



EPS指纹采集的含义和应用场景

iMC EPS

马永鸿

2021-12-29 发表

问题描述

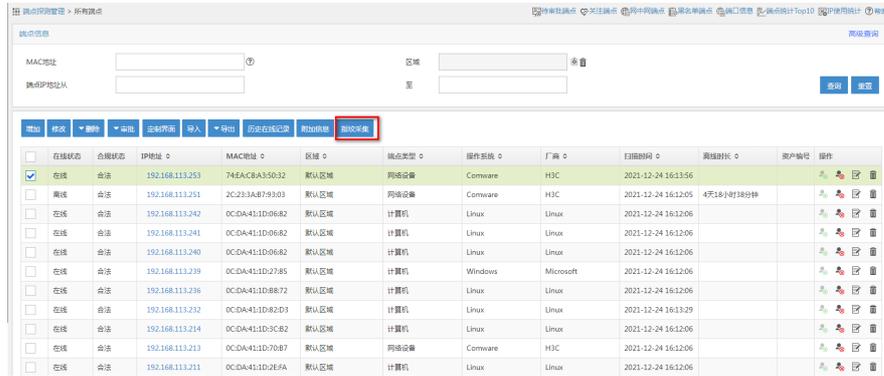
EPS指纹采集是什么意思？什么场景下可以应用？

解决方法

鹰视扫描器对终端的信息识别，基本原理是通过对终端各通信端口进行扫描，然后对回应报文进行七层分析，基于预定义的终端指纹，进行报文匹配，从而识别出终端的操作系统、厂商和类型等信息。而对于某些类型终端（例如IP电话等哑终端），只能通过有限端口获取到少量数据，就可尝试应用指纹采集。当采集到未知设备的信息时，应用指纹采集，就会将这种终端类型和已经定义的指纹绑定。

指纹采集实际上就是“自定义”。就是在预定义的指纹库中没有的设备类型，我们先自定义个类型，然后扫描已知的设备从而获得设备的指纹，将这种终端类型和已经定义的指纹绑定。等下次再扫描就可以识别出了。

如图所示，勾选扫描出的端点，点击“指纹采集”即可。



The screenshot shows the Eagle Eye scanning interface. At the top, there are search filters for MAC address and IP address. Below that is a table of scanned endpoints. The 'Fingerprint Collection' button is highlighted in red. The table contains the following data:

在线	在线状态	IP地址	MAC地址	区域	端点类型	操作系统	厂商	扫描时间	关联时长	用户输入	操作	
<input checked="" type="checkbox"/>	在线	合法	192.168.113.253	74EAC8A35032	默认区域	网络设备	Comware	H3C	2021-12-24 16:13:56			指纹采集
<input type="checkbox"/>	离线	合法	192.168.113.251	2C233A879303	默认区域	网络设备	Comware	H3C	2021-12-24 16:12:05	4天18小时18分钟		指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.242	0C-DA41D-0682	默认区域	计算机	Linux	Linux	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.241	0C-DA41D-0682	默认区域	计算机	Linux	Linux	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.240	0C-DA41D-0682	默认区域	计算机	Linux	Linux	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.239	0C-DA41D-0785	默认区域	计算机	Windows	Microsoft	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.236	0C-DA41D-8872	默认区域	计算机	Linux	Linux	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.232	0C-DA41D-882D3	默认区域	计算机	Linux	Linux	2021-12-24 16:13:29			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.214	0C-DA41D-3C-B2	默认区域	计算机	Linux	Linux	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.213	0C-DA41D-7087	默认区域	网络设备	Comware	H3C	2021-12-24 16:12:06			指纹采集
<input type="checkbox"/>	在线	合法	192.168.113.211	0C-DA41D-2E5A	默认区域	计算机	Linux	Linux	2021-12-24 16:12:06			指纹采集

