Nmap及漏洞扫描实践

姓名：任宇 学号：33920212204567

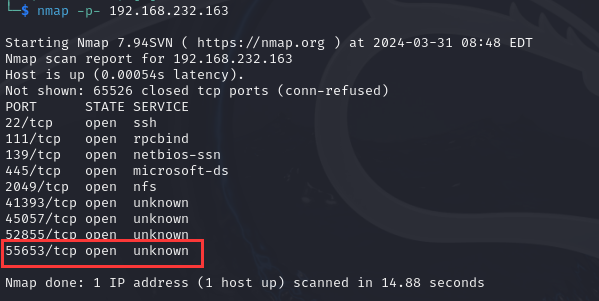
1. Nmap扫描实践

实践任务：使用Nmap开源软件对某本地靶机环境（Ubuntu18.04，IP地址为192.168.232.163）进行扫描，回答如下问题并给出操作命令：

1. 开启的最大TCP端口号是多少？

要找出开启的最大TCP端口号，可以扫描所有65535个端口，然后观察结果中最大的端口号。命令为：

nmap -p- 目标IP

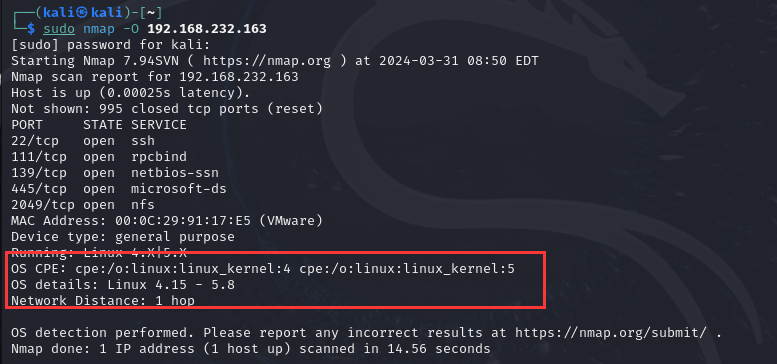


可见最大TCP端口号为55653

1. 操作系统和版本是多少（格式：类型 大版本号.中版本号.X）？

