Secure Server Policies and Procedures for Novell NetWare Compliance

Servers are never 100 percent secure, especially straight out of the box. Certain steps need to be taken to ensure servers are made as secure as possible before placing them into production. There are five basic areas of security which need to be considered when securing servers. These areas include: 1. Physical Security 2. Server and Operating System Security 3. End User Access 4. Monitoring 5. Maintenance This paper outlines these areas and provides generalized policy guidelines to be used when security any server, r...

Secure Server Policies

and

Procedures for Novell NetWare Compliance

GSEC Certification Practical
Version 1.4b
By Dale Daugherty
September 26, 2003

Table of Contents

Abstract

Servers are never 100 percent secure, especially straight out of the box. Certain steps need to be taken to ensure servers are made as secure as possible before placing them into production. There are five basic areas of security which need to be considered when securing servers. These areas include:

1. Physical Security
2. Server and Operating System Security
3. End User Access
4. Monitoring
5. Maintenance

This paper outlines these areas and provides generalized policy guidelines to be used when security any server, regardless of the operating system. From these generalized policy guidelines, procedures specific to the Novell NetWare 6 operating system have been created and should be applied when securing a NetWare server running in a Windows environment. While these procedures are geared towards securing a server running NetWare 6, many of the steps may also apply to NetWare 4.x and 5.x operating systems.

Secure Server Policies

Physical Security

Establishing physical security is the first essential step in securing a server. Even if a server has been logically hardened to prevent unauthorized access or activity, if the server is located in a coat closet in the lobby, the server is not secure. Some placement planning must be taken into consideration before a system administrator can even begin to restrict logical access to the server. The information below describes the steps to take to ensure a server is physically secure.

- Place the server in a secure room with limited access to authorized individuals.
  - If the server cannot be placed in a secure room, it should be placed in a locking closet or cabinet with access limited to authorized individuals.
  - If a locking closet or cabinet is not available, a less preferred option is to secure the console to a stationary object using a cable and removing the mouse and keyboard.
  - A power on password should be set in the BIOS in all circumstances.
- Ensure there is adequate environmental protection over the server regardless of the location. Environmental protection includes:
  - Protection from extreme temperatures
  - Protection from water damage
  - Protection from smoke or dust
  - Protection from fire
    - A chemical retardant which would not damage computer hardware should be utilized. This can either be an automatic system or a hand held fire extinguisher.
- Establish a disaster recovery plan to address the loss of the server.
  - This plan should be tested annually.
  - If access to the server is considered imperative to operations, a redundant server should be considered.
- Protect the server from unauthorized reboot.
  - Configure the server BIOS to ensure the computer boots from the hard drive only and not from a floppy disk or CD ROM.
- Place the monitor so the information displayed cannot be seen from areas adjacent to the server. This may include facing monitors away from windows and doors.
- Do not allow modems to be connected to servers unless they are required for server functionality. If they are required, ensure they are turned off or disabled when not in use.

<u>Uninterruptible Power Supply</u>

To ensure NetWare servers continue to provide the functionality they were designed for, each server should be connected to an Uninterruptible Power Supply (UPS) which can supply power to the server for a minimum of one hour. This should allow the system

administrator ample time to save the information on the server and shut it down before power is completely lost.

These are the first steps to securing network server. The next step is to ensure the network operating system is secure.

Operating System Security

Securing the server operating system is one of the most essential tasks in protecting the data that resides on the server. This task begins with the installation of the operating system and continues with limiting unnecessary services or applications from being installed on the server as well as securing the services or applications that are required for server functionality. Recommendations for securing servers are listed below, beginning with the logical location of the server.

Logical Location

The logical location of a server means placing the server behind a firewall or series of firewalls depending on the access requirements of the server and the information that resides on the server.

When placing a server behind a firewall, the theory of "Defense-in-Depth" should be followed. In a network following the theory of defense-in-depth, a server containing confidential customer information would be placed under several layers of logical security whereas a web server would be placed closer to the top of the logical security layer. However, servers should not be connected to the Internet unless they have been placed in a DMZ.

Installation

The next step in securing a server is to ensure the operating system is properly installed. Upgrading to the most recent version of the operating system should be done where applicable as vulnerabilities discovered in earlier versions of the operating system generally will have been eliminated.

When installing or upgrading server operating systems, it is essential to ensure that only one operating system is installed on the server. Multi-boot systems should not be used as this creates added vulnerabilities to the server.

In connection with multi-boot systems, each server should also only be used for one dedicated and single-purpose function. This involves only installing services or products that are required for the server to perform its dedicated function. Running extra services or products on a server also creates additional vulnerabilities and adds to the security concerns.

Console Security

Steps also need to be taken to secure a server console regardless of the logical location of the server. One of the security provisions that should be implemented is to disable access to the console after ten minutes of inactivity. This can be done using a screen saver password or other similar security feature. Disabling access to the console should include restricting unauthorized individuals from viewing information on the monitor as well as entering commands.

The console should remain disabled until a valid user ID and password combination have been entered. When possible, the user ID and password combination should be different from the ID's and passwords used by users to log into server accounts. This is especially important for the Admin or system administrator accounts.

As an added security provision, a login or authorization banner should be displayed when a user attempts to log into a server. This banner should state that the use of the server is for authorized individual only and that unauthorized access may result in criminal prosecution.

Remote Access

Another control that needs to be implemented is remote access to the server. Securing remote access to a server is essential in protecting the data residing on servers as well as protecting against unauthorized access to the network. Some of the security provisions that should be implemented on any remote access connection include:

1. Requiring a strong password consisting of 8 upper and lower case alphanumeric characters.
2. Changing the password at least every 90 days or more often if it is believed the password has been compromised or if the information on the server is sensitive.
3. Encrypting the strong password with a minimum of 128 bit encryption.
4. Automatically terminating a remote session after ten minutes of inactivity.
5. Re-locking the terminal after the remote session has been terminated.

Remote access to network servers should only be provided to a limited number of individuals who have demonstrated a need to have this access. The more remote access capabilities allowed, the greater the risk of the server being compromised.

Secure Services

In addition to securing remote access to servers, system administrators need to make sure that all services and applications on the server are properly secured. When installing services or products, a good rule of thumb to follow is deselect, then re-install. Following this method, all default services will be de-selected during installation if the option is available and re-installed after installation if the service is necessary for the functionality of the server. Even after de-selecting services, many unnecessary

services may still be installed. The system administrator should review all services that may have been installed and delete or disable any that are not required for the functions of the server.

To provide an added level of security, all services or products that are installed should be installed in a separate partition on the hard drive.

Secure Ports

In connection with securing services running on a server, all unnecessary ports should be disabled or filtered. Ports should only be opened on a server if they are required for the functions of that server or services running on that server. All unnecessary ports should be closed, even if a firewall is being utilized to secure the network.

After all ports have been closed or filtered, a port scan should be performed on the server to ensure only necessary ports are open. A tool such as NMap[1] can be used to perform this function. If after performing a port scan on the server it is discovered that unnecessary ports are still open, a further review of the services and ports should be conducted.

Virus Protection

Computer viruses are becoming more and more prevalent and the potential for damage to servers is immeasurable. It is imperative that each server has virus scanning software installed and actively running and that the software be updated with new anti-virus DAT files as soon as they are available. For added protection, a complete scan of the server hard drives should be performed at least weekly.

There are several vendors to choose from when selecting anti-virus software and each perform basic scanning functions. However, the application that is chosen should meet the following minimum criteria:

- Update anti-virus definitions automatically or alert the administrator if new definitions are available.
- Send an immediate virus notification to the administrator if the server has become infected.
- Scan both incoming and outgoing files.
- Scan various files types, including .EXE, .DLL, .ZIP, NLM, etc.
- Quarantine infected items.

All of these features should be enabled on the anti-virus software that is chosen. If a product is selected for these features but they are not enabled, the product is not performing the tasks for which it was purchased.

[1] NMap Security Scanner. http://www.insecure.org/nmap/

End Use Security

One of the main functions of servers is to provide end users with access to files, folders, objects, and other information or services which reside on a central server. As with restricting unnecessary services and ports, users should be restricted from accessing information on the server that is not required for their job duties. A good rule of thumb to follow in this instance is deny first, then allow, meaning all access is denied first and only allowed once a user has demonstrated a need for that access.

An end users access to files, folders, and other information maintained on a server depends on the rights that end user has been assigned. Unauthorized individuals could gain access to confidential information if access restrictions are not placed on end user accounts. To secure against unauthorized use of end user accounts, certain security provisions need to be implemented. When imposing end user security restrictions, special considerations may need to be taken into account depending on the environment in which the server is installed. At a minimum, system administrators should ensure they have implemented the security provisions discussed in the following pages.

To assist in setting up user accounts, these minimum security provisions should be incorporated into a user or group template that can be applied to all new end user accounts. Utilizing a template to set up new end user accounts will not only assist the system administrator in setting up new users, it will also ensure all end user accounts are set up with minimal security provisions.

