



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>

Validation of Network Traffic Encryption

GSNA Practical Assignment version 3.0
Option 1

Author: Michael Jenkins
May 02, 2004

© SANS Institute 2004, Author retains full rights.

Table of Contents

Overview	3
Part #1 (01.0) Research in Audit, Measurement Practice, and Control	4
Part #1 (01.1) Identify the System to be Audited	4
Part #1 (01.2) Evaluate the Most Significant Risk to the System.....	6
Part #1 (01.3) What is the Current State of Practice.....	9
Part #2.....	11
Part #2 (02.0) Create an Audit Checklist	11
Part #2 (02.1) Policy Review	11
Part #2 (02.2) Physical Security Review.....	11
Part #2 (02.3) Access Control Review	11
Part #2 (02.4) Review of Administrative of Logs and Monitoring	12
Part #2 (02.5) Checklist	13
Part #3.....	19
Part #3 (03.0) Conduct The Audit	19
Part #3 (03.1) Testing	19
Part #3 (03.2) Evidence	27
Part #4.....	28
Part #4 (04.0) Audit Report or Risk Assessment	28
Part #4 (04.1) Audit Findings	28
Conclusion	30
Appendix A Server and Network Documentation.....	31
Appendix B Protocol Analyzer - Ethereal Capture PC Client Port 9090	36
Appendix C Nessus Scan Results	41
Appendix D Qualysguard Consultant Scan Results.....	42
Appendix E Antivirus, Backup Scripting.....	45
Appendix F MS Baseline Security Analyzer - Results	49
Appendix G Protocol Analyzer - Ethereal Capture Port 3389	52
Appendix H References.....	54

Overview

Loanaranger.tld sells a loan management package used by financial institutions. The purpose of the audit is to validate the assertion of a third party software developer that the version update to the Loanaranger software application provides encryption of the data while transiting the network between a Windows PC client and the central Windows 2003 Standard server. A previous audit obtained by Loanaranger.tld showed that the traffic was encrypted in the earlier version of this same software.

The scope requested by Loanaranger.tld management was to exclusively validate the encryption on the network. The scope was increased by agreement to include a vulnerability scan of the Windows 2003 server to determine if it continues to conform to the previous baseline.

© SANS Institute 2004, Author retains full rights.

Part #1 (01.0) Research in Audit, Measurement Practice, and Control

Part #1 (01.1) Identify the System to be Audited

Client (End User) PC - Not In Scope

The Loanranger client application can be deployed on any Windows PC operating system from 95 to XP. The third party software developer terms the application a 'Thin Client'. Deployment frequently involves multiple branch premises communicating through a VLAN or VPN operated by the consumer and constituting a secure LAN within the financial institution. The client system (PC) operating system security is out of scope for this audit.

The client application consists of a single compiled executable and one configuration file (.ini). The contents of the configuration file are clear text (ASCII). Two discrete entries in the configuration file contain sensitive information.

- 1) One entry contains the 'FQDN name' (Fully Qualified Domain Name) of the remote server pointing to the external firewall (WAN) interface of Firewall One. See Appendix A.
- 2) One entry contains the unique TCP port number which is common to all PC systems operated by a single consumer of Loanranger software.

Possession of the configuration file contents would require possession of a valid USERID and PASSWORD in addition to the Loanranger executable client to constitute a security threat.

Server – In Scope

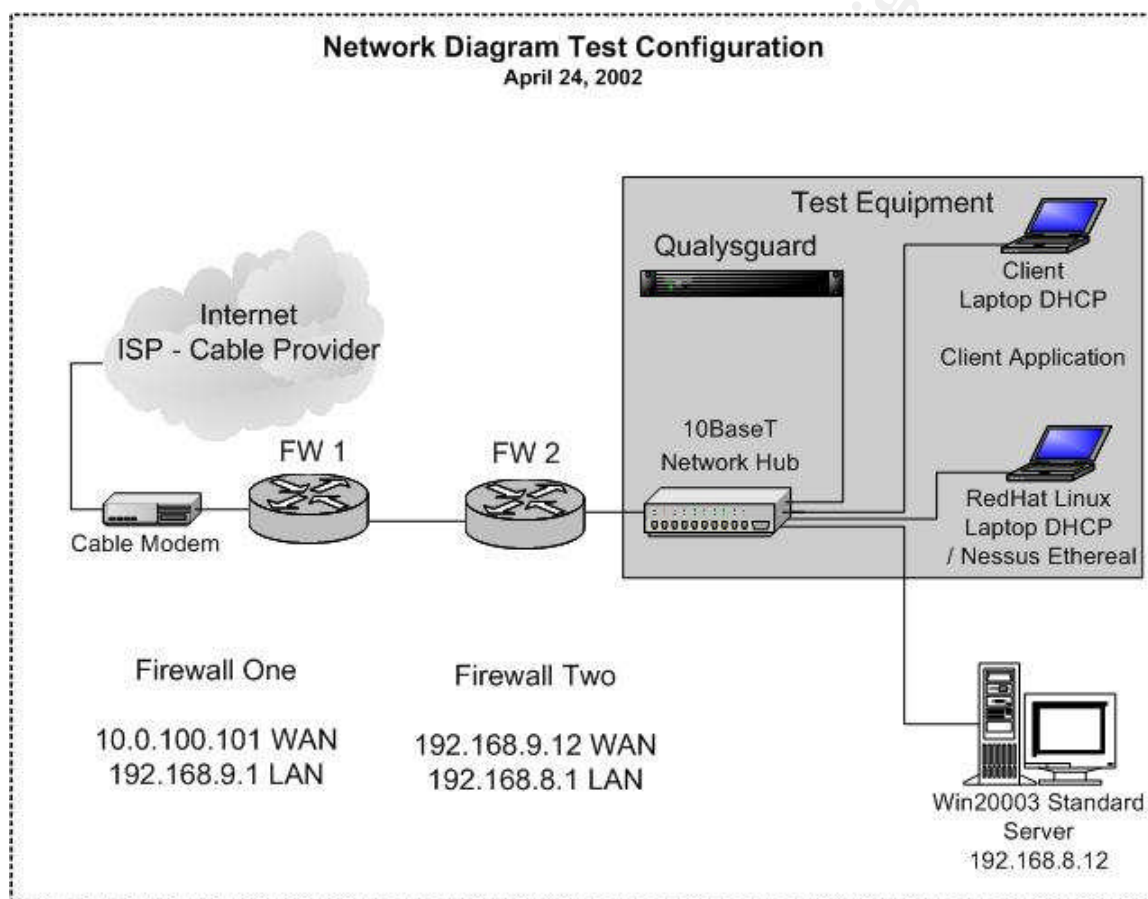
A single Windows 2003 Standard server hosts data for multiple financial institutions. Borland Interbase version 6.0 [<http://www.borland.com/interbase/>] and Asta version 1.0 [<http://www.astatech.com/index.asp>] are implemented on the server. Interbase is an SQL database application. Asta is implemented as a service listening on server TCP ports. The Asta components are embedded in the compiled executable aboard both the client PC and central server.

In this implementation Asta passes the SQL queries from the client PC system to the central server and returns results from the Interbase database.

Interbase is outside the scope of this audit. The Asta server is configured to exclusively accept traffic from TCP ports at IP Address 192.168.8.12. A single discrete port is allocated for each remote financial institution. Multiple PC clients can have simultaneous connection to the single TCP port.

The traffic between the client PC and the central server is in scope for this audit. Traffic on the TCP Port for the test system (in this case port 9090) will be captured and reviewed for content.

By agreement the scope includes vulnerability scanning of the Windows 2003 Standard server. The client administration staff periodically executed an audit scope against this server using Nessus. An additional scan will be executed with Qualysguard and a comparison of results presented to Loanaranger management. See Appendices [C](#) and [D](#).



Part #1 (01.2) Evaluate the Most Significant Risk to the System

The Loanaranger system is not a critical (Tier 1) business system. Information products (paper reports) from the Loanaranger system are utilized for regulatory disclosure, monthly and board-of-directors reporting functions. These are internal business functions and paper reports can be replaced with modest difficulty and low cost substitute processes.

Any core financial processes are implemented on other servers responsible for day-to-day transactions and business operations of the financial institution operating Loanaranger.

The data contained in the Loanaranger system is located on paper based records maintained within the financial institution without exception. The reports and information products produced by the system can be produced manually. The balances and values calculated by the Loanaranger system are cross checked against information products from the Tier 1 core business systems.

Description of Risk Source	Likelihood	Consequence	Risk (1=Low)
Data in Transit on Network			
- Checklist Item T2	MEDIUM	MEDIUM	6
Server			
Audit Local Policy			
- Ensure Event Logs Contain Account Logon Audit			
- Checklist A3	MEDIUM	MEDIUM	7
Physical Risks			
- Server damaged or stolen			
- Unauthorized persons gain access to console			
- Checklist Items P1	LOW	LOW	2
Administrative Risks			
- Configuration degraded			
- Checklist Items A1, A2	HIGH	HIGH	8
Remote Access Risks			
- Attacker obtains access			
- Checklist Items T1, T7	HIGH	HIGH	8
Operating System Vulnerabilities			
- Attacker obtains access or degrades configuration or service using wide variety of vulnerabilities and exploits			
- Checklist Items T1, T3, T4, T5, T6	MEDIUM	MEDIUM	7

Technical Checklist Items, T1, T2, T3, T4, T5, T6, T7

Administrative Checklist Items, A1, A2, A3

Physical Checklist Items, P1

Significant Risk	Description
Threat	Insecure Windows Operating System
Capacity to inflict damage	HIGH – using the default settings for Windows 2003 Standard server leaves the system open to exploitation by reasonably unskilled attackers. Example - the default setting allows anonymous FTP access enabled.
Major information asset	Data used to produce reports is stored in the back end (Interbase) database. Loss or unavailability of this data precludes producing reports with the system.
Major Vulnerability	Operating system vulnerabilities are a broad category of issues. The dynamic nature of operating systems involving patches and upgrades presents opportunity for new exploits with increasing frequency. Example: Guest account access is not disabled and a potential attacker could gain access and with proper exploit tactics escalate the account privilege.
Control Objective	Verify configuration implements 'best practices' recommended for known vulnerabilities and exploits for Windows operating system. Test against the SANS Top 20 vulnerabilities: W1 Internet Information Services (IIS) W2 Microsoft SQL Server (MSSQL) W3 Windows Authentication W4 Internet Explorer (IE) W5 Windows Remote Access Services W6 Microsoft Data Access Components (MDAC) W7 Windows Scripting Host (WSH) W8 Microsoft Outlook and Outlook Express W9 Windows Peer to Peer File Sharing (P2P) W10 Simple Network Management Protocol (SNMP)
Risk	HIGH – well publicized avenues of attack with 'exploitation kits' readily available
Compliance	Vulnerability scanning
Test	T1, T3, T4, T5, T6, T7, A1, A2
Objective/Subjective	
Reference	
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

Significant Risk	Description
Threat	Unencrypted information in transit on network
Capacity to inflict damage	HIGH – the client / server model of deployment requires that user input, database queries and responses are sent between the client (end-user) PC and the central Windows 2003 Standard server. If this data is not encrypted it is likely that reasonably untrained attackers can utilize shareware tools and capture the information.
Major information asset	Information on customers of financial institutions frequently includes sufficient information to facilitate identity theft. Additionally the Loanaranger.tld information products could be used to produce significant competitive advantage for those competing with customers of the financial institution in the business place.
Major Vulnerability	Data is not encrypted in TCP packets
Control Objective	Ensure executables provided by the 3 rd party software vendor encrypts the data between the client (end-user) PC and the central Windows 2003 Standard server.
Risk	HIGH – UserID and Password information along with SQL requests in clear text can be exploited against the server. This would require having direct physical access to an account authorized to execute SQL queries or a copy of the Loanaranger executable software.
Compliance	Network Protocol Analysis
Test	T2
Objective/Subjective	
Reference	
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

© SANS Institute

Part #1 (01.3) What is the Current State of Practice?

Shareware and Commercial Audit Tools - GNSA Practical v. 3.0

Tool	Purpose	Source for Info.	Type of Tool
ISS' Internet Scanner	Vulnerability Scanner	http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php	Commercial
Tcpdump	Network Protocol Analyzer	www.tcpdump.org	Shareware/Freeware
Nmap	Network Port mapper	www.insecure.org/nmap	Shareware/Freeware
HFNetChk	Windows OS Security Patch Status	www.microsoft.com/technet/security/tools/hfnetchk.msp	Shareware/Freeware
John the Ripper	Password Cracker	www.openwall.com/john/	Shareware/Freeware
L0phtCrack	Password Cracker	www.evadenet.com/downloads/lophtcrack.shtml	Shareware/Freeware
Router Audit Tool (RAT)	Router Configuration Analysis	http://www.cisecurity.org/bench_cisco.html	Shareware/Freeware
Toolset Selected for This Audit			
Qualysguard	Vulnerability Scan	www.qualys.com	Commercial
Nessus	Vulnerability Scan	http://www.nessus.org	Shareware/Freeware
Ethereal	Network Protocol Analyzer	www.ethereal.com	Shareware/Freeware
Microsoft Baseline Security Analyzer V1.2	Windows OS Security Patch Status	http://www.microsoft.com/technet/security/tools/mbsahome.msp	Shareware/Freeware

Toolset Selected for This Audit

Qualysguard is a commercial vulnerability scanning tool. It has features which are available in shareware / freeware products. The Qualysguard scanner is was selected for this audit and the results will be compared to the Nessus product (briefly) for the purposes stated in the scope. Features in Qualysguard produce network maps (similar to Nmap), it uses brute force password cracking (features similar to Brutus (<http://www.hoobie.net/brutus/index.html>)) and there are many more examples. Qualys provides over 3400 vulnerability tests at this writing.

Nessus is a shareware / freeware vulnerability scanning toolset. It has over 2100 (<http://cgi.nessus.org/plugins/dump.php3?viewby=family>) vulnerability plug-ins at this writing. The administrative staff for Lonaranger.com is presently using Nessus. The

comparison to Qualysguard will give management the ability to assess the sufficiency of the tactics used by the administrative staff.

Ethereal is a network protocol analyzer and was selected over TCPDUMP due to easy availability on the Red Hat 'Fedora Core 1' test platform prepared for this audit. Ethereal has an excellent selection of protocol decoders (<http://www.ethereal.com/docs/user-guide/x56.html>). None are required for this audit.

