Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator (GCWN) Practical Assignment Version 3.1

Option 2 – Securing a Firewall Management Server With Security Templates

SANS Network Security
Orlando, FL
April 1-7, 2002

Prepared by Tomas Alex

September 20, 2002

Table of Contents

Table of Figures

1. Executive Summary

With the advent of Windows 2000, a number of improved security features and options have been added over the previous Microsoft operating systems which, when properly configured, can effectively harden a system. A greater majority of these security settings can be configured through the use of templates. Templates represent a collection of security settings that can be configured and applied to one system or many. Several pre-defined templates are available from Microsoft and other sources that can achieve a specific security stance for a specific type of system.

This paper's focus is to apply a selected security template on a firewall management server. The firewall management server represents a single location to manage a corporate firewall and to store firewall security policies. Testing will be conducted of the template's security settings and also the server's key applications to ensure their proper functionality. Also, a step-by-step review is discussed on how to apply this template to a server of this specific type.

Lastly, an evaluation of the template will be conducted to judge its effectiveness on the firewall management server and what suggestions to apply to the default template in order to optimize it for this server. Further, aspects of the server's security that cannot be secured by the template will be reviewed.

2. Description of System

2.1. Type of System

The type of system to be secured with a security template is a firewall management server. The server's primary role is to provide a single location to manage a corporate firewall and to house the centrally managed firewall security policies. The security policies are downloaded to the firewall (i.e. the security policy enforcement point) to "run" as the firewall rulebase. This architecture is specific to the Checkpoint VPN-1/Firewall-1 Next Generation (NG) software. The firewall management server maintains the security policies which are comprised of databases, including network object definitions, policies, and log files. In addition to the management server software, the Checkpoint GUI software is also installed, which acts as a front end to define the security policy, browser logs, check firewall status, etc.

This server's secondary role is to provide a central location to remotely administer the firewall using Secure Shell (SSH). This server represents a centralized point of firewall management and houses the firewall databases and logs. It has remote administration access capability to the corporate firewall and has been deployed in a secured management server network (described in Section 2.3 below). Further to this, the firewall management server will run Terminal Services enabling selected remote internal systems access in addition to the local console access.

2.2. System's Hardware and Software Configuration

For this paper, the following system was employed:

Server Hardware - Compaq Proliant DL360

- Pentium III Processor x 2
- 2 GB RAM Memory
- 36.4-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″) x 2
- Embedded Smart Array 5i Controller
- 2 Compaq NC7780 Gigabit Ethernet NIC Embedded 10/100/1000
- 24x IDE CD-ROM Drive
- 1.44 MB Floppy Drive

Software Installed

- Microsoft Windows 2000 Server, 5.00.2195, Service Pack 3
- Compaq ROMPaqs
- Checkpoint VPN-1/Firewall-1 NG Management Server, FP2
- Checkpoint Firewall-1 GUI FP2 Build 520144
- F-Secure SSH Client 5.2 Build 10
- Microsoft Internet Explorer v5.5

Physical/Logical Disk and File System Breakdown

- 2 x 36.4 GB Drives mirrored (Raid 1) providing 1 logical drive
- 1 NTFS file system (C:\) located on logical disk 0

2.3. System's Security Requirements

Based on the role and the function of the firewall management server, the security risks for the server are:

- The server houses the firewall security policies, rulebases, databases, and log files, data considered critical and sensitive.

- The firewall is remotely administered from this server and only this server has access to apply and manage the firewall rulebase.

Therefore, based on these high security risks, the security requirements must follow the defence in-depth philosophy of not relying on any one device (i.e. border router, firewall, etc.) for protection. The perimeter defences provide the first layer of security to the firewall management server and measures must also be taken to reduce the security vulnerabilities to the server itself:

- The firewall management server must be located in a secured management network in order to restrict access to it (**figure 1**).

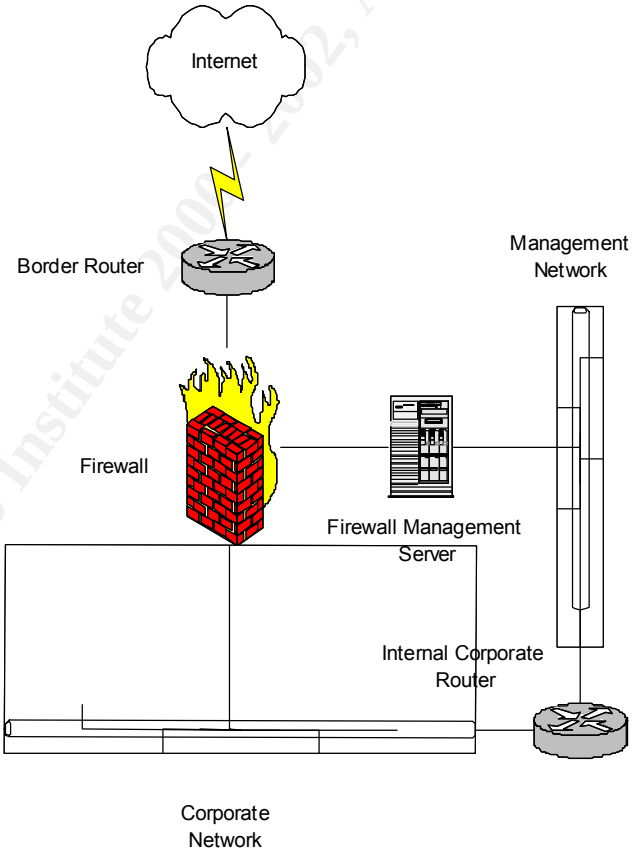

Figure 1 – Firewall Management Server Deployment

Internally the corporate management network is secured with restrictive ACLs implemented on an internal router that allows traffic from/to internal sources that have explicit requirements to access the various systems management servers. The firewall management server is classified as one of these systems. Equally, on the NIC connected to the firewall, traffic is restricted from/to the firewall management server by the firewall itself.

- The following security requirements apply to the firewall management server itself:
    - Minimize the number of system services by disabling any unnecessary services.
    - Ensure that only Administrator can start, stop, or change a service.
    - The server is standalone and not a member of a domain.
    - Allow only Administrators logon access to the server locally (on system console) or remotely (via RDP). No other types of users are required to be supported.
    - Maintain 30 days worth of server logs (i.e. system, security, and application) locally.
    - Ensure the server is time synchronized to an internal source used by other systems management servers on the secured management network. This is required if the firewall management server logs will be evaluated with other servers' audit logs when an intrusion is detected.
    - Employ inbound TCP/IP filters on both NICs to allow only explicitly permitted traffic to the server.

3. Checklist or Template?

3.1. Selecting a Template

An existing template, provided from a reputable source (e.g. Microsoft, the National Security Agency (NSA), SANS, etc.) ensures a reliable security baseline in hardening the operating system. There are several types of existing templates in existence to accommodate the varying levels of security. For example, an internal corporate server acting as a domain controller plus supplying file and print services will have different security requirements from an externally DMZ-located web server facing the Internet. Several different types of checklists would have to be built in order to accommodate the security requirements for each of these servers. The number of manual edits required to build these checklists increase the chance of error and time to complete them.

Based on the role of the server and the security requirements to address the high risk, the NSA Windows 2000 Server/Advanced Server template (http://nsa2.www.conxion.com/win2k/guides/inf/w2k_server.inf) was selected. It provides enhanced security settings for standalone servers and is extremely well documented. It should also be noted that the documentation for the Microsoft templates was lacking when compared with NSA's. The NSA provides a well-documented description of its templates that can be downloaded from: http://nsa2.www.conxion.com/win2k/download.htm. The w2k_server.inf is included in Appendix A.

4. Security Settings

Prior to the actual deployment of the NSA w2k_server.inf template on the firewall management server, a review of its security settings will be conducted. The template makes several changes to the Account Policies, Local Policies, Event Log, Restricted Groups, Registry and File System security settings. All relevant security settings to the firewall management server will be explained in this section. Any non-relevant settings will be marked with an "N/A". Section 5.4 below will discuss whether the settings are optimal.

