



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

Securing Windows GCNT Practical Assignment v3.0

Option 2 – Securing Windows 2000 With Security templates

Date Prepared: April 1, 2002

Prepared by: Michael J. Léger

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

TABLE OF CONTENTS

TABLE OF CONTENTS	I
WINDOWS 2000 DNS SERVER	3
SYSTEM DESCRIPTION.....	3
OPERATING SYSTEM AND INSTALLED SOFTWARE	3
SYSTEM CONFIGURATION	3
WINDOWS 2000 INSTALLATION.....	4
POST WINDOWS 2000 SERVER INSTALLATION	4
Figure 1.....	4
DNS CONFIGURATION.....	5
Zone File and Registry Security.....	5
Zone Transfers.....	5
Logging.....	5
Advanced Properties.....	5
Firewall	6
TEMPLATE SELECTION	6
ADDING ENTRIES TO THE TEMPLATE SECURITY OPTIONS	6
TEMPLATE SECURITY SETTINGS	7
ACCOUNT POLICIES	7
Password Policy.....	7
Account Lockout Policy.....	8
Kerberos Policy.....	9
LOCAL POLICIES	10
Audit Policy.....	10
User Rights Assignment.....	11
Security Options.....	14
EVENT LOG	20
Settings for Event Logs.....	20
RESTRICTED GROUPS	21
SYSTEM SERVICES.....	21
REGISTRY PERMISSIONS.....	23
FILE SYSTEM.....	24
APPLYING AND TESTING THE SECURITY TEMPLATE	25
Secedit.....	25
Applying the Template	25
Security Analysis.....	25
Automation of Analysis	26
TESTING THE APPLICATION OF THE TEMPLATE.....	27
Figure 2.....	27
Figure 3.....	27
Figure 4.....	28
TESTING SERVER FUNCTIONALITY	29
Remote Administration	29
Figure 5.....	29
Name Resolution.....	30
Figure 6.....	30
DNS Administration.....	31
Figure 7.....	31
VULNERABILITY ASSESSMENT SCAN	32
Figure 8.....	32

TEMPLATE EVALUATION33
REFERENCES.....34
APPENDIX A – SCEREGVL.INF35
APPENDIX B – SECURITY CONFIGURATION LOG FILE39

© SANS Institute 2000 - 2002, Author retains full rights

WINDOWS 2000 DNS SERVER

System Description

MAZE, the system that will be used throughout this paper, is a public DNS server used by an e-business company that hosts their own public DNS. The server is the primary DNS server and is a standalone server. This server is not a member of a domain. There is a secondary public DNS server, BLUE, that is also a standalone server. The e-business company has requested that the public DNS server be secure from DNS related attacks. The server must be unavailable to hackers or malicious users who wish to use the server for attacking other systems internally or externally.

Operating System and Installed Software

The operating system chosen for the DNS server is Microsoft's Windows 2000 Server. OpenSSH is installed on the server. SSH will be used to remotely administer the server.

System Configuration

The hardware configuration for MAZE consists of the following:

Generic "Build your Own" Server

- AMD Duron 800 CPU
- Two 20 GB Maxtor EIDE Hard Drives
- 512 MB of physical RAM
- CDROM
- CDRW
- Floppy Drive

Both hard drives on MAZE have been upgraded to Dynamic Disks. The hard drives have been partitioned in the following manner:

- Dynamic Disk0 C: "system" partition is 6GB and mirrored with a 6GB partition on Dynamic Disk1.
- Dynamic Disk0 D: "swap0" partition is 2GB.
- Dynamic Disk0 E: "Logs" partition is 11GB and mirrored with a 11GB partition on Dynamic Disk1.
- Dynamic Disk1 F: "swap1" partition is 2GB

Windows 2000 Installation

Windows 2000 Server was installed from a Windows 2000 Server CDROM. The system was installed at C:\WINNT.

Post Windows 2000 Server Installation

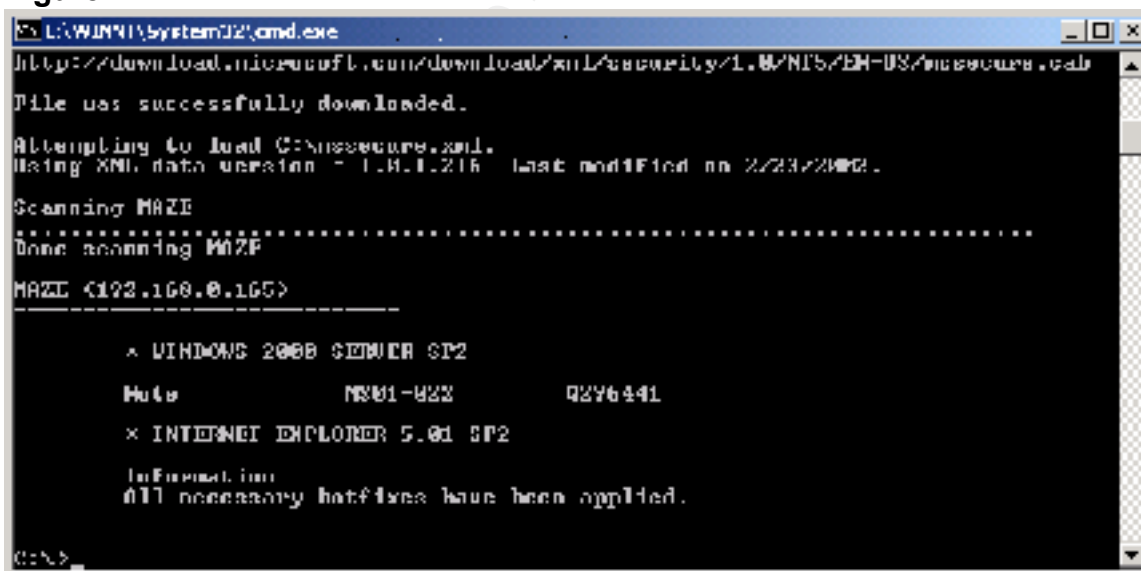
Following the installation of the Windows 2000 Server operating system the following were installed.

- Service Pack 2
- Windows 2000 Security Rollup Package January 2002

After the installation of the above, Windows Update was run to obtain any outstanding security updates. After Windows Update was completed, the server was rebooted. Hfnetchk.exe was executed to determine if any security hot fixes were missing. Figure 1 is a screen shot of the results from hfnetchk.exe. At this point all available hot fixes have been installed. Hfnetchk.exe can be downloaded from Microsoft.

<http://download.microsoft.com/download/win2000platform/Utility/3.3/NT45/EN-US/Nshc332.exe>

Figure 1



```
C:\WINNT\System32\cmd.exe
http://download.microsoft.com/download/win2000platform/Utility/3.3/NT45/EN-US/nshc332.exe
File was successfully downloaded.
Attempting to load C:\nshc332.xml.
Using XML data version = 1.0.1.215 Last modified on 2/23/2002.
Scanning MAZE
.....
Done scanning MAZE
MAZE <192.168.0.165>
-----
x WINDOWS 2000 SERVER SP2
Name           MS01-022      Q876441
x INTERNET EXPLORER 5.01 SP2
Information
All necessary hotfixes have been applied.
C:\>
```

Although all available hot fixes have been applied we do get a NOTE error message. ¹NOTE messages appear when hfnetchk.exe is unable to determine the patch installation status. This happens when the file and registry information

¹ Microsoft. Hfnetchk.exe Returns NOTE Messages for Installed Patches (Q306460). Oct. 24, 2001. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306460>.

is not available. The NOTE error is generated when the XML data file doesn't contain that information.

²MS01-022 (Q296441) updates Msdaipp.dll file to version 8.103.4004. Normally the Mssecure.xml file would contain the name of the file, the version, and the checksum. If this particular patch information is stored in the XML file, false positives will be generated during the scan. Certain Microsoft Office programs use versions of this file that are not vulnerable. These other versions of this file are greater than 8.103.4004. The higher version number would be interpreted as a file version and checksum mismatch. To reduce false positive WARNING messages, the XML database does not contain the file details. If the correct version of the file is verified, the NOTE message may be ignored. The file version should be greater than 8.103.4004.

DNS Configuration

The DNS service has been split into internal and external service. This configuration is known as split DNS. Split DNS is used to hide internal hostnames and their IP addresses.

Zone File and Registry Security

³It is recommended to secure DNS zone files if the DNS server records are not being stored in a Windows 2000 Active Directory. The DNS zone files will be secured through file and registry permissions that are applied by template.

Zone Transfers

Zone transfers are allowed to the secondary public name server only.

Logging

The server is configured to log Notify and Update events.