"The Microsoft® Baseline Security Analyzer (MBSA) is a tool that allows users to scan one or more Windows®-based computers for common security miss-configurations. MBSA will scan a Windows-based computer and check the operating system and other installed components, such as Internet Information Services (IIS) and SQL Server™, for security miss-configurations and whether or not they are up-to-date with respect to recommended security updates." quote from their site at (<http://www.microsoft.com/technet/security/tools/mbsawp.mspx>).

Alternative useful toolsets not selected for this audit.

"Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing." quoted from their website (reference above). This is a useful tool but with the diagram (Appendix A) there is no uncertainty as to LAN topology in the scope of this audit. The tool was not used for this audit.

HFNetChk v3.82 is available through the command line interface of the [Microsoft Baseline Security Analyzer \(MBSA\) Version 1.1.1](http://www.microsoft.com/technet/security/tools/hfnetchk.mspx). This tool has not been selected for this audit. It is useful to confirm the status of patches and hot fixes for Microsoft Windows operating systems.
<http://www.microsoft.com/technet/security/tools/hfnetchk.mspx>

TCPDUMP was not selected for this audit. <http://www.tcpdump.org/> It is a useful tool with similar features to Ethereal. TCPDUMP will 'dump' traffic from the network so that it can be inspected.

ISS' Internet Scanner This is a commercial vulnerability scanner with features similar to Qualys and Nessus with overlap to other toolsets mentioned above. It was not available for this audit.
http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php

Part #2

Part #2 (02.0) Create an Audit Checklist

Part #2 (02.1) Policy Review

Loanaranger.tld does not have published security or administrative procedures. The administrative staff maintains deployment documentation on selected configuration items. The audit will attempt to compare the configuration of the deployment as found with the deployment documentation. See Step A2.

Part #2 (02.2) Physical Security Review

The network equipment, cable modem, firewall one, firewall two, and central server are located in a locked premise. Only system administrative staff has physical access to the equipment. Locked doors on the premise preclude unauthorized access. Two administrators have keys to the premise.

Uninterruptible power (UPS) systems with adequate battery capacity for the equipment are provided.

Alternate server equipment is located in a hot spare configuration at a remote site. See Physical Checklist item P1.

Part #2 (02.3) Access Control Review

Access to the client or end user PC systems is at the discretion of the consumer of the Loanaranger software. Access to central Windows 2003 server is controlled by :

- 1) Remote Access via Windows Terminal Services (Remote Desktop)
 - a. Three administrators have user accounts with access
 - b. One business owner has an account with access
 - c. Security logging is enabled by Windows 2003 Server policy
See Step A3.
- 2) Appropriate training has been provided to the administrators
- 3) Network access is controlled by :
 - a. configuration of ICF (Internet Connection Firewall)
 - b. the Windows 2003 Standard server (see Appendix A diagram)
is the only device on the LAN during production use

Part #2 (02.4) Review of Administrative of Logs and Monitoring

The central Windows 2003 Standard server security policy and audit policies need to be validated to ensure they are configured to gather sufficient information into the event logs to enable monitoring of use, access, and operational parameters. See Step A3.

Procedures are in place for the administrative staff to periodically review the logs and take appropriate actions. However, these procedures are not formalized nor written.

© SANS Institute 2004, Author retains full rights

Part #2 (02.5) Checklist

Technical Checklist

STEP # T1	Insecure Windows Operating System
Control Objective	Verify configuration implements 'best practices' recommended for known vulnerabilities and exploits for Windows operating system. Test against the SANS Top 20 vulnerabilities. W1 Internet Information Services (IIS) W2 Microsoft SQL Server (MSSQL) W3 Windows Authentication W4 Internet Explorer (IE) W5 Windows Remote Access Services W6 Microsoft Data Access Components (MDAC) W7 Windows Scripting Host (WSH) W8 Microsoft Outlook and Outlook Express W9 Windows Peer to Peer File Sharing (P2P) W10 Simple Network Management Protocol (SNMP)
Risk	HIGH – well publicized avenues of attack with 'exploitation kits' readily available
Compliance	Vulnerability scanning Qualysguard and Nessus tests to be compared Expect Ports 21, 3389 and 9090 open Unavailability of other ports will confirm compliance
Test	Nessus Configure for all testing, exclude dangerous using the 'plug-in's' Set the safety and optimization features Configure the target system as 192.168.8.12 Execute the scan Qualysguard Configure in-depth testing Full TCP scan, Bandwidth Impact Maximum, Exhaustive Password Brute Forcing, standard UDP port list, Perform 3-way Handshake, scan up to 15 hosts in parallel, Load balancer detection OFF, ICMP Host Discovery. Configure the target system as 192.168.8.12 Execute the scan
Objective/Subjective	Objective
Reference	http://www.sans.org/top20/
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # T2	Unencrypted information in transit on network
Control Objective	Ensure executables provided by the 3 rd party software vendor encrypts the data between the client (end-user) PC and the central Windows 2003 Standard server
Risk	HIGH – UserID and Password information along with SQL requests in clear text can be exploited against the server. This would require having direct physical access to an account authorized to execute SQL queries or a copy of the Loanranger executable software.
Compliance	Network Protocol Analysis Ethereal
Test	Ethereal Initiate a capture session Execute the capture
Objective/Subjective	Objective
Reference	http://www.ethereal.com
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # T3	Antivirus software installed
Control Objective	Verify that an antivirus software package is installed, configured correctly, obtaining and deploying updates properly
Risk	HIGH – new threats discovered daily
Compliance	Visually confirm software present and configuration
Test	Symantec Antivirus Corporate Edition v8.00 Open the Symantec application Select Configure Menu – verify real time protection Select OK – verify Virus Definition file date and version Review Application Event Log to confirm updates Alternately verify file dates in LiveUpdate Directory
Objective/Subjective	Objective
Reference	Installation Guide for Symantec AntiVirus Corporate Edition 8.1.
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # T4	Perimeter Protection
Control Objective	Verify the firewall configuration implements controls to incoming packets
Risk	HIGH – Systems without firewall protection are open to external attack.
Compliance	Review Windows 2003 Standard Server 'Advanced' properties on Network Properties interface Business Requirements allow TCP traffic on ports for each financial institution, 3389 (Remote Desktop) and 21 (FTP)
Test	Click Start – Settings – Network Connections Select LAN interface Right Mouse Select Properties Select Advanced Tab Observe Checkmark for “ Internet Connection Firewall” Select Settings Observe Ports Allowed
Objective/Subjective	Objective -
Reference	http://support.microsoft.com/default.aspx?scid=kb;en-us;317530&Product=winsvr2003
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # T5	NTFS File System
Control Objective	Ensure that the file system uses NTFS
Risk	HIGH – security is not available on other Microsoft file systems
Compliance	FAT and FAT32 file systems should not be used
Test	From a DOS command C:\>chkntfs c: Alternately observe finding in MS Baseline Report Appendix F
Objective/Subjective	Objective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # T6	Communications between central Windows 2003 Standard server and remote administrative platforms
Control Objective	Ensure that communications is encrypted
Risk	MEDIUM – security is not available on other Microsoft file systems
Compliance	Windows Remote Desktop can be configured to enable encryption of the session Ethereal can be used to capture session (Appendix G)
Test	Select Start > Programs > Administrative Tools Select Terminal Services Configuration Select Connections in the left console panel Select RDP-TCP in the right console details pane Select Right Mouse > Properties Click the General tab Observe the details stating all communications are encrypted or the client cannot connect. Review Ethereal Protocol Analysis in Appendix G
Objective/Subjective	Objective
Reference	http://support.microsoft.com/default.aspx?scid=kb;en-us;814590&Product=winsvr2003
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

© SANS Institute 2004

Administrative Checklist

STEP # A1	Backup and Recovery
Control Objective	Ensure the system has adequate backup and that a recovery process or procedure can be executed
Risk	HIGH – The Windows 2003 Standard Server is a single point of failure unless there are adequate provisions for continued operations in the event the server is unavailable
Compliance	Review backup procedures, verify the backup is executing on schedule, verify the restore process results in a working system
Test	Review procedures and documentation with administrative staff
Objective/Subjective	Subjective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # A2	Compliance of deployment to administrative deployment notes
Control Objective	Validate that the method of deploying the ASTA server component is consistent with established tactics
Risk	Improper configuration can cause the system to fail
Compliance	Review the Windows Scheduled Task command line
Test	Open the Windows Control Panel Select Scheduled Tasks Select the Asta Server item (Testbank) Right Mouse Select Properties Compare the Run, Start In, and Run as, Items to the administrative documentation. Sample Value Expected: d:\directory\testbank\AstaIBExpressServer.exe PORT=9090 DATABASE=127.0.0.1:d:\directory\testbank\testbank.gdb USER_NAME=xxxxxxx PASSWORD=xxxxxxx
Objective/Subjective	Objective
Reference	http://www.astatech.com/support/servers.htm Select the IBExpress .zip package
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

STEP # A3	Audit Policy – Local Security Settings
Control Objective	Validate that the audit policy
Risk	Improper configuration precludes review of vital security information
Compliance	Review the Windows Local Security Settings
Test	Select Run from the Start menu %SystemRoot%\system32\secpol.msc /s Select Local Policies Select Audit Policy Observe security settings include failure at minimum: Confirm Security Events
Objective/Subjective	Objective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

Physical Checklist

STEP # P1	Access to central server
Control Objective	Protect server from unauthorized access
Risk	HIGH – unauthorized access permits malicious configurations, removal of power, theft of system, modification of data
Compliance	Premise has locks and control procedures
Test	Review premise security with administrative staff
Objective/Subjective	Objective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	
Detailed Results	
Stimulus Response	

Part #3 (03.0) Conduct the Audit

Part #3 (03.1) Testing Technical Checklist

STEP # T1	Insecure Windows Operating System
Control Objective	Verify configuration implements 'best practices' recommended for known vulnerabilities and exploits for Windows operating system. Test against the SANS Top 20 vulnerabilities: W1 Internet Information Services (IIS) W2 Microsoft SQL Server (MSSQL) W3 Windows Authentication W4 Internet Explorer (IE) W5 Windows Remote Access Services W6 Microsoft Data Access Components (MDAC) W7 Windows Scripting Host (WSH) W8 Microsoft Outlook and Outlook Express W9 Windows Peer to Peer File Sharing (P2P) W10 Simple Network Management Protocol (SNMP)
Risk	HIGH – well publicized avenues of attack with 'exploitation kits' readily available
Compliance	Vulnerability scanning Qualysguard and Nessus tests to be compared Expect Ports 21, 3389 and 9090 open Unavailability of other ports will confirm compliance
Test	Nessus Configure all testing, exclude dangerous using 'plug-in's' Set the safety and optimization features Configure the target system as 192.168.8.12 Execute the scan Qualysguard Configure in-depth testing Full TCP scan, Bandwidth Impact Maximum, Exhaustive Password Brute Forcing, standard UDP port list, Perform 3-way Handshake, scan up to 15 hosts in parallel, Load balancer detection OFF, ICMP Host Discovery. Configure the target system as 192.168.8.12 Configure the target system from the support interface Execute the scan
Objective/Subjective	Objective
Reference	http://www.sans.org/top20/
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	Appendix C (Nessus) Appendix D (Qualys)
Stimulus Response	

STEP # T2	Unencrypted information in transit on network
Control Objective	Verify that data sent between client PC and central server is encrypted while in transit
Risk	Medium – SQL requests in clear text can only be exploited against the server by having direct physical access to an account authorized to execute SQL queries
Compliance	Network Protocol Analysis Ethereal
Test	Ethereal Initiate a capture session Execute the capture
Objective/Subjective	Objective
Reference	http://www.ethereal.com
RESULTS -	Complete after execution
Test Successful?	NO
Detailed Results	Appendix B (Ethereal)
Stimulus Response	

Ethereal Testbank capture 2 April 25 2004.dat - Ethereal									
File Edit View Go Capture Analyze Statistics Help									
No. .	Time	Source	Destination	Protocol	Info				
72	48.994311	192.168.8.12	192.168.8.200	TCP	9090 > 1162	[ACK]	Seq=14910 Ack=4349 win		
73	48.994571	192.168.8.12	192.168.8.200	TCP	9090 > 1162	[ACK]	Seq=16370 Ack=4349 win		
74	48.994733	192.168.8.12	192.168.8.200	TCP	9090 > 1162	[PSH, ACK]	Seq=17830 Ack=4349 win		
75	48.994737	192.168.8.200	192.168.8.12	TCP	1162 > 9090	[ACK]	Seq=4349 Ack=16370 win		
76	48.994868	192.168.8.200	192.168.8.12	TCP	1162 > 9090	[ACK]	Seq=4349 Ack=18109 win		
77	49.015793	192.168.8.200	192.168.8.12	TCP	1162 > 9090	[PSH, ACK]	Seq=4349 Ack=18109 win		
78	49.025764	192.168.8.12	192.168.8.200	TCP	9090 > 1162	[PSH, ACK]	Seq=18109 Ack=4569 win		
79	49.198101	192.168.8.200	192.168.8.12	TCP	1162 > 9090	[ACK]	Seq=4569 Ack=19238 win		
80	50.614881	192.168.8.200	192.168.8.255	BROWSER	Local Master Announcement N170PLAPTOP, w				
81	51.794800	192.168.8.200	192.168.8.12	TCP	1162 > 9090	[PSH, ACK]	Seq=4569 Ack=19238 win		
82	51.805063	192.168.8.12	192.168.8.200	TCP	9090 > 1162	[PSH, ACK]	Seq=19238 Ack=4709 win		
83	51.905933	192.168.8.200	192.168.8.12	TCP	1162 > 9090	[ACK]	Seq=4709 Ack=19583 win		