Nmap提供了一个功能强大的操作系统检测功能，通过分析响应来猜测目标操作系统类型和版本。命令为：

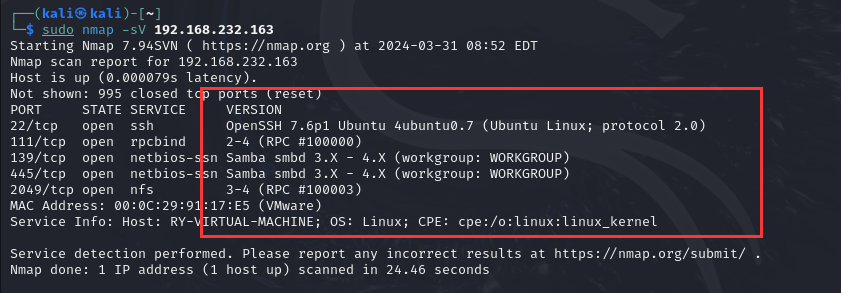
nmap -O 目标IP



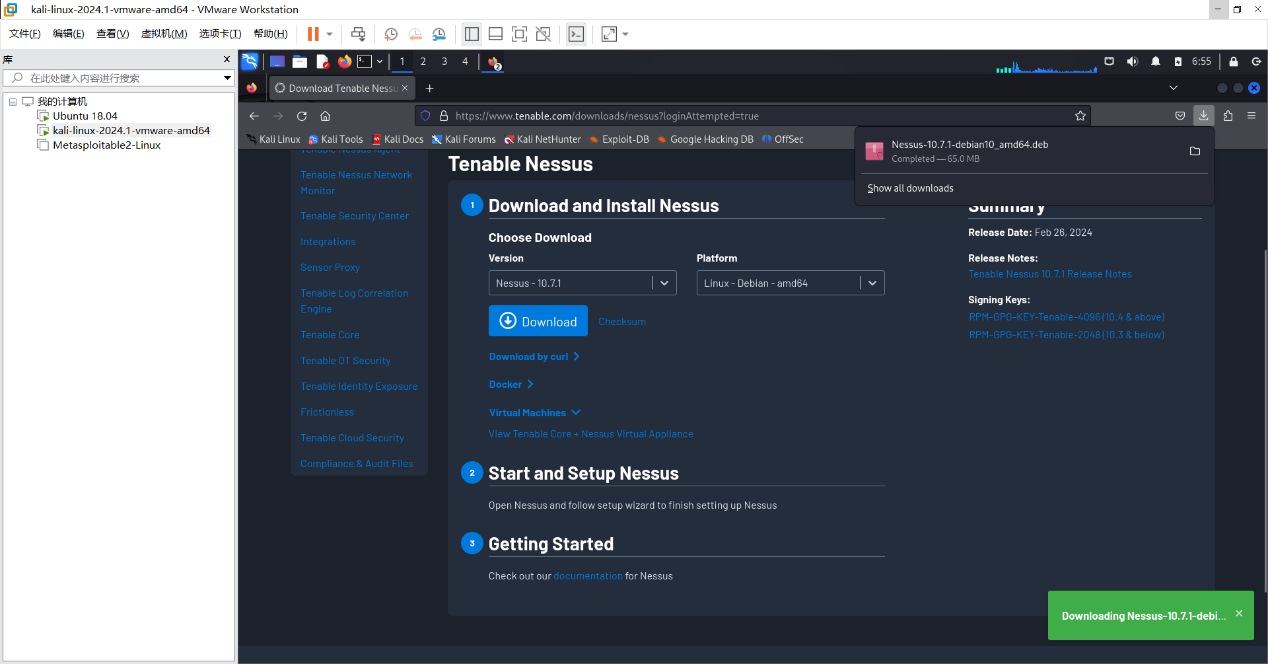
1. 包含的网络服务及其版本号是多少？

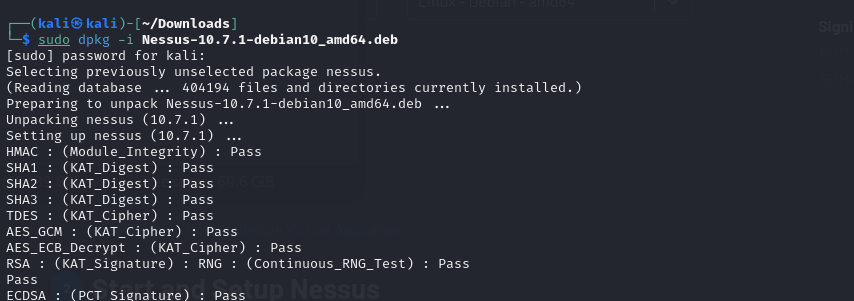
要识别开放端口上运行的服务及其版本号，可以使用Nmap的服务版本探测功能。命令为：

nmap -sV 目标IP

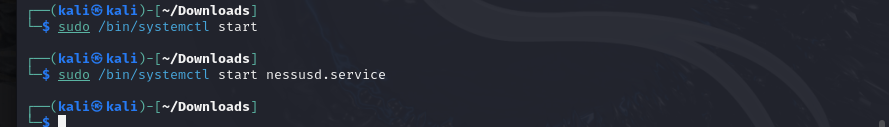
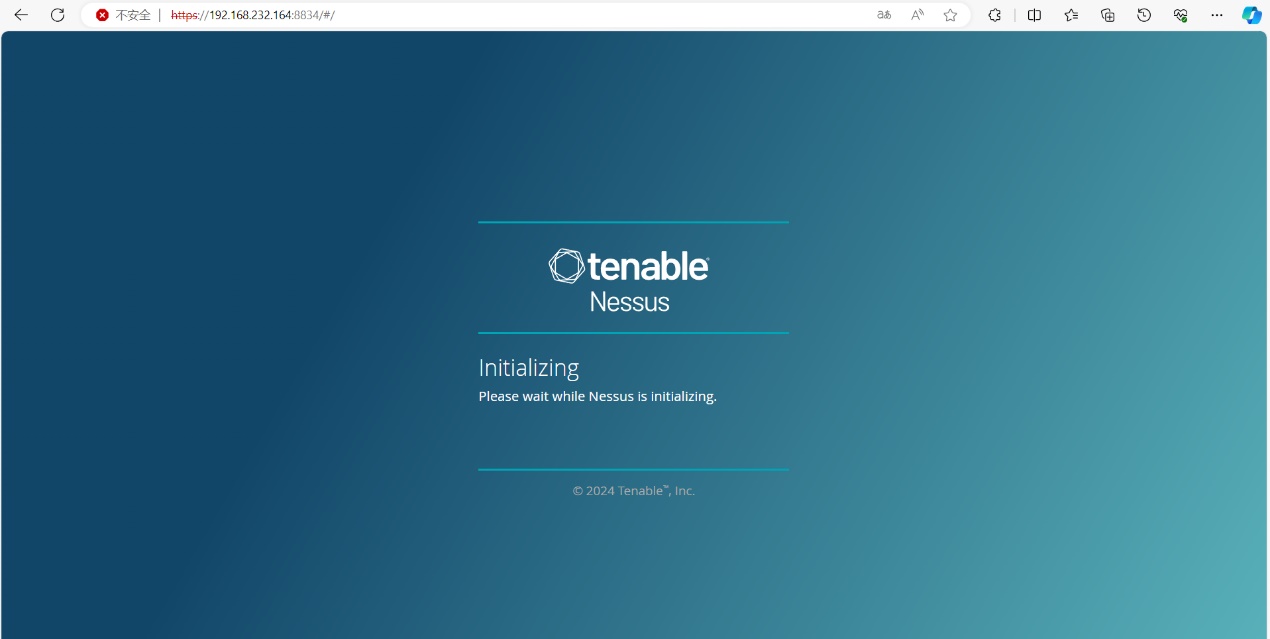


