Microsoft®

Microsoft Solutions for Security

Testing the Windows Server 2003 Security Guide

patterns & practices

proven practices for predictable results

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e – mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e – mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Table of Contents

Introduction 1
  Scope 1
  Testing Objectives 1
Testing Strategy and Methodology 2
  Strategy 2
  Testing Environment and Tools 2
    Lab Network Diagrams 4
  Test Cycles 6
  Types of Test Procedures 7
    Base Deployment Tests 7
    Functionality Tests 7
    Interoperability 7
  Pass and Fail Criteria 7
  Security Build Phases 7
    Test Prep Phase 8
    Manual Server Configuration Phase 8
    Group Policy Configuration Phase 9
    IP Sec Configuration Phase 9
Test Execution Details 10
  Chapter 2 10
  Chapter 3 11
  Chapter 4 11
  Chapter 5 11
  Chapter 6 12
  Chapter 7 12
  Chapter 8 13
  Chapter 9 13
  Chapter 10 13
  Chapter 11 14
Release Criteria 15
  Bug Classification 15
Penetration Testing 16
Conclusion 17

Introduction

The *Windows Server 2003 Security Guide* was tested in a lab environment to ensure that the technology works as expected and to ensure a high degree of confidence in the recommended solution.

The documentation was checked for consistency, and all recommended procedures were tested by the *Windows Server 2003 Security Guide* test team, thus ensuring that users of the solution save on costs and time associated with building and testing their own implementations of the solution.

Scope

The *Windows Server 2003 Security Guide* was tested in a lab environment based on the three environment scenarios defined in Chapter 1, "Introduction to the Windows Server 2003 Security Guide." Testing was conducted based on the criteria described in the "Testing Objectives" section below.

Vulnerability assessment of the test lab environment secured by the *Windows Server 2003 Security Guide* solution was out of scope for the test team. Penetration testing was performed by partners, details of which are presented in the Chapter 12 of this guide, "Conclusion."

The bastion host was tested in the High Security client scenario. A bastion host was tested with Microsoft Internet Information Services (IIS), File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP) functionality.

The Internet Authentication Service (IAS) Server was tested only against a Remote Authentication Dial-In User Service (RADIUS) database (raddb) and not the Microsoft® Active Directory® database.

The Certificate Services Server was tested only in the enterprise client scenario.

Testing Objectives

The objectives of the *Windows Server 2003 Security Guide* test team were to verify the following:

- All statements made in the solution guide are accurate.
- All prescriptive guidance in the *Windows Server 2003 Security Guide* is correct. The guidance should be repeatable and reliably usable by a Microsoft Certified Systems Engineer (MSCE) with two years of experience.
- The core functionality of the secured Microsoft Windows® 2003 Server roles is not negatively impacted.
- Users in any of the three environments defined in the guide can access the services provided by the secured Windows 2003 Server roles.

Testing Strategy and Methodology

This section details the overall strategy of the test effort. It begins with an overview of the test strategy and then presents the details on which the test execution is based. These include a description of the test environments, tools and software used, test cycle progression, the phases of each test cycle and the tests that were executed in each phase.

Strategy

To achieve the testing objectives, the test team developed a test lab based on the three scenarios identified for hardening Microsoft Windows Server 2003™ to different levels of security. The test team executed two test cycles to validate the guidance in the *Windows Server 2003 Security Guide*.

A test cycle was defined as a sequence of the following three incremental security build phases:

1. Manual Server Configuration Phase
2. Group Policy Configuration Phase
3. IP Security (IPSec) Configuration Phase

The details of these phases are provided in the "Security Build Phases" section of this guide along with the Test Prep phase that describes the steps undertaken to ensure that the lab environment itself was free of any issues that could cause a misinterpretation of the actual test results after the three scenarios defined in the guide had been hardened through the three security build phases.

At various stages in a test cycle, different sets of tests were executed from each of the three categories mentioned below and further explained in the "Types of Test Procedures" section of this guide.