Policy / Description	***Computer Setting***
Account Policies / Password Policy	
Enforce password history The number of unique passwords that are associated with an account before an old or previous password can be reused.	24 passwords remembered
Maximum password age The number of days that a password can be used with an associated account before it has to be changed.	90 days
Minimum password age The number of days that a password with an associated account can be used before it can be changed.	1 days
Minimum password length The least number of characters required in an account's password. The longer the password, the more difficult it is to crack.	12 characters
Password must meet complexity requirements The password must not contain all or part of the associated account name, must be at least 6 characters in length, and must contain 3 of the 4 categories: upper case, lower case, digits, and non-alphanumeric. With password complexity enabled, the ability to thwart malicious users in trying to guess the password is greatly increased.	Enabled
Store password using reversible encryption for all users in the domain Storing passwords with this method is the same as storing the password in clear text and should NEVER be enabled.	Disabled

Policy / Description	***Computer Setting***
Account Policies / Password Policy	
Account lockout duration Determines the number of minutes that a user account is locked out.	15 minutes
Account lockout threshold Limits the amount on invalid logon attempts to 3 before the account is locked out.	3 invalid logon attempts
Reset account lockout counter after The number of minutes before a locked out account's failed logon attempts are reduced to 0.	15 minutes

The Account Policies / Password Policy mechanisms are intended to temporarily disable a user account if a malicious user attempts to guess the passwords by brute force, known as a dictionary attack. A dictionary attack is an attack that tries to potentially send thousands of account password attempts relying on a predefined list of passwords. These mechanisms also prevent the malicious user from further break-in attempts.

Kerberos Policy

Since Active Directory is necessary for Kerberos authentication and this is a standalone firewall management server (i.e. Active Directory is not deployed), Kerberos policies are not required.

Policy / Description	***Computer Setting***
Local Policies / Audit Policy	
Audit account logon events Records when an attempt to logon to an account is successful or fails.	Success, Failure
Audit account management Records events that are related to account management. Specifically when user accounts are changed, added, and deleted. Also, any password changes are captured as well.	Success, Failure
Audit directory services access Applies to Active Directory so this is not applicable.	No auditing
Audit logon events Records each occurrence of an account logging on, logging off, or making a network connection to this server.	Success, Failure
Audit object access Records failed access to objects such as files, directories, registry keys and printers.	Failure
Audit policy change Records successful and failed changes to the user rights policies and audit policies.	Success, Failure
Audit privilege use Records attempts to exercise a right that has not been assigned to the particular user.	Failure
Audit process tracking If activated, this would facilitate the generation of an event that details program activation and exits. With the setting activated, a substantial additional amount of logging activity may be generated. This could also affect both performance and disk storage. This setting is useful for short-term activation when the need arises.	No auditing
Audit system events Records when account initiates a shutdown or restart of the server. Also, any events that affect the server security are recorded here.	Success, Failure
Policy / Description	***Computer Setting***

Local Policies / User Rights Policy	
Access this computer from the network Allows Administrators and Users to connect to the server over the network.	Administrators, Users
Act as part of the operating system N/A	Not defined
Add workstations to domains N/A	Not defined
Backup files and directories Allows only Administrators the privilege of bypassing file and directory permissions in order to backup the system. This is an override to the regular file and directory permissions.	Administrators
Bypass traverse checking Allows Users to bypass the normal restrictive permissions on a directory and permits them to ability traverse the directory trees.	Users
Change the system time Allows Administrators to change the data and time on the internal server clock.	Administrators
Create a pagefile Allows only Administrators the privilege to create and modify the size of a pagefile (i.e. known as Virtual Memory).	Administrators
Create a token object N/A	Not defined
Create permanent shared objects N/A	Not defined
Debug programs N/A	Not defined
Deny access to this computer from the network N/A	Not defined
Deny login as a batch job N/A	Not defined
Deny logon as a service N/A	Not defined
Deny logon locally N/A	Not defined
Enable computer and user accounts to be trusted for delegation N/A	Not defined
Force shutdown from a remote system Allows Administrators the privilege to shutdown the server remotely.	Administrators
Generate security audits N/A	Not defined
Increase quotas N/A	Administrators
Increase schedule priority N/A	Administrators
Load and unload device drivers N/A	Administrators
Lock pages in memory N/A	Not defined
Log on as a batch job N/A	Not defined

Policy / Description	***Computer Setting***
Local Policies / User Rights Policy	
Log on as a service N/A	Not defined
Log on locally Allows only Administrators the privilege to logon to the server at the server console.	Administrators
Manage auditing and security log N/A	Administrators
Modify firmware environment values N/A	Administrators
Profile single process N/A	Administrators
Profile system performance N/A	Administrators
Remove computer from docking station N/A	Not defined
Replace a process level token N/A	Not defined
Restore files and directories Allows Administrators to bypass file and directory permissions when restoring files and directories that have been backed up.	Administrators
Shut down system Allows Administrators the privilege to shut down the server.	Administrators
Synchronize directory service data N/A	Not defined
Take ownership of files or other objects N/A	Administrators

Policy / Description	***Computer Setting***
Security Options	
Additional restrictions for anonymous connections Any anonymous connections must be granted explicit privileges to any required resources. Specifically, Everyone and Network are removed from the anonymous users token.	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only) N/A	Not defined
Allow system to be shut down without having to logon The server can only be shutdown after successful logon.	Disabled
Allow to eject removable NTFS media This is consistent with default Windows 2000 setting and is applicable to this server.	Administrators
Amount of idle time required before disconnecting session Specifies that 30 minutes of continuous idle time must pass in a SMB session before the session is terminated due to inactivity.	30 minutes

Policy / Description	***Computer Setting***
Security Options	
Audit the access of global system objects Enables objects such as semaphores, mutexes, etc., to be created with System Access Control Lists (SACLs) that can then be used to audit any access to these objects.	Enabled
Audit use of Backup and Restore privilege Enables auditing of user rights including Backup and Restore which can be recorded in the security log if "Audit privilege use" is enabled as well.	Enabled
Automatically log off users when logon time expires N/A	Not defined
Automatically log off users when logon time expires (local) Disconnects any SMB client sessions to be disconnected when client's logon time expires.	Enabled
Clear virtual memory pagefile when system shuts down The Virtual Memory pagefile is cleared after a clean shutdown.	Enabled
Digitally sign client communication (always) N/A	Disabled
Digitally sign client communication (when possible) An SMB client connection is required to perform SMB packet signing when communicating with an SMB server that also support packet signing.	Enabled
Digitally sign server communication (always) N/A	Disabled
Digitally sign server communication (when possible) Enables the SMB server to perform packet signing.	Enabled
Disable CTRL+ALT+DEL requirement for logon Requires CTRL+ALT+DEL before logon to server. Not disabling this before the logon may leave the connection open to a malicious user to intercept the password.	Disabled
Do not display last user name in logon screen Prevents the name of the last successful logon user from being displayed. This prevents a malicious user from acquiring it.	Enabled
LAN Manager Authentication Level Only accepts NTLMv2 authentication. This is ideal for maximum security. For NTLMv2, password-derived keys are 128-bit encrypted.	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on N/A	Not defined
Message title for users attempting to log on N/A	Not defined
Number of previous logons to cache (in case domain controller is not available) N/A since this is a standalone server. A value of 0 disables this setting.	0 Logons
Prevent system maintenance of computer account password Prevents the server from requesting a weekly computer account password change.	Disabled
Prevent users from installing printer drivers Enabled to prevent users form installing print drivers on the server.	Enabled
Prompt user to change password before expiration administrator? N/A	14 days