0180	68 65 69 72 20 70 6c 61	6e 73 2e 20 20 54 68 65	heir plans. The						
0190	79 20 61 72 65 20 6f 6e	20 74 61 72 67 65 74 20	y are on target						
01a0	77 69 74 68 20 74 68 65	69 72 20 6e 65 74 20 69	with the fir net i						
01b0	6e 63 6f 6d 65 20 74 68	69 73 20 79 65 61 72 20	ncome th is year						
01c0	64 65 73 70 69 74 65 20	74 68 65 20 6c 6f 77 20	despite the low						
01d0	68 6f 67 20 70 72 69 63	65 73 2e 20 20 47 6f 76	hog prices. Gov						
01e0	65 72 6e 6d 65 6e 74 20	6d 6f 6e 65 79 20 62 72	ernment money br						
01f0	6f 75 67 68 74 20 69 6e	20 6d 6f 72 65 20 74 68	ought in more th						
0200	61 6e 20 74 68 65 79 20	65 78 70 65 63 74 65 64	an they expected						
0210	20 61 6e 64 20 6d 61 64	65 20 75 70 20 74 68 65	and made up the						
0220	20 64 69 66 66 65 72 65	6e 63 65 2e 20 20 41 6c	difference. Al						
0230	61 6e 20 69 73 20 70 6c	61 6e 6e 69 6e 67 20 74	an is pl anning t						
0240	6f 20 70 72 65 70 61 79	20 74 6f 20 74 68 65 20	o prepay to the						
0250	74 75 6e 65 20 6f 66 20	24 35 30 2c 30 30 30 2e	tune of \$50,000.						
0260	20 20 54 68 65 69 72 20	4c 4f 43 20 69 73 20 70	Their LOC is p						
0270	61 69 64 20 6f 66 66 20	61 6e 64 20 74 68 65 79	aid off and they						
0280	20 68 61 76 65 20 24 32	39 4b 20 69 6e 20 63 68	have \$2 9K in ch						
0290	65 63 6b 69 6e 67 20 72	69 67 68 74 20 6e 6f 77	ecking r ight now						
02a0	2e 20 20 54 68 65 79 20	68 61 76 65 20 61 20 6c	. They have a l						
02b0	61 6e 64 20 70 61 79 6d	65 6e 74 20 64 75 65 20	and paym ent due						
02c0	74 6f 20 57 61 6c 74 65	72 2c 20 77 68 69 63 68	to walte r, which						
02d0	20 73 68 6f 75 6c 64 20	74 61 6b 65 20 74 68 65	should take the						
02e0	69 72 20 44 44 41 20 63	61 73 68 2c 20 61 6e 64	ir BDA c ash, and						
02f0	20 74 68 65 69 72 20 4c	4f 43 20 62 61 6c 61 6e	their L OC balan						
0200	62 65 70 68 61 72 20 61	70 6d 61 78 20 6f 66 20	ce has a max of						
Filter:									
				Add Expression...	Clear	Apply	File: Ethereal Testbank capture 2 April 25 2004.dat		

Proprietary Data
Clear Text

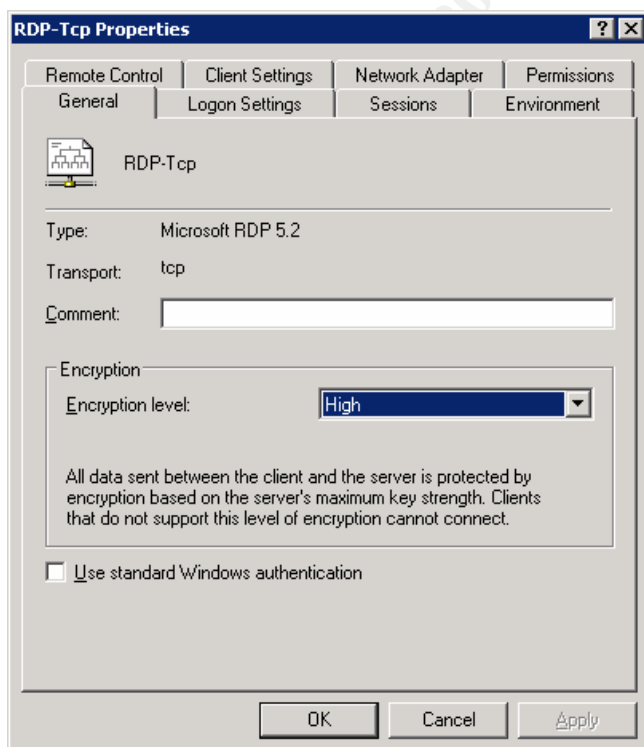
STEP # T3	Antivirus software installed
Control Objective	Verify that an antivirus software package is installed, configured correctly, obtaining and deploying updates properly
Risk	HIGH – new threats discovered daily
Compliance	Visually confirm software present and configuration
Test	Symantec Antivirus Corporate Edition v8.00 Open the Symantec application Select Configure Menu – verify real time protection Select OK – verify Virus Definition file date and version Review Application Event Log to confirm updates Alternately verify file dates in LiveUpdate Directory
Objective/Subjective	Objective
Reference	Installation Guide for Symantec AntiVirus Corporate Edition 8.1.
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	Appendix E (Antivirus)
Stimulus Response	

STEP # T4	Perimeter Protection
Control Objective	Verify the firewall configuration implements controls to incoming packets
Risk	HIGH – Systems without firewall protection are open to external attack.
Compliance	Review Windows 2003 Standard Server 'Advanced' properties on Network Properties interface Business Requirements allow TCP traffic on ports for each financial institution, 3389 (Remote Desktop) and 21 (FTP)
Test	Click Start – Settings – Network Connections Select LAN interface Right Mouse Select Properties Select Advanced Tab Observe Checkmark for “ Internet Connection Firewall” Select Settings Observe Ports Allowed
Objective/Subjective	Objective -
Reference	http://support.microsoft.com/default.aspx?scid=kb;en-us;317530&Product=winsvr2003
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	Appendix A
Stimulus Response	

STEP # T5	NTFS File System
Control Objective	Ensure that the file system uses NTFS
Risk	HIGH – security is not available on other Microsoft file systems
Compliance	FAT and FAT32 file systems should not be used
Test	From a DOS command C:\>chkntfs c: Alternately observe finding in MS Baseline Report Appendix F
Objective/Subjective	Objective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	The type of file system is NTFS.
Stimulus Response	

© SANS Institute 2004, Author retains full rights

STEP # T6	Communications between central Windows 2003 Standard server and remote administrative platforms
Control Objective	Ensure that communications is encrypted
Risk	MEDIUM – security is not available on other Microsoft file systems
Compliance	Windows Remote Desktop can be configured to enable encryption of the session Ethereal can be used to capture session (Appendix G)
Test	Select Start > Programs > Administrative Tools Select Terminal Services Configuration Select Connections in the left console panel Select RDP-TCP in the right console details pane Select Right Mouse > Properties > Click the General tab Observe the details stating all communications are encrypted or the client cannot connect. Review Ethereal Protocol Analysis in Appendix G
Objective/Subjective	Objective
Reference	http://support.microsoft.com/default.aspx?scid=kb;en-us;814590&Product=winsvr2003
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	Encryption is set to HIGH (RDP-TCP Properties capture) Ethereal Capture Appendix G
Stimulus Response	



Administrative Checklist

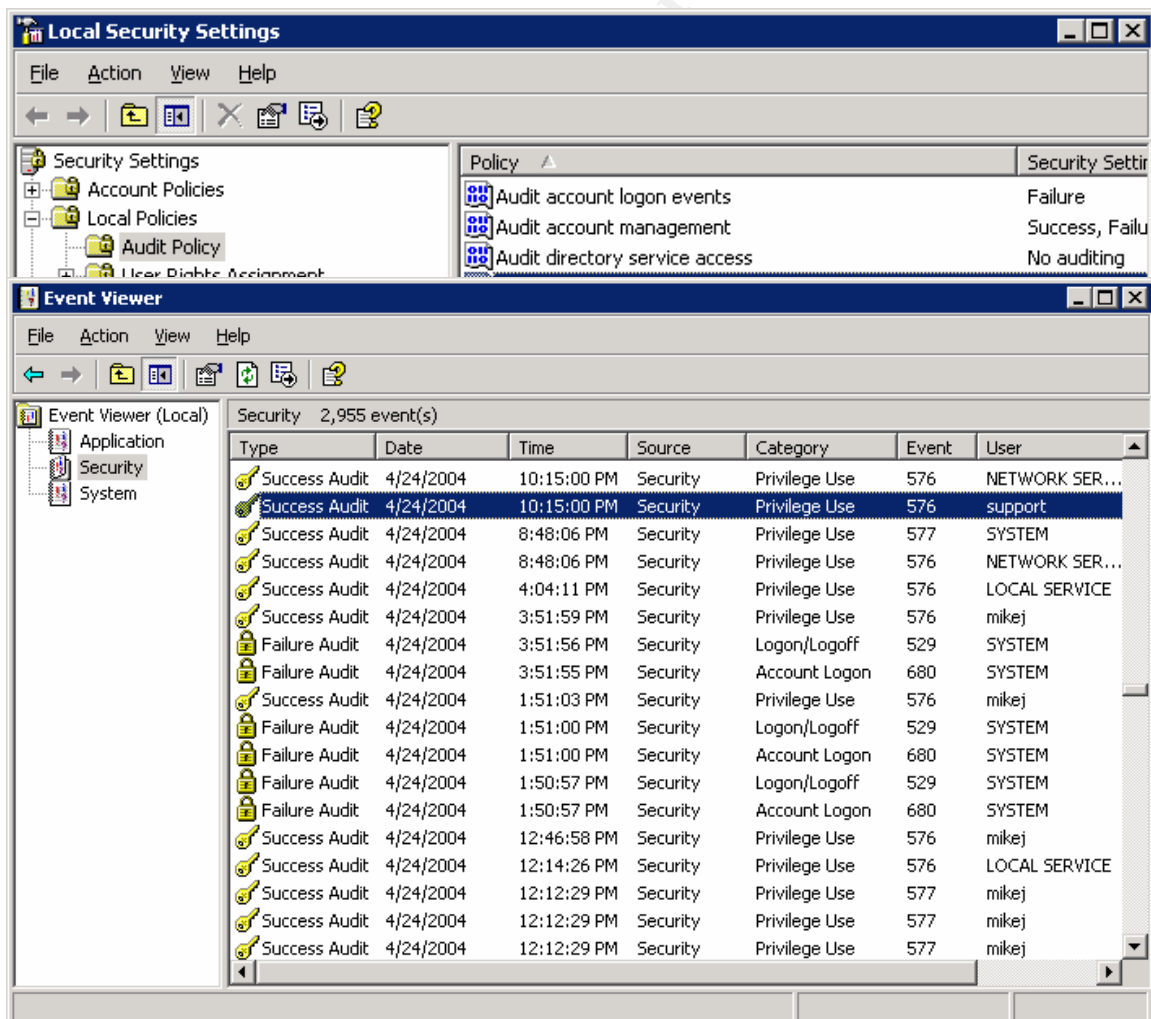
STEP # A1	Backup and Recovery
Control Objective	Ensure the system has adequate backup and that a recovery process or procedure can be executed
Risk	HIGH – The Windows 2003 Standard Server is a single point of failure unless there are adequate provisions for continued operations in the event the server is unavailable
Compliance	Review backup procedures, verify the backup is executing on schedule, verify the restore process results in a working system
Test	Review procedures and documentation with administrative staff
Objective/Subjective	Subjective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	Backup scripts are present, logs show they are executing properly. Review of scripts on off-site server show that the twice daily backup is executing correctly. Appendix E
Stimulus Response	

© SANS Institute 2004, Author retains full rights.

STEP # A2	Compliance of deployment to administrative deployment notes
Control Objective	Validate that the method of deploying the ASTA server component is consistent with established tactics
Risk	Improper configuration can cause the system to fail
Compliance	Review the Windows Scheduled Task command line
Test	Open the Windows Control Panel Select Scheduled Tasks Select the Asta Server item (Testbank) Right Mouse Select Properties Compare the Run, Start In, and Run as, Items to the administrative documentation. Sample Value Expected: d:\directory\testbank\AstaIBExpressServer.exe PORT=9090 DATABASE=127.0.0.1:d:\directory\testbank\testbank.gdb USER_NAME=xxxxxxx PASSWORD=xxxxxxx
Objective/Subjective	Objective
Reference	http://www.astatech.com/support/servers.htm Select the IBExpress .zip package
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	The configuration in place matches the documentation. d:\directory\testbank\AstaIBExpressServer.exe PORT=9090 DATABASE=127.0.0.1:d:\directory\testbank\testbank.gdb USER_NAME=xxxxxxx PASSWORD=xxxxxxx Appendix E
Stimulus Response	

© SANS Institute

STEP # A3	Audit Policy – Local Security Settings
Control Objective	Validate that the audit policy
Risk	Improper configuration precludes review of vital security information
Compliance	Review the Windows Local Security Settings
Test	Select Run from the Start menu %SystemRoot%\system32\secpol.msc /s Select Local Policies Select Audit Policy Observe security settings include failure at minimum: Confirm Security Events
Objective/Subjective	Objective
Reference	
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	below
Stimulus Response	



Physical Checklist

STEP # P1	Access to central server
Control Objective	Protect server from unauthorized access
Risk	HIGH – unauthorized access permits malicious configurations, removal of power, theft of system, modification of data
Compliance	Premise has locks and control procedures
Test	Review premise security with administrative staff
Objective/Subjective	Objective
Reference	Personal Experience
RESULTS -	Complete after execution
Test Successful?	YES
Detailed Results	Review of premise and discussion with staff shows satisfactory physical access controls. Appendix E
Stimulus Response	

Part #3 (03.2) Evidence

([Appendix B Ethereal](#)) is the focus of the audit. The other vulnerability and procedural checks are good practice and were added to the scope by agreement. See Appendices A, B-G

Part #3 (03.3) Findings

As noted in Technical Checklist step T2 (above) and ([Appendix B Ethereal](#)) the audit findings are that the data is not encrypted on the network.

The vulnerability scan comparison between Qualys and Nessus shows the two methods to be in agreement. The scans indicate that the ICF (Internet Connection Firewall) on Windows 2003 Standard server can be configured to permit selected business processes to function while providing a good level of security. There is essentially no difference between the Nessus and Qualys results in this instance.

On the subjective question of performance degradation to a production server during the Nessus and Qualys vulnerability scans the high level assessment is that there is no significant degradation. However, it is noteworthy that the server stopped responding on the TCP service port (9099) used by the Loanranger application and required reboot to restore business function. This would indicate that the application is likely vulnerable to a DOS (denial of service) attack by flooding the port with unexpected packets. Further investigation on the part of the system administrators is warranted.

Part #4

Part #4 (4.0) Audit Report or Risk Assessment

Loanaranger.tld management required an objective reply to the veracity of the claim of the software developer regarding encryption of data in transit between PC client and central server. The findings show that the data is not encrypted.

Additional audit tasks were executed to confirm the continued security of the central Windows 2003 Standard server. The findings show that the server continues to be secure with the exceptions necessary to accommodate the business processes required by the Loanaranger software.

Part #4 (04.1) Audit Findings

Exposure of Data in Transit over the Network

ASCII data is transmitted over the network. Unfortunately the claim of the software developer is not borne out by testing with Ethereal protocol analyzer. The developer has agreed to revise the application and testing will be repeated when the revisions are available for testing.