1. Base deployment tests
2. Functionality tests
3. Interoperability tests

For the complete details on how each chapter was tested and how each test phase was sequenced, refer to the "Test Execution Details" section of this guide.

Testing Environment and Tools

The test environment consisted of computers running Windows Server 2003 to function using the following features and services: Active Directory, Infrastructure Servers for Windows Internet Naming Service (WINS) Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP), File servers, Printer servers, IIS servers, and Microsoft Exchange 2000 Server. Scenario 2, which is for the enterprise client environment, also contained the Public Key Encryption (PKI) Certification Server and IAS server roles.

For the Level 1 lockdown scenario, the Microsoft Solutions for Security (MSS) test environment consisted of four clients with the following operating systems:

1. Microsoft Windows 98 SR2
2. Windows NT® 4.0 Workstation SP6a
3. Windows 2000 Professional SP3
4. Windows XP Professional SP1 Desktop Clients

For the Level 2 and Level 3 lockdown scenarios, the MSS test environment consisted of three clients with the following operating systems:

1. Windows 2000 Professional SP3
2. Windows XP SP1 for desktop clients
3. Windows XP SP1 for laptop clients

For testing IAS in the Level 2 scenario, a RADIUS client was used The RADIUS client software emulates a Network Access Server (NAS) which can send, among others things, RADIUS Access–Request messages to a RADIUS server.

The Level 3 scenario also consisted of a stand–alone Windows 2003 Server configured to run the Bastion Host.

Lab Network Diagrams

The following illustration shows the three scenarios that were implemented in the test lab.

