in Latin America: Argentina (Buenos Aires), Chile (Santiago), Peru (Lima) and Venezuela (Caracas).

The company has also outside parties (customers, suppliers, and partners) that interact with an Extranet through systems developed using a Microsoft DNA platform.

The main datacenter and Internet connections are centralized in Sao Paulo. 256Kbps leased lines connect all other offices.

Sao Paulo's office maintains 4 departments: Research and Development, Sales and Marketing, Finance and Human Resources and Information Technology. All other offices only provide support for local salesperson, logistic and product distribution. Each branch office has a local IT support technician.

GIAC Enterprises' web site is responsible for 70% of direct sales. The company considers information security a very important issue to support their business. Strong network structure is required to protect assets against internal and external threats.

Network Design and Diagram

25 servers, 165 workstations and 15 notebooks compose GIAC Enterprises' network. All computers are based on Compaq hardware platform.

GIAC Enterprises' workstations and notebooks run Windows 2000 Professional with Office XP installed. Servers are based on Windows 2000 Server platform. Firewall and IDS boxes are the only exceptions, running Windows NT 4.0 and OpenBSD respectively.

GIAC Enterprises' network is segmented into several perimeters. The concepts used for segmentation design are layered security and least privilege. Effective countermeasures are set up together to achieve higher protection.

Bellow is the network map. Each network perimeter design criteria will be discussed in the next sections.

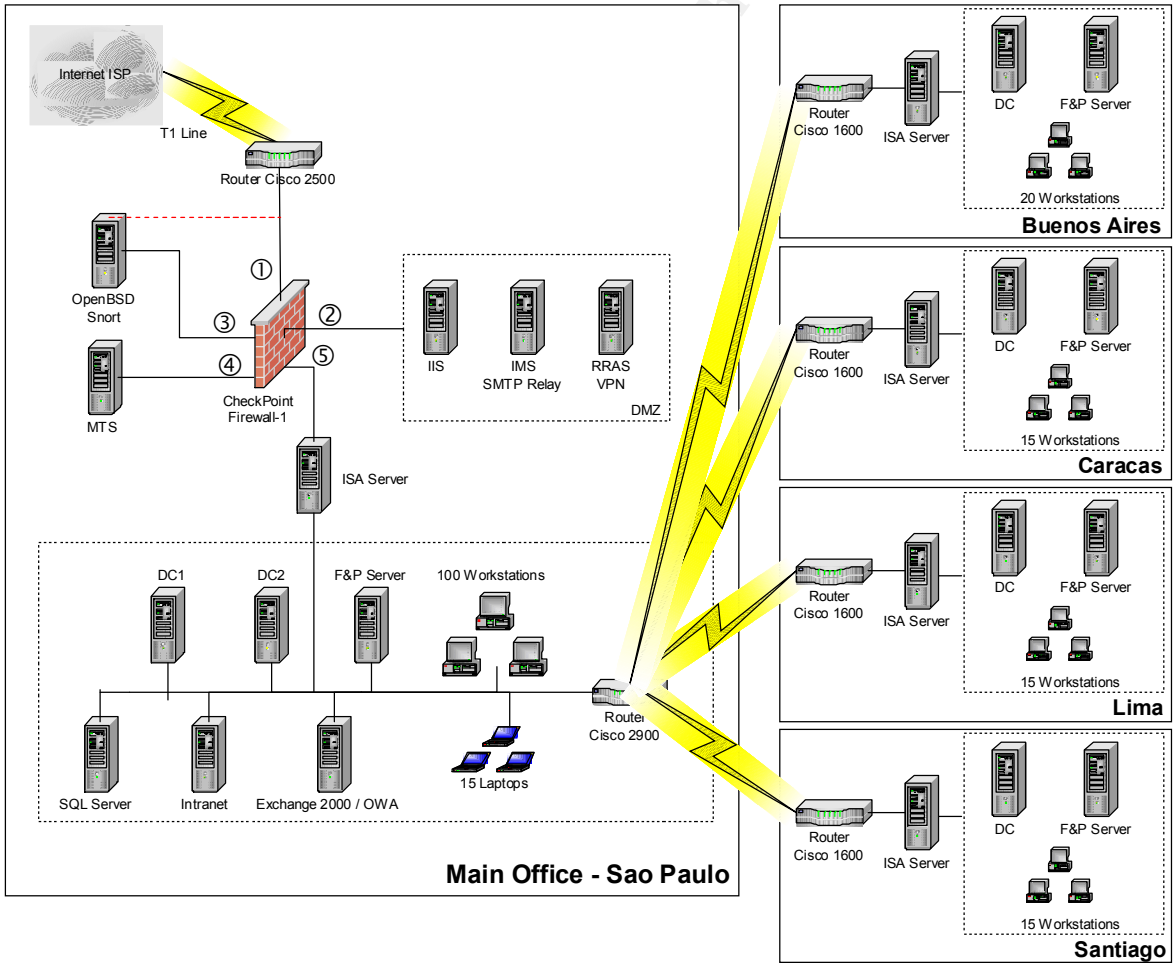

Figure 1 – Network Structure

1 – Outside

GIAC Enterprises uses a T1 line from a CISCO 2500 router to connect to an ISP. An IDS (Intrusion Detection System) box is used to monitor suspicious hacking activities. The IDS stealth network adapter is configured using a switch SPAN port, capturing all inbound and outbound network traffic.

2 – DMZ

In this segment is set up the main Web server (IIS 5) that also acts as primary Internet DNS.

The inbound and outbound SMTP connections are made using an IMS (Internet Mail Service). The internal Exchange server sends and receives SMTP messages through this server that also acts as a secondary DNS server.

GIAC Enterprises VPN server is configured using MS-PPTP. The only authentication protocol enabled is EAP (Extensible Authentication Protocol), requiring valid smart cards to log on. This VPN is used for internal users' remote access (Exchange MAPI clients, OWA and File Server – CIFS). Outside partners also use this VPN to access internal applications. Only specific protocols are enabled from this box to internal network. All authentication process is done using a RADIUS server located in the internal network.