Account Restrictions

Account restrictions should be enable to limit the possibilities of unauthorized individuals gaining access to server information using know account information. Some of the restrictions that should be followed are:

- Assign each end user a unique account.
- Limit each end user to one active session on the network.
- Impose time constraints for user accounts which should never be used to access the server during specified times.
- Require each user account to authentication to a particular network by setting network address restriction.
- Immediately delete user accounts for individuals no longer needing the account.
- Verify terminated employee listings to user accounts quarterly to ensure there are no accounts open for terminated employees.
- If it is necessary to set up a temporary account, set it to expire on a specific date.
- Disable and remove Anonymous and Guest accounts.
    - When removing any account, be aware of object inheritances.
    - If these accounts cannot be deleted or disabled, they should at least be protected using a strong password consisting of 18 upper and lower case

alphanumeric characters and symbols. This will be discussed in more detail in the Password Restriction section.

While many of these restrictions can only be enforce through strict compliance with corporate policy, computerized tools should be utilized to enforce compliance where available.

Password Restrictions

Passwords are the first line of defense when it comes to securing access to computer systems. Because of this, it is important that users utilize strong passwords to protect against unauthorized access to their account. When enforcing password restrictions, the following guidelines should be included the following.

- Passwords should have a minimum length requirement.
  - 8 upper and lower case alphanumeric characters and symbols for end users.
  - 18 upper and lower case alphanumeric characters and symbols for admin accounts.
- Passwords should be changed at least every 90 days.
  - If the information is considered critical or sensitive, the password should be changed more frequently.
- A grace log period of 3 days should be implemented for passwords that have expired.
- Unique passwords should be required with a history of passwords maintained for 8 regular changes.
- Do not allow anonymous or blank passwords.

Again, these restrictions should be enforced through strict compliance with corporate policy as well as computerized tools where available.

Intruder Detection

Even with implementing account and password restrictions, additional security provisions need to be taken to detect attempts to gain unauthorized access to end user accounts. Computer tools or applications should be implemented which will lock a user account for a minimum of 12 hours if an incorrect user ID and password combination has been entered 3 times within a 30 minute time period. Logs of locked accounts should be maintained and reviewed daily for suspicious activity.

Securing Admin

Securing the Admin account is essential to protecting a server as this account has the most elevated privileges and is the account most likely to be target by attackers. While the admin account should never be characterized as an end user account, the security provisions for end user accounts should also be applied to admin accounts. In addition, special provisions also need to be taken when securing the Admin account. Theses

provisions, outline below, are in addition to the basic end user security provisions discussed above.

- First, create an account with rights equivalent to the Admin account. Name the account using the same naming convention used for all users.
- Assign the new Admin equivalent account to the system administrator and move it to a container separate from general users. This new account should be used for the system administrator's day-to-day activities.
    - Ensure the rights of the new account only provide the system administrators with the access needed to perform their job duties, nothing more.
    - Do not allow the system administrators to perform their day-to-day tasks using the Admin account.
- Create a strong password of 18 upper and lower case alphanumeric characters and symbols for the Admin account.
- Rename the Admin account to something similar to that used within the working environment.
- Hide the re-named Admin account and place it in a container that will not be used by others and that cannot to be easily identified with the Admin account.
- Use the re-named Admin account only when absolutely necessary.
- Limit the number of individuals who know the Admin password to 4 individuals.
- Maintain a listing of individuals with access rights similar to Admin.
- Create a separate, bogus Admin account with no rights or privileges. Audit this account to determine if someone is trying to gain unauthorized Admin access.
    - This may be good for information gather but is not necessarily required.

Object and Property Security

Object and property rights should also be restricted when possible. Object rights provide users access to a particular object on the server tree. Property rights give trustees access to properties of a particular object on the server tree. Implementing object and property rights can provide even greater security by only allowing trustees to view or modify certain object and properties. Rights should be applied to provide the least amount of access necessary.

File System Security

Limiting access to files is an essential piece to securing information maintained on servers. In a networked environment, user access to files should be based on minimums, meaning individuals should be provided the minimum file access level necessary for that individual to perform their assigned duties. System administrators need to evaluate each individuals needs for file access rights and limit those rights on a need-to-know basis.

Inherited Rights

When securing user access rights, it is also important to be aware of the various inherited rights that may be associated with individual files, folder, or objects. In network trees, many times individuals are provided access to areas on the server and through inherited rights, are granted access to areas which may contain confidential information. Again, individuals should only be provided access to the areas of the server that are necessary for that individual to perform the necessary functions.

Generic Accounts

In addition to securing user accounts created by the system administrator, it is important to be aware of the rights that are assigned to generic accounts that may be set up in connection with other services on the server. Several accounts, including Powerchute, Antivirus, Backup, Printer, User Template, Mail, Post, etc. may require access to the network to perform various functions. These accounts may have or may require Admin equivalent access rights and may be installed with a default or no password. These accounts, like the Admin account, should be protected using a strong password consisting of 18 upper and lower case alphanumeric characters and symbols and the password should be changed immediately after installation and regularly there after. For added security with these special network accounts, network address restrictions should also be used when possible.

Additional Security Provisions

Listed below are some additional security provisions which should be followed when securing network servers. This list may not be all inclusive but should be followed to provide added security over network servers.

- Disable users who have not logged in for at least 90 days.
- Prevent or limit tree browsing capabilities
- Remove [Public]'s browse rights to the [Root] of the tree.
- Ensure a login script exist for each user but do not allow unauthorized individuals to access login scripts.
- Dismount any volumes that are not used or that are rarely used.

Monitoring

Even after implementing the security provisions discussed above, it is important to monitor the servers for unauthorized activity to ensure the server is maintained in a secure manner. Monitoring servers involves utilizing various tools or utilities to audit for unauthorized activity or attempts to perform unauthorized functions on a server.

Regardless of the method of monitoring or auditing, audit reports should be generated and reviewed daily for any security related events, which may include:

- Unsuccessful attempts to access the Console
- Unsuccessful attempts to access the "Admin" account
- Successful attempts at accessing the "Admin" account
    - This account should only be used on a limited basis to perform specific tasks on the servers. Any activity performed using the "Admin" account should be monitored.
- Unsuccessful attempts to access user accounts (i.e. password guessing).
- Attempts to gain elevated privileges or access to unauthorized accounts.
- Modifications made to software, applications, and systems.
- Modifications made to server configurations.
- Modifications made to account settings.
- Creation of new volumes.

All logs should contain the date, time, IP addresses, user, and a description of the event and should be reviewed daily by someone independent of the system administration function. Logs should be saved to a file, folder, or container which can only be accessed by the individual(s) responsible for reviewing these logs. Saving log information to an insecure or unrestricted location would allow an attacker to easily delete or modify the logs to ensure their activity can not be detected. In addition to storing the audit logs in a secure location, log information should be backed up and maintained in paper or electronic form for at least seven years.

Trustee Assignments

In addition to reviewing logs, system administrators should review trustee assignments quarterly to ensure no hidden objects have been created on the server and to ensure the rights of authorized accounts have not been elevated.

When reviewing trustee assignment, the system administrator should also consider any inherited rights of individual accounts. If individuals have a business need to access a specific object outside their home directory, it is important to understand that this individual will also have access to all objects and information under that object unless otherwise restricted. If the access rights noticed are not required for a particular user account, the rights should be removed or restricted.

Security Equivalences

Security equivalences are a method by which similar rights to objects can be assigned to different accounts or objects. Setting security equivalences can create major security holes as individuals may have access to objects and information that they do not need. In addition, an attacker may use this technique to gain advanced privileges on the server. To help alleviate this problem, security equivalences should also be reviewed quarterly if available. Any security equivalences should be removed and individual security rights should be assigned.

Third Parties

Third parties are often called upon to perform specialized functions or to provide software for specific purposes. Third party access to servers should be closely scrutinized and monitored. The system administrator should observe the activity of third parties and monitor logs during and after the third party has completed their task to verify the work was done within pre-defined parameters.

Third party products should be installed and run on a test server prior to being placed into production. This will allow the system administrator the opportunity to learn exactly what functions the application is performing. In learning the application, the system administrator will be able to verify that the application is only performing the designated tasks as well as determine what constitutes normal activity and what activity should be reported to a central security log.

To help system administrators with their monitoring procedures, third party applications should be kept to a minimum and should be installed in separate objects, volumes, or drives on the network servers. User rights to the location in which applications are installed should be "execute" only and individual should not have rights to copy, delete, rename, etc, any of the files associated with the products.

In addition to third party applications, third party personnel should only be granted access to servers after the server administrator has given them explicit written permission. Each third party should be assigned a unique user ID which should be set to expire within a specified time period. The rights third party personnel are assigned to network volumes and objects should be strictly limited to the information that is necessary for them to perform their function. Allowing third parties unnecessary access to the server could result in a compromise of the server and the information on that server.

Maintenance

In addition to monitoring servers for unauthorized activity, a certain activity which must be performed by often gets overlooked is the maintenance of a server and the information maintained on that server. Performing regular maintenance will ensure the server continues operating in a secure manner and that the information residing on the server will not be compromised. Some of the basic maintenance tasks which should be performed are discussed below.

Patching and Updating

New vulnerabilities in operating systems are discovered every day. To make sure a server is not susceptible to new vulnerabilities, individuals should review news bulletins, company web sites, and other security resources frequently (daily for critical servers) for security updates or advisories. System administrators should monitor resources for the following types of maintenance information:

- Patches
- Updates
- Hot fixes
- Driver versions
- BIOS versions

As with any program that is loaded on a server, all patches, driver versions, BIOS versions, etc. should be tested on a test machine before being applied to the production server.