Ethereal Testbank capture 2 April 25 2004.dat - Ethereal

No.	Time	Source	Destination	Protocol	Info
72	48.994571	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [ACK] Seq=14920 Ack=4349 win
73	48.994571	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [ACK] Seq=16370 Ack=4349 win
74	48.994733	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=17830 Ack=434
75	48.994737	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4349 Ack=16370 win
76	48.994868	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4349 Ack=18109 win
77	49.015793	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=4349 Ack=1810
78	49.025764	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=18109 Ack=456
79	49.198101	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4569 Ack=19238 win
80	50.614881	192.168.8.200	192.168.8.255	BROWSER	Local Master Announcement N170PLAPTOP, w
81	51.794800	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=4569 Ack=1923
82	51.805063	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=19238 Ack=470
83	51.905933	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4709 Ack=19583 win

0180 68 65 69 72 20 70 6c 61 6e 73 2e 20 20 54 68 65 heir plans. The
0190 79 20 61 72 65 20 6f 6e 20 74 61 72 67 65 74 20 y are on target
01a0 77 69 74 68 20 74 68 65 69 72 20 6e 65 74 20 69 with the fir net i
01b0 6e 63 6f 6d 65 20 74 68 69 73 20 79 65 61 72 20 ncome th is year
01c0 64 65 73 70 69 74 65 20 74 68 65 20 6c 6f 77 20 ncome the low
01d0 68 6f 67 20 70 72 69 63 65 73 2e 20 20 47 6f 76 hog prices. Gov
01e0 65 72 6e 6d 65 6e 74 20 6d 6f 6e 65 79 20 62 72 ernment money br
01f0 6f 75 67 68 74 20 69 6e 20 6d 6f 72 65 20 74 68 ought in more th
0200 61 6e 20 74 68 65 79 20 65 78 70 65 63 74 65 64 an they expected
0210 20 61 6e 64 20 6d 61 64 65 20 75 70 20 74 68 65 and made up the
0220 20 64 69 66 66 65 72 65 6e 63 65 2e 20 20 41 6c difference. Al
0230 61 6e 20 69 73 20 70 6c 61 6e 6e 69 6e 67 20 74 an is pl anning t
0240 6f 20 70 72 65 70 61 79 20 74 6f 20 74 68 65 20 o prepay to the
0250 74 75 6e 65 20 6f 66 20 24 35 30 2c 30 30 30 2e tune of \$50,000.
0260 20 20 54 68 65 69 72 20 4c 4f 43 20 69 73 20 70 Their LOC is p
0270 61 69 64 20 6f 66 66 20 61 6e 64 20 74 68 65 79 aid off and they
0280 20 68 61 76 65 20 24 32 39 4b 20 69 6e 20 63 68 have \$2 9k in ch
0290 65 63 6b 69 6e 67 20 72 69 67 68 74 20 6e 6f 77 ecking r ight now
02a0 2e 20 20 54 68 65 79 20 68 61 76 65 20 61 20 6c . They have a l
02b0 61 6e 64 20 70 61 79 6d 65 6e 74 20 64 75 65 20 and paym ent due
02c0 74 6f 20 57 61 6c 74 65 72 2c 20 77 68 69 63 68 to walte r, which
02d0 20 73 68 6f 75 6c 64 20 74 61 6b 65 20 74 68 65 should take the
02e0 69 72 20 44 44 41 20 63 61 73 68 2c 20 61 6e 64 fir DDA c ash, and
02f0 20 74 68 65 69 72 20 4c 4f 43 20 62 61 6c 61 6e their L OC balan
0300 62 65 70 68 61 72 20 61 70 64 61 78 20 6f 66 20 co has a max of

Proprietary Data
Clear Text

Operating System Exposure

The vulnerability scan testing (Nessus and Qualys) reveals that the Internet Connection Firewall is configured to provide a reasonably good degree of security. Selected TCP ports are exposed to facilitate required business processes.

Port 21 FTP is required in order to transfer data to and from administrative workstations and for backup.

Port 3389 Remote Desktop is required in order to remotely administer the system.

Port 9090 is required to enable the Loanranger business application.

Business Exposure

The backup scripts utilize File Transfer Protocol (FTP) to move the critical information to an off-site server. FTP passwords transit the network in the clear. The exposure can be mitigated by implementing a VPN between the central Windows 2003 Standard server and the remote backup storage system. See Appendix E.

Part #4 (04.2) Audit Recommendations

1) Increase the frequency of periodic assessment:

- Vulnerability - run vulnerability scanner
- Administrative review
 - Event Logs
 - User Access
- Microsoft Baseline Security Analyzer

2) Establish a VPN

Used to secure the FTP session within the off-site backups

3) Establish and Document Security Policy

4) Formalize Documentation of Administrative Procedures

Conclusion

Executive Summary

Management posed two questions of the audit team:

- Q1) Does the data from Loanaranger transit the network securely?
- Q2) Does the administrative team conduct appropriate security practices on the central Windows 2003 Standard server?

- A1) The software developer's claim is not upheld by the audit testing.
- A2) Loanaranger.tld has made reasonable effort to ensure the security of the central Windows 2003 Standard server.

Recommendations

Security improvements are available in the form of increased periodic administrative review for vulnerability and from establishing secure connectivity for the remote backup server.

The primary source of improvement would be to establish written procedures for Security and Administrative Procedures. Additional benefit would be obtained by implementing an IDS (Intrusion Detection System) such as SNORT. See Appendix G References. Improved security would be obtained by implementing a VPN connection between the central Windows 2003 Standard server and the off-site backup system.

© SANS Institute 2004. Author retains full rights.

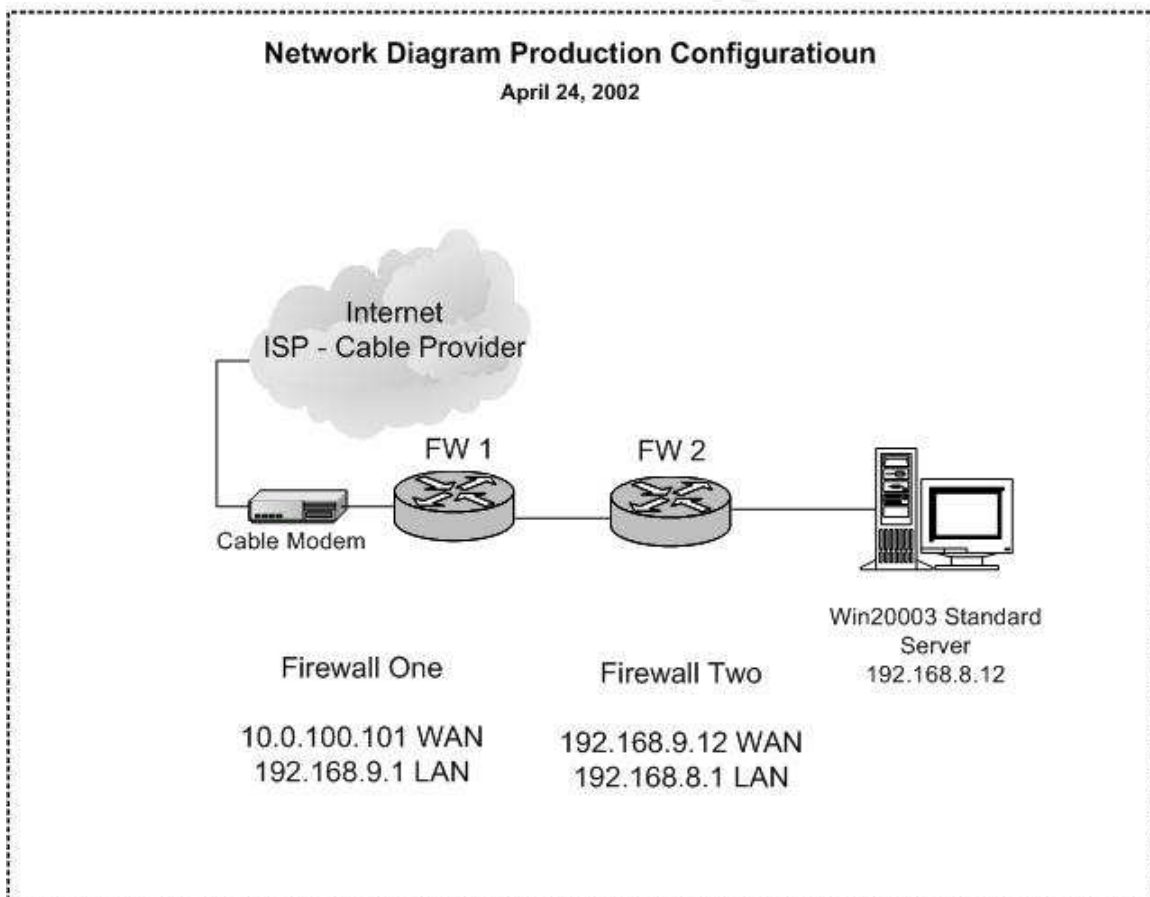
Appendices

Appendix A Server and Network Documentation

Created April 26, 2004

Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)
Application Client: Windows XP Professional (Audit Testing Client)
LAN address: (DHCP)
Ethereal Fedora Core 1 (Audit Testing Client)
LAN address: (DHCP)

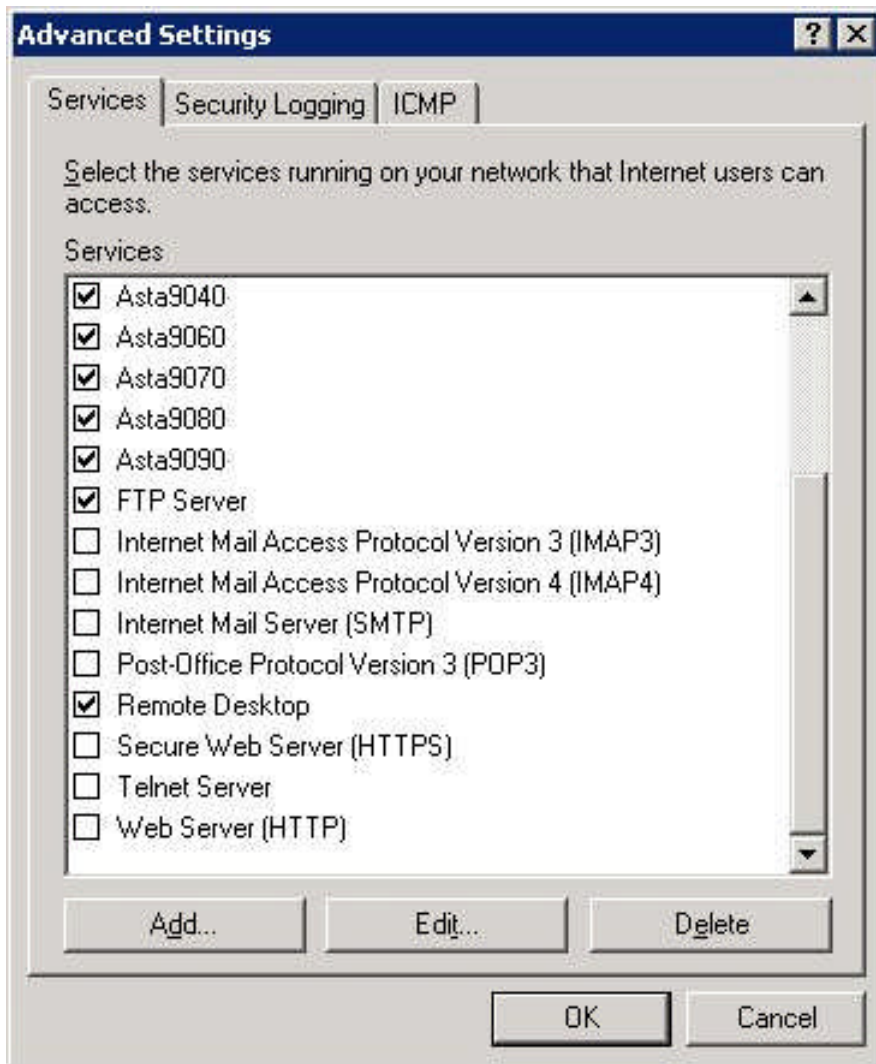
Visio Diagram (1 of 5)



Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)

Screen Capture (2 of 5)

ICF Internet Connection Firewall Configuration

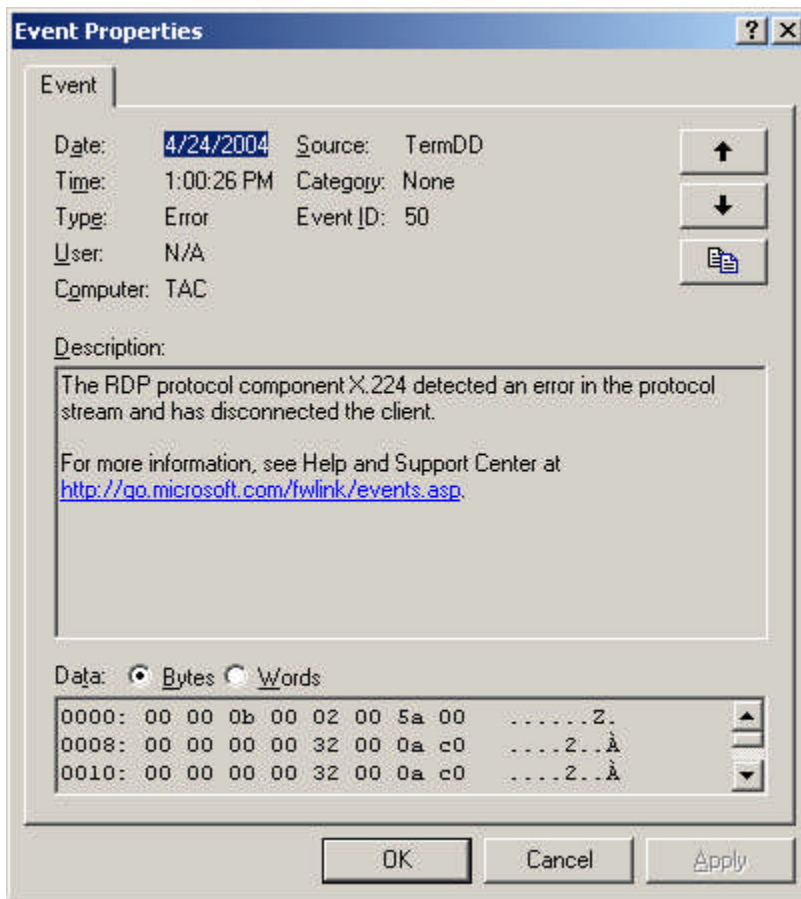


After Audit Follow-up –
Server was no longer responding to client application.
Reboot solved the issue.

