Global Information Assurance Certification Paper

Windows 2000 Security Plan

for

GIAC ENTERPRISES

J. Coleson

This document is presented in partial fulfillment of the requirements for the GCWN Certification offered by the SANS Institute and satisfies the v3.1 practical assignment.

Table of Contents

Abstract:
An overview of the network security design for a homogeneous Windows 2000 network spanning two sites is given. The overview describes, on a high level, elements of the network topology, Active Directory design, Group Policy objects, IPSec implementation, and certain registry modifications. The network topology is demonstrated to be key to supporting solid security policies through Active Directory.

1 GIAC Enterprises Overview

GIAC Enterprises is a single-focused, start-up company that is well financed and poised to grow quickly in the years ahead. It has quickly become the industry leader in the burgeoning internet-ready appliance software market with its first offering, “Toaster Tattoos.” The “Toaster Tattoos” product line of interchangeable toast templates and associated software for internet-ready toasters represent the best of breed technology in this market, the standard against which all other internet-ready appliance software has already begun to be judged.

GIAC Enterprises is located in a large, metropolitan area in the southwestern United States. Its two campuses are divided along functional lines. The first is relatively small and functions as the corporate headquarters, housing not only the corporate office suites, but the Human Resources and Finance departments as well. The second site serves as the home for the operational side of the company. It houses the Sales and Marketing department and the crown jewel of GIAC Enterprises, the department of Research, Development, and Technical Support. GIAC Enterprises realizes that continuing improvement of their existing product line and cutting edge research and development of new, state-of-the-art products is its life’s blood. The development network is therefore given special attention with regard to security, attention both in terms of Windows 2000 Security Policy and network structure. The overall network structure is built to protect the development network with support of Windows 2000 Group Policy.

The two GIAC Enterprises sites have been designed to function as a single network. This is an important point to GIAC Enterprises because it enhances interdepartmental communication and fosters unity among all employees. Both of these sites are new and, as such, had no existing infrastructure on which to build. For these reasons and others a homogeneous Windows 2000 deployment, where all servers and workstations are within a single domain, has been chosen for both sites. A carefully designed network topology, coupled with all the features of Active Directory and Group Policy, allows GIAC Enterprises to attain the high level of security and functionality it needs at minimal cost and effort.

Since GIAC Enterprises expects to grow in size as well as market share in the near future, the network infrastructure has been designed, and hardware chosen, to support the expected growth. Router, switch, and general network throughput, server and workstation memory size and processing speed have all been chosen with this in mind. Relevant hardware specifics will be discussed briefly in a later section. Similarly, redundancy, high-availability, and failover of network components will, likewise, only be briefly touched upon. This document focuses on the aspects of network design and operating system configuration that enhance the security of the Windows 2000 deployment.

2 Infrastructure

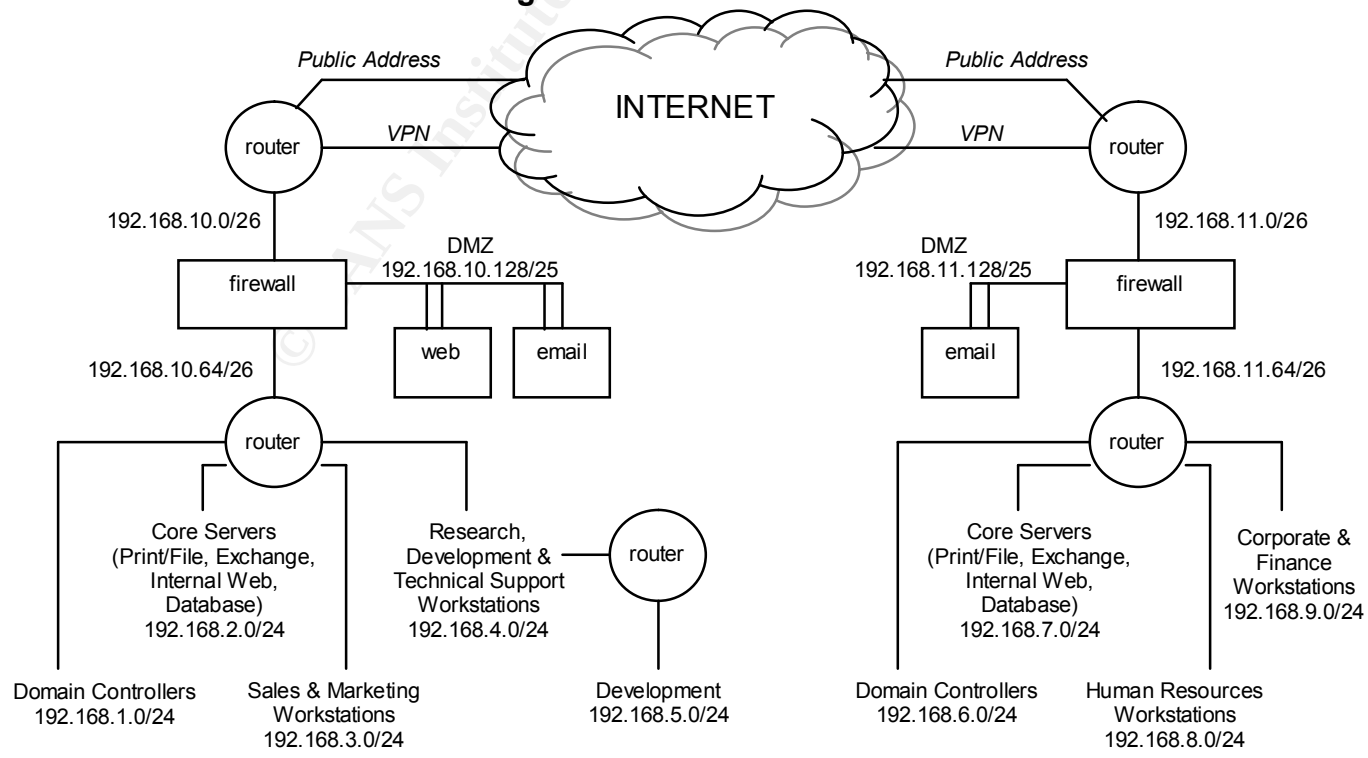
2.1 Network Design

The internal network of GIAC Enterprises has been designed with the following three equally important design objectives.