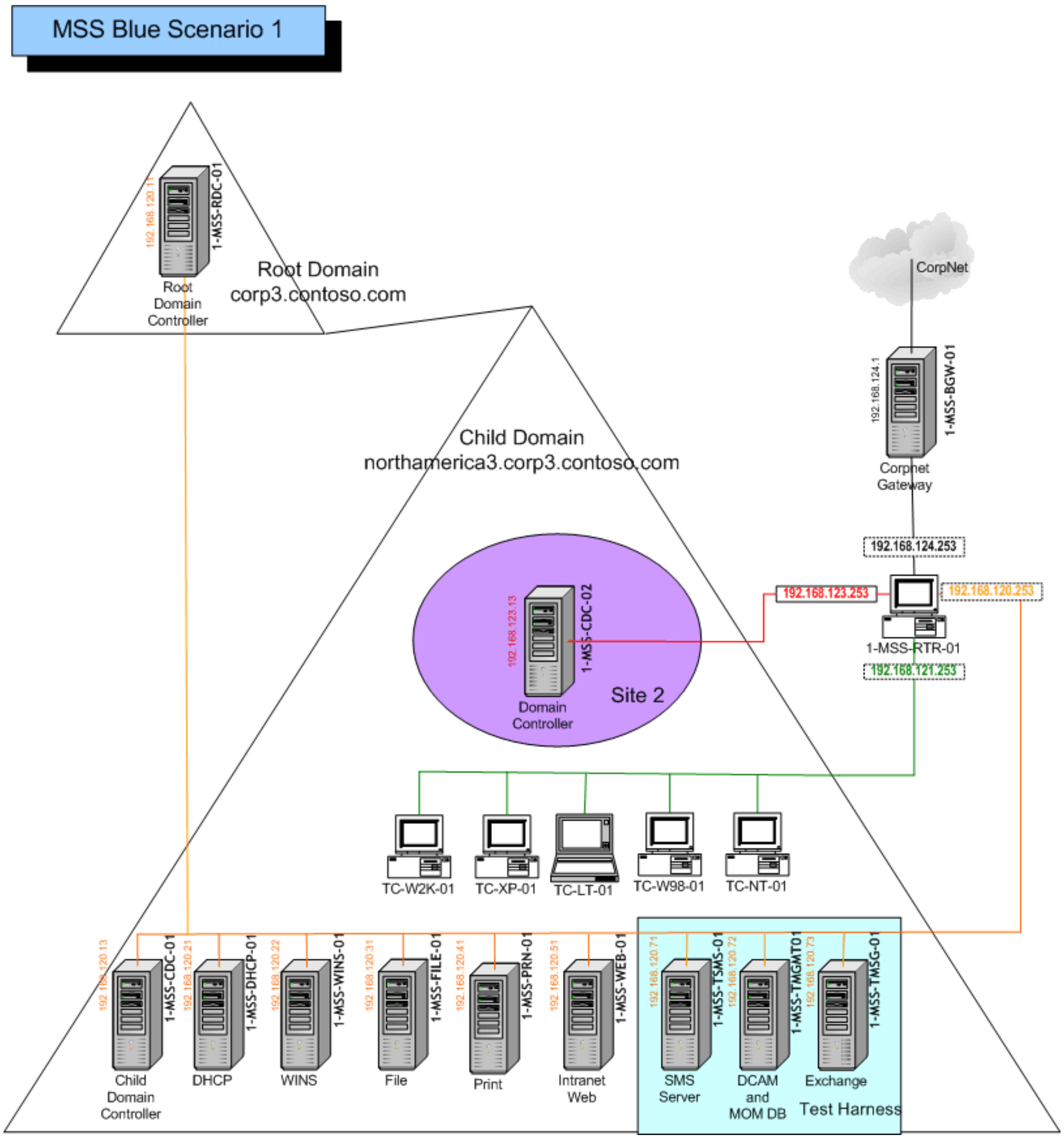

Figure 1.1

Lab diagram for scenario 1: Legacy Client environment

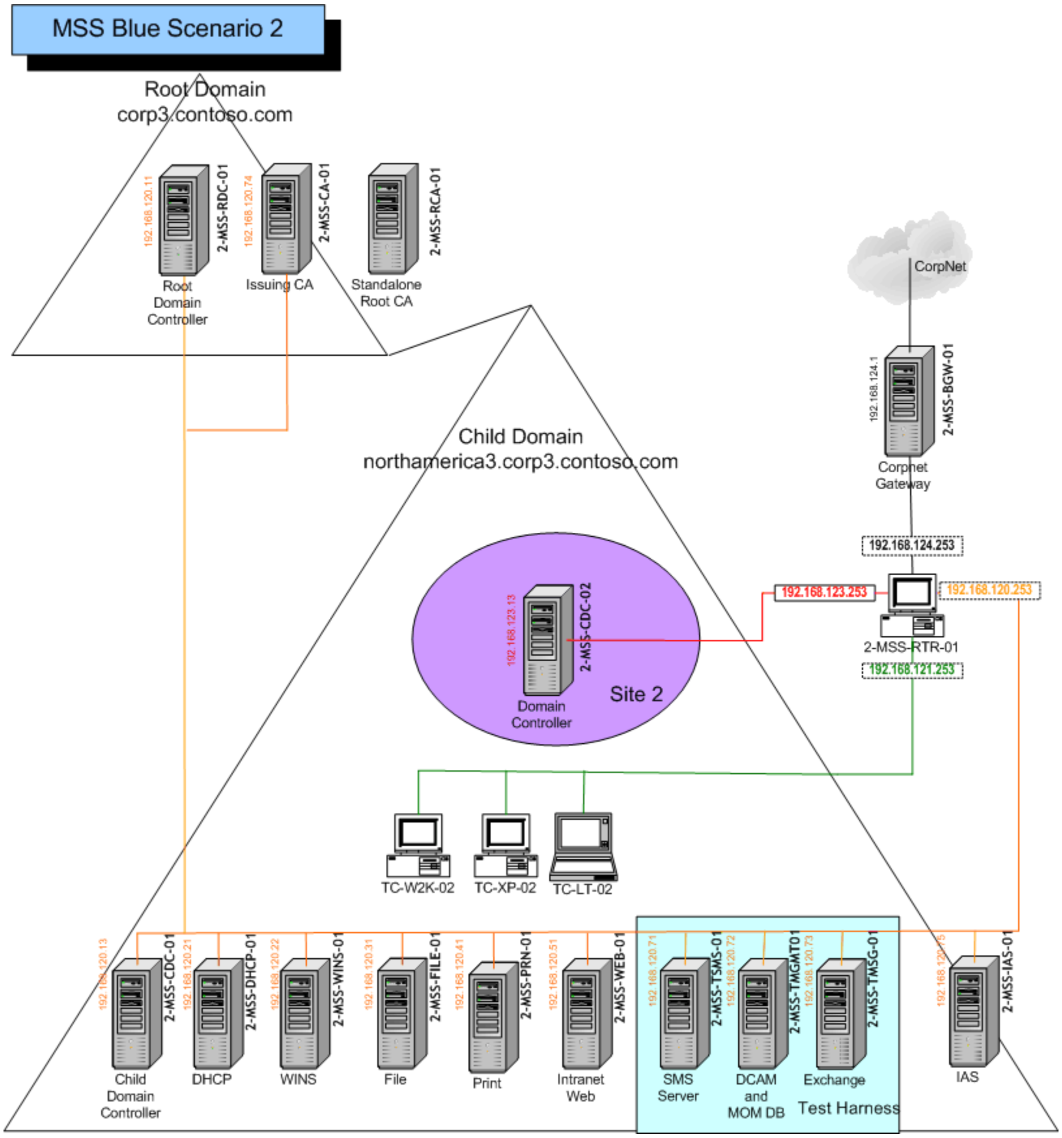

Figure 1.2

Lab diagram for scenario 2: Enterprise Client environment

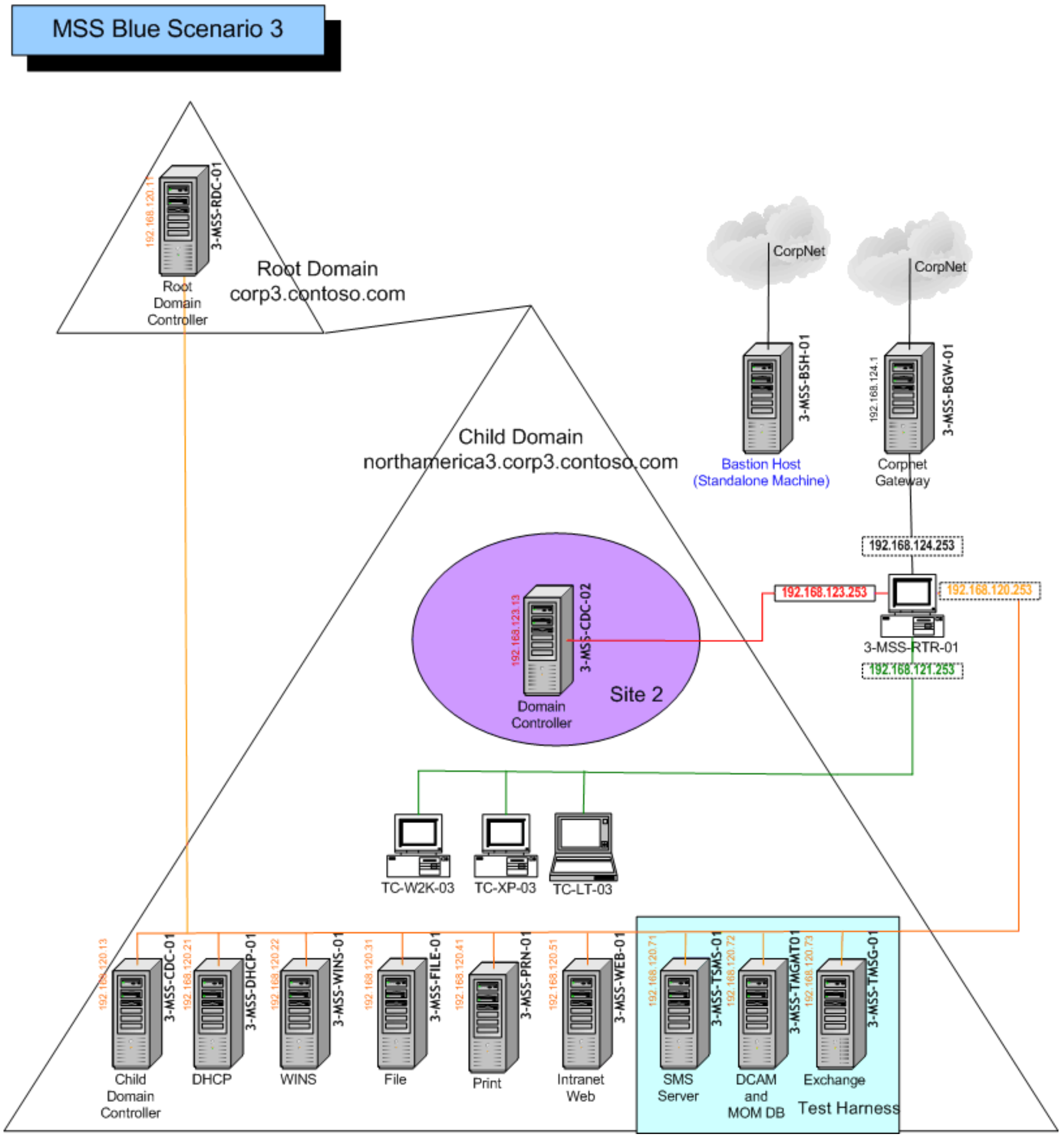

Figure 1.3
Lab diagram for scenario 3: High Security Client environment

Test Cycles

Testing with multiple test cycles ensures that issues found in test cycle *N* are resolved in regressive test cycle *N* + 1. This process ensures a high quality solution. The test team executed two identical test cycles.

Before starting the first test cycle, a test prep phase was undertaken. This phase is explained in the "Security Build Phases" section of this guide. The baseline images of the test machines were used as the starting point of the second test cycle. Therefore, the test prep phase was not undertaken before the second test cycle.

At the end of the second test cycle, the solution reached a stable state.

Types of Test Procedures

The test team performed the following three kinds of tests to ensure that the build met the test objectives of the project.

Base Deployment Tests