To help alleviate some of the overhead with patching activities, an automated patch management system should be utilized to ensure all servers are up-to-date. While this is not a necessity, it may alleviate some of the daily tasks that system administrators have to perform.

Backup and Recovery

One of the daily tasks a system administrator must perform is the backup of the server. The steps for backing up a server should be documented for each individual server and backups should include the system registry, configurations, and data residing on the server. Backups should be stored in a secure location while on-site and should be transferred to an off-site location as soon as possible after the backup has been completed. A schedule should be devised for rotating backup media on and off-site to ensure the media is not overused and to ensure the most recent information is not stored on site with the server. In addition, local laws should be reviewed to determine if a retention schedule is required for the information that is backed up.

Backup media should be tested monthly to ensure the process and backup media are functioning as prescribed. Tests should be conducted by restoring one or more files from the backup media onto a test server. All tests of backup media should be document indicating the date the restore was attempted, the label on the backup media, the information that was restored on the media, and if the restore was successful. When testing backup media, it is not necessary to conduct a full restore of a system. Simply restoring a file, folder, or other information should provide enough evidence that the backup procedures and media are functioning as necessary.

Novell NetWare 6 Security Procedures

The Procedures section of this paper provides specific steps which should be followed when implementing the Secure Server Policies on a NetWare 6 server. When implementing policy requirements, it is important to remember that there may not be specific steps to correspond with each policy guideline as some of the guidelines are general in nature and do not require action specific to NetWare 6 servers.

Physical Security

All physical security provisions outlined in the Policies section of this paper should be implemented as describe. However, when choosing a UPS to support a NetWare 6 server, it is recommended that the UPS provide NLM management support. With NLM support, the server can be shut down automatically without human intervention if power is not restored within the designated time frame of one hour.

Operating System Security

Installation

Upgrading to the most recent version of NetWare is the first step in securing a NetWare server. Vulnerabilities that were reported in earlier versions of NetWare have been addressed and corrected in the most current version of the operating system. While it may not always be feasible to upgrade all servers to the most current version of the operating system, it is recommended that this be done where possible.

NetWare, unlike many other operating systems, provides the system administrator the option to install certain services on the server. However, there are certain steps that need to be taken to ensure unnecessary services are not installed. These steps are listed below.

- Select *Custom* installation when upgrading or creating a new NetWare server. With NetWare 6, performing an Express install will install Native File Access, iManage, and Novell Advance Audit Services by default. Some of these services may not be necessary for the purposed of the server.
- When prompted to select the services that should be installed, all services should be de-selected.
- If other services are necessary for the functionality of the server, they can be selected at this time but it is recommended that services be installed after the installation has been completed. While Novell NetWare does not install as many unnecessary default services as other operating systems, the system administrator needs to remember that some services may install components that are not necessary for the purposes of the server. These extra services can create additional vulnerabilities that need to be protected against.

When installing NetWare servers, they should also be converted from an IPX to a TCP/IP based environment. The IPX protocol should only be selected if there are currently servers or services running which require the use of this protocol. Any servers or services which require the use of IPX should be converted to TCP/IP as soon as possible.

After the installation has been completed, the following communication parameters should be enabled. These parameters can be enabled by entering the corresponding commands at the command prompt. In addition, these commands should also be added to the AUTOEXEC.NCF file located in the SYS:\SYSTEM directory to ensure the parameters are set every time the server is rebooted. (A sample AUTOEXEC.NCF file is illustrated in the Appendix with the added sections highlighted.)

SET IPX NetBIOS Replication Option = 0 (If running IPX)
SET FILTER PACKETS WITH IP HEADER OPTION = ON
SET FILTER SUBNET BROADCAST PACKETS = ON
SET DISCARD OVERSIZED UDP PACKETS = ON
SET DISCARD OVERSIZED PING PACKETS = ON
SET TCP DEFEND SYN ATTACKS = ON
SET ALLOW UNENCRYPTED PASSWORDS = OFF
SET AUTOMATICALLY REPAIR BAD VOLUMES = ON

Some of these commands may not yield a response from the server as the service may not have been installed or a message may be displayed stating that the setting has already been established. However, these commands should still be entered as indicated to ensure the settings have been established.

Console Security

The server console of a server running NetWare 6 can be secured with a screen saver by entering the following command at the command prompt and in the AUTOEXEC.NCF file;

SCRSAVER ENABLE

This feature can be set with many different variables but the default settings for this command provide the security necessary by locking the console after ten minutes of inactivity. In addition, the “enable” screen will clear after one minute of inactivity.

Please note that the SCRSAVER ENABLE command can only be used with NetWare 5 and 6. In NetWare 4, this feature can be enabled by using the MONITOR.NLM utility.

Another NetWare 6 utility that should be enabled is the Secure Console utility. Secure Console prevents any modules from being loaded if they are not located in SYS:/SYSTEM or C:\NWSERVER, prevents keyboard entry into the system debugger,

and prevents unauthorized individuals from making changes to the server date and time. To enable this feature, type the following command at the command prompt:

SECURE CONSOLE

Because this command places such restrictions on the server, it may cause problems with the installation and use of various services or products. Therefore, this command should only be entered after all required services and products have been installed and again after every re-boot.

In order to ensure the security of the console, logging should be enabled to track any attempts of unauthorized activity. To enable console logging in NetWare, the following command should be entered at the command prompt;

LOAD CONLOG ARCHIVE=YES NEXT=05:00 ENTIRE=YES MAXIMUM=10000

The LOAD CONLOG command is included in the AUTOEXEC.NCF file by default. However, the parameters listed above have not been set. The default command line should be replaced with the command line above. (Again, a sample of the AUTOEXEC.NCF file is illustrated in the Appendix with these changes.)

The logs generated from the SECURE CONSOLE utility will be saved to CONSOLE.LOG under the SYS:\ETC directory. These logs should be reviewed daily. Reviewing logs will be covered in more detail in the Monitoring section.

Remote Access

When using NetWare, it is imperative that RCONSOL and RCONSOLJ not be used for remote access to the server unless there are no other options available. These services transmit information in clear text, allowing attackers to easily view passwords and other confidential information. Third party applications which provide encryption and secure communications should be used for remote access connects to NetWare servers.

To prevent remote access using these utilities, enter the following command in the AUTOEXEC.NCF file:

REMOTE LOCK OUT

If it is necessary to use RCONSOL or RCONSOLJ, the following procedures should be followed to at least encrypt the remote access password;

- Install the latest version of RCONSOLE or RCONSOLJ
- Type the following commands at the command prompt.

- Note: Some of these services may not be loaded but these commands should still be entered to ensure they are unloaded before encrypting the remote password.

UNLOAD RSPX.NLM
UNLOAD RS232.NLM
UNLOAD REMOTE.NLM
LOAD REMOTE –NP
REMOTE ENCRYPT

- Enter a password when prompted and select "Y" when asked to write the command to the SYS:SYSTEM\LDREMOTE.NCF file. Then type;

UNLOAD REMOTE.NLM
SYS:SYSTEM\LDREMOTE.NCF

- If using RCONSOL or RCONSOLJ, these last two commands should also be entered in the AUTOEXEC.NCF file to ensure the remote encryption service is started when the server is rebooted.

Secure Services

Some of the more common services that are installed on NetWare servers are listed below along with procedures to follow for securing these services. The procedures may include disabling, uninstalling, or taking other measure to secure the service. This is only a small listing of services which may be installed on a custom install of NetWare. System Administrators should perform a thorough investigation of any other services or products that will be installed to determine if additional security measures need to be taken.

- Perl
  - The Perl program is installed by default but is generally not necessary for the functions of a server. If the service is not needed, the Perl.nlm file should be deleted from the SYS:SYSTEM directory. Alternatively, the system administrator could enter the following command at the command prompt;

UNLOAD PERL

- FTP
  - Ensure the server is running the most recent version of FTP.
  - Anonymous FTP access should be disabled on all NetWare servers. To unload this service, type the following command at the command prompt;

UNLOAD NWFTPD

- LDAP (Lightweight Directory Access Protocol)
  - If any applications are running this service, it should be upgraded to the most current version, currently version 3.
- Internetworking Configuration (INETCFG)
  - This service should only be used when necessary. To unload the service, type the following command at the command prompt;

UNLOAD INETCFG

- Netbasic.nlm
  - Netbasic is a scripting language and is installed be default. The Netbasic.nlm file as well as the Netbasic folder should be removed from the SYS:\SYSTEM directory.
- Rconag6
  - This service could allow an attacker to gain access to the console by entering the rconj.exe command. While the service is installed by default, it is not loaded. To ensure the server is not compromise using this server, the encrypted version should be loaded. To load the encrypted version of Rconag6, follow these procedures:
    - At the command prompt, enter;

UNLOAD RCONAG6
LOAD RCONAG6 ENCRYPT

    - Proceed through the choices and ACCEPT the file LDRCONAG.NCF.
    - Search the AUTOEXEC.NCF file for #LOAD RCONAG6.NLM PASSWORD 2034 16800 and replace it with LDRCONAG.NCF.

- NLIST.NLM
  - NLIST can be used to obtain user account information. This service which is loaded in the SYS:PUBLIC directory, should be renamed to prevent unauthorized individuals from gaining user account information. While this service can also be deleted, it may be utilized by the system administrator in checking user compliance with policy.