1) Facilitate an easy-to-use and efficient processing environment for all employees. Thus, GIAC Enterprises has adopted a VPN between sites and a private address space to create a single virtual network.
2) Support near-term expansion of the network due to company growth. This design goal influenced the sizing of the network infrastructure.
3) Support a defense-in-depth approach to securing proprietary information assets and company-owned computing hardware. This necessitates not only a sound network security approach, but also sufficient site physical security. A DMZ, protected by router ACLs and firewall ACLs and proxies implements this design objective.

Both physical sites have been designed with the same general structure. This structure provides a basic "DMZ"-type approach to the perimeter security. An internet-connected front router is directly connected to a firewall controlling three interfaces. The first and third of these interfaces connect to the front router and internal router, respectively. The second interface serves as the gateway into the DMZ, a small subnet containing servers providing internet services. The front routers both have two external interfaces. One provides general internet access; the other is dedicated to a VPN that connects the two sites. [See figure 2.1.]

Fig. 2.1 Network Architecture



2.2 Hardware and Base Software

Each server machine, except the database servers, is equipped with 4 CPUs and dual 36.4 Gb hard drives for plenty of memory and processing power. The Sales and Marketing database server has additional RAID associated with it to accommodate the expected growth in client and contact lists and information. Each server is loaded with Windows 2000 Advanced Server (for the multiple CPU support) with Windows 2000 Advanced Server Service Pack 3. At the time of this writing, Service Pack 3 brings the Windows 2000 Advanced Server installation up to date with Microsoft recommendations. This includes Internet Information Services (IIS) 5.0 and Internet Explorer (IE) 6.0. To distribute mail within the back end networks, Exchange 2000 Server with Service Pack 3 is run. External mail traffic, incoming or outgoing, will be processed through an email gateway in the DMZ. This server will be running the SMTP Virtual Server as part of Exchange 2000 Enterprise Server with Service Pack 2. All hard drives are formatted as NTFS drives.

The external web server and the email gateways are equipped with two 36.4 Gb and one 18 Gb hard drive. The operating system is installed on the 18 Gb drive. One of the 36 Gb drives is used for the application (IIS or Exchange 2000 Enterprise Server) and the remaining 36 Gb drive is used for event logs.

All workstations will be running Windows 2000 Professional with Windows 2000 Professional Service Pack 3.

2.3 Traffic Patterns

The network has been designed to take full advantage of router and firewall capabilities with regard to security. Router ACLs and firewall ACLs and proxies are fully exploited to route traffic only along authorized paths. The front interfaces of the routers allow only 3 types of traffic into the internal network.

1) Web traffic from non-GIAC Enterprises addresses (only the operational site);
2) Email traffic from non-GIAC Enterprises addresses (both sites);
3) Any traffic from GIAC Enterprises addresses.

All web traffic (HTTP – 80/TCP or HTTPS – 443/TCP) directed to the operational site's public address, originating from a non-GIAC Enterprises address, is routed from the front router, through the web proxy on the firewall, and is directed to the web server in the DMZ. (External web traffic directed to the corporate site's public address is simply dropped.) Email traffic (SMTP – 25/TCP) to either site's public address that originates from a non-GIAC Enterprises address is routed through the SMTP proxy on the firewall and also routed into the DMZ, to the email gateway. The internal Exchange server periodically pulls the incoming email from and pushes the outgoing email to the email gateway if the mail is coming from or going to a non-GIAC Enterprises address. This also allows all incoming email to be scanned for viruses before it is allowed into the internal

network. All other traffic, arriving at the external public address and originating from a non-GIAC Enterprises address, is simply dropped. The only exception to this is any traffic required by the company's ISP that is destined for the router itself, such as routing protocols. These are allowed *to* the router, but not *through* the router.

All traffic completely contained within the GIAC Enterprises private address space is either routed locally or tunneled through the VPN to the other site. All such internal GIAC Enterprises traffic is routed through the firewall and directly to the back end router. Since the end point of the VPN is the front router, the firewall provides protection from unauthorized services within the internal network.

As discussed in the next section, the Active Directory design places the entire GIAC Enterprises directory tree into a single domain. For this reason, the domain controllers must replicate through the firewalls and across the VPN. To minimize the number of firewall ports that are opened and help secure the domain controller to domain controller traffic, the use of IPSec transport mode for this traffic has been adopted. This causes no problems because network address translation (NAT) is not applied to the interfaces forming the endpoints of the VPN.