In this test category, the test team verified the correctness of procedures and functions for building security into computers running Windows Server 2003. This test category helped identify inconsistencies between the Security Guide, the functional design specification document and the tools developed with the Security Guide. These tests were done prior to server hardening. No test cases were exclusively designed for this purpose and testing was ad–hoc in nature.

Functionality Tests

This test category consisted of a set of core functionality test cases designed to confirm the expected behavior of each server role defined in the guide that Windows Server 2003 is capable of performing. Specifically, the roles developed and tested in the test environment included those for domain controllers, WINS, DHCP, IIS, File, Print, CA, IAS and Microsoft Operation Manager (MOM). The MOM server was not hardened and was considered as a part of the test harness. Test cases were designed to ensure that there is no unexpected loss of functionality after each server was hardened according to the guidance provided in the Security Guide.

Interoperability

This test category consisted of test cases used to determine that clients could continue to use the core services of all servers after the servers had been hardened.

Pass and Fail Criteria

Before starting test execution cycle 1, the following criteria were defined to ensure defect prevention and bug resolution:

- All test cases must pass with expected results as outlined in the individual test case spreadsheets.
- A test case is considered to have passed if the actual result matched the expected result documented for the test case. If the actual result does not match the expected result, it was treated as a failed test case and a bug was created and a severity score assigned.
- If a test case failed, it was not assumed that the solution guidance was necessarily defective. For example, misinterpretation of product documentation, incomplete documentation, or inaccurate documentation, as well as Windows Feature Bugs could cause failures. Each failure was analyzed to discover its cause based on actual results, and the results described in project documentation as well as escalated to the correct Microsoft owners of the respective products.

Security Build Phases

A security build phase had a clear set of procedures. Any critical issues found in a build phase were documented as bugs and resolved in that phase before the test team moved on to the next incremental build phase. This ensured that critical issues were resolved in a short duration. This saved time and the cost of debugging preventable issues found in the test lab in later phases.