As a second security layer, each group of users has specific ports allowed through customized IP packet filters in RADIUS remote access policies profiles. This VPN box has no other communication with internal network.

VPN servers are common holes in network security design. Countermeasures like isolation and two-factor authentication adopted here provide far more protection. For instance, if the VPN box were connected directly to Internal Network, it would allow unrestricted access to all internal devices in case of a password compromise.

These hosts were all put together in this perimeter because they are the only ones directed accessible via Internet, i.e., with IP static mappings (NAT).

3 – IDS Management

Due its specific and critical role in network security, the IDS management interface must be isolated from any other servers.

Alerts from security events are published into its own web server. Only HTTP and SSH traffic originated from specific management hosts on Internal Network are allowed.

4 – MTS
Segment used to isolate the MTS server. The goal here is to really put into practice an isolated 3-tier database access.

Components in MTS use fixed port ranges restricted on the firewall allowing them to communicate with application front-end (IIS Server). The MTS box has a NAT mapping to access internal SQL Server using port TCP 1433. No other protocols like NetBIOS or CIFS are allowed between this host and other perimeters. The goal is to protect the internal network restricting access to corporate SQL Server.

If an attacker compromises the IIS Server, he could only uses fixed RPC ports ranges to take control of MTS server. The two hosts have no domain relations nor use same passwords. If, after all, the attacker had succeeded, he would only be able to access corporate SQL's TCP port 1433, with no System Administrator (SA) privileges.

5 – Internal Network
GIAC Enterprises internal servers, workstations and connections to other sites are set up into this segment. No inbound IP mappings to the Internet (outside perimeter) are configured.

The network has 2 domain controllers / DNS servers for fault-tolerance (DC1 and DC2), a file & print server, an Intranet server running IIS 5.0, a corporate SQL server and an exchange 2000 server running OWA (Outlook Web Access).

The Internet access is done through ISA server web-proxy and circuit-level gateway services (ISA firewall client is required on all workstations). ISA configuration allows only specific Internet protocols to specific groups of users.

Each branch office has the same structure. They are composed by a local domain controller and a file & print server. Both servers and workstations are located behind an ISA server firewall. This server is responsible for web proxy services, circuit-level gateway, access control, logging and web cache.

The other purpose of branch office's ISA server is to limit network access. IP filters are used, restricting access to specific hosts and ports in the main office. The main idea is to reduce the risk of compromise if internal attacks are originated from branch offices. No modems or other ways of Internet access are allowed throughout the entire network.

Version and patch level of servers, services and applications:

System	Version	Patches applied
Windows NT Server	4.0 SP6a	MS99-041, MS01-022, Post-Windows NT 4.0 Service Pack 6a Security Rollup Package (SRP), MS01-043, MS01-048
Windows 2000	5.0 SP2	MS00-077, MS00-079, MS01-007, MS01-011, MS01-013, MS01-022, MS01-024, MS01-025, MS01-031, MS01-033, MS01-036, MS01-037, MS01-040, MS01-041, MS01-043, MS01-046, MS01-052
MS SQL Server	2000 SP1	MS01-060
MS Exchange Server	2000 SP2	
MS ISA Server	2000 SP1	
MS Office	2002 SP1	MS01-034, MS01-038, MS01-050
CheckPoint Firewall-1	4.1 SP5	
OpenBSD	3.0	
Snort	1.8.3	

Simplified Firewall Security Policy

Direction	Protocol	Source Host	Dest. Host
Inbound	HTTP (TCP 80),HTTPS (TCP 443)	Any	IIS
Inbound	DNS (UDP 53)	Any	IIS, IMS
Inbound	SMTP (TCP 25)	Any	IMS
Inbound	GRE (IP 47), PPTP (TCP 1723)	Any	RRAS
Inbound	RADIUS (UDP 1812, 1813)	RRAS	DC1, DC2
Inbound	SMTP (TCP 25)	Exchange	IMS
Inbound	HTTP (TCP 80), SSH (TCP 22)	Management	IDS
Inbound	RDP (TCP 3389)	Management	Any
Outbound	DNS (UDP 53)	IIS, IMS	Any
Outbound	SMTP (TCP 25)	IMS	Any
Outbound	SMTP (TCP 25)	IMS	Exchange
Outbound	EPM (TCP 135)	IIS	MTS
Outbound	dynamic range (TCP[6000 - 7000])	IIS	MTS
Outbound	SQL (TCP 1433)	MTS	SQL
Outbound	All ports (TCP, UDP)	ISA	Any

Active Directory (AD) Design and Diagram

The GIAC Enterprises' Active Directory structure is based on a single domain model. The main factor to use this model is centralization. Some issues regarding company organization support this model. First, the only purpose of branch offices is to provide local customer and sales support. Besides, each one has less than 25 employees and all company management is done in Sao Paulo. Finally, there is no need for different account policies across the organization.

A single domain structure will provide easier administration and better performance. In this case, organizational units represent the branch offices. If the current scenario changes after an independency of branch offices, the AD structure could be changed to a subdomain model, creating local subdomains to represent each office.

There are two other great advantages of a single domain model. Any user from any office could logon and work transparently while in transit visiting other offices. Besides, when an employee definitively moves from one office to another, his/her account could quickly be moved to other OU, simplifying administration.

We have some Security issues to deal with users' logon names. First, logon names must be less obvious as possible, and totally different from users' E-mail addresses. E-mail addresses are public; users publish their E-mail addresses in discussion lists, websites and application forms. Logon names are important information needed prior to password guessing. GIAC Enterprises logon names are internal ID numbers gathered from HR department. A friendly alias E-mail address is configured in Exchange Server instead of the ID number.

Organizational Units (OU) Design

The OU design takes into account delegation of administration and deployment strategy of group policy.

Basically there are 3 types of OUs in GIAC Enterprises AD Design:

- Departmental OUs;
- Branch Offices OUs;
- Servers OUs.