Troubleshooting Notes Screen Capture (3 of 5)

Windows 2003 Standard Server
Event Log

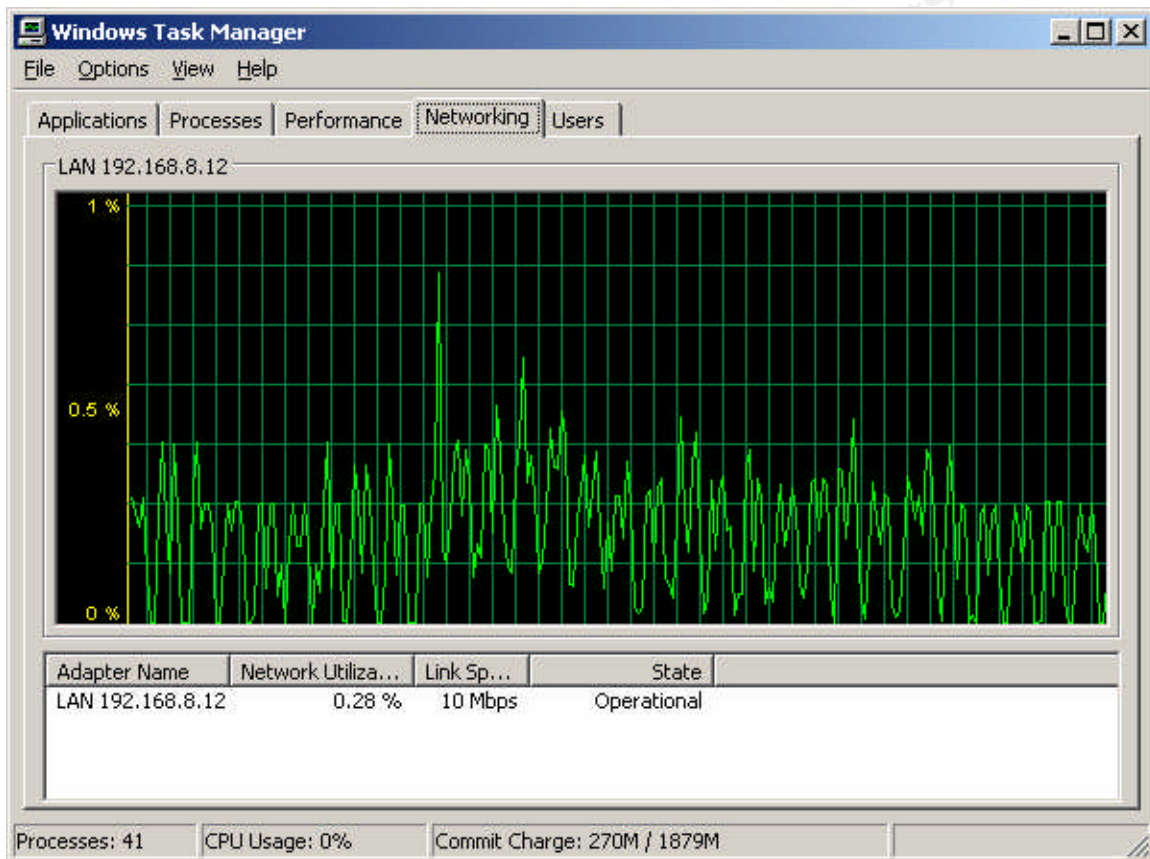
Produced during Qualys and Nessus Scan activity



During Audit Performance Evaluation –
Client application received consistent response from server during vulnerability scanning.
Server evidenced no undue network load during scan activity.

Network Performance Typical Screen Capture (4 of 5)

Gigabit LAN Network Interface (note scale)

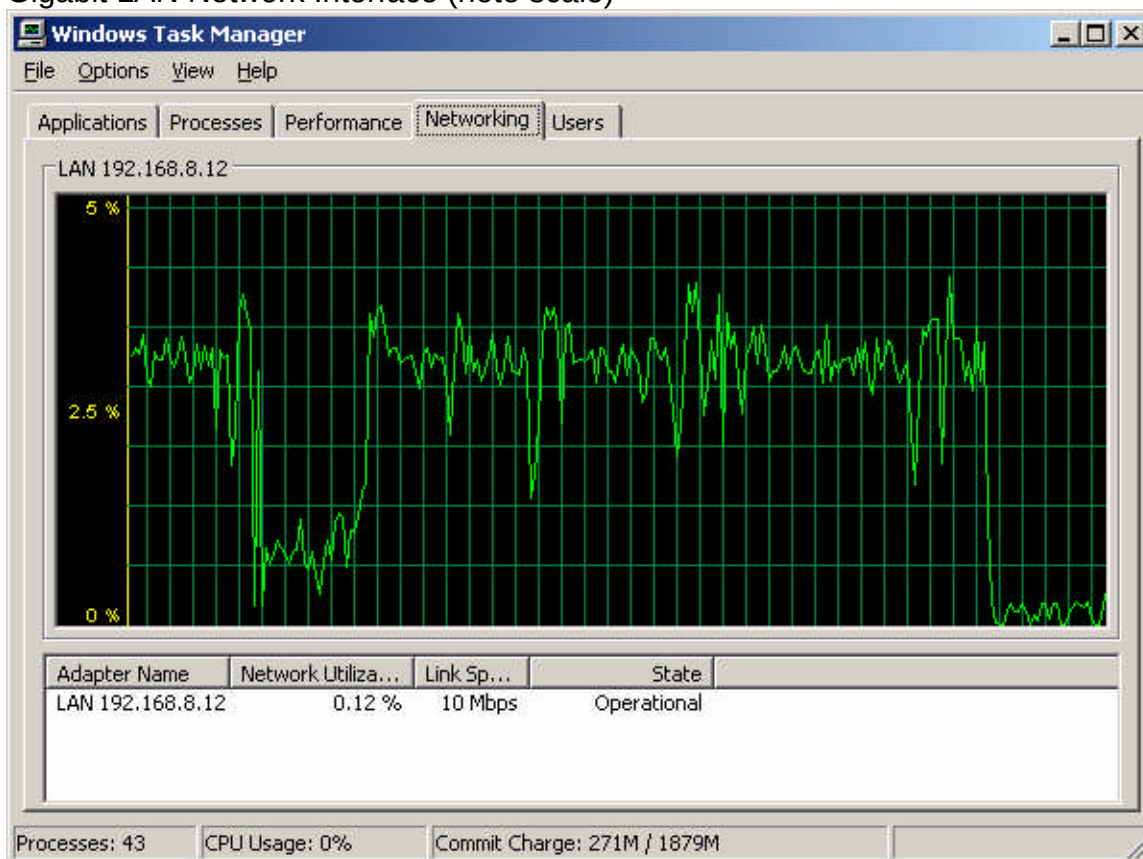


© SANS

During Audit Performance Evaluation –
Attempt to increase network load.
Large FTP session initiated during scan activity.

Network Performance Typical Screen Capture (5 of 5)

Gigabit LAN Network Interface (note scale)



```
230 User mikej logged in.  
ftp> bin  
200 Type set to I.  
ftp> mput *.zip  
mput sdi21.zip? y  
200 PORT command successful.  
150 Opening BINARY mode data connection for sdi21.zip.  
226 Transfer complete.  
ftp: 19082921 bytes sent in 621.48Seconds 30.71Kbytes/sec.  
ftp
```

Appendix B Protocol Analyzer - Ethereal Capture PC Client Port 9090

Obtained April 24, 2004

Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)
Client: Application Client Laptop
LAN address: (192.168.8.200 DHCP)

Ethereal Capture (1 of 5)

Frame 13 – username 'MJ', password is 'mj'

Ethereal Testbank capture 2 April 25 2004.dat - Ethereal

No.	Time	Source	Destination	Zoom 100%	Info
7	7.690381	129.6.15.29	192.168.8.200	NTP	NTP
8	10.470052	192.168.8.200	192.168.8.12	ICMP	Echo (ping) request
9	15.482074	192.168.8.200	192.168.8.12	ICMP	Echo (ping) request
10	23.741295	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [SYN] Seq=0 Ack=0 win=16384
11	23.741300	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [SYN, ACK] Seq=0 Ack=1 win=1
12	23.741581	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=1 Ack=1 win=17520
13	23.801591	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=1 Ack=1 win=1
14	23.811583	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=1 Ack=75 win=
15	23.961321	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=75 Ack=151 win=173
16	23.962005	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=151 Ack=75 wi
17	23.981311	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=75 Ack=487 wi
18	23.982262	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=487 Ack=180 wi

Frame 13 (128 bytes on wire, 128 bytes captured)

Offset	Time	Source	Destination	Protocol	Length	Info
0000	00 40 05 83 17 dd 08 00	46 5c b0 11 08 00 45 00	.@.....	F\....E.		
0010	00 72 35 f0 40 00 80 06	32 71 c0 a8 08 c8 c0 a8	.r5.0...	2q.....		
0020	08 0c 04 8a 23 82 cd 9e	ab 53 d5 f8 6f ef 50 18	...#....	.S..O.P.		
0030	44 70 2f d4 00 00 46 00	00 00 11 00 00 00 00 06	dp/...F.			
0040	01 00 00 00 02 00 00 00	00 02 00 00 00 04 00 00				
0050	00 00 04 00 00 00 06 00	00 00 00 06 00 00 00 0d				
0060	00 00 00 00 0d 00 00 00	15 00 00 00 31 4d 4a 6d		1MJm		
0070	6a 38 2e 32 2e 30 2e 31	38 2e 32 2e 30 2e 31 02	j8.2.0.1	8.2.0.1.		

UserID = MJ
Password = mj

Ethereal Scan Results

Obtained April 24, 2004

Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)
Client: Application Client Laptop
LAN address: (192.168.8.200)

Ethereal Capture (2 of 5)

Frame 14 Response with Welcome Information

Ethereal Testbank capture 2 April 25 2004.dat - Ethereal

No.	Time	Source	Destination	Protocol	Info
7	7.690381	129.6.15.29	192.168.8.200	NTP	NTP
8	10.470052	192.168.8.200	192.168.8.12	ICMP	Echo (ping) request
9	15.482074	192.168.8.200	192.168.8.12	ICMP	Echo (ping) request
10	23.741295	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [SYN] Seq=0 Ack=0 win=16384
11	23.741300	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [SYN, ACK] Seq=0 Ack=1 win=1
12	23.741581	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=1 Ack=1 win=17520
13	23.801591	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=1 Ack=1 win=1
14	23.811583	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=1 Ack=75 win=1
15	23.961321	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=75 Ack=151 win=173
16	23.962005	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=151 Ack=75 win=1
17	23.981311	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=75 Ack=487 win=1
18	23.982262	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=487 Ack=190 win=1

Frame 14 (204 bytes on wire, 204 bytes captured)

```
0000 08 00 46 5c b0 11 00 40 05 83 17 dd 08 00 45 00 ..F\...@ .....E.
0010 00 be 2e f8 40 00 80 06 39 1d c0 a8 08 0c c0 a8 ....@... 9.....
0020 08 c8 23 82 04 8a d5 f8 6f ef cd 9e ab 9d 50 18 ...#.... 0.....P.
0030 44 26 cf a6 00 00 92 00 00 00 0f 00 00 00 00 06 D&.....
0040 01 00 00 00 04 00 00 00 00 04 00 00 00 61 00 00 .....a..
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 36 36 37 57 .....667w
0070 65 6c 63 6f 6d 65 20 4d 69 6b 65 20 4a 65 6e 6b e!come M ike Jenk
0080 69 6e 73 2c 0a 0a 59 6f 75 20 61 72 65 20 63 6f ins...Yo u are co
0090 6e 6e 65 63 74 65 64 20 74 6f 20 54 65 73 74 20 nnnected to Test
00a0 4e 61 74 69 6f 6e 61 6c 20 42 61 6e 6b 2e 0a 0a National Bank...
00b0 59 6f 75 72 20 64 65 6d 6f 20 77 69 6c 6c 20 65 Your dem o will e
00c0 78 70 69 72 65 20 6f 6e 20 2e 0d 0d xpire on ...
```


Ethereal Scan Results

Obtained April 24, 2004

Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)
Client: Application Client Laptop
LAN address: (192.168.8.200)

Ethereal Capture (3 of 5)

Frame 16 – SQL Response populating default initial screen

The screenshot displays the Ethereal network protocol analyzer interface. The title bar reads "Ethereal Testbank capture 2 April 25 2004.dat - Ethereal". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, navigation, and analysis. The main pane shows a list of captured packets. Packet 16 is selected, showing a TCP segment from 192.168.8.12 to 192.168.8.200, port 9090 to 1162, with flags [PSH, ACK] and sequence number 487. The packet data is displayed in hexadecimal and ASCII. The ASCII column shows a large block of text, which appears to be a SQL response containing a list of bank names and their details, such as "BANK", "NAME", "ADDRESS", "STATE", "CALLNAME", "CALLP", "HONEY", "OTEDLTYP", "FREG", "FREGULAT", "LASTCIFI", "VERS", "ION7", and "BANKTD".

No.	Time	Source	Destination	Protocol	Info
13	23.801591	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=1 Ack=1 win=
14	23.811583	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=1 Ack=75 win=
15	23.961321	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=75 Ack=151 win=172
16	23.962005	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=151 Ack=75 w
17	23.981311	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=75 Ack=487 w
18	23.993363	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=487 Ack=180 w
19	24.011319	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=180 Ack=1319
20	24.021603	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=1319 Ack=405
21	24.031334	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=405 Ack=1682
22	24.043720	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=1682 Ack=637
23	24.063790	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=637 Ack=3043

Filter: Add Expression... Clear Apply File: Ethereal Testbank capture 2 April 25 2004.dat

Ethereal Scan Results

Obtained April 24, 2004

Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)
Client: Application Client Laptop
LAN address: (192.168.8.200)

Ethereal Capture (4 of 5)

Frame 17 – SQL query

The screenshot displays the Ethereal Testbank capture 2 April 25 2004.dat - Ethereal window. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help) and a toolbar with various icons for file operations, navigation, and analysis. The main pane shows a list of captured packets with columns for No., Time, Source, Destination, Zoom 100%, and Info. Packet 17 is selected, showing a TCP segment from 192.168.8.200 to 192.168.8.12, port 1162 to 9090, with a [PSH, ACK] flag and sequence/acknowledgment numbers. Below the packet list, the details pane shows the raw data of Frame 17 (159 bytes on wire, 159 bytes captured) in hexadecimal and ASCII format. The ASCII data shows a SQL query: "SELECT * FROM sdsyste ..-10". The status bar at the bottom indicates the filter is empty and the file is Ethereal Testbank capture 2 April 25 2004.dat.

