



INTERNET
SECURITY
SYSTEMS

Internet Scanner™
Technical Overview

Updated: December, 2000

Introduction and Scope

About Internet Scanner

Internet Scanner is a network security solution that provides automated security vulnerability detection and analysis for devices on a network. From a single, easy to use interface, Internet Scanner automatically scans a network for vulnerabilities, and displays scan results and fix information in clear reports that allow users to respond quickly to critical vulnerabilities. Internet Scanner is a dynamic security solution that adapts to meet the demands of both a changing security landscape and an individual organization's needs through X-Press Updates™, product integration, and wizards. Knowledge is the crucial first step to protecting the availability, integrity, and confidentiality of critical information assets. Internet Scanner's automated assessment and reporting incorporate Internet Security Systems' security management expertise to provide customers the resources necessary to know their networks.

About this document

This document provides an overview of the design and operation of Internet Scanner 6.1. Beginning with a brief description of the four main modules that make up Internet Scanner, it proceeds to more detailed descriptions of each module. The Appendix describes the tables in the Internet Scanner Database.

Overview

Description

Internet Scanner is an automated tool consisting of four modules:

- **Scan Engine** – Executes network tests that identify devices and vulnerabilities. The Scan Engine module comprises a number of engines and process and resource managers that will be discussed in greater detail in the following sections.
- **Report Environment** – Paper and electronic reports can be generated for distribution to appropriate parties. Different levels of information are available depending on the chosen report type: technical details, including fix information, for system administrators; summaries for security managers; and high-level graph and trend reports for executives.
- **Internet Scanner Database** – Stores vulnerability information, scan results, and other data used by Internet Scanner. Internet Scanner offers over 800 unique tests based on the knowledge provided by the X-Force™, Internet Security Systems' team of security researchers. This knowledge, including detailed descriptions and fix information for vulnerabilities, is stored in a database and presented to users through Internet Scanner's technician-level reports. Monthly X-Press Updates easily and quickly add new vulnerability checks, product improvements, and defect corrections to existing deployments of Internet Scanner.
- **User Interface** – Internet Scanner supports two different user interfaces, one graphical and the other command line, that allow the operator to configure and execute risk assessments, run reports, and perform administrative tasks. When graphical interface

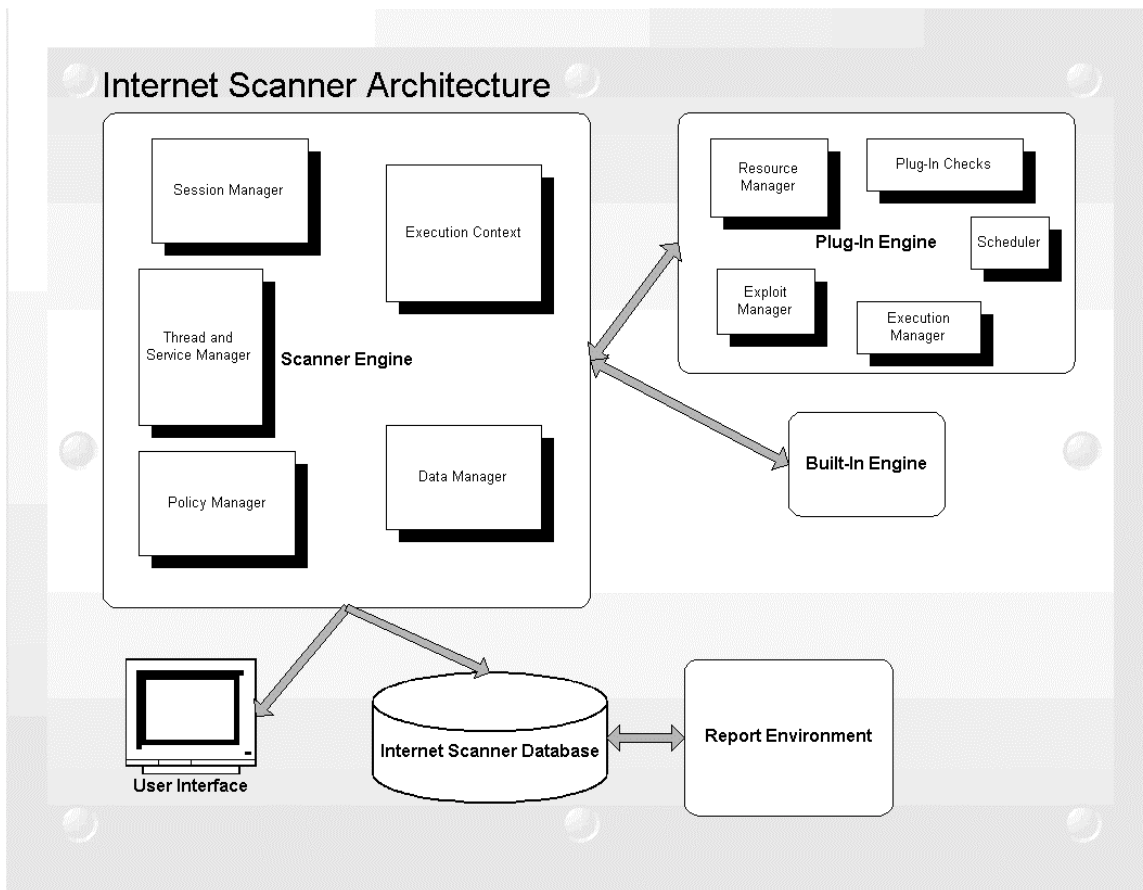
users perform assessments, vulnerability information is displayed on the user interface as it is collected, allowing on-line analysis of risk information. The command line interface allows sophisticated control of Internet Scanner, including scheduling and automation.