The next subsections describe the Test Prep Phase, and the three Security Build phases.

Test Prep Phase

Before executing the build phases, a test prep phase was executed.

This phase consisted of setting up the base network to which the solution was applied and consisted of the following steps:

1. Setting up the Lab setup according to the Network diagram with the Base operating system installed on all servers and clients.
2. Configuring each server role.
3. Installing all third–party applications on clients.
4. Executing tests to verify the functioning of Test Harness servers.
5. Executing interoperability test to verify client accessibility of a limited set of services provided by domain controllers and member servers (DNS, DHCP, File, Print, and IIS, IAS, CS, Bastion Host).
6. Taking ghost images of builds based on successful execution of the above mentioned tests with appropriate results. This ghosted environment was used as the baseline for the testing of the solution.

Manual Server Configuration Phase

This phase usually, but not, allows the first security build phase. Typically this phase consists of the following security build procedures.

1. The Microsoft Computer Management Console (MMC) is used to change the prescribed settings such as the local administrator account and password on each member server in the Security Guide. Specific steps in the direction of securing the Domain Accounts (guest and administrator accounts) are to:
   - Disable the guest account.
   - Ensure that the built-in administrator account has a complex password, has been renamed, and has had its default account description removed.
   - Follow the Security Guide prescription on additional steps to take towards securing the domain accounts.
2. Securing the Service Account: Windows 2003 services can be run under the local system account, domain account or local account. It was ensured that services were run under local account rather than domain user accounts and local system accounts. It was also ensured that these service accounts have the minimal rights and privileges that they needed to function and that they had complex passwords.
3. Following the other applicable manual hardening procedures as prescribed by each chapter of the guide.

Group Policy Configuration Phase

In this phase the Group Policy objects (GPOs) were applied to the computers in the domain. This phase consists of the following security build procedures.

1. Creating Organization Units (OU) to support Group Policy recommendations in the security guide.
2. Moving the member servers to the appropriate OU.
3. Adding a new GPO Link for each OU.

   You might need to move the GPO links higher up in the priority list in cases where a default GPO link is already present.
4. Importing the security template into the GPO.
5. Applying the Group Policy on the particular OU depending on which chapter is being tested and on which scenario.

IP Sec Configuration Phase

This phase consisted of implementing IPSec filters on domain controllers and other server roles in the domain. This phase was only applicable to Scenario 3, which requires extremely high security settings. The filters were applied by using the scripts provided with the guide. These scripts have been released in the format: `PacketFilter – `*`XXXX`*`.cmd`, where XXXX represents the member server being hardened.

Test Execution Details

Chapters 2 through 11 of the security guide provide recommendations for securing the domain, domain controller and all the member servers for each of the client environments. These are accompanied by security templates, IPSec filter scripts, and explanation of manual hardening procedure. Based on these recommendations, this section of the test guide explains the details of test execution for validating the guidance contained in chapters 2 through 11 of this guide.

As mentioned earlier, the security build phases are undertaken during the test execution of each chapter. As you read the following section, bear in mind that the Manual Server Configuration phase and the Group Policy Configuration phase were applied to all three client scenarios, however, the IPSec Configuration Phase is undertaken only on the High Security client environment.

Chapter 2

To test this chapter, proceed as follows:

1. Verify that the Test Prep Phase passed successfully.
2. Execute the base deployment tests.
3. Start the manual configuration phase which consists of the following:
    - Synchronize the time of all the Windows Server 2003 member servers and the client computers with the domain controller.
    - Disable the guest account.
    - Rename the administrator and guest accounts.
    - Change the administrator password.
4. Implement the Group Policy configuration phase, which consists of the following steps:
    - In the northamerica3.corp3.contoso.com domain create an OU for Member Servers and within that create OUs for Infrastructure (DHCP, WINS), File, Print IIS, IAS, and CA, and then move the member servers to their respective OUs.
    - Create administrative groups, include the appropriate domain members in these groups, and delegate administrative rights to them over the appropriate OUs.
    - Link a new GPO to the domain, up its precedence and import the Domain.inf security template into it.