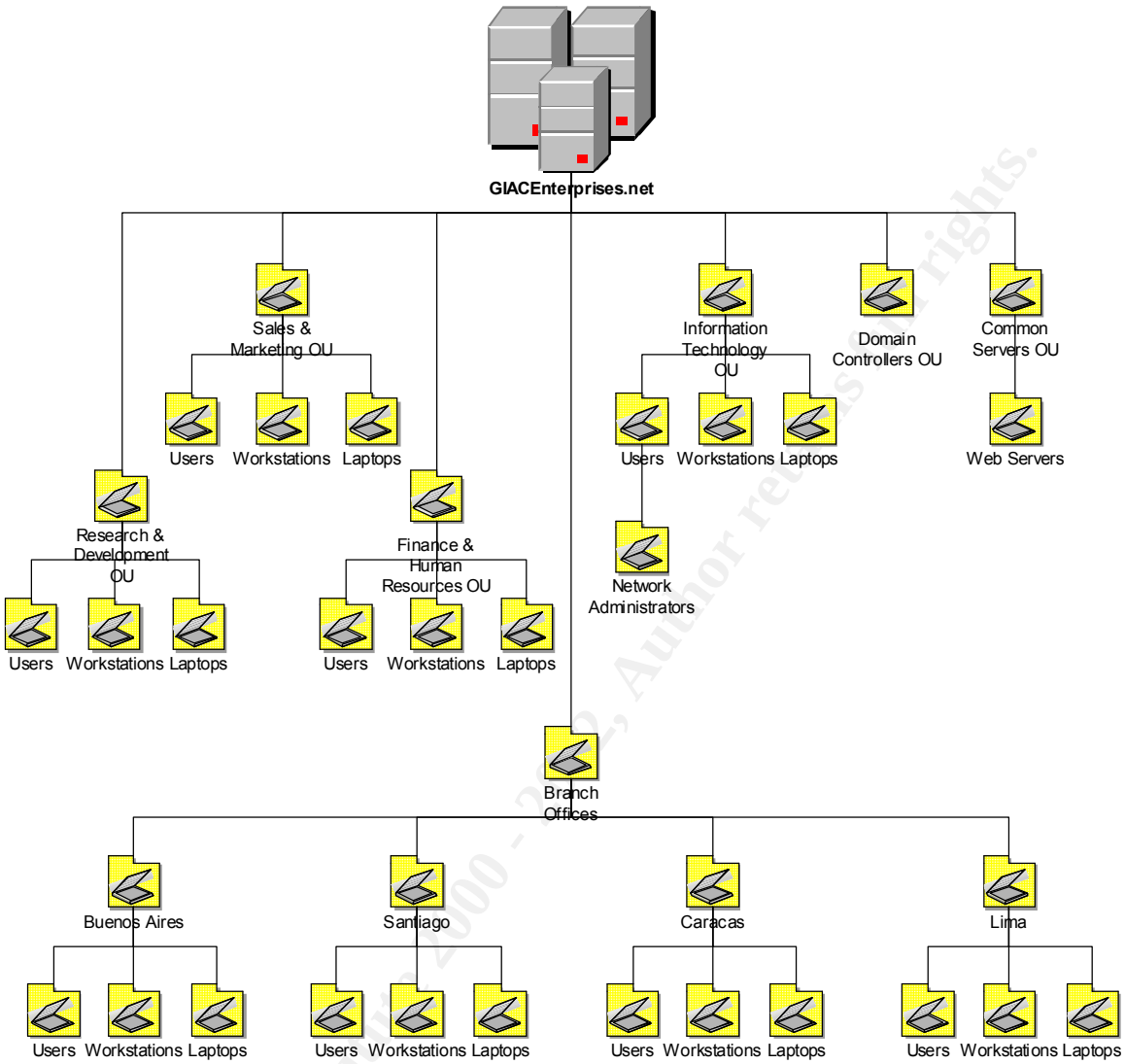

Figure 2 – Active Directory Structure

This division model was built to provide better organization of resources throughout all offices. Inside each OU there are other 3 OUs, each one holding different types of resources (users, workstations and laptops). This hierarchy will be very useful to apply specific group policies. There are different needs regarding group policy related to workstations and laptops.

The departmental OUs are: Research & Development, Sales & Marketing, Finance & Human Resources and Information Technology. All of them use almost the same structure. IT is an exception because of a Network Administrators OU inside Users OU. This division was done as more restrictive security configurations must be applied to network administrators.

The branch offices OUs are: Buenos Aires, Santiago, Caracas and Lima. Each one has the same structure, similar to departmental. One IT support person is present

in each office. Instead of giving him domain administrator privileges, he has delegation over local resources to perform basic tasks like: reset passwords, change account information, add workstation to the domain, and so on.

The servers OUs are Domain Controllers and Common Servers. There is no need, at least for a while, to the use of departmental servers. The IT staff manages all common servers, including those ones hosted in branch offices. All servers have the same security policy. The exception is web servers (Exchange - OWA and Intranet) running IIS that were placed on a Web Servers OU.

AD Sites and Replication

Each office has its own site with a respective subnet. The site link between them is configured to occur outside business hours. If an urgent synchronization or group policy update is needed during the restricted interval time, it must be done manually.

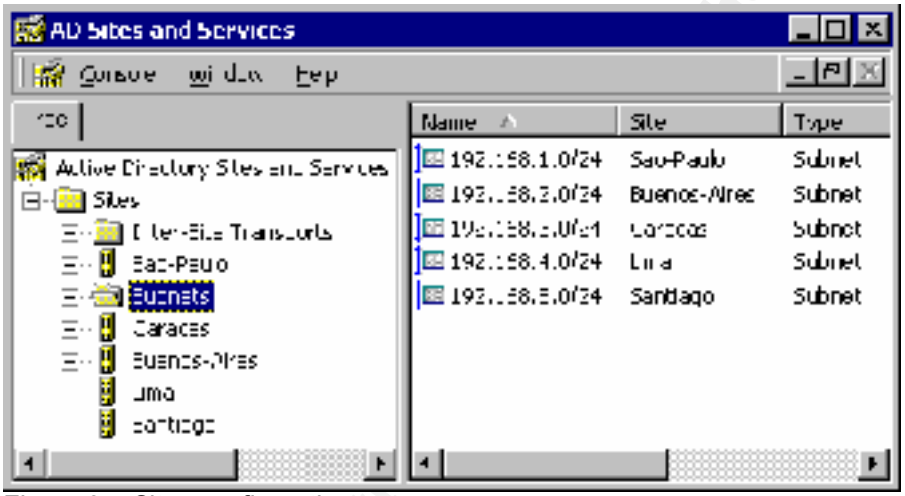

Figure 3 – Sites configuration screen

DMZ Structure

The Windows 2000 servers placed in other perimeters outside Internal (IIS, IMS, RRAS and MTS) are not included in the AD structure previously discussed. The risks associated to them forbid any NetBIOS/CIFS traffic to pass through the firewall.