Advanced Properties

The DNS server is configured with the following additional settings:

- Secure cache against pollution
- Enable netmask ordering

² Microsoft. Hfnetchk.exe Returns NOTE Messages for Installed Patches (Q306460). Oct. 24, 2001. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306460>.

³ Stephens, Capt Robin G., USAF. Guide to Securing Microsoft Windows 2000 DNS (Version 1.0). National Security Agency. April 9, 2001. 9

Firewall

The primary and secondary server will be placed on a DMZ segment of redundant Cisco PIX 515 firewalls. The Firewall will have static translations so the DNS server can be queried from the Internet. Access-lists will allow UDP 53 inbound to the servers. TCP 53 will not be allowed since zone transfers will not be allowed from Internet. Secure Shell (SSH) will require TCP port 22 to be open.

TEMPLATE SELECTION

The NSA's (National Security Agency) w2k_server.inf was chosen for this system. The template was chosen based on the following reasons:

1. The NSA's reputation for security provides a sense of assurance that the appropriate steps were taken to ensure an aggressive starting point for securing a Windows 2000 server.
2. The template is readily available for download.
3. Documentation supporting the template that can be used for reference is also available for download.

Although the template provides an aggressive starting point for hardening this system; there is no 'Cookie Cutter' template. All templates, for any type of system, should be evaluated and modified to ensure compliance with security policies. Templates should be applied and tested in a lab environment before being applied to a production server.

The NSA template and supporting and documents can be accessed and downloaded from the following URL:

<http://nsa1.www.conxion.com/win2k/download.htm>

ADDING ENTRIES TO THE TEMPLATE SECURITY OPTIONS

Changes to the registry can be done manually but are prone to error and are time consuming. Changes that are done manually are also less likely to be analyzed for security compliance. If added to the template, these changes can be routinely analyzed with the entire template.

⁴To add an entry to the security options, edit the file %SystemRoot%\inf\sceregvl.inf. Prior to making any changes back up the sceregvl.inf file. Add a line that follows the form regpath,value type, displayname, displaytype. The commented lines from the sceregvl.inf file provide a key for adding the entries.

```
; First field: Full Path to Registry Value
; Second field: value type
;     ; REG_SZ                ( 1 )
;     ; REG_EXPAND_SZ        ( 2 ) \\ with environment variables to expand
;     ; REG_BINARY           ( 3 )
;     ; REG_DWORD            ( 4 )
;     ; REG_MULTI_SZ         ( 7 )
; third field: Display Name (localizable string),
; fourth field: Display type 0 - boolean, 1 - number, 2 - string, 3 - choices
```

After adding the lines to sceregvl.inf, save your changes. Scecli.dll will need to be re-registered by running regsvr32 scecli.dll from the command prompt.

Registry changes relating to Dynamic DNS, SYN attacks, and TCP/IP hardening will be added to this template. The changes to sceregvl.inf can be viewed in Appendix A.

⁵TEMPLATE SECURITY SETTINGS

⁶Account Policies

Password Policy

Enforce password history – 24 passwords remembered

By preventing users from rotating through their favorite passwords the risk that a hacker will discover passwords is significantly lower. The maximum value of 24 is the best option for a public DNS server.

Maximum password age – 90 days

Too weak set to 45 days.

⁴ Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set (Version 1.1). National Security Agency, 22 January 2002. 50

⁵ In the template security settings section, it is assumed that all settings and subsections of a category inherit the reference cited for that category unless specifically cited.

⁶ Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set (Version 1.1). National Security Agency, 22 January 2002. 21-26

The ranges of values for maximum password age are 0 (password never expires) to 999 days. The period of time that a password is valid should never be set to 0. The setting of 45 days for a public DNS server is stringent but not too stringent that an administrator can't set up a schedule for changing passwords.

Minimum password age – 1 day

Too weak set to 30 days.

The minimum password age is used to prevent users from changing their passwords in an effort to get back to the previous password. With the maximum password age set to 45 days and minimum password age set to 30 days the chances of rotating through previous passwords is greatly reduced.

Minimum password length – 12

Strong but recommend setting to maximum of 14.

Short passwords can be easily guessed by a hacker's password cracking tool. Passwords should be at least 12 – 14 characters in length to prevent passwords from being cracked. The maximum minimum password length in the security template interface is 14. Although longer password lengths normally will encourage a user to write his or her password down on paper, the public DNS server will be accessed by an administrator and a setting of 14 is appropriate.

Password must meet complexity requirements – Enabled

Complexity requirements are made up of 4 areas: upper case, lower case, numbers, and special characters. When this setting is enabled, passwords must contain characters from 3 of the 4 areas. Passwords cannot match logon names. Password complexity requirements can aid in the defense against tools that password guess and use dictionary attacks. This should be enabled regardless of system type.

Store password using reversible encryption for all users in the domain – Disabled

The password policies for this template are strong, aggressive, and appropriate.

Account Lockout Policy

Account lockout duration – 15

Too Weak

This setting determines the number of minutes an account will be locked out. A setting of 0 would indicate lockout until administrator unlocks it. The maximum setting is 99999 minutes. For a stand alone server a setting of 0 may be the ideal setting, but may create a potential for a denial of service attack. Some high setting like 720 (12hrs) is a good setting for a stand-alone public DNS server.

Account lockout threshold – 3 invalid logon attempts

Account lockout threshold helps to prevent brute force attacks on the system. Failed logon attempts are tracked for each account. When the number of failed attempts reaches the specified value the account becomes locked. The setting should be set low but not 0. The 0 setting would create a condition that will not allow an account to lock out. 3 is an aggressive and appropriate setting for a standalone public DNS server.

Reset account lockout counter after – 15

Too weak

This setting determines how long after a failed attempt the account lockout counter resets to 0. This setting should be high for a stand-alone public DNS server. With the settings from *account lockout duration* and *account lockout threshold* and the *reset account lockout counter after* set to 720, an attacker would at best be able to make 2 password attempts every 721 minutes. Because administrators will be the only ones that have access to this machine this setting could be set even higher like 1440 or 2880 but 720 is probably sufficient. If logs are properly monitored this type of attack can be recognized and the setting adjusted appropriately.

Kerberos Policy

Kerberos is an authentication method used in Windows 2000 Active Directory. Active directory is necessary for Kerberos authentication. Since this is a standalone DNS server Kerberos policies will not be defined.

Enforce user logon restrictions – Not defined

Maximum lifetime for service ticket – Not defined

Maximum lifetime for user ticket – Not defined

Maximum lifetime for user ticket renewal – Not defined

Maximum tolerance for computer clock synchronization – Not defined

⁷Local Policies

Audit Policy

Audit account logon events – Success, Failure

This audit policy tracks login events with other computers from which the local computer was to authenticate the account. This audit policy should be configured for success and failure.

Audit account management - Success, Failure

This audit policy tracks changes to the security account database. These changes are when accounts are created, changed or deleted. This audit policy should be configured for success and failure.

Audit directory service access – No auditing

Only applies to Active Directory. Since this server is a standalone DNS server, the audit policy should be configured for no auditing.

Audit logon events - Success, Failure

This audit policy tracks users who have logged on or off, or made a network connection. This policy also records whether the logon request was interactive, network, or service. This audit policy should be configured for success and failure.

Audit object access – Failure

Too weak

This audit policy tracks unsuccessful attempts to access objects such as directories, files, and printers. Object auditing is not automatic and must be enabled in the object's properties. This audit policy should be configured for success and failure.

Audit policy change - Success, Failure

This audit policy tracks changes in security policy. This audit policy should be configured for success and failure.

Audit privilege use – Failure

⁷ Haney, Julie M. [Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set](#) (Version 1.1). National Security Agency, 22 January 2002. 27-50

Too weak

This audit policy tracks any unsuccessful attempts to use privileges. The rights assigned to an administrator are a privilege. The list of user rights that are not audited by this policy are: Bypass Traverse Tracking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Backup Files and Directories, and Restore Files and Directories. This audit policy should be configured for success and failure.

Audit process tracking – No auditing

This audit policy tracks events such as program activation and exits. If you believe you are under attack it would be useful to record these events in detail. This audit policy should initially be configured for no auditing.

Audit system events - Success, Failure

This audit policy tracks events that affect the system or audit log itself. These types of events are restart and shutdown. This audit policy should be configured for success and failure.

Security logs should be monitored on a regular basis for any unusual activity. The audit policies for this template are configured for maximum logging. On some machines this can cause capacity issues on the hard drive. On our DNS server disk space is available therefore maximum logging should be configured.