In addition to securing these services, all incoming remote connections to FTP, e-mail, or web servers should be filtered by designated IP where available. Use the FILTCFG command to filter the IP's that will be connecting remotely to the server. Using the FILTCFG command will be discussed later in this paper.

Port Security

The system administrator should evaluate the purposes of a particular NetWare server and determine the ports that must be open to run the services on that server. For a

basic file and print sharing server, only port 524 should be open. All other ports should be closed or filtered.

To close any unnecessary ports, the service running on those ports should be unloaded and the ports should be filtered. Unnecessary ports can be filtered by enabling Packet Forwarding Filters in the TCP/IP Filter Configuration. Follow these procedures to enable this feature;

- Enable TCP/IP filtering support by typing INETCFG at the command prompt.
- Select PROTOCOLS from the Internetworking Configuration menu.
- Select TCP/IP.
- Press enter when TCP/IP Status is highlighted and select ENABLED.
- Escape back to the Internetworking Configuration window.
- Select REINITIALIZE SYSTEM.
- Press Alt+Esc to get back to the Internetworking Configuration window.
- Press Esc and exit INETCFG.
- Type FILTCFG at the command prompt.
- Select CONFIGURE TCP/IP FILTERS then PACKET FORWARDING FILTERS.
- Ensure the status is enabled and modify the filters and exceptions to meet the needs of the server.

To check for open ports using NetWare utilities, follow these procedures;

- Type TCPCON at the command prompt
- Select PROTOCOL INFORMATION
- Select TCP
- Press the Enter key when TCP CONNECTIONS is highlighted.

If all unnecessary ports have not been closed, the filtering process should be re-visited.

NCP Security

One communication parameter specific to NetWare is the use of NCP or NetWare Control Protocol. NCP is the means by which basic network functions are performed on a Novell network. To protect communications across a network, Novell has established the NCP packet signature feature for use in a NetWare environment. With NCP packet signatures, the server and client must sign each packet with a different signature before authorization can be granted. This process prevents packet forgery and restricts individuals from posing as a more privileged user.

While the use of NCP packet signatures appears to be an ideal way to secure network communications, there are certain conditions under which NCP packets can be falsified. In order to prevent and detect NCP exploits, the following procedures should be followed.

- Using ConsoleOne, select the properties of SECURE.NCF file located in the SYS:SYSTEM.
- Remove the Read only check box and click Apply.
- Open the SECURE.NCF file using NetWare editor.
- Remove the "#" sign before the follow commands;

SET NCP PACKET SIGNATURE OPTION = 3
SET CHECK EQUIVALENT TO ME = ON
SET ADDITIONAL SECURITY CHECKS = ON

- Add the following lines to the file;

SET DISPLAY NCP BAD LENGTHS WARNINGS = ON
SET DISPLAY NCP BAD COMPONENET WARNINGS = ON

- Add the SECURE.NCF command to the AUTOEXEC.NCF file

Alternatively, these SET parameters as well as the ones included in the SECURE.NCF file can be added to the AUTOEXEC.NCF as illustrated in the same file in the Appendix.

Setting these parameters on Novell NetWare servers will provide increased security over the server and communication across the network. Setting these parameters will also ensure the server is C2 Redbook compliant.

Virus Protection

There are several vendors that provide basic anti-virus scanning and updating features and no particular one is recommended in this paper. However, when choosing a specific vendor or product for a NetWare server, system administrators should ensure the application is NLM based and is capable of scanning NetWare system files. A listing of certified Novell compatible virus protection applications can be found at http://www.novell.com/partnerguide/software.html#100001.

End User Security

End user access rights to a NetWare 6 server can be defined using the freely available ConsoleOne utility. ConsoleOne should be used to enforce the policy requirements outlined below.

User Templates

To set user templates using ConsoleOne, right click on the container in which the template will be stored, selecting NEW and then OBJECT. Select TEMPLATE from the class list and select OK and name the template. Once a template has been created, the security provisions discussed below can be applied with greater ease.

Account Restrictions

To set Login Restrictions;

- Right click on the object or user account to be secure and select PROPERTIES.
- Click on the RESTRICTIONS tab and select LOGIN RESTRICTIONS.
- Check the LIMIT CONCURRENT CONNECTIONS check box and set the maximum connections to 1.

To set Time Restrictions;

- Right click on the object or user account to be secured and select PROPERTIES.
- Click on the RESTRICTIONS tab and select TIME RESTRICTIONS.
- Select the time blocks when users should not have access to the server.

To set network address restrictions;

- Right click on the object or user account to be secure and select PROPERTIES.
- Click on the RESTRICTIONS tab and click on the ADD button.
- Select the NETADDRESS TYPE from the drop down box and enter the appropriate information. (Note: This feature may not be feasible in all situations.)

To set temporary accounts;

- Right click on the object or user account to be secure and select PROPERTIES.
- Click on the RESTRICTIONS tab and select LOGIN RESTRICTIONS.
- Check the ACCOUNT HAS EXPIRATION DATE check box and enter the date the account is to expire.

Password Restrictions

To ensure users abide by strong password policies, set password restrictions by right clicking on the object or user account to be restricted and selecting PROPERTIES. Click on the RESTRICTIONS tab and select PASSWORD RESTRICTIONS. Select the following check boxes and enter the corresponding restrictions:

- Select the REQUIRE A PASSWORD box.
  - Set the minimum password length of 3.
- Force periodic password changes.
  - Days between forced changes = 90 (Unless the sensitivity of the information requires the days to be fewer than 90).
  - Do not change the DATE AND TIME PASSWORD EXPIRES field. The default settings will require a password change when the user logs on.
  - Require unique passwords
  - Limit grace logins
    - Grace logins allowed = 3
    - Remaining grace logins = 3

Intruder Detection

Intruder Detection is the utility used in NetWare to detect unauthorized access attempts. To set Intruder Detection in NetWare 6, open ConsoleOne and right click on the container in which the user accounts will be created and select PROPERTIES. Click on the GENERAL tab and select INTRUDER DETECTION. Mark the DETECT INTRUDERS check box and change the incorrect login attempts to 3. Then mark the LOCK ACCOUNT AFTER DETECTION check box and modify the settings to 12 hours.

Securing Admin

ConsoleOne can again be used to administer the majority of policy guidelines on the Admin account. Some of these steps such as setting password restrictions were just covered and should be applied to the Admin account where necessary. For those procedures that were not previously covered, follow the procedures listed below.

To create a user account with rights similar to admin:

- Right click on a newly created administrative user.
- Select TRUSTEES OF THIS OBJECT.
- Assign the NDS rights to match those of the Admin account.

To move the Admin account:

- Right click on the account and select MOVE.
- Select a container in which to place this account. This container should not be one used by others and access should be restricted.

To hide the Admin account:

- Right click on the renamed Admin account.
- Select TRUSTESS OF THIS OBJECT.
- Delete [Public] and [Root].
- Select the renamed Admin account and change the rights to supervisor only.
- Click on the NDS Rights tab and select INHERITED RIGHTS FILTERS.
- Deselect all rights.

Object and Property Security

To ensure proper security over database objects, the following settings and actions should be implemented in a NetWare 6 environment.

- Update Novell Directory Services and eDirectory software.
- Do not allow user accounts to have global access to objects or properties.
- Provide users with the least amount of object and property rights that are necessary for that individual to perform their job duties.
    - Users should not be granted access to objects if they do not have a business need to have them.
- Only allow users Read and File Scan rights to SYS:LOGIN

- Only allow users Create rights to SYS:MAIL
- Only allow users Read and File Scan rights to SYS:PUBLIC
- Never allow users access to the SYS:ETC or SYS:SYSTEM directories.

File security

When setting up user home directories, the directory should be placed on a volume other than SYS and users should not be able to access NCF files within the directory.

In a Novell NetWare environment, end users receive all rights except for Supervisory to their home directory when they are set up. Because of these file access rights granted, users should be limited to accessing their home directory unless it is absolutely necessary that they access directories outside their home directory.

If it is necessary to set a user up with access outside of their home directory, file access rights should be limited to the files and folders necessary for that individual to perform their designated responsibilities.

The table below lists various tasks that users may need to a specific file system and the minimum rights required to perform that task. This table is not all inclusive but should be used as a guide when assigning the minimum user rights to file systems outside of a user's home directory.

Task	Minimum Rights Required
Open and read a file	Read
See a filename	File Scan
Search a directory for files	File Scan
Open and write to an existing file	Write, Create, Erase, Modify
Execute a .EXE file	Read, File Scan
Create and write to a file (but not view it)	Create
Copy files from a directory	Read, File Scan
Copy files to a directory	Write, Create, File Scan
Make a new directory	Create
Delete a file	Erase
Salvage deleted files	Read, File Scan on the files; Create on the directory
Change directory or file attributes	Modify

Rename a file or directory	Modify
Change the IRF	Access Control
Change trustee assignments	Access Control
Modify a directory's disk space assignment for users	Access Control

[2]

Note: Users should not be granted Access Control rights to any directory other than their home directory as Access Control rights are similar to Supervisor rights in some of the functions that the user can perform. In addition, users should never be given rights to the root directory or SYS:SYSTEM. Only the system administrator should have these access rights.

File access rights can be restricted using Novell's ConsoleOne utility for NetWare 6. To review and modify these rights, follow these procedures;

- Right click on the user or object on which file restrictions will be placed.
- Select PROPERTIES.
- Click on the RIGHTS TO FILES AND FOLDERS tab and add, delete, or modify the information as necessary for the designated purposes.