These servers were installed as stand alone servers and all security configurations are done locally through local group policy / security templates. Other important issue is that each one has totally different local administrators' passwords and they're managed using terminal services by IT staff.

Certificate Authority (CA) Structure

GIAC Enterprises' remote users, administrators and critical staff members log on using smart cards. To accomplish this, a certificate authority is required. This role is performed by DC2, the enterprise issuing CA. For security reasons due risks of CA private key compromise, DC2 is not the root CA. DC2 certificate was generated in an offline standalone root CA. This server generated DC 1 CA certificate and was taken offline after a complete backup. The backup tape, including the root CA private key, is kept locked into a safe.

Group Policy and Security

It's almost impossible to do security without standards. To build these standards, it's necessary to technically design all settings needed to satisfy the company needs.

Regarding Windows 2000, there are lots of configurations needed to reach an acceptable security standard. These configurations are based on software updates, registry settings, permissions settings, local policies, etc. But, before the development of these security standards, some questions arose:

- How to assure that all Windows 2000 computers throughout organization really have the security standard applied?
- How to deploy customized security standards dependent on how critically a computer is?
- How to automatically apply the security standards when a computer is added to the network?

All these tasks could be performed using group policy. Group policy is a critical tool to enforce and maintain security in a Windows 2000 network. GIAC Enterprises will use this tool in order to manage its security environment.

The central component of group policy is the Group Policy Object (GPO). A GPO is a complete set of settings that could be applied in a site, domain or organization unit (OU) level.

In the next sections we will discuss the most important security configurations used in GIAC Enterprises' group policy structure.

The default domain policy and default domain controllers policy contain the main security settings needed. Due specific OU characteristics only few configurations must be specified. These OUs are: Common Servers, Notebooks, Information Technology Users and Network Administrators.

Default Domain Policy

The default domain policy is the first GPO that is applied to all computers in the domain. The settings discussed here will affect every computer and user, unless they've been overridden by other GPOs on site or OU levels.

The GPO structure is split into computer and user configuration. The computer configuration deals with settings applied to computers regardless of which user is logged on. It's first applied during boot process. The user configuration deals mainly with user's environment restrictions, forcing registry settings under HKEY_CURRENT_USER section of computer's registry wherever computer the user is logging in.

Computer Configuration:

Default Domain Policy > Computer Configuration > Software Settings

It's possible to force the installation of any software using group policy. This process is done assigning MSI (Microsoft Installer) files to computers. Several vulnerabilities are mitigated by simply applying a Service Pack or hotfixes. We use this functionality to force the installation of Windows 2000 SP2.

The process is very simple. The Windows 2000 SP2 already has a MSI file located in *\386\update\update.msi*. You must copy all files to a network share, right click the software installation icon, select new > package and point to the MSI file using the UNC path (in our case:*\\dc1\updates\i386\update\update.msi*). Automatically all computers will install the package during boot.

It's pretty good, but some performance issues must be remembered before deploying it. If not, some users will complain (something like: "Hey man! What the hell did you make? Nobody could work!").

The problem is that almost every computer will copy around 100 MB from the same server at the same time (9:00 am). First, if only few computers have SP2 installed is better to use ACLs to control in which groups of computers this setting will be applied. To do this, the default Authenticated Users group on the security tab of package properties must be removed and specific computer accounts are granted read permissions. Second, GIAC has offices in a WAN environment. It's better to create a site GPO for each office pointing to a share in the local network or to create a DFS (Distributed File System) link.

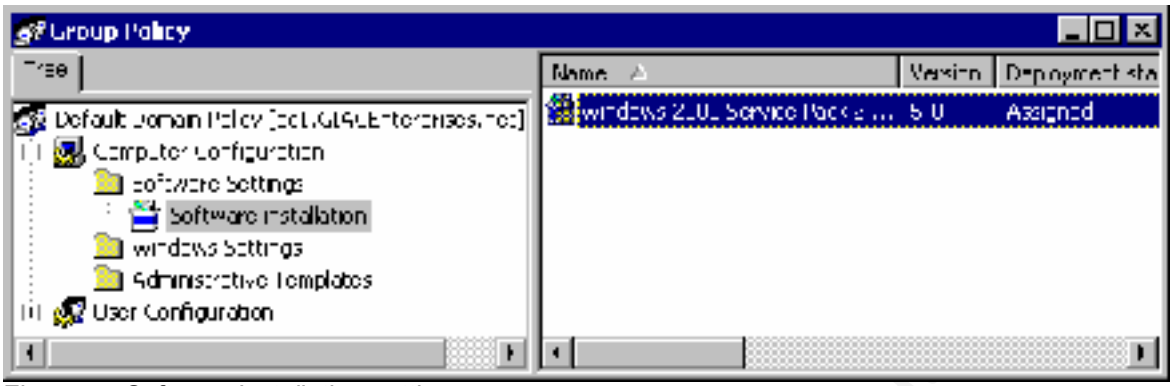

Figure 4– Software Installation settings

Default Domain Policy > Windows Settings > Scripts (Startup / Shutdown)

Not all security settings could be deployed using group policy. Other relevant settings could be done using startup scripts. For instance, hotfixes deployment isn't so easy because they don't include built-in MSI files. GIAC Enterprises uses a customized startup script to quickly deploy hotfixes. The scripts are configured in the startup item inside the scripts section. The script runs each time a computer boots.