User Rights Assignment

Access this computer from the network – Administrator and Users

Too weak

This privilege allows the user to access the server via the network. Always limit access to the servers. This is a standalone public DNS server. Administrator is the only access required.

Act as part of the operating system – Not Defined

Add workstations to domains – No Defined

Backup files and directories – Administrators

This privilege allows the user to backup files and directories. This setting overrides file and directory permissions.

Bypass traverse checking – Users

Too Weak

This privilege allows a user to maneuver through the directory structure and gain access to the files and subdirectories they have permission to access even if the user has no permission to access the parent directories.

Change the system time – Administrators

This privilege allows the user to set the internal clock of the system.

Create a pagefile – Administrators

This privilege allows the user to create new or make adjustment to existing pagefiles. Pagefiles are used for virtual memory swapping.

Create a token object – Not Defined

Create permanent shared objects – Not Defined

Debug programs – Not Defined

Deny access to this computer from the network – Not Defined

Deny login as a batch job – Not Defined

Deny logon as a service – Not Defined

Deny logon locally – Not Defined

Enable computer and user accounts to be trusted for delegation – Not Defined

Force shutdown from a remote system – Administrators

This privilege allows the user to shut down the system remotely.

Generate security audits – Not Defined

Increase quotas – Administrators

Increase schedule priority – Administrators

Load and unload device drivers – Administrators

This privilege allows the user to load and unload device drivers which are necessary for plug and play operation.

Lock pages in memory – Not Defined

Log on as a batch job – Not Defined

Log on as a service – Not Defined

Log on locally – Administrators

This privilege allows the user to log on to the systems console.

Manage auditing and security log – Administrators

This privilege allows the user to view and clear the security log. The user can also specify the types of object access that are to be audited. This privilege does not, however, allow the user to enable file and object access auditing in general. Object auditing must be enabled by setting the *audit object class* under the Audit Policies.

Modify firmware environment values – Administrators

Not applicable should be set to Not Defined.

Profile single process – Administrators

This privilege allows the user to profile processes for the sake of performance measurement.

Profile system performance – Administrators

This privilege allows the user to profile the system for the sake of performance measurement.

Remove computer from docking station – Not Defined

Replace a process level token – Not Defined

Restore files and directories – Administrators

This privilege allows the user to restore back-up files and directories. This privilege overrides file and directory permissions.

Shut down system – Administrators

This privilege allows the user to shut down the system.

Synchronize directory service data – Not Defined

Take ownership of files or other objects – Administrators

This privilege allows the user to take ownership of files and directories, printers and other objects on the system.

The User Rights Assignment settings for this template are strong, aggressive, and appropriate.

Security Options

Additional restrictions for anonymous connections – No access without explicit anonymous permissions

This security setting places one of three restrictions options on anonymous users.

- None. Rely on default permissions
- Do not allow enumeration of SAM accounts and shares. This option replaces the “Everyone” group with “Authenticated Users”.
- No access without explicit anonymous permissions. This option requires that “Anonymous” be given explicit permissions to access resources by removing the “Everyone” and “Network” groups from the anonymous user token. This is the best option for a standalone server.

Allow server operators to schedule tasks (domain controllers only) – Not Defined

This security setting is for domain controllers only. This security setting allows the use of the Schedule Service for task automation. By disabling this setting, only administrators can schedule tasks.

Allow system to be shut down without having to logon – Disabled

This security setting requires users to log on to a system to be able to it shut.

Allow to eject removable NTFS media – Administrators

By default only Administrators are allowed to eject removable NTFS media. This security setting allows for the following settings:

- Administrators

- Administrators and Power Users
- Administrators and Interactive Users

For this standalone server the setting should be Administrators Only.

Amount of idle time required before disconnecting session – 30

Too Weak

This security setting sets the amount of time before an idle SMB session will be disconnected. There should not be any SMB connections to this server. This should be set low to 5 or less.

Audit the access of global system objects – Enabled

This security setting enables auditing for global system objects. Audit Object Access must be also be enabled under auditing in order to audit global system objects.

Audit use of Backup and Restore privilege – Enabled

If Audit Privilege Use is enabled this security setting will enable the auditing of backup and restore user privileges.

Automatically log off users when logon time expires – Not defined

Automatically log off users when logon time expires (local) – Enabled

This security setting forces a user with logon restrictions to be logged off when that user's logon time expires.

Clear virtual memory pagefile when system shuts down – Enabled

This security setting wipes the pagefile clean when Windows 2000 shuts down. This prevents any information that may be helpful for a malicious user to be unavailable.

⁸***Determine whether TCP uses fixed or attempts to detect MTU*** – Uses MTU of 576 for all connections to computers outside the local subnet

This setting causes an MTU of 576 to be used for any connection to hosts not local.

Digitally sign client communication (always) – Disabled

⁸ Fossen, Jason. 5.4 Securing Internet Information Server 5.0. (Version 12.0). SANS Institute, October 3, 2001. 73

Digitally sign client communication (when possible) – Enabled

This security setting enables an SMB client to perform digital packet signing when communicating with an SMB server that also supports packet signing.

Digitally sign server communication (always) – Disabled

Digitally sign server communication (when possible) – Enabled

This security setting enables an SMB server to perform digital packet signing when communicating with an SMB client that also supports packet signing.

Disable CTRL+ALT+DEL requirement for logon – Disabled

This security setting is recommended for standalone servers.

⁹***Disable DNS dynamic update*** – Disable Dynamic Updates

This setting disables dynamic updates.

¹⁰***Disable ICMP Redirects*** – Disable ICMP Redirects

This server will not need ICMP redirects. ICMP redirects can be spoofed in order to change the server's route table. This setting will disable route table modification due to an ICMP redirect.

⁹***Disable IP Source Routing*** – Drop all source-routed packets

This setting will drop all incoming source-routed packets.

Do not display last user name in logon screen – Enabled

This security setting should be enabled to prevent a malicious user from acquiring any information about user names. This is very important for a standalone such as this one where login names will always be an administrator.

LAN Manager Authentication Level – Send NTLMv2 response only/refuse LM & NTLM

⁹ Fossen, Jason. 5.1 Windows 2000: Active Directory and Group Policy. (Version 5.0.2). SANS Institute, August 8, 2001. 105

¹⁰ Fossen, Jason. 5.4 Securing Internet Information Server 5.0. (Version 12.0). SANS Institute, October 3, 2001. 71-73

This security setting is the default challenge/response authentication for network logons with non-Windows 2000 clients.

⁹ **Limit damage caused by SYN flooding** – Reduce retransmission of SYN-ACK retries and require full 3-way handshake

This setting will reduce the number of SYN-ACK retries.

¹⁰ **Maximum number of TCP connections in the SYN_RECEIVED state before SynAttackProtect starts** – 100

This setting determines the maximum number of TCP connections in the SYN_RECEIVED state allowed. Once this value has been exceeded SynAttackProtect protection starts.

¹¹ **Maximum TCP connections in the SYN_RECEIVED state before SynAttackProtect protection starts when each of these connections has sent at least one SYN response retransmission** – 80

This setting determines the maximum number of TCP connections in the SYN_RECEIVED state allowed. When each of these connections sends a minimum of one retransmission of a SYN response in an attempt to negotiate a TCP session, SynAttackProtect starts.

Message text for users attempting to log on – Unauthorized access to this computer system and network is prohibited without explicit prior permission. Unauthorized use may result in criminal prosecution in a court of law and/or termination of employment. Your continued use of this computer and network constitutes your agreement to have your activities logged and monitored, including your keystrokes and mouse clicks.

This is the message text that is displayed when a user attempts to log on.

Message title for users attempting to log on – IMPORTANT LEGAL NOTICE!

This is the title bar text for the window that displays the message for user attempting log on.

Number of previous logons to cache (incase domain controller is not available) – 0 logons

The server is a standalone server not a member server. Setting this to 0 effectively disables this option.

¹¹ Fossen, Jason. 5.4 Securing Internet Information Server 5.0. (Version 12.0). SANS Institute, October 3, 2001. 72-73

¹²**Only accept DNS resolution replies from the same IP address of the DNS server originally queried** – Do not accept DNS resolution replies from IP other than originally queried.

This will help prevent the poisoning of the hostname cache on the server.

Prevent system maintenance of computer account password – Disabled

This server is a standalone server not a member server. This setting is not enabled.

Prevent users from installing printer drivers – Enabled

This setting prevents members of user groups from adding printer drivers on the local machine.

Prompt user to change password before expiration – 14

This security setting sets how many days in advance a user is warned to change their password. Not applicable to this server.

Recovery Console: Allow automatic administrative logon – Disabled

Never allow automatic administrator logon. If this is enabled anyone with physical access can log on to the server.