Policy / Description	***Computer Setting***
Security Options	
Recovery Console: Allow automatic administrative logon Requires the Administrator password to be provided when utilizing the Recovery Console. This is a must to maintain secure authenticated access to the server.	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders Disables various Recovery Console environmental variables that are allowed very unrestrictive access to files, folders, and media on the server.	Disabled
Rename administrator account Renaming the Administrator account is critical to protecting against malicious user attacks. This is not defined in this template and is left up to the Administrator to rename it. If it was set in this template, a malicious user would use this setting as well.	Not defined
Rename guest account Similar to the Administrator account, protecting the guest account is critical as a malicious user could also target it.	Not defined
Restrict CD-ROM access to locally logged-on user only Only allows interactive logon users to access the CD-ROM and not remote users.	Enabled
Restrict floppy access to locally logged-on user only Only allows interactive logon users to access the floppy and not remote users.	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always) N/A as this is a standalone server.	Disabled
Secure channel: Digitally encrypt secure channel data (when possible) N/A as this is a standalone server.	Enabled
Secure channel: Digitally sign secure channel data (when possible N/A as this is a standalone server.	Enabled
Secure channel: Require strong (Windows 2000 or later) session key N/A as this is a standalone server.	Disabled
Secure system partition (for RISC platforms only) N/A	Not defined
Send unencrypted password to connect to third-party SMB servers If enabled, SMB client connection will send clear text passwords to non-Microsoft SMB server.	Disabled
Shut down system immediately if unable to log security audits Collecting and preserving security logs are critical; therefore shutting down the server for this reason is acceptable. Note: The firewall itself will continue to run without the need for a firewall management server.	Enabled
Smart card removal behavior N/A	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links) The Discretionary Access Control List (DACL) for objects is stronger by only allowing non-Administrator accounts to read shared objects but not modify them.	Enabled
Unsigned driver installation behavior N/A	Warn but allow installation
Unsigned non-driver installation behavior Produces a warning to the installer that the non-device software has not been certified.	Warn but allow installation

Policy / Description	***Computer Setting***
Event Log	
Maximum application log size Sets the application log file size to the maximum possible. Disk storage permitting, this setting is probably ideal as collecting all system logs on this server is critical.	4194240 kilobytes
Maximum security log size Sets the security log file size to the maximum possible. Disk storage permitting, this setting is probably ideal as collecting all system logs on this server is critical.	4194240 kilobytes
Maximum system log size Sets the system log file size to the maximum possible. Disk storage permitting, this setting is probably ideal as collecting all system logs on this server is critical.	4194240 kilobytes
Restrict guest access to application log Prevents guests from accessing the application log.	Enabled
Restrict guest access to security log Prevents guests from accessing the security log.	Enabled
Restrict guest access to system log Prevents guests from accessing the system log.	Enabled
Retain application log Determines how long the application log will be retained before being overwritten.	Not defined
Retain security log Determines how long the security log will be retained before being overwritten.	Not defined
Retain system log Determines how long the system log will be retained before being overwritten.	Not defined
Retention method for application log Determines what to do with application events when the application log is full.	Manually
Retention method for security log Determines what to do with security events when the security log is full.	Manually
Retention method for system log Determines what to do with system events when the system log is full.	Manually
Shut down the computer when the security audit log is full As documented by Microsoft, the "Shut down system immediately if unable to log security audits" setting should be used instead of this one: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/563.asp. It is unknown why the this option is set in the NSA template, contrary to Microsoft's recommendations.	Enabled

Restricted Groups

This option allows the management of membership in sensitive groups by defining two properties: Members and Members Of. Members defines who should and should not belong to the restricted group. Members Of defines which other groups the restricted group should belong to. The template places the Power Users local group in the Restricted Groups where they can be tracked and managed by the security policy. Power Users is a sensitive group since it possesses most administrative privileges with some restrictions.

System Services

System services can have the startup mode configured as either automatic, manual, or disabled. Since system services are environment and application specific, they were not configured in this template. Unnecessary services should be disabled as they may be vulnerable to buffer overflow or denial of service (DoS) attacks.

Registry

A high level inspection of the registry keys reveals that the template has removed certain user groups and imposed more restricted permissions on the Discretionary Access Control Lists (DACL) for selected registry keys. A DACL itself forms part of the security descriptor for an object. Further detailed analysis (not in the scope of this paper) of these registry key changes would be required to obtain a comprehensive understanding of the security settings they introduce.

File System

This template modifies security permissions on the %SystemDrive%, %SystemDirectory%, %SystemRoot%, and %ProgramFiles% directory structures and some of their respective directories and files contained in them. Certain directories and files contain sensitive configuration, system log, and authentication data such as account passwords. Two key directory security permissions modified by the template are:

- %SystemDirectory%\config (%SystemDirectory% is C:\WINNT\system32)
  is modified by:
  "%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
- %SystemRoot%\repair (%SystemRoot% is C:\WINNT)
  is modified by:
  "%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

Only the SYSTEM account and those in the Administrators group may now access these files.

By default in Windows 2000, the access permissions on both directories allow any account to access and read their contents. Specifically, %SystemDirectory%\config directory contains the system's event logs and the %SystemRoot%\repair directory contains copies of parts of the registry that are used to create an emergency repair disk. Both of these directories are known to be targets of malicious users. This vulnerability is documented by CERT at:

http://www.cert.org/security-improvement/implementations/i029.01.html

5. Apply, Test, and Evaluate the Template

5.1. Apply The Template

This template has been created for a firewall management server (or servers with similar security requirements) that is configured to be a standalone server with restricted user access (only Administrator) and is not part of an Active Directory deployment. The template will be applied by using a command script that calls secedit. Secedit is a program that is used to perform a security analysis and configuration as part of a script. The command line syntax for secedit is:

secedit {/**analysis** | **/configure**} [**/DB** *filename*] [**/CFG** *filename*] [**/overwrite**][**/areas** *area1 area2...*] [**/log** *logpath*] [**/verbose**] [**/quiet**]

Complete documentation for secedit can be found at:

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_secedit_analyze.htm

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_secedit_configure.htm

Apply the template to existing systems by completing the four steps:

1. Apply template with a command line script that calls secedit as demonstrated below:

   secedit /configure /db c:\WINNT\security\Database\w2k_server.sdb /cfg c:\WINNT\security\templates\w2k_server.inf /log c:\WINNT\security\logs\w2k_server.log

2. Review the w2k_server.log file log to ensure the template was successfully applied.

3. Test that the template's security settings are working and have been applied as expected.

4. Test the system's functionality to ensure the modified security settings did not adversely affect any applications on the server.

Note: The four steps above were completed for the "test" firewall management server used for analysis in this paper.

Ensure the template is first applied to a non-production server with an appropriate back out plan in place to restore the server to its former revision of security settings if application of the template fails. This non-production or test server would also serve as a facility to perform a security analysis of the template.

The template (including all of its revisions) should be maintained on the systems management server. When required, the template could be distributed via a command script to all relevant servers. As detailed above, the template would be applied to the server manually.

The Microsoft and NSA websites should also be monitored to see if updated security settings should be applied to the template.

5.2. Test The Template's Security Settings

The following four tests of the template security settings confirm that the security is working as expected:

Security Setting Test 1	***Computer Setting***	***Test Steps***	***Result***
Account Policy / Password Policy / Password must meet complexity requirements	Enabled	1. Logon to console as Administrator. 2. Launch Computer Management and right click Users to bring up New User dialog box. 3. Attempt to create User name "sansuser" with password of "abcdeabcde1234" (password only meets 2 of 4 areas required for complexity requirements).	Password fails to meet complexity requirements (**Figure 2**).

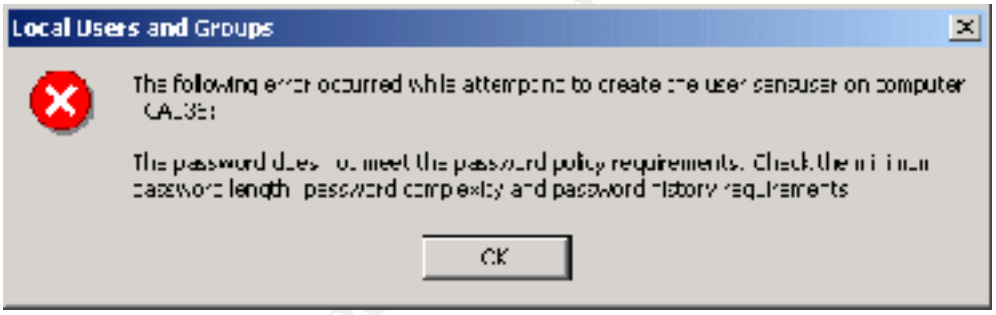

Figure 2 – Failure to Meet Minimum Password Length

Security Setting Test 2	***Computer Setting***	***Test Steps***	***Result***
Account Policy / Account Lockout Policy / Account lockout threshold	3 invalid logon attempts	1. Launch Computer Management and right click Users to bring up New User dialog box. 2. Create User name "sansuser". 3. Logout as Administrator. 4. Logon as "sansuser" and enter incorrect password. 5. Repeat incorrect password entry 3 additional times.	Creation of "sansuser" account demonstrates security setting Local Policies / Audit Policy / Audit account management as captured in the Event Security Logs (**Figure 3**). Account is locked out after 3rd invalid password attempt (**Figure 4**).