Other startup script will apply some registry settings not included in the default domain policy. This script also removes some registry keys, action not possible with group policy itself.

The most important setting applied is removing the LAN Manager Hash storage in AD and local SAM database. This action has a very critical impact to improve overall security. Even if an attacker can get the SAM, he will expend a significant longer time to break passwords. The LAN Manager hash vulnerability makes brute force attacks against SAM database easier. (See page 181 – Hacking Exposed Second Edition).

The script also mitigates other known vulnerability: the use of default administrative shares (Admin$, C$, D$, etc). First, any attacker will already know that all drivers and SYSTEMROOT are shared. Second, the tool used to remotely dump the SAM database (pwdump3) needs the default Admin$ share enabled. More info about pwdump3 can be found at http://www.ebiz-tech.com/html/pwdumpfaq.html.

Other relevant action is to remove the unused subsystems OS2 and POSIX.

Key created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\NoLMHash

Values created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\AutoShareServer - Value: 0

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\AutoShareWks - Value: 0

Values / keys removed:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Optional
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\OS2
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\POSIX

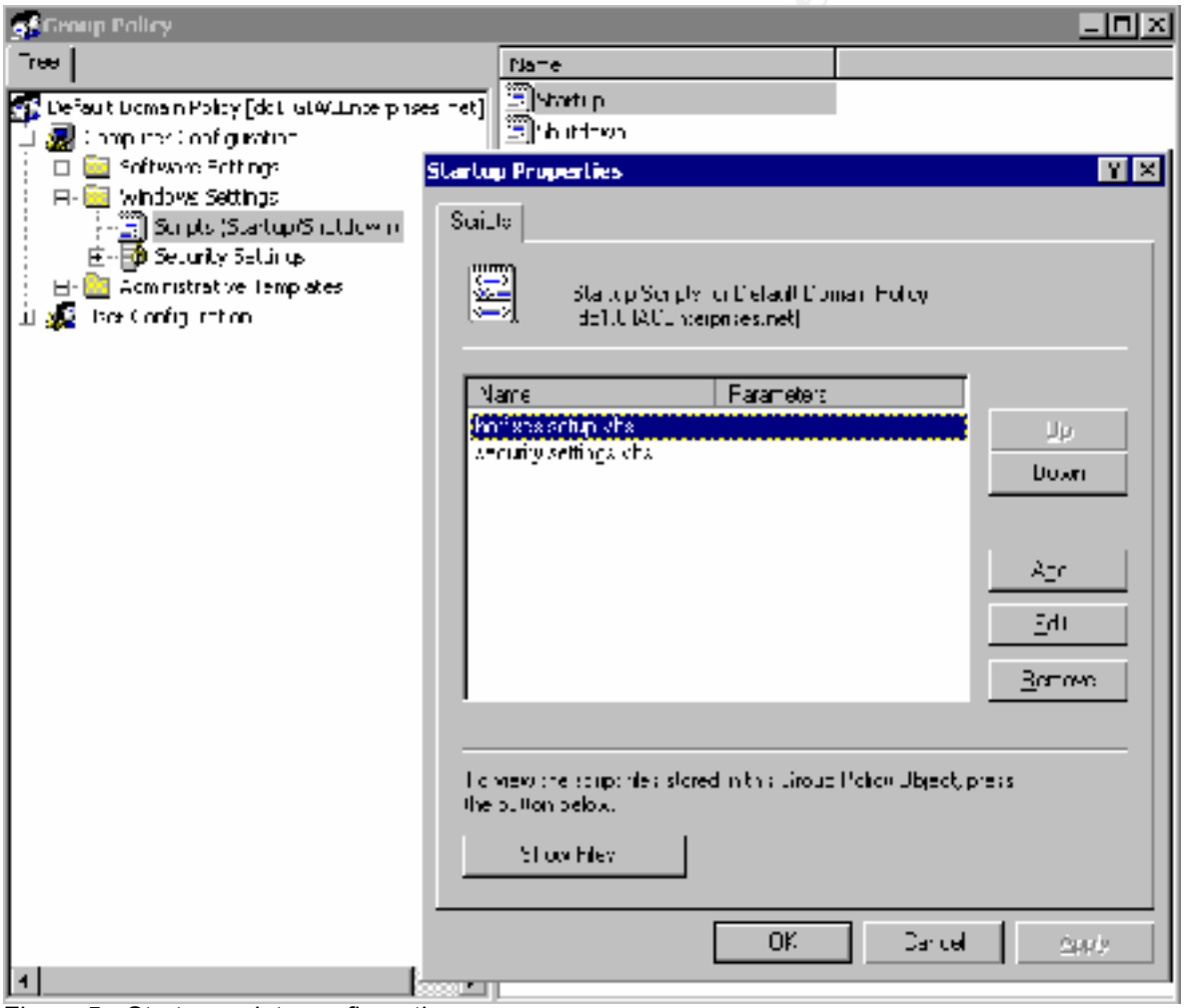

Figure 5 - Startup scripts configuration

Default Domain Policy > Windows Settings > Security Settings > Account Policies > Password Policy

The password policy configuration described here will only be applied to local accounts on Windows 2000 Professional computers and member servers. The domain account policy needs to be different and will be overridden by the Default Domain Controller Policy.

GIAC Enterprises' structure only permits use of domain accounts. The administrator built-in account is the only local account enabled in member servers and workstations. The only exception is the IIS internal accounts that are created and maintained by IIS itself. Thus, this policy can be very aggressive because general users will not be affected.

There's no need for the use of protocols like PAP, CHAP nor digest authentication, so passwords will not be stored using reversible encryption.

Policy	Computer Setting
Enforce password history	10 passwords remembered
Maximum password age	30 days
Minimum password age	5 days
Minimum password length	14 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Default Domain Policy > Windows Settings > Security Settings > Account Policies > Account Lockout Policy

This is an important configuration against local brute force logon attacks. Sometimes attackers prefer to stay guessing local accounts, disguising their activities and avoiding large bad logon log entries in domain controllers. The local account will remain locked until domain administrators remotely unlock it.