The IPSec Policy Configuration Phase is not applicable for this chapter. You are now ready to execute the Functionality and Interoperability tests for this chapter. For this chapter test cases have to be run on all servers. The Functionality test cases for different servers are provided on different sheets of a Microsoft Excel workbook included with this guide.

Chapter 3

This chapter addresses the issue of creating a member server baseline policy (MSBP) where all servers have the same basic level of security. Test execution is as follows:

1. Execute the Base Deployment tests and verify that all the recommendations in the guide are appropriate for your environment. Modify the security template settings as needed before you proceed.
2. Execute the Manual Configuration Phase based on specific requirements included at the end of the chapter.
3. Link a new GPO to the Member Server OU. Import the appropriate (client-scenario specific) Member Server Baseline.inf security template into the GPO.
4. There are no IPSec scripts to be run in this chapter so proceed to the execution of functionality and interoperability tests. Refer to Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 4

This chapter addresses the issue of hardening the domain controllers. Test execution is as follows:

1. Execute the Base Deployment tests.
2. Execute the Manual Configuration Phase based on specific manual execution steps recommended at the end of the chapter.
3. Link a new GPO to the Domain Controllers OU. Import the appropriate Domain Controller.inf security template into the GPO.
4. Execute the IPSec Configuration phase on the High Security client environment. This consists of running the IPSec filter scripts, provided with the Security Guide, on each of the domain controllers.
5. Execute the functionality and interoperability tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 5

This chapter deals with hardening the Infrastructure servers namely DHCP and WINS. Although a DNS server is also an Infrastructure server, in the case of the Active Directory Integrated DNS, the domain controllers themselves take on the role of DNS server. Hence, the Infrastructure OU in the three client environments described in Chapter 1 of the security guide only consists of the DHCP and WINS server. Keep in mind that the WINS server is an absolute must in the Legacy Client environment but is optional in the other two environments.

Test Execution for this chapter proceeds as follows:

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Execute the Manual Configuration Phase based on specific manual execution steps recommended at the end of the chapter.
3. Link a new GPO to the Infrastructure OU. Import the appropriate Infrastructure Servers.inf security template into the GPO.
4. Execute the IPSec Configuration phase on the High Security client environment. This consists of running the IPSec filter scripts, provided with the Security Guide, on the respective infrastructure server.
5. Execute the functionality and interoperability tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 6

Test Execution for this chapter proceeds as follows:

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Execute the Manual Configuration Phase based on specific manual execution steps recommended at the end of the chapter.
3. Link a new GPO to the File Server OU. Import the File Server.inf security template into the GPO.
4. Execute the IPSec Configuration phase on the High Security client environment. This consists of running the IPSec filter script provided with the security guide, on the file server(s).
5. Execute the functionality and interoperability tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 7

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Execute the Manual Configuration Phase based on specific manual execution steps recommended at the end of the chapter.
3. Link a new GPO to the Print Server OU. Import the Print Server.inf Security Template into the GPO.
4. Execute the IPSec Configuration phase on the High Security client environment. This consists of running the IPSec filter scripts, provided with the Security Guide,) on the print server(s).
5. Execute the functionality and interoperability tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 8

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Link a new GPO to the IIS Server OU. Import the IIS Server.inf security template into the GPO.
3. Execute the Manual Configuration Phase based on specific manual execution steps recommended in the chapter.
4. Execute the IPSec Configuration phase on the High Security client environment. This consists of running the IPSec filter scripts, provided with the security guide, on the IIS server(s).
5. Execute the functionality and interoperability tests Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 9

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. There is no Manual Configuration needed for this chapter
3. Link a new GPO to the IAS Server OU. Import the IAS Server.inf security template into the GPO.
4. There are no IPSec Filters to be applied on the IAS Server so proceed with the execution of the functionality tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 10

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Execute the Manual Configuration Phase based on specific manual execution steps recommended at the end of the chapter.
3. Link a new GPO to the CA Server OU. Import the CA Server.inf security template into the GPO.
4. There are no IPSec Filters to be applied on the IAS Server so proceed with the execution of the functionality tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls, Interoperability Test Cases.xls, and Interoperability Automated Test Cases.xls for the test cases executed.

