

# In The Boxing Ring



## IN THIS ISSUE

### 2. **ISO 27001:2005**

To ensure quality, consistency, and effectiveness; it is vital to work within a well defined, documented, and audit-able framework. Michael Gazeley (chairman, Network Box) provides a guest column to talk about the importance of certification and the ongoing ISO 27001:2005 process.

### 3. **VULNERABILITY SCANNING**

The first in a two-part series on the current state of the art in Network Vulnerability Scanning. This month, we outline what this technology can do for you, and talk about how Network Box can assist you to be pro-active in the defense of your network and its data.

### 3. **IPHONE AND IPAD APP**

The launch of v3.1 of the Network Box App, and the upcoming v3.2 with native iPad support.

### 4. **APRIL 2010 FEATURES**

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBR3-3.0 customers.

## Network Box Technical News from Mark Webb-Johnson, CTO Network Box

### Welcome

Welcome to the April 2010 edition of 'In the Boxing Ring'. In this edition, we'll be looking at certification, vulnerability scanning, and support for the upcoming Apple iPad.

On page 2, Michael Gazeley (Chairman, Network Box) provides a guest column to talk about the importance of certification and the ongoing ISO 27001:2005 process that Network Box operation centres around the world conform to.

On page 3, I spend some time discussing the current state of the art in Network Vulnerability Scanning. I present the three types of scanning currently available, and talk about how Network Box can assist you with this important opportunity to be pro-active concerning the defense of your network and the information protected. This is the first of a two-part article, with the second half to be provided in next month's newsletter.

Also on page 3, I announce the availability of v3.1 of the Network Box iPhone App, including support for the upcoming Apple iPad. The new v3.2 version (providing native resolution support on the iPad) is also in progress and is planned for release during April.

On page 4, we present the usual monthly hint (this month regarding obsolescence of the Microsoft's Internet Explorer v6 browser), and outline the software updates delivered as part of this month's software release.

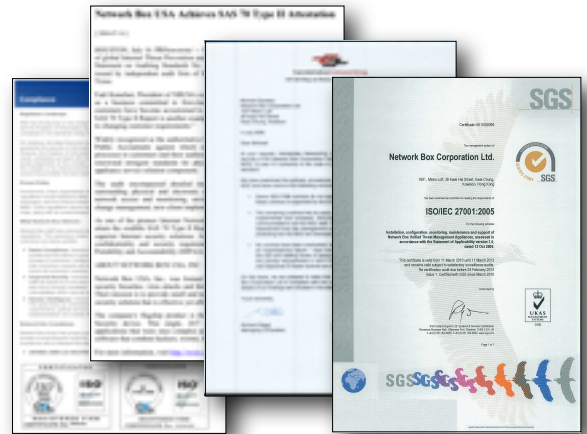
As usual, if you have any feedback, or comments, they are always appreciated. You can contact us here at HQ via eMail ([nbhq@network-box.com](mailto:nbhq@network-box.com)). Or, drop by our office next time you are in town.

You can also keep in touch by following our Network Box Security Response twitter feed at:

**[twitter.com/networkboxhq](https://twitter.com/networkboxhq)**

Mark Webb-Johnson  
CTO, Network Box Corporation  
April 2010





**ISO/IEC 27001:2005**

By Michael Gazeley, Chairman Network Box

As information security management increasingly becomes a mainstream topic of conversation; both within governments and in company board rooms across the world; more and more IT Managers find themselves needing to actively demonstrate that the IT Security solutions they have put in place for their organizations are, "up to standard."

When IT Security news is regularly making newspaper, radio and television headlines, and is at the very forefront of President Obama's current foreign policy initiatives, it is clearly no longer a subject restricted to the niche computer magazines and insider blogs.

Certainly, most IT Managers now understand that installing some "do-it-yourself" firewall, along with some traditional pull update anti-virus software, is just not going to "cut it" anymore. But what does being, "up to standard," actually mean?

At Network Box, we believe that a very large part of being "up to standard," means ensuring that the security solutions in place, are installed, configured, monitored, maintained and supported to ISO/IEC 27001:2005 standards.

It is not good enough to just have the latest firewall, intrusion detection and prevention, virtual private networking, anti-malware, anti-spam, content filtering, company policy management, business continuity facilitation and automated reporting systems in place; someone (or more accurately a team of experts) needs to be monitoring, managing and updating all of the aforementioned network security systems, around the clock and all year round.

The reason that ISO/IEC 27001:2005 has become so important, is because although most organizations have some type of information security control, without a formal management system in place, even organizations which

theoretically do have everything listed above in place, still suffer from results which are often uneven in nature, inconsistent in execution, and therefore suboptimal almost by very definition.

Security should never be "ad hoc" in nature. Consistency is the cornerstone of every standard.

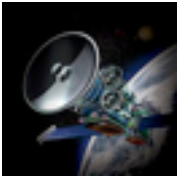
So the question before IT Managers across the globe is fast becoming, "how do I get all of the required security systems in place, ensure they are managed to ISO/IEC 27001:2005 standards, yet achieve all of this in an economic environment where the goal is actually to cut spending?"

As a fully Managed Security Service, with management systems certified to ISO/IEC 27001:2005 standards, Network Box offers by far the best (and most economic) answer.

Not only the best answer for government departments, large multi-nationals, hospitals, banks, public companies, and retail operations with PCI requirements; but also for all the small and medium sized organizations around the world, that almost have no chance of affording (or wanting to afford) everything required to do the necessary work in-house, without expert third-party help.

Network Box's highly dedicated Security Operations Centre engineers work nonstop; through every night, through every holiday, and even through tornado warnings, hurricanes and floods; to help secure your computers, networks, and organizations, on a real-time basis, using PUSH update technology, all while conforming to ISO/IEC 27001:2005 standards.

In the end, true network security is a service, not just a mix of hardware and software. And that is what the ISO/IEC 27001:2005 standard is all about.



## Vulnerability Scanning

In today's security environment, vulnerability scanning plays an important role in the pro-active testing and benchmarking of security systems.

There are three main types of network scan available today:

- Network enumerators (an advanced form of network mapping) - in which a network is scanned to find connected hosts, and then those hosts are scanned to enumerate information (such as version of operating system, available services, users logged in, network shares, etc).
- Network vulnerability scanners - in which an in-depth scan is conducted against particular hosts and responding services, to determine if any of a set of known vulnerabilities are present.
- Network application scanners - an advanced and targeted form of network vulnerability scan in which specific applications are tested in-depth, often using generic heuristic tests as well as known signature-based tests.

Vulnerability scanning tools are regularly used by malicious hackers on the Internet to identify vulnerable machines for compromise. It makes good sense for you to make use of similar tools to proactively protect your network - to identify the vulnerabilities before someone else does.

These vulnerability scans can typically be either external (from a scanner on the Internet, showing the Internet's point of view) or internal (from a scanner on the LAN/DMZ, showing the point of view of an internal, privileged, network user).

It is very important that the scans are tuned to the particular environment being scanned, and the direction (either internal or external). For example, we've often seen vulnerabilities falsely reported regarding open proxies (ie; smtp or web proxies which allow open access to the Internet) - from an external scan, such proxies should not be accessible or open, but from an internal scan it is expected that such proxies should be available. Similarly, we've seen false reports of vulnerabilities assuming a particular vulnerability just because a particular service is open (effective vulnerability scanners should test for the actual vulnerability itself, rather than just assume a particular version is vulnerable).

The false-report rate with automated vulnerability scans is typically exceptionally high. The requirements of standards such as PCI regarding vulnerability scanning, combined with the availability of automated scanning software, has led to an explosion of scanning services. Most of these services offer an automated scan of your network, at a prearranged time, and then present you an unfiltered report of vulnerabilities (both real and imagined). It takes an expert to then go through each of those reports to determine the status of each vulnerability and make recommendations as to follow-up actions to be performed.

Such automated vulnerability scans are usually external only, and offer no insight as to the internal vulnerabilities in the network. They ignore the internal threats of malicious staff already inside your organisation.

It is also important to be able to compare scans over time. To look at last quarter's scan compared to this quarter; both to see new vulnerabilities as well as to ensure that planned follow-up actions have been performed correctly.

Correctly used, and expertly handled, vulnerability scans are an invaluable tool for pro-active protection of your network. Even if your organisation doesn't have the compliance requirement for a scan, please consider using them. Network Box operation centres around the world are there to help you and can assist with this important task.

In next months In The Boxing Ring newsletter, I plan to complete this article by explaining in more detail how Network Box can help with the tasks and management of vulnerability scans, as well as what we recommend the requirements are for an effective regular vulnerability assessment.



## iPhone App v3.1

Version v3.1 of the Network Box iPhone App is now available in the Apple App Store. The changes made in this version include:

- Compatibility with v3.2 OS (adding support for Apple's new iPad in 1x and 2x zoom modes)
- Improvements in local caching for improved performance
- Auto-Refresh enhancements to main views (showing previous cached content, while retrieving the latest content from the server)
- Auto-Refresh enhancements to global map (showing previous cached map, while retrieving the last status from the server).
- Minor bug fixes

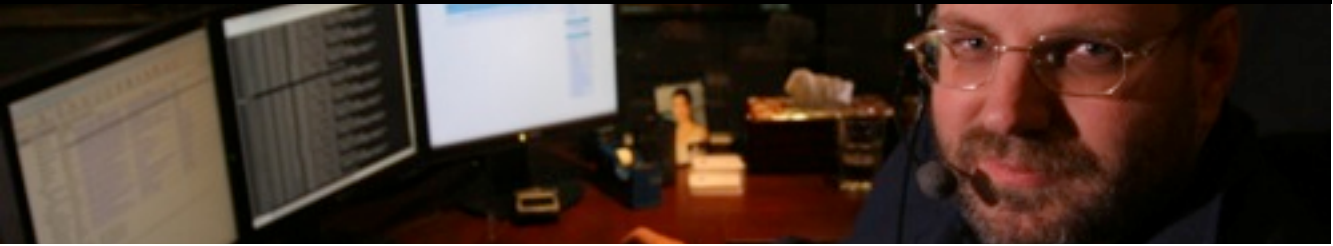
We are working on further upgrades to our application and the next release will be a "universal App" supporting the iPhone, iPod Touch and iPad at native resolutions. This next version (tentatively known as v3.2) is scheduled to be released within this month (April 2010) once Apple starts accepting these universal Apps and once the final iPad hardware is shipping.

As well as support for the 1024x768 resolution of the iPad, the new version adds support for the larger keyboard (as well as external/bluetooth keyboards).

The v3.2 update will be delivered as a standard update through the Apple App store.



Network Box v3.2 iPad App



**April 2010 Features**



On Tuesday, 6<sup>th</sup> April 2010, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Further firmware support for new box models.
- Enhancements to the Box Office portal, to support the v3.2 iPhone/iPad application.
- Enhancements to the POP3 acceleration system, to improve compatibility with some non-standards compliant POP3 servers.
- Support for per-domain routing in our transparent SMTP proxy. Also add support for fail-safe session timeouts in this.
- Performance improvements to our web proxy URL categorisation and policy enforcement system.
- Minor security patches to the NTP service we offer (normally accessible to LAN/DMZ but not to NET).
- Minor sensor adjustments for some box models, in the health monitoring system.
- Minor cosmetic changes to some my.network-box.com administrative screens.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

**April Hint: Internet Explorer v6 RIP**

It is time for Internet Explorer v6 to Rest In Peace. Really. The product has served us well, but is now just too old, too incompatible with modern standards, and just too insecure.

Microsoft has, over the past few years, done a tremendous job in improving the security of their Internet Explorer browser. But, those improvements are for the latest versions and IE6 is lagging behind. For example, look at the table below regarding the ten vulnerabilities recently announced as part of Microsoft's MS10-018 out-of-band security update. Of those, 8 affect IE6, 7 affect IE7 and only 3 affect IE8.

Web developers, as well as large public services, are increasingly dropping support for IE6 as it is becoming harder to justify downgrading the modern web 2.0 experience solely to support this venerable browser.

Currently, 10% of Network Box users are still using IE6, and we need to get that down to 0%. Really.

Mark Webb-Johnson,  
CTO, Network Box Corporation

CVE	IE 6	IE 7	IE 8
CVE-2010-0267	Critical	Critical	NA
CVE-2010-0488	Important	Important	NA
CVE-2010-0489	Critical	Critical	NA
CVE-2010-0490	Critical	Critical	Critical
CVE-2010-0491	Critical	NA	NA
CVE-2010-0492	NA	NA	Critical
CVE-2010-0494	Critical	Important	Important
CVE-2010-0805	Critical	NA	NA
CVE-2010-0806*	Critical	Critical	NA
CVE-2010-0807	NA	Critical	NA

MS10-018 Simplified View (source: Microsoft)

**MARCH 2010 NUMBERS**

Key Metric)	#	% difference (since last month)
PUSH Updates	1,022	-23.7
Signatures Released	257,006	+2.3
Firewall Blocks (/box)	628,606	-5.6
IDP Blocks (/box)	161,793	-19.9
Spams (/box)	45,820	-14.8
Malware (/box)	767	-70.0
URL Blocks (/box)	78,214	-2.6
URL Visits (/box)	3,255,137	-4.3

**NEWSLETTER STAFF**

**Mark Webb-Johnson**  
Editor

**Michael Gazeley**

**Jason Law**

**Nick Jones**

Production Support

**Network Box Australia**

**Network Box Hong Kong**

**Network Box UK**

Contributors

**SUBSCRIPTION**

Network Box Corporation  
[nbhq@network-box.com](mailto:nbhq@network-box.com)

or via mail at:

**Network Box Corporation**

16th Floor, Metro Loft,  
38 Kwai Hei Street,

Kwai Chung, Hong Kong

Tel: +852 2736-2078

Fax: +852 2736-2778

[www.network-box.com](http://www.network-box.com)