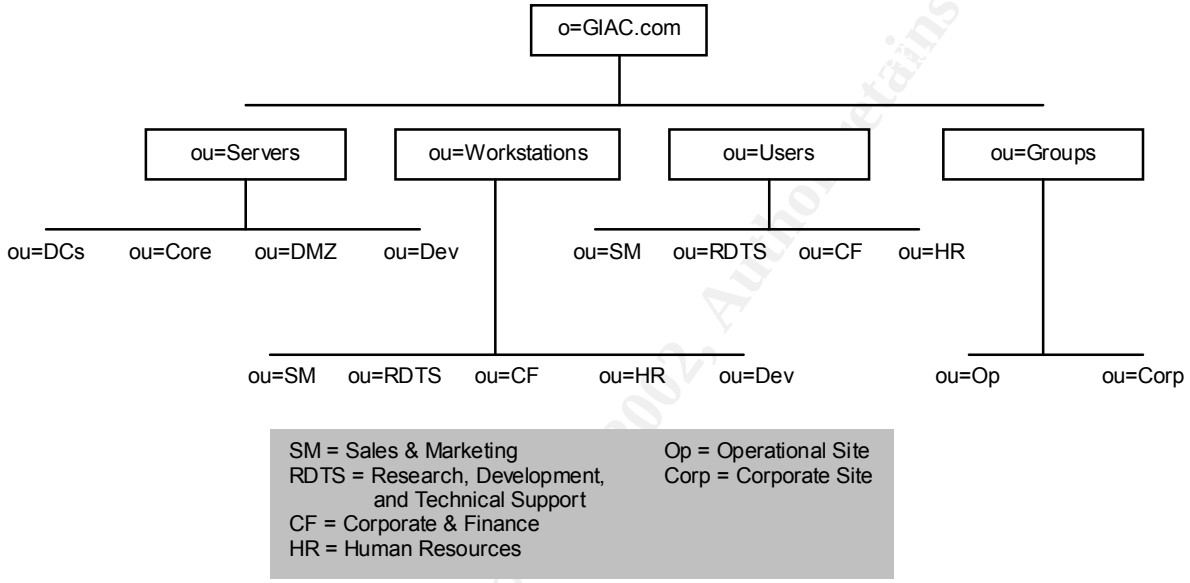
The access control list (ACL) on the development router only allows traffic between the development network and the Research, Development, and Technical Support network or the operational site's domain controllers. All other traffic is denied. No file or print sharing is allowed from this network. Other than this isolation, the development network is wide open. This allows the development engineers to create whatever subnets and development strings are deemed necessary to support the research effort. Development engineers can transfer files to and from the development network and conduct outside communication and day-to-day tasks on their workstations in the RDTS network.

3 Active Directory Design

Active Directory is the centerpiece of a Windows 2000 network. Its structure shapes the Group Policy objects which rely on it and must work hand in hand with the network infrastructure detailed above. GIAC Enterprises has adopted an Active Directory design that puts the entire company within a single domain. The tree structure has as its root, the organization o=GIAC.com. Below this level, the tree structure follows a standard design that is organized along functional lines rather than following the structure of the business organization. Such a structure supports simplified Group Policy objects and their assignment higher in the tree. This structure also helps to make ongoing maintenance of the tree and the Group Policy objects simpler. [See figure 3.1.]

The first level of organizational units subdivides the computers by function. This allows Group Policy to be specifically applied to a particular function enterprise wide. The second level provides further subdivision according to functionality and conceptual location within the network. Below this level are containers (not shown in figure 3.1) that allow Group Policy differences according to site location. The ou=Groups container has been created for administrative groups and the like that might become necessary in the future. This container has site-specific sub-containers and also holds enterprise-wide groups.

Fig. 3.1 Active Directory Tree Structure



4 Group Policies

The Group Policy design is one of the focuses of the GIAC Enterprises security effort. The settings provided, particularly the IPSec settings, make the Group Policy objects, not only very powerful, but also highly customizable. GIAC Enterprises has created Group Policy objects that apply to the servers in the core subnet and the servers in the DMZ, as well as the Default Domain Policy and the Default Domain Controller Policy. For each of these policies, the IPSec policies and associated filters are covered in the next section.

4.1 Default Domain Policy

The Default Domain Policy applies to all machines in the domain and includes the following security settings.

Windows Settings
Security Settings
Account Policies

Password Policy

Enforce Password History: 10
Maximum Password Age: 90 days
Minimum Password Age: 3 days
Minimum Password Length: 8
Passwords Must Meet Complexity Requirements: Enable
(Password complexity requires 3 of the 4 character groups.)
Store Passwords Using Reversible Encryption Algorithm: Disable

Good security must often be balanced with functionality and ease of use. Nowhere is this more obvious than with the Password Policy settings. This is the point where users most directly interact with security. For this reason, some of the settings, although within accepted security recommendations, are not set to the maximum value allowed. Password change policy requires the users to change their password only 4 times per year. A password history list of 10 passwords, coupled with a minimum password age of 3 days restricts the users to reusing a password every 30 days, at least.

Account Lockout Policy

Account Lockout Duration: 2 hours
Account Lockout Threshold: 5 (attempts)
Reset Account Lockout Counter After: 2 hours

Five chances to get the password correct should be enough to get a user past typical typing mistakes. If not, finding something else to do for 2 hours or putting in a call to the helpdesk is not too onerous.

Local Policies

Audit Policy

Audit Account Logon Events: Success/Failure
Audit Account Management: Success/Failure
Audit Logon Events: Success/Failure
Audit Object Access: Success/Failure
Audit Policy Change: Success/Failure
Audit Privilege Use: Success/Failure
Audit Process Tracking: None
Audit System Events: Success/Failure

In accordance with good security practice, system auditing is given a high priority. Auditing successful logon events, object access, and directory service access on domain controllers especially will generate a large amount of data. The GIAC Enterprises infrastructure has been sized, across the board, to handle such a load.

Security Options

Additional Restrictions for Anonymous Connections: “No Access

Without Explicit Permissions"
Allow Automatic Administrator Logon: Disable
Allow System to be Shut Down Without Having to Logon: Disable
Audit the Use of Backup and Restore Privilege: Enable
Digitally Sign Client Communication: Always
Digitally Sign Server Communication: Always
Do Not Display Last User Name in Logon Screen: Enable
LAN Manger Authentication Level: "Send NTLMv2 Response Only\Refuse LM & NTLM"
Message Text for Users Attempting to Logon: "This is a GIAC Enterprises computer system and is for the expressed use of GIAC Enterprises employees and for authorized GIAC Enterprises business purposes. All use of this computer system must adhere to GIAC Enterprises computer system policy. Use of this computer system constitutes consent to be monitored and recorded. All unauthorized use is prohibited. GIAC Enterprises reserves the right to seek all legal remedies for unauthorized use. Evidence of suspected illegal use may be given to law enforcement."
Message Title for Users Attempting to Logon: "ATTENTION!"
Number of Previous Logons to Cache: 0
Prevent System Maintenance of Computer Account Password: Disable
Recovery Console: Allow Automatic Administrative Logon: Disable
Rename the Administrator Account: WWallace
Rename the Guest Account: GIACguest
Restrict the CD-ROM Drive Access to Locally Logged On User Only: Enable
Restrict the Floppy Drive Access to Locally Logged On User Only: Enable
Secure the NetLogon Channel: Digitally Encrypt or Sign Secure Channel Data (Always): Not Configured
Secure the NetLogon Channel: Digitally Encrypt Secure Channel Data (When Possible): Enable
Secure the NetLogon Channel: Digitally Sign Secure Channel Data (When Possible): Enable
Smart Card Behavior: Lock Workstation
Strengthen Default Permissions of Global System Objects: Enable
Unsigned Non-Driver Installation Behavior: "Warn But Allow Installation"