Chapter 11

1. Execute the Base Deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Execute the Manual Configuration Phase on the Bastion Host based on specific manual execution steps recommended at the end of the chapter. Bear in mind that the bastion host settings are provided only for the High Security client environment and have been tested thus.
3. Since the Bastion Host is a stand–alone server outside the perimeter network (also known as DMZ, it cannot be hardened through Group Policy application on the domain controller. Instead you need to follow the local policy application steps outlined in the Applying the Bastion Host Local Policy subsection detailed in Chapter 11, "Hardening Bastion Hosts," of the Security Guide.
4. Execute the IPSec Configuration phase. This consists of running the IPSec filter scripts, provided with the security guide, on the bastion host.
5. For purposes of testing the Bastion Host, both FTP, Web, and SMTP functionality was verified. For this the appropriate Windows Components were enabled through the Add/Remove programs in the control panel.
6. Execute the functionality tests. Refer to the attached Excel workbooks: Functionality Test Cases.xls and Interoperability Test Cases.xls, for the test cases executed.

Release Criteria

The primary release criterion for the *Windows Server 2003 Security Guide* was tied to the severity of bugs still open after all major test phases for the guide were completed. However, other issues not being tracked through bugs were also discussed. The criteria for release are listed below:

1. No open bugs with severity levels of 1 or 2.
2. All open bugs are triaged by the leadership team, and their impacts are fully understood.
3. Solution guides are free of comments and revision marks.
4. Solution successfully passes all test cases in the Test Lab environment.
5. Solution contents are without conflicting statements.

Bug Classification

The bug severity scale is described in the table below. The scale ranges from 1 to 4, where 1 represents the highest severity, and 4 the lowest.

Table 1: Bug Severity Classification

Severity	Most Common Types	Conditions Required
1	Bug blocked build or further test. Bug caused unexpected user accessibility. Steps defined in the documentation were not clear. Results or behavior of a function or process contradicts expected results (as documented in functional specification).	Solution did not work. User could not begin to use significant parts of the system. User had access privileges that should not be allowed. User access was blocked to certain server that should be allowed. Expected results were not achieved.
2	Steps defined in the guide are not clear. Documented functionality is missing (in this case, test was blocked). Documentation is missing or inadequate.	User had no simple workaround to mend situation. User could not easily figure out workaround. Primary business requirements could not be met by the system.
3	Documented format issue. Minor documentation errors and inaccuracies. Text misspellings.	User has a simple workaround to mend situation. User can easily figure out workaround. Bug does not cause a bad user experience. Primary business requirements are still functional.
4	Suggestions. Future enhancements.	Clearly not a bug related to this version.

Penetration Testing

To validate this guidance, Microsoft employed a third party to perform simulated penetration tests against the enterprise and high security environments defined in this guide. The penetration tests were performed in two phases: The first phase consisted of external attacks on the environments with no knowledge of the systems or their configuration. The second phase consisted of attempts to elevate an authorized user's privileges in each of the environments.

The penetration testing identified one vulnerability that was previously determined as out of scope for the *Windows Server 2003 Security Guide*. This reported vulnerability was related to the fact that Kerberos traffic could potentially be intercepted and attacked to obtain the users password using brute force methods. This vulnerability could be mitigated by encrypting all network traffic with IPSec or through the use of complex passwords. This guide mitigates this issue by recommending the implementation of complex passwords for all accounts. Because of this recommendation, this vulnerability could not be exploited within the testing time frame.

Aside from this known issue, no other vulnerabilities were discovered. The servers remained secure after several weeks of penetration attacks.

Conclusion

All of the test cases executed by the test team passed with expected results. The test team was able to confirm that after applying the prescription provided by the *Windows Server 2003 Security Guide* for the three client scenarios defined in the guide, requisite functionality that the servers were expected to provide was indeed available.