No.	Time	Source	Destination	Zoom 100%	Info
7	7.690381	129.6.15.29	192.168.8.200	NTP	NTP
8	10.470052	192.168.8.200	192.168.8.12	ICMP	Echo (ping) request
9	15.482074	192.168.8.200	192.168.8.12	ICMP	Echo (ping) request
10	23.741295	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [SYN] Seq=0 Ack=0 win=16384
11	23.741300	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [SYN, ACK] Seq=0 Ack=1 win=1
12	23.741581	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=1 Ack=1 win=17520
13	23.801591	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=1 Ack=1 win=1
14	23.811583	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=1 Ack=75 win=
15	23.961321	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=75 Ack=151 win=173
16	23.962005	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=151 Ack=75 wi
17	23.981311	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=75 Ack=487 wi
18	23.982262	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=487 Ack=151 wi

Frame 17 (159 bytes on wire, 159 bytes captured)

```
0000 00 40 05 83 17 dd 08 00 46 5c b0 11 08 00 45 00 .@.....F\....E.
0010 00 91 35 f2 40 00 80 06 32 50 c0 a8 08 c8 c0 a8 ..5.@...2P.....
0020 08 0c 04 8a 23 82 cd 9e ab 9d d5 f8 71 d5 50 18 ....#... ..q.P.
0030 42 8a 98 9a 00 00 65 00 00 00 03 01 00 00 00 00 B.....e.....
0040 01 00 00 00 31 00 00 00 06 31 00 00 00 33 00 00 ....1... .1...3..
0050 00 06 33 00 00 00 34 00 00 00 00 34 00 00 00 34 ..3...4. ...4...4
0060 00 00 00 00 00 00 00 00 00 00 00 00 53 45 4c 45 ..... ..SELE
0070 43 54 20 2a 20 20 20 20 20 20 20 20 20 20 20 20 CT *
0080 20 20 0d 0a 46 52 4f 4d 20 73 64 73 79 73 74 65 ..FROM sdsyste
0090 6d 20 20 20 20 20 20 20 20 20 0d 0a 2d 31 30 m ..-10
```


Ethereal Scan Results

Obtained April 24, 2004

Host: Loanaranger.tld Production Server
LAN address: (192.168.8.12)
Client: Application Client Laptop
LAN address: (192.168.8.200)

Ethereal Capture (1 of 5)

Frame 78 – proprietary data in clear text

Ethereal Testbank capture 2 April 25 2004.dat - Ethereal

No.	Time	Source	Destination	Protocol	Info
72	48.994311	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [ACK] Seq=14320 Ack=4349 win
73	48.994571	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [ACK] Seq=16370 Ack=4349 win
74	48.994733	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=17830 Ack=434
75	48.994737	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4349 Ack=16370 win
76	48.994868	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4349 Ack=18109 win
77	49.015793	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=4349 Ack=1810
78	49.025764	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=18109 Ack=456
79	49.198101	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4569 Ack=19238 win
80	50.614881	192.168.8.200	192.168.8.255	BROWSER	Local Master Announcement N170PLAPTOP, w
81	51.794800	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [PSH, ACK] Seq=4569 Ack=1923
82	51.805063	192.168.8.12	192.168.8.200	TCP	9090 > 1162 [PSH, ACK] Seq=19238 Ack=470
83	51.905933	192.168.8.200	192.168.8.12	TCP	1162 > 9090 [ACK] Seq=4709 Ack=19583 win

0180 68 65 69 72 20 70 6c 61 6e 73 2e 20 20 54 68 65 heir pla ns. The
0190 79 20 61 72 65 20 6f 6e 20 74 61 72 67 65 74 20 y are on target
01a0 77 69 74 68 20 74 68 65 69 72 20 6e 65 74 20 69 with the ir net i
01b0 6e 63 6f 6d 65 20 74 68 69 73 20 79 65 61 72 20 ncome th is year
01c0 64 65 73 70 69 74 65 20 74 68 65 20 6c 6f 77 20 despite the low
01d0 68 6f 67 20 70 72 69 63 65 73 2e 20 20 47 6f 76 hog pric es. Gov
01e0 65 72 6e 6d 65 6e 74 20 6d 6f 6e 65 79 20 62 72 ernment money br
01f0 6f 75 67 68 74 20 69 6e 20 6d 6f 72 65 20 74 68 ought in more th
0200 61 6e 20 74 68 65 79 20 65 78 70 65 63 74 65 64 an they expected
0210 20 61 6e 64 20 6d 61 64 65 20 75 70 20 74 68 65 and mad e up the
0220 20 64 69 66 66 65 72 65 6e 63 65 2e 20 20 41 6c differe nce. Al
0230 61 6e 20 69 73 20 70 6c 61 6e 6e 69 6e 67 20 74 an is pl anning t
0240 6f 20 70 72 65 70 61 79 20 74 6f 20 74 68 65 20 o prepay to the
0250 74 75 6e 65 20 6f 66 20 24 35 30 2c 30 30 30 2e tune of \$50,000.
0260 20 20 54 68 65 69 72 20 4c 4f 43 20 69 73 20 70 Their LOC is p
0270 61 69 64 20 6f 66 66 20 61 6e 64 20 74 68 65 79 aid off and they
0280 20 68 61 76 65 20 24 32 39 4b 20 69 6e 20 63 68 have \$2 9k in ch
0290 65 63 6b 69 6e 67 20 72 69 67 68 74 20 6e 6f 77 ecking r ight now
02a0 2e 20 20 54 68 65 79 20 68 61 76 65 20 61 20 6c . They have a l
02b0 61 6e 64 20 70 61 79 6d 65 6e 74 20 64 75 65 20 and paym ent due
02c0 74 6f 20 57 61 6c 74 65 72 2c 20 77 68 69 63 68 to walte r, which
02d0 20 73 68 6f 75 6c 64 20 74 61 6b 65 20 74 68 65 should take the
02e0 69 72 20 44 44 41 20 63 61 73 68 2c 20 61 6e 64 ir bDA c ash, and
02f0 20 74 68 65 69 72 20 4c 4f 43 20 62 61 6c 61 6e their L OC balan
0300 62 65 20 6e 61 72 20 61 20 6d 61 78 20 6f 66 20 co has a max of

Filter: / Add Expression... Clear Apply File: Ethereal Testbank capture 2 April 25 2004.dat

Appendix C Nessus Scan Results

Obtained April 25, 2004

Host: Loanaranger.tld Production Server
 LAN address: (192.168.8.12)

Detailed Capture (1 of 1)

192.168.8.12		
Service	Severity	Description
unknown (9040/tcp)	Info	Port is open
ms-term-serv	Info	Port is open
unknown (9002/tcp)	Info	Port is open
unknown (9001/tcp)	Info	Port is open
unknown (9000/tcp)	Info	Port is open
unknown (9020/tcp)	Info	Port is open
unknown (9010/tcp)	Info	Port is open
unknown (9030/tcp)	Info	Port is open
ftp (21/tcp)	Info	Port is open
unknown (9060/tcp)	Info	Port is open
unknown (9070/tcp)	Info	Port is open
unknown (9080/tcp)	Info	Port is open
zeus-admin (9090/tcp)	Info	Port is open
ftp (21/tcp)	Low	The service closed the connection after 0 seconds without sending any data It might be protected by some TCP wrapper
ms-term-serv	Low	The Terminal Services are enabled on the remote host. Terminal Services allow a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host). If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to
		steal the credentials of legitimates users by impersonating the Windows server. Solution : Disable the Terminal Services if you do not use them, and do not allow this service to run across the internet Risk factor : Medium CVE : CAN-2001-0540 BID : 7258
general/tcp	Low	The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself. Solution : drop source routed packets on this host or on other ingress routers or firewalls. Risk factor : Low
general/udp	Low	For your information, here is the traceroute to 192.168.8.12 : 192.168.8.201 192.168.8.12

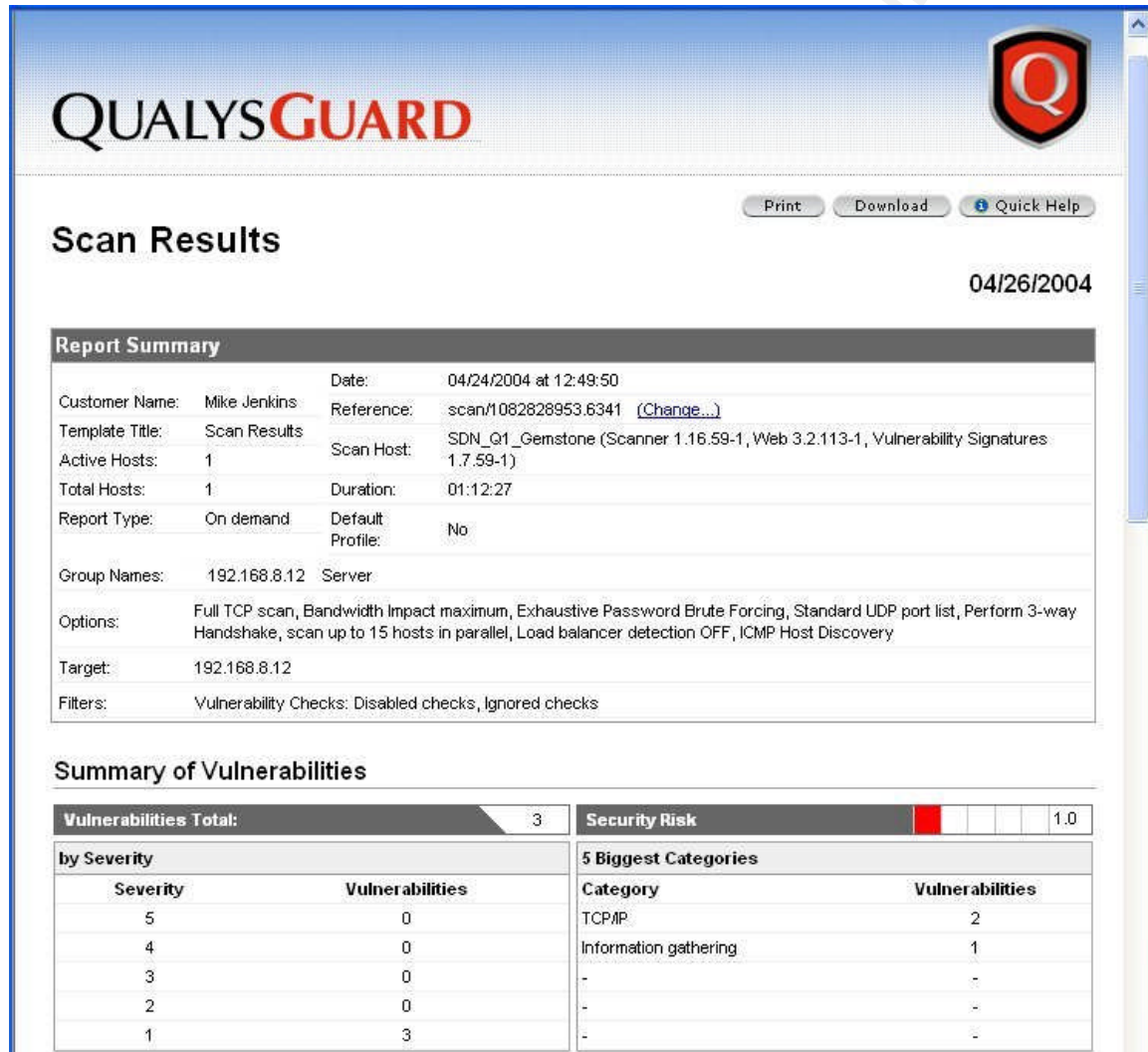
Appendix D Qualysguard Consultant Scan Results

Obtained April 24, 2004

Target: Loanaranger.tld Production Server
LAN address: (192.168.8.12)

Overview

Detailed Capture (1 of 3)



The screenshot displays the QualysGuard web interface for a scan report. At the top, the QualysGuard logo is on the left, and a shield icon with a 'Q' is on the right. Below the logo, there are buttons for 'Print', 'Download', and 'Quick Help'. The main heading is 'Scan Results' with the date '04/26/2004' to its right. A 'Report Summary' section follows, containing a table with scan details. Below this is a 'Summary of Vulnerabilities' section, which includes a table for vulnerabilities by severity and a table for the 5 biggest categories of vulnerabilities. The interface has a blue header and a light blue sidebar on the right.

Scan Results

04/26/2004

Report Summary

Customer Name:	Mike Jenkins	Date:	04/24/2004 at 12:49:50
Template Title:	Scan Results	Reference:	scan/1082828953.6341 (Change...)
Active Hosts:	1	Scan Host:	SDN_Q1_Gemstone (Scanner 1.16.59-1, Web 3.2.113-1, Vulnerability Signatures 1.7.59-1)
Total Hosts:	1	Duration:	01:12:27
Report Type:	On demand	Default Profile:	No
Group Names:	192.168.8.12	Server:	
Options:	Full TCP scan, Bandwidth Impact maximum, Exhaustive Password Brute Forcing, Standard UDP port list, Perform 3-way Handshake, scan up to 15 hosts in parallel, Load balancer detection OFF, ICMP Host Discovery		
Target:	192.168.8.12		
Filters:	Vulnerability Checks: Disabled checks, Ignored checks		

Summary of Vulnerabilities

Vulnerabilities Total:	3	Security Risk		1.0
-------------------------------	---	----------------------	--	-----

by Severity		5 Biggest Categories	
Severity	Vulnerabilities	Category	Vulnerabilities
5	0	TCPAP	2
4	0	Information gathering	1
3	0	-	-
2	0	-	-
1	3	-	-

Qualysguard Consultant Scan Results

Obtained April 24, 2004

Target: Loanaranger.tld Production Server

LAN address: (192.168.8.12)

Detailed Capture (2 of 3)

192.168.8.12 (No registered hostname)

Vulnerabilities Total:	3	Security Risk		1.0
-------------------------------	---	----------------------	--	-----

by Severity

Severity	Vulnerabilities
5	0
4	0
3	0
2	0
1	3

5 Biggest Categories

Category	Vulnerabilities
TCP/IP	2
Information gathering	1
-	-
-	-
-	-

Information Gathered (3)

1

 Reachable Host List

1

 Option to Use Three-Way Handshake TCP Port Scanning Enabled

1

 Open TCP Services List

Information Gathered (3)

1

 Reachable Host List

OID: 6 **Category:** Information gathering **CVE ID:** N/A

First Detected: 04/24/2004 at 13:55:49 **Last Detected:** 04/24/2004 at 13:55:49 **Times Detected:** 1

DESCRIPTION:

The host(s) listed responds to one or more of the probes sent to it. The probes used to detect live hosts include TCP, UDP and ICMP packets.