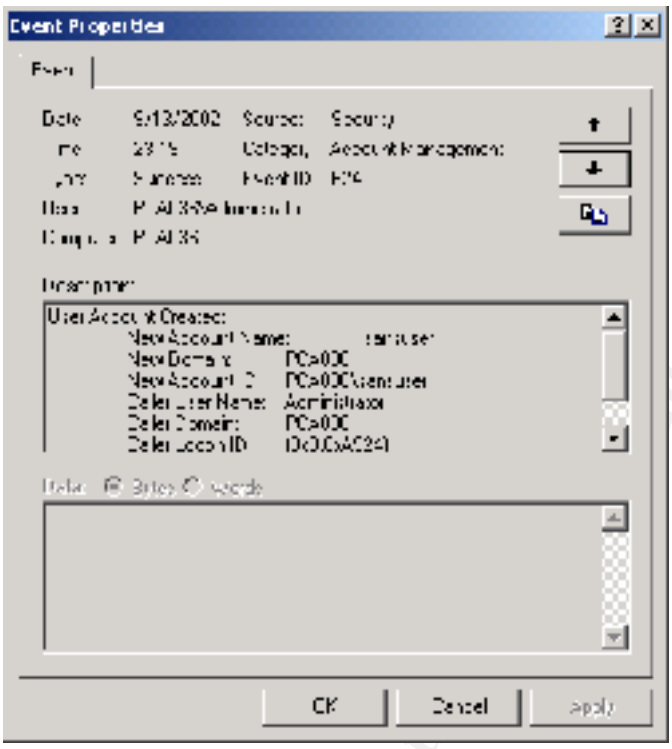

Figure 3 – Successful User Account Creation Security Log Entry

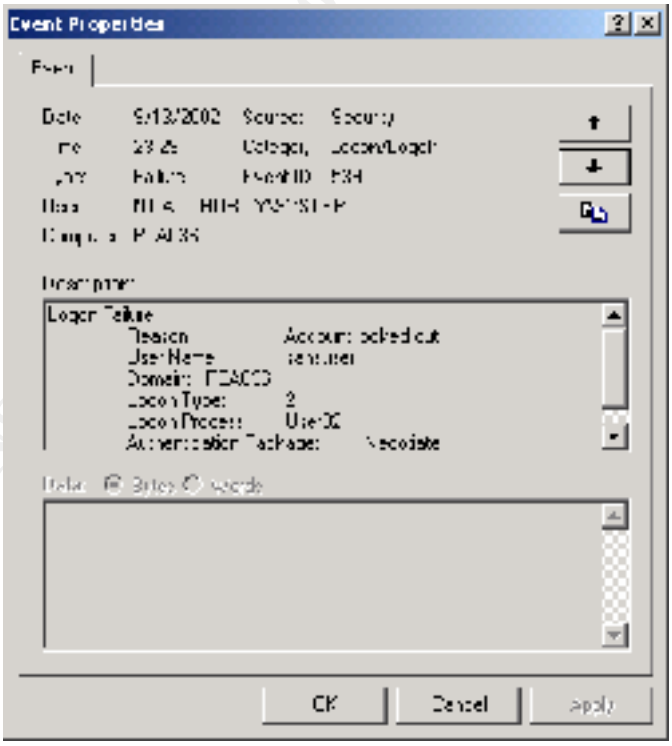

Figure 4 – Account Locked Out After 3rd Invalid Password Entry

Security Setting Test 3	***Computer Setting***	***Test Steps***	***Result***
Local Policy / User Rights Policy / Logon on locally	Administrators	1. Logon as Administrator. 2. Launch Computer Management and right click Users to bring up New User dialog box. 3. Create User name "sansuser". 4. Logout as Administrator. 5. Logon as "sansuser".	The "sansuser" is not permitted to logon locally (**Figure 5**).

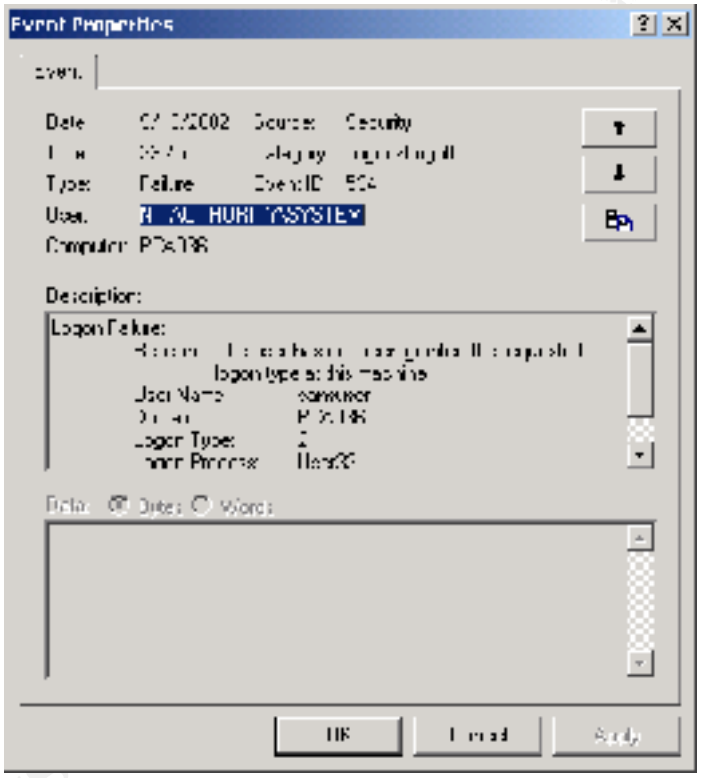

Figure 5 – Failure of User Account to Logon Locally

Security Setting Test 4	***Computer Setting***	***Test Steps***	***Result***
File System / Access to %SystemRoot%\repair directory	**Figure 6**	1. Logon as Administrator. 2. Launch Local Security Settings and right click Log on locally under Local Policies / User Rights Assignment. 3. Select Security… and add "sansuser" to Log on locally policy (Note: This is required in order to allow "sansuser" the ability to logon locally to verify this test). 4. Logout as Administrator. 5. Logon as "sansuser". 6. Launch Windows Explorer and click on C:\WINNT\repair folder.	The "sansuser" is not permitted to access to the C:\WINNT\repair folder (**Figure 7**).