"Additional restrictions for anonymous connections" prevents snooping for available usernames and shares on a networked machine. Since this is a new network, the policy to always digitally sign client and server secure channel traffic will not be as restricting as it might first appear. All third party products introduced onto the system will be tested for compatibility with this configuration. There are no legacy NT domain controllers or workstations on the network. With only

Windows 2000 workstations and servers on the network, not allowing LM or NTLM authentication is appropriate.

Event Log
Settings for Event Logs
Maximum Application Log Size: 2097120 Kbytes (2 Gb)
Maximum Security Log Size: 2097120 Kbytes (2 Gb)
Maximum System Log Size: 2097120 Kbytes (2 Gb)
Restrict Guest Access to Application Log: Enable
Restrict Guest Access to Security Log: Enable
Restrict Guest Access to System Log: Enable
Retention Method for Application Log: Manual
Retention Method for Security Log: Manual
Retention Method for System Log: Manual

The maximum log sizes are all set to 2 Gb to hold many days' worth of normal data and to allow plenty of room for logs of abnormal events that tend to consume log space. Also, log file auditing, while being one of the most important tasks of system and security administrators, is one of the tasks that, on a daily basis, tends to be relegated to a low priority. The large file sizes, along with the manual retention method, relieves the administrators of the immediacy of purging log files, thus allowing the logs to be more carefully monitored.

System Services
NTLM Provider: Disable
Internet Connection Sharing: Disable
TCP/IP NetBIOS Helper: Disable
Telnet: Disable

Most services have been left in an "Enable" state only in this default policy. Many of these will be disabled in group policy objects that are applied to specific nodes of the Active Directory tree. Permissions for these services are set to "Full Control" for administrators and system, and to "Read" for authenticated users.

Administrative Templates
Windows Components
Internet Explorer
Disable Install of Internet Explorer Components: Enable
Disable Periodic Check for Internet Explorer Software Updates: Enable
Disable Software Update Shell Notifications on Program Launch: Enable
Windows Installer
Enable User Controls Over Installs: Disable
Enable User to Browse for Source While Elevated: Disable
Enable User to Patch Elevated Products: Disable

One of the goals of this default policy is to put the ability to load software and upgrade products solely in the hands of the administrators. This will ensure workstation and server configurations conform to company policies. The above values are set to meet this goal.

System
Run These Programs at User Logon: Disable
Disable the Run Once List: Enable
Disable the Legacy Run List: enable
Group Policy
Disable Background Refresh of Group Policy: Disable

The first three settings help to prevent unauthorized processes from running on the machine at logon. The last setting will allow Group Policy settings to be updated during a user's active session.

Network
Network and Dial-Up Connections
Prohibit Configuration of Connection Sharing: Enable

This setting removes the Internet Connection Sharing page from the network connection wizard and the sharing tab from the properties dialog box of a LAN connection. This effectively prevents "everyday users" from sharing drives over the network.

Printers
Web-based printing: Disable

This turns off web-based printing.

User Configuration
Windows Settings
IE Maintenance
Security
Authenticode Settings: "Enable Trusted Publisher Lockdown"

The "Enable Trusted Publisher Lockdown" setting helps minimize the possibility of network objects blindly trusting a bad certificate. This forces administrators to manually import trusted certificates through the "Import Current Authenticode Security Information" process.

4.2 Default Domain Controller Policy

This section presents the settings, beyond those in the Default Domain policy, that are applied to domain controllers.

Windows Settings
Security Settings
Local Policies
Security Options
Allow Server Operators to Schedule Tasks: Disable
Event Log
Settings for Event Logs
Maximum Application Log Size: 10485600 Kb (10 Gb)
Maximum Security Log Size: 16776960 Kb (16 Gb)
Maximum System Log Size: 10485600 Kb (10 Gb)
Restricted Groups
Enterprise Administrators: No Members
Schema Administrators: No members

Disabling the "Allow Server Operators to Schedule Tasks" setting limits the ability to schedule domain controller tasks to administrators. Making the event logs much larger for the domain controllers will reduce the possibility of losing log information, naturally, but will also reduce the possibility of a domain controller having processing problems or even going down because a log file is full. By making the Enterprise Administrators and Schema Administrators groups restricted and setting them to "No Members," domain administrators must manually add accounts to these groups. This provides a complete audit trail when tasks requiring such membership are necessary.

4.3 Core Server Policy

This section lists the differences between the Default Domain Policy and the policy applied to the servers in the core networks.

Windows Settings
Security Settings
Local Policies
Security Options
Allow Server Operators to Schedule Tasks: Disable
Administrative Templates
Windows Components
NetMeeting
Disable Remote Desktop Sharing: Enable
Windows Installer
Disable the Windows Installer: Enable
Allow Admin to Install From Terminal Services Session: Disable

These settings help enforce GIAC Enterprises policy that only administrators, logged in locally, can install and configure applications on critical servers. Sharing server desktops remotely is also prohibited by company policy.

4.4 DMZ Server Policy

This policy applies to the external web server and the email gateways.