1. Nessus扫描实践
2. 安装Nessus

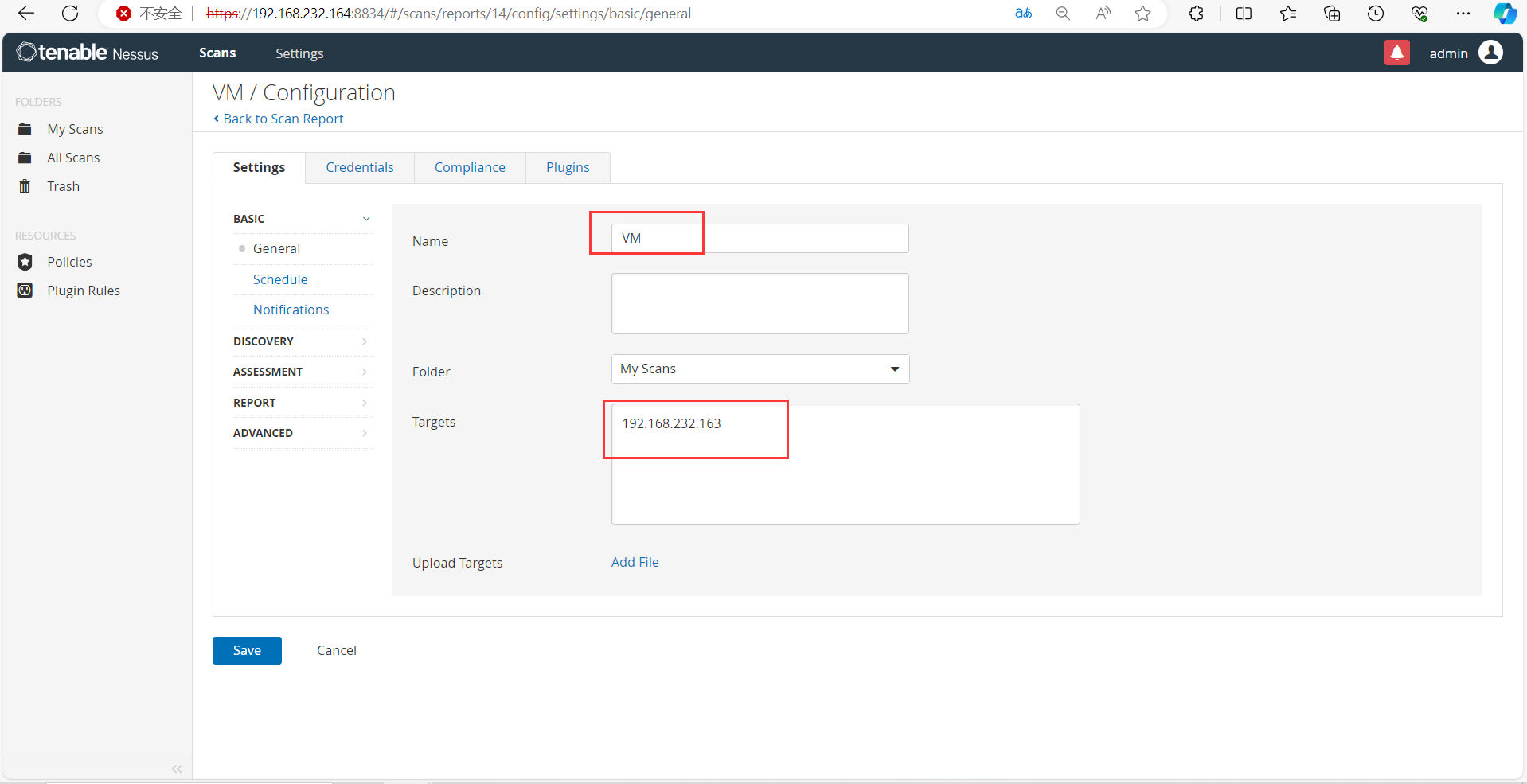




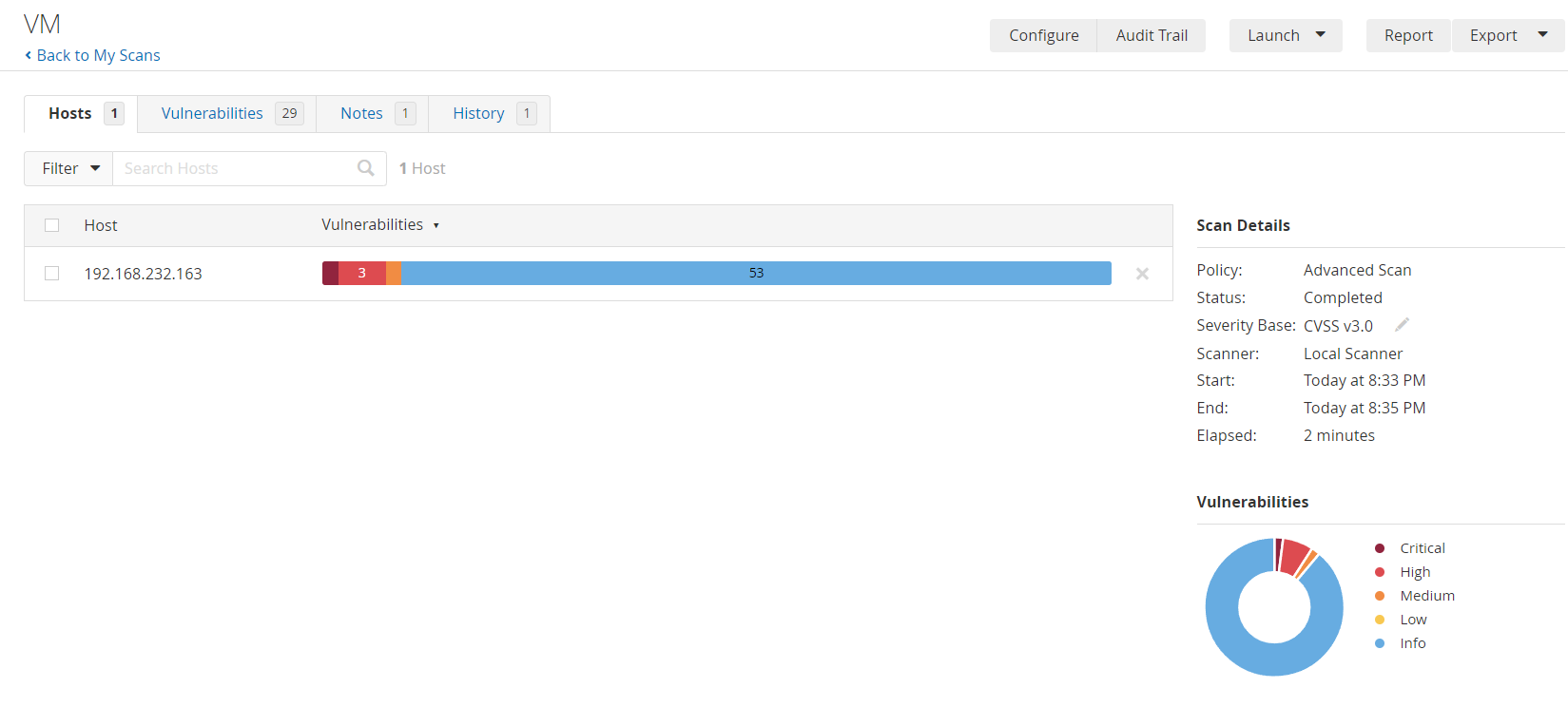