Recovery Console: Allow floppy copy and access to all drives and all folders – Disabled

This security setting enables the Recover Console Set command, which is used for setting console environment variables.

Rename administrator account – hismajesty

Always rename the administrator account. This will prevent a hacker who targets the default administrator account.

Rename guest account – theking

Always rename the guest account. This will prevent a hacker who targets the default guest account. The guest account should also be disabled if not needed.

Restrict CD-ROM access to locally logged-on user only – Enabled

¹² Fossen, Jason. 5.1 Windows 2000: Active Directory and Group Policy. (Version 5.0.2). SANS Institute, August 8, 2001. 105

This security setting allows an interactive user to access the CDROM.

Restrict floppy access to locally logged-on user only – Enabled

This security setting allows an interactive user to access the Floppy Drive.

Secure channel: Digitally encrypt or sign secure channel data (always) – Disabled

Secure channel: Digitally encrypt secure channel data (when possible) – Enabled

This security setting enables a computer to digitally encrypt secure channel data.

Secure channel: Digitally sign secure channel data (when possible) – Enabled

This security setting enables a computer to digitally sign secure channel data.

Secure channel: Require strong (Windows 2000 or later) session key – Disabled

This server is a standalone server not a member server. This setting is not enabled.

Secure system partition (for RISC platforms only) – Not defined

Send unencrypted password to connect to third-party SMB servers – Disabled

This security setting allows unencrypted password exchanges with 3rd party SMB servers.

Shut down system immediately if unable to log security audits – Enabled

This security setting is enabled because a secondary public DNS server exists in this scenario. If a secondary did not exist this should be disabled.

Smart card removal behavior – Lock Workstation

This setting is not applicable to this server and should be set to Not Defined.

Strengthen default permissions of global system objects (e.g. Symbolic Links) – Enabled

This security setting prevents a user from modifying global system objects not created by that user.

Unsigned driver installation behavior – Warn but allow installation

This security setting determines what action to take when a device driver that was not digitally signed attempts to install.

Unsigned non-driver installation behavior – Warn but allow installation

This security setting determines what action to take when a non-device driver that was not digitally signed attempts to install.

¹³ **Event Log**

Settings for Event Logs

Maximum application log size – 4194240 kilobytes

Maximum security log size -4194240 kilobytes

Maximum system log size - 4194240 kilobytes

The above event log settings are set to the maximum allowable values. This ensures that the system will still halt if the event log exceeds 4 GB, even if there is space on the hard drive.

Restrict guest access to application log – Enabled

Restrict guest access to security log – Enabled

Restrict guest access to system log – Enabled

The above settings prevent guests from viewing any event logs.

Retain application log – Not defined

Retain security log – 8 days

Retain system log – Not defined

This above event log settings control how long the event logs will be retained before they are overwritten.

Retention method for application log – As Needed

Retention method for security log – By Days

Retention method for system log – As Needed

The above event log settings determine how each log will be handled after it has become full.

¹³ Haney, Julie M. [Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set](#) (Version 1.1). National Security Agency, 22 January 2002. 53-54

Shut down the computer when the security audit log is full – Enabled

This event log setting if enabled allows the system to be halted immediately if events cannot be written to the security log. This is the recommended setting where there is a secondary DNS server.

Event log settings can vary depending on hard disk space and whether security is a priority over availability. There is a secondary public DNS server, which makes security a priority because availability is not an issue.

Event logs must be carefully monitored to determine if any policies should be changed. Event logs can also determine if a hacker or malicious user is trying to work around security policies.

Restricted Groups

Users

Users will be removed. This template will not apply any restricted groups.

System Services

Services can be configured for one of three settings: automatic, manual or disabled. Because services are system specific this template initially sets all services to Not Defined. It is recommended that services not required for proper operation of the system and it's applications be set to disabled.

Alerter - Disabled

Application Management – Not Defined

ClipBook - Disabled

COM+ Event System – Not Defined

Computer Browser - Automatic

DHCP Client – Disabled

Distributed File System – Disabled

Distributed Link Tracking Client – Disabled

Distributed Link Tracking Server – Disabled

Distributed Transaction Coordinator – Not Defined

DNS Client – Not Defined

DNS Server – Automatic

Event Log - Automatic

Fax Service – Disabled

File Replication - Disabled

Indexing Service – Disabled

Internet Connection Sharing – Disabled

Intersite Messaging – Disabled
IPSec Policy Agent - Automatic
Kerberos Key Distribution Center - Disabled
Licensing Logging Server – Not Defined
Logical Disk Manager – Not Defined
Logical Disk Manager Administrative Service – Not Defined
Messenger - Disabled
Net Logon – Not Defined
NetMeeting Remote Desktop Sharing - Disabled
Network Connections – Not Defined
Network DDE - Disabled
Network DDE DSDM - Disabled
NT LM Security Support Provider - Automatic
NVIDIA Driver Helper Service – Not Defined
OpenSSH Server - Automatic
Performance Logs and Alerts – Not Defined
Plug and Play – Not Defined
Print Spooler - Disabled
Protected Storage - Automatic
QoS RSVP - Disabled
Remote Access Auto Connection Manager - Disabled
Remote Access Connection Manager - Disabled
Remote Procedure Call (RPC) - Automatic
Remote Procedure Call (RPC) Locator - Automatic
Remote Registry Service - Disabled
Removable Storage - Disabled
Routing and Remote Access - Disabled
RunAs Service - Disabled
Security Accounts Manager – Not Defined
Server - Automatic
Smart Card - Disabled
Smart Card Helper - Disabled
System Event Notification – Not Defined
Task Scheduler - Disabled
TCP/IP NetBIOS Helper Service - Disabled
Telephony - Disabled
Telnet - Disabled
TermService - Disabled
Uninterruptible Power Supply – Not Defined
Utility Manager – Not Defined
Windows Installer – Not Defined
Windows Management Instrumentation - Disabled
Windows Management Instrumentation Driver Extensions - Disabled
Windows Time - Disabled
Workstation - Automatic

OpenSSH required that the Computer Browser service be running. Setting the Computer Browser service to Automatic ultimately required the following to run: Remote Procedure Call, Server, and Workstation. The services required by OpenSSH demonstrate that services that are normally preferred disabled, occasionally need to run.

Registry Permissions

In the registry section the tool set can be used to configure DACLs (discretionary access control lists) for registry keys. These changes can be done manually with regedt32.exe, but it is error prone and time consuming. These changes are necessary to provide an adequate level of security in Windows 2000.

¹⁴The template has configured DACLs for a list of registry keys.

```
CLASSES_ROOT
machine\software
machine\software\microsoft\netdde
MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT
machine\software\microsoft\protected storage system provider
MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands
machine\software\microsoft\windows nt\currentversion\perflib
machine\software\microsoft\windows\currentversion\group policy
machine\software\microsoft\windows\currentversion\installer
machine\software\microsoft\windows\currentversion\policies
machine\system\
machine\system\clone
machine\system\controlset001
machine\system\controlset002
machine\system\controlset003
machine\system\controlset004
machine\system\controlset005
machine\system\controlset006
machine\system\controlset007
machine\system\controlset008
machine\system\controlset009
machine\system\controlset010
machine\system\currentcontrolset\control\securepipeservers\winreg
machine\system\currentcontrolset\control\wmi\security
machine\system\currentcontrolset\enum
machine\system\currentcontrolset\hardware profiles
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\
```

¹⁴ Haney, Julie M. [Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set](#) (Version 1.1). National Security Agency, 22 January 2002. 67-71

ValidCommunities
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\
PermittedManagers
users\.default\software\microsoft\protected storage system provider
users\.default\software\microsoft\netdde
users\.default

Although these DACLs are appropriate and probably satisfactory, most of the settings had permissions for Users and CREATED OWNER. Permissions for Users and CREATED OWNER are not necessary for this server. All the DACLs except for CLASSES_ROOT, machine\software\, machine\system\, and users\.default were removed from the template. All permissions were deleted except for Administrators and SYSTEM on the remaining keys. The settings are configured to replace existing permissions on all subkeys with inheritable permissions.

File System

The template set the security levels on the %Program Files%, %System Directory%, %System Drive%, %System Root%, and various files, executables, and directories within them.

The template has been adjusted to configure %System Drive% only. The setting is configured to replace existing permissions on all subfolders and files with inheritable permissions. The permissions are set for Full Control for Administrator and SYSTEM.

APPLYING AND TESTING THE SECURITY TEMPLATE

The security template was applied and analyzed using the `secdit.exe` command line utility. Secedit can be used to configure the system from a security template or analyze system compliance to a template. The command line tool was used in order to understand how to configure or analyze the security templates without the Security Console. This will be useful when using SSH for remote management.

