网络嗅探攻防实践报告

姓名：任宇 学号：33920212204567

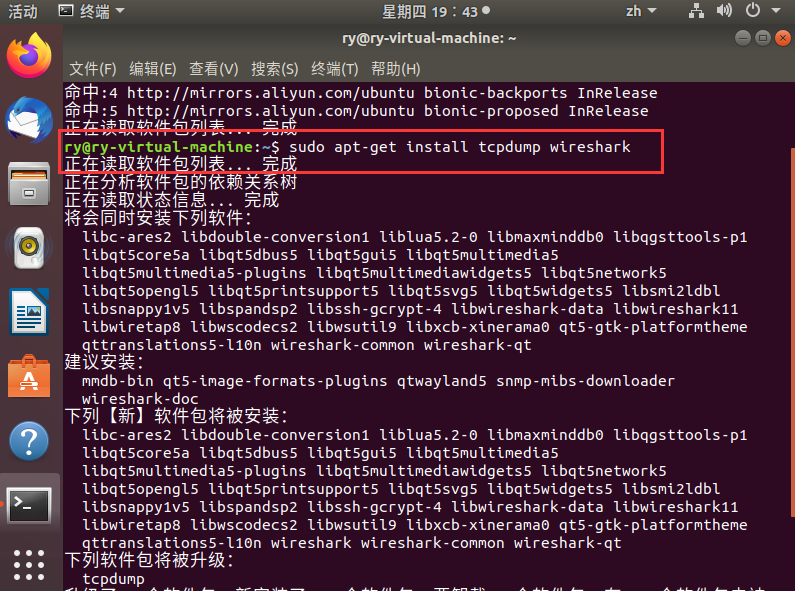
1. 实践题目

攻击方用nmap扫描（达到特定目的），防守方tcpdump嗅探，用wireshark分析，并分析出攻击方的扫描目的以及每次扫描使用的nmap命令。

1. 实践环境

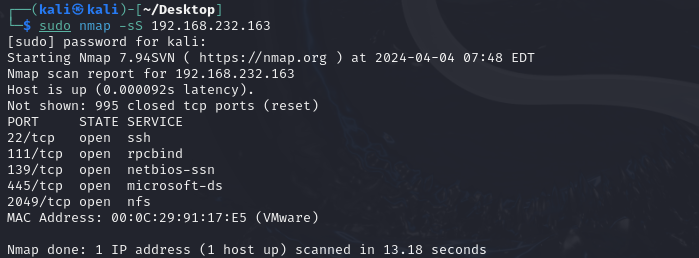
此次实践在虚拟机环境下进行，攻击方为Kali系统，而防守方系统版本为Ubuntu18.04。

1. 实践步骤
2. 首先在Ubuntu18.04上安装tcpdump和wireshark。



1. 在攻击方上用nmap扫描，以达到特定目的。

此处以nmap -sS 命令为例，SYN扫描的主要目的是快速且隐秘地确定目标机器上哪些端口是开放的。它被称为“半开放扫描”是因为它从不完成TCP的三次握手过程。扫描者发送一个SYN包到目标端口，如果收到一个SYN-ACK包（表示端口开放并准备建立连接），扫描者不会发送最终的ACK包来完成连接的建立，而是发送一个RST包。这样做可以避免在目标系统日志中留下明显的痕迹。



1. 防守方使用tcpdump嗅探并保存抓取到的网络包。

如果知道攻击方的IP地址，可以使用：

sudo tcpdump ip host <攻击方IP> -w capture.pcap

这将捕获所有来自和发往攻击方IP地址的包，并将它们保存到capture.pcap文件中，之后可以使用Wireshark进行分析。

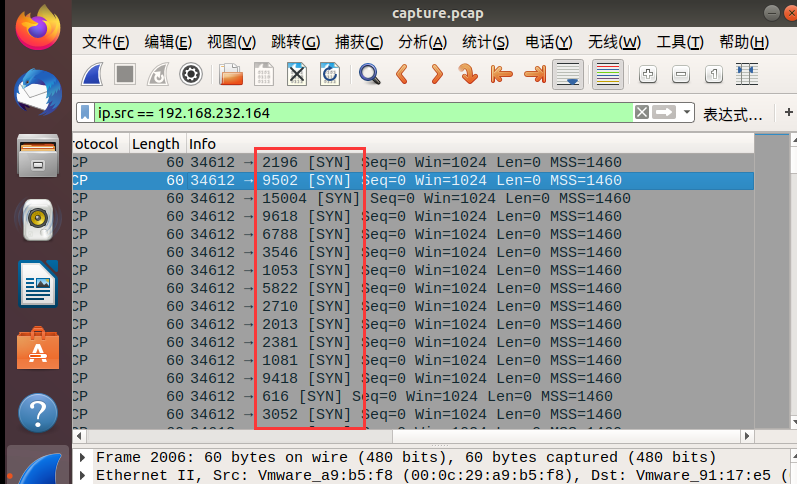
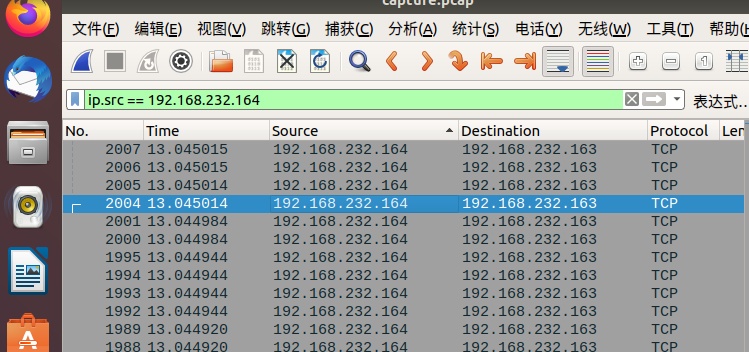