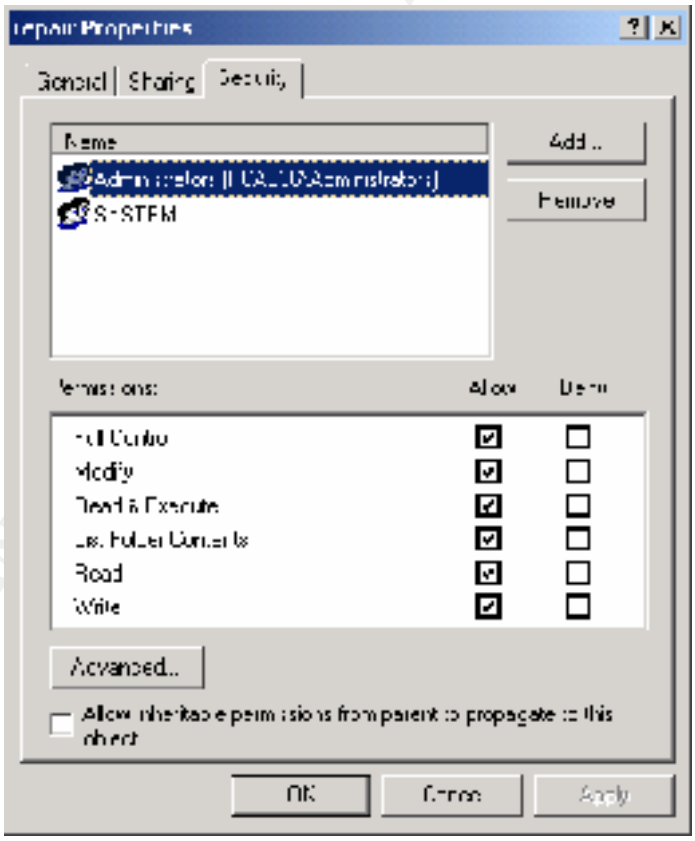

Figure 6 – Repair Directory Security Properties

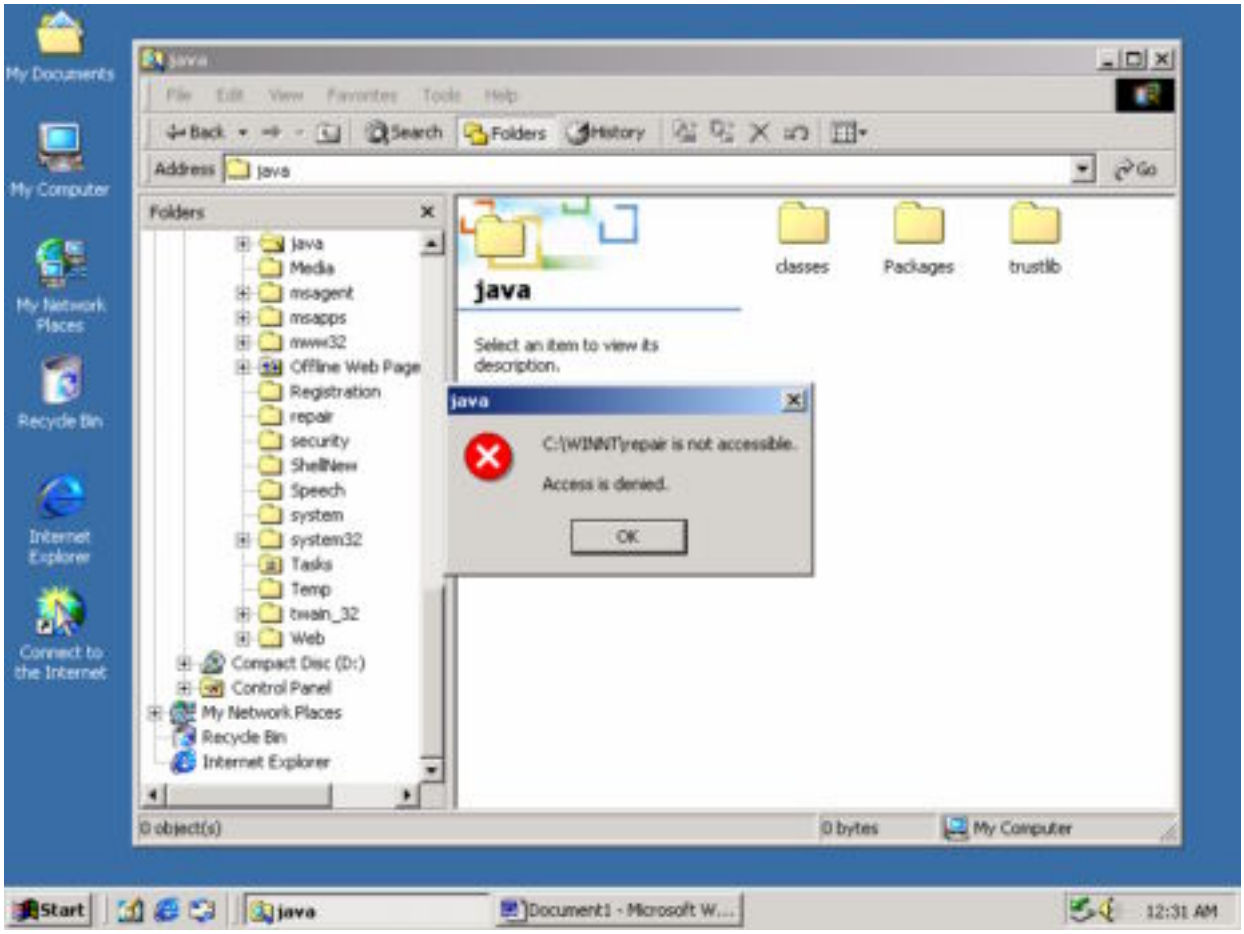

Figure 7 – Failure of User Account to Access C:\WINNT\repair.

5.3. Test the System's Functionality

Applying a security template can potentially cause the system not to function properly. The following four tests of the server's applications were conducted to confirm their functionality. **Note: Some of the images below have been modified. Any information considered sensitive (i.e. specific IP addresses and hostnames) has been omitted.**

System Functionality Test 1	***Test Steps***	***Observations / Results***
Remote Connectivity to Firewall Management Server (pca036) This is performed from a network attached Windows 2000 desktop via the Remote Desktop Connection tool (uses RDP) to firewall management server's terminal services.	1. Launch Remote Desktop Connection client on remote desktop. 2. Connect to firewall management server. 3. Login as Administrator. 4. Browse Checkpoint software directory with Windows Explorer **(figure 8).**	Access to the firewall management server was completed successfully. **Results:** No anomalies were detected. Remote connectivity functioned as expected.