The hostname(s) displayed was obtained from a DNS server.

RESULT:

IP address	Host name
192.168.8.12	No registered hostname

1

 Option to Use Three-Way Handshake TCP Port Scanning Enabled

OID: 82042 **Category:** TCP/IP **CVE ID:** N/A

First Detected: 04/24/2004 at 13:55:49 **Last Detected:** 04/24/2004 at 13:55:49 **Times Detected:** 1

DESCRIPTION:

You have enabled three-way handshake TCP port scanning. This option may be selected to protect the host against some potential issues with half-open TCP port scanning.

When this option is enabled, you may experience some increase in the scanning time. No attempt is made to detect the presence of a firewall and the version of the operating system. Consequently, the host is not tested for vulnerabilities, whose detection is dependent on the detection of a firewall or the operating system.

RESULT:

No results available

Qualysguard Consultant Scan Results

Obtained April 24, 2004

Target: Loanaranger.tld Production Server
LAN address: (192.168.8.12)

Detailed Capture (3 of 3)

▼ 1 Open TCP Services List

QID: 82023 **Category:** TCPAP **CVE ID:** N/A

First Detected: 04/24/2004 at 13:55:49 **Last Detected:** 04/24/2004 at 13:55:49 **Times Detected:** 1

DESCRIPTION:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

CONSEQUENCES:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the [CERT Web site](#).

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
3389	ms-wbt-server	MS WBT Server	win remote desktop	
9000	cslistener	CSlistener	unknown	
9002	unknown	unknown	unknown	
9010	unknown	unknown	unknown	
9020	unknown	unknown	unknown	
9030	unknown	unknown	unknown	
9040	unknown	unknown	unknown	
9060	unknown	unknown	unknown	
9080	unknown	unknown	unknown	
9090	websm	WebSM vqserver administration port	unknown	

© SANS I

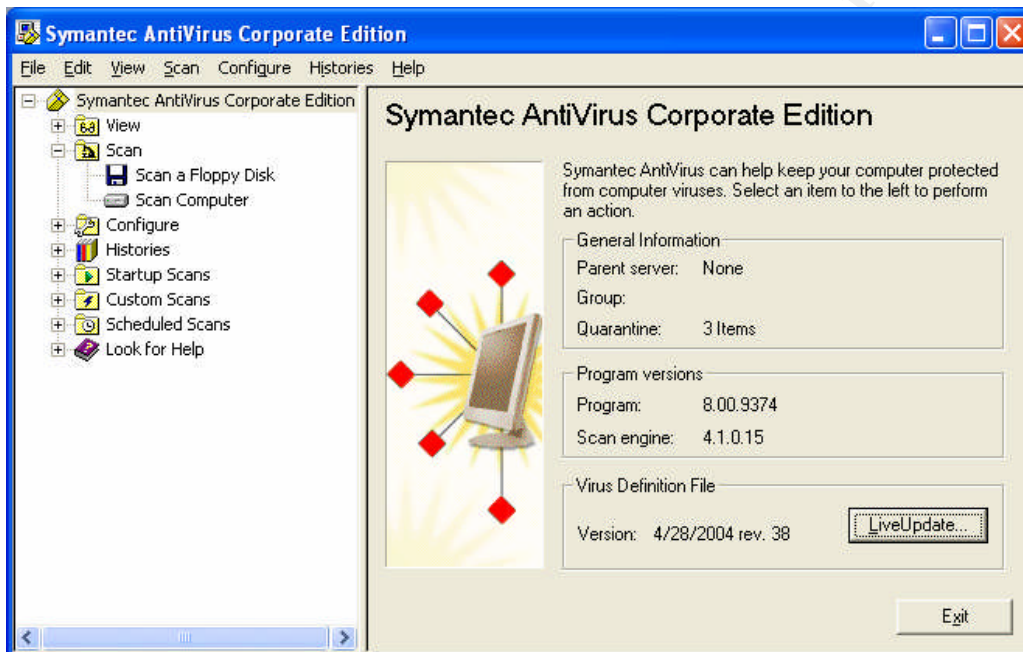
Appendix E Antivirus, Backup Scripting

Symantec Corporate Edition Antivirus screen capture

Obtained April 28, 2004

Target: Loanaranger.tld Production Server
LAN address: (192.168.8.12)

Detailed Capture (1 of 2)



© SANS Institute

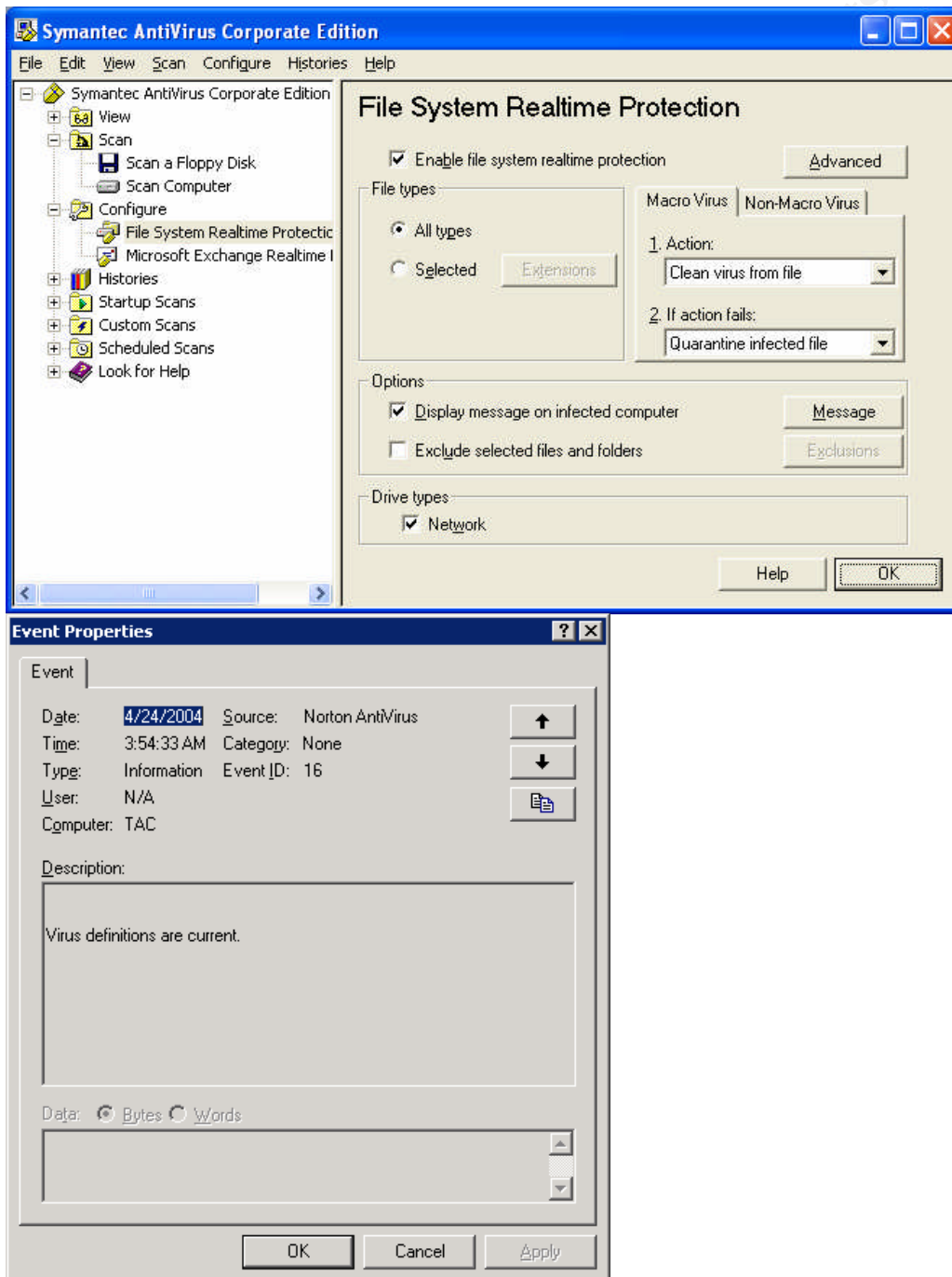
Symantec Corporate Edition Antivirus screen capture

Obtained April 28, 2004

Target: Loanaranger.tld Production Server

LAN address: (192.168.8.12)

Detailed Capture (2 of 2)



An alternate means of confirming the current Symantec antivirus files is to manually observe the dates on the Symantec Antivirus files:

The reference to Symantec documentation is:

http://service1.symantec.com/SUPPORT/ent-security.nsf/9d94c8571a91ba4788256bf3007f62b5/6bf39452b1634d1c88256d81005b645a?OpenDocument&prod=Symantec%20AntiVirus%20Corporate%20Edition&ver=8.x&src=ent&pcode=sav_ce&dtype=corp&svy=&prev=&miniver=sav_8_ce

```
C:\Documents and Settings\All Users\Application
Data\Symantec\LiveUpdate>dir <enter>
```

```
Volume in drive C has no label.
Volume Serial Number is 0C1E-E5C4
```

```
Directory of C:\Documents and Settings\All Users\Application
Data\Symantec
Update
```

```
05/02/2004  03:54 AM    <DIR>      .
05/02/2004  03:54 AM    <DIR>      ..
05/02/2004  03:54 AM                633 1.Log.LiveUpdate
05/02/2004  03:54 AM            2,286 1.Product.Catalog.LiveUpdate
05/02/2004  03:54 AM            2,357 1.Settings.LiveUpdate
05/02/2004  03:54 AM                633 2.Log.LiveUpdate
05/02/2004  03:54 AM            2,286 2.Product.Catalog.LiveUpdate
05/02/2004  03:54 AM            2,357 2.Settings.LiveUpdate
05/01/2004  03:54 AM            3,870 3.Log.LiveUpdate
05/01/2004  03:54 AM            2,286 3.Product.Catalog.LiveUpdate
05/01/2004  03:54 AM            2,357 3.Settings.LiveUpdate
10/04/2003  04:33 PM                917 Configuration.Log.LiveUpdate
05/02/2004  03:54 AM    <DIR>      Downloads
05/02/2004  03:54 AM            6,326 Log.LiveUpdate
05/02/2004  03:54 AM            2,286 Product.Catalog.LiveUpdate
05/02/2004  03:54 AM            2,357 Settings.LiveUpdate
               13 File(s)            30,951 bytes
               3 Dir(s)    5,651,161,088 bytes free
```

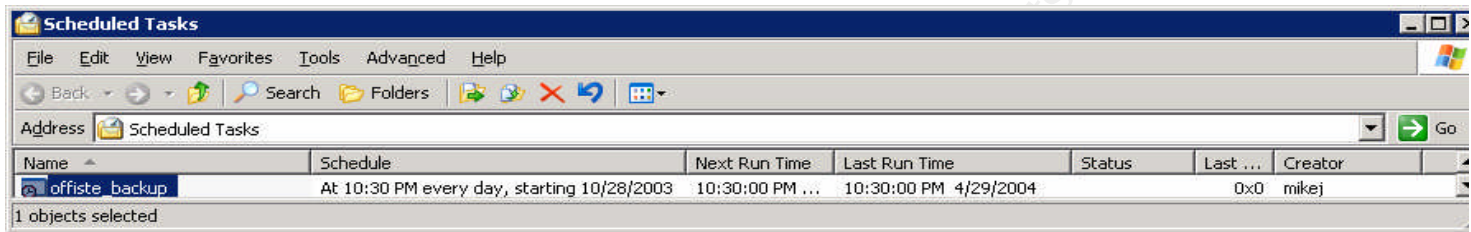

Windows 2003 Standard Server Off-Site Backup Test Results

Obtained April 30, 2004

Target: Loanaranger.tld Production Server

LAN address: (192.168.8.12)

Detailed Capture (1 of 2)



Confirmation that the off-site backup process is working:

Obtained from central Windows 2003 Standard Server

Directory of C:\inetpub\ftproot\xxxxxxx

```
04/29/2004  10:31 PM    <DIR>          .
04/29/2004  10:31 PM    <DIR>          ..
04/29/2004  10:31 PM                19,442,445 offsitebackup.zip
                1 File(s)      19,442,445 bytes
                3 Dir(s)      5,657,600,000 bytes free
```

Obtained from remote off-site backup server

Directory of C:\util

```
03/13/2004  07:00 AM    <DIR>          .
03/13/2004  07:00 AM    <DIR>          ..
04/30/2004  06:09 AM                19,442,445 offsitebackup.zip
                7 File(s)      19,445,477 bytes
                2 Dir(s)     14,416,826,368 bytes free
```

Appendix F MS Baseline Security Analyzer - Results

Obtained April 28, 2004

Target: Loanaranger.tld Production Server

LAN address: (192.168.8.12)

Detailed Capture (1 of 3)

Computer name: [REDACTED] IP address: [REDACTED] Security report name: [REDACTED] 11 PM) Scan date: 4/28/2004 9:11 PM Security update database version: 2004.4.21.0 Office update database version: 11.0.0.6416 Security assessment: Severe Risk

Redacted Information

Security Updates

Score	Issue	Result	Reason
	Windows Security Updates	1 security updates could not be confirmed. Security Update Description MS03-030 Unchecked Buffer in DirectX Could Enable System Compromise (819896)	Please refer to 306460 for a detailed explanation.
	IIS Security Updates	No critical security updates are missing.	
	Windows Media Player Security Updates	No critical security updates are missing.	
	MDAC Security Updates	No critical security updates are missing.	
	MSXML Security Updates	No critical security updates are missing.	
	Office Security Updates	No critical security updates are missing.	

