Automated Vulnerability Detection System

Key Features

- Scans servers, routers, firewalls, switches, phones, operating systems–anything that speaks IP
- No software or agents to install or maintain
- Flexible scan frequency: scheduled or on-demand
- Differential reports–quickly spot new vulnerabilities, changes from security baseline and track remediation efforts over time
- Automatic daily vulnerability database updates–stay ahead of the latest threats
- 24/7 unlimited phone support with access to the Beyond Security network of security experts

"We now have the ability to scan at any time. Regular vulnerability assessments scans are like having sonar on our own network. We always know what is going on around us."
–Mike Gutknecht
Network Engineer
Rayovac Corporation

AVDS (Automated Vulnerability Detection System) is a network vulnerability assessment appliance. AVDS locates and exposes security breaches and vulnerabilities and lists their exact location and description along with suggested solutions.

With each scan, AVDS will automatically find new equipment and services and add them to the inspection schedule. It then tests every active node based on its characteristics and records responses creating a network security baseline.

AVDS is able to scan all IPs automatically, or schedule tests for specific IP addresses or segments at specific times. Each scan includes the widest range of security tests available today.

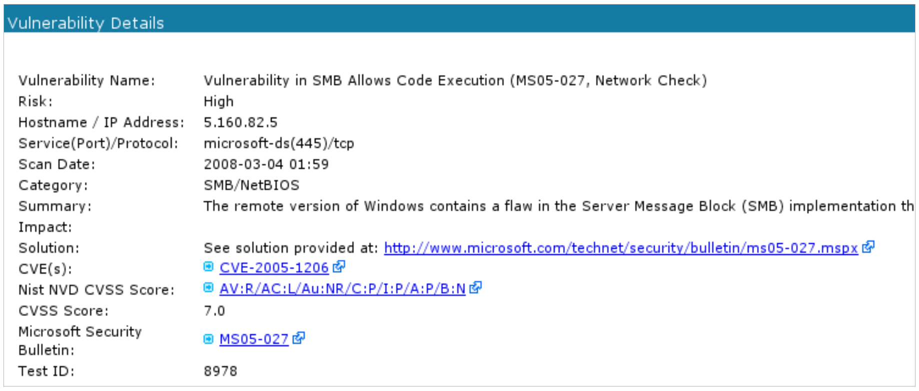
Security Appliance

The AVDS Scanner is a 19” 1U rack mount appliance. The dedicated appliance design provides fast scanning and allows the security administrator to focus on performing vulnerability assessments quickly and directly, without the worry of administering an operating system or a disparate suite of tools.

- Easy setup–up and running in about an hour
- Self-contained appliance–no integration with your existing hardware required
- No software or agents to install
- Appliance OS is hardened against attack

Focused Reporting

AVDS standard reports provide a comprehensive analysis of all vulnerabilities found grouped by risk severity. Every detected vulnerability contains technical information specific to that risk, including a short summary, severity, possible impact, recommended solution and relevant information such as links to software vendor patches. An Executive Summary section includes an overall summary for quick assessment of discovered risks.



Vulnerability Details

Vulnerability Name:	Vulnerability in SMB Allows Code Execution (MS05-027, Network Check)
Risk:	High
Hostname / IP Address:	5.160.82.5
Service(Port)/Protocol:	microsoft-ds(445)/tcp
Scan Date:	2008-03-04 01:59
Category:	SMB/NetBIOS
Summary:	The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation th
Impact:	
Solution:	See solution provided at: http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx
CVE(s):	CVE-2005-1206
Nist NVD CVSS Score:	AV:R/AC:L/Au:NR/C:P/I:P/A:P/B:N
CVSS Score:	7.0
Microsoft Security Bulletin:	MS05-027
Test ID:	8978

Web Site Security Audits?

AVDS performs internal and external scanning of networks consisting of any number of servers, services, ports or IP addresses.

For security scanning targeted at web sites, web servers, shopping carts and all Internet-facing IP addresses, scans can be done by our hosted AVDS servers and the results combined with local internal scan results for a comprehensive vulnerability report.

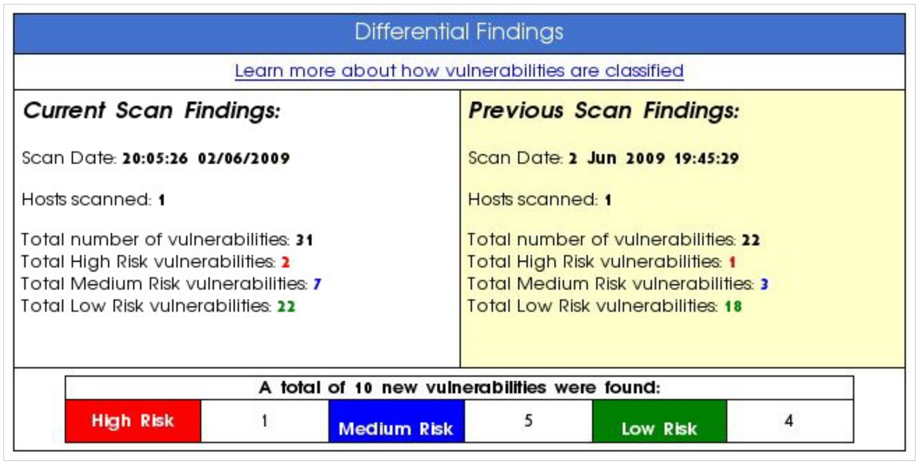
Managed Service Providers

Easily integrate AVDS with your existing infrastructure. Installed in a Security Operating Center (SOC), ASP farm, co-location or as an outsourced service, AVDS can become a part of your service offering quickly and with minimal capital outlay.

> *"AVDS graphically, unobtrusively and with great detail demonstrated to me the situation of our network/firewall and web server after scanning our system with a huge range of tests. Reports were sent to me that were concise and clear and then the technical staff of Beyond Security talked me through the results of the scans, interpreting areas with which I was unfamiliar and suggesting simple and precise fixes. From the moment of my first contact with Beyond Security, I have been impressed and enjoyed their friendliness, clear talking, approach to confidentiality and technical knowledge."*
>
> –Paul Sheriff
> IT Manager
> City of Geraldton

Differential Reports

Differential reports show changes from the previous scan. New vulnerabilities, open ports, running services or new/removed hosts are listed, as well as a summary of any problems resolved since the last scan. Differential reports are a valuable tool to monitor changes to the security baseline and track remediation efforts over time.



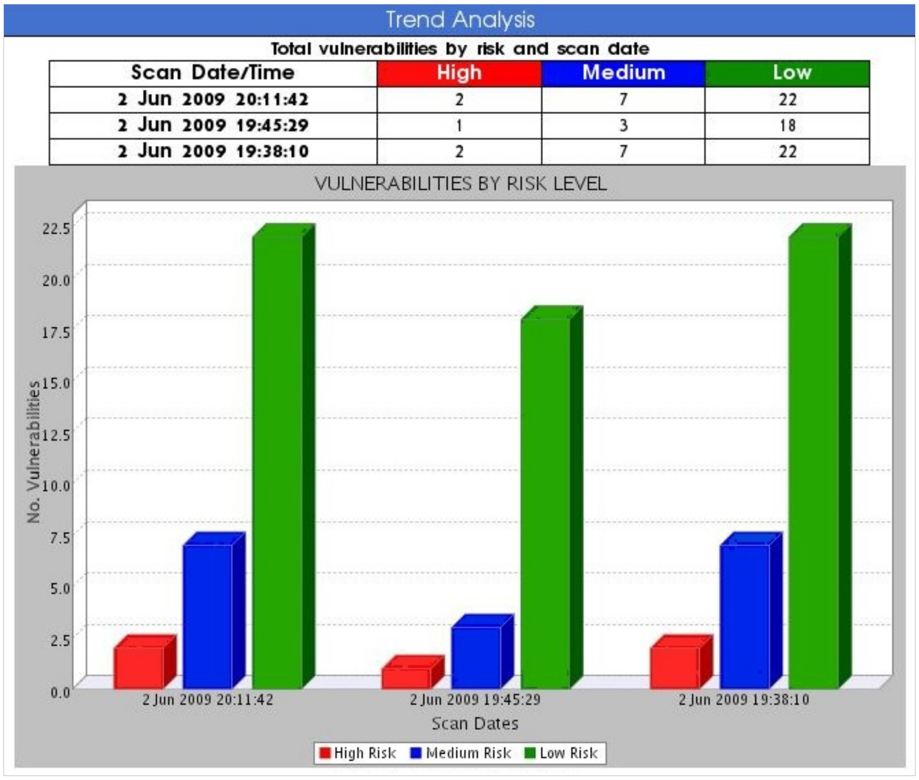
Differential Findings

Learn more about how vulnerabilities are classified

Current Scan Findings:	Previous Scan Findings:
Scan Date: 20:05:26 02/06/2009	Scan Date: 2 Jun 2009 19:45:29
Hosts scanned: 1	Hosts scanned: 1
Total number of vulnerabilities: 31 Total High Risk vulnerabilities: 2 Total Medium Risk vulnerabilities: 7 Total Low Risk vulnerabilities: 22	Total number of vulnerabilities: 22 Total High Risk vulnerabilities: 1 Total Medium Risk vulnerabilities: 3 Total Low Risk vulnerabilities: 18

A total of 10 new vulnerabilities were found:

High Risk	1	Medium Risk	5	Low Risk	4



Trend Analysis

Total vulnerabilities by risk and scan date

Scan Date/Time	High	Medium	Low
2 Jun 2009 20:11:42	2	7	22
2 Jun 2009 19:45:29	1	3	18
2 Jun 2009 19:38:10	2	7	22

Distributed Architecture for Large Networks

For large networks (from 2,000 to 2 million nodes), AVDS employs a distributed scanning architecture to effectively scan and manage vulnerability assessment and tracking from a single administration console. Multiple AVDS appliances on separate networks can connect to a centralized management system for distributed scanning and consolidated report collection.

New Vulnerabilities

With an average of 310 new operating system and application vulnerabilities announced each and every month regular active network scanning is essential. An automated, ongoing vulnerability assessment and management solution is your best option for the assessment and management of corporate network vulnerabilities.

"The information provided in the reports is very clear and concise. It explains to engineers what the problem is, where to look for more information, and how to fix it. "With these reports we can be sure after every change to the network if we are making the right change in terms of our security requirements.

"We tried the free services. But when we piloted AVDS, we saw zero false positives and the differential reports make Management Reporting easy. These features are huge. They allow us to focus on delivering ICT services instead of chasing down vulnerabilities."
–Cody Phang
Head of IT for the Australian Government National Capital Authority (NCA)

Vulnerability Checks

Scans	Sample Checks
Web Applications	Apache, Microsoft IIS®, Oracle WebLogic®, IBM WebSphere®, Adobe ColdFusion®, shopping carts
Databases	Oracle®, MySQL, Microsoft SQL Server®, Lotus Notes®, DB2®
Network Systems	Routers, Firewalls, Switches/Hubs, Remote Access Servers, Wireless Access Points, IPSec, PPTP, DHCP, DNS, LDAP, SNMP, VPNs, FTP, SSH, TELNET, Modems, Anti-Virus Systems
Operating Systems	Microsoft Windows NT, 2000, Server 2003 and 2008, XP, Vista®, Windows 7®, Solaris®, AIX®, HP-UX®, SCO Unixware®, BSD (OpenBSD, NetBSD), Linux, AS/400®, VMS®, Mac OS X®, Novell NDS
Languages	SQL, ASP, PHP, CGI, JavaScript, PERL, Ruby, .NET
OSI Layer 7 Apps	Web server, Database server, Mail server, FTP server, Proxy server

Features

- Scans unlimited IP ranges to identify active IPs
- Quick Scan feature provides ad-hoc scans within seconds on individual nodes or network segments
- Schedule automatic daily/weekly/monthly scans
- Differential reporting highlights and automatically tests newly added IPs, ports and services
- Powerful search engine–quickly filter and search reported vulnerabilities
- Distributed scanning architecture for large networks and multiple AVDS appliances with enterprise-wide scans and consolidated reports
- Scan Profiles can check large networks quickly for a small subset of problems
- Non-intrusive and consumes minimal bandwidth. Scan rate can be limited by administrator to control bandwidth requirements
- Web browser administrative interface
- Scales to 2 million active IPs
- Automated daily updates of threat database
- Vulnerability database supplied by SecuriTeam Portal (www.securiteam.com), a industry respected security clearinghouse with over 2 million visits annually and 8,500 online articles
- 24/7 unlimited phone support with access to Beyond Security experts

Penetration Testing Replacement

Many organizations are required to perform periodic penetration testing on their networks and web sites. These tests are intrusive and costly. Further, with the rapid rate new vulnerabilities are discovered, exploited and made available to the hacker community at large, penetration test results can be rendered out of date as soon as they are complete. AVDS provides results equivalent to most penetration testing procedures, on demand and at a fraction of the cost.

Request a Free Evaluation

Our free 30-day evaluation includes an AVDS appliance and unlimited testing of up to 2,500 IP addresses.

"We needed a way to discover and audit network assets, understand and prioritize current network vulnerabilities, then track and manage the remediation efforts over time. After a three month review of nearly ten different vulnerability scanning vendors we chose Beyond Security's AVDS. We had specifically selected AVDS because it would cause no disruption to our systems and required no installation of any new software on our systems."
–Gary Anton
VP of Strategic Sourcing and IT
Illinois Tool Works (ITW)

Contact Us

For more information, visit
www.beyondsecurity.com
or call us at
+61 401 778 124

For pricing details, contact us at
steveh@beyondsecurity.com

Scanning Performance

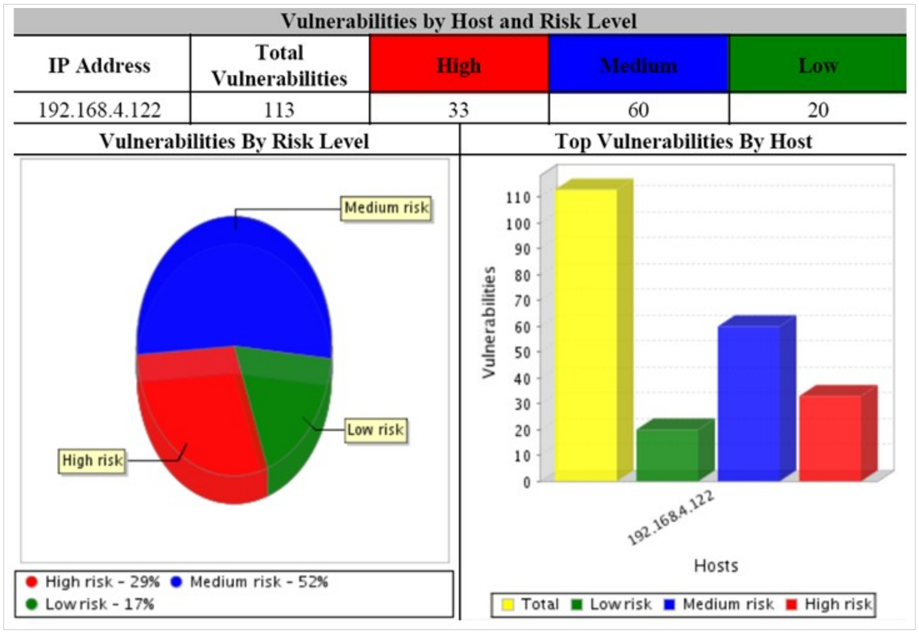
	Default	Min	Max
Rate of Scan (Packets/Second)	300	35	1200
Number of Sessions per Scan	8	2	32
Throughput per Scan (Kilobits / Second)	60	6	240
Average Scanning Time	Scans a typical Class C network in ~12 minutes		

Appliance Hardware Specifications

Form Factor	1U 19” Rack Mount (with Dell Rapid/Versa Rails) or Mini Tower
Processor	Dual Core Xeon E3110
RAM	2GB DDR2, 800MHZ, 2X1G
Hard Disk	250GB, 7.2K RPM, SATA, 3Gbps, 3.5-in
NIC	2 Gigabit Ethernet ports
OS	Linux (hardened)

Requirements

- IE 6.0 or later, Mozilla Firefox 1.5 or later (for administrative console)
- IP address on your internal network



Vulnerabilities by Host and Risk Level

IP Address	Total Vulnerabilities	High	Medium	Low
192.168.4.122	113	33	60	20