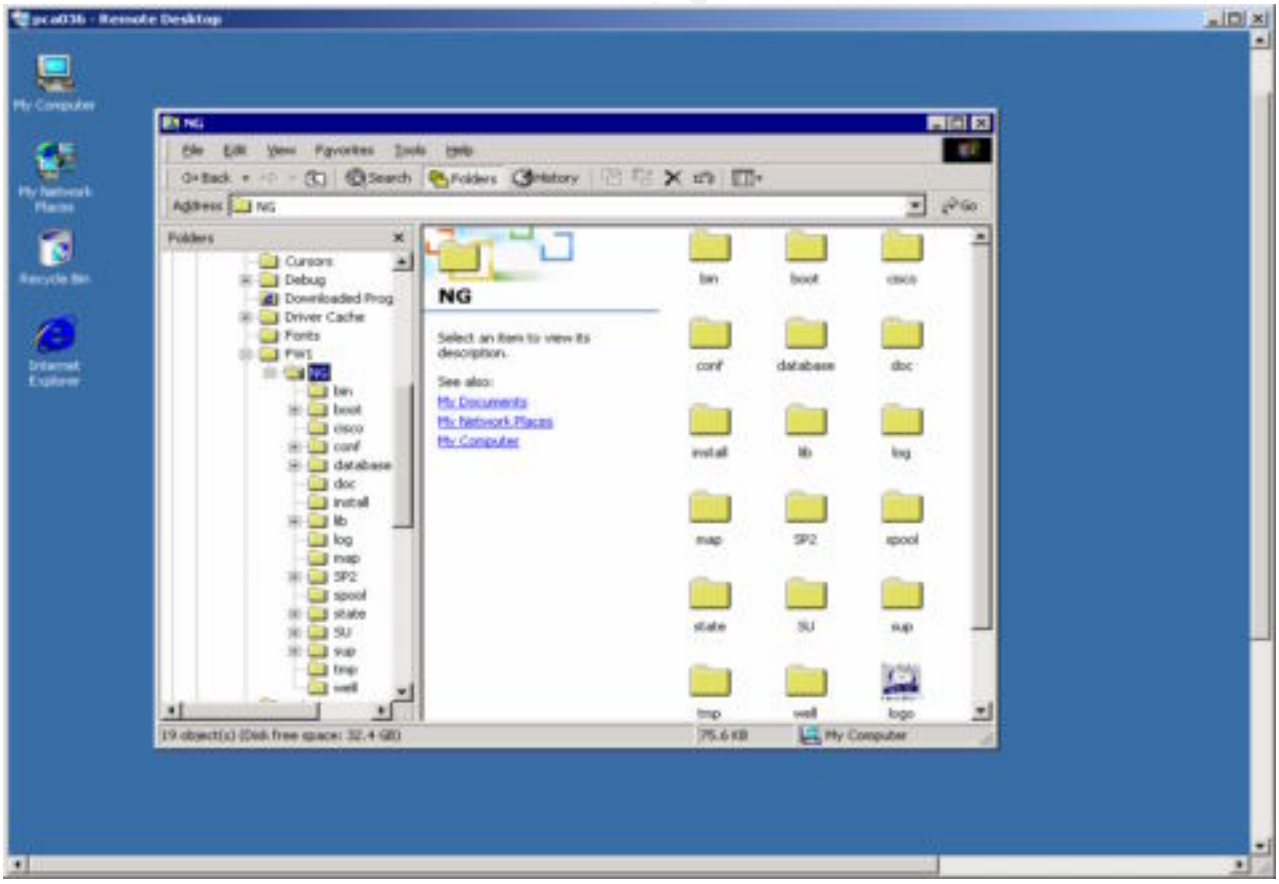

Figure 8 – Successful RDP Connection to Firewall Management Server

System Functionality Test 2	***Test Steps***	***Observations / Results***
Remote Connectivity to Firewall This is performed from the firewall management server by utilizing the F-Secure SSH client and establishing a connection to the firewall's sshd daemon.	1. Launch F-Secure SSH client. 2. Connect to firewall. 3. Logon to firewall admin account. 4. Set terminal type and get to logon prompt. 5. Logoff and disconnect SSH session.	Access to the firewall from the firewall management firewall was completed successfully. **Results:** No anomalies were detected. Remote connectivity functioned as expected.

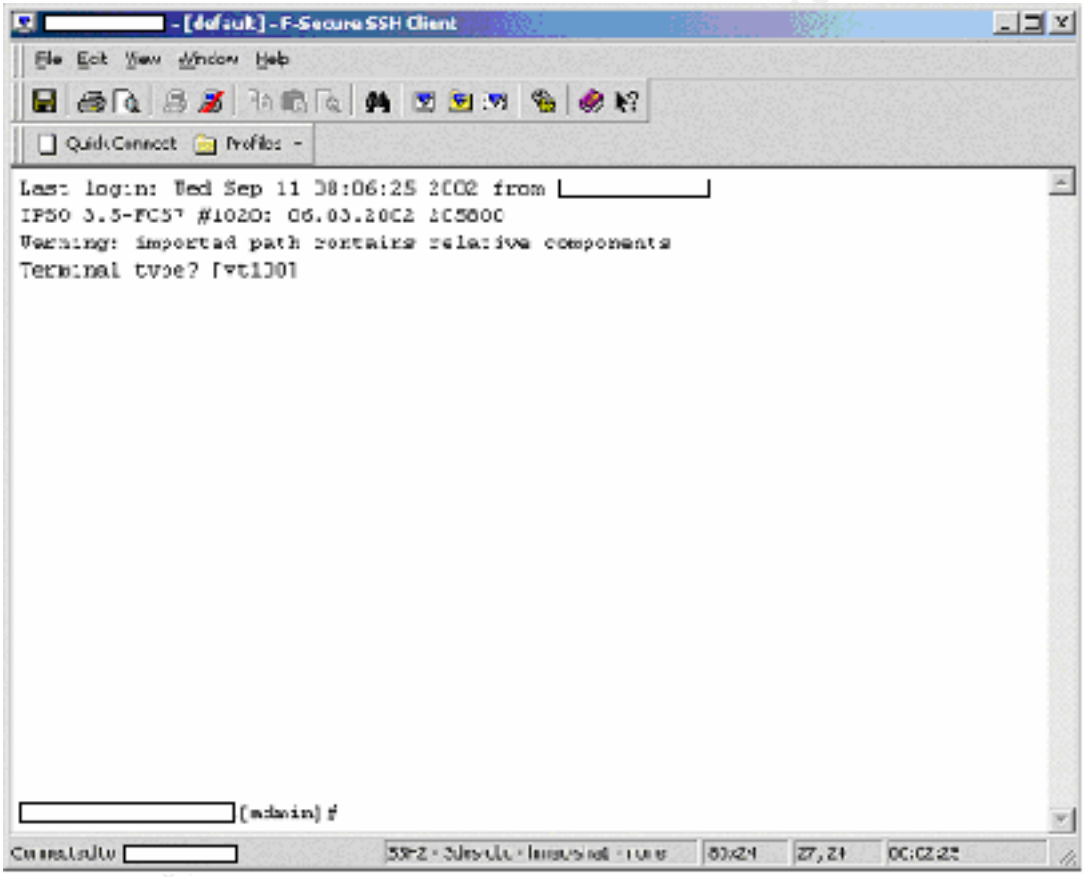

Figure 9 – Successful F-Secure SSH Client Connection to the Firewall

System Functionality Test 3	***Test Steps***	***Observations / Results***
Connectivity to Firewall Secure Web Management Site This is performed from the firewall management server by launching Internet Explorer and connecting and authenticating to the firewall web server.	1. Launch Internet Explorer and connect to the firewall. 2. Logon to admin account. 3. Connect to administration website and navigate through various links. 4. Close Internet Explorer.	Access to the firewall was completed successfully. **Results:** No anomalies were detected. Web connectivity functioned as expected.