1. 防守方使用wireshark分析攻击方的扫描目的和使用的命令。

使用wireshark打开第四步中抓取的capture.pcap文件，并进行分析。

可以发现，捕获的数据包主要是TCP并带有SYN标志位而没有ACK标志

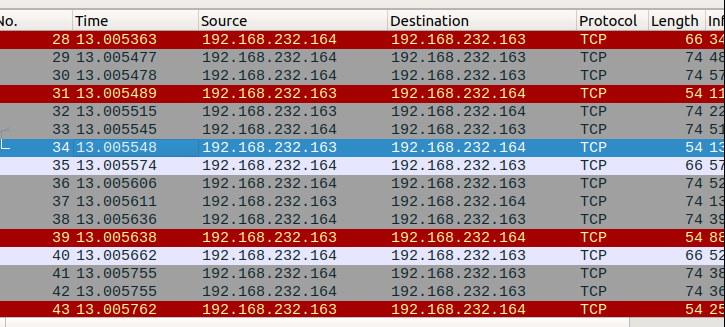
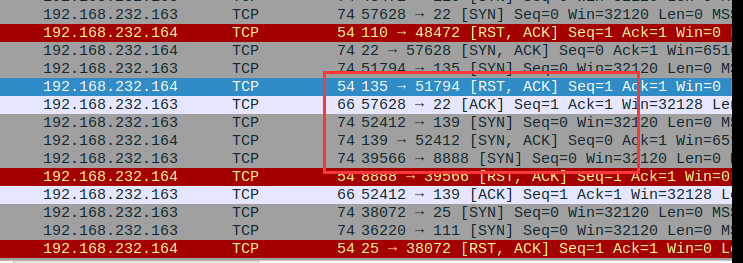
位，可以判定为攻击方进行的是SYN扫描，其命令为nmap -sS。



1. 其他命令

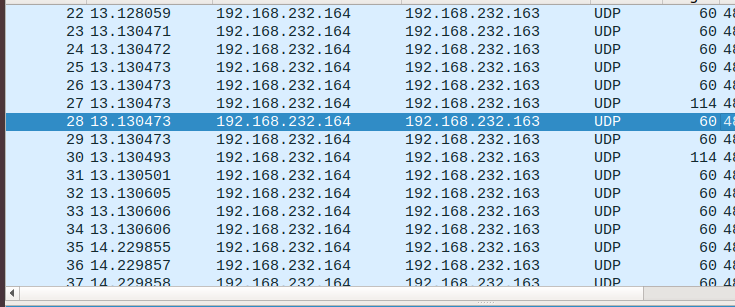
对于其他常见nmap命令，如果数据包有以下特征也可以进行判断。

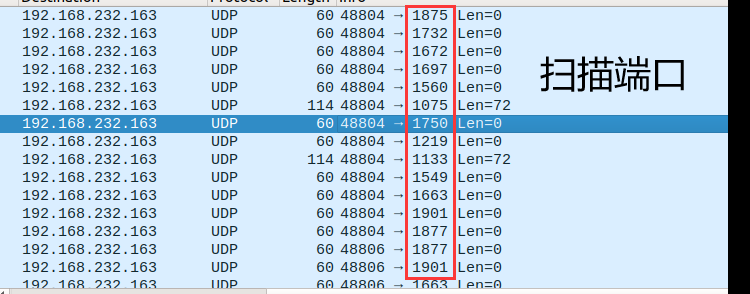
* 全连接扫描 (nmap -sT): 如果数据包完成了TCP的三次握手（SYN, SYN-ACK, ACK），这表明进行了全连接扫描。

