VULNERABILITY ASSESSMENT WHITEPAPER

Automating Vulnerability Assessment

This paper describes how enterprises can more effectively assess and manage network vulnerabilities and reduce costs related to meeting regulatory requirements.

Automated Vulnerability Assessment / Vulnerability Management (VA/VM) solutions are supplementing and in some cases replacing manual penetration testing with an overall improvement in network security without increasing costs.

New advances have eliminated the high management overhead and false positive rate issues that plagued open source and early market VA/VM entries.

This whitepaper discusses:

- Speed of change in networks, equipment and applications plus the speed of exploit deployment is revealing weakness in corporate policies specifying relatively infrequent manual penetration testing.
- Perimeter defences (anti-virus, firewall and IPS/IDS) are vital, but can be bypassed by determined effort to reach and exploit known vulnerabilities that reside just inside the fence.
- The introduction of an automated network scanning mechanism and consolidated reporting to identify and track mitigation of known vulnerabilities is establishing a higher overall security level often using already existing budget and manpower.

Table of Contents

Introduction

A new approach is emerging for detecting and managing vulnerabilities in complex networks. The security provided by annual or quarterly manual vulnerability assessments can now be substantially improved. At the same time vulnerability assessment and management overhead can be reduced and better risk management and vulnerability control can be accomplished.

Today's business network infrastructure is rapidly changing with new servers, services, connections, and ports added often, sometimes daily, and with a non-stop inflow of laptops, storage media and wireless devices. With the growing number of vulnerabilities and exploits associated with the continual evolution of IT infrastructure, organisations now require more frequent vulnerability assessments. These assessments must naturally be performed with the latest of vulnerability knowledge and expertise. Thus security expenses have been rising when overall budgets have not.

The typical perimeter defence mechanisms that inspect traffic such as antivirus, firewalls, and IPS/IDS are now commonplace and even the average hacker or bot assumes their presence and is continuously re-engineering their attacks to avoid them. To compensate, network security administrators with valuable assets or having high visibility (including many small businesses and local government entities) are now adopting the VA/VM tools that have long been used only by the largest corporations and governments.

With these factors in mind, the automation of the VA/VM process to reduce the effort required for each test and to increase the frequency of tests has become a cost effective way of managing the increasingly complex problems of keeping a network secure.

As with the decision to automate any business function, it must be based on whether or not an automated solution can perform the job in a more efficient, effective and hopefully faster way than by manual means. When examining vulnerability scanning as an automated service, three important factors must be taken into consideration.

1. The ability of the solution to provide accurate and complete vulnerability assessment
2. Analysis and representation of assessment data as meaningful information
3. Tracking and reporting the effectiveness of mitigation efforts.

We will now examine by what means these factors relate to how vulnerability assessments are currently performed and then discuss evolving roles for vulnerability assessments in an automated process paradigm.

The Challenges of Network Security Assessments

Network vulnerability assessments (manual or automated) are widely recognized as a crucial component of network security and are a key component of any security plan. Vulnerability assessments are performed to determine the actual security posture of a network environment. They are designed to explore whether or not an attack which bypasses or overcomes the perimeter defences (antivirus, firewall or IPS/IDS) will find an exploitable element residing within the network that could be used to affect the confidentiality, availability or integrity of information.

Nearly all data loss events resulting from outside attack, and most losses to insider attack, consist of the exploit of a known, but unhandled vulnerability. By 'known' we mean that it had been documented in security literature and solutions are available. In 2009 every one of the 70 largest security breaches (resulting in the total loss of 275 million records) were accomplished via the manipulation of a known vulnerability. As a matter of fact every one of the vulnerabilities used in these 70 breaches had been known about for over a year.

Every one of these 70 breaches – and in fact nearly all reported security breaches – were accomplished in spite of the presence of reasonably diligent staff, current antivirus, correctly installed firewalls and IPS/IDS that was correctly configured.

This is the challenge. And current best practice indicates that it is best answered by performing regular vulnerability assessments to identify the known vulnerabilities in a network before hackers find them.

Protection of the Organisation’s Assets

IT departments today find themselves in the unenviable position of managing increasingly complex network environments.

Enterprise infrastructures today consist of multiple device types, operating systems, and applications that have a diverse range of security and access requirements. Hence enterprises have had to rely on fragmented multivendor solutions to provide everything from intrusion prevention, access control to patch management. Such a strategy involves deploying and supporting an array of independent security products and services.

This inevitably leads to manual vulnerability assessment being a complicated, time consuming and costly exercise, making it a major drain on IT productivity, especially given today’s threat environment in which malicious code is being developed faster than ever before.

VA/VM solutions themselves often require skilled and dedicated attention to ensure that scans are complete and to then sort through the 'false positives'.

With such a significant investment required by an organisation to do each assessment, available resources may not allow a reasonable frequency of testing. This can leave the organisation unprotected but since occasional testing meets policy and regulatory requirements, this lack of resourcing is ignored.

The Organisation’s Security Team

In a heterogeneous environment, any manual assessment requires a security team that has current, broad and deep technical expertise in a myriad of technologies. Which leads to the question: What kind of in-house staffing or what consulting skills are required to perform a complete vulnerability assessment?

In brief, an assessment simulates the capabilities of knowledgeable attackers. Simulating these capabilities manually requires specialised knowledge and tools, both of which tend to be sparse and expensive. There are not that many Certified Information Systems Security Professionals (CISSPs) worldwide, and not all of these are qualified to perform a network security and vulnerability assessment.

While there are a growing number of tools, use of these by non-expert personnel can produce reports listing an overwhelming number of vulnerabilities. Typically this includes false positives (making up as much as 20%) and many other 'vulnerabilities' that are unlikely to be critical for a specific network, and all of which result in excessive effort and expense to confirm and correct. This is where expertise and assessment against the real network environment is necessary.

The shortage of qualified personnel is compounded by the fact that security is alarmingly dynamic. The knowledge and software that was last used to successfully test your network may now be obsolete due to newly discovered vulnerabilities.

Maintaining the appropriate level of technical competency in vulnerability testing in house would require a multidisciplinary team well versed in the countless hardware and software combinations used in your network. Very few organizations can afford to dedicate the necessary resources to effectively perform these monitoring tasks.

For all but the largest of security assessment organisations, attracting and retaining a qualified security team is difficult. This often explains why so many organizations have in the past used third party consultants, a solution that gets the job done, but calls for deep pockets.

Automated vulnerability detection systems side-step the issue of either building an in-house team of specialists or hiring external consultants at great expense to do infrequent tests.

Regulatory Compliance

As the regulatory landscape becomes steadily more complex, the risks associated with noncompliance grow more costly. Additionally organisations and their network security administrators are increasingly required to demonstrate compliance to a variety of internal policies, and industry standards.

Automated vulnerability assessment systems that keep up-to-date reports on file regarding the current status of network security dramatically speed the response time to new regulations, policies and standards as there is always current data available to meet each compliance request. Networks that are regularly scanned no longer require a 'fire drill' style response to each new requirement and deadline.

The Future of Network Security Assessments

With hundreds of new operating system and application vulnerabilities announced each month the need to establish vulnerability testing as an ongoing, continuous process has become essential. Like automated antivirus and patching, an automated, ongoing vulnerability assessment and management solution is now a genuine option.

Today’s business network now has a need for two types of vulnerability assessments: A snapshot analysis of current network posture and on-demand evaluation of any changes in the environment. Some environments may require a weekly (or even daily) test frequency due to the value of the resources being protected and the increasing complexity of networks and the speed at which vulnerabilities can now be exploited.

Take into consideration that network complexity and connectivity continually increases. The number of vulnerabilities being discovered daily and the speed at which exploits can launch malicious code has grown. Combine this with the ease of which rogue devices can be installed, connected or communicate with your network. Performing vulnerability and network security assessments annually, biannually or even quarterly is no longer a sufficient risk mitigation strategy for today’s well protected network.

Similarly, the challenge of staying up to date with current vulnerabilities is now a highly specialist task which can and should be assigned to a dedicated solution capable of updating automatically for new threats and scanning periodically based on a predefined schedule.

Real-World Security

The concept of Automated Vulnerability Detection can be described in this simplified analogy:

Say your building has a high perimeter wall and a motion detection alarm system. Like network perimeter security products (antivirus, firewalls and IPS/IDS) you are likely to be alerted that someone is approaching. But it does not tell you that your back door was left unlocked by the last person leaving – or worse yet, left standing wide open.

If a hacker or thief sees a known vulnerability, or unlocked door, there isn't a high enough fence or alarm system in the world that will keep them from trying to get in. They will get very inventive as to how they will scale the wall so as to not set off the alarm – if there is an open door beckoning!

Automated VA/VM consists of assessing the mechanical condition of your network's doors and windows, the relative merit of their locks and reporting on their state of readiness in near real time.

A house or network that presents NO apparent weaknesses to a hacker or thief is simply skipped over. He'll go down the road and find an easier target, there are many to choose from.

In the real world of network security it is not about being 'perfectly' secure – which is an illusion given the speed of change of networks and the rate at which new exploits are developed. It is about being secure enough that you are simply left alone.

Naturally, VA/VM will never replace your walls or alarm systems, but with no known vulnerabilities to entice an attacker you will have fewer attempts on your network.

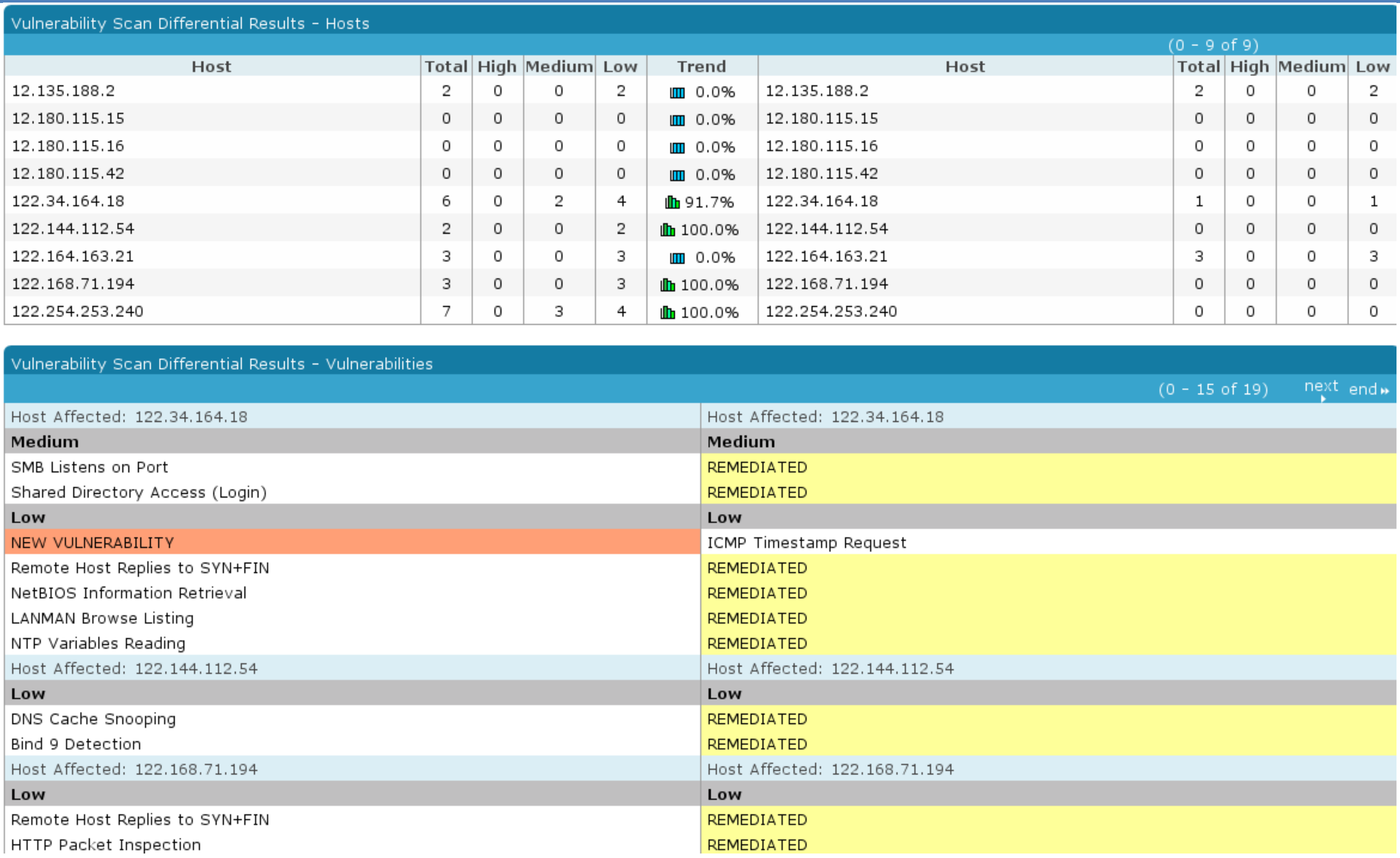
Automated Vulnerability Detection Now a Reality

AVDS (Automated Vulnerability Detection System) is a series of hardware appliances that run dedicated online connected software; capable of simulating both internal and external hacker attacks for networks of 200 to 2 million nodes.

AVDS performs a comprehensive vulnerability assessment on the network and produces a detailed report that contains:

- An executive summary of the vulnerabilities found
- A comprehensive list of all vulnerabilities discovered
- A wide range of solutions to those vulnerabilities
- The list of all simulated attacks performed

Figure 1: Comprehensive Differential Results on Previous Scan Results



Vulnerability Scan Differential Results - Hosts

(0 - 9 of 9)

Host	Total	High	Medium	Low	Trend	Host	Total	High	Medium	Low
12.135.188.2	2	0	0	2	0.0%	12.135.188.2	2	0	0	2
12.180.115.15	0	0	0	0	0.0%	12.180.115.15	0	0	0	0
12.180.115.16	0	0	0	0	0.0%	12.180.115.16	0	0	0	0
12.180.115.42	0	0	0	0	0.0%	12.180.115.42	0	0	0	0
122.34.164.18	6	0	2	4	91.7%	122.34.164.18	1	0	0	1
122.144.112.54	2	0	0	2	100.0%	122.144.112.54	0	0	0	0
122.164.163.21	3	0	0	3	0.0%	122.164.163.21	3	0	0	3
122.168.71.194	3	0	0	3	100.0%	122.168.71.194	0	0	0	0
122.254.253.240	7	0	3	4	100.0%	122.254.253.240	0	0	0	0

Vulnerability Scan Differential Results - Vulnerabilities

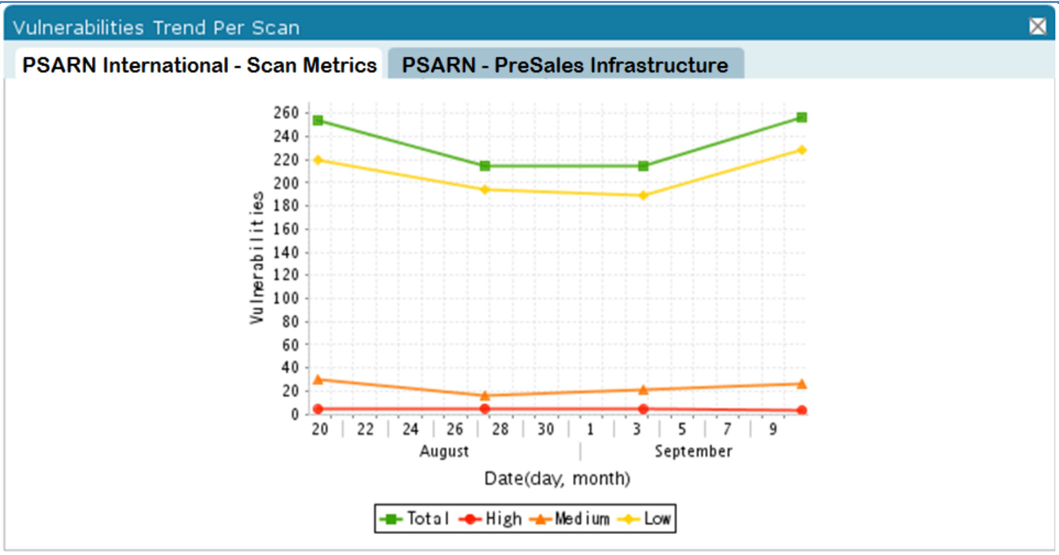
(0 - 15 of 19) next end

Host Affected: 122.34.164.18	Host Affected: 122.34.164.18
Medium	**Medium**
SMB Listens on Port	REMEDIATED
Shared Directory Access (Login)	REMEDIATED
Low	**Low**
NEW VULNERABILITY	ICMP Timestamp Request
Remote Host Replies to SYN+FIN	REMEDIATED
NetBIOS Information Retrieval	REMEDIATED
LANMAN Browse Listing	REMEDIATED
NTP Variables Reading	REMEDIATED
Host Affected: 122.144.112.54	Host Affected: 122.144.112.54
Low	**Low**
DNS Cache Snooping	REMEDIATED
Bind 9 Detection	REMEDIATED
Host Affected: 122.168.71.194	Host Affected: 122.168.71.194
Low	**Low**
Remote Host Replies to SYN+FIN	REMEDIATED
HTTP Packet Inspection	REMEDIATED

Additional reporting features available in AVDS also include:

- Technical analysis including links for immediate remedial action
- Differential reporting mechanisms that shows the difference from previous scans (figure 1), allowing you to track both infrastructure changes (figure 2) as well as the vulnerabilities
- Data mining allows you to target specific hosts, vulnerability types or services and export these results in multiple formats

Figure 2: Track the changes in the organization networks over a time period.



The AVDS reports can be used as an extensive network management tool, providing a powerful Sarbanes Oxley, PCI and HIPAA compliance tool.

Automated Vulnerability Detection System

AVDS is updated with new attack profiles on a daily basis using information from the www.securiteam.com security portal, which is one of the largest and most respected security information gathering portals on the Internet.

Using AVDS, it is possible to conduct security scans on:

- The corporate LAN and WAN (from within the organization)
- The DMZ and the external network (from the Internet and outside world)
- Anything that talks “IP” on a network including VoIP network elements and endpoint devices.

AVDS provides the following major features:

- Simulates attacks on the organisation’s network by using 'sanitized' versions of hacking techniques, tools and methodologies.
- Uses a pre-determined network bandwidth, eliminating negative effect on the performance or availability.
- Performs on-demand and scheduled penetration testing, according to your predefined schedule including daily, weekly, monthly or any other combination you require.
- Includes built-in data mining capabilities, allowing on-the-fly generation of statistical and historical information about your network posture.
- Distributes vulnerability scanning tasks and reports to stakeholders. This provides distant administrators access to the scanning system for use in their network segment.
- Allows tracking of all vulnerabilities across an entire network and multiple sites.
- Generates a network map, detailing what servers and services exist, or alternatively, have been added, removed or changed since the last scan.
- Export results for external reference in multiple formats: HTML, PDF, CSV and XML.

Securing Your Network Provides a Return on Investment

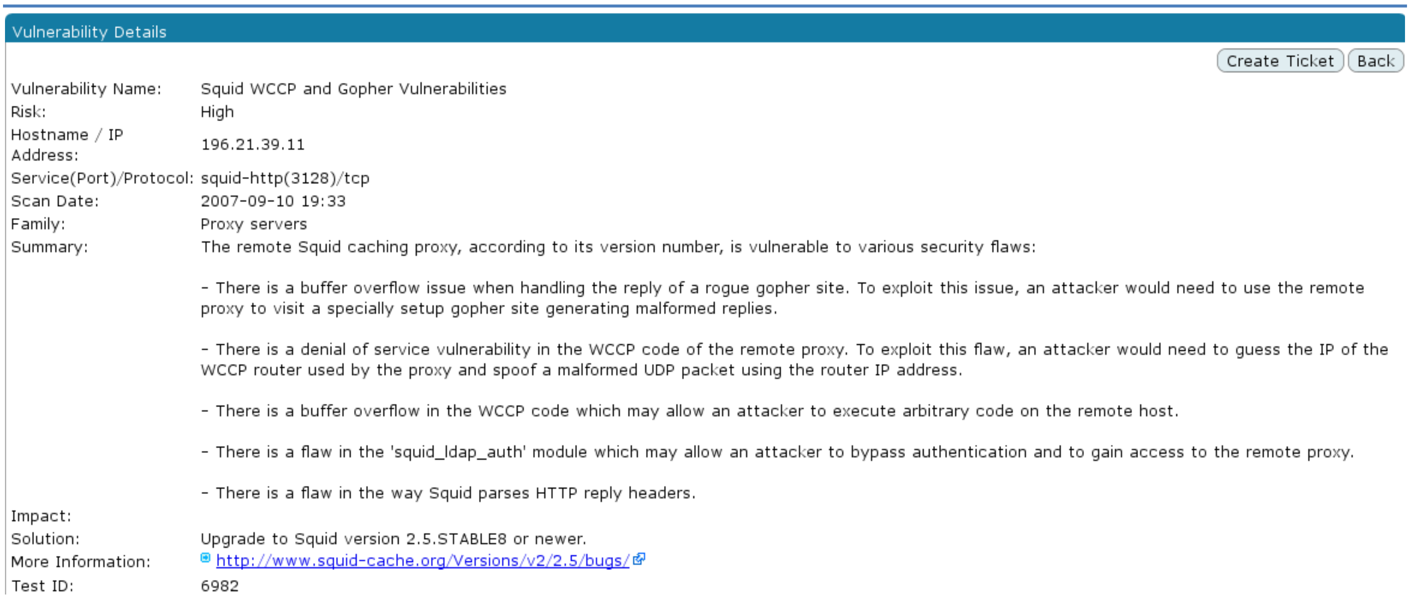
The benefits of using AVDS to effectively manage the detection, tracking, reporting and resolution of network vulnerabilities are outlined below:

- Address network security threats regularly, ensure you are continually safeguarding the network
- Accurate vulnerability assessment data increases business confidence and reputation
- Free up resources from discovering, analysing and researching threats to your network, ensures you can focus on resolving or mitigating threats before they can be exploited
- Meaningful results, including corrective actions enables a more efficient resolution
- Lead time required by a security consultant could leave your organisation vulnerable as his findings will be out-of-date within weeks of the test
- Ongoing costs required to maintain the same level of network security are lowered due to the automated and timely manner in which assessments can be performed and acted upon

In summary, performing threat assessments on a more regular basis reduces the window of opportunity of unknown vulnerabilities being exploited. Manual vulnerability assessments are by their very nature outdated by the time the report is received. Improving the timeliness and quality of report results strengthens your security confidence.

Return on investment is short due to the continual delivery of up-to-date threat assessment techniques and methodologies. This can provide opportunity to widen the assessment scope from just a limited set of business critical services.

Figure 3: Sample of a High-risk Vulnerability



Vulnerability Details

Vulnerability Name:	Squid WCCP and Gopher Vulnerabilities
Risk:	High
Hostname / IP Address:	196.21.39.11
Service(Port)/Protocol:	squid-http(3128)/tcp
Scan Date:	2007-09-10 19:33
Family:	Proxy servers
Summary:	The remote Squid caching proxy, according to its version number, is vulnerable to various security flaws: - There is a buffer overflow issue when handling the reply of a rogue gopher site. To exploit this issue, an attacker would need to use the remote proxy to visit a specially setup gopher site generating malformed replies. - There is a denial of service vulnerability in the WCCP code of the remote proxy. To exploit this flaw, an attacker would need to guess the IP of the WCCP router used by the proxy and spoof a malformed UDP packet using the router IP address. - There is a buffer overflow in the WCCP code which may allow an attacker to execute arbitrary code on the remote host. - There is a flaw in the 'squid_ldap_auth' module which may allow an attacker to bypass authentication and to gain access to the remote proxy. - There is a flaw in the way Squid parses HTTP reply headers.
Impact:	
Solution:	Upgrade to Squid version 2.5.STABLE8 or newer.
More Information:	http://www.squid-cache.org/Versions/v2/2.5/bugs/
Test ID:	6982

AVDS Quick Facts and Differentiators

Some AVDS highlights:

- Fully automated and hardened appliance

- Preinstalled, self-contained system

- Less than 0.1% false positive rate, the lowest in the industry

- Utilises the www.securiteam.com portal as the primary information source. Securiteam.com is one of the largest sources of vulnerability information and solutions on the Internet and is referenced by many vulnerability scanning products

- Capable of automatically discovering, indentifying and reporting on:
    - Rogue Wireless Access Points, devices & software applications, modems, USB storage devices, Trojans and SpyWare
    - Network equipment such as Routers, Access Points, VoIP phones and gateways
    - Security appliances such as Firewalls, Content filtering systems and AntiVirus
    - Scans “anything that talks IP”

- Appliance deployment features in (or outside) your network include:
    - Distributed information management
    - Distributed scanning servers
    - Scans through wireless networks (802.11a/b/g/n, GPRS, Bluetooth)
    - Discovers and maps wireless access points
    - Completely agent-less, requiring no special privileges or software installations, giving you an accurate “hacker’s view” of your network
    - At theoretical maximum performance, scan an entire Class C network in less than 30 minutes
    - Network load controls allows scanning without disruption of users

- Specifically tests and checks against:
    - Multiple Operating systems, not limited to UNIX, Linux, MAC OS, AS400, Novell, Windows 95/98, Windows NT, Windows XP, Windows 2000/2003, Vista and Windows 7
    - Common attack signatures along with behavioural patterns
    - Application Layer 7 checks
    - Denial of Service scans, configurable as on demand
    - Multiple levels, the only scanning tool capable of performing automated scans for vulnerabilities in the system, database, network, applications and web site.

- Management Interface and Configuration options allow you to:
    - Completely manage the scanning appliance through a simple to use web interface
    - Manage multiple scanning servers from a single location
    - Control each scanning server’s configuration within the distributed management system
    - Create multiple users and assign them one or more security management roles
    - Track and maintain security events as tickets across the whole managed system
    - Scan specific IP addresses, view reports of scans, schedule new scans, etc
    - Generate differential reports, allowing you to track changes in network security posture

- Each report provides remedial action recommendations

- Completely conforms to the CVE standard

White Paper Composition and Contact Information

About the Author

Mr. Noam Rathaus

Noam Rathaus is Cofounder and CTO of Beyond Security, a leading developer of security assessment technologies and products.

Noam is the editor-in-chief of SecuriTeam.com, one of the largest vulnerability databases on the Internet, and is involved in active vulnerability research. Over the years, Noam has found and reported vulnerabilities and weaknesses in over a dozen major products and protocols that are in everyday use.

Mr. Rathaus has contributed to several security related open-source projects including an active role in the Nessus security scanner and the FreeSWAN VPN project.

He has co-authored several books including: “Open Source Fuzzing tools”, “Nessus Network Auditing” and “Customizing Open Source Security Applications”.

Noam holds an electrical engineering degree from Ben Gurion University.

About the Technical Editor

Mr. James Mouat

Mr. Mouat is a lead technology consultant for AVDS in Australia and provides support and infrastructure planning services to Australian businesses and government departments.

James holds a Master of Information Technology specialising in forensic computing and software engineering from the University of Canberra.

Contact Information

Web Site	www.BeyondSecurity.com
Research Site	www.SecuriTeam.com
USA	
1616 Anderson Road McLean, VA 22102	+1 800 801 2821 sales@beyondsecurity.com support@beyondsecurity.com partners@beyondsecurity.com
19925 Stevens Creek Blvd. Cupertino, CA 95014	+1 408 329-6041 donw@beyondsecurity.com
UK	
105 London St. Suite 609 Reading RG1 4QD United Kingdom	+44 203 006 3022 sales@beyondsecurity.com support@beyondsecurity.com partners@beyondsecurity.com
EMEA	+972 54 794 0053 zvim@beyondsecurity.com
Asia Pacific	
Post Office Box 4 Mount Colah NSW 2079 Australia	+61 401 778 124 steveh@beyondscurity.com
China	
5/F South Block Tower C, Rathcom Info Tech Park, No 2 Kexueyuan South Rd. Haidian District Beijing 100190	+86 10 598 22211 thomasz@beyondsecurity.com