防火墙未检测到漏洞扫描行为案例分析

域间策略/安全域 攻击防范 IPS防攻击 **孔凡安** 3天前 发表

组网及说明

不涉及

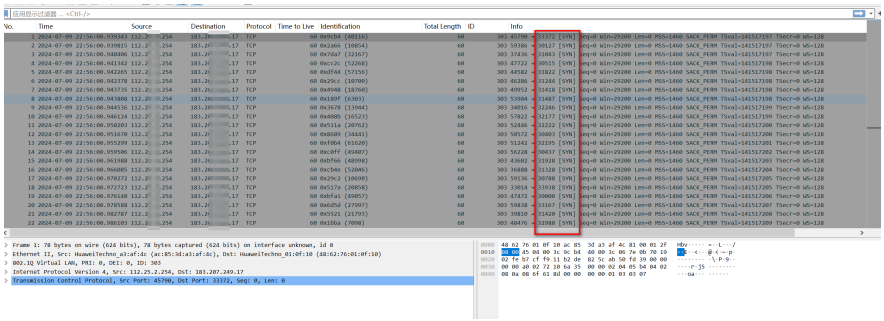
问题描述

防火墙旁挂部署，inline转发。漏扫的流量镜像到防火墙上做检测。

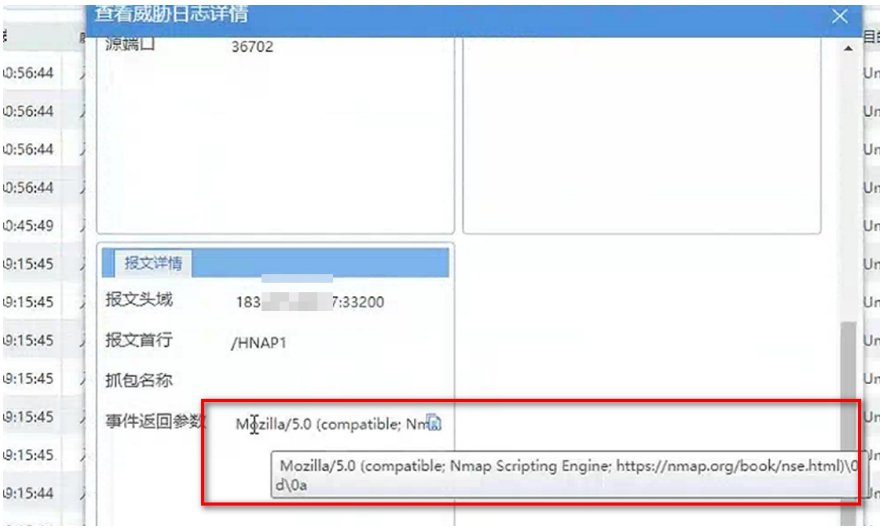
测试发现NMAP扫描可以产生威胁日志，但是某安全厂商（简称S）漏扫过程中没有产生任何日志。

过程分析

查看漏扫的流量，可以发现扫描工具先进行端口扫描，检测到存活端口后进行连接。



NMAP扫描工具连接存活端口的过程中有对应的特征被设备捕获到，可以正常产生威胁日志。如下：



但是某S厂商扫描过程中没有特征可以捕捉，导致无威胁日志产生。

解决方法

端口扫描行为没有明显特征被设备捕获，可以开启攻击防范模块里的端口扫描进行检测。

开启攻击防范策略后需要应用于接口或者安全域x

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入攻击防范策略视图。

attack-defense policy *policy-name*

(3) 开启指定级别的扫描攻击防范。

scan detect level { { **high** | **low** | **medium** } | **user-defined** { **port-scan-threshold** *thresh old-value* | **ip-sweep-threshold** *threshold-value* } * [**period** *period-value*] } **action** { { **blo ck-source** [**timeout** *minutes*] | **drop** } | **logging** } *

缺省情况下，扫描攻击防范处于关闭状态。