Windows Settings
Security Settings
Local Policies
System Services
Alerter: Disable
ClipBook: Disable
Computer Browser: Disable
DHCP Client: Disable
Distributed File System: Disable
Distributed Link Tracking Client: Disable
Distributed Link Tracking Server: Disable
Distributed Transaction Coordination: Disable
DNS Client: Disable
Fax Service: Disable
File Replication Services: Disable
Indexing Services: Disable
Internet Connection Sharing: Disable
License Logging Service: Disable
NetMeeting Remote Desktop Sharing: Disable
Network DDE: Disable
Network DDE DSDM: Disable
Print Spooler: Disable
QoS RSVP: Disable
Remote Access Auto Connection Manager: Disable
Remote Access Connection Manager: Disable
Remote Registry Service: Disable
Removable Storage: Disable
Server Service: Disable
Task Scheduler: Disable
Telephony: Disable
Event Log
Settings for Event Logs
Maximum Application Log Size: 10485600 Kb (10 Gb)
Maximum Security Log Size: 16776960 Kb (16 Gb)
Maximum System Log Size: 10485600 Kb (10 Gb)

We disable all services that are not absolutely necessary on the web server or the email server. These servers are the doors from the internet into the internal network. The increased log sizes reflect the need to track all connection attempts on these machines.

5 IPSec Policy

GIAC Enterprises policy dictates strict traffic routing guidelines. This heavily influences the router access control lists, as have already been touched upon, but also influences the IPSec policies. IPSec is used extensively in the GIAC Enterprises network, but mainly for its filtering and authentication capabilities. One notable exception to this is the encryption of domain controller-to-domain controller traffic between the two sites.

5.1 Filters and Filter Actions

IP filter lists, corresponding to the various subnets, have been created for use within the GIAC Enterprises domain. These filter lists and the IP addresses to which they apply are given below. Each one applies to all traffic entering or exiting the given network, or list of networks.

1) GIAC Network (without DCs) –192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, 192.168.5.0/24, 192.168.7.0/24, 192.168.8.0/24, 192.168.9.0/24, 192.168.10.128/25, 192.168.11.128/25
2) Operational DMZ -192.168.10.128/25
3) Corporate DMZ - 192.168.11.128/25
4) Operational Core - 192.168.2.0/24
5) Corporate Core - 192.168.7.0/24
6) Operational DC - 192.168.1.0/24
7) Corporate DC - 192.168.6.0/24
8) Sales & Marketing - 192.168.3.0/24
9) RDTS - 192.168.4.0/24
10) Development - 192.168.5.0/24
11) Corporate Users - 192.168.8.0/24, 192.168.9.0/24
12) All Traffic

There are also four filters that are specific to particular functionalities.

13) External Web Traffic – Traffic to the external web server on TCP ports 80 (HTTP) or 443 (HTTPS).
14) Web Server FTP – Traffic from Sales & Marketing network and the web server over TCP ports 20 and 21 (FTP).
15) Mail Transfer Traffic – Traffic between the email gateways and the back end Exchange 2000 Servers which are configured as POP clients. This filter isolates traffic on TCP port 110 (POP).
16) External Mail Traffic – Traffic to the external email gateways on TCP port 25 (SMTP).

To accompany these filter lists, the following set of filter actions have also been created.

1) Deny – This action blocks all traffic to the machine.
2) Allow – This action allows all traffic to the machine.
3) Require Digital Signatures – This action requires digital signatures on all traffic to and from the machine. This provides a higher level of authentication between the network components. The HMAC hash is negotiated in the order HMAC-SHA1 and then HMAC-MD5.
4) Require Encryption – This action requires 3DES encryption on all traffic to and from the machine and is applied to domain controller to domain controller replication traffic. The ESP confidentiality is set to 3DES and the ESP integrity is negotiated in the order HMAC-SHA1 and then HMAC-MD5. Keys are regenerated after every 100 Mb of data have been passed or every 15 minutes, which ever comes first.

These filters and actions are used to create the IPSec policies used in the GIAC Enterprises domain. The policy rules in each policy are applied from most to least specific. All the IPSec policies are applied to the Active Directory nodes after which they are named.

5.2 Default Domain IPSec Policy

These are the IPSec settings that are applied in the Default Domain Policy.

1) GIAC Network (without DCs) - Require digital signature
2) Corporate DC - Require digital signature
3) Operational DC - Require digital signature
4) All Traffic - Allow

This policy enforces required authentication between all network components in the GIAC Enterprises domain. The authentication method is chosen to be certificates. GIAC Enterprises uses its own certificate authority, located in the core network, to create and distribute certificates to all domain members. The IPSec filter makes this apply to all machines in the GIAC Enterprises network.

5.3 Default Domain Controller Policy

This policy is applied to the domain controllers through the Default Domain Controller Group Policy.

1) GIAC Network (without DCs) - Require digital signature
2) Corporate DC – Require Encryption
3) Operational DC – Require Encryption
4) All Traffic – Deny

These rules force domain controller-to-domain controller traffic to be encrypted. This helps protect this traffic as it travels between sites, over and above the VPN encryption. The traffic will be encrypted as it traverses the firewalls, making the firewall rules much simpler.

5.4 Operational Core Policy

The Operational Core Policy applies to the servers in the core network of the operational site. These servers handle all the day to day server duties within the operational site including internal web services, file and print sharing services, database services for the Sales & Marketing department, and internal mail service.

1) Operational DC - Require digital signature
2) Operational Core - Require digital signature
3) Operational DMZ - Require digital signature
4) Sales & Marketing - Require digital signature
5) RDTS - Require digital signature
6) All Traffic – Deny

These require all traffic with the operational core servers to be from the operational site.

5.5 Operational DMZ Policy

The Operational DMZ Policy defines the boundaries applied to the DMZ traffic at the operational site.

1) Operational DC - Require digital signature
2) Operational Mail Transfer Traffic - Require digital signature
3) Operational External Mail Traffic – Allow
4) External Web Traffic – Allow
5) Web Server FTP - Allow
6) Sales & Marketing - Require digital signature
7) All Traffic – Deny

The only traffic allowed between the DMZ servers at the operational site consists of web and SMTP from the internet, mail transfer (POP) traffic between the mail gateway and the back end Exchange 2000 server, FTP between users in the Sales & Marketing network and the web server, and logon traffic to the domain controllers. The standing GIAC Enterprises policy is to require authentication between all internal network machines.