These modules are all installed as part of the Internet Scanner application on one or more computer systems in an organization. Assessments can be centrally managed in order to detect and manage risks in the entire organization, or assessments can be decentralized, with each business unit or project performing its own assessment and risk management.

The location of the Internet Scanner in a network has an important impact on the scan results, and the relation of the scanner to a firewall is especially significant. Scanning a network from outside the firewall protecting that network will show vulnerabilities or misconfigurations in the firewall. Such a scan, also known as a “tiger run,” can provide valuable information about the effectiveness of an organization’s firewall configuration, but will not produce a meaningful assessment of the network’s internal security posture. Scanning a network from an internal location (i.e., both Internet Scanner and the network are on the same side of the firewall) will show the network’s vulnerability to internal compromise or misuse.

Architecture

The drawing below shows a general diagram of the Internet Scanner architecture.



Scan Engine

The Scan Engine module consists of the following components:

- Scanner Engine
- Plug-In Engine
- Built-In Engine

These components are described in the following sections.

Scanner Engine

The Scanner Engine performs the operations related to initiating, running, and terminating scans. The Scanner Engine component of the Scan Engine consists of the following subcomponents:

- Session Manager
- Thread and Service Manager (TSM)
- Execution Context
- Policy Manager
- Policy Editor
- Data Manager

These subcomponents are described in the following sections.

Session Manager

The Session Manager creates and manages a collection of scanning session objects. Each session object contains a target address list, a license file name, and policy file name. The Session Manager has an execution context that manages the startup and shutdown of session objects.

Thread and Service Manager (TSM)

The Thread and Service Manager (TSM) creates the pool of threads and a number of background processes used by exploits in the engine. A thread is the series of checks run on a given host, one thread per host, and the maximum number of threads that can be open simultaneously is 128. The individual threads provide an execution context for running a scan of an individual target. The TSM also opens listening processes for exploits that involve a response from the target host, such as port scans.

Execution Context

After receiving a target and a policy from the Session Manager, an execution context provides a context in which all of the checks specified by the policy are run against the target within a given thread. When all of the checks in the policy have completed, the execution context requests a new policy and target from the Session Manager. If another target is available, execution (i.e., the session) continues; otherwise, execution terminates.

Policy Manager

The Policy Manager maintains the list of scan policy objects. Each scan policy object describes the configuration properties for all enabled vulnerability checks.

Policy Editor

The Policy Editor displays the policy information, allowing users to customize their scan sessions and obtain detailed Help information about specific vulnerability checks.

Data Manager

The Data Manager saves the Host Found, Vulnerability Found, and Service Found result objects that each vulnerability check can produce.

Plug-In Engine

The Plug-In Engine loads and manages the execution of plug-in vulnerability checks. The Plug-In Engine component of the Scan Engine consists of the following subcomponents:

- Resource Manager
- Plug-In Checks
- Exploit Manager
- Scheduler
- Execution Manager

These subcomponents are described in the following sections.