Policy	Computer Setting
Account lockout duration	0 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout after	30 minutes

Default Domain Policy > Windows Settings > Security Settings > Local Policies > Audit Policy

GIAC Enterprises will audit almost everything. The most important audit settings are logon and account management. These logs could reveal attacks attempts to

the system. Object access quantity of log entries will depend on auditing settings configured in each file, registry key or AD object.

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not defined
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Not defined
Audit system events	Success, Failure

Default Domain Policy > Windows Settings > Security Settings > Event Log

These settings will be very important in case of a forensics investigation process. It's almost impossible to monitor each member server or workstation local log database.

Policy	Computer Setting
Maximum application log size	10240 kilobytes
Maximum security log size	51200 kilobytes
Maximum system log size	20480 kilobytes
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed
Shut down the computer when the security audit log is full	Disabled

A fixed amount of disk space is defined to logs, mainly to security log (50 MB) and System (20 MB). Disk space is not a problem, as all GIAC Enterprises' computers have at least 30 Gigabytes of disk space. If the logs become full, the older events will be overwritten. The DC event log settings are a bit different and will be detailed later.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > User Rights Assignment

There are some settings different from default user rights to fit security requirements:

Policy	Computer Setting
Access this computer from the network	Authenticated Users
Bypass traverse checking	Administrators
Debug programs	None

The basic change that must be done is to replace the group everyone to authenticated users regarding access from the network. Bypass traverse checking is the possibility to access a subfolder even if a user has no permissions on parent folders. This ability must be restricted to administrators.

One of the most important changes is related to the Debug programs right. At first, this right doesn't appear as a vulnerability to the system. The problem is that tools used to dump the SAM database from memory need an administrator account with this right. The technique used is "DLL code injection". More information could be found at http://www.webspan.net/~tas/pwdump2/. It works even if syskey is enabled, what is default in Windows 2000. It's obvious that if attackers have local administrator privileges, they could give themselves this right. However, the goal is to make their work as difficult as possible.

Default Domain Policy > Windows Settings > Security Settings > Local Policies > Security Options

We will discuss the main issues regarding security configurations done via registry in GIAC Enterprises' default domain policy.

Policy	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions

Null Session is one of the most critical vulnerabilities in a Windows environment. Typically, is the first thing an attacker tries to gather information about the target Windows host. This configuration prevents anonymous users from enumeration of users, shares and other information.

Policy	Computer Setting
Audit use of Backup and Restore privilege	Enabled

This policy is needed to track record of backup and restore operations. This privilege use is not audited by default, even if the audit privilege use is enabled in audit policies.

Policy	Computer Setting
Clear virtual memory pagefile when system shuts down	Enabled

By default, when a computer shuts down, the pagefile is not wiped. Critical information like files, emails and datasets could remain in the memory pagefile. If an attacker has physical access to disk, he could load this file into a hexadecimal editor and look for information. This setting will avoid it, forcing the wiping of memory pagefile before shutdown.

Policy	Computer Setting
Digitally sign client communication (always)	Enabled
Digitally sign server communication (always)	Enabled

All SMB communications are susceptible to man-in-the-middle attacks by default. These two settings will force the SMB client and server components to sign every message during communication. Doing this, it's almost impossible (at least more difficult) to replay or hijack SMB sessions.

Policy	Computer Setting
Do not display last user name in logon screen	Enabled

This basic security setting avoids "tips" to internal attackers trying to logon as previous logged users.

Policy	Computer Setting
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM

In a pure Windows 2000 environment, Kerberos is the main authentication protocol. It is far more secure than any LAN Manager authentication protocol. Therefore, it's still possible to use legacy authentication, even with Kerberos.

There are 3 LAN Manager authentication protocols:

- LAN Manager (LM)

The default authentication protocol used in Windows 9x systems. It's very insecure. LM hashes are sent in clear-text over the network. Tools like L0pth crack (http://www.atstake.com/lc3) could easily sniff the hashes and crack the passwords.

- NTLM

Early Windows NT systems use this protocol. It tries to protect the hashes during authentication process, but weaknesses in its protocol design make still possible the sniffing of the hashes during authentication.

- NTLMv2

NTLMv2 is the Microsoft response to known NTLM weaknesses. It uses a key exchange algorithm to avoid capture of NTLM hashes during authentication. L0pth Crack sniffing tool isn't able to get the hashes during NTLMv2 authentication.

The only reason to permit other protocols than NTLMv2 is pre-compatibility with legacy systems. GIAC Enterprises' internal network has only Windows 2000 systems. Therefore, it will only allow NTLMv2 authentication and refuse any attempt to use LM or NTLM.

Policy	Computer Setting
Message text for users attempting to log on	The use of this system must adhere with GIAC Enterprises Security Policy. All system activity is being monitored.
Message title for users attempting to log on	Important Information

Here, we configured a basic awareness message shown to users before interactive logon. This message is part of company's security policy.

Policy	Computer Setting
Prevent users from installing printer drivers	Enabled

By default, any user could install a printer driver. This privilege could be dangerous if a user is tricked to install a fake printer driver that, in fact, is a Trojan-horse program. Only administrators or power users are able to install printer drivers.

Policy	Computer Setting
Rename administrator account	675437

This is an important security setting. Default administrator account logon names it's an invite to brute-force attacks. The good practice is to rename this account to something obscure.

It's worthless to rename administrator account if DNS servers hold a SOA (Start of Authority) record that could reveal the new administrator account. The information in this record was changed to avoid showing administrator's real account.

Policy	Computer Setting
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled

Critical information is exchanged using secure channels. By default, a computer could not require encryption / signing if the domain controller is not capable. These settings will enforce the strength of secure channels and will require a strong session key.

Policy	Computer Setting
Smart card removal behavior	Lock Workstation

When a user logs on using a smart card it's possible to set up the system to immediately lock the computer if the card is removed from reader. GIAC Enterprises has some smart card users and this setting provides easy lockout of their interactive sessions.