Inherited Rights

The list below illustrates information that has been compiled by The University of Michigan regarding inherited rights on a NetWare server. These rights apply to NetWare versions 4.x and later and should be taken into consideration when creating or deleting accounts.

- The Supervisor right cannot be blocked in the file system.
- Granting the Supervisor right to an NDS or eDirectory Server object automatically grants the Supervisor file system rights to all volumes on that server.
- The Supervisor right to the NDS or eDirectory Server object can be inherited through the Supervisor right to any parent container.
- All Properties rights are inherited whereas Selected Properties rights are not. Therefore, avoid assigning rights through the All Properties option.
- The Write property right effectively gives the trustee the ability to grant anyone, including himself or herself, all rights, including the Supervisor right. Therefore, use caution when assigning the Write property right to the Object Trustees (ACL) property of any object. [3]

[2] Foust, Mark. "NetWare Security: Closing the Doors to Hackers." Novell Copyright 2000. June 7, 2000. URL:http://developer.novell.com/research/appnotes/2000/june/03/a000603.htm.
[3] "Novell NetWare." R1409. Rev 5/99. URL:http://www.umich.edu/~opde/top_tens/novell.html.

Additional Security Provisions

Below are some additional security procedures which should be performed on NetWare 6 servers:

- Disable users who have not logged in for at least 90 days by using the NLIST utility. At a DOS command prompt, type the following command;

NLIST USER WHERE "LAST LOGIN TIME" LT MM/DD/YY
(For MM/DD/YY, enter a date which is the same number of days from the current date as the number of days individuals are required to change their password.)

  - Note: If NLIST has been renamed as recommended in a previous step, the new name must be entered in place of NLIST.
- Limit tree browsing with Inheritance Rights filters by right clicking on the object for which filters will be applied and select TRUSTEES OF THIS OBJECT. Click on the NDS Rights drop down and select INHERITED RIGHTS FILTERS. Add filters as necessary.
- Remove bindery contexts from the servers by removing the "set Bindery Context" line from the AUTOEXEC.NCF file.
- Configure the directory services to perform checks for access control which is not backwards compatible with previous versions of NDS. At the command prompt type;

SET ADDITIONAL SECURITY CHECKS = ON

Monitoring

Auditing NetWare

Several default logs are generated in NetWare which should be reviewed daily. The log names, along with a description of the information contained in the log, are listed in the table below.

Log File	Contents
SYS$LOG.ERR	Found in the \SYSTEM directory, this file contains file server errors and general status information.
CONSOLE.LOG	Found in the \ETC directory, this file maintains a copy of all console screen activity. It is started by the CONSOLE.NLM that is automatically loaded in NetWare 5 AUTOEXEC.NCF file. The file size limit is set to 100KB by default, but you can change this if necessary.
VOL$LOG.ERR	Automatically created and stored at the root of each volume, this file contains little of interest for security except the mounting and dismounting of volumes and VREPAIR operations.

ABEND.LOG	Found in the SYSTEM directory, this file keeps a record of server Abends. Sometimes hackers just want to Abend your server. NetWare 4.x and 5.x offer automated Abend recovery. You can also use third-party tools such as the AlexanderLAN Server Protection Kit to notify the administrator of Abend messages and other alerts. Visit http://support.novell.com/alexanderlan/ for more information.

[4]

In addition to reviewing these log reports, Novell's NAAS (Novell Advanced Audit Services) auditing tool for NetWare6 or other third party tool should be used to ensure compliance with policy guidelines.

If the NAAS tool is chosen to provide additional auditing services, the tool should be set up as recommended by Novell. The steps for setting up this tool are extensive and are beyond the scope of this paper. Information on this tool and steps required for setting it up to audit volumes and containers can be found on Novell's web site at http://www.novell.com/documentation/lg/nw6p/pdfdoc/naas_enu/naas_enu.pdf. System administrator should ensure these documents are thoroughly reviewed before implementing this utility.

A list of possible third party auditing tools which are compatible with NetWare 6 servers can be found on the Novell Partner Product Guide page at http://www.novell.com/partnerguide/software.html#100012.

Trustee Assignments

A tool has been created to assist system administrators in monitoring NetWare servers for hidden objects. The Hidden Object Locator (HOBJLOC) is a free tool offered by Novell and can be downloaded at http://www.novell.com/coolsolutions/tools/1098.html. This tool should be used quarterly to review for any hidden objects. Hidden objects should be thoroughly investigated and deleted if not necessary.

Security Equivalence

Setting end users up with security equivalences was standard practice in earlier versions of NetWare. While the method of assigning end users equivalent security rights is similar to assigning object rights, the utilization of security equivalences should not be performed. Instead of assigning security equivalences, the system administrator should assign similar rights to different objects. This is especially important for the Admin account.

To determine if security equivalents have been used in a NetWare environment, the system administrator should enter the following NLIST (or re-named NLIST) commands at a DOS prompt.

[4] Fischer, Jeff. "Administering Right in ConsoleOne: Part 1." Novell AppNotes. November 2002. URL:http://developer.novell.com/research/sections/netmanage/netnovice/2002/november/n021101.htm.

NLIST USER WHERE 'EQUIVALENT TO ME" EXISTS
SHOW "EQUIVALENT TO ME" /r /s

NLIST SERVER WHERE "EQUIVALNET TO ME" EXISTS
SHOW "EQUIVALENT TO ME" /r /s

NLIST GROUP WHERE "EQUIVALENT TO ME" EXISTS
SHOW "EQUIVALENT TO ME", "MEMBER" /r /s

NLIST "ORGANIZATIONAL ROLE" WHERE "EQUIVALENT TO ME" EXISTS
SHOW "EQUIVALENT TO ME", "OCCUPANT" /r /s

Maintenance

Patching and Updating

Novell maintains a listing of recent patches that should be applied to NetWare 6 servers. This listing can be found at http://support.novell.com/produpdate/patchlist.html. There are also links on this page which can be followed to obtain patches for older NetWare Operating Systems and Novell applications or services.

Backup and Recovery

Novell has created the Storage Management Services or SMS utility to assist the System Administrator in performing backups. SMS is an additional service installed by default on NetWare 6 servers. Much like the NAAS auditing utility, there are third party products that can be used in place of SMS and there are specific steps that must be followed when installing and using SMS. These steps are beyond the scope of this paper. If the SMS product is chosen, the specifics on the utility should be reviewed at (http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/back_enu/data/hjc2z4tu.html) prior to implementation.

A listing of possible third party tools that can be used for backup and recovery of NetWare servers can be found on the Novell Partner Product Guide page at http://www.novell.com/partnerguide/software.html#100003.

When backing up information on Novell NetWare servers, it is important to note that audit flags may not be included with the backup of the server registry and other information. Audit flags must be recorded manually so they can be re-installed if a server needs to be re-built.

Directory Service Utilities

A tool that is specific to maintaining NetWare servers is DSREPAIR. This tool helps system administrators identify various errors with the directory database and services and allows the administrator to take appropriate action to fix these errors. Such

problems may include bad records, schema mismatches, bad server addresses, and external references. DSREPAIR can also perform advanced changes to the NDS schema.[5]

DSREPAIR should be run quarterly to ensure server integrity. Novell recommends only running the "Unattended Full Repair" unless otherwise specified by a Novell technician. To run the unattended full DSREPAIR, enter the following command at the command prompt;

DSREPAIR –U

Or type the following command for more repair options;

DSREPAIR

It is important to ensure this utility is not aborted while it is in processes and, as with any maintenance that is performed on a server, a full backup be performed prior to performing the function.

[5] "DSREPAIR." Novell NetWare 6 Utilities Reference. 103-000153-001. February 2002. URL:http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/utlrfenu/data/hneidcah.html.

Conclusion

Servers are very rarely secure straight out of the box. Securing a server requires ensuring the server is both physically and logically secure and can not be accessed by unauthorized individuals.

With the information outlined in this paper, individuals should be able to establish a base for securing any server regardless of the operating system as well as perform specific procedures to secure a server running the Novell NetWare 6 operating system.

While a server can never be 100 percent secure, following the Secure Server Policies and the Novell NetWare 6 Security Procedures outlined in this paper will help the system administrator sleep a little easier knowing appropriate steps have been taken to provide the utmost security over their servers and the information residing on them.