Windows Scan Results

Vulnerabilities

Score	Issue	Result
	Password Expiration	Some user accounts (10 of 12) have non-expiring passwords. User AdminBackup

© SANS

MS Baseline Security Analyzer – Screen Capture

Obtained April 28, 2004

Target: Loanaranger.tld Production Server

LAN address: (192.168.8.12)

Detailed Capture (2 of 3)

	Internet Connection Firewall	1 of 1 network connections either do not have Internet Connection Firewall enabled or have open ports.			
	Connection Name	Firewall	Open Ports		
	LAN 192.168.8.12	Enabled	Open		
	Local Account Password Test	Some user accounts (1 of 12) have blank or simple passwords, or could not be analyzed.			
	User	Weak Password	Locked Out	Disabled	
	Guest	Weak	-	Disabled	
	SUPPORT_388945a0	-	-	Disabled	
	tim	-	-	Disabled	
	AdminBackup	-	-	-	
	IUSR_TAC	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	-	-	-	-	
	File System	All hard drives (2) are using the NTFS file system.			
	Drive Letter	File System			
	C:	NTFS			
	D:	NTFS			
	Guest Account	The Guest account is disabled on this computer.			
	Autologon	Autologon is not configured on this computer.			
	Restrict Anonymous	Computer is properly restricting anonymous access.			
	Automatic Updates	Updates are automatically downloaded and installed on this computer.			

© SANS

MS Baseline Security Analyzer – Screen Capture

Obtained April 28, 2004

Target: Loanaranger.tld Production Server

LAN address: (192.168.8.12)

Detailed Capture (3 of 3)

Desktop Application Scan Results

Vulnerabilities

Score	Issue	Result																																																																																
	IE Zones	Internet Explorer zones do not have secure settings for some users.																																																																																
		<table><tr><th>User</th><th>Zone</th><th>Level</th><th>Recommended Level</th></tr><tr><td></td><td>Internet</td><td>Custom</td><td>High</td></tr><tr><td>Setting</td><td></td><td>Current</td><td>Recommended</td></tr><tr><td>Run components not signed with Authenticode</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Run components signed with Authenticode</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Download signed ActiveX controls</td><td></td><td>Prompt</td><td>Disable</td></tr><tr><td>Run ActiveX controls and plug-ins</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Script ActiveX controls marked safe for scripting</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>File download</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Font download</td><td></td><td>Enable</td><td>Prompt</td></tr><tr><td>Java permissions</td><td></td><td>High safety</td><td>Disable Java</td></tr><tr><td>Allow META REFRESH</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Drag and drop or copy and paste files</td><td></td><td>Enable</td><td>Prompt</td></tr><tr><td>Installation of desktop items</td><td></td><td>Prompt</td><td>Disable</td></tr><tr><td>Launching programs and files in an IFRAME</td><td></td><td>Prompt</td><td>Disable</td></tr><tr><td>Navigate sub-frames across different domains</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Software channel permissions</td><td></td><td>Medium safety</td><td>High safety</td></tr><tr><td>Submit nonencrypted form data</td><td></td><td>Enable</td><td>Prompt</td></tr><tr><td>UserData persistence</td><td></td><td>Enable</td><td>Disable</td></tr><tr><td>Active scripting</td><td></td><td>Enable</td><td>Disable</td></tr></table>	User	Zone	Level	Recommended Level		Internet	Custom	High	Setting		Current	Recommended	Run components not signed with Authenticode		Enable	Disable	Run components signed with Authenticode		Enable	Disable	Download signed ActiveX controls		Prompt	Disable	Run ActiveX controls and plug-ins		Enable	Disable	Script ActiveX controls marked safe for scripting		Enable	Disable	File download		Enable	Disable	Font download		Enable	Prompt	Java permissions		High safety	Disable Java	Allow META REFRESH		Enable	Disable	Drag and drop or copy and paste files		Enable	Prompt	Installation of desktop items		Prompt	Disable	Launching programs and files in an IFRAME		Prompt	Disable	Navigate sub-frames across different domains		Enable	Disable	Software channel permissions		Medium safety	High safety	Submit nonencrypted form data		Enable	Prompt	UserData persistence		Enable	Disable	Active scripting		Enable	Disable
User	Zone	Level	Recommended Level																																																																															
	Internet	Custom	High																																																																															
Setting		Current	Recommended																																																																															
Run components not signed with Authenticode		Enable	Disable																																																																															
Run components signed with Authenticode		Enable	Disable																																																																															
Download signed ActiveX controls		Prompt	Disable																																																																															
Run ActiveX controls and plug-ins		Enable	Disable																																																																															
Script ActiveX controls marked safe for scripting		Enable	Disable																																																																															
File download		Enable	Disable																																																																															
Font download		Enable	Prompt																																																																															
Java permissions		High safety	Disable Java																																																																															
Allow META REFRESH		Enable	Disable																																																																															
Drag and drop or copy and paste files		Enable	Prompt																																																																															
Installation of desktop items		Prompt	Disable																																																																															
Launching programs and files in an IFRAME		Prompt	Disable																																																																															
Navigate sub-frames across different domains		Enable	Disable																																																																															
Software channel permissions		Medium safety	High safety																																																																															
Submit nonencrypted form data		Enable	Prompt																																																																															
UserData persistence		Enable	Disable																																																																															
Active scripting		Enable	Disable																																																																															

© SANS Institute

Appendix G Protocol Analyzer - Ethereal Capture Port 3389 Windows RDP Remote Desktop

Capture review of port 3389 traffic from 192.168.8.200 test client using Windows RDP Remote Desktop client. Username 'mike' initiating session the server is responding to the client on ephemeral port 1037. The next data from the client will be the password.

Port 3389 Capture.dat - Ethereal

File Edit View Go Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [SYN] Seq=0
2	0.000004	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [SYN, ACK] Seq=1
3	0.000272	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [ACK] Seq=1
4	0.000749	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1
5	0.001409	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [PSH, ACK] Seq=1
6	0.002028	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1
7	0.002031	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [PSH, ACK] Seq=1
8	0.003097	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1
9	0.003100	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1
10	0.003103	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [ACK] Seq=34
11	0.003106	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [PSH, ACK] Seq=1
12	0.003367	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1
13	0.003370	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [PSH, ACK] Seq=1
14	0.003866	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1
15	0.003869	192.168.8.12	192.168.8.200	TCP	3389 > 1037 [PSH, ACK] Seq=1
16	0.004124	192.168.8.200	192.168.8.12	TCP	1037 > 3389 [PSH, ACK] Seq=1

Frame 4 (88 bytes on wire, 88 bytes captured)

Ethernet II, Src: 08:00:46:5c:b0:11, Dst: 00:40:05:83:17:dd

Internet Protocol, Src Addr: 192.168.8.200 (192.168.8.200), Dst Addr: 192.168.8.12 (192.168.8.12)

Transmission Control Protocol, Src Port: 1037 (1037), Dst Port: 3389 (3389), Seq: 1, Len: 88

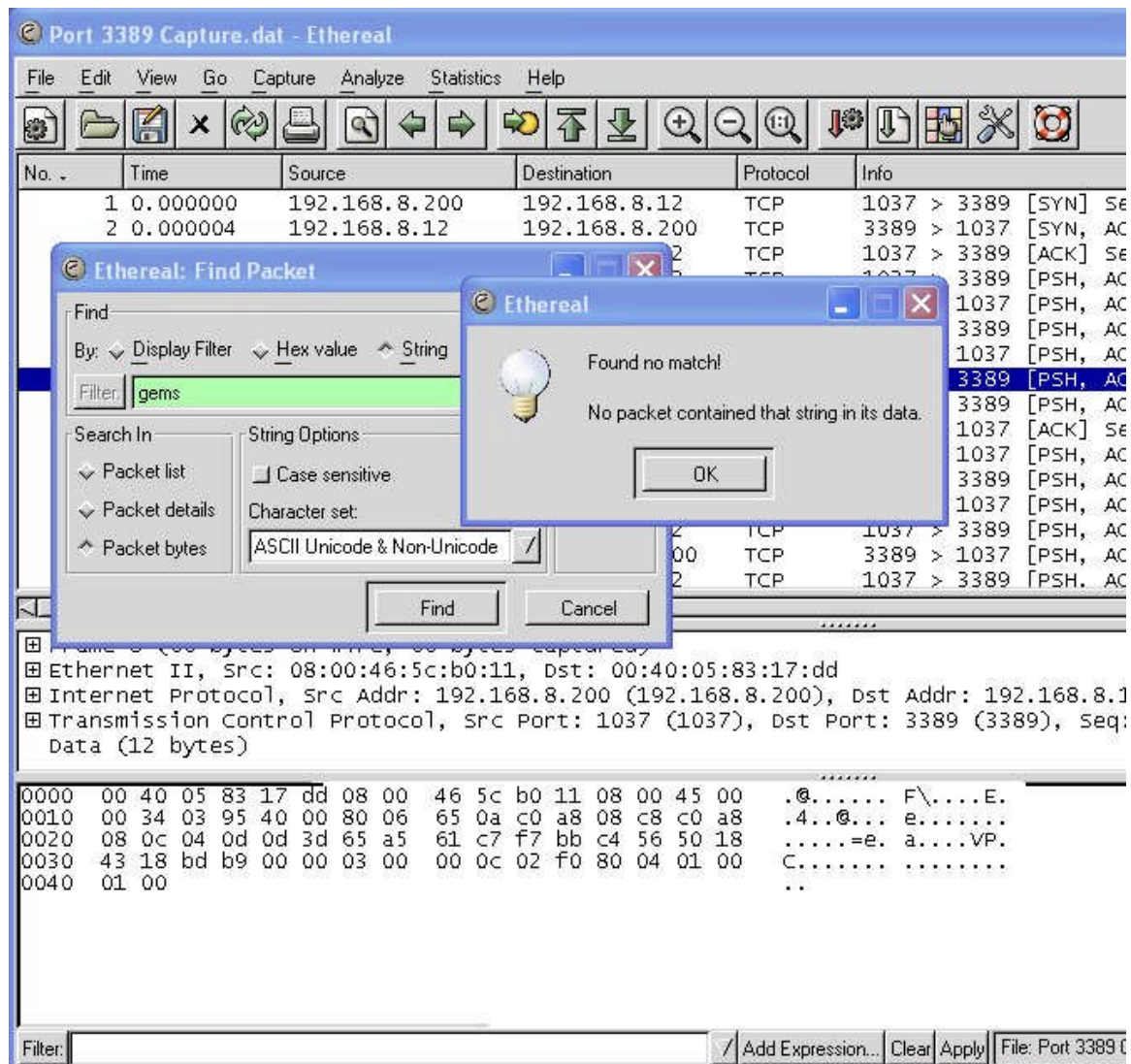
Data (34 bytes)

```
0000  00 40 05 83 17 dd 08 00 46 5c b0 11 08 00 45 00  .@.....F\....E.
0010  00 4a 03 93 40 00 80 06 64 f6 c0 a8 08 c8 c0 a8  .J..@...d.....
0020  08 0c 04 0d 0d 3d 65 a5 60 09 f7 bb c2 fe 50 18  ....=e.....P.
0030  44 70 2f 36 00 00 03 00 00 22 1d e0 00 00 00 00  dp/6... ..
0040  00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73  .Cookie: mstshas
0050  68 3d 6d 69 6b 65 0d 0a                          h=mike..
```

Filter: / Add Expression... Clear Apply Data (data), 34 bytes



Search for the start of the password ' gems ' revealed no ASCII data captured.



Appendix H References

Nessus

SANS Course Materials

Track 7, Auditing Networks, Perimeters, and Systems

7.4 Network Auditing Essentials (2003) , Page 5.25

Getting Started with Nessus

SANS Course Materials

Track 2, Defense In-Depth

2.4, Firewalls, Perimeter Protection and VPNs, Page 5-7

Ethereal

SANS Course Materials

Track 7, Auditing Networks, Perimeters, and Systems

7.4 Network Auditing Essentials (2003) , Page 4-26

Security Policy

SANS Certification Series (GIAC PREP) 2003

9.4 Information Security Policy

Authors: S. Fried, F. Kerby, S. Northcutt, D. Rice

SNORT

“Intrusion Detection with SNORT”

Author: Rafeeq Ur Rehman

ISBN: 0-13-140733-3

© 2003

Pub: Prentice Hall

1.1.2 Where IDS Should be Placed in Network Topology

IT Auditing for Financial Institutions

“IT Auditing for Financial Institutions”

Author: Jimmy R. Sawyers

ISBN: n/a

© 2003

Pub: www.alexinformation.com

Qualysguard

Qualysguard is a commercial vulnerability scanning product available to current subscribers. The on-line help modules are not public URL links. The overview of the 'Consultant' product is available publicly at http://www.qualysguard.com/docs/ConsultantDS_ME.qxd.pdf

Screen Capture from Qualysguard Consultant control panel indicating that currently they provide 3412 vulnerability tests similar to Nessus 'plug-in's' though Nessus offers over 2100 vulnerabilities.

1 to 200 of 3412

EditQID	Category	Name	Severity	CVE ID
27238	File Transfer Protocol	RhinoSoft Serv-U FTP Server Denial of Service Vulnerability	3	
12066	CGI	OpenBB Multiple Input Validation Vulnerabilities	3	
86651	Web server	Apache Cygwin Directory Traversal Vulnerability	4	CAN-2004-0173
12065	CGI	Artmedic Webdesign Hpmaker Script Multiple Vulnerabilities	3	
86650	Web server	BEA WebLogic Authentication Provider Privilege Inheritance Vulnerability	3	
38270	General remote services	Novell NetWare BTCPCOM CPU Hog ABEND Vulnerability	3	
43056	Hardware	Cisco Internet Operating System SNMP Message Processing Denial of Service Vulnerability	3	
12064	CGI	NewsTraXor Remote Database Disclosure Vulnerability	3	
38269	General remote services	CVS Server Piped Checkout Access Validation Vulnerability	4	
38268	General remote services	Real Networks Helix Universal Server Denial of Service Vulnerability	3	CAN-2004-0389
74146	Mail services	Ipswitch IMail Express Web Messaging Buffer Overrun Vulnerability	4	
27237	File Transfer Protocol	Ipswitch WS_FTP Server Resource Consumption Remote Denial Of Service Vulnerability	3	
38266	General remote services	SurgeLDAP Insecure Password Storage Vulnerability	3	
86649	Web server	IBM HTTP Over SSL Server Denial of Service Vulnerability	3	
90109	Windows Backdoors and	Windows 2000 Service Packs 2, 3, 4 Not Installed	5	

The following screen capture indicates how Qualys ranks the severity of vulnerabilities and provides a key to the color rating system.

Severity Levels

Every vulnerability is assigned a severity level, which is determined by the security risk associated with its exploitation. The following tables describe the possible consequences for each severity level for vulnerabilities, possible threats and information gathered. Note that a complete list of all checks performed by the scanning engine is available in the [Vulnerability KnowledgeBase](#).

Alternatively, Managers can apply a custom severity level to any vulnerability in the KnowledgeBase. To learn how, see [Customizing Severity Levels](#).

Vulnerabilities

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

SEVERITY	LEVEL	DESCRIPTION
	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

© SANS Institute