Resource Manager

The Resource Manager maintains a list of network scanning resources, the namespace scope the resource lives in, and its activation lifetime. A resource can be either a TCP connection, a Password List, an RPC connection, or other resource utilized by an exploit. Internet Scanner uses the Resource Manager to provide uniform access to all types of objects regardless of their implementation.

Plug-In Checks

Plug-in Checks are an improved type of vulnerability check that can be updated through the XPU process without requiring a full update of the product.

Exploit Manager

Checks are represented in the Exploit Manager as exploit objects. The Exploit Manager maintains a collection of exploit objects and exposes an interface to retrieve references to these objects.

Scheduler

The Scheduler generates a task list of checks to be run, orders this task list, and provides the Execution Manager with the current check to run and its target information.

Execution Manager

The Execution Manager works with the Scheduler to execute all of the exploits in the task list. The Execution Manager retrieves an exploit object and its target information from the Scheduler, prepares the exploit to be run, executes the exploit, and then processes the results. The Execution Manager is the component that performs the function call for found vulnerabilities that is sent to the Data Manager.

Built-In Engine

The Built-in Engine loads and manages the execution of built-in vulnerability checks. These are checks that were created before the implementation of Internet Scanner's Plug-In / Built-in architecture. The primary difference between the two types of checks is that the built-in checks have resources that are embedded in the exploits, resulting in dependency relationships between some exploits.

Report Environment

Internet Scanner produces reports using the Seagate® Crystal Reports™ report environment. Reports are available in the following types:

- Executive Reports
- Line Management Reports
- Technician Reports
- User Imported (or Custom) Reports

These report types are described in the following sections. All reports are exportable to HTML, Microsoft Word, and DIF (for importing to spreadsheet applications) file formats.

Executive Reports

The Executive Reports provide high-level summary information, including graphs, for rapid assessment of top-level security issues. These reports can be generated in a number of languages.

Line Management Reports

The Line Management reports show details of network scans sorted by DNS Name, IP address, or operating system. These reports are designed to facilitate resource planning.

Technician Reports

The Technician Reports provide detailed information about network security status, including instructions on how to fix or patch the vulnerabilities detected by Internet Scanner.

User Imported Reports

Users can create custom (or user-imported) reports based on their own network and reporting needs. The User Imported folder in the Internet Scanner installation directory is empty by default, and can be populated using the Import Custom Report option from the Reports menu.

Internet Scanner Database

X-Force vulnerability check information, scan results, and other data are stored in Internet Scanner's database. This is an Open Database Connectivity (ODBC)-compliant database that makes data accessible for custom reports, corporate applications, and other databases.

The schema for the Internet Scanner Database is described in Appendix A of this document.

User Interface

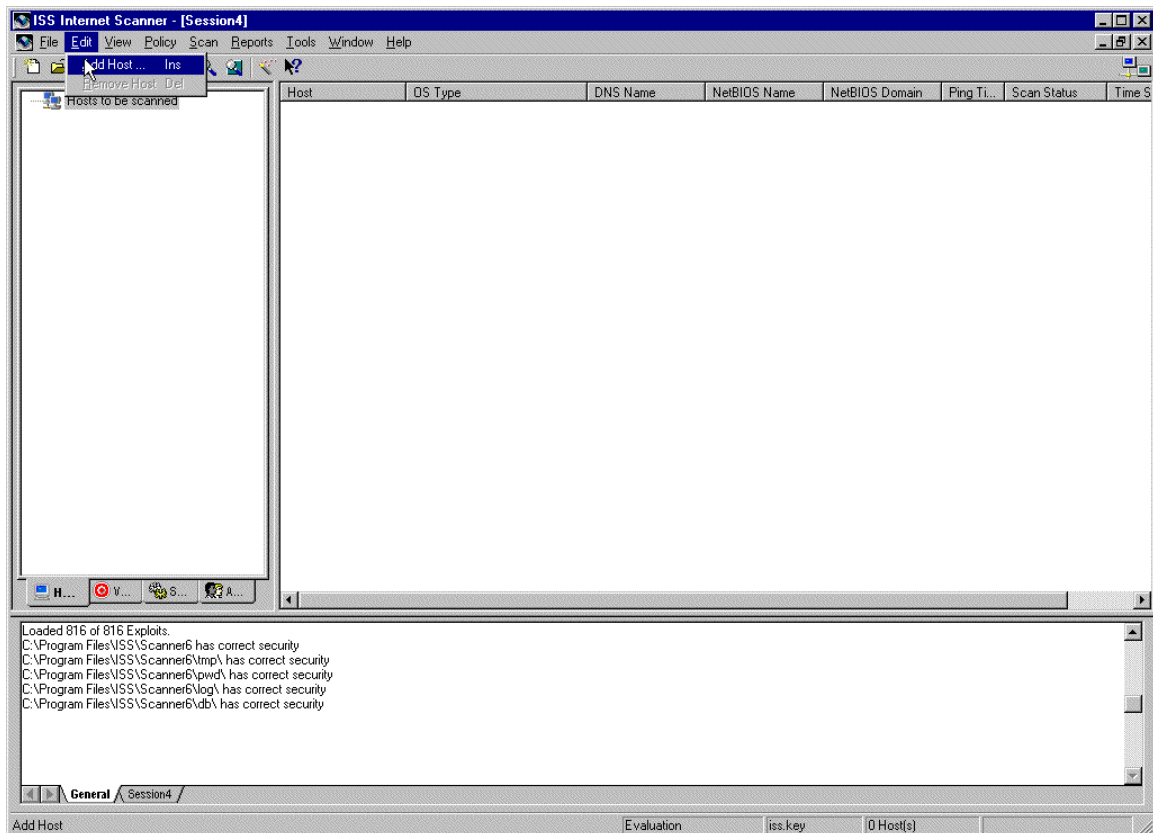
Internet Scanner supports the following types of user interface:

- Graphical User Interface
- Command Line Interface

These interfaces are described in the following sections.

Graphical User Interface

The Internet Scanner graphical user interface (GUI) is an easy-to-use, Windows-based application that allows users to run scans, work with policies and vulnerabilities, perform administrative tasks, and access the application's online Help. When performing a scan from the GUI, host and vulnerability information are displayed as they are discovered by Internet Scanner.

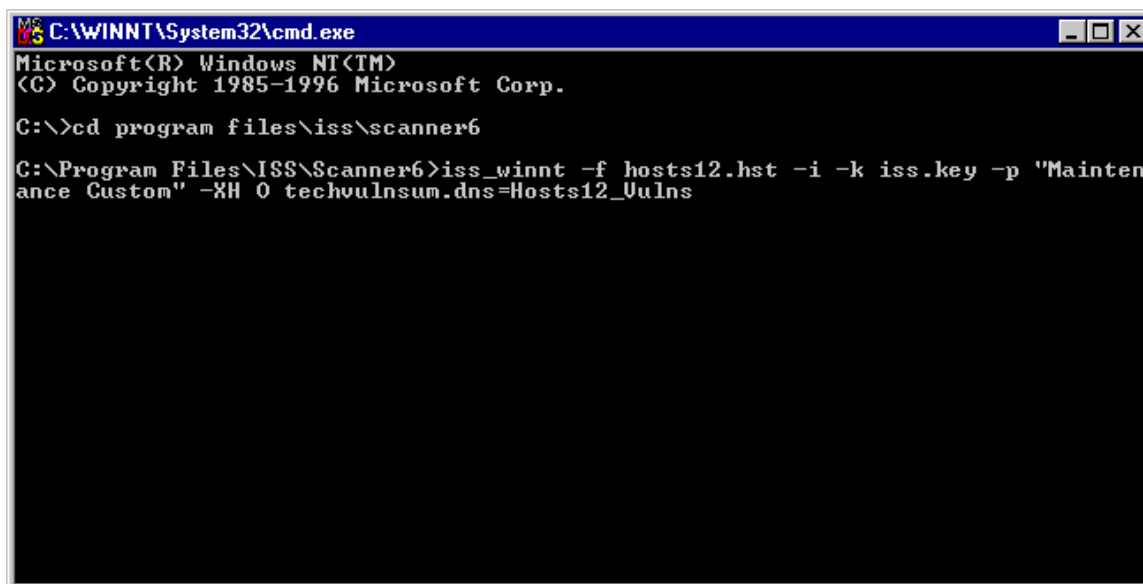


Users can also run scans from the GUI in Console Mode, which initiates a command line scan and reduces the overhead associated with the GUI.