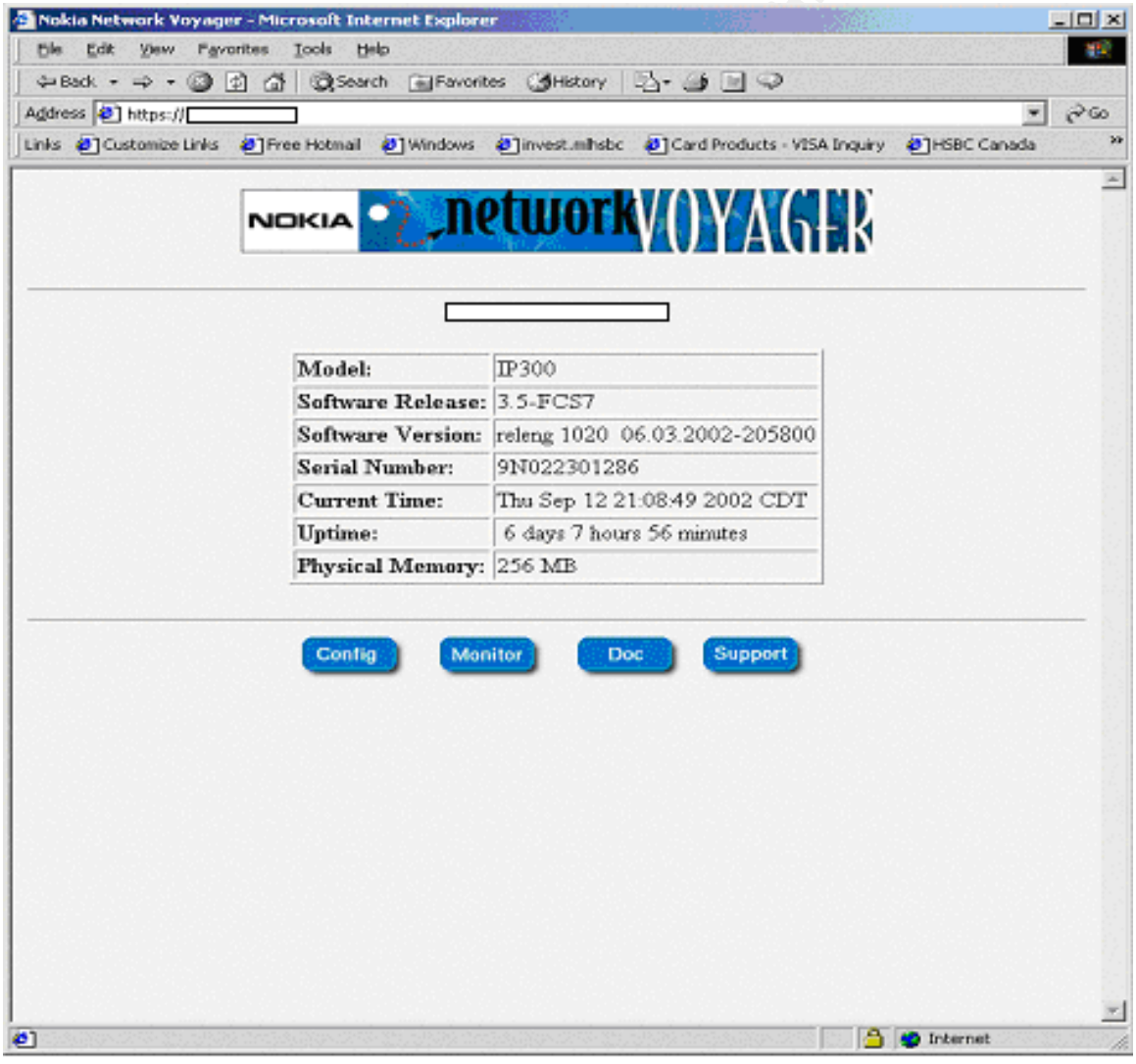

Figure 10 – Successful Connection to Firewall Secure Web Server

System Functionality Test 4	***Test Steps***	***Observations / Results***
Connectivity to Firewall via the Checkpoint GUI. This is performed from the firewall management server by launching the Checkpoint firewall management software that connects to the firewall. The GUI is used to manage the firewall rulebase.	1. Launch the Checkpoint firewall management GUI software. 2. Logon to the firewall with the admin account. 3. Verify the connection and examine the firewall's current "Standard" rulebase (**figure 11**). 4. Exit the Checkpoint GUI.	Access to the firewall and examination of the current loaded running rulebase was completed successfully. **Results:** No anomalies were detected. Checkpoint GUI connectivity functioned as expected.

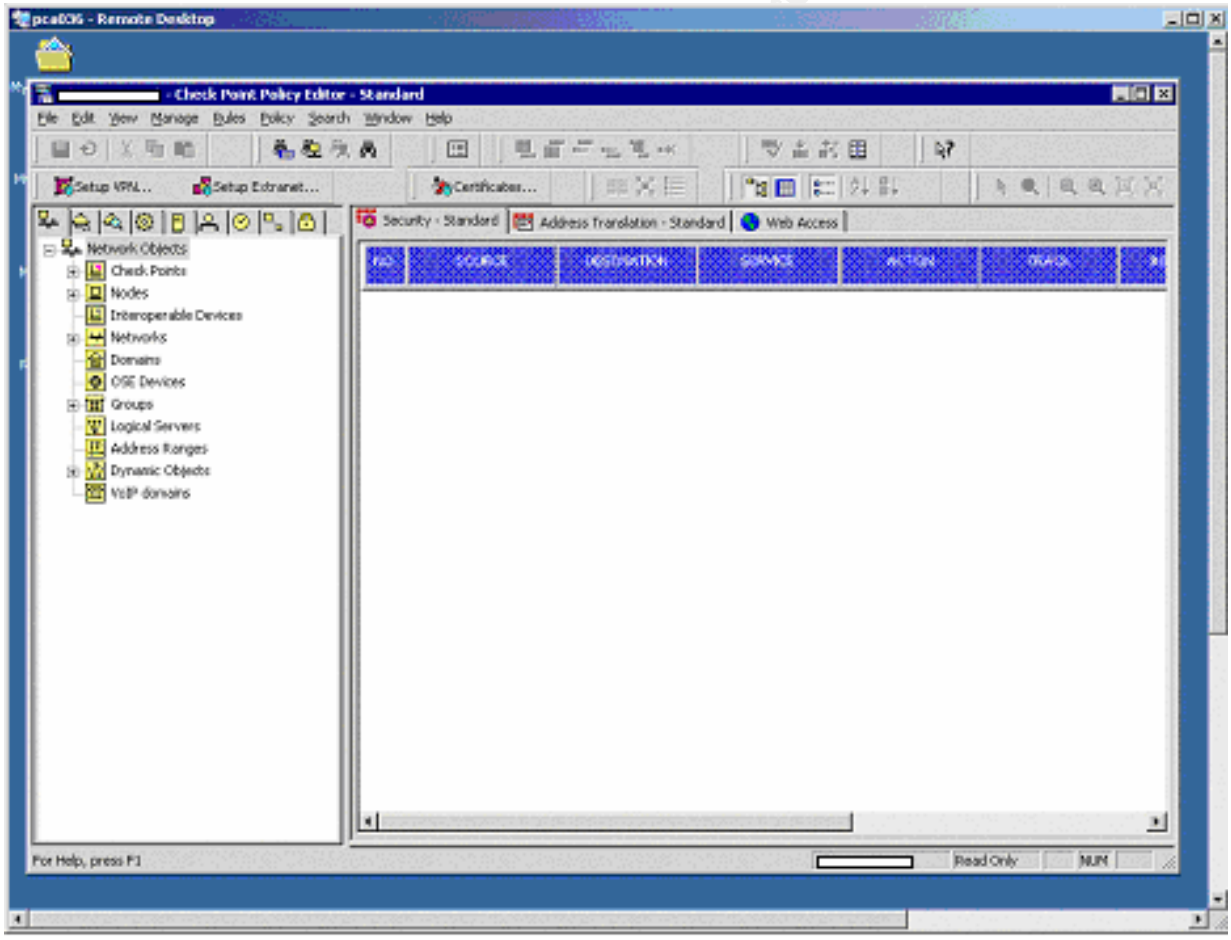

Figure 11 – Successful Connection to Firewall from Checkpoint GUI

5.4. Evaluate the Template

Default Security Provided by the Template

Based on the research and testing conducted, the default security provided by the w2k_server.inf template provides an acceptable starting point for hardening the Windows 2000 operating system on standalone and member servers. The follow-up step is to change this template to reflect the specific needs of the applications installed on the server and the types of users who require access. The template will also have to comply with any corporate security policies that may be relevant.

As noted in Section 2.3, System's Security Requirements, the risks that the firewall management server faces are rated as high. The following security settings are too weak and require tuning: Account Policies, Local Policies, Event Log, Restricted Groups, and Systems Services.

Policy	***Default Setting***	***Too Strong***	***Too Weak***	***Revised Setting***	***Explanation***
Account Policies / Password Policy					
Minimum password age	1 days		•	30 days	Increased to further restrict the repeated cycling through passwords.
Account Policies / Account Lockout Policy					
Account lockout duration	15 minutes		•	60 minutes	Increased to further restrict how long an account is locked out. Another considerations is setting the value to 0 which means an account is locked out until the Administrator unlocks it. However, this poses a new problem as a malicious user can lock out the account after the 3 repetitive tries thereby causing a denial of service attack.
Reset account lockout counter after	15 minutes		•	60 minutes	Increased to further restrict when an account lockout is reset.

Note: Even though this server only has the Administrator account configured, the above Account Policies are revised if the requirement for user accounts to be created is required. It is recognized these settings do not apply to the Administrator account. The Administrator account will never be locked out hence the importance of renaming the Administrator account (discussed below).

Policy	***Default Setting***	***Too Strong***	***Too Weak***	***Revised Setting***	***Explanation***
Local Policies / Audit Policy					
Audit object access	Failure		•	Success, Failure	Any object access and privilege use should be logged for either success or failure. This is a firewall management server and security activity should be logged. Care must be taken as increasing logging means increasing the amount of disk storage used.
Audit privilege use	Failure		•	Success, Failure	
Local Policies / User Rights Policy					
Access this computer from the network	Administrators, Users		•	Administrators	Only the Administrator is a valid user on this machine.
Bypass traverse checking	Users		•		Restrict users from viewing any server directory information.
Amount of idle time required before disconnecting session	30 minutes		•	99999	No SMB sessions should ever take place. Setting this value to the maximum value disables this setting.
Message text for users attempting to log on	Not defined		•	<Insert appropriate corporate message text here>	For legal reasons, anyone attempting to logon to this server needs to be warned about the ramifications of misusing company systems and that their actions may be audited.
Message title for users attempting to log on	Not defined		•	ATTENTION!	
Rename administrator account	Not defined		•	twotall	An account named "Administrator" provides a target for malicious users. Renaming this account is vital to the server's security.
Rename guest account	Not defined		•	jones	Rename this account to prevent a malicious user from targeting the default guest account name. Further to this, disable the guest account, as it is not needed.