Secedit

The command line syntax for `secdit` when used for system analysis or configuration is:

```
15Secedit {/analysis | /configure} [/cfg filename] [/db filename]
[/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

Applying the Template

The following shows the complete command that was run to configure the system.

```
secdit /configure /db e:\security\My_Security_Template.sdb /cfg
e:\security\My_Security_Template.inf /log e:\security\My_Security_template.log
```

'Task is completed. See log.' was the visual result. The log was reviewed and it was determined that the template was applied successfully. When examining the log, errors appeared because some files and registry settings did not exist. These types of errors can be safely ignored. See the log output in Appendix B.

Security Analysis

After applying the template and confirming it's successful application, it is important to continue the security process by analyzing system security settings on a regular basis. The `secdit` command can be used to perform this analysis. This security analysis is done against a database. The configuration file or files that have been imported into the database make up the baseline for the analysis. Security settings from the configuration file are compared to the current system settings. Analysis results are presented in the results file with the baseline side by side with the current system settings. After reviewing the results, modifications can be made and exported into a configuration file for bringing the system back into compliance.

¹⁵ Frisch, Aeleen. Windows 2000 Commands, Pocket Reference. O'Reilly, March 2001. 87-88

Automation of Analysis

Template security settings could be analyzed automatically. It is possible to write a script utilizing the secedit.exe command line utility. The script could be scheduled to run once a week or twice a month. The script could also email the results to the person responsible for log analysis.

The script could be written utilizing VBScript or Perl Script. A free script may be out on the Internet that may only need minor adjustment to work on this system. It is important to note that any script that is downloaded from the Internet must be understood thoroughly before executing, and should be done so in a non-production lab environment before being put on a production server.

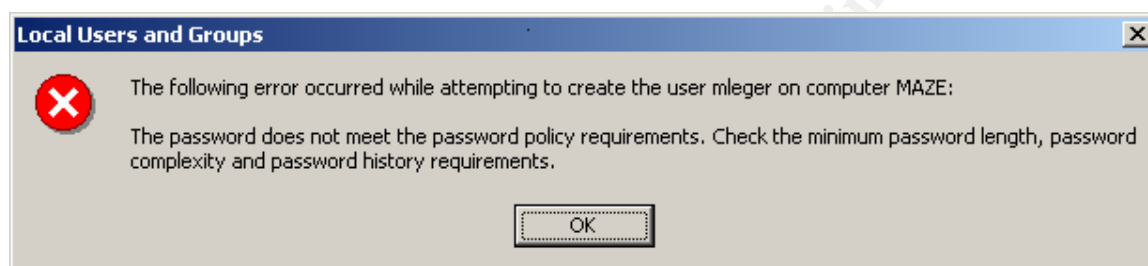
© SANS Institute 2000 - 2002, Author retains full rights.

Testing the Application of the Template

It is necessary to determine whether application of the security template and its configuration changes are working properly. Three security settings will be tested.

An attempt to add a new user with a password less than 14 characters has generated the pop window shown in figure 2. This is in accordance with the security policy that states the passwords will be no shorter than 14 characters.

Figure 2



After turning the system date past 45 days a pop up window appeared during logon informing me that my password had expired and it would need to be changed. The following log file in figure 3 supports the expiration of the account password. This is in compliance with maximum password age.

Figure 3

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 535
Date: 8/30/2002
Time: 10:22:08 PM
User: NT AUTHORITY\SYSTEM
Computer: MAZE
Description:
Logon Failure:
Reason: The specified account's password has expired
User Name: mleger
Domain: MAZE
Logon Type: 2
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: MAZE

Using the account mleger and deliberately typing the wrong passwords 4 times, a pop up window was generated indicating the password had been locked out. By entering the wrong password 4 continuous times the lockout policy of 3 attempts was exceeded. The following log in figure 4 indicates the account for mleger has been locked out.

Figure 4

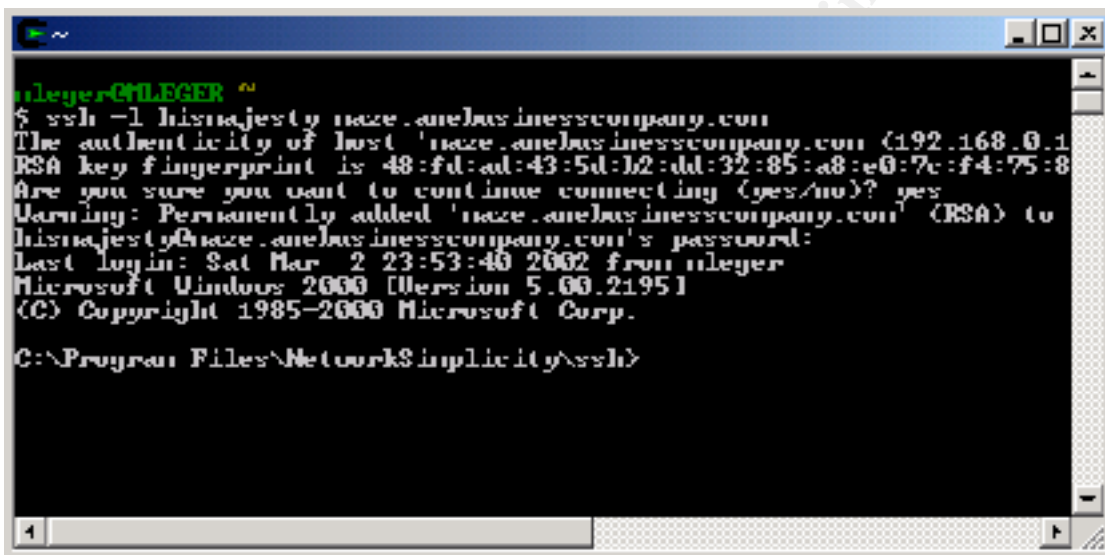
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 539
Date: 3/30/2002
Time: 11:12:23 PM
User: NT AUTHORITY\SYSTEM
Computer: MAZE
Description:
Logon Failure:
Reason: Account locked out
User Name: mleger
Domain: MAZE
Logon Type: 2
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: MAZE

Testing Server Functionality

Remote Administration

OpenSSH is used for remote administration. Figure 5 demonstrates that an SSH connection can be made to the server after the template has been applied. The connection was made from my laptop.

Figure 5



```
fileger@OLEGER ~
$ ssh -l hismajesty maze.anebusinescompany.com
The authenticity of host 'maze.anebusinescompany.com (192.168.0.1)'
RSA key fingerprint is 48:fd:ad:43:5d:12:dd:32:85:a8:e0:7c:f4:75:8
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'maze.anebusinescompany.com' (RSA) to
hismajesty's maze.anebusinescompany.com's password:
Last login: Sat Mar 2 23:53:40 2002 from fileger
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

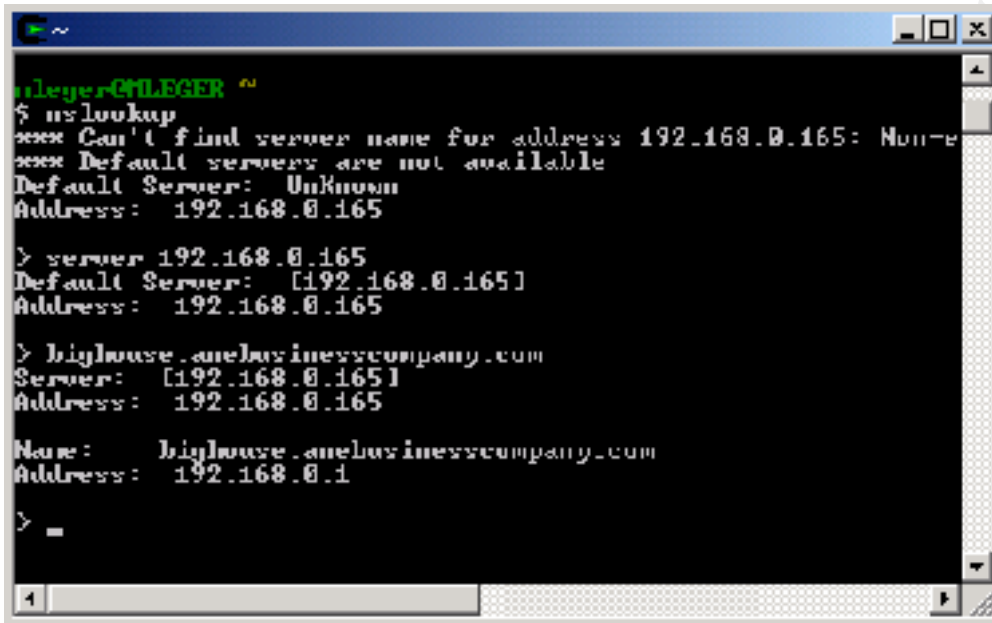
C:\Program Files\Network$implicit>ssh
```

My laptop is configured to use MAZE as its only DNS Server. When the SSH client requested a connection to the server by the name maze.anebusinescompany.com the DNS server resolved the name.

Name Resolution

Another tool for testing DNS, nslookup, is simple but useful. I can use nslookup to directly query the name server. See figure 6.

Figure 6