Default Domain Policy > Windows Settings > Security Settings > Restricted Groups

Users are not administrators of their own machines. This is a requirement regarding workstation security. This domain policy setting will help GIAC Enterprises to enforce that Domain Admins group and the renamed local administrator account are the only members of the local administrators group.

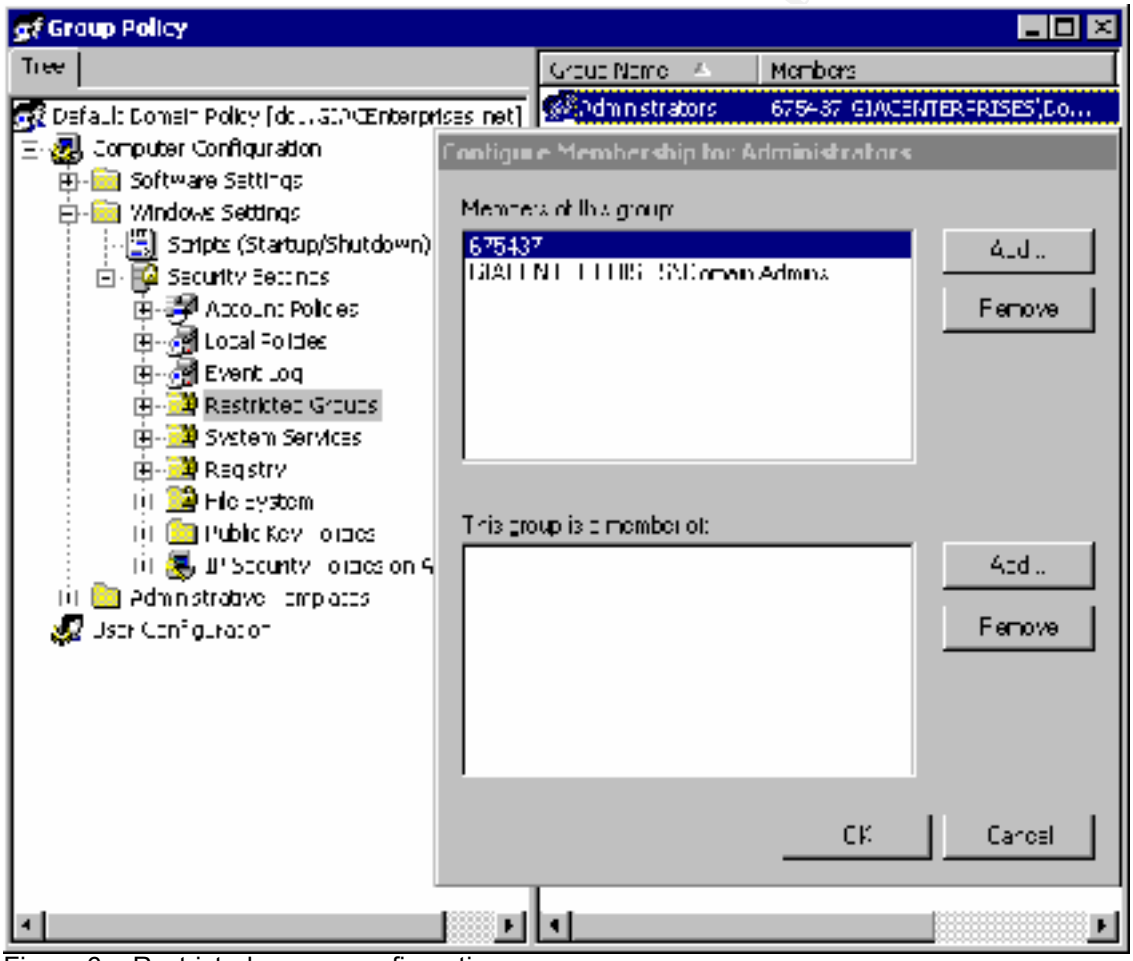

Figure 6 – Restricted groups configuration

Default Domain Policy > Windows Settings > Security Settings > System Services

Telephony service is required for creation of dial-in connections in Windows 2000. This policy disables this service, denying the use of internal or external modems.

Service Name	Startup	Permission
Telephony	Disabled	Configured

Default Domain Policy > Administrative Templates > Network > Offline Files

Policy	Setting
Enabled	Disabled
Disable user configuration of Offline Files	Enabled

Windows 2000 introduced a new feature called Offline files. Basically it will copy selected files/folders to the local machine and synchronize the changes. It's a very useful feature regarding mobile users.

The main problem is that offline files are copied to the <*SYSTEMROOT*>*CSC* directory without any encryption. This feature is not compatible with Windows EFS (Encrypted File System). If you try to encrypt this directory, offline files will not work properly.

Security risks related to stolen notebooks will avoid the use of this feature. Instead of using it, users are instructed to manually copy the files to a local folder encrypted with EFS.

This drawback is not present in Windows XP. GIAC Enterprises is analyzing migration to this platform.

User Configuration:

Some user desktop restrictions must be applied to reduce the risk of misconfigurations done by users. These settings will not be deeply discussed here. Basically, users' access is denied to overall system configuration, control panel, MMC snap-ins, Internet explorer configuration and network & dial-up connections.

Two important security settings are explained bellow.

Default Domain Policy > Administrative Templates > System > Disable Autoplay

Policy	Setting
Disable Autoplay	Enabled

Autoplay is a very nice and risky feature to Windows users. An attacker could insert a disk into a user's CD-ROM drive while he/she is not present. Any program

specified in the autorun.inf file will run, regardless if the workstation is locked or not. GIAC Enterprises will disable Autoplay in all computer drives.

Default Domain Policy > Administrative Templates > Control Panel > Display

This policy forces screen saver password protection in all computers. The screen saver executable name is *scrnsave.scr*, blank screen saver present in any Windows 2000 system.

The user will not be able to change these settings. The specified timeout set for overall users is 5 minutes.

