Contribution ID: **38** Type: **分会报告**

网络边界安全威胁 IP 阻断技术

Sunday, 30 June 2024 15:45 (15 minutes)

伴随 Internet 网络的高速发展和不断扩大的网络应用，网络安全威胁屡见不鲜，只要是对外网开放服务的系统，每天都可能承受着成千上万次的尝试攻击，这些攻击可以造成网络性能下降，影响业务系统正常工作，甚至会成功地入侵，给系统造成破坏或损失。如何快速阻断和减少这类攻击，成为网络安全管理的一个重要问题。本文结合高能所网络安全管理的应用讲述了基于边界的安全威胁 IP 封锁方案和相关技术。

通过在网络数据通讯边界设备（防火墙或路由器）上配置访问策略，动态封锁或解封存在安全威胁的IP通讯；与网络安全

本系统部署在高能所网络运行，通过接收来自 SOC 威胁监测系统，Bro 入侵检测平台以及人工监测或情报收集发现的黑 IP 资源，快速封堵存在安全威胁的 IP 地址，给来自网络的黑客攻击增加了阻力。封锁过程中收集积累了大量 IP 地址，可作为网络安全威胁的情报资源。

基于边界路由器的有害 IP 地址封锁是局域网络安全的重要部分，利用静态路由表的封锁技术应用简单可靠，与在防火墙上封锁 IP 地址相比，性能开销要小的多，以高能所使用的华为路由器为例，可以封锁百万数量级的 IP 地址。

Primary author: Mr 安, 德海 (高能所)

Presenter: Mr 安, 德海 (高能所)

Session Classification: 科研信息化管理与系统