5.6 Development Network Policy

This policy applies to the development network.

1) Development – Allow
2) RDTS - Require digital signature
3) Operational DC - Require digital signature
4) All Traffic – Deny

The only traffic allowed into the development network is from the RDTS network or from the domain controllers at the operational site.

5.7 Corporate Core Policy

The servers in the corporate core are restricted to communication with only machines within the corporate site network. Strong authentication is required.

1) Corporate DC - Require digital signature
2) Corporate Core - Require digital signature
3) Corporate DMZ - Require digital signature
4) Corporate Users - Require digital signature
5) All Traffic - Deny

5.8 Corporate DMZ Policy

The Corporate DMZ Policy mirrors the Operational DMZ Policy. The differences are derived from the fact that the corporate site does not host an external web server. So, no external web traffic or FTP from an internal network is required.

1) Corporate DC - Require digital signature
2) Corporate Mail Transfer - Require digital signature
3) Corporate External Mail Traffic - Require digital signature
4) All Traffic – Deny

6 Other Security Settings

Aside from Group policy settings, other settings and modifications are necessary in any Windows 2000 environment to increase the level of security. Restricting access to files, folders, and registry entries limits the visibility of these objects and prolongs an intruder's time on the system, giving security personnel a better chance of tracking and catching the intruder. Carefully crafting the registry, still the core of the Windows 2000 operating system, pushes security-specific alterations to the lowest level making them much more difficult to reach during an attack.

6.1 File and Folder Permissions

GIAC Enterprises has adopted the general policy to give "Full Control" to administrators and the system and "Read and Execute" permission to all authenticated users for the entire Windows installation directory *(%windir%*) and all subfolders and files. Some notable additions or modifications to this policy are listed below.

Folder/File	Administrators & System	Authenticated Users
C:\	Full Control	Read and Execute
C:\boot.ini	Full Control	N/A
C:\ntdetect.com	Full Control	N/A

C:\ntldr	Full Control	N/A
C:\ntbootdd.sys	Full Control	N/A
C:\autoexec.bat	Full Control	Read and Execute
C:\config.sys	Full Control	Read and Execute
C:\Program Files	Full Control	Read and Execute
%windir%\config*.*	Full Control	List
%windir%\temp*.*	Full Control	Traverse, Add File, Add Subdir
%userprofile%	Full Control	Change

6.2 Registry Key Settings

In the same vein as the file and folder permissions given above, GIAC Enterprises has given "Full Control" to administrators and the system and only "Read" access to authenticated users for all registry keys with the following exceptions.

HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg
Administrators & System: N/A
Everyone: None

HKLM\System\CurrentControlSet\Control\WMI\Security
Administrators & System: Full Control
Authenticated Users: None

6.3 Registry Modifications

The following registry values have been set to help protect the system against network attacks against the TCP/IP stack and IP networking functions.

The SynAttackProtect registry key reduces the number of SYN-ACK retries and requires a completed TCP handshake before route cache entries are made.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: SynAttackProtect
Type: REG_DWORD
Value: 2

This registry key disables RFC-1256 compliant route discovery by an interface.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[Interface Name]
Value Name: PerformRouterDiscovery
Type: REG_DWORD
Value: 0

The registry key value below disables the acceptance of source-routed packets.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DisableIPSourceRouting
Type: REG_DWORD
Value: 2

Reducing the “keep alive” time will allow the stack to free up idle TCP sessions more quickly.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: KeepAliveTime
Type: REG_DWORD
Value: 300000

The EnableICMPRedirect key determines whether the server will accept modifications to its route table through an ICMP redirect packet. Hackers could use this functionality to send spackets to a spoofed address.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnableICMPRedirect
Type: REG_DWORD
Value: 0

The next two registry values alter default Windows 2000 behavior. Providing the machine name over the network gives hackers one less piece of valuable information that they must gather. Since the GIAC Enterprises infrastructure is new and uniformly Windows 2000, backward compatibility is not an issue. Therefore, the “8.3” filename convention is unnecessary.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: NoNameReleaseOnDemand
Type: REG_DWORD
Value: 1

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Filesystem
Value Name: NTFSDisable8dot3NameCreation
Type: REG_DWORD
Value: 1

6.4 DMZ Web Server

The Sales & Marketing Department of GIAC Enterprises relies heavily upon the public presence provided by the external web server in the DMZ of the

operational site. Although not very complex or artistically striking, this web site provides critical contact information and a first line of product support to potential and established customers alike. This sections documents the steps taken to harden the web server.

GIAC Enterprises policy dictates that web pages and web-based services be thoroughly tested on the internal web server before being placed on the external server. Therefore, Internet Information Server sample and help files are not needed on the external web server. Removal, on the other hand, will prevent hackers from exploiting known security holes in some of the sample scripts. Also, all support for the Remote Data Service (RDS) has been completely removed. The following files have been deleted.

1) \Inetpub\iissamples\
2) \Program Files\Common Files\System\msdac\Samples\
3) %systemroot%\help\iishelp\
4) %systemroot%\system32\Inetsrv\iisadmpwd\
5) %systemroot%\web\printers\
6) \printers (virtual folder)
7) \MSADC (virtual folder)

All the scripts in the folder \Inetpub\AdminScripts (listed below) have been copied to %systemroot%\system32\ and then deleted from their default location. Furthermore, in their new location, these scripts have been assigned only the permissions “Full Control” for administrators and the system.

1) adsutil
2) chaccess
3) contftp
4) contsrv
5) contweb
6) dispnode
7) disptree
8) findweb
9) mkw3site
10) mkwebdir
11) pauseftp
12) pausesrv
13) pauseweb
14) startftp
15) startsrv
16) startweb
17) stopftp
18) stopsrv
19) stopweb
20) synciwam

The following executable files, found in the %systemroot%\system32\ folder, have been moved from the web server and placed on a CD-ROM for administrative use only.