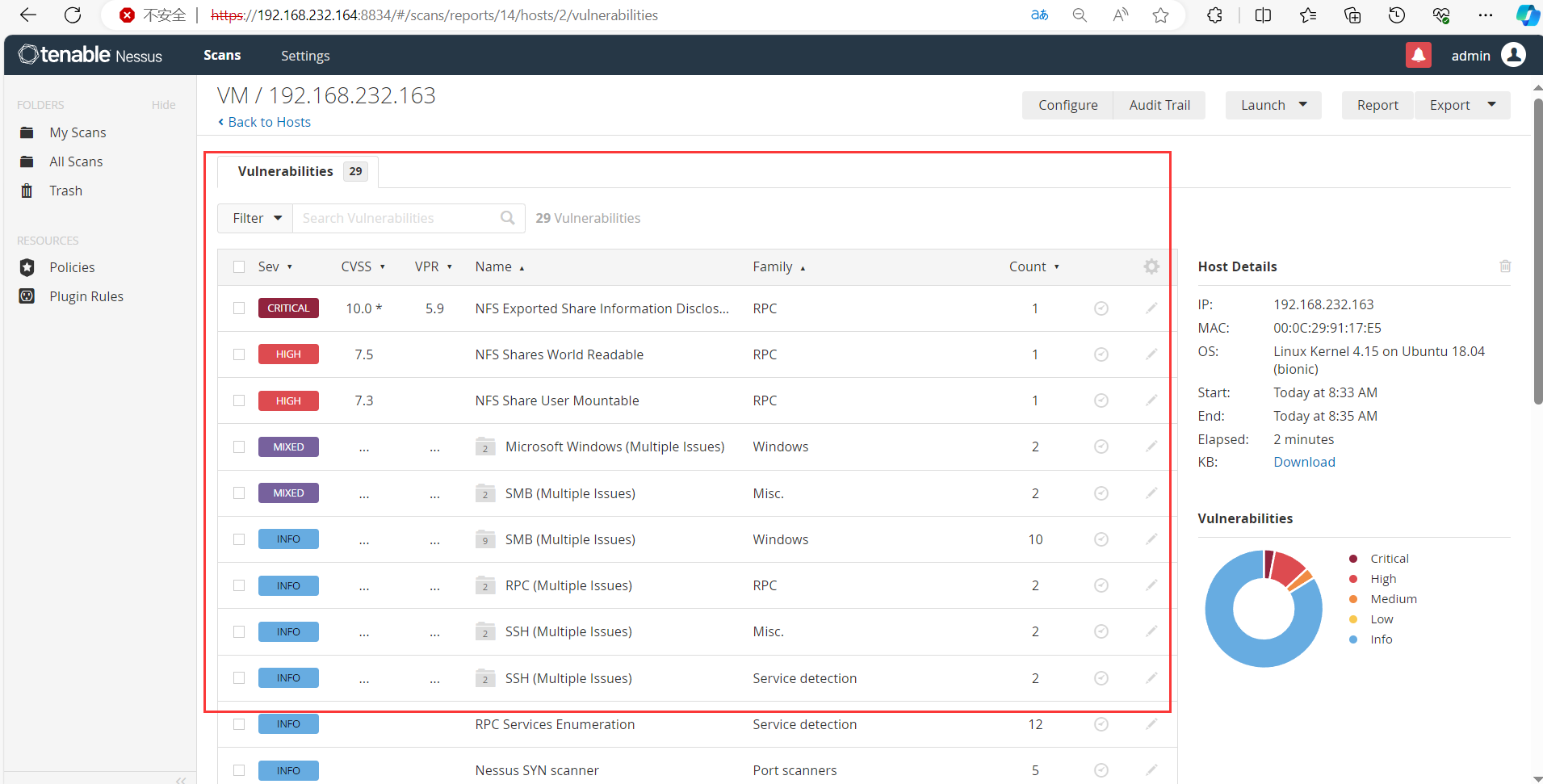
1. 在Kali虚拟机上启动Nessus服务，并在主机上登录：

