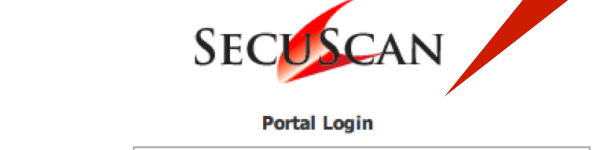
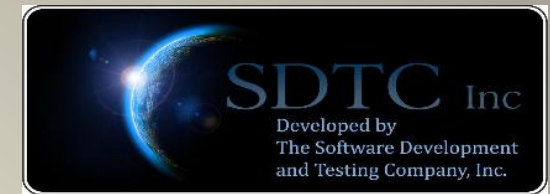




Secured Log in Prompt



SECUSCAN

Portal Login

Email

Password

☐ Remember me on this computer

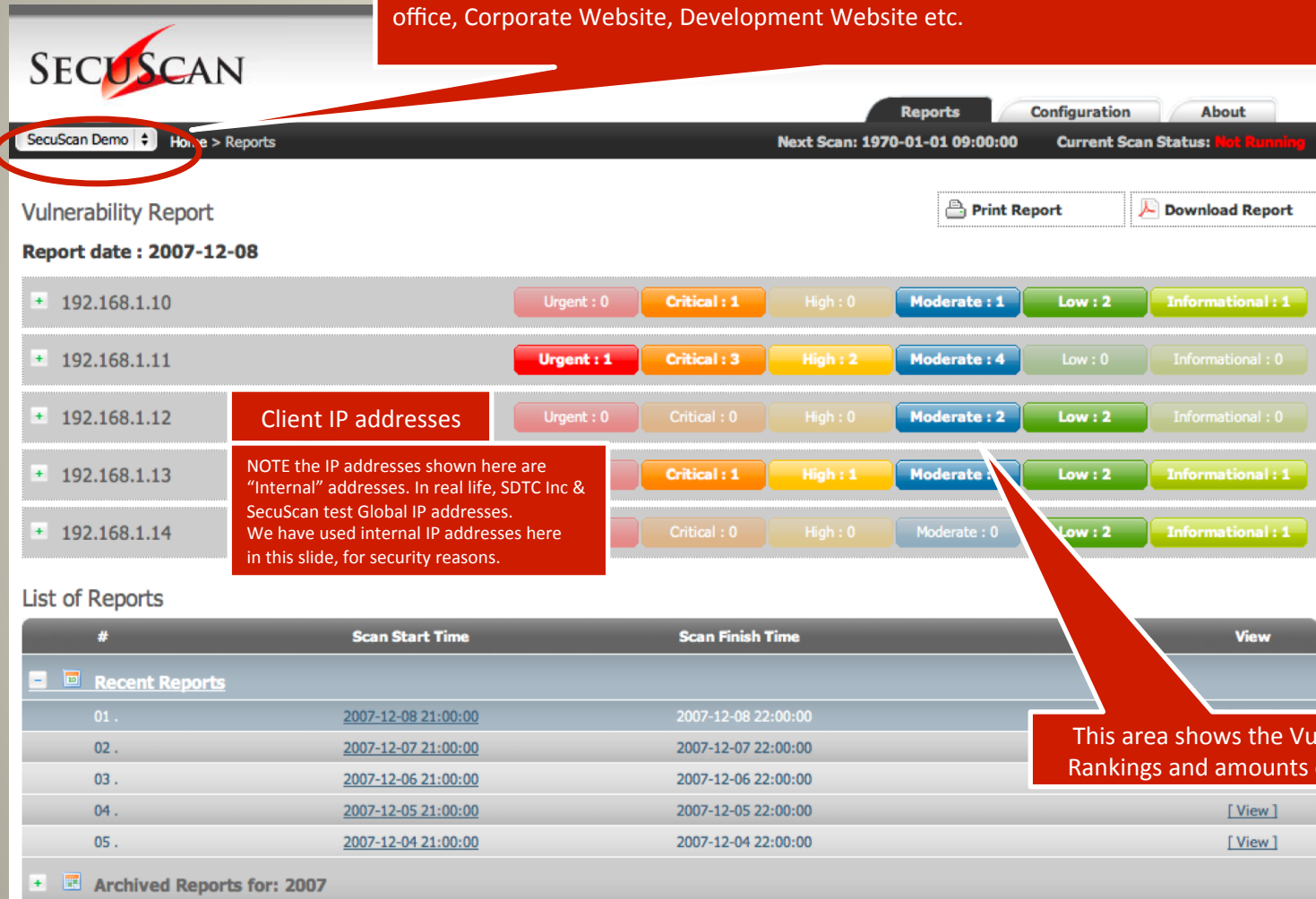
Sign In

[Forgot your password ?](#)

This is where the client uses their unique User name and Password, to view their Scan Vulnerability report.

© Copyright 2008 SecuSolutions Ltd.

The first view the client will see is their IP profile. If the client has many profiles, they can view each separate profile from this drop down list. Eg New York office, Los Angeles office, Tokyo office, Corporate Website, Development Website etc.



SECUSCAN

SecuScan Demo | Home > Reports | Next Scan: 1970-01-01 09:00:00 | Current Scan Status: **Not Running**

Vulnerability Report

Report date : 2007-12-08

Print Report | Download Report

IP Address	Urgent	Critical	High	Moderate	Low	Informational
192.168.1.10	0	1	0	1	2	1
192.168.1.11	1	3	2	4	0	0
192.168.1.12	0	0	0	2	2	0
192.168.1.13	0	1	1	1	2	1
192.168.1.14	0	0	0	0	2	1

Client IP addresses

NOTE the IP addresses shown here are "Internal" addresses. In real life, SDTC Inc & SecuScan test Global IP addresses. We have used internal IP addresses here in this slide, for security reasons.

List of Reports

#	Scan Start Time	Scan Finish Time	View
Recent Reports			
01 .	2007-12-08 21:00:00	2007-12-08 22:00:00	
02 .	2007-12-07 21:00:00	2007-12-07 22:00:00	
03 .	2007-12-06 21:00:00	2007-12-06 22:00:00	
04 .	2007-12-05 21:00:00	2007-12-05 22:00:00	[View]
05 .	2007-12-04 21:00:00	2007-12-04 22:00:00	[View]
Archived Reports for: 2007			

This area shows the Vulnerability Rankings and amounts discovered



SecuSolutions

IP Summary View



sales@secuscan.net : [Sign Out]

ReportsConfigurationAbout

SecuScan Demo Home > Reports

Next Scan: 1970-01-01 09:00:00 Current Scan Status: Not Running

Vulnerability Report
Report date : 2007-12-08

A detailed summary of the IP address(s) displaying the hostname, the likely Operating System, whether the system is ping able or not, as well as the open TCP and UDP ports.

192.168.1.10

Moderate : 1Low : 2Informational : 1

192.168.1.11

Urgent : 1High : 2Moderate : 4Low : 0Informational : 0

Summary

Urgent : 1High : 1Moderate : 4Low : 0Informational : 0

Web Findings

Urgent : 0Critical : 0High : 0Moderate : 0Low : 0Informational : 0

Network Findings

Urgent : 0Critical : 0High : 0Moderate : 0Low : 0Informational : 0

192.168.1.12

Urgent : 0Critical : 1High : 0Moderate : 1Low : 2Informational : 1

192.168.1.13

Urgent : 1Critical : 3High : 2Moderate : 4Low : 0Informational : 0

192.168.1.14

Urgent : 0Critical : 0High : 0Moderate : 0Low : 0Informational : 0

List of Reports

#	Scan Date
01 .	2007
02 .	2007

192.168.1.11

Urgent : 1Critical : 3High : 2Moderate : 4Low : 0Informational : 0

Summary

Hostname	www.somehost.jp
Likely OS	Windows
Open TCP Ports	21, 80, 135, 443, 445
Open UDP ports	161
Ping	NO

Web Findings

Urgent : 1Critical : 0High : 1Moderate : 0Low : 0Informational : 0

Network Findings

Urgent : 0Critical : 3High : 1Moderate : 4Low : 0Informational : 0



SecuSolutions

Web App. Vulnerabilities Expanded View

SECUSCAN

sales@secuscan.net : [Sign Out]

Reports Configuration About

SecuScan Demo Home > Reports

Next Scan: 1970-01-01 09:00:00 Current Scan Status: Not Running

Vulnerability Report

Report date : 2007-12-08

Print Report Download Report

192.168.1.10 Urgent : 0 Critical : 1 High : 0 Moderate : 1 Low : 2 Informational : 1

192.168.1.11 Urgent : 1 Critical : 3 High : 2 Moderate : 4 Low : 0 Informational : 0

Summary

Web Findings

Network Findings

192.168.1.12

192.168.1.11 Urgent : 1 Critical : 3 High : 2 Moderate : 4 Low : 0 Informational : 0

Summary

Web Findings

Network Findings

192.168.1.11

Urgent : 1 Critical : 3 High : 2 Moderate : 4 Low : 0 Informational : 0

Urgent : 1 Critical : 0 High : 1 Moderate : 0 Low : 0 Informational : 0

Possible SQL injection in MS SQL

Possible Cross Site Scripting

Network Findings

Urgent : 0 Critical : 3 High : 1 Moderate : 4 Low : 0 Informational : 0

The name of the web application vulnerability(s) and the risk rank classification are clearly displayed and color coded



Web App. Vulnerabilities Explanation and Remediation Recommendation

The screenshot displays the SecuSolutions web application security scanner interface. At the top, a summary bar for IP 192.168.1.11 shows the following counts: Urgent: 1, Critical: 3, High: 2, Moderate: 4, Low: 0, and Informational: 0. Below this, a 'Web Findings' section lists several vulnerabilities, including 'Possible SQL injection in MS SQL' and 'Possible Cross Site Scripting'. A red arrow points from the 'Possible SQL injection in MS SQL' finding to a detailed view of this vulnerability.

Each Vulnerability has a unique ID# as well as easily understandable Risk explanation along with a Remediation Recommendation

Recommendations are written so that nearly anyone can follow the instructions and repair issues discovered by SDTC Inc & SecuScan

Vulnerability ID: #00151

Risk:
SQL injection vulnerabilities can allow an attacker to extract, modify, add or delete information from database servers. The results of a successful SQL injection attack can vary greatly depending upon the environment and configuration in which it occurs. For instance, if the database connection utilizes the security context of the database owner (dbo), a successful exploitation would give an attacker the means to modify table contents, create new tables, etc. If the default account SA is utilized, successful exploitation of a SQL Injection vulnerability could lead to an attacker gaining complete control over the SQL server itself, or even (by creating user accounts) to taking control of the server that houses the database itself.

Recommendation:
SQL injection is caused by programming techniques that allow client-supplied values to interfere and modify SQL statement syntax. Thus, the best solution is to design and program web applications in a manner that prevents client-supplied values from being treated as SQL syntax. By using stored procedures to execute SQL statements and command objects or prepared statements to access them, it is possible to ensure that any client-supplied values used will be treated as an expression and will not be able to modify the SQL syntax.
If this is not possible, use data sanitization. Data sanitization is the practice of removing potentially malicious characters from client-supplied values before using them in SQL statements. To use data sanitization effectively, make sure all client-supplied values are placed inside single quotes. Filter these values according to the type of input expected. For instance, a phone number value should only be allowed to contain numbers. If potentially malicious characters such as single quotes and semicolons must be used, encode them in a manner that ensures they will not interfere with the SQL query.



SecuSolutions

Network Vulnerabilities Expanded

SECUSCAN

sales@secuscan.net : [Sign Out]

Reports Configuration About

SecuScan Demo Home > Reports

Next Scan: 1970-01-01 09:00:00 Current Scan Status: Not Running

Vulnerability Report

Report date : 2007-12-08

Print Report Download Report

IP Address	Urgent	Critical	High	Moderate	Low	Informational
192.168.1.10	0	1	0	1	2	1
192.168.1.11	1	3	2	4	0	0

Summary

Web Findings

Network Findings

192.168.1.12

192.168.1.13

192.168.1.14

List of Reports

#

Scan Start Time

Web and Network Vulnerabilities are separated, for ease of understanding

192.168.1.11

Urgent: 1 Critical: 3 High: 1 Moderate: 4 Low: 0 Informational: 0

Web Findings

Network Findings

- IIS 5.0 Sample App reveals physical path of web root
- ASN.1 Vulnerability Could Allow Code Execution
- Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)
- IIS directory traversal
- Anonymous FTP Service
- SNMP Public String
- NetBIOS : Null Session
- HTR Extension

Network Vulnerabilities are clearly listed in their order of urgency



Network Vulnerabilities Explanation and Remediation Recommendation

192.168.1.11

Urgent: 1Critical: 3High: 2Moderate: 4Low: 0Informational: 0

Summary

Web Findings

Network Findings

Urgent: 1Critical: 0High: 1Moderate: 0Low: 0Informational: 0

Urgent: 0Critical: 3High: 1Moderate: 4Low: 0Informational: 0

IIS 5.0 Sample App reveals physical path of web root

ASN.1 Vulnerability Could Allow Code Execution

Vulnerabilities in MSDTC and COM+ Could Allow

IIS directory traversal

Anonymous FTP Service

SNMP Public String

NetBIOS : Null Session

HTR Extension

Each vulnerability is easily viewable by expanding the tree, to see the Risk and the Recommended action

NetBIOS : Null Session

Moderate

Vulnerability ID: #00113

Risk:
A Null Session occurs when an attacker sends a blank username and blank password to try to connect to the IPC\$ (Inter Process Communication) pipe. If an attacker is successful in creating a Null session to IPC\$ he is then able to gain a list of user names, shares, etc.

Recommendation:
All Netbios ports should be blocked with a filtering device such as a firewall and they should never be open to the Internet.
Set the following registry key settings: Hive: HKEY_LOCAL_MACHINE Path: System\CurrentControlSet\Control\LSA Key: RestrictAnonymous Type: REG_DWORD Value: 1 Security configuration manager from Microsoft can assist in creating scripts to make this change in an automatic fashion.
<http://support.microsoft.com/default.aspx?scid=kb;en-us;246261>



SecuSolutions

Report Archive and Comparison

SECUSCAN

sales@secuscan.net : [Sign Out]

SecuScan Demo Home > Reports

Vulnerability Report

Print Report Download Report

Current Scan Status: Not Running

01-01 09:00:00

Moderate : 1 Low : 2 Informational : 1

Critical : 3 Moderate : 4 Low : 0 Informational : 0

192.168.1.11

Summary

Web Findings

Network Findings

192.168.1.12 Urgent

192.168.1.13 Urgent

192.168.1.14 Urgent

List of Reports

#	Scan Start Time	Scan Finish Time	View
Archived Reports for: 2007			
December			
<input type="checkbox"/> 01.	2007-12-08 21:00:00	2007-12-08 22:00:00	[View]
<input type="checkbox"/> 02.	2007-12-07 21:00:00	2007-12-07 22:00:00	[View]
<input type="checkbox"/> 03.	2007-12-06 21:00:00	2007-12-06 22:00:00	[View]
<input type="checkbox"/> 04.	2007-12-05 21:00:00	2007-12-05 22:00:00	[View]
<input type="checkbox"/> 05.	2007-12-04 21:00:00	2007-12-04 22:00:00	[View]
<input type="checkbox"/> 06.	2007-12-03 21:00:00	2007-12-03 22:00:00	[View]
<input type="checkbox"/> 07.	2007-12-02 21:00:00	2007-12-02 22:00:00	[View]
<input type="checkbox"/> 08.	2007-12-01 21:00:00	2007-12-01 22:00:00	[View]
November			
Select Latest Unselect All Compare			

Clients can select the report date(s) and view a date in time or several dates in time

Many security compliances require "proof" of regular security audits. Reports can be archived here for up to 12 months.



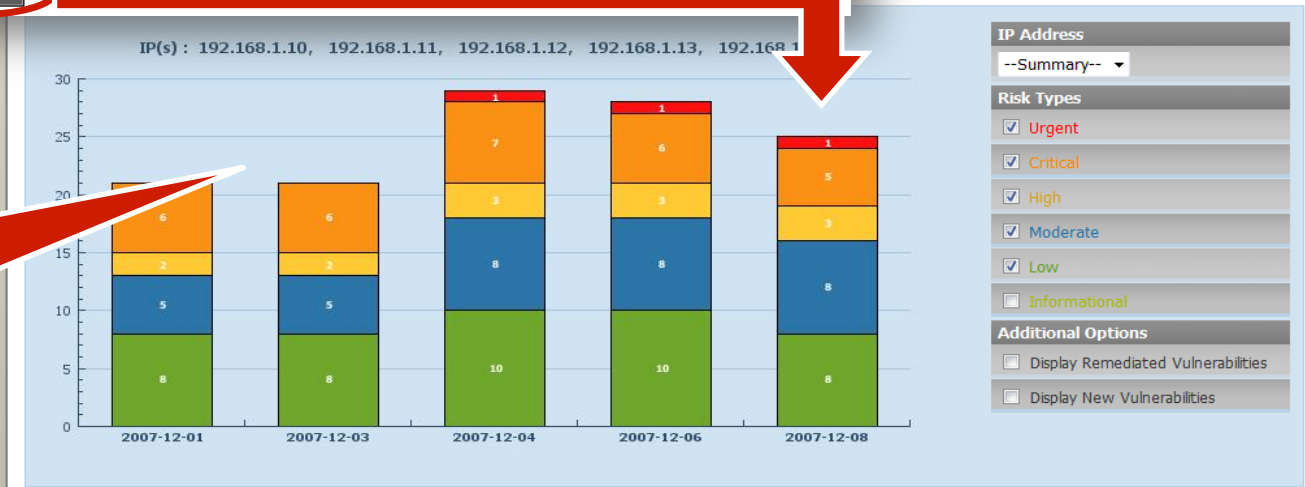
Graph View of IP Addresses, Date Ranges and Vulnerability View

#	Scan Start Time	Scan Finish Time	View
Archived Reports for: 2007			
December			
<input checked="" type="checkbox"/> 01.	2007-12-08 21:00:00	2007-12-08 22:00:00	View
<input type="checkbox"/> 02.	2007-12-07 21:00:00	2007-12-07 22:00:00	View
<input checked="" type="checkbox"/> 03.	2007-12-06 21:00:00	2007-12-06 22:00:00	View
<input type="checkbox"/> 04.	2007-12-05 21:00:00	2007-12-05 22:00:00	View
<input checked="" type="checkbox"/> 05.	2007-12-04 21:00:00	2007-12-04 22:00:00	View
<input checked="" type="checkbox"/> 06.	2007-12-03 21:00:00	2007-12-03 22:00:00	View
<input type="checkbox"/> 07.	2007-12-02 21:00:00		View
<input checked="" type="checkbox"/> 08.	2007-12-01 21:00:00		View
November			
Select Latest Unselect All Compare			

Select the desired date ranges

Click the compare button

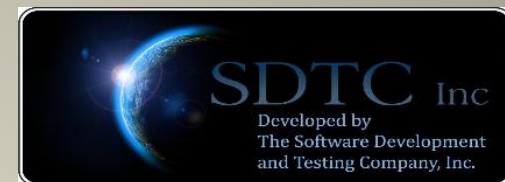
View a detailed graph that shows each IP address, the date, the vulnerability ranks and the amount of vulnerabilities found





SecuSolutions

Graph Flexibility



Flexibility is built into SecuScan. The client can choose to view what they want. Remediated Vulnerabilities, New Vulnerabilities, or any combination of Urgent, Critical, High, Moderate, Low or Informational vulnerabilities

#	Scan Start Time	Scan Finish Time	View
Archived Reports for: 2007			
December			
<input checked="" type="checkbox"/> 01.	2007-12-08 21:00:00	2007-12-08 22:00:00	View
<input type="checkbox"/> 02.	2007-12-07 21:00:00	2007-12-07 22:00:00	View
<input checked="" type="checkbox"/> 03.	2007-12-06 21:00:00	2007-12-06 22:00:00	View
<input type="checkbox"/> 04.	2007-12-05 21:00:00	2007-12-05 22:00:00	View
<input checked="" type="checkbox"/> 05.	2007-12-04 21:00:00	2007-12-04 22:00:00	View
<input checked="" type="checkbox"/> 06.	2007-12-03 21:00:00	2007-12-03 22:00:00	View
<input type="checkbox"/> 07.	2007-12-02 21:00:00	2007-12-02 22:00:00	View
<input checked="" type="checkbox"/> 08.	2007-12-01 21:00:00	2007-12-01 22:00:00	View
November			
<input type="button" value="Select Latest"/> <input type="button" value="Unselect All"/> <input type="button" value="Compare"/>			





IP Specific & Date Range and Vulnerability View


Use the drop down menu to select the IP address you wish to view





SecuSolutions

Comprehensive FAQ View

sales@secuscan.net : [\[Sign Out\]](#)

[Scan and Reports](#)[Password](#)[Support](#)[About](#)

SecuScan Demo ▾ [Home](#) > [Frequently Asked Questions](#)

Frequently Asked Questions

[Search](#)

Login

Q

What does remember me on the login page mean?

Reports

Q

Why does a report page open up immediately after I login?

Q

In the report, what does likely OS mean?

Q

What does Open TCP Ports mean?

Q

What are the codes that might appear in my Open TCP ports?

Q

What does the likely OS mean?

Q

What are the codes that might appear in my Open UDP ports?

Q

What are the recommendations that were given to me in the report. What are my options?

A very comprehensive FAQ is available on the client portal. The FAQ is separated into "topic specific" areas so you can get the answers you need, when you need them.



Comprehensive Service Description

- Contact Info:
 - E-mail: support@fortiscan.com

[Click here to download Service Level Agreement \[PDF 79KB\]](#)

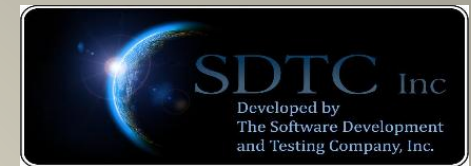
FortiScan Vulnerability Risk Ranking Criteria

Risk Level (Recommended Response Time)	Damages Estimated ₁	Security Expertise and Knowledge ₂	Interaction or knowledge about the target before attacking ₃	Description
Urgent (Immediately)	Entire system could be compromised at any moment.	Unnecessary	Unnecessary	<ul style="list-style-type: none">• The 'Urgent' rating is applied to remotely exploitable vulnerabilities which have very high potentials to cause a full system compromise/access.• Successful exploitation of your network and information does not normally require any prior interaction or knowledge about your system. Most often the exploits that take advantage of the vulnerabilities are still in the wild.
<div>Our Engineers have documented every possible detail that explains the Vulnerability Service to our clients such as tests performed, risk rankings explained, Scanning details</div>	Could be compromised in a short period	Necessary	Almost Unnecessary	<ul style="list-style-type: none">• The 'Critical' rating is applied to remotely exploitable vulnerabilities, which can lead to a system compromise/access.• The difference between 'Urgent' and 'Critical' is that to exploit a 'Critical' vulnerability, it may require some interaction or knowledge about your system prior to the exploitation attempt. As for an Urgent Risk Level, prior interaction or knowledge about your system may not be required.

Our Engineers have documented every possible detail that explains the Vulnerability Service to our clients such as tests performed, risk rankings explained, Scanning details



View or Save the Report Using Adobe Acrobat Reader



SECUSCAN sales@secuscan.net : [Sign Out]

Scan and Reports Password Support About

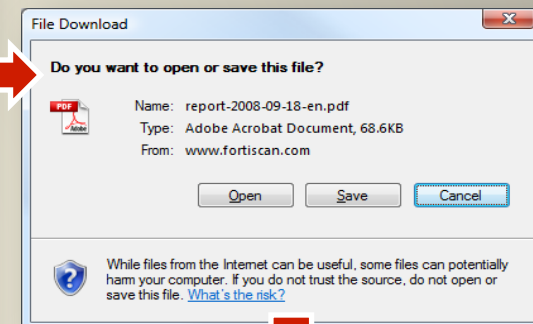
SecuScan Demo Home > Reports

Vulnerability Report
Report date : 2007-12-08

Print Report Download Report

IP Address	Urgent	Critical	High	Moderate	Low	Informational
192.168.1.10	0	1	0	1	2	1
192.168.1.11	1	3	2	4	0	0
192.168.1.12	0	0	0	2	2	0
192.168.1.13	0	1	1	1	2	1
192.168.1.14	0	0	0	0	2	1

All of the Security Scan reports can be saved in PDF format to your local computer



SECUSCAN Vulnerability Report

Company Name: SecuSolutions Ltd.
Scan Date: 2007-12-08 22:00:00

IP Address	Urgent	Critical	High	Moderate	Low	Informational
192.168.1.10 gw.somehost.jp	0	1	0	1	2	1
192.168.1.11	1	3	2	4	0	0





SecuSolutions

Security Scans that clients can See and Trust

About Us

SecuSolutions Ltd. is taking a "byte" out of security!

SecuSolutions Ltd., is a specialized security company that is incorporated in Calgary, Alberta Canada. SecuSolutions Ltd provides security products, service and solutions to large, medium and small Enterprises throughout North America. Members of SecuSolutions Ltd team have provided high level network and web application security audits, security consulting, security e-learning education, security software development, security compliance, security conferences and seminars around the globe since August of 2001. Key members have been performing security consulting in North America for the past 22 years.

SecuSolutions Ltd provides security products, service and solutions to large, medium and small Enterprises throughout North America. Members of SecuSolutions Ltd team have provided high level network and web application security audits, security consulting, security e-learning education, security software development, security compliance, security conferences and seminars around the globe since August of 2001. Key members have been performing security consulting in North America for the past 22 years.

Our Vision is to remove security from the minds of our clients, by providing products and solutions that empower their business, not impede it.

When the SecuScan Certified logo is clicked, the SecuScan website will appear and explains what the SecuScan Certification means. This reassures your clients that the certification is genuine.

Each site SecuScan tests, will have a SDTC Inc SecuScan Certified logo placed on it, showing the Company name and successful scan date

Why SecuScan?

- Service Information
- Compliance
- Order

This Site Has Been Certified by the SecuScan Daily Audit Service

WEBSITE: www.secsolutions.com
IP ADDRESS: 206.174.200.196
COMPANY: SecuSolutions Ltd.
LAST SCAN: 2009-04-01 00:21:58

This site has been tested and is certified to meet the SecuScan Daily Audit Security Scan Standard. This Daily Security Audit is your assurance that the above mentioned company is taking the necessary precautions to protect confidential data; the live SecuScan mark only appears when a web site meets the SecuScan standard.

About SecuScan

SecuScan is an automated service that has been developed by Certified Security Professionals that possess the CISSP, CISM, CISA, and CHS-III certifications. SecuScan was developed to provide the end user with a comprehensive daily report on the security status of their mission critical networks, and web applications.

SecuScan utilizes its own proprietary technology and Security Standards in combination with several other world class technologies to pinpoint potential vulnerabilities identified within the client's networks and web applications. SecuScan's report identifies the issues, explains the risk associated, and provides a solution to the problem.