1) ARP.EXE
2) AT.EXE
3) ATTRIB.EXE
4) CACLS.EXE
5) CLIPSRV.EXE
6) CMD.EXE
7) COMMAND.COM
8) CSCRIPT.EXE
9) DEBUG.EXE
10) EDIT.EXE
11) EDLIN.EXE
12) FINGER.EXE
13) FTP.EXE
14) HYPERTRM.EXE
15) IPCONFIG.EXE
16) MSIEXEC.EXE
17) NBTSTAT.EXE
18) NET.EXE
19) NET1.EXE
20) NETSH.EXE

21) NETSTAT.EXE
22) NSLOOKUP.EXE
23) OS2.EXE
24) OS2SS.EXE
25) OS2SRV.EXE
26) PING.EXE
27) POSIX.EXE
28) RCP.EXE
29) REGEDT.EXE
30) REGINI.EXE
31) REGSVR32.EXE
32) REXEC.EXE
33) ROUTE.EXE
34) RSH.EXE
35) RUNAS.EXE
36) RUNONCE.EXE
37) SYSEDIT.EXE
38) SYSKEY.EXE
39) TELNET.EXE
40) TFTP.EXE
41) TRACERT.EXE
42) TSKILL.EXE
43) WSCRIPT.EXE
44) XCOPY.EXE

Permissions on the following dynamic link libraries have been changed to “Deny” for everyone.

1) %systemroot%\system32\psxdll.dll
2) %systemroot%\system32\psxss.dll

In order to further the removal of the OS/2 and Posix subsystems and the removal of support for RDS, the following registry keys have been modified.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Session Manager\SubSystem\
Value: The “Optional”, “Posix”, and “Os2” values have been removed.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Session Manager\Environment\
Value: The “Os2LibPath” value has been removed.

Hive: HKEY_LOCAL_MACHINE
Key: \SOFTWARE\Microsoft\OS/2 Subsystem for NT\
Value: All subkeys under this key have been removed.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADLaunch\
Value: This key has been deleted.

The permissions on these files have been set as follows.

Folder/File	Administrators & System	Authenticated Users
%systemroot%\system32\os2\	N/A	Everyone=”Deny”
\Program Files\Common Files\System\msdac	Full Control	N/A

These permissions complete the removal of the OS\2 and Posix subsystems and support for RDS.

Several TCP/IP parameters have set to further harden the stack against attacks. One of the main focuses of these setting is the protection from SYN flood attacks. The first two settings determine when the SynAttackProtect protection set with the SynAttackProtect key above starts.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: TcpMaxHalfOpen
Type: REG_DWORD
Value: 300-0xffff

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: TcpMaxHalfOpenRetried
Type: REG_DWORD
Value: 200-0xffff

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DisableDynamicUpdate
Type: REG_DWORD
Value: 1

This last value disables dynamic updates to a DDNS server.

One of the most important techniques used to secure an Internet Information Server is to disassociate all filename extensions with ISAPI processors except those authorized for use in the web server. GIAC Enterprises' web site, while being very informative, is kept very simple. By policy, static web pages are used as much as possible and only the small, necessary set of filename extensions listed below are allowed except with special authorization.

- .htm
- .html
- .asp
- .txt
- .jpg
- .jpeg
- .gif
- .pdf
- .bmp

The .htm extension is mapped to the ASP.DLL. This helps hide the fact that active server pages are being used. The .html extension is used for static pages. The external web server is bound to the IP address 192.168.10.130. This interface is used for all external traffic. The IP address 192.168.10.140 is configured on a second interface for communication to the back end. The folder \WebSrvs\home.giac.net has been created on a separate hard disk from the one on which Windows is loaded. Under this folder, four subfolders have also been

created and serve as the working directories for the web server applications. These directories are given below.

- \root
- \scr
- \exec
- \images

This directory structure serves as the web server home. Files with extensions .htm, .html,.txt, and .pdf are stored in the root directory and its subdirectories. The .asp files are stored in the scr directory. Image files, .jpg, .jpeg,.gif, and .bmp files, are stored in the images directory. The exec directory holds .exe and .dll files when they are authorized for use. The NTFS file permissions for these folders is given below.

\root	System: Full Control Administrators: Full Control Operators: Full Control Authors: Modify Browsers: Read
\scr	System: Full Control Administrators: Full Control Operators: Full Control Authors: Modify Browsers: Read
\exec	System: Full Control Administrators: Full Control Operators: Full Control Authors: Modify Browsers: Traverse Folder / Execute Files
\images	System: Full Control Administrators: Full Control Operators: Full Control Authors: Modify Browsers: Read

The web server permissions are also set to the minimum that will maintain functionality. All permissions are set to “No” with the following exceptions.

\root	Read: Yes Log: Yes Execute: None
\scr	Log: Yes Execute: Scripts Only
\exec	Log: Yes Execute: Scripts and Executables
\images	Execute: None

Hackers often use various HTTP commands ("verbs") to launch attacks against websites. Limiting the type and number of verbs the ASAPI extensions will accept restricts the tools potential hackers could use in this manner. The verbs DELETE, PUT, COPY, LOCK, MOVE, HEAD, and OPTIONS are disabled for all extensions where it is applicable.

Lastly, the "UseHostName" metabase value has been disabled to prevent static, non-ASP pages making the true IP address of the server (even behind a NAT'ed router) available to a client browser. This value controls the display of the "Content-Location" field in the HTTP response header.

6.5 External Email Gateway

GIAC Enterprises realizes that providing a communication channel between its employees and the internet community is vital in today's world. Furthermore, this channel provides a valuable link between its Sales & Marketing department and potential customers and its RDTS department and existing customers. The importance of the email gateway necessitates security similar to the external web server. Many of the same steps have been taken for both.

The External Email Gateway is created using an installation of Exchange 2000 Enterprise Server SP 2. The installation is put on its own 36 Gb disk drive. To administer the Exchange server, an administrative group named "ExAdmins" has been created. The installation directory is set with the following NTFS file permissions.

