DragonSoft Vulnerability Management

The DragonSoft Vulnerability Management (DVM) is a completed enterprises solution which is the best solution to manage the network security. The functions include Security Scanner and Vulnerability Risk management. DragonSoft DVM is the world class Network Vulnerability Assessment and Management solution. It can assists MIS/Administrator to handle all weakness of the network, and centralized the security issues of inside and outside host that is an indispensable management tool enable MIS/Administrator to make decision rapidly.

DragonSoft Vulnerability Management (DVM) Network scanner aims to detect the potential vulnerability and analyzes the network environment. The Functions include network exposure scanning, vulnerabilities evaluation, risk centralized assessment, reporting and remediation. It supports more than 3000 audit items of network security vulnerability, and provides complete risk assessment report for Windows 9x/NT/2000/XP/2003, Sun Solaris, BSD, Linux, Router, Switch, Firewall and different types of database (MySQL, MSSQL, Oracle, Access and IBM DB2).

The DragonSoft Vulnerability Management solution may generate the management report and the technical report and has the complete automated module update and weakness knowledge database update. The reports are include detailed vulnerability description, graphical mapping and patch recommendation. You also can setup up to 50 auto scanning schedule and the result will auto delivery to you and auto save to database.

Feature:

1. **The Comparison Report:**
   DVM Conforms to the ISO 27001 information security management standard.
2. **The databases vulnerability auditing:**
   It examines Oracle, MSSQL, MySQL, IBM DB2 and various databases vulnerability.
3. **The Network Devices vulnerability auditing:**
   It examines various network equipment vulnerability like router and firewall.
4. **HTTPS website vulnerability auditing:**
   It detects the e-commerce transaction website, is the on-line banking transaction website vulnerability.
5. **The website un-listed directory guess ability**
6. **The website penetration test:**
   It tests the website vulnerability and simulates the hacker to carry on the homepage replacement test.

7. **Has the Common Vulnerability Scoring System (CVSS) rating:**
   The vulnerability degree of hazard has the rating standardization.
8. **Has the FPP (False Positives Prevention) to sentence the prevention technology by mistake:**
   It can reduce the vulnerability which sentences by mistake
9. **Has the Microsoft Windows system software property information collection ability:**
   It will detect the Software tabulation of the Microsoft Windows system installment.
10. **Has the Microsoft Windows system service information collection ability:**
    It can detect the Service Tabulation of the Microsoft Windows system.
11. **The Real Time Result:**
    The Real Time result enables user to check the various statistical graphs result while scanning.
12. **The customizable scanning policy:**
    DVM allows administrator set up customizable scanning policy.

Model No. : DVM-00016-IP, DVM-0032-IP, DVM-00064-IP, DVM-00128-IP,

DVM-00256-IP DVM-00512-IP, DVM-01024-IP

What system DVM can install and scan?

DVM can install on Windows 2003、 Windows 2000 and Windows XP. It can scan Window, UNIX, SUN OS Solaris, TCP/IP, BSD, Linux , Web server, Mail server, FTP server and common network devices.

What's difference between DVM vulnerability scanner and an IDS (Intrusion detection System)?

Take fire security for example, an intruder Defection System is like a fire alarm. When there is thick smoke indoors, it will make the alarm sound. DVM Vulnerability Scanner is like fire security experts who will inspect a system and equipment piece by piece to find out places which increase the probability of a fire occurring. It has a preventive function.

What should we do for completed protection after scanning?

1. Patch vulnerabilities according to the scanning result.
2. Rescan and reexamine if patching vulnerabilities is complete.
3. Set up audit scanning schedule for regular scanning!

DragonSoft
www.dragonsoft.com

For more information, please kindly contact us at marketing@dragonSoft.com