```
~\
C:\Users\aleger> nslookup
nslookup
Can't find server name for address 192.168.0.165: Non-existent
Default servers are not available
Default Server: Unknown
Address: 192.168.0.165

> server 192.168.0.165
Default Server: [192.168.0.165]
Address: 192.168.0.165

> highhouse.anelaxinexcompany.com
Server: [192.168.0.165]
Address: 192.168.0.165

Name:      highhouse.anelaxinexcompany.com
Address:   192.168.0.1

> -
```


DNS Administration

The dnscmd command line utility will be used to administer the DNS server. To display basic information about the DNS server the following command is invoked.

```
dnscmd /Info
```

Figure 7



```
C:\Program Files\Network$implicity\ssh>dnscmd /Info
Query result:
Server info:
    ptr - 00075E78
    server name - name
    version - 02000005
    DS container - (null)

Configuration:
    debugLevel - 00000000
    debugLevel - 00000000
    doRpcProtocol - P P P P P P P P
    doNameCheckFlag - 00000002
    cAddressRangeLimit - 0
    doRecursionRetry - 3
    doRecursionTimeout - 15
    doDsPollingInterval - 300

Configuration Flags:
    fBootMethod - 3
    fAdminConfigured - 1
    fAllowUpdate - 1
    fDsAvailable - 0
    fAutoReverseZone - 1
    fAutoCacheUpdate - 0
    fSlave - 0
    fNoRecursion - 0
    fRoundRobin - 1
    fLocalNetPriority - 1
    fStrictFilePassing - 0
    fLooseWildcarding - 0
    fBindSecondary - 1
    fWriteAuthorityNs - 0

Aging Configuration:
    ScavengingInterval - 0
    DefaultAgingState - 0
    DefaultRefreshInterval - 168
    DefaultNoRefreshInterval - 168

ServerAddresses:
    Addr Count - 1
    Addr[0] -> 192.168.0.165

ListenAddresses:
    NULL IP Array.

Forwarders:
    Addr Count - 1
    Addr[0] -> 198.77.116.8
    forward timeout - 5
    slave - 0

Command completed successfully.

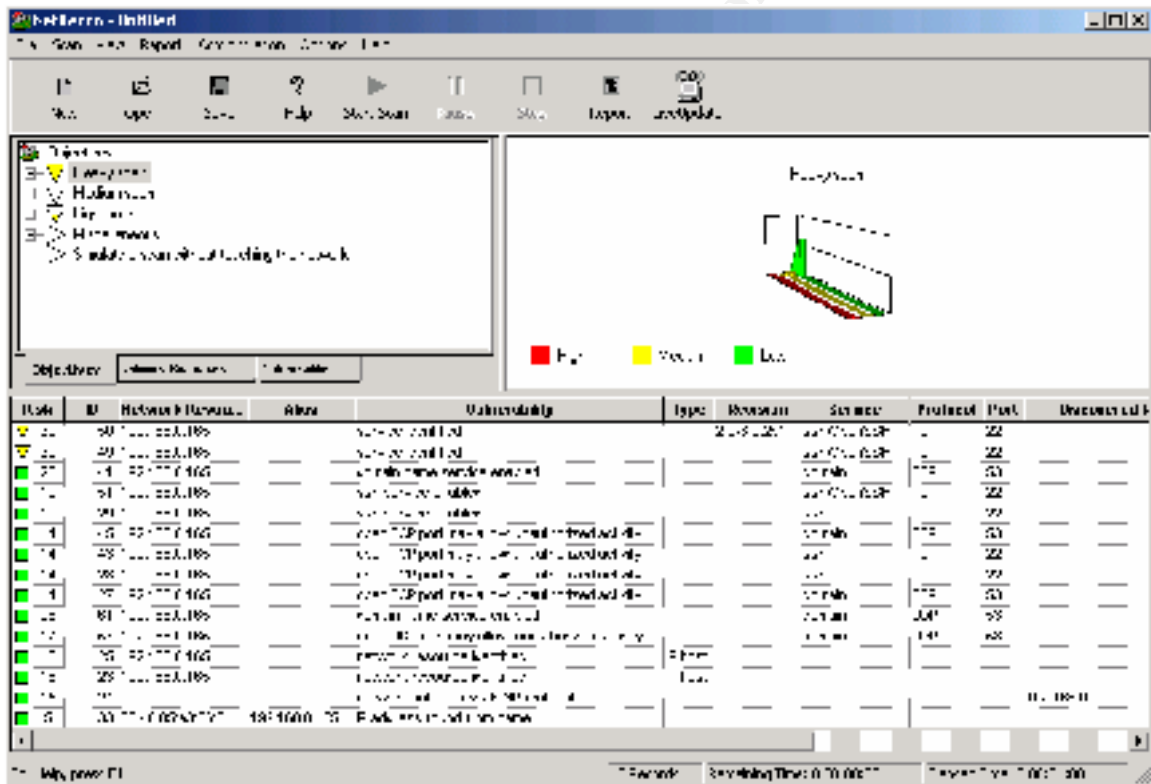
C:\Program Files\Network$implicity\ssh>
```

The ability to perform an nslookup, and connect to MAZE by name when using the SSH client demonstrates the DNS servers ability to resolve names. Connecting via the SSH client proves the SSH server is running and remote administration is available. Successful use of the dnscmd /Info command line utility to request information about the DNS server indicates the DNS server can be administered with dnscmd over SSH.

Vulnerability Assessment Scan

After successful application and testing of the template, Symantec's NetRecon was used to scan the DNS server. The laptop with NetRecon was placed on the DMZ subnet. Figure 8 shows the result of a heavy scan.

Figure 8



The results of the heavy scan showed that NetRecon was able to determine the version of OpenSSH running on the server. This information could be used by a hacker if there was a known vulnerability with that version. The other results are related to the DNS server and the OpenSSH server, which is expected and is acceptable. No other results i.e. unauthorized services, open ports, or authorization for a Null user sessions appeared when the server was scanned.

TEMPLATE EVALUATION

Overall I would describe this template as an acceptable starting point for a standalone Windows 2000 server. This template can be modified to work with standalone or member servers.

I felt this template needed adjustment to the password and account lockout policies. These policies were too weak for this server. Although, I wouldn't say it was a shortcoming. Every machine is going to be different and depending upon company security policies and the services provided these settings could be adjusted accordingly.

Although I got aggressive with changes to the registry and file system permissions, the template was low strong to high weak in these areas. The template would have been flexible if there had been other applications running and users that did not have administrator privileges when accessing the system. If that flexibility had been required, the template settings would have been an appropriate starting point. This system did not need that flexibility and therefore any unneeded permissions were not necessary. Again I don't feel this a shortcoming. Security policies and services provided by a system will dictate changes that are made to file and registry permissions.

I do believe one shortcoming of the template would be the lack of TCPIP hardening. Certain TCPIP parameters should be a configurable security option in all templates. These options should start out as defaults and should be adjusted appropriately to defend specific system types. Some examples of these options were added to the template applied to this server. An example of these options is DisableIPSourceRouting. This option gives a sender the ability to determine the destination path for a packet. This can be legitimate, but attackers can use it to penetrate networks.

The template does not appear to have affected system performance. Administration and remote management of the system has not been disrupted or hindered by the application of template. Continued analysis of system performance and log files will assist in determining if any adjustments will need to be made to the template configuration.

REFERENCES

Stephens, Capt Robin G., USAF. Guide to Securing Microsoft Windows 2000 DNS (Version 1.0, 09 April 2001). National Security Agency.

Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set (Version 1.1, 22 January 2002). National Security Agency.

Larson, Matt and Liu, Cricket. DNS on Windows 2000. O'Reilly, September 2001.

Frisch, Aeleen. Windows 2000 Commands, Pocket Reference. O'Reilly, March 2001.

Fossen, Jason. 5.1 Windows 2000: Active Directory and Group Policy. (Version 5.0.2, 08 August 2001). SANS Institute.

Fossen, Jason. 5.4 Securing Internet Information Server 5.0. (Version 12.0, 03 October 2001). SANS Institute.

Microsoft. Hfnetchk.exe Returns NOTE Messages for Installed Patches (Q306460). Oct. 24, 2001. URL:
[HTTP://SUPPORT.MICROSOFT.COM/DEFAULT.ASPX?SCID=KB;EN-US;Q306460](http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q306460).

APPENDIX A – SCEREGVL.INF

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: SCERegVL.INF
; Template Version: 05.00.DR.0000
;
; Revision History
; 0000 - Original
```

```
[version]
signature="$CHICAGO$"
DriverVer=11/14/1999,5.00.2183.1
```

```
[Register Registry Values]
;
; First field: Full Path to Registry Value
; Second field: value type
; ; REG_SZ ( 1 )
; ; REG_EXPAND_SZ ( 2 ) \\ with environment variables to expand
; ; REG_BINARY ( 3 )
; ; REG_DWORD ( 4 )
; ; REG_MULTI_SZ ( 7 )
; third field: Display Name (localizable string),
; fourth field: Display type 0 - boolean, 1 - number, 2 - string, 3 - choices
```

```
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects,4,%AuditBaseObjects%,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail,4,%CrashOnAuditFail%,0
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing,3,%FullPrivilegeAuditing%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel,4,%LmCompatibilityLevel%,3,0%LMCL
ve10%,1%LMCLlevel1%,2%LMCLLevel2%,3%LMCLLevel3%,4%LMCLLevel4%,5%LMCLLevel5%
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous,4,%RestrictAnonymous%,3,0%RA0%,1%RA
1%,2%RA2%
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl,4,%SubmitControl%,0
```

```
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers,4,%AddPrintDrivers%,0
```

```
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown,4,%ClearPageFileAtShutdown%, 0
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode,4,%ProtectionMode%,0
```

```
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature,4,%EnableSMBSi
gnServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature,4,%RequireSMB
SignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff,4,%EnableForcedLo
goff%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect,4,%AutoDisconnect%,1,%
Unit-Minutes%
```

```
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature,4,%EnableS
MBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature,4,%Requir
eSMBSignRDR%,0
```

