Information Security Vulnerability Assessment

DragonSoft Vulnerability Management

Information is managed, integrated and quantized by Security Vulnerability Audit, efficiently achieve all-round IT security with improved ROI. Following the principles of ISO 27001:2005/BS7799 and ISMS, International CVE certifications, saving costs and time spent on evaluation of total network information security environment, the end result – mitigate risk level of network vulnerability.

Introduction

The Top 20 Most Critical Internet Security Vulnerabilities identified by SANS/FBI 2007 can be classified in 6 categories: (1) Client-side Vulnerabilities in: Web Browsers, Office Software, Email Clients, Media Players. (2) Server-side Vulnerabilities in: Web Applications, Windows Services, Unix and Mac OS Services, Backup Software, Anti-virus Software, Management Servers, Database Software. (3) Security Policy and Personnel: Excessive User Rights and Unauthorized Devices, Phishing/Spear Phishing, Unencrypted Laptops and Removable Media. (4) Application Abuse: Instant Messaging, Peer-to-Peer Programs. (5) Network Devices: VoIP Servers and Phones. (6) Zero Day Attacks. Corporate must take vulnerability audit as basic policy and practice in evaluation, planning, execution and monitoring and control of their information security on network equipment and infrastructure.

Solutions

The challenges facing by corporate are doing good internal information security planning to meet legal requirements with limited budget and employees. The quest to avoid major attacks like Nimda、CodeRed、Blaster or SQL Slammer, not to fall into hackers target list, methodologies to find potential risks and react before disasters strike are imminent to everyday task? How do we spot the unfixed in the network system infrastructure ?

DragonSoft dedicates to development of network security products. The award-winning,

standard approved products are invincible. The total effective management in heterogeneous environment such as Windows, Unix, Linux, SUN, IBM. The latest vulnerability database is kept updated continuously by DragonSoft R&D team, to ensure all the latest found vulnerability are resolved timeously.

DragonSoft Vulnerability Management Characteristics

- **Conform with international risk management regulations:** DVM risk assessment conforms with ISO 27001:2005, BS7799 / CNS 17799, the vulnerability evaluator includes CVSS(Common Vulnerability Scoring System).

- **Reinforced Vulnerability Scan Engine:** High stability and accuracy using following unique technologies:

  VH（Virtual Hacker）digging

  FPP（False Positives Prevention）

  AIT（Artificial intelligence Technology）scan

  PSF（Protocol Signature Filter）

  HVS（Hardware Vulnerable Scanning）

  RTS（Real Time Scanning）message

  DS（Dictionary Search）for password solving

- **Graphical User Interface (GUI) :** IT personnel will get hands-on experience in short period of time, and be able to execute basic vulnerability audit, shortening the time spent to meet required regulatory compliance.

- **Automated procedure,** to ease pressure on IT personnel:
  Auto Update – Automatically acquire any new modular program and vulnerability database update announced by DragonSoft.
  Auto Scan – Administrator can set up to 50 scheduled scans with different policies.

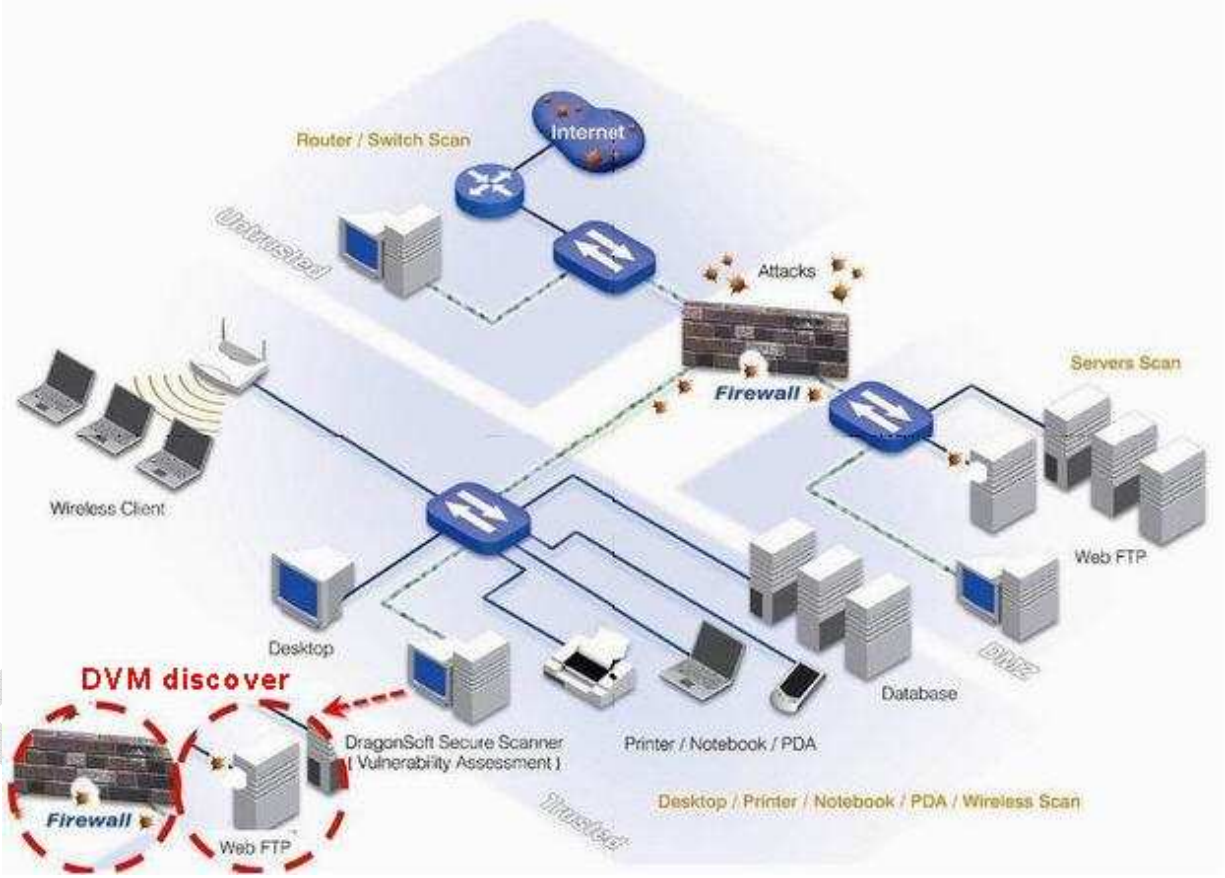
Auto Save - Automatically save information – built in ODBC database, customizable.

Auto Send - Automatically email result to designated email box after scheduled Scan.

Case Example

DragonSoft Vulnerability Management has intuitive humane interface, highly flexible policy and fast deployment characteristics, it enables immediate tracking and remediation status of vulnerability in important locations. The following illustrate is a deployment of a Bank using DragonSoft Vulnerability Management:

Diagram 1、Deployment for VA Networks



Three corporate network deployment location suggestions are summarized from above network model:

1. **Internet –** Continuous following the security policy and check for new vulnerability

externally, the information is logged and kept in database. It works with IPS and IDS to match those attacked IP addresses in the database, extensively decrease the chances of IPS/IDS misjudge from external attacks.

2. **Intranet –** Continuous internal security audit to ensure the significant servers and newly added equipment and applications in most secured state. A single primary console and integrated database carry out internal vulnerability analysis and remediation.

3. **DMZ zone –** Scan vulnerability tolerance and intermediate prevention device on close-by hosts, it reviews vulnerability on service host and tells if the intermediate prevention device is easy to breach, and to provide necessary remediation.

DVM- FAQ

★How many versions are there for DVM ?

DVM comes in FOUR versions:

- DragonSoft Vulnerability Management – CENTER Edition
- DragonSoft Vulnerability Management – PLATINUM Edition
- DragonSoft Vulnerability Management – ENTERPRISE Edition
- DragonSoft Vulnerability Management – PROFESSIONAL Edition

Detail specification can be found at DragonSoft's official web site:
http://www.dragonsoft.com/en/product/overview

Is there a trial DVM version to download ?

Yes, we supply 30-day English trial version at DragonSoft official web site:

. DVM Platinum (Unlimited) - English Version
http://www.dragonsoft.com/en/trial/DVM_4115.exe

. DVM Enterprise (256 Hosts)- English Version
http://www.dragonsoft.com/en/trial/DVM_ENT.exe

. DVM Professional (128 Hosts)- English Version
http://www.dragonsoft.com/en/trial/DVM_PRO.exe

Is there any other way to learn about DVM except the user manual ?

DragonSoft provides training courses for DVM. You can apply through agents or resellers, or through official web site at : http://www.dragonsoft.com.tw/certification/ , or send email to service@dragonsoft.com

On what OS can DVM be installed ? What OS and equipment can it perform scans ?

DVM can be installed on:
Microsoft Windows
9x/NT/2000/XP/2003.

DVM scan ssystem:
Windows base, UNIX base, SUN OS Solaris, Web Server, Mail Server, FTP Server.

DVM scans network equipment include Router, Switch, Firewall…to help easily identify the system vulnerability.

DVM scans following services:

HTTP、FTP、POP、SMTP、IMAP、LDAP、NNTP、NetBIOS、DNS、SSH、SNMP…

Can I install DVM again if other version has been installed before?

No, please uninstall the old version before install the new one, or it may cause both versions no working.

Please Note：

DVM is limited to once-off installation, please do not install in any other machine, it can cause DVM lock automatically. (Unlock application from manufacturer will be active after three working days)

Can I switch the installation to another machine ?

Yes, please contact your agent/reseller, to apply for unlock from the manufacturer.

Is there any limitation if I reinstall DVM in the same host machine?

No, you can install freely, but remember to update DVM module and vulnerability database after installation to keep your network in best protected state.

Why showing product key expiry when I reinstall DVM ?

DVM is designed to one installation on one machine, if your server is already DVM-installed, the reinstallation on other machine will cause auto lock and become unable to operate. Kindly approach your service agent to obtain DVM unlock from the manufacturer (will be installable after 3 working days).

Please Note：

There will be locking if DVM is removed on original server or reinstalled/repeat install on new server for the same customer.

Is DVM unusable after expiry date ?

The main program is usable after DVM expires, except for the auto update and vulnerability database services. Please contact your supplier if you still wish to continue using the service, there will be a temporary extension for DVM vulnerability assessment function and network protections during the application period and the system can be kept in the best state.

How do users renew license once the product service expires ?

DragonSoft follows the principle of helping customers' emergency matters. In case of expired license, please purchase the renewal service through your local agent/resellers, or send email to manufacturer's customer service department: service@dragonsoft.com

How to get vulnerability bulletin from DragonSoft ?

Please subscribe with your email at DragonSoft official web site - http://www.dragonsoft.com.tw/epaper/

Is the renew cost the same on the expiry notice letter ?

The cost on expiry notice letter is the market list price, please contact your agent/resellers, a sales representative will approach you for quotation.

How to seek guidance whenever I encounter problems ?

DragonSoft provides post-sales service as follows:

Emails: Customer service： service@dragonsoft.com

Suggestion : webmaster@dragonsoft.com

Does DVM support multi-scan ?

Yes, it supports up to 50 scheduled audit scans in DVM Platinum Edition,.

How to evaluate network vulnerability assessments ?

Convenience	Report
● Installing, handling and operating grade ● Manual security policy grade ● Auto update, scheduled scan functions ● Customized policy flexibility ● Target scanning flexibility	● Degree of report classification and customization ● Easy to read or not ● Readability of items and vulnerability ● Degree of information abundance ● Easy to export or not
Efficiency	**Vulnerability Database**
● Time consumed per scan port ● Vulnerability numbers and time consumed ● Accuracy to identify network service & OS ● Reliability of vulnerability assessment ● Bandwidth usage by network ● Comparison ability from multi-scan result ● Ability to identify degree of risk value ● Scan result to show how safe is user's network environment	● Frequency of database update ● Speed of newly added vulnerability ● Clarity and patch integrity of vulnerability ● Vulnerability identity by international security organization ● Compatibility with other security codes

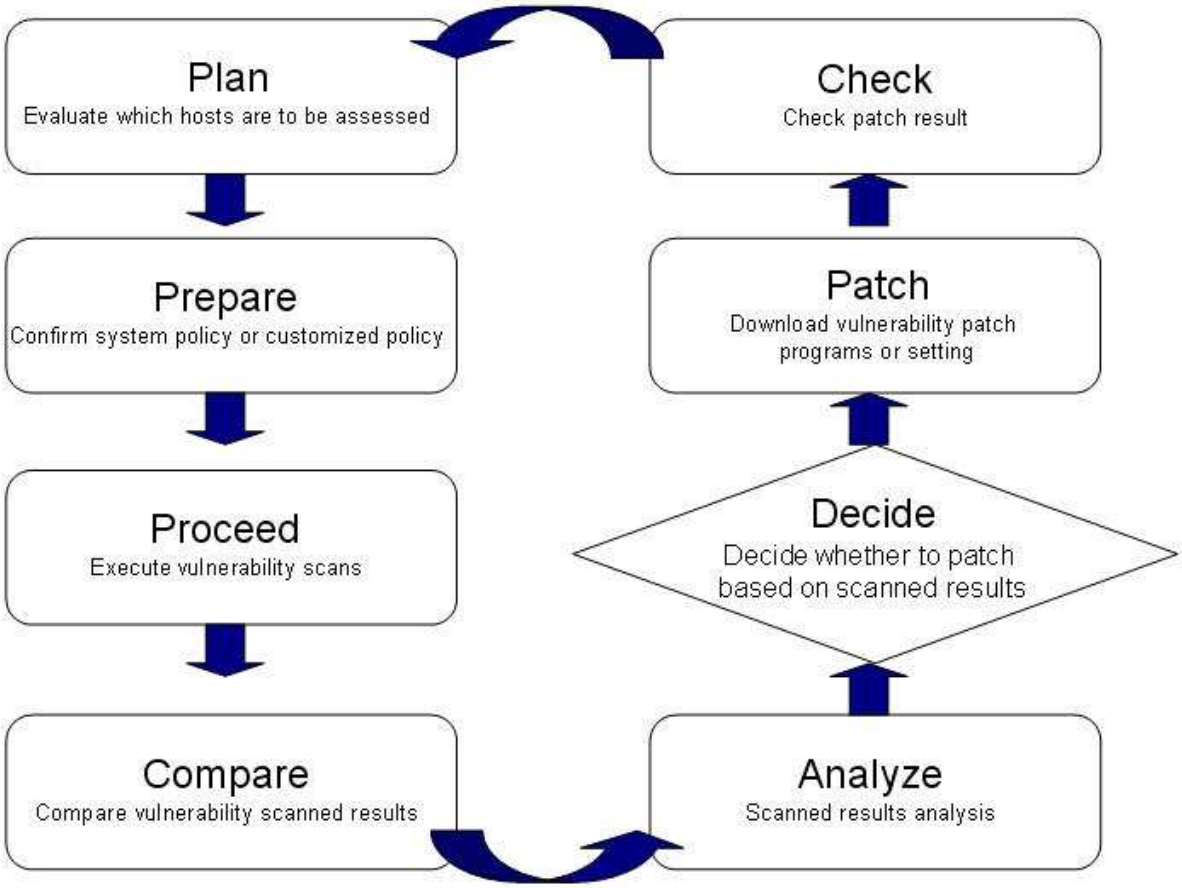
How does DVM patch the vulnerability on the host ?

DVM evaluates the security risk of corporate vulnerability and yields report, in which solutions are provided for all vulnerability. Each information personnel can fix with his professionalism and actual situation.

Does DVM support security scan on wireless network ?

DVM is a network vulnerability assessment system. It can perform network equipment audit and protection as long as it is connected with wired or wireless network, and analyze the vulnerability on scanned equipments.

How does DVM network vulnerability assessment system operate ?



1. PLAN on which host needs scanning:
   - First plan for host numbers you wish to purchase, and your scan range.
   - Scan the IPs you can designate, name or range to scan.
   - The scan operation is cross-platform, it identifies the OS in the environment. (such as Windows, Unix ……)

2. PREPARE customized policy or default policy in the system:
   - Identify if the policy used is system default
   - Identify if default policy should be amended
   - Identify whether to add customized policy or not

3. PROCEED with vulnerability scan execution:
   - Produce report including OS scan, audit items, remediation, and provide real time recovery for registry.
   - Graphical analysis + risk level = an easy to understand and readable security report.

4. ANALYZE the vulnerability scan result.
   - Evaluate statistics such as OS scan, audit items, remediation and real time recovery for registry.

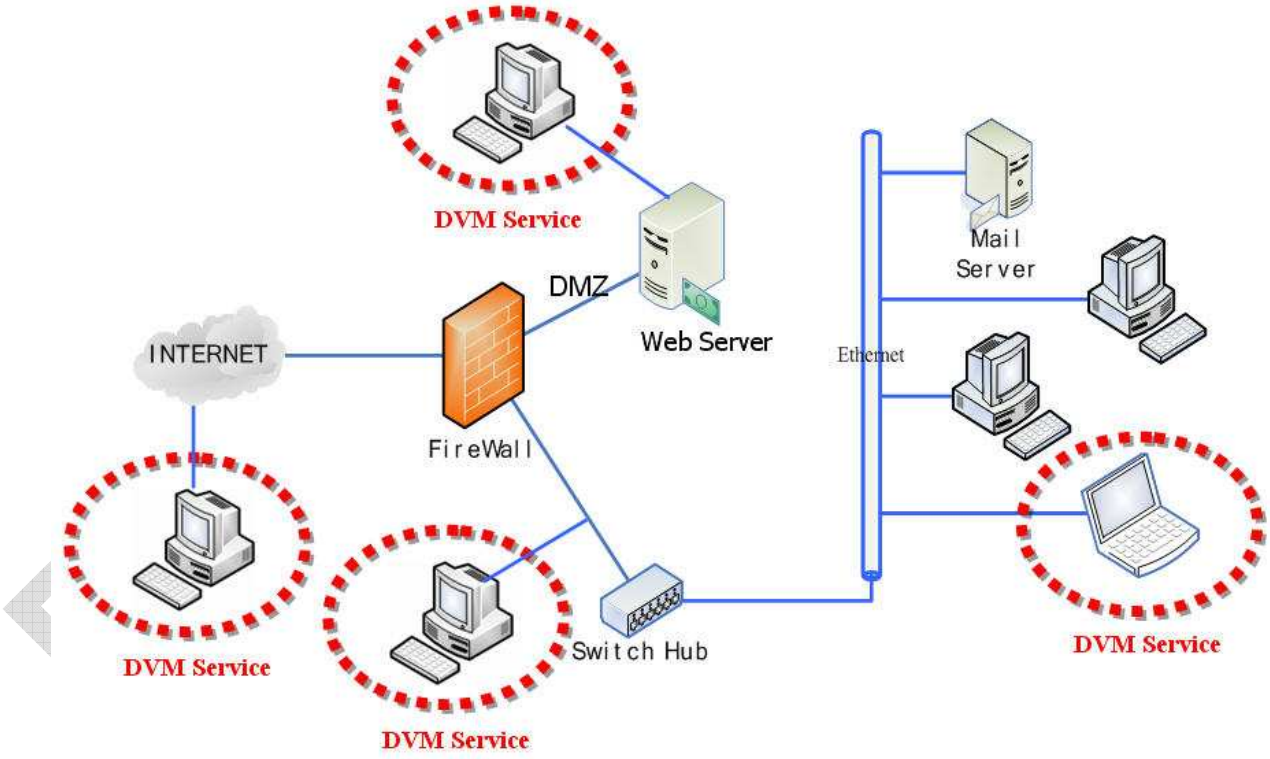
5. DECIDE whether to patch or not based on scanned results:
   - Identify the priority remedy item and important host list to monitor base on environment and company regulation.
   - Make decision on vulnerability patches.

6. PATCH the vulnerability and perform security rectification:
   - Proceed with patch download update or service setting adjustment to the vulnerability found on the report.

7. CHECK on vulnerability scan
   - Do all patches complete ?
   - Repeat step 1 to 7 until the remediation is complete.

Where can DVM be installed in the company ?

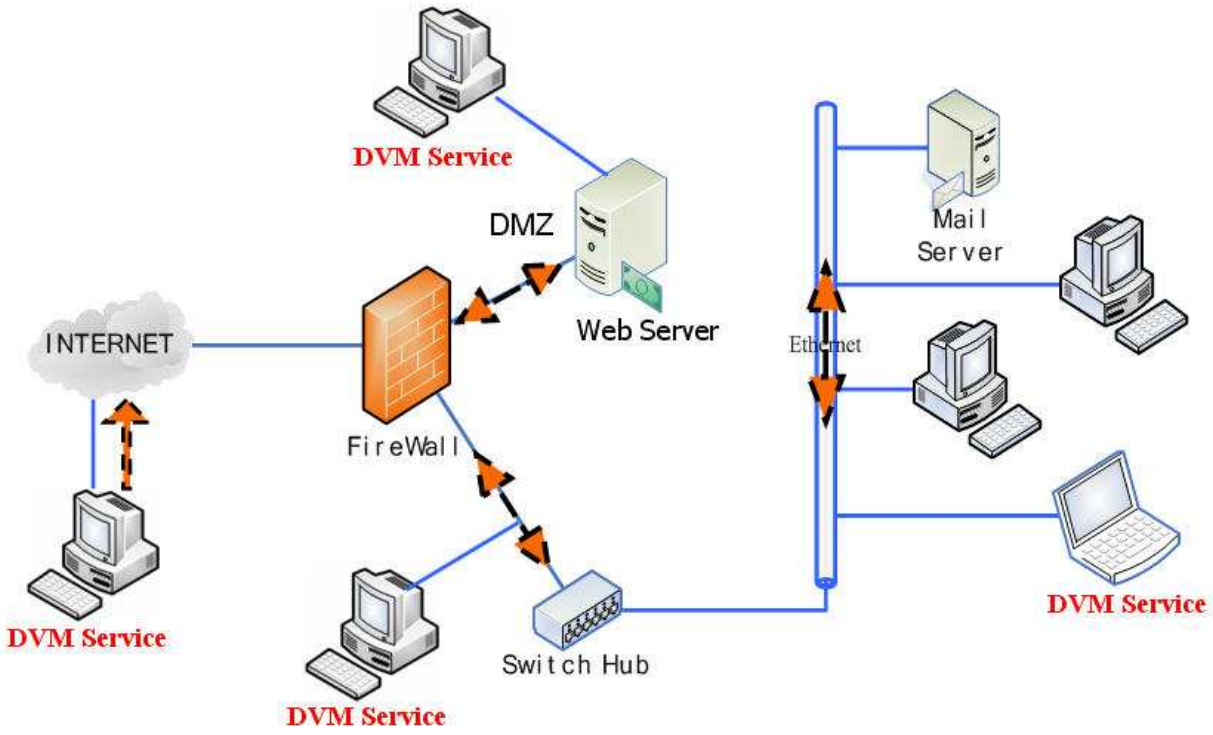
It can be installed at 4 locations mentioned below, the different results tell information on network security protection and identify the defense strength within the corporate. MIS / IT personnel can be more clear to plan for solutions.



1. Install on remote host to imitate hacker's scanning attack mode.
2. Install on front-end of firewall to scan, the result will show if your firewall, IDS, IPS or system strength are vulnerable to the attackers.
3. Install on DMZ zone (non-military zone) to scan.
4. Install on back-end of firewall to scan internal network.

Can DVM scan on internet hosts across different domains ?

DVM is able to scan on internet hosts because it surpasses Gateway to reach internet hosts outside its domain.



The predetermined condition is that the scanning host account must gain adequate authority by scanned host in order to produce most complete and accurate result.

Do I have to stand-by while DVM is scanning ?

No, it is unnecessary. DVM activates automatic scheduling with timing according to user's need. The user can set the email function to send to relevant personnel once the scans are complete.

Does the personal firewall activation limit the vulnerability scan ?

If the firewall is activated, the result will reveal if the firewall setting reach expected goal. If the firewall is deactivated, one can tell exactly how many vulnerability are un-remedied. The two purposes are different.

When executing force scan, are all the communication ports being targeted under all audit policies ?

DVM performs prioritized intelligent scan on default communication ports. Users can also set communication ports or customize audit policy based on one's network requirement.

How to use DVM to find out which communication ports are open in corporate environment and to prevent the openness of unauthorized communication ports ?

User can select〔Port Scan〕policy to scan, the result will show how many unauthorized communication ports are being opened in the corporate environment.

Does the Password Check provide commonly used password file ?

Yes, the FTP / HTTP / POP3 / IMAP…use built-in password file in DIC index under installation index. You can add files by your demand and rules to facilitate the password scan. DVM provides built-in account dictionary and password dictionary. The stored location will be different if the version used is different.

How to compile risk spread chart on different scan results ?

You can use DragonSoft Vulnerability Management database to customize search condition of high risk vulnerability audit reports.

What action to take to conclude DVM scan ?

The protection will be completed after following steps:

1. Proceed with remediation based on audit result.
2. Re-scan to make sure system remediation is complete, to reinforce information security mechanism.
3. Set scan schedule to complete information security mechanism.

The DVM scans on Switch showing openness of unauthorized port 110 ? why ?

Port 110 is a POP3 (Post Office Protocol - Version 3) service, please confirm if you have anti-virus software (email scanning) service.

Do the found vulnerability must be fixed ? Does DragonSoft provide remediation service ?

There are solutions in vulnerability descriptions, we categorize as following:

- Auto fix：One can patch on registry directly with administrator authority.
- Patch setting：Change system or service setting based on patch description.
- Download patch：Download patch files based on patch description.

- Patch suggestion：Users identify installed version and obtain patch support from his service agent or product source.

Contact DragonSoft for more paying services.

Can I use other information security product with DVM ?

Yes, DVM can work jointly with〔Firewall〕,〔IDS〕or other anti-virus programs to reinforce information security mechanism on corporate network environment.

Only detect Port 21 when XP SP2 firewall is open

The firewall activation will affect scan result, it is suggested to deactivate firewall on the installed DVM host before scanning.

Does DVM provide import of scan result to database and multi-scheduling ?

DVM provides import of scan result to database such as MS-SQL…., as well as multi-scheduling.

Can I set own number of ranking on the default top 6 most vulnerable list ?

It is tested and proven by DragonSoft R&D that top 6 list is most readable and convenient report, therefore the maximum value is 6. It will show all if the scanned host is less than 6. User cannot set one's own number of ranking.

Can I convert the DVM report from HTML to PDF file ?

You can convert to PDF file using PDF creator or graphic creator software.

Can I export the high risk vulnerability report only ?

Yes, you can customize search condition to high risk vulnerability audit report in DVM database.

Does the update notice letter only do updates on vulnerability database but not on the policy ?

The DVM auto update function updates vulnerability database, audit module and new policies automatically. It will not update policies already exist in main program if you choose manual update or online update on vulnerability database.

Does update on vulnerability database add more audit items ?

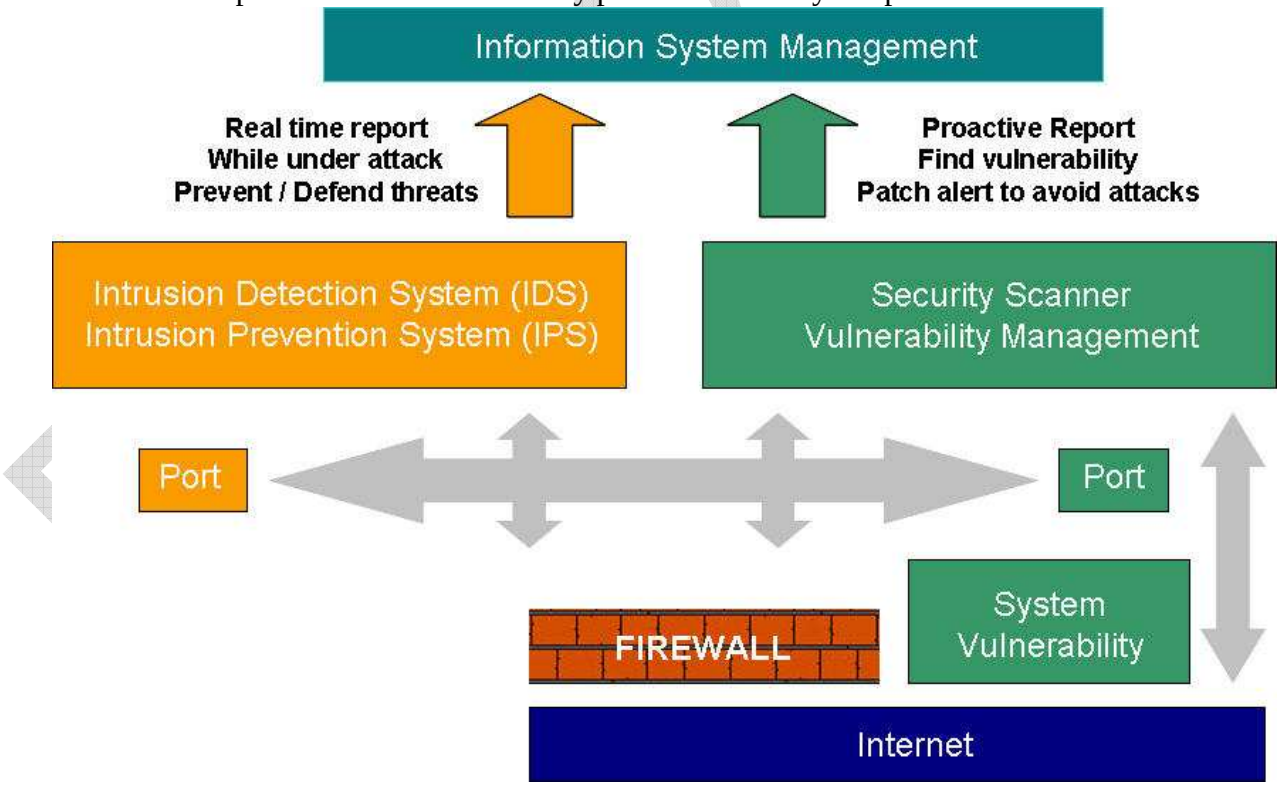
Yes, the audit database adds latest vulnerability items whenever the product updates more vulnerability items.

Is there limited period for vulnerability database and scan modules ?

The product support is one year when you purchase DVM related products, the service period is negotiable with the reseller. You can start using the main program and vulnerability database update service within the service period. We will contact the customer to help in case of registration abnormity. Customers can call the customer hotline to talk to product service personnel whenever there is a usage problem.

What is the difference between DVM and IDS ?

The difference is that DVM will check for existing vulnerability proactively, so the information security personnel can download patch or execute security measures, it is an aggressive protection. Whereas IDS is real time monitor system, it detects intrusions whenever it happens, it is a passive protection. Take fire emergency for example, IDS acts as fire alarm, it triggers when there is smoking indoor, and activate water spread system, fire alarm etc. The DVM is a fire security expert who checks the pipelines and equipment, spot the potentially dangerous hazards and report to information security personnel to carry out patch and remediation.

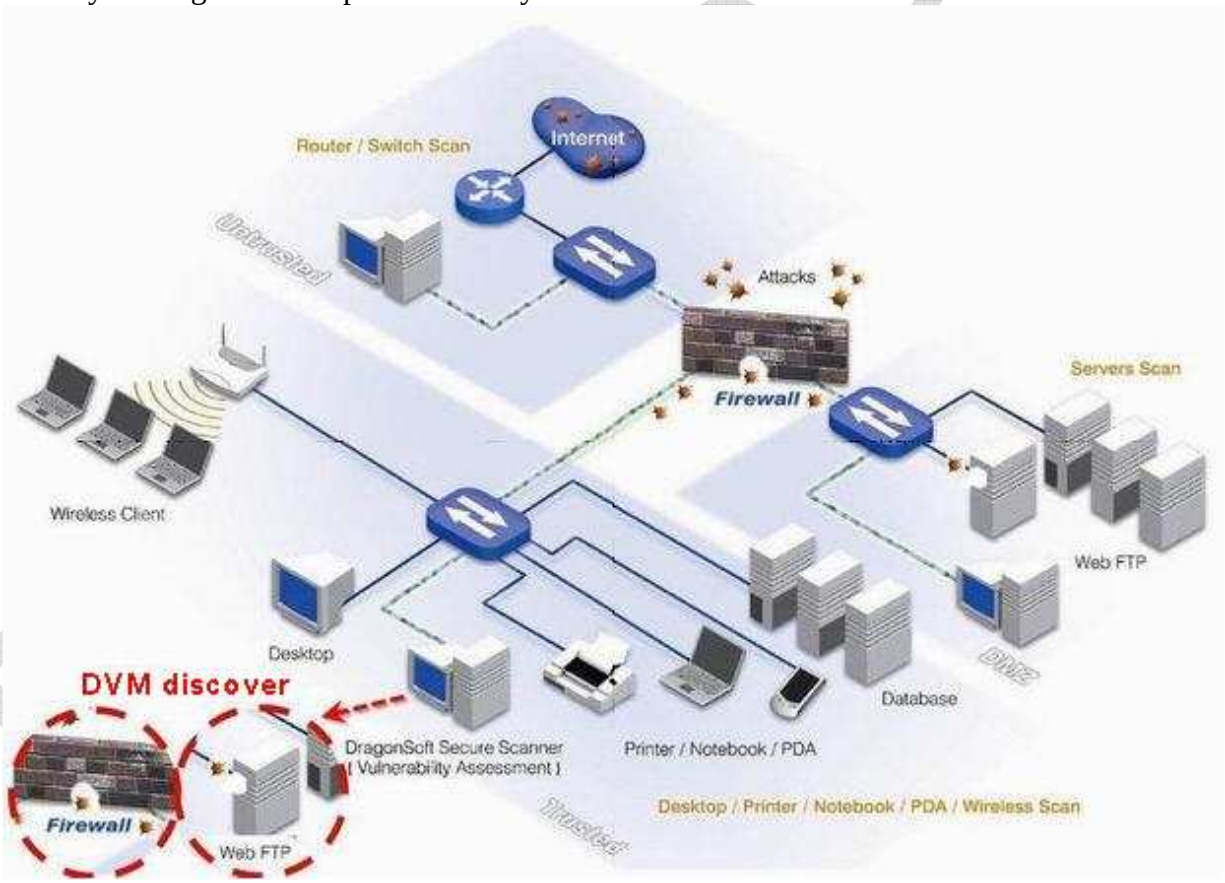


Is vulnerability assessment system that important in information security ?

Vulnerability scan is most fundamental and important one in the information security management. All network equipment can be intruded and attacked any time. Therefore it is a key to know and forecast the vulnerability to corporate security. The vulnerability assessment system can detect vulnerability whereabouts, list the unsecured, and provide appropriate patch suggestions to administrators like a security consultant. To prevent the un-prevented and immensely reduce the losses caused by network risk.

The company is using firewall as information security protection, is there need to use network vulnerability assessment to reinforce the information security mechanism ?

A few reasons to use network vulnerability assessment system:
Most hackers possess ability to penetrate firewall restrictions, and 70%~80% of the hackers, computer viruses, worms come from corporate internal network, which put the information security in danger and not protect-able by firewalls.



Reinstall DVM on new computer finds manual or auto update un-connectable to Update Server

The main program can be outdated, keep installing several times to find successful installation. Or the customer service engineer will verify the “main program and vulnerability database” version with customer and provide solution.

1. Download the latest exe. file from official website if main program is outdated.
2. Make sure if MAC address is locked by system.
3. Confirm login authority if main program is not the latest version.
4. Confirm link capability to internet (with firewall/proxy or not) if main program is not the latest version.

Is report analysis service available after customer scan result ?

This is a payable service provided by DragonSoft Security Associates Inc.

Is there any other format except HTML for the report ?

DragonSoft R&D concluded that HTML is the most commonly used format because it handles information linkage or print job with ease.

The HTML is editable if the users prefer word processing software, it is easy and convenient to use after editing, that is why DVM uses HTML as default report format.

DVM is expired and unable to update

Once DVM expires, the update service of main program and vulnerability database will cease. Please renew the service to keep DVM service in functional state.