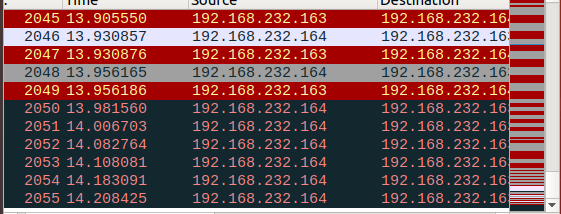
* UDP扫描 (nmap -sU): 如果捕获的是UDP数据包，特别是针对特定端口的，这表明进行了UDP扫描。

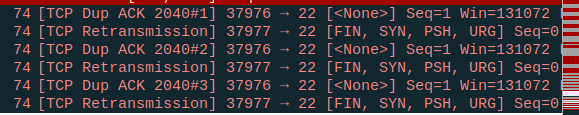




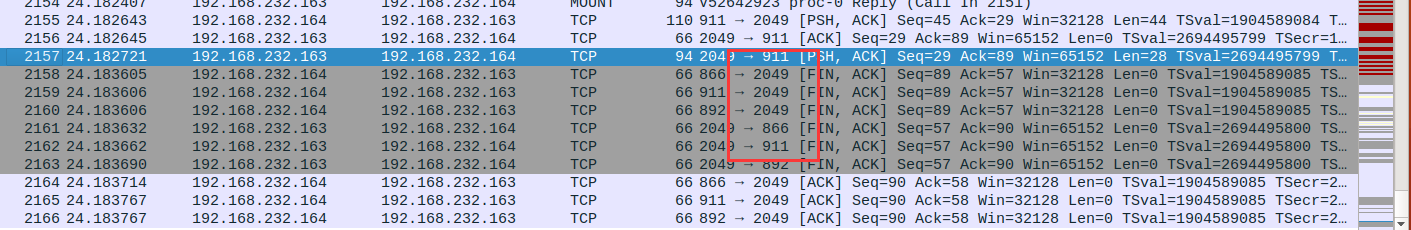
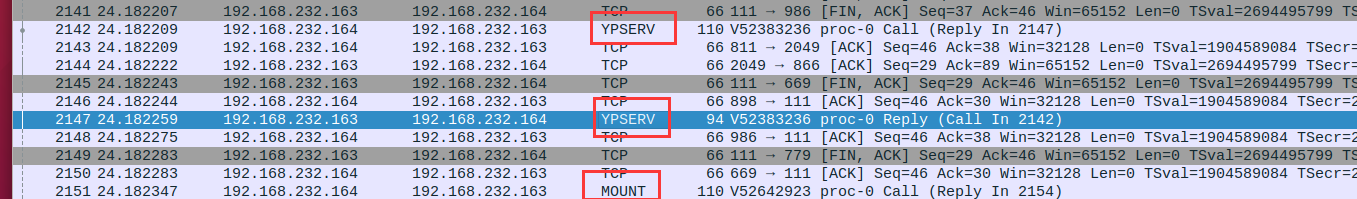
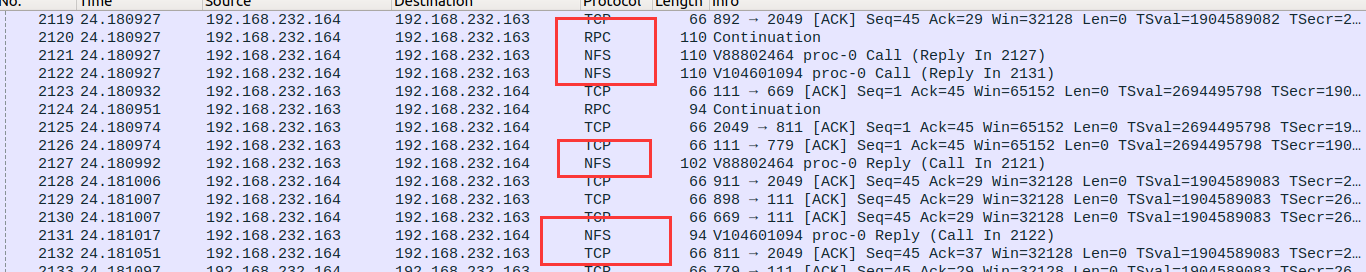


* 操作系统检测 (nmap -O): 包含多个不同的TCP或UDP端口的扫描，并伴随特定的TCP标志位组合或者特殊的TCP选项，可能是进行操作系统检测。





* 服务版本检测 (nmap -sV): 如果捕获的数据包显示尝试与多个服务建立连接并发送特定于应用层协议的数据，这可能是服务版本检测。

1. 实践总结

通过这次实践，我学习了如何使用nmap进行不同类型的网络扫描，并利用tcpdump和Wireshark对网络流量进行捕获和分析。通过分析捕获的数据包，防守方能够识别出攻击方使用的nmap命令及其扫描目的，例如通过ACK标志位的存在与否来区分是SYN扫描还是全连接扫描，或通过数据包类型判断是进行了UDP扫描、操作系统检测，还是服务版本检测。这次实践加深了我对网络扫描技术的理解，并提高了我分析和防御此类扫描的能力。