Appendix A - Sample AUTOEXEC.NCF file

The lines highlighted in this sample AUTOEXEC.NCF file are lines that were added or changed after installation.

```
#SET BINDERY CONTEXT = O=SECURITY-TREE
SET TIME ZONE = MST7MDT
SET DAYLIGHT SAVINGS TIME OFFSET = 1:00:00
SET START OF DAYLIGHT SAVINGS TIME  = (APRIL SUNDAY FIRST  2:00:00 AM)
SET END OF DAYLIGHT SAVINGS TIME = (OCTOBER SUNDAY LAST  2:00:00 AM)

#Additional SET parameters entered after installation.
SET FILTER PACKETS WITH IP HEADER OPTION = ON#
SET FILTER SUBNET BROADCAST PACKETS = ON#
SET DISCARD OVERSIZED UDP PACKETS = ON#
SET DISCARD OVERSIZED PIN PACKETS = ON#
SET TCP DEFEND SYN ATTACKS = ON#
SET ALLOW UNENCRYPTED PASSWORDS = OFF#
SET AUTOMATICALLY REPAIR BAD VOLUMES = ON#

#SET parameters that can be entered individually or included with the SECURE.NCF
#command.  They have been commented out in this example as they will be included in
#the SECURE.NCF command entered below.
#SET IPX NETBIOS REPLICATION OPTION = 0
#SET DISPLAY NCP BAD LENGTHS WARNINGS = ON#
#SET REJECT NCP PACKETS WITH BAD LENGTHS = ON#
#SET DISPLAY NCP BAD COMPONENT WARNINGS = ON#
#SET REJECT NCP PACKETS WITH BAD COMPONENTS = ON#
#SET NCP PACKET SIGNATURE OPTION = 3#
#SET CHECK EQUIVALENT TO ME = ON#

#The SECURE.NCF command entered below replaces the SET parameters
#above that have been commented out.
SECURE.NCF

# Note: The Time zone information mentioned above
# should always precede the SERVER name.
SEARCH ADD SYS:\JAVA\NWGFX
SEARCH ADD SYS:\JAVA\NJCLV2\BIN
# WARNING!!
FILE SERVER NAME XXXXXXX
# WARNING!!
# If you change the name of this server, you must update
# all the licenses that are assigned to this server. Using
# NWAdmin, double-click on a license object and click on
# the Assignments button. If the old name of
```

```
# this server appears, you must delete it and then add the
# new server name. Do this for all license objects.
LOAD CONLOG ARCHIVE=YES NEXT=05:00 ENTIRE=YES MAXIMUM-10000
SEARCH ADD SYS:\JAVA\BIN
; Network driver LOADs and BINDs are initiated via
; INITSYS.NCF. The actual LOAD and BIND commands
; are contained in INITSYS.NCF and NETINFO.CFG.
; These files are in SYS:ETC.
sys:etc\initsys.ncf
#LOAD TCPIP
#LOAD CE1000.LAN SLOT=10009 FRAME=ETHERNET_II  NAME=CE1000_1_EII
#BIND IP CE1000_1_EII addr=172.XXX.XXX.XXX mask=255.XXX.XXX.XXX
gate=172.XXX.XXX.XXX
MOUNT ALL

SYS:\SYSTEM\NMA\NMA5.NCF
BSTART.NCF
load nile.nlm
load httpstk.nlm /SSL /keyfile:"SSL CertificateIP"
LOAD PORTAL.NLM
LOAD NDSIMON.NLM
LOAD NICISDI.XLM s
LOAD SASDFM.XLM
LOAD SAS.NLM
LOAD PKI.NLM
LOAD NLDAP.NLM
UNLOAD REMOTE.NLM
SYS:SYSTEM\LDREMOTE.NCF

# Storage Management Services components required for Backup
SMSSTART.NCF
#Commands added after installation.
SCRSAVER ENABLE
REMOTE LOCK OUT

SEARCH ADD SYS:\TOMCAT\33\BIN
TOMCAT33
#Apache is now the NetWare Web Manager server
SEARCH ADD SYS:\APACHE
NVXADMUP
#RCONAG6.NLM is required by RConsoleJ
LDRCONAG.NCF
UCS.NCF
STARTX
```

Appendix B - Sample SECURE.NCF file

The lines highlighted in this sample SECURE.NCF file are lines that were added or changed after installation.

```
#############################################################
#
# Version: 1.01
# Date:          May 14, 1997
#
# This NetWare script file, SECURE.NCF, is the enhanced
# security options configuration file.  It chooses the
# options that are required to run NetWare in the trusted
# configuration, which is designed to meet the US Class
# C2 security criteria and the European Class F-C2/E2
# security criteria.
#
# Enhanced security options not required for the trusted
# configuration (not required by C2 and European Class
# F-C2/E2 standards) are also included in this file but are
# commented out. More information regarding enhanced
# security options may be found in the Enhanced Security
# Server Administration manual.
#
# The server may be configured to automatically execute
# this configuration file during server boot after the
# execution of AUTOEXEC.NCF.  This can be done by setting
# the set parameter "Enable SECURE.NCF" to ON.  This can
# be done from SERVMAN (Server parameters/Miscellaneous
# menu) or in either AUTOEXEC.NCF or STARTUP.NCF.  This
# configuration file can also be executed from the NetWare
# Console command line.
#
# Each of the SET parameters in this file (SECURE.NCF) can
# be set individually from the NetWare console command line,
# from SERVMAN, or in AUTOEXEC.NCF.
#
# SECURE.NCF may be modified using EDIT.NLM or another
# ASCII editor.  The file is stored in the SYS:/SYSTEM
# directory.
#
# The following commands are required for the trusted
# configuration.  Refer to the Utilities Reference manual
# for more information about each of these commands.
#
# The following command configures the server to disallow
```

```
# the use of unencrypted passwords.  The default value is
# OFF. The trusted configuration value is also OFF.
#
     SET Allow Unencrypted Passwords = OFF
#
# The following command configures the server to disallow
# the use of passwords to identify auditors.  The default
# value is OFF.  The trusted configuration value is also
# OFF.
#
     SET Allow Audit Passwords = OFF
#
# The following command configures the server to
# automatically run VREPAIR when a volume fails to mount.
# The default value is ON. The trusted configuration
# value is also ON.
#
     SET Automatically Repair Bad Volumes = ON
#
# The following command configures the server to reject
# NCP packets that fail boundary checking.  Older client
# utilities may fail if this SET parameter is set to ON.
# The default value is OFF. The trusted configuration
# value is ON.
#
     SET Reject NCP Packets with bad lengths = ON
     SET DISPLAY NCP BAD LENGTHS WARNINGS = ON
#
# The following command configures the server to disallow
# replication of NetBIOS broadcast packets. The default
# value is 2. The trusted configuration value is 0.
#
     SET IPX NetBIOS Replication Option = 0
#
# The following command configures the server to reject
# NCP packets that fail component checking.  Older client
# utilities may fail if this set parameter is set to ON.
# The default value is OFF.  The trusted configuration
# value is ON.
#
     SET Reject NCP Packets with bad components = ON
     SET DISPLAY NCP BAD COMPONENT WARNING = ON
#
# The following command configures NetWare Directory
# Services to perform access control checks which are
# not backwards compatiable with previous versions of
```

```
# NetWare Directory Services.  The default value is OFF.
# The trusted configuration value is ON.
#
    SET Additional Security Checks = ON
#
# The above commands are required for your server to be
# in the trusted configuration, designed to meet the
# Class C2 criteria and the Class F-C2/E2 criteria.
#
############################################################


############################################################
#
# The following commands provide additional enhanced
# security options that are not required to meet the
# Class C2 criteria and the Class F-C2/E2 criteria.
# These have been commented out but may be enabled by
# removing the comment symbol (# ) from the beginning of
# the line.  EDIT.NLM or another ASCII editor may be used
# to edit this file.  For more information about each of
# these commands refer to the Utilities Reference manual.
#
# The following command configures NetWare Directory
# Services to enforce the checking of the Equivalent To
# Me attribute during authentication.  DSREPAIR must be
# used to synchronize the Equivalence attribute and the
# Equivalent To Me attribute if the Check Equivalent to
# Me parameter is set to ON.  Setting this parameter to
# ON will also adversely affect the authentication
# performance.  The default value is OFF. For enhanced
# security the value may be set to ON.
#
    SET Check Equivalent to Me = ON
#
# The following command configures the server to reject
# NCP packets that are not signed and to sign all reply
# packets.  Setting this parameter to 3 will adversely
# affect the communication performance of the server.
# The default value is 1, which signs NCP packets only if
# required by the client.  For enhanced security the
# value may be set to 3.
#
    SET NCP Packet Signature Option = 3
#
# The following command secures the NetWare server
```

```
# console in the following ways: it removes DOS paths
# from the search path; it allows only NLMs from the
# search path to be loaded; it disallows the setting of
# certain SET parameters; it prevents the server date and
# time from being changed; and it prevents keyboard entry
# into the operating system debugger.  This command does NOT
# remove the requirement that the server console be
# physically secured.  By default, SECURE CONSOLE is not
# invoked. For enhanced security SECURE CONSOLE may be
# invoked.
#
#     SECURE CONSOLE
#
# The above commands provide enhanced security options
# that are NOT required for your server to be in the
# trusted configuration -- to meet the Class C2
# criteria and the Class F-C2/E2 criteria.
#
##############################################################
```

Appendix C - Server Security Checklist

NetWare Server Security Checklist		
Indicate Operating System ☐ **NetWare 6.X** ☐ **NetWare 5.X** ☐ **NetWare 4.X**		
Physical Security		
Yes	No	
☐	☐	Is the server located in a room physically secured by combination, biometric, or other locking system? Explain how the room is secure. ☐
☐	☐	Is the server placed in a locking cabinet within the secure area?
☐	☐	Have the keyboard and mouse been removed from the server?
☐	☐	Has a power on password been set in the BIOS?
☐	☐	Are there sufficient environmental controls in the area where the server is maintained? Indicate the controls in place: ☐ Water detection/alarm ☐ Dust detection/alarm ☐ Temperature detection/alarm ☐ Smoke and fire detection/alarm ☐ Fire suppressant. Indicate suppressant type:_____
☐	☐	Has a disaster recovery plan been established and testing scheduled? Indicate testing date:
☐	☐	Has booting from the floppy drive and CD ROM drive been disabled in the BIOS?
☐	☐	Has the monitor been place to limit unauthorized viewing of information?
☐	☐	Are modems connected to this server?
☐	☐	Are modems necessary for the functions of this server?
☐	☐	If modems are connected, are they turned off when not in use?
Yes	No	**UPS**
☐	☐	Is a UPS being utilized to supply backup power to the server?
☐	☐	Is the UPS capable of supplying power to the server for a minimum of one hour?
☐	☐	Does the UPS support the use of NLM management and shutdown?
Securing the Operating System		
Yes	No	**Installation**
☐	☐	Has the server been place behind a firewall and other logical securing following the theory of Defense-in-Depth?

