In the Boxing Ring
MAR 2021

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the March 2021 edition of In the **Boxing Ring**

This month, we are talking about **Vulnerability Scanning**. Sometimes, having someone independent looking over your work is helpful and not at all a bad thing. In the IT security industry, a security auditor normally performs this kind of work as part of your certification requirements. Even if you don't have any certification requirements (such as ISO, PCI, or SAS, for example), conducting or commissioning regular vulnerability scans is generally a good idea. On pages 2 to 3, we discuss this in detail.

In this month's Media Coverage, Network Box's Managing Director, Michael Gazeley, was on **RTHK Radio 3** to discuss the HK Government's LeaveHome-Safe App's privacy implications. Additionally, Network Box Germany's Dariush Ansari was interviewed about security issues by **Online Focus**. Finally, the latest episode of **HPCC Hackpod Club** is now available.

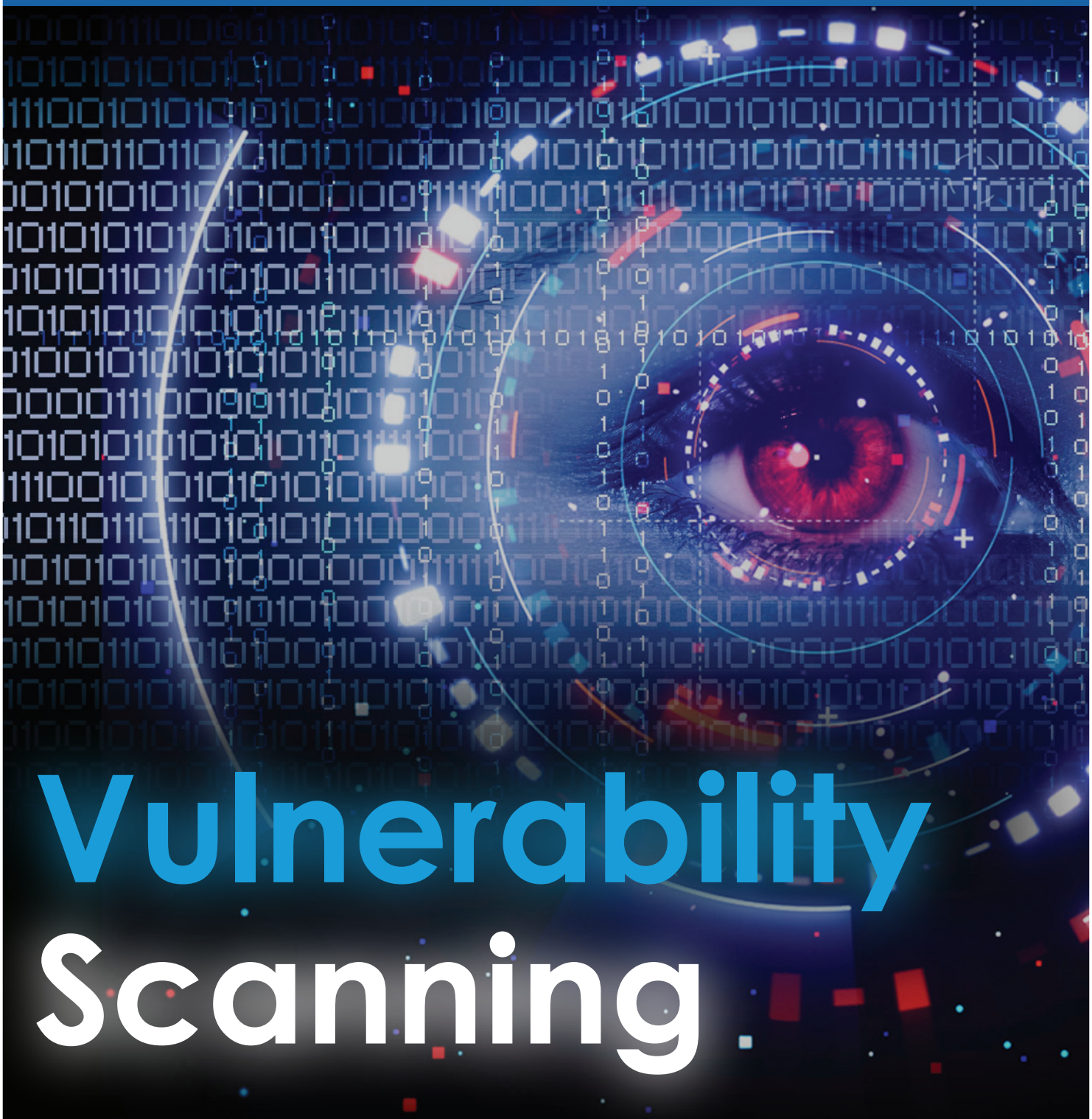
Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2021

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:



Vulnerability Scanning

Sometimes, having someone independent looking over your work is helpful and not at all a bad thing. Examples include an auditor checking your company accounts, a licensed inspector checking your construction work adheres to regulations, or a regular periodic fire safety inspection.

In the IT security industry, a security auditor normally performs this kind of work as part of your certification requirements. Pretty much all certifications require regular external penetration tests and/or vulnerability scans, checking your systems are up to date and not vulnerable to commonly known security issues.

Even if you don't have any certification requirements (such as ISO, PCI, or SAS, for example), conducting or commissioning regular vulnerability scans is generally a good idea. Think of it as a seat belt - there in case you or others make a mistake.

What is a vulnerability scan?

Vulnerability scans may be conducted either internally (from inside your network) or externally (usually from the public Internet), and generally consist of four stages:

1. Enumeration of all the active IP addresses and open ports on those devices in the targeted network.
2. Identification of the services running on those enumerated IP addresses and ports.
3. Scanning each of those services with known attack patterns, and interpretation of responses to determine if vulnerabilities exist.
4. Reporting on results.

These scans can be configured to be unauthenticated or authenticated with valid credentials. In general, authenticated scans provide more accurate results and are preferred (especially for internal vulnerability scans).

What do you get from a scan

Typically, the results of the scan will include:

- A high-level management overview.
- A detailed list of every discovered device IP address, port, and service found.
- A detailed list of every vulnerability found.
- Summary tables. This may be delivered as a PDF report or an online drill-down facility.

The more sophisticated vulnerability scans provide online workflow style actions to allow you to follow-up on discovered issues, and track and correlate these issues between successive scans.

The Problem of False Positives

The quality of the scan results you get varies tremendously with the scanner, it's configuration, and rulesets employed. Some scanners simply identify the version of software running on a particular port (usually by the greeting banner issued on connection/request), and then report you impacted by all vulnerabilities known to exist for that software version.

More sophisticated scanners actually try to exploit the vulnerability or test for its presence before reporting it. The better scanning services employ human engineers to review initial scan results and remove false positives before publishing the report to you. Penetration Testing services commonly use vulnerability scanning as one of their core tools and interpret the results to highlight areas of concern.

It is important to recognise that the report issued by a vulnerability scanner is not a guilty verdict beyond a reasonable doubt. Think of it more as a set of accusations that need to be investigated. The vulnerabilities reported may simply not be there, or may have been mitigated in some manner (such as via patching). It is up to the network administrator, often in cooperation with the software or equipment vendor, to investigate and resolve each reported issue. There are also often different tolerances for issues identified; something considered a vulnerability by one may be a feature to another.

Regular Vulnerability Scanning is a powerful tool in your security arsenal that can help you identify common known security vulnerabilities in your network. But it is important to recognise that this report requires follow-up action to investigate and resolve the issues addressed. Even if you don't have a certification requirement for vulnerability scans, they are recommended for all organisations, particularly those with services exposed to the public Internet.

Network Box HIGHLIGHTS

Network Box Media Coverage

RTHK Radio 3

Backchat with Hugh Chiverton:
Leave Home Safe App
LINK: https://bit.ly/37SZRbh

Online Focus

IT Security Awareness: Staff training is the most important IT security measure
LINK: https://bit.ly/2PhmmQR

HPCC Hackpod Club

Episode #7:
From zero to home office
LINK: https://bit.ly/3q5jfbB

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	Network Box Corporation 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 2736-2083 Fax: +852 2736-2778 www.network-box.com

Global Security Headlines

CNN

6 coronavirus vaccine scams that target your money and personal information - and what to do about them
LINK: https://cnn.it/3ky4bSr

Hackers intercepted a Covid-19 vaccination appointment hotline in Pennsylvania
LINK: https://cnn.it/3q77Qb4

North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report
LINK: https://cnn.it/3q4Ftun

SC Media

Security gaps in operational tech exposed with hacker attempt to poison Florida city water
LINK: https://bit.ly/2NPunMr

BBC News

Milan's 'acrobat thieves' use Instagram tags 'to rob rich and famous'
LINK: https://bbc.in/3pZmVeZ

Channel News Asia

Nearly 130,000 Singtel customers' personal information, including NRIC details, stolen in data breach
LINK: https://bit.ly/3uJR8SW