nmap

主机探测方式：各种响应包

1. ICMP echo request

2. a TCP SYN packet to port 443

3. a TCP ACK packet to port 80

4. an ICMP timestamp request

使用wireshark抓包观察主机发现过程

端口扫描：6种状态

开关屏蔽 不确定

TCP SYN scanning TCP connect scanning TCP ACK scanning

TCP FIN/Xmas/NULL scanning

UDP scanning

版本侦测：

首先检查open与open|filtered状态的端口是否在排除端口列表内。如果在排除列表，将该端口剔除。

如果是TCP端口，尝试建立TCP连接。尝试等待片刻（通常6秒或更多，具体时间可以查询文件nmap-services-probes中Probe TCP NULL q||对应的totalwaitms）。通常在等待时间内，会接收到目标机发送的“WelcomeBanner”信息。nmap将接收到的Banner与nmap-services-probes中NULL probe中的签名进行对比。查找对应应用程序的名字与版本信息。

如果通过“Welcome Banner”无法确定应用程序版本，那么nmap再尝试发送其他的探测包（即从nmap-services-probes中挑选合适的probe），将probe得到回复包与数据库中的签名进行对比。如果反复探测都无法得出具体应用，那么打印出应用返回报文，让用户自行进一步判定。

如果是UDP端口，那么直接使用nmap-services-probes中探测包进行探测匹配。根据结果对比分析出UDP应用服务类型。

如果探测到应用程序是SSL，那么调用openSSL进一步的侦查运行在SSL之上的具体的应用类型。

如果探测到应用程序是SunRPC，那么调用brute-force RPC grinder进一步探测具体服务。

防火墙/IDS规避：

分片（Fragmentation）

将可疑的探测包进行分片处理（例如将TCP包拆分成多个IP包发送过去），某些简单的防火墙为了加快处理速度可能不会进行重组检查，以此避开其检查。

IP诱骗（IP decoys）

在进行扫描时，将真实IP地址和其他主机的IP地址（其他主机需要在线，否则目标主机将回复大量数据包到不存在的主机，从而实质构成了拒绝服务攻击）混合使用，以此让目标主机的防火墙或IDS追踪检查大量的不同IP地址的数据包，降低其追查到自身的概率。注意，某些高级的IDS系统通过统计分析仍然可以追踪出扫描者真实IP地址。

IP伪装（IP Spoofing）

顾名思义，IP伪装即将自己发送的数据包中的IP地址伪装成其他主机的地址，从而目标机认为是其他主机在与之通信。需要注意，如果希望接收到目标主机的回复包，那么伪装的IP需要位于统一局域网内。另外，如果既希望隐蔽自己的IP地址，又希望收到目标主机的回复包，那么可以尝试使用idle scan或匿名代理（如TOR）等网络技术。

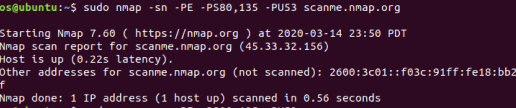
指定源端口

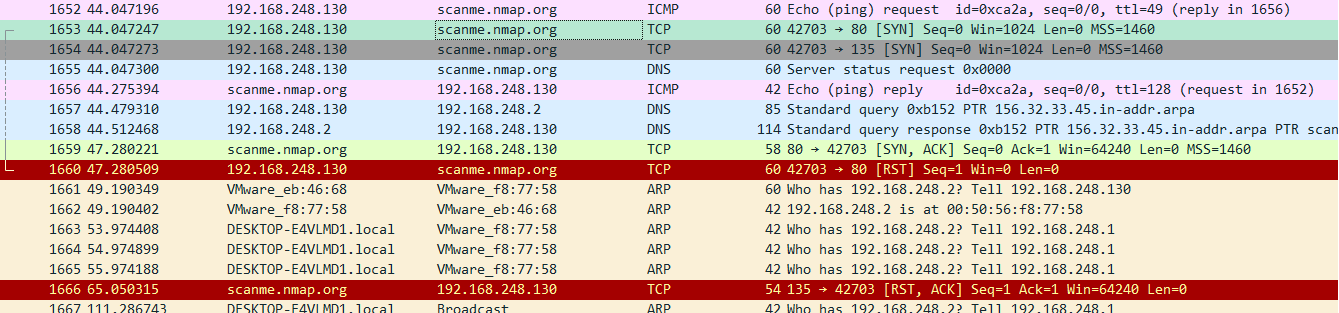
某些目标主机只允许来自特定端口的数据包通过防火墙。例如FTP服务器配置为：允许源端口为21号的TCP包通过防火墙与FTP服务端通信，但是源端口为其他端口的数据包被屏蔽。所以，在此类情况下，可以指定Nmap将发送的数据包的源端口都设置特定的端口。

扫描延时

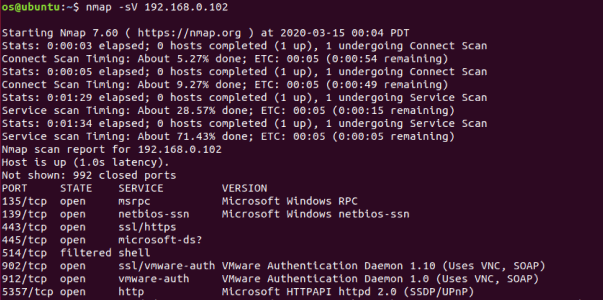
某些防火墙针对发送过于频繁的数据包会进行严格的侦查，而且某些系统限制错误报文产生的频率（例如，Solaris 系统通常会限制每秒钟只能产生一个ICMP消息回复给UDP扫描），所以，定制该情况下发包的频率和发包延时可以降低目标主机的审查强度、节省网络带宽。

主机发现实例，使用wireshark抓包





版本检测实例：



3.15进度：使用kali容器安装了webploit、nmap、SQLmap工具，尝试使用了nmap和SQLmap。学习使用脚本来代替手动扫描。