In the Boxing Ring 2023年7月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2023年7月份的 In the **Boxing Ring**

本月，我们将讨论"扫描 "和"外部视图"。在分析计算机网络的安全态势时，可以考虑各种视图：内部视图、特权外部视图和公共外部视图。要了解一个人的安全状况，关键是要清楚地了解哪些主机和服务暴露在这些视角下。Network Box Security Response 发布了一项扫描外部视图云服务来协助实现这一点。在第 2 至第 3 页，我们将对此进行更详细的讨论，并重点介绍该服务的主要功能。

在其他新闻中，Network Box香港为富士胶片的员工举办了一次网络安全研讨会。此外，Network Box香港还参加了香港数字金融协会的IT活动。而在本月的全球安全头条中，Fortinet、Google Chrome、Barracuda Networks和Outlook都发现安全问题。

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

本月要闻:

扫描和外部威胁视图

当分析计算机网络的安全状况时，可以考虑各种视图，其中通常最重要的三个是：

1. 内部视图：
对于一个潜在的恶意入侵者从局域网（LAN）/ 隔离区（DMZ）内部访问的情况下，哪些服务是可达的。

2. 特权外部视图：
查看外部特权合作伙伴在互联网上可达的服务 - 通常是通过特权源地址、MPLS网络或VPN进行访问。

3. 公共外部视图：
对一般互联网可达的服务。

公共外部视图虽然不是唯一的关注点，但通常是违规/入侵最可能的途径。因此，它是许多保护技术和策略的重点。

为了了解您的安全状况，清楚地知道哪些主机和服务面向这些视图至关重要。虽然配置审查可以在某种程度上通过扫描（包括可达主机和服务的枚举以及对其进行尝试识别）来帮助网络侦察，但仍然是最有效的技术手段。

Network Box 外部威胁视图

从2023年6月的"Patch Tuesday"开始，Network Box安全响应团队将逐步按照分阶段的方式全球范围内向所有客户推出一个名为"Scan External View"的云服务。该服务的操作方式如下所述：

- 首先，我们需要确定进行扫描的内容。为此，我们会建立每个受管资产的公共和私有IP地址、域名和其他相关信息的清单。这些“资产属性”可以通过解析Network Box配置自动维护，但也可以手动进行管理（对于配置中未直接可见的属性）。管理员和SOC工程师可以在NBSIEM+的资产界面上查看这些属性。

- 定期地（默认情况下每周一次或在主要配置更改后），我们会从公共互联网来源对所有公共IP地址进行UDP和TCP端口的全面扫描。这次扫描通常包括以下四个部分：

  1. **扫描:**
  对打开的UDP或TCP端口，并从这些可达服务中检索欢迎信息。

  2. **服务识别:**
  基于欢迎信息分析和其他指纹技术。

  3. **HTTP/HTTPS 识别:**
  专门寻找Web服务。

  4. **基本通用漏洞识别:**
  强调最佳实践发现。

- 扫描的结果（发现的主机、服务和漏洞）将存储在数据库中，并可以在NBSIEM+的"资产" > "扫描"界面中进行查看，以及用于报告目的。

这个扫描并不旨在进行完整的漏洞扫描。它纯粹是一次侦察性扫描，只显示对公共互联网开放和可见的服务（协议/端口）和主机（IP地址）。这个扫描是轻量级的，并仅发出在日常的互联网流量中常见的请求。

作用

这些结果主要被Network Box SOC工程师用于配置审查过程中。它们是一致性检查的一部分，以确保配置正确地反映了客户策略。

Network Box安全响应工程师在处理新出现的漏洞时也会使用数据库。我们可以快速搜索受影响的服务，并确定所管理的网络中是否存在可从公共互联网访问的服务。

Network Box 扫描外部视图云服务已发布，并已在全球范围内投入运营。这些扫描的结果将在今年夏季在NBSIEM+的下一个版本中提供给客户。这是 Network Box 红队即将提供的几项服务中的第一项。

Network Box HIGHLIGHTS

Network Box 香港
富士胶片 - 网络安全研讨会

Network Box香港举办了一场研讨会，向富士胶片的员工介绍了Network Box的托管网络安全服务，最新的功能、认证、合规性和KPI报告能力。其他讨论主题包括MESH网络安全架构、风险管理、ISO 31000、In-Situ SIEM+、虚拟修补和其他关键技术，以保持对黑客、恶意软件和其他网络威胁的领先地位。

月刊主办	联系方式
Mark Webb-Johnson 主编 **Michael Gazeley** **Kevin Hla** 产品支持 **Network Box HQ** **Network Box USA** 贡献者	Network Box CNNOC cnnoc@network-box.cn 或者上门到: 深圳市福田区深南大道 竹子林求是大厦西座 920 +86 (755) 3336 1581 www.network-box.cn

Network Box 香港
香港数字金融协会 - IT活动

Network Box的董事总经理Michael Gazely受邀参加由香港数字金融协会举办的关于网络犯罪和网络安全的座谈会。在亚洲国际博览馆举行的此次活动中，Gazeley 先生与香港数码金融协会会长 Emil Chan、Kornerstone Institute 的 Catherine Chan、Baobab Tree Event 的 Culsin Li 以及香港警务处网络安全及科技罪案调查科的总督察 Lester Ip 共同参与了讨论。

全球安全头条

Bleeping Computer
Fortinet: 新的FortiOS RCE漏洞可能已被利用进行攻擊 LINK: https://tinyurl.com/3dvvy5dj

GB Hackers
谷歌浏览器零日漏洞被广泛利用
LINK: https://tinyurl.com/3a7hpfs8

Bleeping Computer
Barracuda鱼称必须立即更换被黑客攻击的 ESG 设备
LINK: https://tinyurl.com/2et9zhyy

Bleeping Computer
黑客宣称 DDoS 攻击，Outlook.com 遭到中断
LINK: https://tinyurl.com/3cunk8mv