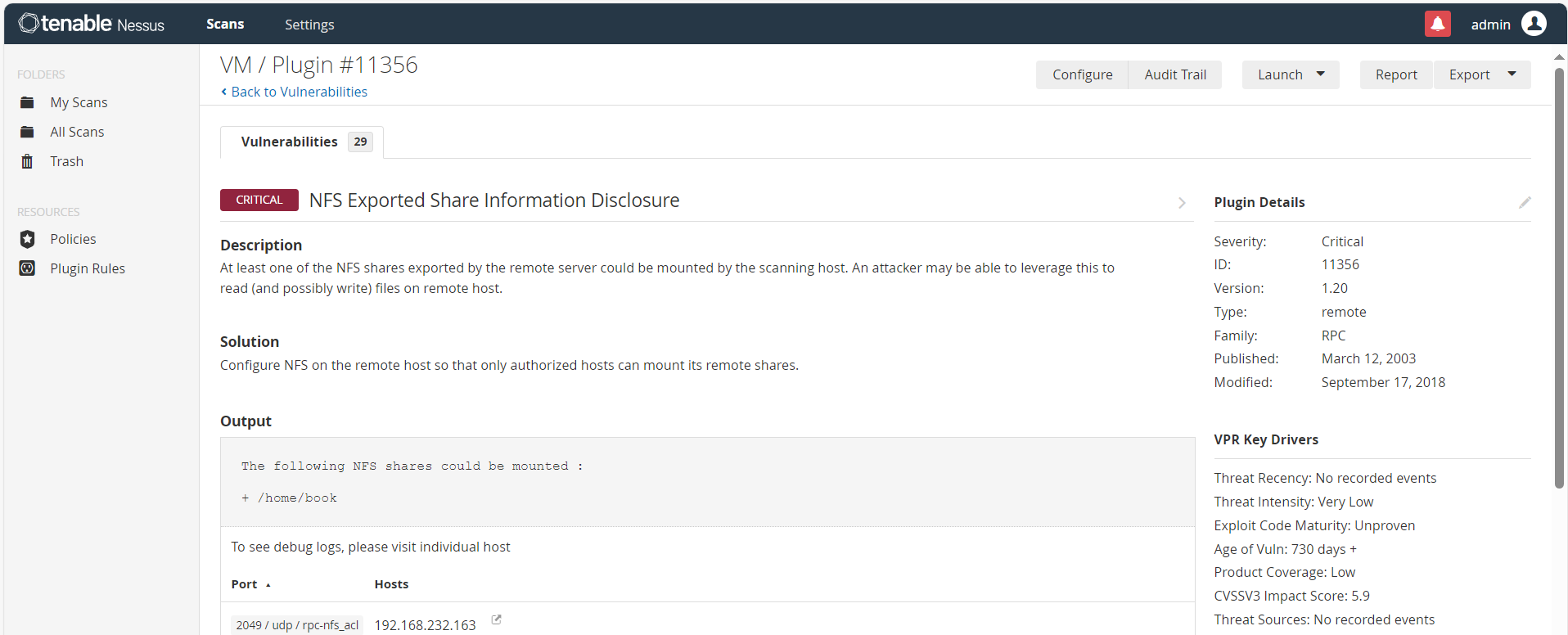
1. 使用Nessus扫描靶机漏洞



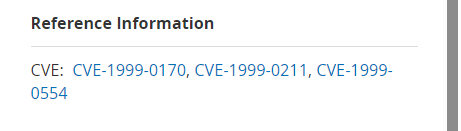