Policy	***Default Setting***	***Too Strong***	***Too Weak***	***Revised Setting***	***Explanation***
Event Log					
Retain application log	Not defined		•	30	These values are increased to provide a useful amount of historical detail if required for any forensics. Ensure there is sufficient disk storage to hold 30 days worth of logs.
Retain security log	Not defined		•	30	
Retain system log	Not defined		•	30	
Retention method for application log	Not defined		•	Overwrite events by days	The following retention methods need to be set to "Overwrite events by days" in order to facilitate the retaining of logs by days.
Retention method for security log	Not defined		•	Overwrite events by days	
Retention method for system log	Not defined		•	Overwrite events by days	

The template made no changes to system services configuration. As noted in the NSA documentation for this template, this was not done since tuning services is environment and system specific. It is recommended to disable any unnecessary services that are not required as they take up system resources and can potentially open holes into the operating system. Consideration should be given to disabling the following services on the firewall management server:

Alerter
Computer Browser
DHCP Client
DHCP Server
Distributed Link Tracking Client
Distributed Link Tracking Server
Distributed Transaction Coordinator
DNS Client
DNS Server
Fax Service
File Replication
Indexing Service
Internet Connection Sharing
License Logging Service
Messenger
NetMeeting Remote Desktop
Network DDE
Network DDE DSDM
Print Spooler

QoS RSVP
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Registry Service
Removable Storage
Run as a Service
Simple Mail Transport Protocol (SMTP)
Smart Card
Smart Card Helper
Task Scheduler
TCP/IP NetBios Helper Service
Telephony
Telnet
Uninterruptible Power Supply
Windows Time
Workstation

A more secure solution is to completely remove (uninstall) any unnecessary services identified above which would prevent them from ever being started.

In terms of Restricted Groups, the Power Users group should be removed, as there is no requirement for this. The system only supports Administrators.

To further lockdown the Registry Keys, all occurrences of User Groups/Permissions DACLs with the exception of Administrators and SYSTEM could be removed. Again, the system only supports Administrators.

Similar to Registry Keys, all File System Folder and File entries with User Groups/Permissions DACLs other than Administrators and SYSTEM could also be removed.

Impact of Default Template on Applications and System

As observed in the testing, the default template did not adversely affect any application functionality or user accessibility to the system. Use of the primary applications, Checkpoint Firewall Management GUI, F-Secure SSH Client, Terminal Services, and Internet Explorer, displayed no anomalies or generated any errors.

Is the Template Enough to Secure the System?

Clearly, the answer is no. Although, this template (after being modified as detailed above) can be applied to secure the core functionality of the Windows 2000 operating system, there are many aspects of the server that are left unsecured. Securing a system is accomplished with a combination of the application of an appropriately configured template and the following:

- NetBIOS poses a security risk and is not required for the server's applications to run. Unbind NetBIOS from TCP/IP to prevent a malicious user from accessing the system by null session enumeration with tools such as NBTSTAT.

- Ensure the system time is synchronized to the same time source as other systems you are collecting logs from. This can be accomplished with the following command:

  net time /setsntp:"<insert time source here>"

- Utilize SCP ("Secure Copy" is part of SSH) to regularly transfer all logs being collected from firewall management server to a backup server running sshd.

- Ensure all application communication from the firewall management server is done via secure encrypted channel. This is already performed by the existing applications.

- Perform access control on any incoming TCP/IP network connections coming into the firewall management server on both NICs. This can be accomplished in one of three ways (Norberg, p. 85):

  - TCP/IP Security
  - Incoming Access Control Lists in the Routing and Remote Access Server (RRAS)
  - IPSec Policy agent via IPSec policy filters

  Allow only selected remote systems (by IP address and port) to connect to the firewall management server on the internal NIC (on the management network). Only allow the firewall IP address access to specific ports on the external NIC.

- The NSA has produced an additional template, sceregvl.inf (http://nsa2.www.conxion.com/win2k/guides/inf/w2k_server.inf), that introduces several new security options. This template should be downloaded and investigated.

6. References

1. Fossen, Jason, 5.1 Windows 2000/XP: Active Directory and Group Policy, Version 5.2, SANS Institute, January 9, 2002.

2. Haney, Julie M., Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set, Version 1.1, National Security Agency, URL: http://nsa2.www.conxion.com/win2k/guides/w2k-3.pdf, January 22, 2001

3. Microsoft, "Security Settings", URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/563.asp, 2002

4. Morris, Jason, "Step-By-Step Guide To Securing Windows 2000 Server Using the Security Configuration & Analysis Tool", URL: http://www.giac.org/practical/Jason_Morris_GCNT.doc, March 2001.

5. Norberg, Stefan, Securing Windows NT/2000 Servers for the Internet, Sebastopol, O'Reilly, January 2001.

6. Robichaux, Paul, Managing the Windows 2000 Registry, O'Reilly, August 2000

7. Scanbray, Joel and Stuart McClure, Hacking Windows 2000 Exposed: Network Security Secrets & Solutions, McGraw Hill, September 2001

7. Appendix A – w2k_server.inf Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       W2k Server.INF
; Template Version:    05.00.DR.0000
;
; Revision History
; 0000  -          Original
; May 2001 - SNAC version 1.01a
; November 2001 -
;          Changed the line "RequireLogonToChangePassword = 1" to
;          "RequireLogonToChangePassword = 0" under the [System Access]
;          section. This line is an artifact from Windows NT 4.0 templates and could have
;          adverse effects on a user's ability to change password at first logon. If you have
;          experienced this problem, please reapply this corrected inf file, or, via a
;          text editor, create and apply an inf file with only the following lines:
;          [Unicode]
;          Unicode=yes
;          [System Access]
;          RequireLogonToChangePassword = 0

;
;          NOTE: This setting does NOT appear when the template file is viewed graphically in
;          the MMC.
;
; ; July 2002 -
;          In the Registry section, corrected the
;          MACHINE\System\CurrentControlSet\Control\Wmi\Security to grant Administrators Full
;          Control on the key and subkeys
;
; Warning : Care should be exercise When using this template on Exchange Server platform.
;          Additional settings and modification to these settings are required, which are site specific.
;          No general .INF templates are available for Exchange Server on Windows 2000 at this
time.


[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 0
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
```

```
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 1
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-545,*S-1-5-32-544
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
```

```
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege =
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Registry Values]
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=
4,1
machine\software\microsoft\driver signing\policy=3,1
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,
1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\print\providers\lanman print
services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\session manager\memory
management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,
1
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,
0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassw
ord=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignatur
e=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignatu
re=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=
4,255
[Profile Description]
Description=NSA Enhanced Security for Windows 2000 Member/Stand-alone Servers
```

[File Security]
"%SystemDrive%\Program Files\Resource Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"c:\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\CSC",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCSWWPLO;;;BU)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDrive%\Documents and Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\My Download Files",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1201bf;;;BU)"

"%SystemDrive%\System Volume Information",1,"D:PAR"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DC
LCWP;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x120
0a9;;;BU)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;B
U)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;;CCDCWP;;;B
U)(A;OIIO;DCLC;;;BU)"
"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;O
ICIIO;DCLCWP;;;BU)(A;OICI;CCSWWPLORC;;;BU)"
"%SystemDirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Inetpub",1,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI
;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1301bf;;;BU)"
"%SystemRoot%\Offline Web Pages",1,"D:AR(A;OICI;FA;;;WD)"
"%SystemDrive%\Documents and Settings\All
Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
[Registry Keys]
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWRPSDRC;;;BO)(A;
CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"
"machine\software\microsoft\windows
nt\currentversion\perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows\currentversion\group
policy",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;
SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\policies",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;
AU)(A;CI;KA;;;SY)"
"machine\system",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\clone",1,"D:AR"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"

"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR
;;;BU)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;KA;;;BA)(A;;
KR;;;BO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\control\wmi\security",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO
)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\enum",1,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\hardware
profiles",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers",2,"D:P
AR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities",2,"D:PA
R(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"

Last Updated: May 27th, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
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 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**