Command Line Interface

Internet Scanner's command line interface (CLI) allows sophisticated control of the application. From the command line, users can perform scans, run reports, and install X-Press Updates. In the example below, executing the command line will run a scan using a custom policy called "Maintenance Custom" on computers listed in the host list

“hosts12.hst”. When the scan completes, it will automatically export an HTML-formatted report to an existing file named “Hosts12_Vulns”.



```
C:\WINNT\System32\cmd.exe
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>cd program files\iss\scanner6

C:\Program Files\ISS\Scanner6>iss_winnt -f hosts12.hst -i -k iss.key -p "Maintenance Custom" -XH 0 techvulnsum.dns=Hosts12_Vulns
```

Using the AT command of the Windows NT® Task Scheduler™, users can schedule scans, reports, and X-Press Updates to run as command lines, or as part of a batch file. This permits extensive automation of Internet Scanner operations.

About Internet Security Systems (ISS)

Internet Security Systems, Inc. (ISS) (NASDAQ: ISSX) is the leading global provider of security management solutions for the Internet. ISS protects critical information and network resources from attack and misuse. By combining best of breed software products, market-leading managed security services, aggressive research and development, and comprehensive educational and consulting services, ISS is the trusted security provider for thousands of customers around the world.

Copyright © 2000 Internet Security Systems, Inc. All rights reserved. Internet Security Systems, X-Force, Internet Scanner, X-Press Update and FlexCheck are trademarks of Internet Security Systems, Inc. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications are subject to change without notice.

Appendix A: Internet Scanner Database Schema

The tables below list the fields, datatype, and a field description for each table in the Internet Scanner Database.

Banners table

Name	Type	Comment
jobID	Number (Long)	Job ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session
bannerType	Text	Type of banner (SMTP, FTP, Telnet, etc.)
bannerText	Memo	Banner text

FilesInstalled table

Name	Type	Comment
name	Text	Installed data (<i>.dat</i>) files
modifiedDate	Date/Time	The date and the time the data (<i>.dat</i>) files were installed on the computer
versionID	Number (Integer)	Internet Scanner version ID
totalVulns	Number (Integer)	Total number of vulnerability checks installed on this computer

Hosts table

Name	Type	Comment
HostID	Number (Long)	Host ID for specific scan session
ipAddress	Number (Double)	IP Address (Numeric)
firstJobID	Number (Long)	First job ID for this host
lastJobID	Number (Long)	Last job ID for this host
ipAddressStr	Text	IP address as a dotted string
DNSName	Text	DNS name (www.iss.net, for example)
NBName	Text	NetBIOS name
osName	Text	Operating system type
NBDomain	Text	NetBIOS domain

HostsChanged Summary table

Name	Type	Comment
hostID	Number (Long)	Host ID for specific scan session
status	Number (Long)	The status of the host (1=new or 2=inactive)

HostsFound table

Name	Type	Comment
hostID	Number (Long)	Host ID for specific scan session
jobID	Number (Long)	Job ID for specific scan session
pingtime	Number (Long)	Ping response time in milliseconds

Jobs table

Name	Type	Comment
jobID	Number (Long)	Job ID for specific scan session
startTime	Date/Time	Start time
stopTime	Date/Time	Finish time
scanHost	Number (Long)	Scanning host
numHostScanned	Number (Long)	Number of hosts scanned
numHostActive	Number (Long)	Number of active hosts
numHostInactive	Number (Long)	Number of inactive hosts
elapsedTime	Text	Elapsed time of scan session
jobDesc	Text	Job description
jobComment	Text	Job comment
templateName	Text	Scan policy used for scan session
templateVersion	Number (Long)	Version of the scan policy being used
logfileName	Text	Log file used for scan session
termStatus	Text	Scan session termination status
upLoaded	Yes/No	Used by SAFESuite Decisions to determine if the job has been uploaded to the database
keyName	Text	Key file used for the scan session
trendConfigID	Number (Long)	Trend ID for the specific scan session

SchemaVer table

Name	Type	Comment
majorVer	Number (Long)	Database version number
minorVer	Number (Long)	Database version number, if not for a major release of Internet Scanner
reason	Text	The reason information changed in the database
chTime	Date/Time	The date and the time that information changed in the database

Services table

Name	Type	Comment
serviceID	Number (Long)	Service ID for specific scan session
serviceName	Text	Service name
shortdesc	Text	Description
ports	Number (Long)	Port (if any)
assocVuln	Number (Long)	Associated vulnerability
serviceType	Text	Service type (TCP, UDP, RPC, NT)
userNotes	Text	For use by the user