结果如下

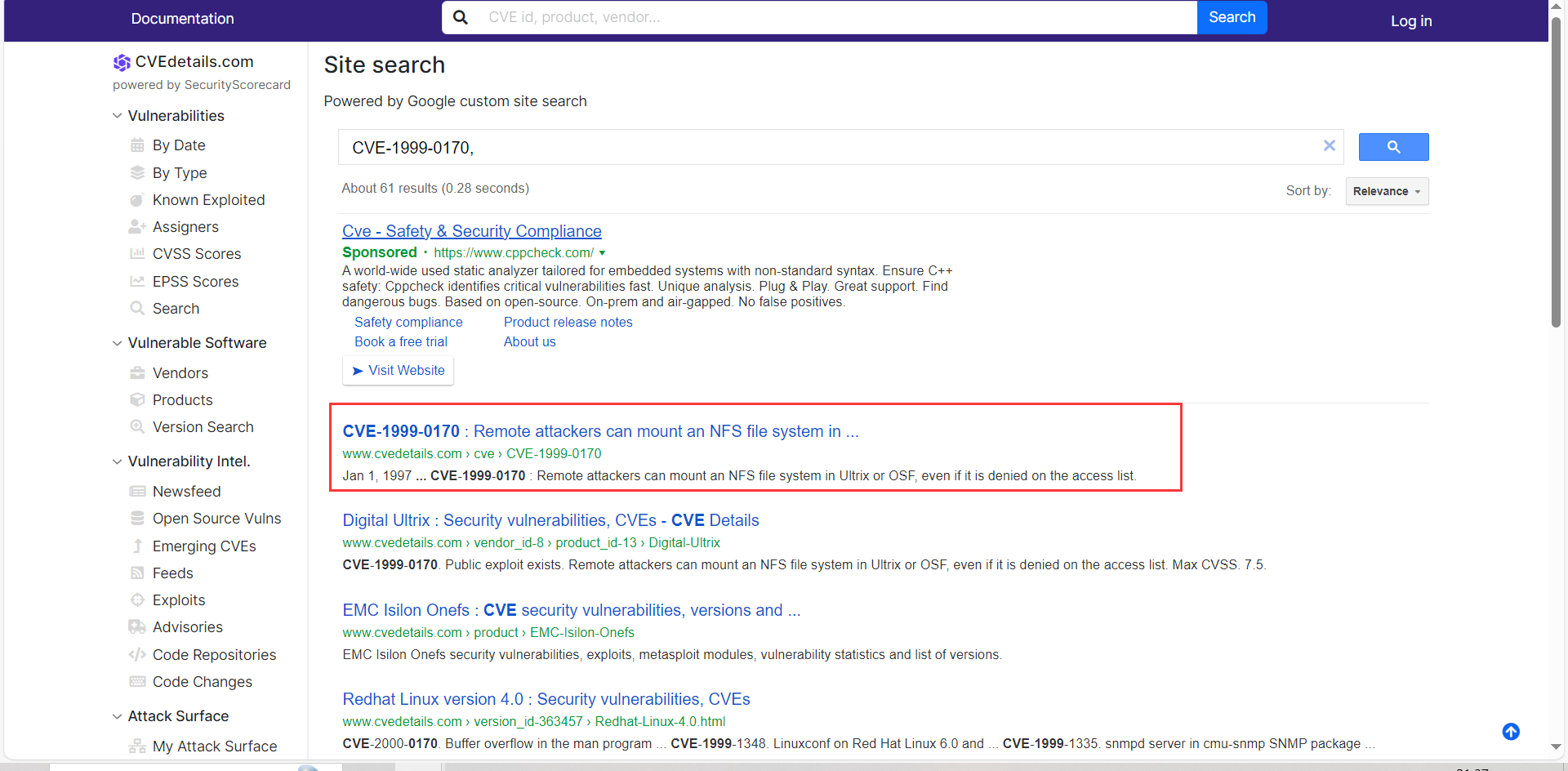
1. 选择漏洞NFS Exported Share Information Disclosure，搜索其PoC验证