Policy	Setting
Hide Screen Saver tab	Enabled
Activate screen saver	Enabled
Screen saver executable name	Enabled
Password protect the screen saver	Enabled
Screen Saver timeout	5 minutes

Default Domain Controllers Policy

Some settings need to be overwritten by default domain controller's policy in order to fit different authentication, auditing and logging requirements.

Default Domain Controllers Policy > Windows Settings > Security Settings > Account Policies > Password Policy

Policy	Computer Setting
Minimum password length	8 characters

The only change needed is to reduce the length of domain user's password to 8 characters. This length is better than the usual length of 7 characters because LM Hashes are not maintained in the system. Otherwise, password crackers could split the original password into 2 halves of 7 and 1 characters length, easily revealing the second half.

Critical users are forced to logon using smart cards. These users have random passwords of 127 characters length configured by administrators.

Default Domain Controllers Policy > Windows Settings > Security Settings > Account Policies > Account Lockout Policy

The goal here is to avoid and detect brute force attacks without excessive user annoyance. An acceptable threshold of 5 invalid logons is set.

Policy	Computer Setting
Account lockout threshold	5 invalid logon attempts

Default Domain Controllers Policy > Windows Settings > Security Settings > Local Policies > Audit Policy

The only auditing setting specific to domain controllers is AD directory access. This setting will not log anything until auditing is set in each AD object.

Policy	Computer Setting
Audit directory service access	Success, Failure

Default Domain Controllers Policy > Windows Settings > Security Settings > Event Log

Due to larger amount of information being stored, log sizes for domain controllers are different. Each DC has a specific disk partition for log files storage. All log files are backed up weekly.

Policy	Computer Setting
Maximum application log size	20480 kilobytes
Maximum security log size	102400 kilobytes
Maximum system log size	40960 kilobytes

Common Servers OU Policy

Common Servers OU Policy > Windows Settings > Security Settings > Local Policies > Security Options

Policy	Computer Setting
Rename administrator account	674287

The renamed local administrator account is different from workstations' one.

Common Servers OU Policy > Windows Settings > Security Settings > Restricted Groups

In restricted groups configuration screen the local administrator account is replaced by the account name defined above.

User settings portion of this policy is disabled for faster processing.

Notebooks OU Policy

Notebooks OU Policy > Windows Settings > Security Settings > System Services

Notebook users need Internet access outside the office. Therefore, the telephony service must automatically start up.

Service Name	Startup	Permission
Telephony	Automatic	Configured

User settings portion of this policy is disabled for faster processing.

Information Technology Users OU Policy

Several desktop restrictions are set up in default domain policy. However, Information Technology Users must not get these restrictions due support tasks.

To avoid the policy heritance from default domain policy, the block inheritance option is set for this OU, denying any user configurations from default domain policy. This OU holds only user objects, thus it will not block computer settings from default domain policy, because information technology computers are joined to other OUs.

The only policies set in this OU are:

Information Technology Users OU Policy > Administrative Templates > System > Disable Autoplay

Policy	Setting
Disable Autoplay	Enabled

Information Technology Users OU Policy > Administrative Templates > Control Panel > Display

Policy	Setting
Hide Screen Saver tab	Enabled
Activate screen saver	Enabled
Screen saver executable name	Enabled
Password protect the screen saver	Enabled
Screen Saver timeout	5 minutes

Network Administrators OU Policy

This OU holds users members of the domain admins group. Workstations used by these users need more restricted settings, limiting network and interactive logons to administrators.

Network Administrators OU Policy > Windows Settings > Security Settings > Local Policies > User Rights Assignment

Policy	Computer Setting
Access this computer from the network	Administrators
Log on locally	Administrators

User settings portion of group policy is disabled for faster processing.

Other Relevant Security Issues

Besides the settings described above, there are other few security issues that must be present to achieve the desired security level.

- Physical Security
  All computers have a BIOS administrator password. This password is restricted to IT staff, forbidding unauthorized BIOS configuration changes. Also, a boot restriction of floppy and CD-ROM is configured. Otherwise, an attacker with physical access to the computer can use a boot disk to snoopy and copy local files without any access restriction.

- Antivirus
  Antivirus software is installed on all GIAC's desktops and file servers. SMTP and Proxy antivirus modules are also installed on main ISA and Exchange servers to forbid malicious programs from being downloaded via Web or E-mail.

- Personal Firewall
  All notebooks have a personal firewall installed and configured to protect GIAC mobile computers from being attacked when connected directly to Internet. Actually third-party software is being used until these machines are migrated to Windows XP that has a built-in firewall feature.

- EFS (Encrypted File System)
  All notebook users are trained and instructed to use encryption into their local files, preventing information leakage in case of theft.

Conclusion

Unfortunately, it's not possible to describe here every required countermeasure in order to protect an organization. Information security is a huge and complex subject.

Lots of aspects were not discussed like: disaster recovery, backups, user awareness, sanitization of used media, router security, DDoS protection, application and database security, content control, change management, monitoring, etc.

However, an important issue that must be taken into account is maintenance. It's worthless to deploy all protections without a well-defined maintenance and auditing process.

GIAC's IT staff must be aware of new vulnerabilities and possibly impacts after changes into its production environment.

To accomplish this, GIAC Enterprises hired a third-party company to perform periodically auditing and penetration testing inside its network. These auditing results will help IT staff to assure that the environment adhere with the security standards previously defined.

References

- MCSE Training Kit – Designing Microsoft Windows 2000 Network Security, Microsoft Press, 2001.
- Windows 2000 Server Resource Kit Supplement 1, Microsoft Press, 2001.
- Hacking Exposed Second Edition, McGraw Hill, 2000.
- Hacking Exposed Windows 2000, McGraw Hill, 2001.
- Securing Windows NT/2000 Servers for the Internet, O'Really, Stefan Norberg, 2001.

Last Updated: October 17th, 2017

Upcoming Training

San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Univ. of California - SEC505: Securing Windows and PowerShell Automation	**Los Angeles, CA**	**Jan 29, 2018 - Feb 03, 2018**	**vLive**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**