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword,4,%EnablePlainTextPassword%,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange,4,%DisablePWChange%,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel,4,%SignSecureChannel%,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel,4,%SealSecureChannel%,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal,4,%SignOrSeal%,0

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey,4,%StrongKey%,0

MACHINE\Software\Microsoft\Driver

SigningPolicy,3,%DriverSigning%,3,0%DriverSigning0%,1%DriverSigning1%,2%DriverSigning2%

MACHINE\Software\Microsoft\Non-Driver

SigningPolicy,3,%NDriverSigning%,3,0%DriverSigning0%,1%DriverSigning1%,2%DriverSigning2%

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD,4,%DisableCAD%,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName,4,%DontDisplayLastUserName%,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption,1,%LegalNoticeCaption%,2

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText,1,%LegalNoticeText%,2

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon,4,%ShutdownWithoutLogon%,0

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel,4,%RCAdmin%,0

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand,4,%RCSet%,0

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms,1,%AllocateCDRoms%,0

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon\AllocateDASD,1,%AllocateDASD%,3,0%AllocateDASD0%,1%AllocateDASD1%,2%AllocateDASD2%

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies,1,%AllocateFloppies%,0

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon\CachedLogonsCount,1,%CachedLogonsCount%,1,%Unit-Logons%

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon>PasswordExpiryWarning,4,%PasswordExpiryWarning%,1,%Unit-Days%

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon\ScRemoveOption,1,%ScRemove%,3,0%ScRemove0%,1%ScRemove1%,2%ScRemove2%

; delete these values from current system - Rdr in case NT4 w SCE

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DisableCAD

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CmdConsSecurityLevel

MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\AddPrintDrivers

MACHINE\System\CurrentControlSet\Services\MRXSMB\Parameters\EnableSecuritySignature

MACHINE\System\CurrentControlSet\Services\MRXSMB\Parameters\RequireSecuritySignature

MACHINE\System\CurrentControlSet\Services\MRXSMB\Parameters\EnablePlainTextPassword

MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnableSecuritySignature

MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecuritySignature

MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword

MACHINE\Software\Microsoft\Windows\CurrentVersion\NetCache\EncryptEntireCache

;Additions for DNS, SYN attacks, TCP hardening

MACHINE\System\CurrentControlSet\Services\DnsCache\Parameters\QueryIpMatching,4,%QueryIpMatching%,3,0%QueryIpMatching0%,1%QueryIpMatching1%

GCNT Practical Assignment 3.0

Option 2 - Securing Windows 2000 With Security Templates

36

MACHINE\System\CurrentControlSet\Services\DnsCache\Parameters\DisableDynamicUpdate,4,%DisableDynamicUpdate%,3,0%DisableDynamicUpdate0%,1%DisableDynamicUpdate1%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%SynAttackProtect%,3,0%SynAttackProtect0%,1%SynAttackProtect1%,2%SynAttackProtect2%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen,4,%TcpMaxHalfOpen%,1,%TCPconnections%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried,4,%TcpMaxHalfOpenRetried%,1,%TCPconnections%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirects,4,%EnableICMPRedirects%,3,0%EnableICMPRedirects0%,1%EnableICMPRedirects1%

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%DisableIPSourceRouting%,3,0%DisableIPSourceRouting0%,1%DisableIPSourceRouting1%,2%DisableIPSourceRouting2%

MACHINE\System\CurrentControlSet\Services\DnsCache\Parameters\EnablePMTUDiscovery,4,%EnablePMTUDiscovery%,3,0%EnablePMTUDiscovery0%,1%EnablePMTUDiscovery1%

[Strings]

SubmitControl = Allow server operators to schedule tasks (domain controllers only)

ShutdownWithoutLogon = Allow system to be shut down without having to log on

AllocateDASD = Allowed to eject removable NTFS media

AllocateDASD0 = Administrators

AllocateDASD1 = Administrators and Power Users

AllocateDASD2 = Administrators and Interactive Users

AuditBaseObjects = Audit the access of global system objects

FullPrivilegeAuditing = Audit use of Backup and Restore privilege

EnableForcedLogoff = Automatically log off users when logon time expires (local)

AutoDisconnect = Amount of idle time required before disconnecting session

ClearPageFileAtShutdown = Clear virtual memory pagefile when system shuts down

RequireSMBSignRdr = Digitally sign client communication (always)

EnableSMBSignRdr = Digitally sign client communication (when possible)

RequireSMBSignServer = Digitally sign server communication (always)

EnableSMBSignServer = Digitally sign server communication (when possible)

DisableCAD = Disable CTRL+ALT+DEL requirement for logon

RestrictAnonymous = Additional restrictions for anonymous connections

RA0 = None. Rely on default permissions

RA1 = Do not allow enumeration of SAM accounts and shares

RA2 = No access without explicit anonymous permissions

DontDisplayLastUserName = Do not display last user name in logon screen

LmCompatibilityLevel = LAN Manager Authentication Level

LMCLevel0 = Send LM & NTLM responses

LMCLevel1 = Send LM & NTLM - use NTLMv2 session security if negotiated

LMCLevel2 = Send NTLM response only

LMCLevel3 = Send NTLMv2 response only

LMCLevel4 = Send NTLMv2 response only\refuse LM

LMCLevel5 = Send NTLMv2 response only\refuse LM & NTLM

LegalNoticeText = Message text for users attempting to log on

LegalNoticeCaption = Message title for users attempting to log on

CachedLogonsCount = Number of previous logons to cache (in case domain controller is not available)

AddPrintDrivers = Prevent users from installing printer drivers

DisablePWChange = Prevent system maintenance of computer account password

PasswordExpiryWarning = Prompt user to change password before expiration

RCAdmin = Recovery Console: Allow automatic administrative logon

RCSet = Recovery Console: Allow floppy copy and access to all drives and all folders

AllocateCDRoms = Restrict CD-ROM access to locally logged-on user only

AllocateFloppies = Restrict floppy access to locally logged-on user only

ProtectionMode = Strengthen default permissions of global system objects (e.g. Symbolic Links)

SignOrSeal = Secure channel: Digitally encrypt or sign secure channel data (always)

SealSecureChannel = Secure channel: Digitally encrypt secure channel data (when possible)

SignSecureChannel = Secure channel: Digitally sign secure channel data (when possible)