☐	☐	Is NetWare the only operating system installed and running on the server?
☐	☐	Is the server only being used for one dedicated purpose? Indicate what the server is being used for. [ ]
☐	☐	Has the protocol been changed from IPX to TCP/IP?
☐	☐	Were all default services been deselected during installation and services added after installation was complete?
☐	☐	Have the following SET parameters been added to the beginning of the AUTOEXEC.NCF file? ▪ SET IPX NETBIOS REPLICATION OPTION = 0 (If running IPX) ▪ SET FILTER PACKETS WITH IP HEADER OPTION = ON ▪ SET FILTER SUBNET BROADCAST PACKETS = ON ▪ SET DISCARD OVERSIZED UDP PACKETS = ON ▪ SET DISCARD OVERSIZED PING PACKETS = ON ▪ SET TCP DEFEND SYN ATTACKS = ON ▪ SET ALLOW UNENCRYPTED PASSWORDS = OFF ▪ SET AUTOMATICALLY REPAID BAD VOLUMES = ON
Yes	No	**Console Security**
		Indicate measure taken to secure the server console. ☐ Utilize SCRSAVER command ☐ Utilized MONITOR utility ☐ Other methods. Please specify. [ ]
☐	☐	If the SCRSAVER command with the default settings is being utilized, has the SCRSAVER ENABLE command been added to the AUTOEXEC.NCF file?
☐	☐	Has the SECURE CONSOLE command been entered at the command prompt?
☐	☐	Have the necessary changes been made to the LOAD CONLOG command in the AUTOEXEC.NCF file to match the following: ▪ LOAD CONLOG ARCHIVE=YES NEXT=05:00 ENTIRE=YES MAXIMUM=10000
Yes	No	**Remote Access**
☐	☐	Will this server be accessed remotely?
☐	☐	Have remote access accounts been restricted to a limited few number of authorized individuals? Indicate number of individuals: _____
		If this server will be access remotely, indicate the method used to access the server. ☐ RCONSOL ☐ RCONSOLJ

		☐ Third party product. Please specify. ☐
☐	☐	If RCONSOL and RCONSOLEJ are not being utilized, has the ability to use these services been denied by entering the following at the command prompt and adding it to the AUTOEXEC.NCF: ▪ REMOTE LOCK OUT
☐	☐	If RCONSOL or RCONSOLJ must be used, has the password been encrypted and have the following commands been added to the AUTOEXEC.NCF file? ▪ UNLOAD REMOTE.NLM ▪ SYS:SYSTEM\LDREMOTE.NCF
		Secure Services and Ports
		Indicate if the recommended measures have been taken to secure the following default services?

☐	Perl	If this service is not necessary, type UNLOAD PERL at the command prompt and delete
☐	FTP	If this service is necessary, update to the most recent version of the service.
☐	LDAP	If this service is necessary, update to the most recent version of the service.
☐	INETCFG	Unload this service by typing UNLOAD INETCFG at the command prompt.
☐	Netbasic.nlm	Delete the NETBASIC.NLM file from SYS:SYSTEM. Also delete the NETBASIC.NLM
☐	Rconag6	Load the encrypted version of this service by following the steps:
☐	Nlist.nlm	Rename this service or delete it from the SYS:PUBLIC directory

		☐	Nlist.nlm	Rename this service or delete it from the SYS:PUBLIC directory
☐	☐	Have services or products other than the default services and products been installed? List and describe these service: **Service Type** | **Description** |
☐	☐	Are all services installed in a separate partition on the server hard drive?
		Port Security
☐	☐	Have necessary services been properly filter to only allow authorized traffic to and from the server?
☐	☐	Have all unnecessary ports been filtered out using the FILTCFG.NLM utility?
☐	☐	Has a port scan been performed on the server to determine the open ports and if these ports are necessary for the functions of the server. List open ports and corresponding service/need. **Port** | **Service/Need** |
Yes	No	**NCP Security**
☐	☐	Have the followed SET parameters been added to the SECURE.NCF file? ▪ SET DISPLAY BAD LENGTHS WARNINGS = ON ▪ SET DISPLAY NCP BAD COMPONENT WARNINGS = ON ▪ SET NCP PACKET SIGNATURE OPTION = 3 ▪ SET CHECK EQUIVALENT TO ME = ON ▪ SET ADDITIONAL SECURITY CHECKS = ON
☐	☐	Has the SECURE.NCF command been added to the AUTOEXEC.NCF file?
☐	☐	If SECURE.NCF is not being used, have the corresponding commands, in addition to the ones listed below been added to the AUTOEXEC.NCF individually? ▪ SET REJECT NCP PACKETS WITH BAD LENGTHS = ON ▪ SET REJECT NCP PACKETS WITH BAD COMPONENTS = ON
Yes	No	**Virus Protection**
☐	☐	Is an anti-virus product being utilized? Indicate product: |
☐	☐	Does the anti-virus product meet the following criteria:

		☐	Update DAT files automatically or alert of new DAT files.	☐	Send immediate virus notification to the system administrator.
		☐	Scan both incoming and outgoing files.	☐	Scan various types of files; .EXE, .DLL, .ZIP, .NLM, etc.
		☐	Quarantine infected items.		
☐	☐	Is the virus protection software NLM based or otherwise certified to be Novell compliant?			
End User Access					
Yes	No	**User Template**			
☐	☐	Are templates being used to set up re-occurring user accounts?			
Yes	No	**Account Restrictions**			
☐	☐	Are end users assigned one unique account to access the server?			
☐	☐	Is each end user limited to one active session on the network?			
☐	☐	Are time restrictions implemented for those areas which require such restrictions?			
☐	☐	Have network address restrictions been established where feasible?			
☐	☐	Have unused accounts been deleted or disabled?			
☐	☐	Have any temporary accounts been set to expire when the account will no longer be necessary?			
Yes	No	**Password Restrictions**			
☐	☐	Indicate if the following password restrictions have been implemented:			
		☐	Require all accounts to have a password.	☐	Allow users to change their passwords.
		☐	For user accounts, minimum password length of 8 characters.	☐	For Admin account, minimum password length of 18 characters.
		☐	Force password changes at least every 90 days.	☐	Require the user to use unique passwords.
		☐	Allow a maximum of 3 grace logins for changing a user password.	☐	
		Please note any deviations.			
Yes	No	**Intruder Detection**			
☐	☐	Has the Intruder Detection feature been turned on?			
☐	☐	If Intruder Detection has been turned on, indicate the settings for each of the following: ▪ Incorrect login attempts: _____ ▪ Intruder attempt reset interval:			

<table>
<tr><td></td><td></td><td>

Days: _____
Hours: _____
Minutes: _____

Lock account after detection:

Days: _____
Hours: _____
Minutes: _____

</td></tr>
<tr><td>Yes</td><td>No</td><td>Securing Admin</td></tr>
<tr><td>☐</td><td>☐</td><td>Has an account been created with rights equivalent to Admin?</td></tr>
<tr><td>☐</td><td>☐</td><td>Have password restrictions requiring a minimum password length of 18 characters been implemented for the Admin account?</td></tr>
<tr><td>☐</td><td>☐</td><td>Has the Admin account been renamed to match the naming scheme of the other user accounts?</td></tr>
<tr><td>☐</td><td>☐</td><td>Has the admin account been moved and/or hidden?</td></tr>
<tr><td>☐</td><td>☐</td><td>Has a separate, bogus Admin account been created for monitoring purposes?</td></tr>
<tr><td>Yes</td><td>No</td><td>Object and Property Security</td></tr>
<tr><td>☐</td><td>☐</td><td>Have Novell Directory Services and eDirectory software been updated?</td></tr>
<tr><td>☐</td><td>☐</td><td>Indicate if the follow object and property rights have been established:
<table>
<tr><td>☐</td><td>User accounts are restricted from having global access to objects or properties.</td><td>☐</td><td>Users are provided with the least amount of object and property rights necessary to perform their job function.</td></tr>
<tr><td>☐</td><td>Users are not granted Write rights to their login script.</td><td>☐</td><td>The [Public] object has the least amount of rights necessary.</td></tr>
<tr><td>☐</td><td>Users only have Read and File Scan rights to SYS:LOGIN</td><td>☐</td><td>Users only have Create rights to SYS:MAIL</td></tr>
<tr><td>☐</td><td>Users only have Read and File Scan rights to SYS:PUBLIC.</td><td>☐</td><td>Users do not have rights to the SYS:ETC directory.</td></tr>
<tr><td>☐</td><td>Users do not have rights to the SYS:SYSTEM directory.</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Yes</td><td>No</td><td>File System Security</td></tr>
<tr><td>☐</td><td>☐</td><td>Are home directories placed in volumes other than SYS?</td></tr>
<tr><td>☐</td><td>☐</td><td>Do users have access to NCF files?</td></tr>
<tr><td>☐</td><td>☐</td><td>Are user accounts established with the least amount of access rights necessary for the user to perform their responsibilities?</td></tr>
<tr><td>☐</td><td>☐</td><td>Have any users been granted access rights to directories outside their home directory?</td></tr>
<tr><td>☐</td><td>☐</td><td>If users have been set up outside their home directory, have rights,</td></tr>
</table>

