In the Boxing Ring
JUL 2023

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

Welcome to the July 2023 edition of In the **Boxing Ring**

This month, we are talking about **Scanning and the External Threat View**. When analyzing the security posture of a computer network, various viewpoints can be considered: the internal view, the privileged external view, and the public external view. To understand one's security posture, it is crucial to have a clear view of what hosts and services are exposed to each of those viewpoints. Network Box Security Response has released a **Scan External View** cloud service to assist with this. On pages 2 to 3, we discuss this in greater detail and highlight the service's key features.

In other news, Network Box Hong Kong hosted a cybersecurity workshop for the staff of Fujifilm. Network Box Hong Kong also participated in HK Digital Finance Association- IT Event. And in this month's global security headlines, there were security issues with Fortinet, Google Chrome, Barracuda Networks, and Outlook.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 2023

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:

Scanning and the External Threat View

When analyzing the security posture of a computer network, various viewpoints can be considered, of which the top three are usually:

1. The Internal View
Which services are reachable for a potentially malicious intruder accessing them from within the LAN/DMZ.

2. The Privileged External View
Looking at services reachable to external privileged partners on the Internet - usually accessing from specifically privileged source addresses, MPLS networks, or via VPNs.

3. The Public External View
Services reachable to the general Internet.

While the public external view is not the only concern, it is commonly the most likely vector for a breach/intrusion. Thus, it is a focus for many protection technologies and policies.

To understand your security posture, it is crucial to have a clear view of what hosts and services are exposed to each of those viewpoints. While configuration reviews can go some way towards helping network reconnaissance by scanning (including enumeration of reachable hosts and services, and attempted identification of these), it is still the most effective technique.

Network Box External Threat View

Commencing with the June 2023 Patch Tuesday and gradually rolling out to all customers globally in a phased manner, Network Box Security Response has launched a **Scan External View** cloud service that operates as follows:

- Firstly, we need to know what to scan. To do this, we build a list of public and private IP addresses, domain names, and other such information for each asset under management. These 'asset attributes' are maintained automatically by parsing Network Box configurations but can also be manually administered (for attributes not directly visible in configurations). Administrators and SOC engineers can view these attributes on the Asset screen of NBSIEM+.

- Periodically (once a week or after major configuration changes by default), we comprehensively scan UDP and TCP ports on all public IP addresses from sources on the public Internet. This scan is typically in four parts:

  1. **Scanning:**
  for open UDP or TCP ports and retrieving welcome banner messages from these reachable services.

  2. **Service Identification:**
  based on banner analysis and other fingerprinting technologies.

  3. **HTTP/HTTPS Identification:**
  specifically looking for web services.

  4. **Basic Common Vulnerability Identification:**
  highlighting Best Practices findings.

- The results of the scan (discovered hosts, services, and vulnerabilities) are stored in a database and made available in the NBSIEM+ **Asset > Scans** screen, as well as for reporting purposes.

This is not intended as a full Vulnerability Scan. It is purely a reconnaissance scan, only showing what services (protocols/ports) and hosts (IP addresses) are open and visible to the public Internet. The scan is lightweight and only issues requests commonly seen daily in such Internet traffic.

Usage of the Results

The results are primarily used by Network Box SOC engineers as part of the configuration review process. They are part of a consistency check to ensure that the configuration correctly reflects the customer policy.

Network Box Security Response engineers also use the database when handling emerging vulnerabilities. We can quickly search for affected services and identify networks under management with those services reachable from the public Internet.

The Network Box *Scan External View* cloud service has been released and is now in operation globally. The results of these scans will be available to customers later this summer in the next release of NBSIEM+. This is the first of several upcoming *Network Box Red Team* services to be offered.

Network Box HIGHLIGHTS

Network Box Hong Kong
Fujifilm - Cybersecurity Workshop

Network Box Hong Kong hosted a workshop to staff from Fujifilm to highlight Network Box's Managed Cybersecurity Services, the latest features, functionality, certifications, compliance, and KPI reporting capabilities. Other discussion topics included MESH Cybersecurity Architecture, Risk Management, ISO 31000, In-Situ SIEM+, Virtual Patching, and other key technologies to stay ahead of hackers, malware, and other cyber threats.

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

Network Box Hong Kong
HK Digital Finance Association- IT Event

Network Box Managing Director, Michael Gazely, was invited by the Hong Kong Digital Finance Association to participate in a panel discussion about cybercrime and cybersecurity. At the event, which took place at the AsiaWorld Expo, Mr. Gazeley was joined by HKECIA President Emil Chan, Kornerstone Institute's Catherine Chan, Culsin Li of Baobab Tree Event, and Chief Inspector Lester Ip of the Hong Kong Police Force Cyber Security and Technology Crime Bureau.

Global Security Headlines

Bleeping Computer
Fortinet: New FortiOS RCE bug may have been exploited in attacks
LINK: https://tinyurl.com/3dvvy5dj

GB Hackers
Google Chrome Zero-Day Vulnerability Exploited Widely
LINK: https://tinyurl.com/3a7hpfs8

Bleeping Computer
Barracuda says hacked ESG appliances must be replaced immediately
LINK: https://tinyurl.com/2et9zhyy

Bleeping Computer
Outlook.com hit by outages as hacktivists claim DDoS attacks
LINK: https://tinyurl.com/3cunk8mv