StrongKey = Secure channel: Require strong (Windows 2000 or later) session key

CrashOnAuditFail = Shut down system immediately if unable to log security audits

EnablePlainTextPassword = Send unencrypted password to connect to third-party SMB servers

GCNT Practical Assignment 3.0

Option 2 - Securing Windows 2000 With Security Templates

ScRemove = Smart card removal behavior
ScRemove0 = No Action
ScRemove1 = Lock Workstation
ScRemove2 = Force Logoff
DriverSigning = Unsigned driver installation behavior
NDriverSigning = Unsigned non-driver installation behavior
DriverSigning0 = Silently succeed
DriverSigning1 = Warn but allow installation
DriverSigning2 = Do not allow installation
Unit-Logons = logons
Unit-Days = days
Unit-Minutes = minutes
QueryIpMatching = Only accept DNS resolutions replies from the same IP address of the DNS server originally queried
QueryIpMatching0 = Accept DNS resolution replies from IP other than originally queried
QueryIpMatching1 = Do Not accept DNS resolution replies from IP other than originally queried
DisableDynamicUpdate = Disable DNS dynamic updates
DisableDynamicUpdate0 = Enable Dynamic Updates
DisableDynamicUpdate1 = Disable Dynamic Updates
SynAttackProtect = Limit damage caused by SYN flooding
SynAttackProtect0 = No SYN flood protection
SynAttackProtect1 = Reduce retransmission of SYN-ACK retries
SynAttackProtect2 = Reduce retransmission of SYN-ACK retries and require full 3-way handshake
TcpMaxHalfOpen = Maximum number of TCP connections in the SYN_RECEIVED state before SynAttackProtect starts
TCPconnections = Connections
TcpMaxHalfOpenRetried = Maximum TCP connections in the SYN_RECEIVED state before SynAttackProtect protection starts when each of these connections has sent at least one SYN response retransmission
EnableICMPRedirects = Disable ICMP Redirects
EnableICMPRedirects0 = Disable ICMP Redirects
EnableICMPRedirects1 = Enable ICMP Redirects
DisableIPSourceRouting = Disable IP Source Routing
DisableIPSourceRouting0 = Forward all packets even if source routed
DisableIPSourceRouting1 = Do not forward source routed packets
DisableIPSourceRouting2 = Drop all incoming source routed packets
EnablePMTUDiscovery = Determine whether TCP uses fixed or attempts to detect MTU
EnablePMTUDiscovery0 = Uses MTU of 576 for all connections to computers outside the local subnet
EnablePMTUDiscovery1 = Attempts to discover the MTU of path to remote host

APPENDIX B – SECURITY CONFIGURATION LOG FILE

05/07/2002 21:19:15

----Configuration engine is initialized successfully.----

----Reading Configuration template info...

Event audit settings are turned off.

----Configure User Rights...

Configure S-1-5-32-544.

User Rights configuration completed successfully.

----Configure Group Membership...

Group Membership configuration completed successfully.

----Configure Registry Keys...

Configure users\default.

Configure machine\software.

Warning 6: The handle is invalid.

Error setting security on machine\software\Microsoft\Windows NT\CurrentVersion\Perflib\009.

Configure machine\system.

Warning 5: Access is denied.

Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error opening machine\system\ControlSet001\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error setting security on machine\system\ControlSet001\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error opening machine\system\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error setting security on machine\system\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error opening machine\system\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error setting security on machine\system\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.

Error opening machine\system\ControlSet001\Control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet001\Control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\ControlSet001\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet001\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\ControlSet001\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet001\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet001\Control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\ControlSet001\Control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet001\Control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\ControlSet002\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet002\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\ControlSet002\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet002\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error opening machine\system\ControlSet002\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error setting security on machine\system\ControlSet002\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\Properties.
Warning 5: Access is denied.
Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error opening machine\system\ControlSet002\Control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error setting security on machine\system\ControlSet002\Control\Class\{4D36E969-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error opening machine\system\ControlSet002\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error setting security on machine\system\ControlSet002\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error opening machine\system\ControlSet002\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error setting security on machine\system\ControlSet002\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error take ownership of machine\system\ControlSet002\Control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error opening machine\system\ControlSet002\Control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.

Warning 5: Access is denied.
 Error setting security on machine\system\ControlSet002\Control\Class\{4D36E980-E325-11CE-BFC1-08002BE10318}\Properties.

Error 234: More data is available.
 Error enumerating info for machine\system\ControlSet002\Control\Print.

Error 234: More data is available.
 Error setting security on machine\system\ControlSet002\Control\Print.

Error 234: More data is available.
 Error setting security on machine\system\ControlSet002\Control.

Error 234: More data is available.
 Error setting security on machine\system\ControlSet002.
 Configure classes_root.

Registry keys configuration completed with error.

----Configure File Security...

Configure c:\.

File security configuration completed successfully.

----Configure General Service Settings...

Configure Wmi.
 Configure WinMgmt.
 Configure W32Time.
 Configure TrkWks.
 Configure TrkSvr.
 Configure TlntSvr.
 Configure TermService.
 Configure TapiSrv.
 Configure Spooler.

Configure SharedAccess.
Configure seclogon.
Configure Schedule.
Configure SCardSvr.
Configure SCardDrv.
Configure RSVP.
Configure RpcSs.
Configure RpcLocator.
Configure RemoteRegistry.
Configure RemoteAccess.
Configure RasMan.
Configure RasAuto.
Configure ProtectedStorage.
Configure PolicyAgent.
Configure OpenSSHd.
Configure NtmsSvc.
Configure NtLmSsp.
Configure NtFrs.
Configure mnmsrv.
Configure Messenger.
Configure LmHosts.
Configure lanmanworkstation.
Configure lanmanserver.
Configure kdc.
Configure IsmServ.
Configure Fax.
Configure Eventlog.
Configure DNS.
Configure Dhcp.
Configure Dfs.
Configure ClipSrv.
Configure cisvc.
Configure Browser.
Configure Alerter.

General Service configuration completed successfully.

----Configure available attachment engines...

Load attachment LanManServer.

LanManServer: Query configuration information

Attachment engines configuration completed successfully.

----Configure Security Policy...

Configure password information.

Rename the Administrator account name to hismajesty.

Rename the Guest account name to theking.

System Access configuration completed successfully.

Configure log settings.

Audit/Log configuration completed successfully.

Configure machine\software\microsoft\driver signing\policy.

Configure machine\software\microsoft\non-driver signing\policy.

Configure machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel.

Configure machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand.

Configure machine\software\microsoft\windows nt\currentversion\winlogon\allocateddrams.

Configure machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd.

Configure machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies.

Configure machine\software\microsoft\windows nt\currentversion\winlogon\autoadminlogon.

Configure machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount.
 Configure machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning.
 Configure machine\software\microsoft\windows\currentversion\policies\explorer\nodrivetypeautorun.
 Configure machine\software\microsoft\windows\currentversion\policies\system\disablecad.
 Configure machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername.
 Configure machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption.
 Configure machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
 Configure machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon.
 Configure machine\system\currentcontrolset\control\lsa\auditbaseobjects.
 Configure machine\system\currentcontrolset\control\lsa\crashonauditfail.
 Configure machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
 Configure machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel.
 Configure machine\system\currentcontrolset\control\lsa\restrictanonymous.
 Configure machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers.
 Configure machine\system\currentcontrolset\control\session manager\memory management\clearpagetableatshutdown.
 Configure machine\system\currentcontrolset\control\session manager\protectionmode.
 Configure machine\system\currentcontrolset\services\dns cache\parameters\disabledynamicupdate.
 Configure machine\system\currentcontrolset\services\dns cache\parameters\enablemudiscovery.
 Configure machine\system\currentcontrolset\services\dns cache\parameters\queryipmatching.
 Configure machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect.
 Configure machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff.
 Configure machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature.
 Configure machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature.
 Configure machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword.
 Configure machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature.
 Configure machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature.
 Configure machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange.
 Configure machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal.
 Configure machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey.
 Configure machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel.
 Configure machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel.
 Configure machine\system\currentcontrolset\services\tcpip\parameters\disableiprouting.
 Configure machine\system\currentcontrolset\services\tcpip\parameters\enableicmpredirects.
 Configure machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxhalfopen.
 Configure machine\system\currentcontrolset\services\tcpip\parameters\tcpmaxhalfopenretried.

Registry values configuration completed successfully.

----Configure available attachment engines...

Attachment engines configuration completed successfully.
Event audit settings are restored.

----Un-initialize configuration engine...

Upcoming Training

Click Here to
{Get CERTIFIED!}



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