In the Boxing Ring
APR 2022

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

Welcome to the April 2022 edition of In the **Boxing Ring**

This month, we are talking about the **Network Box Best Practices**. Network Box has developed a set of Best Practices from over two decades of delivering Managed Security Services, investigating security incidents, and working with our customers to protect their networks. These represent the most common forms of network infiltration and data breaches that we see affecting networks around the world. We have published these to encourage broader awareness and recommend that all customers adhere to them. On pages 2 to 4, we outline these in further detail.

On page 5, we highlight the features and fixes to be released in this quarter's Patch Tuesday for Network Box 5.

In other news, the **Network Box Mobile SIEM+ App** is available for FREE on Google Play and Apple Store. Additionally, the latest Episode of the **HPCC Hackpod Club** is now available. And in this month's Security Headlines, the US Government warns of Russian cyberattacks, and security vulnerabilities were discovered in **Sophos**, **Apple**, and **NVIDIA** products.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2022

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:

Network Box Best Practices

Over the past two decades of delivering Managed Security Services, investigating security incidents, and working with our customers to protect their networks, Network Box has developed a set of Best Practices.

These represent the most common forms of network infiltration and data breaches that we see affecting networks around the world. Many of these best practices can also be found in common standardized security frameworks. These and other Best Practices are continually revised and updated to keep up with the evolving security threat landscape and protection technologies. Today, we have published these to encourage wider awareness and adoption.

https://network-box.com/best-practices

Network Box Security Engineers refer to these Best Practices when designing defense systems for networks under our management, when processing policy change requests, and during periodic configuration reviews. We recommend that all customers adhere to these. While ultimately, the customer decides the policy, we strive to inform, warn, and point out when policies conflict and open up networks to common attack vectors and unnecessary risk.

Remote Administrative Access Open to the Internet

In general, Remote Administrative Access services (such as SSH, RDP, VNC, etc.) capable of providing administrative access should not be open to the Internet. Opening such services to the Internet directly exposes the network to the exploitation of vulnerabilities or insecure credentials, and brute force attacks. Even those services restricted to user-only (non-administrative) access are discouraged due to privilege escalation issues.

As an alternative, it is recommended that VPN / SDWAN services be deployed. These remote administrative services should only be made available over secure VPN / SDWAN links to specific user accounts, VPN endpoints, or source IP addresses.

Weak, Default, or Re-Used, Authentication Credentials

User or administrative authentication credentials should be strong, never re-used, and should not be the defaults originally provided.

Administrative Access Source Restrictions

Access to administrative services should be closed to all by default and only opened to specific sources in order to meet specific access requirements.

Effective Policy Control

Effective policy control, and a 'block all, permit only what is necessary' approach should be applied, following the principle of least privilege.

Domain Name System (DNS)

Network Box (or other reliable, hardened, and secure) DNS servers should be used for all equipment. ISP or shared global DNS resolvers should never be used. When multiple DNS resolvers are specified, they should all be of the same type. When access to local lookup domains is required, that can be implemented using domain forwards. DNS servers should be configured to disable recursion, except for specific source IP address subnets.

Excessive Whitelisting / Bypassing

Whitelisting and bypassing should be applied sparingly and minimally.

Effective Network Segmentation

This should be employed to, at a minimum, separate servers from users and separate different organizational groups wherever possible. VLAN technology, or physical network interfaces, should be used for this; supplemented by layer 3 routing, firewall policy control, and high-level protection (such as WAF, IDPS, etc.).

Weak User Access Restrictions

Access to user services should be restricted and only opened to meet specific requirements.

Effective Anti-Malware

Anti-malware security modules should be enabled and utilized to protect networks at three levels:

1. Gateway
2. Server
3. Workstation

Modules should not be disabled, and software and signatures should be kept up to date.

Effective Anti-Spam

Anti-Spam technology is essential for detecting and blocking phishing and other such malicious emails. This should be enabled and set to quarantine appropriately.

Deploy Intrusion Prevention

Intrusion Prevention should be used in preference to, or in combination with, Intrusion Detection.

- Inline IPS is preferable to active response IDS - subject to performance considerations.
- IPS and IDS systems should be effectively configured, and items such as local network ranges, ports used, etc., should be reviewed and confirmed to match the protected network and services.
- While deploying IDPS systems in alert (not block) mode initially is acceptable, for tuning purposes, such systems should be in blocking mode after such tuning has been completed.
- Frontline IPS systems should be enabled and enforced.
- Infected LAN systems should be enabled and enforced.
- Consider deploying honeypot addresses to improve reconnaissance detection capabilities.

SSL/TLS Traffic Should be Scanned

Traffic encrypted using the SSL/TLS protocol should be scanned. This affects SMTP, IMAP4S, POP3S, and HTTPS at a minimum.

As more and more Internet traffic moves through these protocols (for authentication and privacy reasons), such traffic becomes invisible to policy enforcement, malware detection, and other security controls. Intercepting and decrypting such SSL/TLS traffic is essential to protect laptops, desktop workstations, and servers.

Deploy Web Application Firewalls

Web Application Firewalls should be configured, tuned, and deployed in enforcing mode for any Internet-facing websites or services using the HTTP/HTTPS protocol.

Encrypted Traffic Policy Control

Encrypted traffic should be subject to policy control.

- Web Client HTTPS traffic intercepted.
- SSL (or STARTTLS) offered opportunistically where reasonable.
- WAF SSL offloaded for interception.
- VPNs terminated before policy control enforcement.
- Policy control for other encrypted traffic.

Lack of, or Poor, Encryption for Sensitive Data

Access to sensitive data should be restricted to strongly encrypted channels.

Preparation and Contingency Planning

Preparation and Contingency Planning should be employed to anticipate and prepare for issues.

- Anti-DDoS should be enabled and prepared, so it can be quickly applied if necessary.
- Condition Variables should be used to pre-prepare alternative policy paths for anticipated scenarios.

Most network infiltrations and data breaches that we commonly see are not the result of sophisticated hackers armed with zero-day exploits. Instead, the bad guys tend to target the 'low hanging fruit' - the easy targets. Networks with default administrative credentials, remote access open to the Internet, or well-known vulnerabilities waiting to be exploited are just three examples.

There is an old story of a man who walked into a scuba diving shop and asked for the biggest fins that the shop sells, as he was afraid of sharks. The shopkeeper tells him that no matter how long or powerful the fins are, he will never be able to outswim a shark. But the man replies that he only needs to outswim his dive buddy, not the shark. The same is true for network security. You don't need to make your network perfect. You just need to make sure that your defenses are strong enough that the bad guys will move on to easier targets.

Network Box 5.5

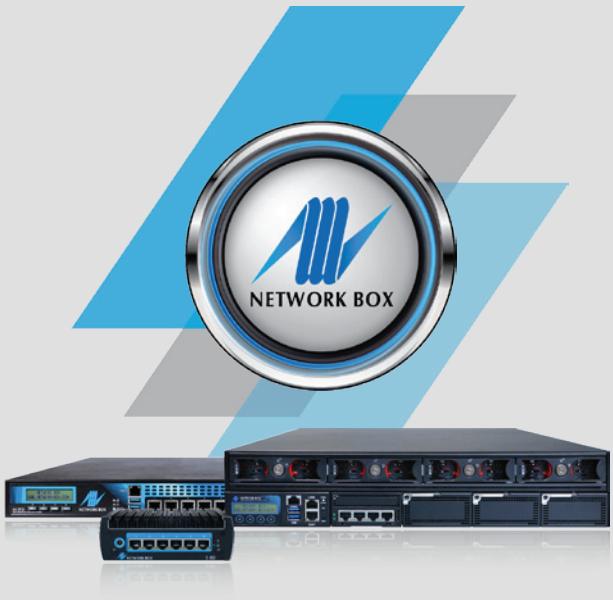
NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th April 2022, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
April 2022

This quarter, for Network Box 5, these include:

- Enhancements and improvements to SOC systems for device maintenance
- Fix for CVE-2022-0778 (openssl BN_mod_sqrt vulnerability) - release out of cycle last week
- Improvements to SOC configuration systems
- Support for customisation of performance for authentication and file object scanning
- Enhanced support for deployment of, and integration to, multi-tenanted cloud services
- Update of US SOC IP address allocations
- Add support for DDoS collection rules, with generic proxy
- Extensions to dhcp server to allow configuration and advertising of server identifier
- Improvements to console audit logging
- Extensions to user portal to allow customisation of : (a) token expire time, (b) visibility of email addresses in header, (c) support for release option text in header, and (d) suppression of statistics in header.



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 SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box HIGHLIGHTS

Network Box Mobile SIEM+

Available for phones and tablets, for both Apple iOS and Android-based mobile devices, the **Network Box SIEM+ App** is designed to provide secure access to administer Network Box managed services. In addition, the app provides access to: *Security News Stories*, *Box Office Ticketing System*, *NBSIEM+ Events*, and *Overview of Managed Assets*.

GET IT ON Google Play **LINK:** https://play.google.com/store/apps/details?id=com.networkbox.siem

Download on the App Store **LINK:** https://apps.apple.com/hk/app/network-box-siem/id1532859749

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

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

Media Coverage & Security Headlines

HPCC Hackpod Club
Episode #14:
Protection of data from Kolsch
LINK: https://bit.ly/3tYKNVm

servereye
Network Box and Server-Eye: Common sensor for blacklist scan
LINK: https://bit.ly/3NDL33x

CNBC
Russia is exploring options for cyberattacks, and companies must be ready, says Biden
LINK: https://bit.ly/3NxAgrT

The Hacker News
Critical Sophos Firewall RCE Vulnerability Under Active Exploitation
LINK: https://bit.ly/3iRHetp

The Register
Apple emits macOS, iOS, iPadOS patches for 'exploited' security bugs
LINK: https://bit.ly/3Dvjc11

Bleeping Computer
NVIDIA confirms data was stolen in recent cyberattack
LINK: https://bit.ly/3uKoGRF