		including inherited, been restricted to the least amount of access necessary?
☐	☐	Do any users have Access Control rights to directories outside of their home directory?
☐	☐	Do any end users have rights to the Root directory?
☐	☐	Do any end users have rights to SYS:SYSTEM?
Yes	No	**Generic Accounts**
☐	☐	List any generic accounts utilized on this server. | | | |---|---| | | | | | | | | | | | |
☐	☐	Do all of these accounts require a password?
☐	☐	Has the password been changed from the default password?
☐	☐	Are strong passwords required for these accounts?
☐	☐	Are address restrictions used to correspond with these accounts?
Yes	No	**Additional Security Provisions**
☐	☐	Are there any users still active on the server who have not logged in for 90 days?
☐	☐	Has the NLIST utility been removed or renamed?
☐	☐	Have tree browsing capabilities to the root of the tree been limiting with inheritance rights filters?
☐	☐	Has the [Public]'s browse rights to the [Root] of the tree been removed?
☐	☐	Has the Bindery Context command been removed from the AUTOEXEC.NCF file?
Monitoring		
Yes	No	**NetWare Logging**
☐	☐	Indicate if the following logs are being reviewed and how often they are being reviewed. | | **Log Name** | **Frequency Reviewed** | |---|---|---| | ☐ | SYS$LOG.ERR \| \| \| ☐ \| CONSOLE.LOG \| \| \| ☐ \| VOL$LOG.ERR | | | ☐ | ABEND.LOG | |
☐	☐	Is the NAAS utility being utilized to audit server events?
☐	☐	Is a third party product being utilized to audit server events?
		Indicate which of the following instances create alerts logged to log files. ☐ Unsuccessful attempts to access the Console.

		☐ Unsuccessful attempts to access the “Admin” account. ☐ Successful attempts at accessing the “Admin” account. ☐ Unsuccessful attempts to access user accounts (i.e. password guessing). ☐ Attempts to gain elevated privileges or access to unauthorized accounts. ☐ Modifications made to software, applications, and systems. ☐ Modifications made to the server configurations. ☐ Modifications made to account settings. ☐ Creation of new volumes.
Yes	No	**Trustee Assignments**
☐	☐	Are trustee assignments reviewed quarterly?
☐	☐	Is a review of hidden objects performed quarterly?
☐	☐	Are unused volumes reviewed and deleted or dismounted quarterly?
Yes	No	**Security Equivalences**
☐	☐	Are user equivalents tested quarterly for unauthorized settings using the following commands: ▪ NLIST USER WHERE “EQUIVALENT TO ME” EXISTS SHOW “EQUIVALENT TO ME” /r /s ▪ NLIST SERVER WHERE “EQUIVALNET TO ME” EXISTS SHOW “EQUIVALENT TO ME” /r /s ▪ NLIST GROUP WHERE “EQUIVALENT TO ME” EXISTS SHOW “EQUIVALENT TO ME”, “MEMBER” /r /s ▪ NLIST “ORGANIZATIONAL ROLE” WHERE “EQUIVALENT TO ME” EXISTS SHOW “EQUIVALENT TO ME”, “OCCUPANT” /r /s
Yes	No	**Third Parties**
☐	☐	Are third party personnel access rights restricted on the server?
☐	☐	Are third party personnel assigned temporary accounts?
☐	☐	Is the activity performed by third party personnel closely monitored? Indicate method:
☐	☐	Are all third party products tested in a test environment before being loaded and deployed on production servers?
☐	☐	Are all third party products installed on a separate partition on the server?
☐	☐	Are user access rights to the object or volume in which products are stored limited to execute only?
Maintenance		
Yes	No	**Patching and Updating**
☐	☐	Indicate if the following items have been updated to the most current

<table>
<tr><td></td><td></td><td>release. Indicate release:

<table><tr><th></th><th>Item</th><th>Release</th><th></th><th>Item</th><th>Release</th></tr><tr><td>☐</td><td>Patches</td><td></td><td>☐</td><td>Updates</td><td></td></tr><tr><td>☐</td><td>Hotfixes</td><td></td><td>☐</td><td>Driver versions</td><td></td></tr><tr><td>☐</td><td>BIOS versions</td><td></td><td>☐</td><td></td><td></td></tr></table></td></tr>
<tr><td>☐</td><td>☐</td><td>Has an automated patching system been implemented to assist with the patching process? Indicate system used:

</td></tr>
<tr><td>Yes</td><td>No</td><td>Backup and Recovery</td></tr>
<tr><td></td><td></td><td>Indicate the method or product used to perform backups.

☐ SMS
☐ Third party product. Specify:_____
☐ Other. Specify: _____</td></tr>
<tr><td>☐</td><td>☐</td><td>Have daily server backup procedures been documented?</td></tr>
<tr><td>☐</td><td>☐</td><td>Do these procedures describe details for backing up the system registry, server configurations, and data residing on the servers?</td></tr>
<tr><td>☐</td><td>☐</td><td>Is backup media maintained in a secure location while on-site?</td></tr>
<tr><td>☐</td><td>☐</td><td>Is backup media transferred to a secure off-site location as soon as possible after the backup has been completed?</td></tr>
<tr><td>☐</td><td>☐</td><td>Is backup media maintained for an appropriate amount of time?</td></tr>
<tr><td>☐</td><td>☐</td><td>Is backup media tested at least monthly? Indicate date last performed:

</td></tr>
<tr><td>☐</td><td>☐</td><td>Are audit flags backed up manually? Indicate frequency:

</td></tr>
<tr><td>Yes</td><td>No</td><td>Directory Service Utilities</td></tr>
<tr><td>☐</td><td>☐</td><td>Is unattended DSREPAIR run quarterly using the DSREPAIR –U command to ensure server integrity?</td></tr>
</table>

References

1. NMap Security Scanner. http://www.insecure.org/nmap/ (August 6, 2003)

2. Foust, Mark. "NetWare Security: Closing the Doors to Hackers." Novell Copyright 2000. June 7, 2000. URL:http://developer.novell.com/research/appnotes/2000/june/03/a000603.htm. (July 19, 2003).

3. "Novell NetWare." R1409. Rev 5/99. URL:http://www.umich.edu/~opde/top_tens/novell.html. (July 29, 2003).

4. Fischer, Jeff. "Administering Right in ConsoleOne: Part 1." Novell AppNotes. November 2002. URL:http://developer.novell.com/research/sections/netmanage/netnovice/2002/november/n021101.htm. (July 28, 2003).

5. "DSREPAIR." Novell NetWare 6 Utilities Reference. 103-000153-001. February 2002. URL:http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/utlrfenu/data/hneidcah.html. (July 17, 2003).

6. Fisher, Jeff. "Administering Rights in ConsoleOne: Part 2." Novell AppNote Copyright 2002. URL:http://developer.novell.com/research/sections/netmanage/netnovice/2002/december/n021201.htm. (July 28, 2003).

7. McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, Third Edition. Berkeley: Osborne/McGraw-Hill, 2001. 275 - 311.

8. Coomans, Patrick. "[PEN-TEST] Novell NetWare security evaluation." Neohapsis Archives. January 8, 2001. URL:http://archives.neohapsis.com/archives/sf/pentest/2001-01/0024.html. (August 6, 2003).

9. Novak, Kevin. "Securing Your NetWare Environment." Network Computing, October 16, 2000. URL:http://www.networkcomputing.com/1120/1120ws1.html. (July 17, 2003).

10. "NDS Health Check 2000." Novell at University of Michigan. May 15, 2003. URL:http://www.umich.edu/~lannos/novell/nds.health.check.html. (July 23, 2003).

11. "Novell NetWare 6 Security." ITS Security at UNC-Chapel Hill. URL:http://novell.unc.edu/security/security.htm. (July 14, 2003).

12. “S 4.102 C2 security under Novell 4.11.” IT Baseline Protection Manual. Copyright by Bundesamt für Sicherheit in der Informationstechnik. URL:http://www.bsi.bund.de/gshb/english/s/s4102.htm. (August 15, 2003).

13. “Protecting Your Network Against Known Security Threats.” Novell AppNote December 1998. URL:http://developer.novell.com/research/appnotes/1997/november/06/apv.htm. (July 14, 2003).

14. “Novell Advanced Audit Service; Installation and Administration Guide.” March 2003. URL:“http://www.novell.com/documentation/lg/nw6p/pdfdoc/naas_enu/naas_enu.pdf. (August 18, 2003).

15. “Partner Product Guide.” URL:http://www.novell.com/partnerguide/software.html. (August 18, 2003).

16. “Storage Management Service Administration Guide.” “NetWare 6.” August 1, 2002. URL:http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/back_enu/data/hjc2z4tu.html. (August 15, 2003).

Last Updated: July 22nd, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced