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 permited without express written permission.

Validating Patch Levels and Baseline Configuration on Windows 2000 Professional Workstations:
An Auditor's Perspective

GSNA Practical Assignment
Version 3.0 (January 9, 2004)

Author: William Rybczynski
Date: 25 April 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

GSNA 3.0

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

GSNA 3.0

Introduction:

The XYZ Corporation is a medium sized business that has begun working with the Department of Defense. They have just landed their first contract with DoD and have requested an independent audit by NetSecPros Consulting of the user workstations at one of their branch offices, Branch X. This audit has been requested by the Corporate Headquarters to ensure that the established baseline configuration for Windows 2000 Professional is currently in place. Additionally, the headquarters mandates a patch level for all branches based on the DISA Windows 2000 Security Checklist, Appendix B (ref 1). This is part of the organization's overall security policy to ensure that all user systems are similarly configured and patched which supports their overall configuration management program. The headquarters' wants to validate the current patch level at each branch as reported by each branch IT Department's patch management system. Current policy dictates that branches found to be non-compliant may be disconnected from the enterprise until patch levels have been verified.

Additionally, XYZ Corporate management has ask NetSecPros to develop an audit methodology that will be used by other auditors within the organization to conduct audits of other branch offices. The checklist will be detailed and organized into 2 categories: Baseline Configuration and Patch Management. The average number of systems to be validated is 10 per branch office.

Research in Audit, Measurement Practice and Control

Identify the system to be audited:

The XYZ Corporation is part of a critical communications network that conducts worldwide operations on a continuous basis. The user workstations are required for constant support of these worldwide operations.

NetSecPros will conduct an audit of the Windows 2000 Professional Workstations in use at Branch X to determine if they meet two critical objectives:

1. Are the Windows 2000 Professional Workstations operating in accordance with the established baseline configuration as set forth by the XYZ Corporation?
2. Does the actual patch level on these systems accurately reflect what has been reported by the Branch X IT Department to the XYZ Corporation?

This will help identify if the patch management system in use by XYZ Corporation is functioning and reporting properly. Currently, the branch reports 100% compliance on all required security patches.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Expected Workstation baseline and patch level are outlined in the table below:

Operating System	Windows 2000 Professional
Processor	Intel Based
OS Service Pack Level	SP4
Patch Level	All Critical MS Patches for Win2K Pro
Browser	Internet Explorer 6.0
Browser Service Pack Level	SP1
Anti-Virus	Symantec Anti-Virus Corporate Edition

Description of Windows 2000 Professional

> Windows 2000 Professional is the Windows operating system for business desktop and laptop systems. It is used to run software applications, connect to Internet and intranet sites, and access files, printers, and network resources.
>
> Built on Windows NT® technology and the easy-to-use, familiar Windows® 98 user interface, Windows 2000 Professional gives business users increased flexibility. The integrated Web capabilities let you connect to the Internet from anywhere, at anytime—giving your company access to host of flexible, cost-effective communications options. In addition, broad peripheral and mobile computer support make Windows 2000 Professional an ideal operating system for a workforce that increasingly relies on notebook computers. Further, your support and administrative staff will particularly appreciate the reliability and manageability enhancements that make desktop management simpler and more efficient. (ref 2)

Description of Symantec Anti-Virus Corporate Edition

Comprehensive virus protection for enterprise workstations and network servers

> Symantec AntiVirus Corporate Edition provides scalable, cross-platform virus protection for workstations and network servers throughout the enterprise.

Key Features:

- Provides advanced, enterprise-wide virus protection and monitoring from a single management console
- NEW! Expanded Threat Detection and Threat Categorization recognizes unwanted applications
- such as spyware and adware

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- NEW! Threat Tracer identifies the source of blended threat attacks that spread via open file shares (e.g. Nimda)
- NEW! Outbound email worm heuristics prevent client systems from spreading worms via email
- NEW! Internet Email Attachment Scanning of incoming emails delivered through POP3 mail clients such as Microsoft® Outlook®, Eudora®, and Netscape Mail (ref 3)

Evaluate the most significant risk to the system:

"How likely is it that something like this could happen to the branch office?" This is the question that was asked when determining the level of risk that the corporation's systems may be exposed to. The following is a listing of the most significant risks to the XYZ Corporation's systems.

1. Compromise of a system may result in unauthorized disclosure of critical data.
2. Failure to meet the baseline configuration may result in users being granted unauthorized access to data outside their scope.
3. Failure to meet the baseline configuration may result in users having higher access permissions on their workstations. If a user has administrator rights on the local machine, he may install unauthorized or malicious software.
4. Failure to maintain mandatory patch levels can result in the enclave being disconnected from the enterprise network. If this occurred, the enclave would loose its ability to support worldwide operations.
5. Failure to meet mandatory patch levels may result in system compromise due to an adversary exploiting a known vulnerability.
6. Failure to maintain current virus signatures may result in system compromise and loss of system services.
7. Backdoor programs may be installed on the system due to lack of effective configuration controls due to the system not meeting the configuration baseline.
8. Compromise of a system due to poor security practices may provide an adversary with a point of entry into the enclave and possibly the enterprise systems.
9. The enterprise patch management system may not be as reliable as it appears. This may indicate that there are a large number of false positives or negatives when the IT Dept reports patch compliance.
10. Failure to properly maintain systems backups may result in the inadvertent and irreparable loss of data.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

What is the current state of practice?

Branch X is directed to maintain the baseline configuration established by Corporate Headquarters. The baseline was developed based on the NIST (Computer Security Division) System Administration Guidance for Windows 2000 Professional (ref 4). Patch levels for all Windows 2000 Professional systems are also directed by Corporate Headquarters. Information on necessary system patches is obtained by referencing the DISA Windows 2000 Security Checklist Appendix B (Information Assurance Vulnerability Management (IAVM) NOTICE COMPLIANCE) (ref 1), which identifies the required patches for DoD systems. Additionally, the primary resource used by the XYZ Corporate IT Department for daily patch alerts is the US CERT mailing list for Cyber Security Alerts and Cyber Security Bulletins (http://www.us-cert.gov/cas/index.html). Because the XYZ Corporation has begun to work extensively with the Department of Defense, they feel that their systems should meet the same security requirements as their DoD counterparts.

The NIST (National Institute of Standards and Technology) Computer Security Division's mission …is to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs:
  - to promote, measure, and validate security in systems and services
  - to educate consumers and
  - to establish minimum security requirements for Federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation. (ref 5)

How the NIST Security Guide was developed:

The special publication was developed by NIST. NIST started with some excellent material developed by the National Security Agency (NSA) and the Security Community. The NIST security templates development were initially based in part on the National Security Agency's (NSA) Win2K Pro guidance. NIST examined the NSA settings and guidance and built on the excellent material they developed. NIST conducted extensive analysis and testing of the NSA settings, substantially extended and refined the NSA template settings, and developed additional template settings. NIST developed detailed explanatory material for the template settings, Win2K

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

> Pro security configuration, and application specific security configuration guidance. Subsequently, NIST led the development of a consensus baseline of Win2K security settings in collaboration with the public and private sectors, specifically NSA, Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), and the SysAdmin Network Security Institute (SANS). Microsoft also provided valuable technical commentary and advice. GSA also reviewed and concurred with the baseline. The consensus settings are reflected in the NISTWin2kProGold.inf security template. (ref 6)

The XYZ Corporation chose to use the NIST Windows 2000 Guide because it is based on the same materials that are used to establish the standards for configuration security guides within the Department of Defense.

When researching the required patches listed in the DISA Windows 2000 Security Checklist Appendix B some additional resources include:

- SecurityFocus.com http://www.securityfocus.com
- Microsoft Security http://www.microsoft.com/security
- CERT Vulnerabilities, Incidents & Fixes http://www.cert.org/nav/index_red.html
- SANS @ Risk Consensus Security Alert Newsletters http://www.sans.org/newsletters/risk/

Create an Audit Checklist

Using information from the NIST Systems Administration Guide for Securing Windows 2000 Professional Systems, the DISA Windows 2000 Security Checklist and Appendix B of the DISA Checklist, I was able to develop an audit checklist that can account for both the baseline configuration guidelines for Branch X, as well as, the required Windows 2000 Professional patches.

The DISA Windows 2000 Security Checklist, in it's entirety is available from the National Institute of Standards and Technology, Computer Security Resource Center at http://csrc.nist.gov/pcig/cig.html The settings audited for the XYZ Corporation are based on those listed in the NIST publication as well as those that are applicable from the DISA Checklist when a more comprehensive understanding of the settings or vulnerability was required. When using the audit checklist to determine if the systems meet the adequate patch level I referred to the DISA Checklist Appendix B. (Note: The DISA Checklist is updated on a monthly basis and should be downloaded and reviewed after an update has been published. Any new items should be added to this audit checklist as required.)

The DISA Checklist was developed from the following referenced documents available in PDF format from the National Security Agency at (http://nsa2.www.conxion.com):

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- *Addendum to the NSA Guide to Securing Microsoft Windows NT Networks* and *NSA Guides to Securing Windows 2000.* Version 3.1, Field Security Operations (FSO)/Defense Information Systems Agency (DISA)
- *Guide to Securing Microsoft Windows NT Networks.* Version 4.2. Systems and Network Attack Center (SNAC)/National Security Agency (NSA). C4-001R-00
- *Guide to Securing Microsoft Windows 2000 Active Directory.* Version 1.0 Network Security Evaluations and Tools Division or the Systems and Network Attack Center (SNAC)/National Security Agency (NSA). C4-056R-00
- *Guide to Securing Microsoft Windows 2000 File and Disk Resources.* Version 1.0. Field Security Operations Agency (DISA) and the Systems and Network Attack Center (SNAC)/National Security Agency (NSA). C4-009R-01
- *Guide to Securing Microsoft Windows 2000 Group Policy.* Version 1.1. Network Security Evaluations and Tools Division or the Systems and Network Attack Center (SNAC)/National Security Agency (NSA). C4-007R-01
- *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set.* Version 1.2. Network Security Evaluations and Tools Division or the Systems and Network Attack Center (SNAC)/National Security Agency (NSA). C4-052R-00

The XYZ Corporation has requested that the audit checklist be developed for the future use of their own team of auditors. The focus is to determine if:

- current desktop configurations are within the baseline parameters for security.
- the patch management system is actually patching the systems.

Because of the small number of systems at each branch office, the audit checklist will focus on those steps that can be taken by the auditor sitting at the workstation with administrative rights.

The top row is the Security Checklist Item Number that can be used for cross-referencing when the auditor is conducting the assessment/audit and compiling his information.

The Threat row defines what the auditor is checking.

The Reference row details where the threat information was found. Explanations and definitions are from the references noted.

The Risk Item Associated row details the risk to the XYZ Corporation as outlined on page 4.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Risk Result row details what the risk is to the system or organization if the threat is not corrected or mitigated.

The Test Procedure - Compliance row details what the testing procedure and/or compliance criteria is to validate that the threat item exists.

The S/O row shows whether the test in the Procedure – Compliance column is subjective (S) or objective (O).

The Evidence/Findings row gives the auditor a place to record his findings for each Security Checklist Item.

The audit checklist is also divided into 2 sections, Baseline Configuration and Patch Management.

Baseline Configuration Audit

System Services Security Item Number 1 (SSS1)	
Threat	The Telnet service is installed.
Reference	NIST Security Administration Guidance for Windows 2000 Professional (p. B-14)
Risk Item	1,2,7,8
Risk Result	If compromised, services may offer direct access to system resources or fall victim to buffer overflows or denial of service attacks. If a service is not required it should be disabled.
Test Procedure – Compliance	1. Open the Computer Management Console a. Right click on My Computer b. Select Manage 2. Expand the Services and Applications object in the tree window 3. Select the Services Object 4. Review the Telnet entry in the services list to determine if it is disabled.
S/O	Objective
Evidence/Findings	
System Management Item Number 1 (SM1)	
Threat	Emergency Repair Disk(s) (ERD) or System information backups are not created, updated, and protected.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. ES-2)
Risk Item	10
Risk Result	Failure to create and periodically update the ERD

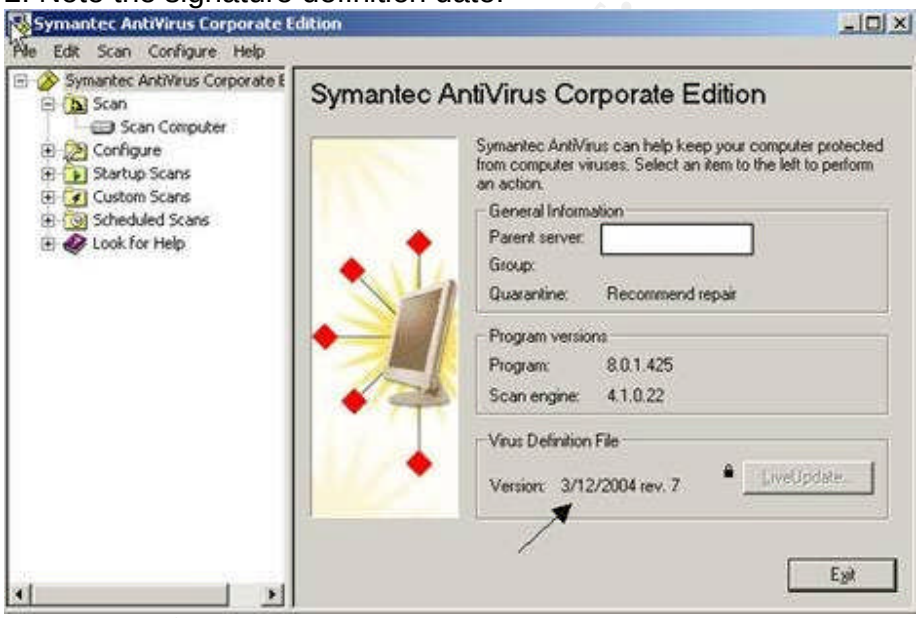
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	will prevent you from being able to successfully recover from system crashes related to bad registry data, corrupted or missing files on the system partition, and a corrupt Kernel, which is the core of the Windows 2000 OS.
Test Procedure – Compliance	1. Ask the SA for the ERD. 2. If no ERD is found, complete the following steps: a. Insert a 3.5 inch, 1.44 MB floppy in disk drive A:. b. Select START→PROGRAMS→ ACCESSORIES→SYSTEM TOOLS→BACKUP c. Select the Emergency Repair Disk button d. On the ERD window check "Also backup the registry to the repair directory" e. Click YES f. Store the disk in a safe and secure place.
S/O	Objective/Subjective
Evidence/Findings	

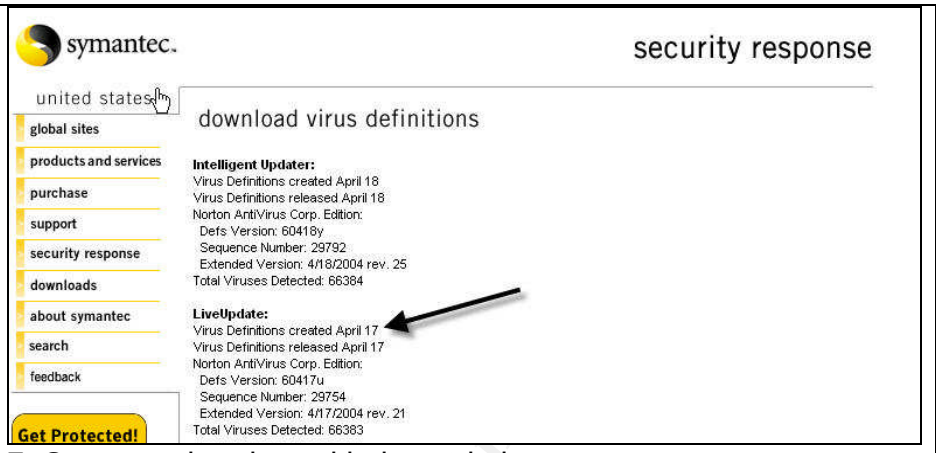
System Management Item Number 2 (SM2)	
Threat	Anti-virus is not installed and enabled.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. ES-3)
Risk Item	4,5,7,8
Risk Result	Failure to have approved anti-virus installed opens the system and interconnected systems to the threat of malicious code and trojan horses.
Test Procedure – Compliance	1. Norton Anti-Virus is the approved program for XYZ Corp. 2. Open the Computer Management Console a. Right click on My Computer b. Select Manage 3. Expand the Services and Applications object in the tree window 4. Select the Services Object 5. Symantec Antivirus Client should appear in the services list. 6. The Startup setting should be Automatic. 
S/O	Objective
Evidence/Findings	

System Management Item Number 3 (SM3)	
Threat	Anti-virus signatures are not up-to-date.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Reference	NIST System Administration Guidance for Windows 2000 Professional (p. ES-3)
Risk Item	6
Risk Result	Anti-virus signatures must be current to protect against new threats from malicious code.
Test Procedure – Compliance	1. Open the anti-virus program. 2. Note the signature definition date.  3. Open a web browser. 4. Go to www.symantec.com 5. Select Download Virus Definitions  6. Confirm latest Live Update Signature date

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	 7. Compare that date with the anti-virus program.
S/O	Objective
Evidence/Findings	Anti-Virus signatures are/are not up-to-date.

System Management Item Number 4 (SM4)	
Threat	Local volumes are not formatted using NTFS.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. 6-1)
Risk Item	2,3
Risk Result	All volumes must use NTFS to achieve the highest level of security. For Windows 2000, only NTFS supports Discretionary Access Control to the directories and files.
Test Procedure – Compliance	1. Open the Computer Management Console a. Right click on My Computer b. Select Manage 2. Expand the Storage Object in the Tree Window 3. Select the Disk Management Object 4. Check the File System column to see if all volumes are NTFS.
S/O	Objective
Evidence/Findings	Local Volumes are/are not formatted for NTFS.

Note: To test the following items the Microsoft Management Console is used. Refer to Microsoft Knowledge Base Article – 300549 for an in depth explanation on the use of MMC (ref 8) The MMC is the primary system configuration tool for Windows 2000. The MMC uses “Snap-ins” to configure various parts of the system. (ref 7) The XYZ Corporation has mandated that all systems will be

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

configured with the NIST baseline (NISTWin2KproGold.inf). To audit the configuration of the Branch X Windows 2000 Professional systems, I am using the Security Configuration and Analysis snap-in, which permits the analysis of the following items:

- Account Policy
- System Auditing
- Local Policies
- Event Logs
- Services
- Registry ACLs and Auditing
- File ACLs and Auditing.

Account Policy Management Item Number 1 (APM1)	
Threat	Password History is not enforced
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. 9-7)
Risk Item	8
Risk Result	Users tend to cycle through their favorite passwords. Enforcing password history at the accepted configuration helps reduce the likelihood that this will occur.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Password Policy 3. Enforce Password History 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 2 (APM2)	
Threat	Maximum password age does not meet minimum requirements.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. 9-7)
Risk Item	8
Risk Result	Having a maximum password age ensures that users change their passwords on a regular basis.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Password Policy 3. Maximum Password Age 4. Compare the Computer Setting to the Database Setting to determine if they match.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 3 (APM3)	
Threat	Minimum password age does not meet minimum requirements.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. 9-7)
Risk Item	8
Risk Result	Having a minimum password age ensures that users cannot cycle through their passwords to keep a particular password.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Password Policy 3. Minimum Password Age 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 4 (APM4)	
Threat	Minimum password length does not meet minimum requirements.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. 9-7)
Risk Item	8
Risk Result	The minimum password length increases the possibility that the password will be difficult to crack if the encrypted copy is compromised.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Password Policy 3. Minimum Password Length 4. Compare the Computer Setting to the Database Setting to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 5 (APM5)	
Threat	Password does not meet complexity requirements
Reference	NIST Systems Administration Guidance for Windows 2000 Professional (p. 9-7)
Risk Item	8
Risk Result	A user's password must meet the complexity requirement to ensure that it is not the same as the user's account name, is at least 8 characters long, and contains characters from three of the following four categories: upper case characters, lower case characters, numbers and special characters (!, #, @, %).
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Password Policy 3. Password must meet complexity requirements 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 6 (APM6)	
Threat	Passwords are stored using reversible encryption for all users on the domain
Reference	NIST Systems Administration Guidance for Windows 2000

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Professional (p. 9-7)
Risk Item	8,1,2
Risk Result	If the user passwords are stored using reversible encryption, then that are stored in clear text versions that can easily be read by malicious individuals.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Password Policy 3. Store passwords using reversible encryption for all users in the domain 4. Compare the Computer Setting to the Database Setting to determine if they match. This setting should NOT be enabled. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 7 (APM7)	
Threat	The account lockout duration does not meet the minimum standard.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. B-3)
Risk Item	1,2,8
Risk Result	If the account lockout duration is not set, a hacker could continue to attempt to crack the user's account indefinitely.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Account Lockout Policy  3. Account lockout duration 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 8 (APM8)	
Threat	The account lockout threshold does not meet the minimum standard.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. B-3)
Risk Item	1,2,8
Risk Result	If the account lockout threshold is not set, a hacker could continue to attempt to crack the user's account indefinitely.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Account Lockout 3. Account lockout threshold 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Account Policy Management Item Number 9 (APM9)	
Threat	The "reset account lockout counter after" setting does not meet the minimum standard.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. B-3)
Risk Item	1,2
Risk Result	If the user's account does not lockout after a set number of failed logon attempts, a hacker could continue to attempt to crack the user's account indefinitely. Users should be required to contact an administrator to unlock their account.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Account Lockout Policy 3. Reset account lockout counter

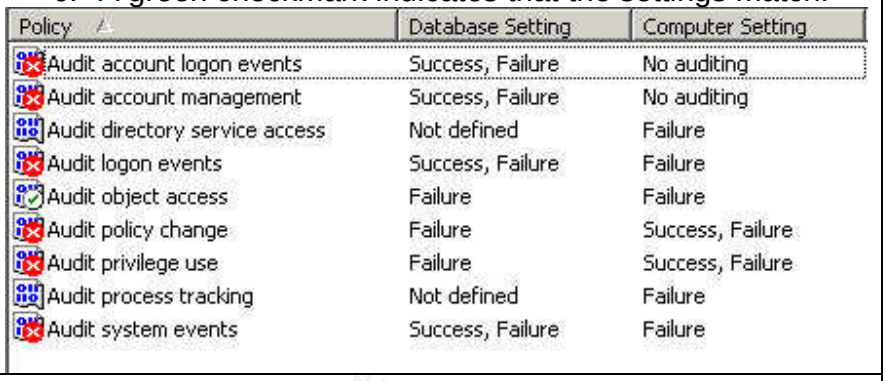
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	after 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective
Evidence/Findings	

Local Policy Management Item Number 1 (LPM1)	
Threat	Auditing is not enabled.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. B-4)
Risk Item	1,2
Risk Result	Failure to enable auditing prevents the organization from monitoring and recording individual system activity and possible malicious compromises.
Test Procedure – Compliance	In the MMC window select 1. Local Policies 2. Audit Policies  3. Review audit policy items to determine if auditing is enabled. If the Computer Setting column shows No Auditing, then it is not enabled for that item.
S/O	Objective
Evidence/Findings	Auditing is/is not enabled.

Local Policy Management Item Number 2 (LPM2)	
Threat	System-auditing configuration does not meet minimum requirements.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. B-4)
Risk Item	1,2
Risk Result	Failure to enable the minimum standard for system auditing prevents the organization from monitoring and recording system activity and possible malicious compromises.
Test Procedure – Compliance	In the MMC window select 1. Local Policies

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	2. Audit Policies 3. Review audit policy items to determine if auditing is enabled correctly. 4. All items listed should be set for either “failure” or “success, failure” 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match. 
S/O	Objective
Evidence/Findings	Auditing is/is not enabled correctly. List the items not audited correctly:

Policy	Database Setting	Computer Setting
Audit account logon events	Success, Failure	No auditing
Audit account management	Success, Failure	No auditing
Audit directory service access	Not defined	Failure
Audit logon events	Success, Failure	Failure
Audit object access	Failure	Failure
Audit policy change	Failure	Success, Failure
Audit privilege use	Failure	Success, Failure
Audit process tracking	Not defined	Failure
Audit system events	Success, Failure	Failure

Security Options Management Item Number 1 (SOM1)	
Threat	Anonymous shares or null sessions are not restricted.
Reference	NIST System Administration Guidance for Windows 2000 Professional (p. B-6)
Risk Item	1,2,3,7
Risk Result	Failure to restrict anonymous access or null sessions to the system allows unauthenticated users to enumerate shares and list account names.
Test Procedure – Compliance	In the MMC window select 1. Account Policies 2. Security Options 3. Additional restrictions for anonymous connections 4. Compare the Computer Setting to the Database Setting to determine if they match. 5. A red X indicates that the settings do not match. 6. A green checkmark indicates that the settings match.
S/O	Objective

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Evidence/Findings	

This listing of auditable items is not exhaustive. Additional settings are listed in the NIST Systems Administration Guidance for Windows 2000 Professional (ref #) Appendix B, NIST Windows 2000 Security Templates.

Patch Management Audit

The XYZ Corporation has instituted a company wide policy that requires all branch offices to meet a required patch level. In an effort to ensure that that their systems are meeting the same security patch requirements as their DoD counterparts, and to simplify patch distribution, each branch office is using Microsoft System Management Server (SMS) for security patch distribution to their Microsoft Windows 2000 Professional Workstations and Servers (if applicable.) The Department of Defense tracks their information assurance vulnerability management (IAVM) program by issuing several different types of notices to the DoD community. For patches that are deemed critical for a system, the notice is issued as an Information Assurance Vulnerability Alert. All IAVAs must be patched within a predetermined timeframe throughout DoD. For patches that are not considered critical, but still required on a system, Information Assurance Vulnerability Bulletins or Technical Advisories are issued. DoD CERT then tracks the patch compliance for units by correlating a DOD CERT Number with a known vulnerability in their Vulnerability Compliance Tracking System (VCTS).

Branch IT personnel have reported a number of problem getting the patches to deploy properly and company management is concerned that their systems are not actually at the patch level reported by the various branch IT departments.

The patch management portion of this auditing checklist is based on the DISA Security Checklist Appendix B. The DISA Security Checklist is updated on a monthly basis. For ease of use I have taken the information provided in DISA Checklist Appendix B and organized it by system component (Operating System and Application Type) and Microsoft Security Bulletin Number. The Appendix has the patches separated by DOD-CERT Numbers and then lists the MS Bulletin numbers. The following checklist items are organized so that they can be updated with new information as it is released. I have provided an example of the patch information found in Appendix B and my corresponding checklist item.

Appendix B Example

DOD-CERT Number	Platform / Application	Description	Patch Information
			Verification (🖷=verified by WIN2K SRR script)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

DOD-CERT Number	Platform / Application	Description	Patch Information Verification (🖶=verified by WIN2K SRR script)
2002-A-SNMP-003 (Applies only to machines on which SNMP is installed)	WIN2K	Multiple Simple Network Management Protocol Vulnerabilities	Microsoft Security Bulletin MS02-006, Microsoft Download site http://www.microsoft.com/technet/security/bulletin/MS02-006.asp 🖶 Verify that the Hot Fix has been applied by confirming that the following registry key has been created: HKLM\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q314147 or Verify that Service Pack 3 or greater is installed (Manual): (Using START -> Run, execute "winver.exe".)
2002-A-SNMP-005 (Applies only to machines on which SNMP is installed)	WIN2K	Multiple Simple Network Management Protocol Vulnerabilities	Microsoft Security Bulletin MS02-006, Microsoft Download site http://www.microsoft.com/technet/security/bulletin/MS02-006.asp 🖶 Verify that the Hot Fix has been applied by confirming that the following registry key has been created: HKLM\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q314147 or Verify that Service Pack 3 or greater is installed (Manual): (Using START -> Run, execute "winver.exe".)

Patch Management Item Number 1 (PM1)	
Threat	The required Windows 2000 Operating System Service Pack is not installed.
Reference	DISA Win2K Security Checklist Appendix B (Section 5.9.1.4)
Risk Item	4,5,7,9
Risk Result	Failure to install the latest service packs may result in not having the latest updates to the Windows 2000 operating system. These updates are a collection of fixes in the following areas: security, application compatibility, operating system reliability, and setup. Windows 2000 SP4 is a required update that includes

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	the updates contained in previous Windows 2000 service packs. Service Pack 4 covers the following Microsoft Security Bulletins items found in DISA Security Checklist 3.1.14 Appendix B: MS02-006 MS03-013 supercedes MS03-007 MS03-0001 MS02-050 MS02-017 MS03-010
Test Procedure – Compliance	1. From the menu bar click “Start” 2. Click “Run” 3. Type “winver.exe” in the dialog box and click OK 4. The About Windows pop-up will appear and list the Service Pack Number.
S/O	Objective
Evidence/Findings	The most current service pack was/was not found on the system.

For the following auditing items, Shavlik Technologies HFNetChkPro4 is the recommended tool. http://www.shavlik.com A trial version of HFNetChkPro4 can be downloaded after registering on the Shavlik web site.

I have also avoided using the DOD-CERT numbers because the tool reports on MS Bulletin numbers. All instructions are in accordance with the client’s guidance that a system administrator be able to run the tool from the machine being audited. (Note: HFNetChkPro4 can also be run from a central point to scan a network or domain.)

Patch Management Item Number 2 (PM2)	
Threat	Required Windows 2000 Operating System patches are not installed
Reference	DISA Win2K Security Checklist

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Appendix B (Sections 5.9.1.x)
Risk Item	4,5,7,9
Risk Result	Failure to apply required Win2K OS patches could lead to system compromise and/or instability. The following MS Security Bulletin patches are required: MS03-043 MS03-049 MS04-007 MS03-041 MS04-001 (ISA Server) MS03-023 MS03-039
Test Procedure – Compliance	1. Open HFNetChkPro4 2. Select Scan My Machine from the right column. 3. Select either Full Scan or Quick Scan (see Appendix C) 4. Click Begin Scan 5. Once scan completes, review scan results 6. A green checkmark indicates that the patch was found. 7. A red X indicates that the patch was not found.
S/O	Objective
Evidence/Findings	The following Win2K OS MS Security Bulletin patches were not found on the system:

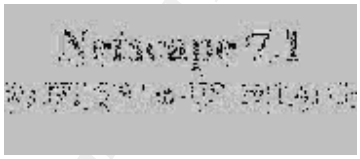
Patch Management Item Number 3 (PM3)	
Threat	Required Microsoft Internet Explorer patches are not installed.
Reference	DISA Win2K Security Checklist Appendix B (Sections 5.9.4.x)
Risk Item	4,5,7,9
Risk Result	Failure to apply required Microsoft Internet Explorer patches could lead to system compromise and/or instability. The following MS Security Bulletin patches are required: MS01-020 MS03-020 MS02-009

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	MS00-033 MS00-049 MS00-043 MS01-012 MS02-009
Test Procedure – Compliance	1. Open HFNetChkPro4 2. Select Scan My Machine from the right column. 3. Select either Full Scan or Quick Scan (see Appendix C) 4. Click Begin Scan 5. Once scan completes, review scan results 6. A green checkmark indicates that the patch was found. 7. A red X indicates that the patch was not found.
S/O	Objective
Evidence/Findings	The following Microsoft Internet Explorer MS Security Bulletin patches were not found on the system:

Patch Management Item Number 4 (PM4)	
Threat	Netscape Navigator (web browser) ver 4.76 or higher is not installed.
Reference	DISA Win2K Security Checklist Appendix B (Section 5.9.4.2)
Risk Item	1,4,5,9
Risk Result	Older versions of Netscape Navigator improperly validate SSL Sessions which can lead to a user being redirected to a malicious and insecure web site
Test Procedure – Compliance	1. Open Netscape Browser 2. Click on the Help drop down menu 3. Select About

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	 4. Review the Netscape Navigator version number installed 
S/O	Objective
Evidence/Findings	Netscape Navigator version 4.76 or higher is/is not installed.

Patch Management Item Number 5 (PM5)	
Threat	Required Microsoft Application patches are not installed.
Reference	DISA Win2K Security Checklist Appendix B (Section 5.9.2.x)
Risk Item	
Risk Result	Failure to apply required Microsoft Application patches could lead to system compromise and/or instability. The following MS Security Bulletin patches are required if the associated application is installed: MS01-050 (MS Excel/PowerPoint) MS02-065 (MDAC) MS02-041 (MCMS) MS03-046 (MS Exchange Server 5.5 or 2000) MS02-025 (MS Exchange 2000) MS02-069 (MS Virtual Machine) MS03-022 (MS Windows Media Services) MS03-036 (MS WordPerfect Converter) MS03-037 (MS Visual Basic) MS03-051 (MS FrontPage) MS04-003 (MDAC)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	MS99-044 (MS Excel 97/2000) MS00-034 (IE & MS Office 2000 Components) MS00-049 (MS Access 97/2000 and/or IE 4.0 or higher) MS00-056 (MS Word, Excel, PowerPoint 2000) MS00-051 (MS Excel 97/2000) MS00-050 (MS Excel 97/PowerPoint 97)
Test Procedure – Compliance	1. Open HFNetChkPro4 2. Select Scan My Machine from the right column. 3. Select either Full Scan or Quick Scan (see Appendix C) 4. Click Begin Scan 5. Once scan completes, review scan results 6. A green checkmark indicates that the patch was found. 7. A red X indicates that the patch was not found.
S/O	Objective
Evidence/Findings	The following Microsoft Application MS Security Bulletin patches were not found on the system:

Additional Considerations

Some additional areas to consider when conducting an audit are:

1. Is there an active and current user awareness program in place? All the security setting in the world are not going to help if an organization does not have a valid user awareness program that educates each individual regarding his or her responsibilities in ensuring the security and integrity of not only their own system, but the other systems in the organization as well.

2. How is the physical security of the organization? Some areas to focus on include

a. Safes or other lockboxes that are used to secure paper copies of data output.
b. Access points into the workspace(s): doors, windows, skylights, etc.
c. Locks on the access points.
d. Fire Alarms
e. CO2 Alarms

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

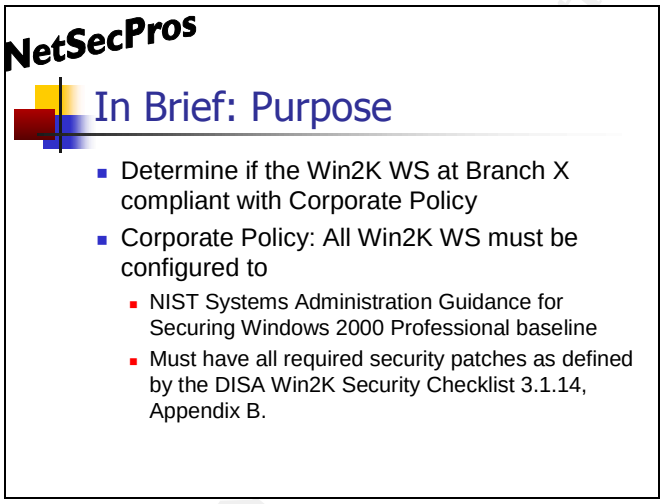
f. Are their guards? How are personnel identified to ensure only the proper personnel are granted access to workspaces?
g. Are systems physically anchored within the workspace to reduce the likelihood of theft?

Conducting the Audit

In Brief

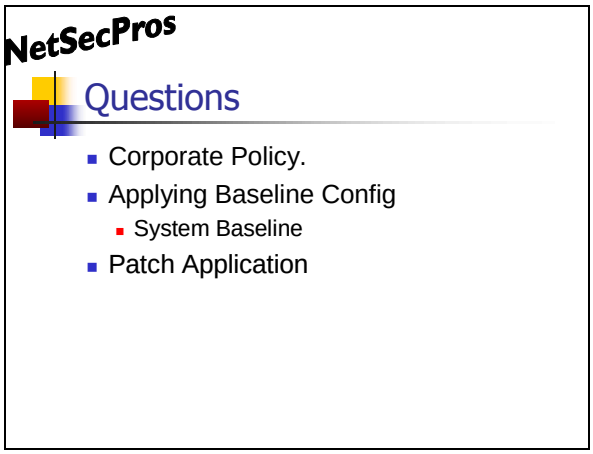
At the beginning of the audit of Branch X, an in brief was conducted with the Branch Manager, the Assistant Branch Manager, and 6 of the users (one of which was also the part-time system administrator.) We briefly reviewed the purpose for the audit and the direction from XYZ Corporate Management.

The purpose of the audit was to determine if the Windows 2000 Professional Workstations in use at Branch X were compliant with Corporate Policy. The Corporate Policy was defined as all Windows 2000 Professional Workstations must be configured to the NIST Systems Administration Guidance for Securing Windows 2000 Professional baseline and must have all required security patches as defined by the DISA Win2K Security Checklist 3.1.14, Appendix B.



I then asked the audience a few questions to determine the user awareness level at the branch office. When asked, the system administrator stated that he was familiar with the Corporate Policy. When asked to produce a copy for review, one was not available on site. Neither the Branch Manager nor Assistant Branch Manager had a copy available. I also asked the system administrator if he knew how the baseline configuration would be applied to a Windows 2000 system. He stated that he did not, but assumed that they were configured prior to shipment to the branch office. He also stated that the security patches were being deployed to the branch systems using SMS and manual installation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Audit Conduct

When conducting the audit for Branch X, I evaluated 10 Windows 2000 Professional Systems. The branch system administrator assisted in the audit.

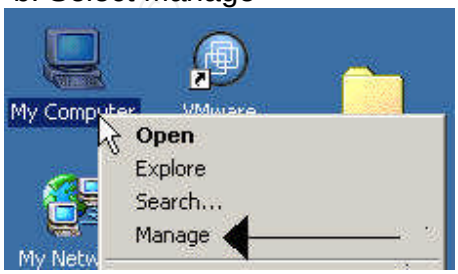
The charts below shows the results for each of the systems based on the items audited. I used a simple pass/fail grading scale due to the fact that the scope of the audit was to determine if the systems at Branch X were compliant with the baseline configuration and if all required security patches had been installed.

I will demonstrate the steps taken on one of the systems.

The first column corresponds to the checklist item numbers defined previously. The Evidence/Findings column is where the results of the checklist item audit are recorded. The Pass/Fail column is to record if the checklist item met the requirement (pass) or did not meet the requirement (fail).

Checklist Item #	Evidence/Findings	Pass/Fail
SSS1	The telnet service has been disabled on this system.	Pass

Steps:
1. Open the Computer Management Console
 a. Right click on My Computer
 b. Select Manage

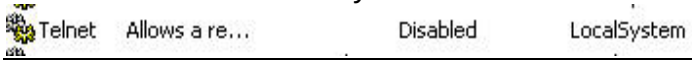


2. Expand the Services and Applications object in the tree window

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Select the Services Object

4. Review the Telnet entry in the services list to determine if it is disabled.

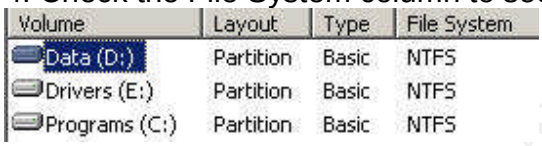


Checklist Item #	Evidence/Findings	Pass/Fail
SM4	All volumes **are** formatted for NTFS	Pass

Steps:

1. Open the Computer Management Console
   a. Right click on My Computer
   b. Select Manage
2. Expand the Storage Object in the Tree Window
3. Select the Disk Management Object

4. Check the File System column to see if all volumes are NTFS.



5. All volumes are formatted for NTFS.

Checklist Item #	Evidence/Findings	Pass/Fail
APM3	The minimum password age does not meet the standard.	Fail

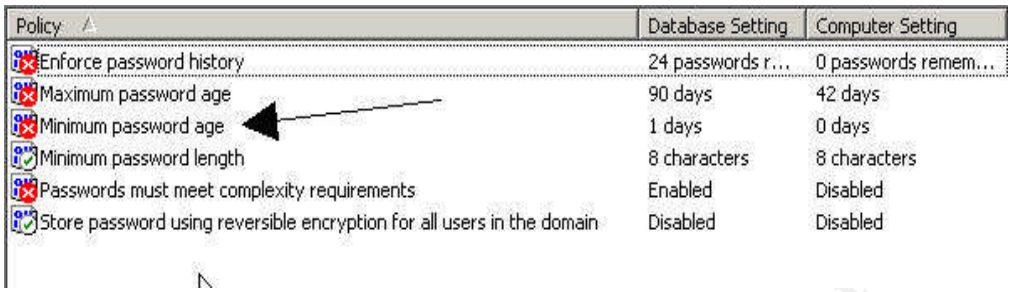
Steps:

In the MMC window select

7. Account Policies
8. Password Policy

9. Minimum Password Age
10. Compare the Computer Setting to the Database Setting to determine if they match.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



11. A red X indicates that the settings do not match.
12. A green checkmark indicates that the settings match.

Checklist Item #	Evidence/Findings	Pass/Fail
APM7	The setting is disabled.	Pass

Steps:
In the MMC window select

7. Account Policies
8. Password Policy

9. Store passwords using reversible encryption for all users in the domain
10. Compare the Computer Setting to the Database Setting to determine if they match. This setting should NOT be enabled.

11. A red X indicates that the settings do not match.
12. A green checkmark indicate that the settings match.

Checklist Item #	Evidence/Findings	Pass/Fail
LPM2	Auditing **is not** enabled correctly. List the items not audited correctly: 1. Audit account logon events 2. Audit account management 3. Audit logon events 4. Audit policy change 5. Audit privilege use 6. Audit system events	Fail

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

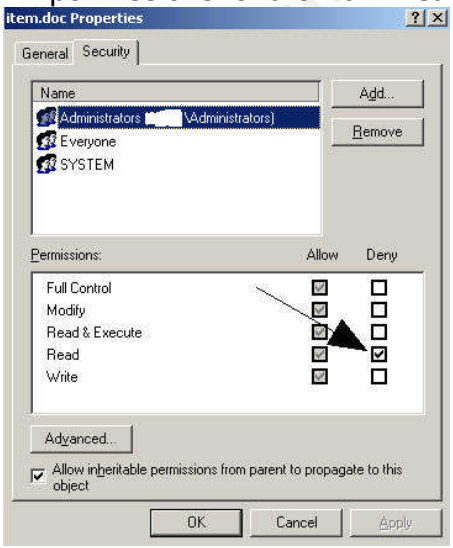
Steps:

7. Local Policies
8. Audit Policies

9. Review audit policy items to determine if auditing is enabled correctly.
10. All items listed should be set for either “failure” or “success, failure” depending on the recommended NIST settings.

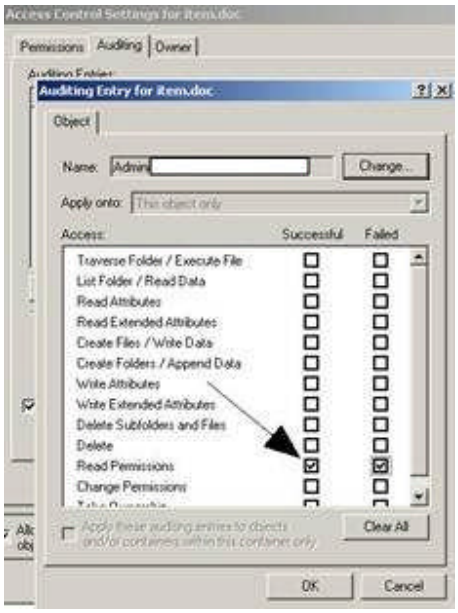
Policy	Database Setting	Computer Setting
Audit account logon events	Success, Failure	No auditing
Audit account management	Success, Failure	No auditing
Audit directory service access	Not defined	Failure
Audit logon events	Success, Failure	Failure
Audit object access	Failure	Failure
Audit policy change	Failure	Success, Failure
Audit privilege use	Failure	Success, Failure
Audit process tracking	Not defined	Failure
Audit system events	Success, Failure	Failure

11. A red X indicates that the settings do not match.
12. A green checkmark indicates that the settings match.
13. I next wanted to confirm that the policy item with the correct setting was actually functioning properly. I used the article “Auditing Windows 2000” by Randy Franklin Smith (ref 9), as a reference when developing the following steps.
14. Because the “Audit Object Access” policy allows you to track access to files, directories, registry keys and printers, I created a DOC file on the system’s desktop called “item.doc”
15. I then had to enable auditing on the object I just created. I opened the file’s properties dialog box, and selected the Security tab. I modified the permissions for the Administrator account to DENY READ ACCESS.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

16. Clicking on Advanced, I then selected the Auditing tab and Added the Administrator user account to audit Read Permissions.



17. I then made a note of the time 5:31 pm and attempted to open the ITEM.DOC file. Microsoft Word displayed and error that the path was not valid. The file would not open.
18. The next step to verify that the system is auditing object access for the ITEM.DOC file was to check the Security audit log.
    a. Click START > SETTINGS > CONTROL PANEL > ADMINISTRATIVE TOOLS

    b. Select EVENT VIEWER >

    c. Select SECURITY LOG and check the Audit Type column for FAILURE AUDIT. A failure audit was generated at 5:31.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Type	Date	Time	Source	Category	Event	User
Success Audit	4/23/2004	5:31:18 PM	Security	Privilege Use	578	Administrator
Success Audit	4/23/2004	5:31:12 PM	Security	Privilege Use	577	Administrator
Failure Audit	4/23/2004	5:31:12 PM	Security	Object Access	560	Administrator
Failure Audit	4/23/2004	5:31:12 PM	Security	Object Access	560	Administrator

d. I opened the Failure Audit item and verified that the Object Name matched for the object I created, ITEM.DOC.

e. The Object Name matched verifying that the setting for auditing object access is correct and functioning properly.

Checklist Item #	Evidence/Findings	Pass/Fail
SOM1	The settings do not match.	Fail * Note

Steps:
In the MMC window select

7. Account Policies
8. Security Options

9. Additional restrictions for anonymous connections
10. Compare the Computer Setting to the Database Setting to determine if they match.

Policy	Database Setting	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions	Do not allow enumeration of SAM accounts and shares

11. A red X indicates that the settings do not match.
12. A green checkmark indicates that the settings match.

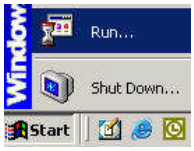
Note: In an attempt to understand the difference between the 2 settings, because they both appear to accomplish the same thing, I reference Randy

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

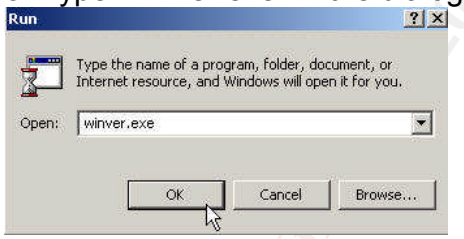
Franklin Smith article “Access Denied” (ref 10) which stated that the NIST setting prevents anonymous access to the system because this setting “prevents Win2K from adding the Everyone group to the access token of anonymous connections at logon. If an anonymous user tries to access an object, the access token doesn’t contain Everyone, and the permissions granted to Everyone won’t apply.” The “Microsoft Windows 2000 Security Hardening Guide” Chapter 5 – Security Configuration (ref 11) states that the NIST setting is recommended for laptops and workstations and that the setting “Do not allow enumeration of SAM accounts and shares” is recommended for Domains and stand-alone servers. The system administrator did not know any reason why the NIST setting should not be applied unless it was not setup prior to shipment, so this is reported as a finding.

Checklist Item #	Evidence/Findings	Pass/Fail
PM1	The correct service pack is installed.	Pass

Steps:
1. From the menu bar click “Start”
2. Click “Run”



3. Type “winver.exe” in the dialog box and click OK



4. The About Windows pop-up will appear and list the Service Pack Number.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Checklist Item #	Evidence/Findings	Pass/Fail
PM2	All required patches were installed.	Pass

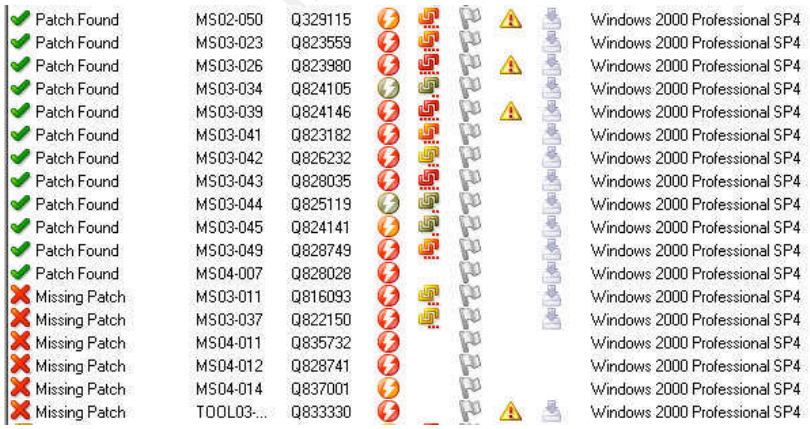
Steps:

8. Open HFNetChkPro4
9. Select Scan My Machine from the right column.

10. Selected Quick Scan

11. Click Begin Scan
12. Once scan completes, review scan results for Windows 2000 Professional to determine if the following Operating System MS Security Bulletin patches are installed:

MS03-043
MS03-049
MS04-007
MS03-041
MS04-001 (ISA Server) Not Required
MS03-023
MS03-039

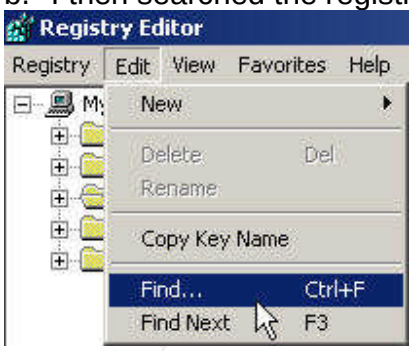


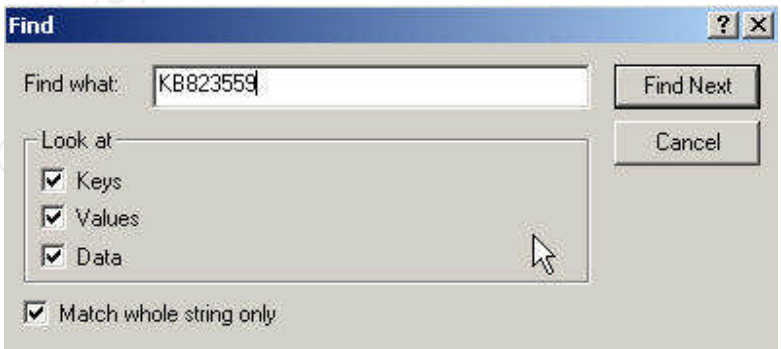
13. A green checkmark indicates that the patch was found.
14. A red X indicates that the patch was not found.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

15. All required patches were found by the tool.
16. To validate the tool's results, I selected one of the required security bulletin patches (MS03-023) and one of the patches that the tool reported as missing (MS03-011).
17. Referencing the respective Microsoft Security Bulletin for MS03-023 (http://www.microsoft.com/technet/security/bulletin/MS03-023.mspx), I then found the registry key that would be created if the patch was installed on the system: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB823559
    a. I searched the registry by running REGEDIT

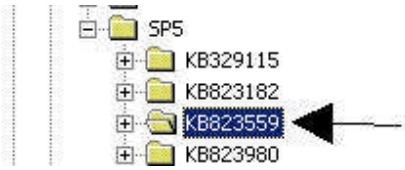
    b. I then searched the registry for the string KB823559



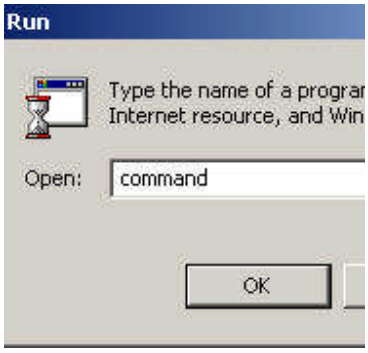


    c. The string was found in the specified location confirming installation.

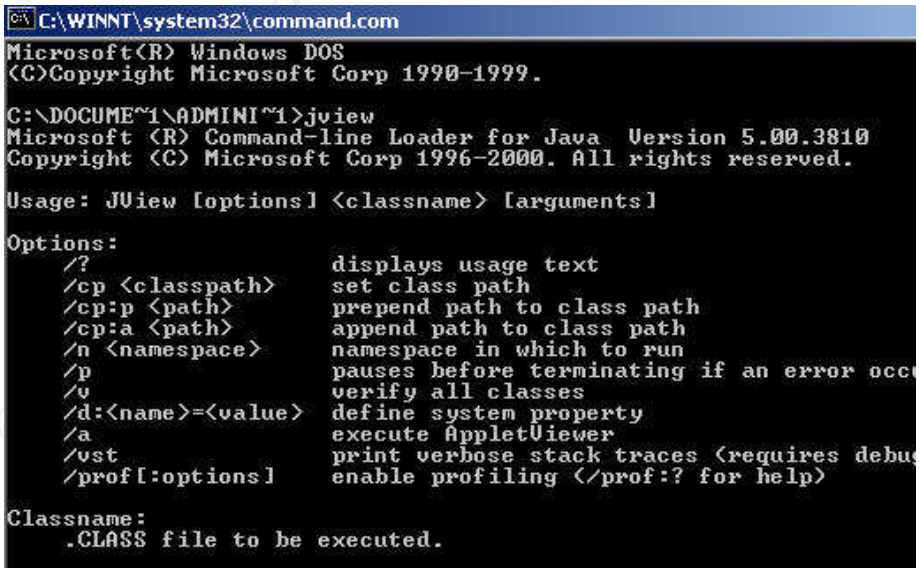
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



18. Again, to validate the tool's results, I referenced the respective Microsoft Security Bulletin for MS03-011 (http://www.microsoft.com/technet/security/bulletin/MS03-011.mspx). This is a Security Update for Microsoft Virtual Machine.
    a. Following the directions on the security bulletin, I first had to determine if the Microsoft VM was running on the machine being audited.
    b. From START > RUN > command



    c. At the command prompt I typed **jview**
    d. Information about java was displayed on the screen indicating that the Microsoft VM was installed.



    e. If the message **Bad command or file name** had displayed, the Microsoft VM would not have been installed.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

f. I was unable to find any information regarding what registry keys are changed, but based on the previous test validating the installation of a security patch and subsequent validation noted below (PM3) I am confident the tool's report is accurate.

Checklist Item #	Evidence/Findings	Pass/Fail
PM3	All required patches are installed.	Pass

Steps:

1. Reviewed Internet Explorer scan results from HFNetChkPro4 scan run previously.
2. Looked for the following required Internet Explorer MS Security Bulletin patches:

MS01-020
MS03-020
MS02-009
MS00-033
MS00-049
MS00-043
MS01-012
MS02-009

3. The tool results failed to show that any of the required patches were installed, however it did report that Internet Explorer SP1 was installed.
4. The fact that the required patches MS Bulletin numbers were not listed does not indicate that the patch does not exist on the system. HFNetChkPro, as explained in the HELP file, only reports those patches needed by a system and does not show earlier patches that had been superceded by later patches.
5. To ensure that the tool did, in fact, check the system for the required patches, I reviewed the mssecure.xml file used by HFNetChkPro. All required patches were referenced. (Refer to the below examples to see where two of the selected patch reference were located in the MSSecure.xml file. Because of the submission size limit for the practical I am only showing two extracts from the file. All patch references were located.)

</Bulletin>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

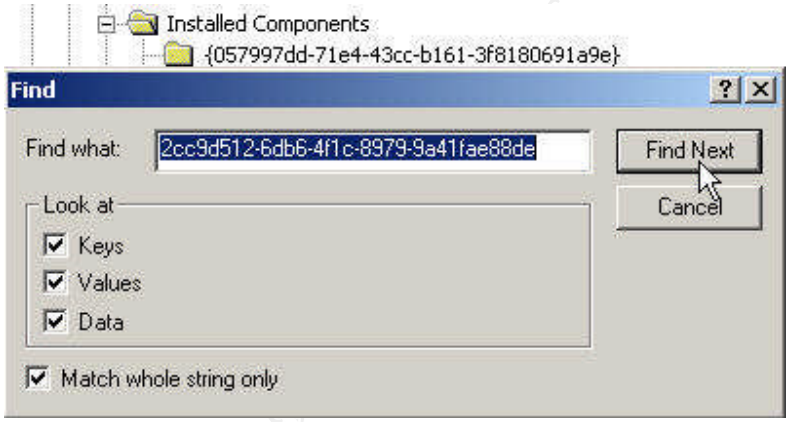
<Bulletin BulletinID="MS01-020" BulletinLocationID="73" FAQLocationID="73" FAQPageName="FQ01-020" Title="Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" DatePosted="2001/03/29" DateRevised="2001/05/25" Supported="Yes" Summary="This update resolves a security vulnerability in Internet Explorer, and is discussed in Microsoft Security Bulletin MS01-020. Download now to prevent a malicious user from running an executable e-mail attachment on your computer. " Issue="Because HTML e-mails are simply web pages, IE can render them and open binary attachments in a way that is appropriate to their MIME types. However, a flaw exists in the type of processing that is specified for certain unusual MIME types. If an attacker created an HTML e-mail containing an executable attachment, then modified the MIME header information to specify that the attachment was one of the unusual MIME types that IE handles incorrectly, IE would launch the attachment automatically when it rendered the e-mail.
An attacker could use this vulnerability in either of two scenarios. She could host an affected HTML e-mail on a web site and try to persuade another user to visit it, at which point script on a web page could open the mail and initiate the executable. Alternatively, she could send the HTML mail directly to the user. In either case, the executable attachment, if it ran, would be limited only by user?s permissions on the system.
" ImpactSeverityID="0" PreReqSeverityID="0" MitigationSeverityID="0" PopularitySeverityID="0">
<BulletinComments/>
<QNumbers>
<QNumber QNumber="Q290108 "/>
</QNumbers>
<Patches>

</Bulletin>
<Bulletin BulletinID="MS03-020" BulletinLocationID="73" FAQLocationID="73" FAQPageName="FQ03-020" Title="Cumulative Patch for Internet Explorer (818529)" DatePosted="2003/06/04" DateRevised="2003/06/04" Supported="Yes" Summary="This is a cumulative patch that includes the functionality of all previously released patches for Internet Explorer 5.01, 5.5 and 6.0. In addition, it eliminates two newly discovered vulnerabilities:

A buffer overrun vulnerability that occurs because Internet Explorer does not properly determine an object type returned from a web server. It could be possible for an attacker who exploited this vulnerability to run arbitrary code on a user's system. If a user visited an attackers website, it would be possible for the attacker to exploit this vulnerability without any other user action. An attacker could also craft an HTML email that attempted to exploit this vulnerability.
A flaw that results because Internet Explorer does not implement an appropriate block on a file download dialog box. It could be possible for an attacker to exploit this vulnerability to run arbitrary code on a user's system. If a user simply visited an attackers website, it would be possible for the attacker to exploit this vulnerability without any other user action. An attacker could also craft an HTML email that attempted to exploit this vulnerability.
In order to exploit these flaws, the attacker would have to create a specially formed HTML email and send it to the user. Alternatively an attacker would have to host a malicious web site that contained a web page designed to exploit these vulnerabilities. The attacker would then have to persuade a user to visit that site. " Issue="" ImpactSeverityID="0" PreReqSeverityID="0" MitigationSeverityID="0" PopularitySeverityID="0">
<BulletinComments/>
<QNumbers>
<QNumber QNumber="Q818529"/>
</QNumbers>
<Patches>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6. Although the system is compliant with the required security patches the tool does report that one critical Microsoft Internet Explorer patch (MS04-013) is missing. This will be noted for the Audit Report.
7. To confirm that the missing patch was not installed I referenced MS Security Bulletin MS04-013 (http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx) and verified that the following registry key, which is created if the patch is installed, did not exist: HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{2cc9d512-6db6-4f1c-8979-9a41fae88de} by taking the following steps using the Registry Editor:
    a. Regedit
    b. I then searched for the string 2cc9d512-6db6-4f1c-8979-9a41fae88de



    c. The key was not found; therefore the patch was not installed.

Checklist Item #	Evidence/Findings	Pass/Fail
PM5	The following required MS Application patches are not installed: MS01-050	Fail

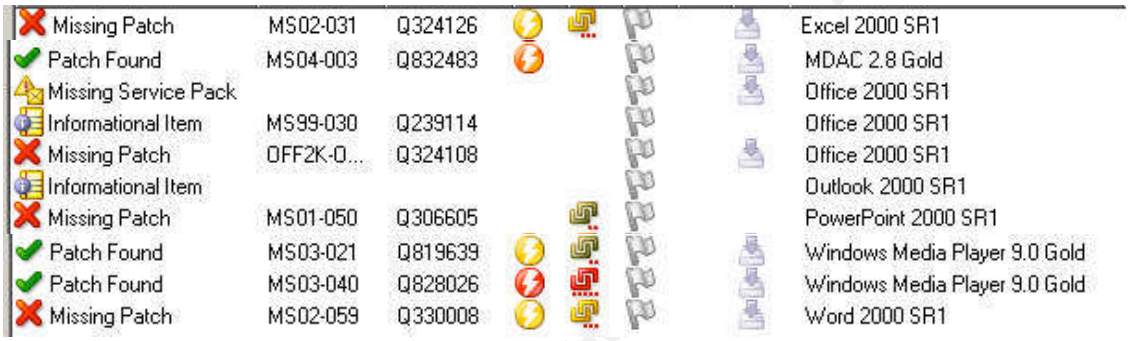
Steps:

1. Reviewed MS Applications scan results from HFNetChkPro4 scan run previously.
2. Looked for the following required MS Security Bulletin patches if the associated application was installed:

MS01-050 (MS Excel/PowerPoint)
MS02-065 (MDAC)
MS02-041 (MCMS)
MS03-046 (MS Exchange Server 5.5 or 2000)
MS02-025 (MS Exchange 2000)
MS02-069 (MS Virtual Machine)
MS03-022 (MS Windows Media Services)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

MS03-036 (MS WordPerfect Converter)
MS03-037 (MS Visual Basic)
MS03-051 (MS FrontPage)
MS04-003 (MDAC)
MS99-044 (MS Excel 97/2000)
MS00-034 (IE & MS Office 2000 Components)
MS00-049 (MS Access 97/2000 and/or IE 4.0 or higher)
MS00-056 (MS Word, Excel, PowerPoint 2000)
MS00-051 (MS Excel 97/2000)
MS00-050 (MS Excel 97/PowerPoint 97)



3. It was noted that not all Bulletins were listed. Again, I could not determine from the tool results if all of the required patches were installed.
4. It was found that Office 2000 SR1 had not been installed. The NIST Win2K Pro Guide does require all systems to be up-to-date on all patches and hotfixes unless there is a reason the organization cannot install the update. Because the systems administrator was with me during the audit, I asked if he knew of a reason the update had not been installed. He stated that all branch offices were directed to update their systems with the latest Service Packs/Service Release for Office. This was noted as a finding.
5. After reviewing the MSSecure.xml file it was determined that all patches not listed in the evidence and finding section were installed or had been superceded by another patch.
6. Below is an example of the patch references in the MSSecure.xml file for two applications installed on the system being audited.

```
</Bulletin>
                <Bulletin BulletinID="MS00-051" BulletinLocationID="73" FAQLocationID="73"
FAQPageName="FQ00-051.asp" Title="Excel REGISTER.ID Function Vulnerability"
DatePosted="2000/07/26" DateRevised="2000/07/26" Supported="Yes" Summary="A
vulnerability has been discovered in REGISTER.ID, a worksheet function. When REGISTER.ID is
invoked from an Excel worksheet, it can reference any DLL on the system. If the referenced DLL
contains malicious code, harmful effects can occur. By design, there is no warning given to the
user when REGISTER.ID calls a DLL from a worksheet." Issue="" ImpactSeverityID="0"
PreReqSeverityID="0" MitigationSeverityID="0" PopularitySeverityID="0">
                        <BulletinComments/>
                        <QNumbers>
                                <QNumber QNumber="Q269252"/>
```

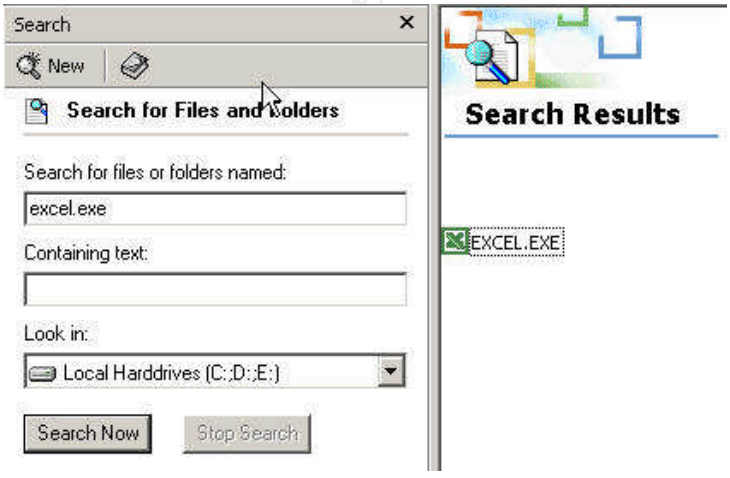

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

<QNumber QNumber="Q269263"/>
</QNumbers>
<Patches>

</Bulletin>
<Bulletin BulletinID="MS04-003" BulletinLocationID="73" FAQLocationID="73" FAQPageName="FQ04-003" Title="Buffer Overrun in MDAC Function Could Allow Code Execution (832483)" DatePosted="2004/01/02" DateRevised="2004/01/02" Supported="Yes" Summary="Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations, such as connecting to remote databases and returning data to a client. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially-crafted packet that could cause a buffer overflow.

An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. The actions an attacker could carry out would be dependent on the permissions under which the program using MDAC ran. If the program ran with limited privileges, an attacker would be limited accordingly; however, if the program ran under the local system context, the attacker would have the same level of permissions." Issue="" ImpactSeverityID="0" PreReqSeverityID="0" MitigationSeverityID="0" PopularitySeverityID="0">
<BulletinComments/>
<QNumbers>
<QNumber QNumber="Q832483"/>
</QNumbers>
<Patches>

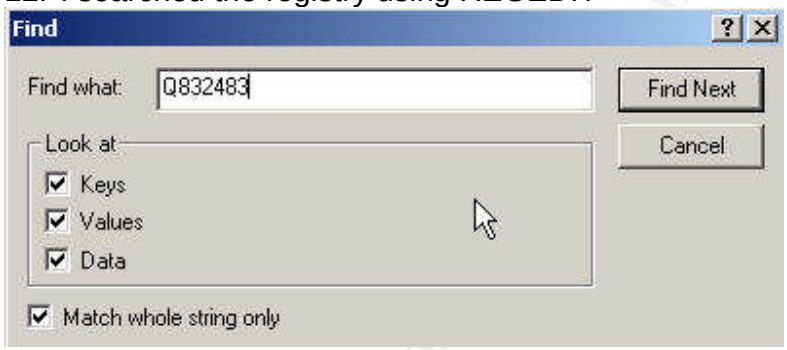
7. To further verify the MS00-051 patch listed above, the DISA Win2K Security Checklist (Section 5.9.2.3) states that the last 4 digits of the version of Excel.exe should be equal to or greater than 4317.
8. I then did a search for Excel.exe and found the file



9. I checked the version number by right clicking on the file and selected the version tab

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

10. The version number exceeded the minimum required indicating that the patch had been installed.
11. The DISA Win2K Security Checklist states that for MS04-003 (http://www.microsoft.com/technet/security/bulletin/MS04-003.mspx) the following registry key should be created if the patch is installed correctly: HKEY_LOCAL_MACHINE\Software\Microsoft\Updates\DataAccess\Q832483
12. I searched the registry using REGEDIT



13. The string was found verify installation of the patch and the accuracy of HFNetChkPro4.

Audit Report

Out Brief

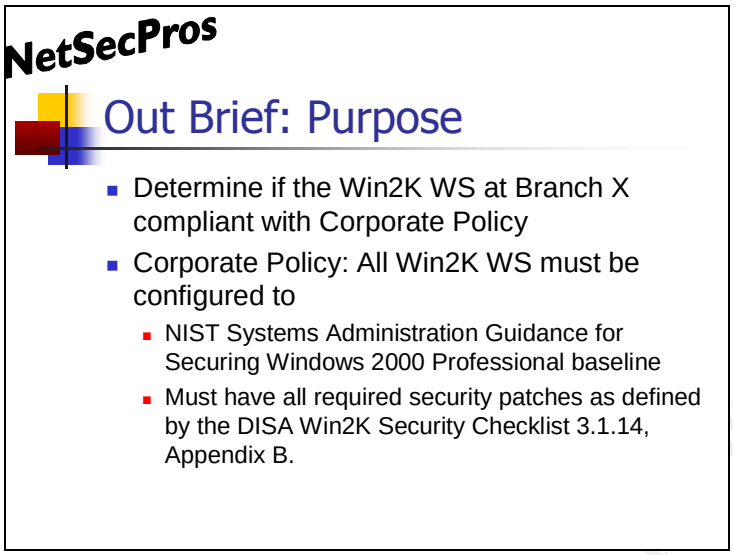
At the conclusion of the audit all information was compiled and an out brief was given to the Branch X Manager, the Assistant Branch Manager, and the same 6 users who had attended the in brief. This included the part-time system administrator. The XYZ Corporation IT Department Manager also attended.

Executive Summary

NetSecPros was hired by the XYZ Corporation for the purpose of conducting an audit of XYZ Corporation Branch X to determine if the systems were compliant

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

with the baseline configuration standard and if the required patches that had been installed via SMS were in fact installed correctly.

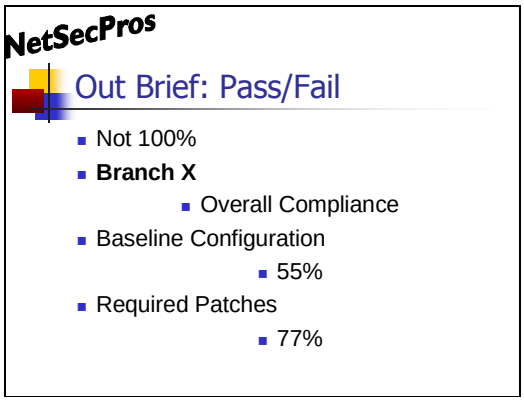


Based solely on a pass/fail criterion, Branch X systems were not compliant in either area. However, the systems were not grossly out of compliance. Rather, some relatively simple actions can bring these systems into compliance in a short period of time.

Additionally, NetSecPros was asked to develop an auditing methodology that can be used by XYZ Corporation auditors for future audits. The audit methodology is outlined in the section “Conducting the Audit” and can be applied to future audits with ease. Ensure that, prior to a new audit, the checklist is updated with the latest information in DISA Windows 2000 Security Checklist Appendix B.

For the two audit areas, baseline configuration compliance and required patch management, the Branch X systems had 77% of all required patches installed. This would indicate that the SMS patching system is functioning well and patching systems as indicated. Branch X systems were 55% compliant in the area of configuration management. Although this number is lower than the compliance percentage for patch management, system administrators can easily correct this using the NIST security template for Windows 2000 Workstations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The next section outlines the audit findings for Branch X.

Audit Findings

The below table references the 10 Checklist Items that were used to demonstrate the audit of the Branch X Windows 2000 Professional systems. The format can easily be expanded as required. The first column lists the Checklist Item Numbers. Each system can then be listed across the top of the table by its machine name. This will ID which items need to be corrected on each machine, simplifying things for the system administrators when they are prioritizing their work. Each machine is graded as either a Pass (P) or Fail (F) based on the Checklist Item.

Checklist Item #	Win2K 01	Win2K 02	Win2K 03	Win2K 04	Win2K 05	Win2K 06	Win2K 07	Win2K 08	Win2K 09	Win2K 010
SSS1	P	P	P	P	P	P	P	P	P	P
SM4	P	P	P	P	P	P	P	P	P	P
APM3	F	P	F	F	F	F	F	F	F	F
APM7	P	P	P	P	P	P	P	P	P	P
LPM2	F	P	F	F	F	F	F	F	F	F
SOM1	F	P	F	F	F	F	F	F	F	F
PM1	P	P	P	P	P	P	P	P	P	P
PM2	P	P	P	P	P	P	P	P	P	P
PM3	P	P	P	P	P	P	P	P	P	P
PM5	F	P	F	F	F	F	F	F	F	F

The next table details the numbers of systems that passed or failed for each Checklist item and the overall percentage for each Checklist Item that was found to be compliant for Branch X.

Checklist Item #	Compliant/Not Compliant	% of each checklist item
SSS1	10/10	100%
SM4	10/10	100%
APM3	1/10	10%
APM7	10/10	100%
LPM2	1/10	10%

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SOM1	1/10	10%
PM1	10/10	100%
PM2	10/10	100%
PM3	10/10	100&
PM5	1/10	10%

Note: Both tables can be modified to reflect whichever Checklist Items a future auditor is assigned. For instance, when assigned to audit Branch Y, the auditor is tasked with only validating the patch compliance. Only those checklist item numbers that correspond to patch management would be listed.

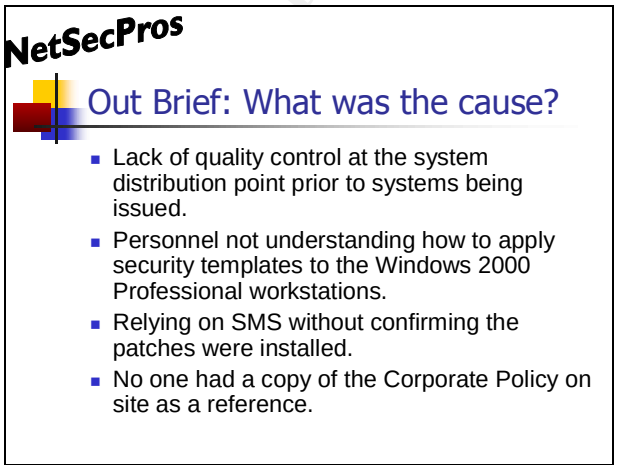
The final table details the percentage of systems, based on the ten items above, found to be compliant with the baseline configuration (6 of 10 items) or the required patches (4 of 10 items) at Branch X.

Branch X	Overall Compliance
Baseline Configuration	55%
Required Patches	77%

Audit Recommendations

What may have caused this in the first place?
A number of factors may have contributed to these findings to include lack of quality control at the system distribution point prior to systems being issued to personnel not understanding how to apply security templates to the Windows 2000 Professional workstations. In the area of required patch installation, no system is 100% accurate. Simply relying on SMS without confirming the patches were installed is the likely cause.

Another item that was discovered during the in brief that can contribute to this is that no one at Branch X had a copy of the Corporate Policy on site as a reference.

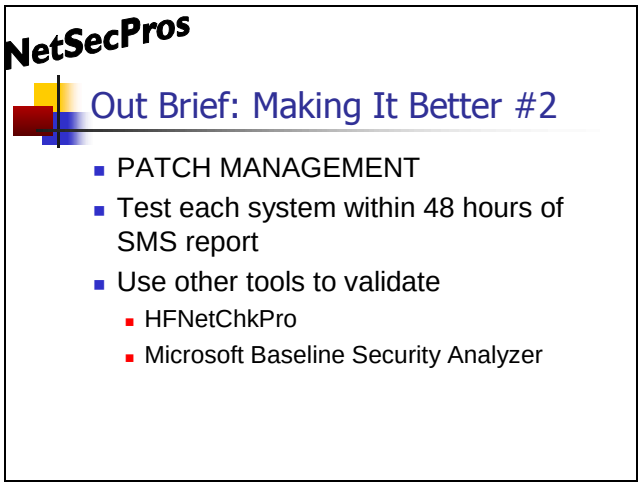


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

What can you do to make things better?
During the in brief it was revealed that the Windows 2000 Professional Workstations at Branch X were delivered pre-configured. Because only 1 of the 10 systems audited was 100% compliant for the baseline configuration, it is recommended that a system be put in place at the corporate distribution point to quality check each computer prior to boxing it for shipment. For the systems already in place at different branch offices, an audit of those systems is required. This can be accomplished easily by using the Microsoft Management Console and comparing the existing system configuration to the required configuration file (NISTWin2KproGold.inf). Follow the same steps outlined for the use of MMC in MS KB300549. If a computer is not compliant, simply apply the required configuration file through the MMC. (Test a system with the configuration file installed to ensure it functions properly in the branch office.) The MMC is pre-installed on Windows 2000 Professional and the configuration file (NISTWin2KProGold.inf) can be downloaded from the NIST web site. (http://csrc.nist.gov/itsec/download_W2Kpro.html)

In the area of patch management it is recommended that branch system administrators test each system within 48 hours of SMS reporting that a required patch has been installed. HFNetChkPro is an excellent tool for this regarding Microsoft Security Patches and can be purchased from Shavlik Technologies either online or directly from an authorized reseller. You can also download the Microsoft Baseline Security Analyzer for free from Microsoft.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



What are the costs associated with fixing the problems?
It will take some additional time to validate the machines before they leave the distribution point, but it is a necessary cost. Failure to do so could result in misconfigured machines being fielded. Not checking the systems already in place at other branches may mean that misconfigured systems are in place that could lead to compromise or loss of data. The security posture of the corporation as a whole would also suffer.

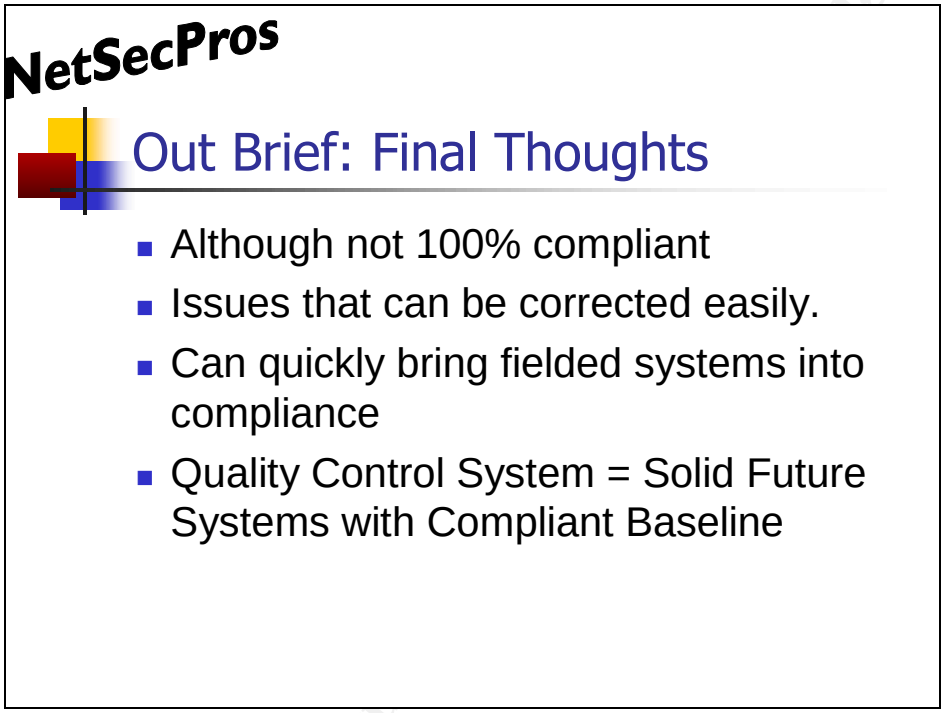
Microsoft Baseline Security Analyzer can be downloaded for free from the Microsoft Web Site.
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

HFNetChkPro4 can be purchased online from Shavlik Technologies for 100 seats or less at a cost of $620.00 for 25 seats to $2080.00 for 100 seats. For purchases larger than 100 seats, an authorized reseller can be located on the Shavlik.com web site (http://www.shavlik.com). Between the two tools, HFNetChkPro is recommended.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Final Comments

Although the systems audited at Branch X were not 100% compliant, I want to stress that these are issues that can be corrected easily. By following the steps recommended above, the XYZ Corporation should be able to quickly bring its fielded systems into compliance and by putting a quality control system in place at the corporate distribution point, future systems should be delivered with a compliant baseline system.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A
References

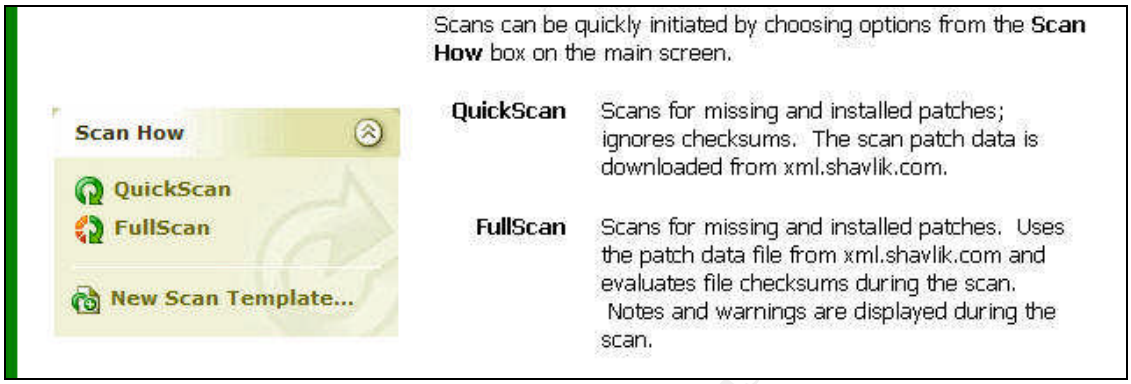
1. DISA Windows 2000 Security Checklist (includes appendices) http://csrc.nist.gov/pcig/CHECKLISTS/win2k-checklist-032604.zip (18 March 2004)
2. Windows 2000 Professional Overview. 30 Jan 2001. URL: http://www.microsoft.com/windows2000/professional/evaluation/business/overview/default.asp (24 April 2004)
3. Symantec AntiVirus Corporate Edition. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155&EID=0 (24 April 2004)
4. NIST Systems Administration Guidance for Windows 2000 Professional. 25 November 2002. URL: http://csrc.nist.gov/itsec/guidance_W2Kpro.html (15 April 2004)
5. Mission: Computer Security Resource Center. 24 August 2001. URL: http://csrc.nist.gov/mission.html (24 April 2004)
6. FAQ 2. Frequently Asked Questions. NIST Systems Administration Guidance for Windows 2000 Professional. 25 November 2002. URL: http://csrc.nist.gov/itsec/guidance_W2Kpro.html (24 April 2004)
7. Microsoft Management Console: Overview. 07 October 1999. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/mmcover.asp (19 April 2004)
8. HOW TO: Enable and Apply Security Auditing in Windows 2000. KB300549. 20 November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;300549 (20 April 2004)
9. Smith, Randy Franklin. “Auditing Windows 2000.” Instant Doc #9633. 20 July 2000. URL: http://www.winnetmag.com/Article/ArticleID/9633/9633.html (23 April 2004)
10. Smith, Randy Franklin. “Access Denied: Preventing Anonymous Users from Gaining Access to Files and Other Resources.” Instant Doc #24671. May 2002. URL: http://www.winnetmag.com/Article/ArticleID/24671/24671.html (23 April 2004)
11. Microsoft Windows 2000 Security Hardening Guide – Chapter 5 – Security Configuration. 2004. URL: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/05sconfg.mspx (23 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

GSNA 3.0

Appendix C

Shavlik Definitions for Full Scan and Quick Scan



QuickScan vs FullScan

QuickScan and FullScan are the default scanning templates provided with HFNetChkPro 4. The primary differences between the two templates:

- A QuickScan will not evaluate file checksums whereas a FullScan will. As a result, a QuickScan can be faster.
- A FullScan will display notes and warnings during the scan.

Neither of these scanning templates can be modified and they both provide the following:

- Use patch data file from xml.shavlik.com
- Allow the scanner engine to scan 64 machines simultaneously
- Report on all installed and missing bulletins

© SANS Institute 2004,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.