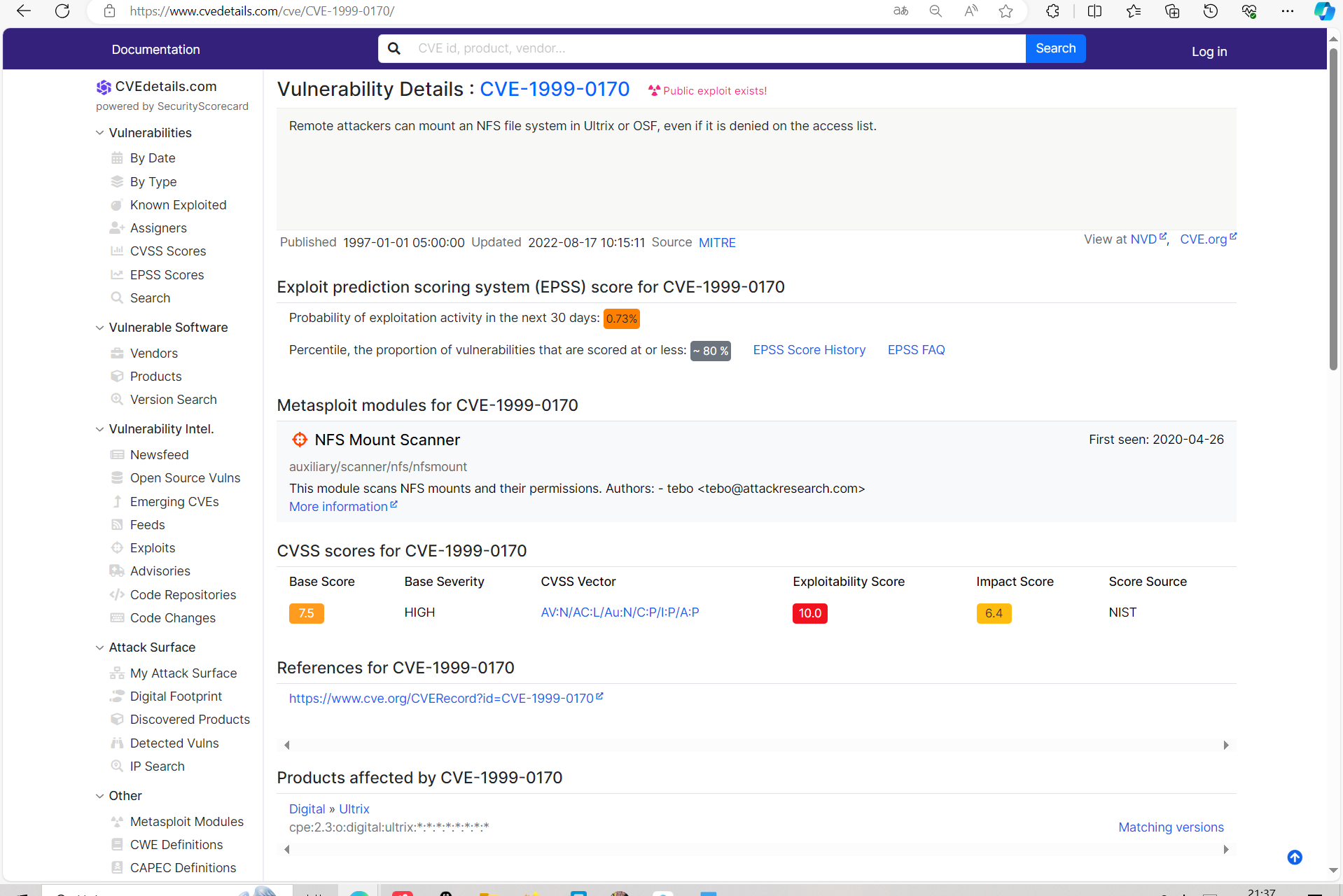


查看其对应CVE编号



使用CVE Details网站进行搜索





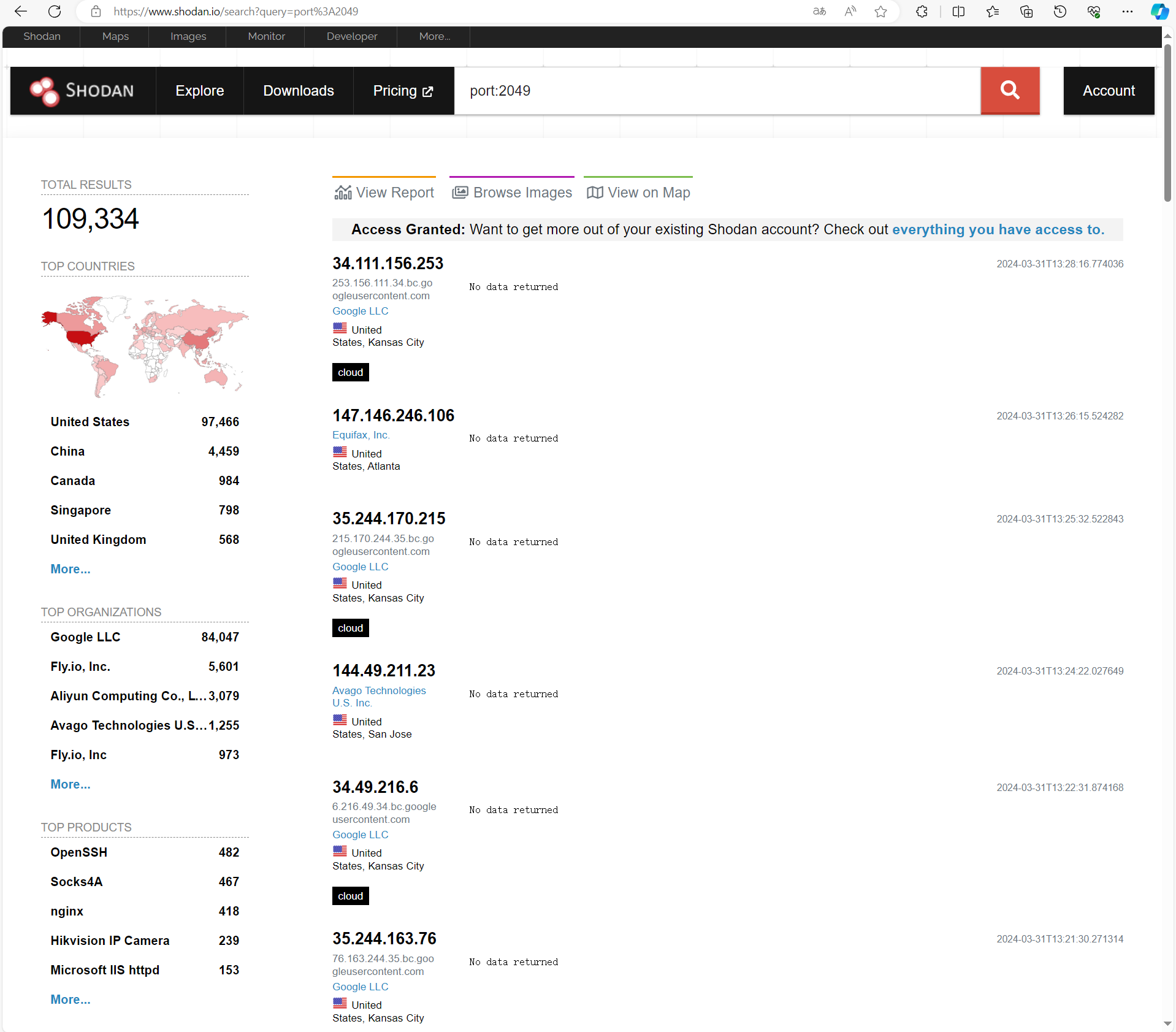
根据漏洞描述可知，这个漏洞允许远程攻击者可以在Ultrix或OSF中挂载NFS文件系统，即使其不在访问列表中。

搜索该漏洞的POC验证



1. 使用Shodan测绘包含相同漏洞的网络资产信息（节选部分）

Shodan的索引基于互联网上的实际服务和设备特征，有效的方法是使用与CVE相关的关键信息进行搜索，比如受影响的应用名称、版本号、具体的协议或服务等。因此过滤出开放2049端口（NFS服务默认端口）的网络资产。



可以查看中国地区的。