ServicesChanged Summary table

Name	Type	Comment
serviceID	Number (Long)	Service ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session
status	Number (Long)	The status of the service (1=new or 2=removed)

ServicesFound table

Name	Type	Comment
serviceID	Number (Long)	Service ID for specific scan session
jobID	Number (Long)	Job ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session

TempVulns table

Name	Type	Comment
vulnID	Number (Long)	Vulnerability ID for specific scan session
severity	Number (Integer)	Severity or risk level (1=low, 2=medium, 3=high)
vulnName	Text	Vulnerability name
shortdesc	Text	Vulnerability title
osAffected	Text	Operating system affected
fullDesc	Memo	Detailed description of the vulnerability
fix	Memo	Detailed fix information
usrSeverity	Number (Integer)	For use by customer
usrVulnName	Text	For use by customer
usrDesc	Memo	For use by customer
usrFix	Memo	For use by customer
vulnTag	Text	X-Force Database tag name

Note: In the *Name* field, only entries with a *usr* prefix can be safely edited and will not be overwritten in future releases of Internet Scanner.

Trend Configurations table

Name	Type	Comment
configID	Number (Long)	Trend ID for specific scan session
name	Text	Name of the scan policy and the scanning IP address for the scan session
templateName	Text	Scan policy used for scan session
templateVersion	Number (Long)	Version of the scan policy being used
minIpAddr	Number (Double)	First IP address used in the scan session
maxIpAddr	Number (Double)	Last IP address used in the scan session
numHosts	Number (Long)	Number of hosts used in the scan session

TrendHosts Summary table

Name	Type	Comment
configID	Number (Long)	Trend ID for specific scan session
jobID	Number (Long)	Job ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session
Severity1	Number (Long)	Number of low risks found in the scan session
Severity2	Number (Long)	Number of medium risks found in the scan session
Severity3	Number (Long)	Number of high risks found in the scan session

TrendJobs Summary table

Name	Type	Comment
jobID	Number (Long)	Job ID for specific scan session
configID	Number (Long)	Trend ID for specific scan session
Severity1	Number (Long)	Number of low risks found in the scan session
Severity2	Number (Long)	Number of medium risks found in the scan session
Severity3	Number (Long)	Number of high risks found in the scan session

Users table

Name	Type	Comment
userID	Number (Long)	User ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session
userName	Text	User login name
fullName	Text	User's full name
comment	Text	For use by the user
userPassword	Text	User's password
imageIndex	Number (Long)	Icons representing a user, a machine, or a group

UsersFound table

Name	Type	Comment
jobID	Number (Long)	Job ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session
userID	Number (Long)	User ID for specific scan session

VersionHistory table

Name	Type	Comment
versionMajor	Number (Long)	Internet Scanner version number
versionMinor	Number (Long)	Internet Scanner version number, if it's not a major release of Internet Scanner
vulnsLoaded	Number (Integer)	Number of vulnerabilities in the database
chTime	Date/Time	The date and the time that information changed in the database
reason	Text	The reason information changed in the database

Vulns table

Name	Type	Comment
vulnID	Number (Long)	Vulnerability ID for specific scan session
severity	Number (Integer)	Severity or risk level (1=low, 2=medium, 3=high)
vulnName	Text	Vulnerability name
shortdesc	Text	Vulnerability title
osAffected	Text	Operating system affected
fullDesc	Memo	Detailed description of the vulnerability
fix	Memo	Detailed fix information
usrSeverity	Number (Integer)	For use by customer
usrVulnName	Text	For use by customer
usrDesc	Memo	For use by customer
usrFix	Memo	For use by customer
vulnTag	Text	X-Force database tag name

Note: In the *Name* field, only entries with a *usr* prefix can be safely edited and will not be overwritten in future releases of Internet Scanner.

VulnsChanged Summary table

Name	Type	Comment
hostID	Number (Long)	Host ID for specific scan session
vulnID	Number (Long)	Vulnerability ID for specific scan session
status	Number (Long)	The status of the vulnerability (1=fixed, 2=new, 3=still present)

VulnFound table

Name	Type	Comment
vulnID	Number (Long)	Vulnerability ID for specific scan session
jobID	Number (Long)	Job ID for specific scan session
hostID	Number (Long)	Host ID for specific scan session
assocInfo	Text	Associated information (such as share name)
moreInfo	Memo	Extended information (such as finger dump)
status	Number (Long)	The status of the vulnerability (1=fixed, 2=new, 3=still present)