System: Full Control
Creator / Owner: Full Control
Domain Admins: Full Control
ExAdmins: Full Control
Everyone: None

The following executable files, found in the %systemroot%\system32\ folder, have been moved from the email gateway and placed on a CD-ROM for administrative use only.

1) ARP.EXE
2) AT.EXE
3) ATTRIB.EXE
4) CACLS.EXE
5) CLIPSRV.EXE
6) CMD.EXE
7) COMMAND.COM
8) CSCRIPT.EXE
9) DEBUG.EXE
10) EDIT.EXE
11) EDLIN.EXE
12) FINGER.EXE
13) FTP.EXE
14) HYPERTRM.EXE
15) IPCONFIG.EXE
16) MSIEXEC.EXE
17) NBTSTAT.EXE
18) NET.EXE
19) NET1.EXE
20) NETSH.EXE

21) NETSTAT.EXE
22) NSLOOKUP.EXE
23) OS2.EXE
24) OS2SS.EXE
25) OS2SRV.EXE
26) PING.EXE
27) POSIX.EXE
28) RCP.EXE
29) REGEDT.EXE
30) REGINI.EXE
31) REGSVR32.EXE
32) REXEC.EXE
33) ROUTE.EXE
34) RSH.EXE
35) RUNAS.EXE
36) RUNONCE.EXE
37) SYSEDIT.EXE
38) SYSKEY.EXE
39) TELNET.EXE
40) TFTP.EXE
41) TRACERT.EXE
42) TSKILL.EXE
43) WSCRIPT.EXE
44) XCOPY.EXE

Permissions on the following dynamic link libraries have been changed to “Deny” for everyone.

1) %systemroot%\system32\psxdll.ll
2) %systemroot%\system32\psxss.ll

In order to further the removal of the OS/2 and Posix subsystems, the following registry keys have been modified.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Session Manager\SubSystem\
Value: The “Optional”, “Posix”, and “Os2” values have been removed.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Session Manager\Environment\
Value: The “Os2LibPath” value has been removed.

Hive: HKEY_LOCAL_MACHINE
Key: \SOFTWARE\Microsoft\OS/2 Subsystem for NT\
Value: All subkeys under this key have been removed.

The permissions on these files have been set as follows.

Folder/File	Administrators & System	Authenticated Users
%systemroot%\system32\os2\	N/A	Everyone=”Deny”

These permissions complete the removal of the OS\2 and Posix subsystems

Several TCP/IP parameters have set to further harden the stack against attacks. One of the main focuses of these setting is the protection from SYN flood attacks. The first two settings determine when the SynAttackProtect protection starts.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: TcpMaxHalfOpen
Type: REG_DWORD
Value: 300-0xffff

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: TcpMaxHalfOpenRetried
Type: REG_DWORD
Value: 200-0xffff

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DisableDynamicUpdate
Type: REG_DWORD
Value: 1

This last value disables dynamic updates to a DDNS server.

The Exchange server is bound to the IP addresses 192.168.10.135 for external connections and 192.168.10.145 for mail transfer to the internal network of the operational site or 192.168.11.135 for external mail traffic and 192.168.11.145 for mail transfer to the internal network of the corporate site. Each site's external Exchange 2000 Server is configured with the SMTP Virtual Server for all external email exchange. The internal mail server is configured as a POP client of the external server at each site. Concerning the external gateway, a few configuration settings can greatly increase the security. These are listed below.

Restricting the massage size prevents large messages from filling up disk space. With the attachments that are common today, a message limit larger than the default value of 4096 Kb is necessary. GIAC Enterprises policy allows a maximum message size of 8192 Kb (8 Mb). This value has been set through the Messages tab in the SMTP Virtual Server Properties page.

Several default behaviors of modern email servers can provide sensitive information to potential attackers. Some of these can be disabled through the Advanced tab under the Global Settings / Internet Message Formats / Default object.

- Allow Out of Office Responses
- Allow Automatic Replies
- Allow Automatic Forward
- Allow Delivery Reports
- Allow Non-Delivery Reports
- Preserve Sender's Display name on Message

These settings have been disabled on the external email servers.

Logging has been configured to be in the "W3C Extended Log File Format," a space-delimited, ASCII text format. The log data includes the properties that are listed below.

- Date
- Time
- Client IP Address
- User Name
- Method
- Bytes Received

Finally, the SMTP banner on initial TCP connection response has been changed to restrict server name and version from being sent to a potential attacker. The configurable part of the banner notice has been changed to "GIAC Enterprises Email Server." The default banner would indicate the fact that the gateway is using "Microsoft ESMTP Mail Service."

References

The following books and articles have supplied the background information used in this paper.

1) Olsen, Gary L. Windows 2000 Active Directory Design & Deployment. New Riders Publishing, 2001.
2) Moskowitz, Jeremy. Windows 2000 Group Policy, Profiles, and IntelliMirror. Alameda, CA: Sybex, 2001.
3) Shawgo, Jeff, ed. Windows 2000 Security Step by Step. Version 1.5. The SANS Institue, 2001.
4) Haney, Julie. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. Version 1.1.1. Ft. Meade, MD: National Security Agency, 2002.
5) Walker, William E. Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0. Version 1.3.1. Ft. Meade, MD: National Security Agency, 2002.
6) Pitsenbarger, Trent. Guide to the Secure Configuration and Administration of Microsoft Exchange 2000. Version 1.11. Ft. Meade, MD: National Security Agency, 2002.
7) Riley, Steve. "Active Directory Replication over Firewalls." Microsoft TechNet White Paper, 2001.
8) "Microsoft Exchange 2000 Server Front-end and Back-end Topology." Microsoft Technical Resources White Paper, 2002.
9) "How to Enable IPSec Traffic Through a Firewall." Microsoft Knowledge Base Article – Q233256, 1999.
10) "Client-to-Domain Controller and Domain Controller-to-Domain Controller IPSec Support." Microsoft Knowledge Base Article – Q254949, 2000.

Last Updated: July 24th, 2017

Upcoming Training

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