Secuguard NSE

Security Vulnerability Assessment! What should you do?

The first step to Information Security is Security Vulnerability Assessment.

Scan and Confirm with NSE!

The Secuguard NSE automatically scans for network security vulnerabilities and provide remedies for the vulnerabilities found. It is a software solution for the preventing hacking and computer related crimes.

NSE automatically detects the system's IP address and operating system to generate a security scan policy for the system. The automatically generated scan policy provides a more automated and intelligent scan procedure. Additionally, multiple hosts can be scanned simultaneously to drastically shorten the time needed for the scan.

NSE provides a comprehensive scan function for network resources on the network to scan for vulnerabilities. This may lead to imprecise results compared with the host based scanner. But NSE is easier to manage because an agent is not necessary for each target server.

NSE Characteristics

✓ Common Vulnerability Exposure (CVE) Certificate

· Certificate of Common Vulnerability Exposure (CVE), The Standard for Information Security Vulnerability Names from MITRE

✓ Ease of Use and Installation

· Windows Explorer style user interface
· Detailed online help for installation and usage
· Real-time scan history, progress and result report

✓ Powerful Vulnerability Scanning Capability

· Powerful password cracking functions
· Various scan policies such as individual, group, operation system, etc
· Shows the risk level, description, impact, remedy, references, etc. for the found
· Reduces scan time by sharing information between modules using the Knowledge Base

✓ Automatic Detection of Scan Targets and It's kind of Operating System

· Detect IP Address
· Detect Operating System
· Detect DNS Name
· Detect Network Node Name if OS is MS Windows

✓ Detailed Vulnerability Information

· Various vulnerability information provided by a assessment tool experts
· Vulnerability information sorted by group, operating system, risk level, etc

✓ Encryption of Communication and Result Data

· Encryption of communication messages between the console and server
· Only valid consoles and users can access scan results

✓ Online and Offline Update

· Updates scan modules, console module and vul-info db via the update server and internet
· Provides offline update option for users without internet access

✓ Ease of Vulnerability Management

· Simultaneous scans for multiple servers on one console
· Shorten scan time due to simultaneous scans

✓ Various Additional Features

· Scheduled scans allows automated scans and automatically sends email to each server administrator
· Support scan modules and vul-infos of new vulnerabilities continuously
· Support information links of vulnerabilities
· Support function to integrate with ESM
· Ignore scanned vulnerabilities for report by user-setting

✓ Easy Installation and Expansion

· Easy installation using InstallShield
· Supports multiple consoles for load balancing

Benefit of Secuguard NSE

Preventing Security Incidents

Periodic vulnerability assessment for running system can prevent unexpected security incidents.

Disaster Recovery Plan

Periodic, daily security vulnerary assessment and action can minimize the damages from system's unexpected disorder and obstacles.

Vulnerability Assessment

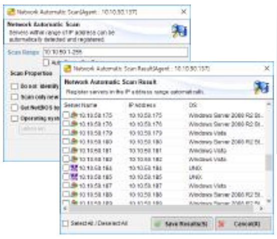
Analyzing current system's security state. Promoting secure system operation based on analyzed security state.

Security improvement

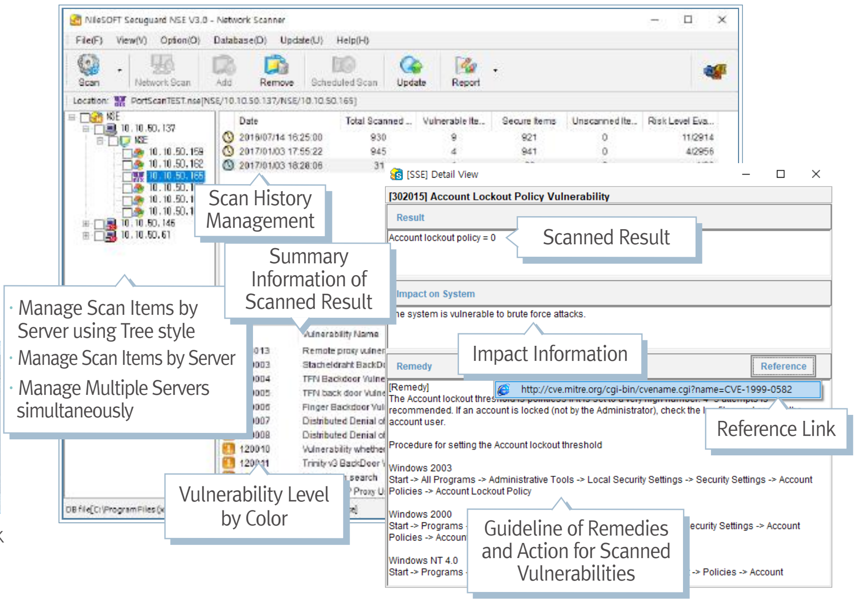
Deep understanding of system with provided various security vulnerability assessment. This can be adapted by Operation policy. It can be used and help increasing higher security system.

NSE Screen Shots and Features

▲ Screen of Scanning Process



▲ Screen of Searching Network



Location: PortScanTEST.nse[NSE/10.10.50.137/NSE/10.10.50.165]

Date	Total Scanned ...	Vulnerable Ite...	Secure Items	Unscanned Ite...	Risk Level Eva...
2016/07/14 16:25:00	930	9	921	0	11/2914
2017/01/03 17:55:22	945	4	941	0	4/2956
2017/01/03 18:28:06	31				

[302015] Account Lockout Policy Vulnerability

Account lockout policy = 0

he system is vulnerable to brute force attacks.

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0582

[Remedy]
The Account lockout thres
recommended. If an account is locked (not by the Administrator), check the l
account user.

Procedure for setting the Account lockout threshold

Windows 2003
Start -> All Programs -> Administrative Tools -> Local Security Settings -> Security Settings -> Account Policies -> Account Lockout Policy

Windows 2000
Start -> Programs ... ecurity Settings -> Account
Policies -> Accoun

Windows NT 4.0
Start -> Programs ... -> Policies -> Account

- Manage Scan Items by Server using Tree style
- Manage Scan Items by Server
- Manage Multiple Servers simultaneously

Scan History Management

Summary Information of Scanned Result

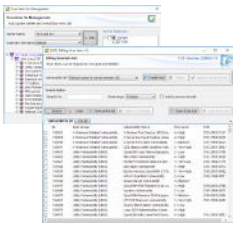
Vulnerability Level by Color

Scanned Result

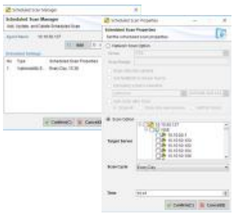
Impact Information

Reference Link

Guideline of Remedies and Action for Scanned Vulnerabilities

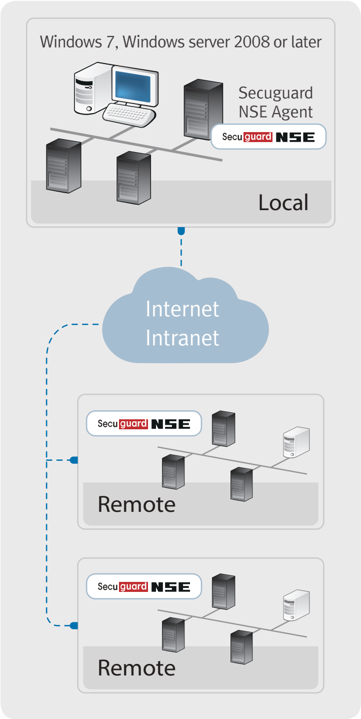


▲ Edit Scan Items



▲ Scheduled scans and Scan by Category or Item

NSE Architecture and Scan Category



Windows 7, Windows server 2008 or later

Secuguard NSE Agent

Local

Internet Intranet

Remote

Remote

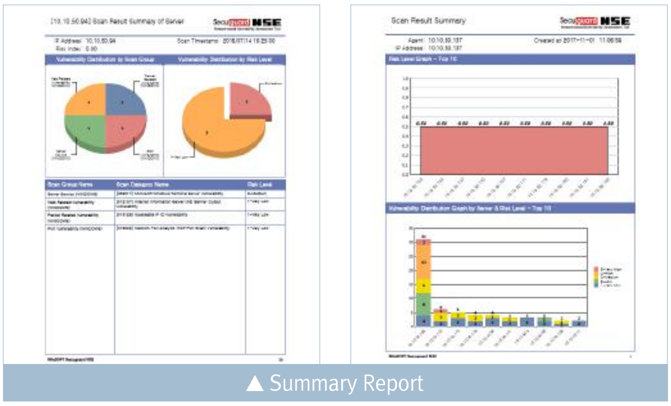
Security Vulnerability Scan Category (UNIX/Linux)

- Password Related Vulnerability
- X Windows Related Vulnerability
- Administrator and User Environment Vulnerability
- Utility Vulnerability
- File System Vulnerability
- DB Vulnerability
- Daemon Vulnerability
- Special File Vulnerability
- FTP Vulnerability
- SMTP and Mail Related Vulnerability
- RPC Vulnerability
- WWW/HTTP and CGI Vulnerability
- DNS/BIND Related Vulnerability
- Remote Access Command Vulnerability
- Packet Related Vulnerability
- Network Related Command Vulnerability
- NIS/NIS+ Vulnerability
- Firewalls/Filters/Proxies Vulnerability
- Port Vulnerability
- Backdoors Vulnerability

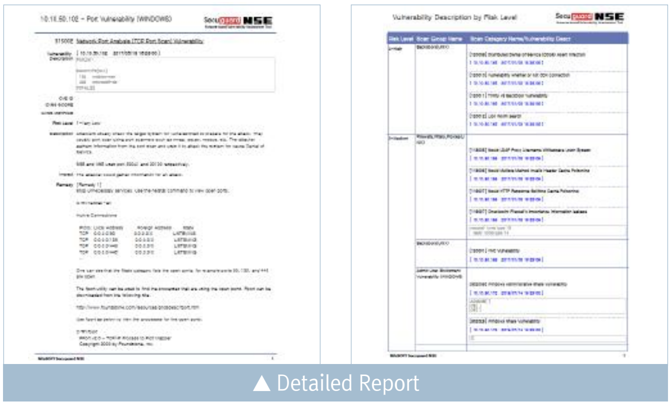
Security Vulnerability Scan Category (Windows)

- Password Related Vulnerability
- Administrator and User Environment Vulnerability
- File System Vulnerability
- DB Vulnerability
- Special File Vulnerability
- Server Service Vulnerability
- Other Server Service Vulnerability
- Application Vulnerability
- Other Application Vulnerability
- Exchange server Vulnerability
- Registry Vulnerability
- WWW/HTTP and CGI Vulnerability
- Packet Related Vulnerability
- Firewalls/Filters/Proxies Vulnerability
- Port Vulnerability
- Internet Explorer Vulnerability
- Internet Information Server Vulnerability
- SMTP and Mail Related Vulnerability
- Backdoors Vulnerability

NSE Various Reports



▲ Summary Report



▲ Detailed Report

NileSOFT
Kolon Digital Tower Billant 10th Fl. #1004, 30, Digital-ro 32-gil, Guro-gu, Seoul, 08390, South Korea
TEL. +82-2-783-0961 FAX. +82-2-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr/eng
Popularization of Information Security! NileSOFT will go together.