2016 年 4 月 17 日星期日

本周汇报工作

1. 本周任务：

   给定一个 IP 地址或者一个子网络，扫描该台主机上的端口是否开启，每个开启的端口上运行的什么服务应用及应用版本，检测主机上正在运行的是什么操作系统。这部分工作是主机渗透与入侵的第一步，通过对开启的某个端口进行漏洞侦查，从而继续渗透工作。

2. 使用工具介绍

   使用工具为 Nmap（Network Mapper），使用这个开源的工具可以完成主机发现，端口扫描，版本检测以及操作系统检测等功能。

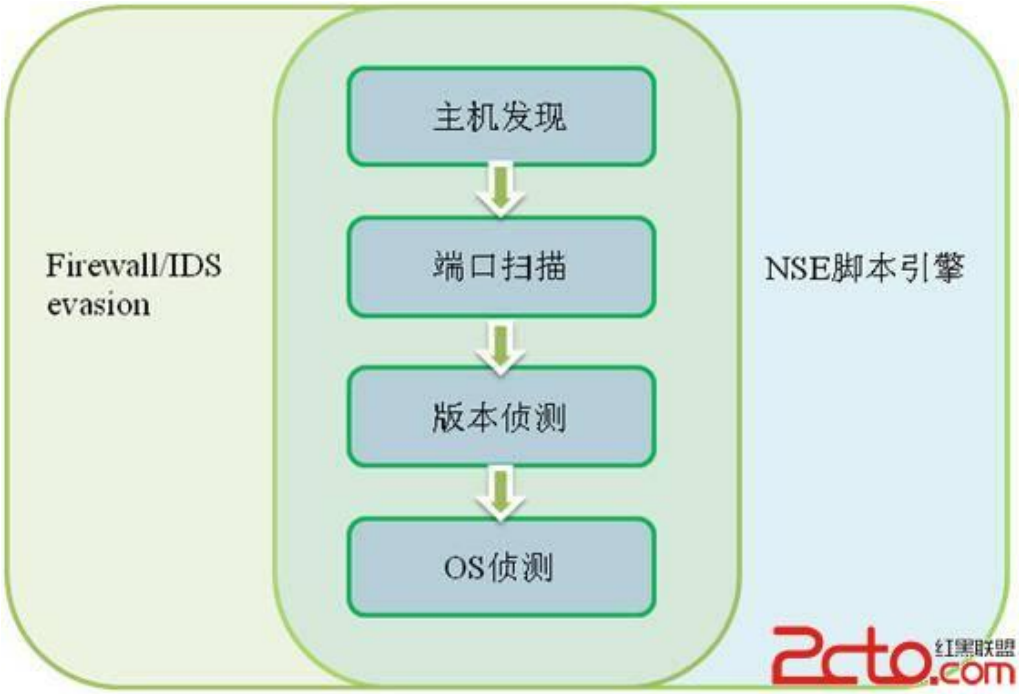


图 1 Nmap 的功能架构图

3. 怎么完成主机扫描

   主机扫描可分为四个步骤：

   一． 主机发现原理：

主机发现（Host Discovery）,即用来发现目标主机是否在线。主机发现的原理与 Ping 命令相似，发送探测包到目标主机，如果收到回复，那么说明目标主机时开启的。探测包是多种多样的，比如发送 ICMP ECHO/TIMESTAMP/NETMASK 报文、发送 TCPSYN/ACK 包、发送 SCTP INIT/COOLIE-ECHO 包。

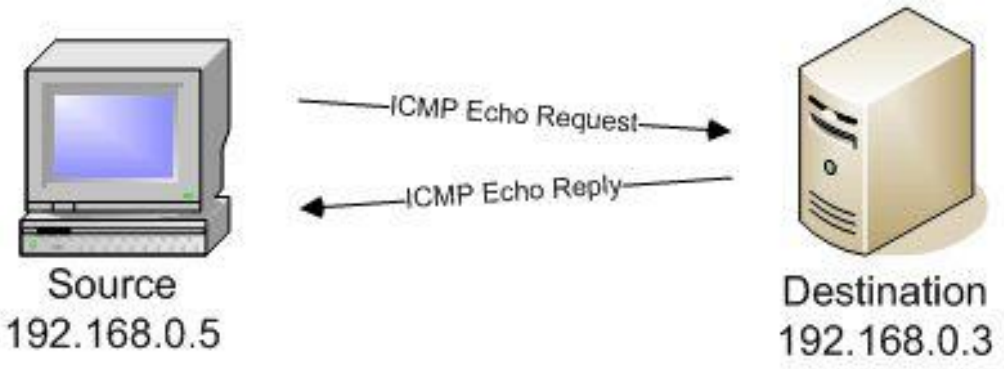


图2 主机发现基本原理（以 ICMP ECHO 为例）

在进行主机发现的时候可以发送多个类型的数据包，只要一个受到回复证明主机开启。使用多种类型的数据包可以避免防火墙或丢包造成的判断错误。

nmap –sn target

nmap –Pn target

二． 端口扫描原理：

端口扫描是整个主机扫描中最核心的功能，用于确定目标主机的 TCP/UDP 的端口的开放情况。Nmap 提供的端口扫描有十几种不同的扫描方法：

1.TCP connect scanning:

TCP connect 方式使用系统网络 API connect 向目标主机的端口发起连接，如果无法连接，说明该端口关闭。该方式扫描速度比较慢，而且由于建立完整的 TCP 连接会在目标机上留下记录信息，不够隐蔽。所以，TCP connect 是 TCP SYN 无法使用才考虑选择的方式。

nmap –sT target

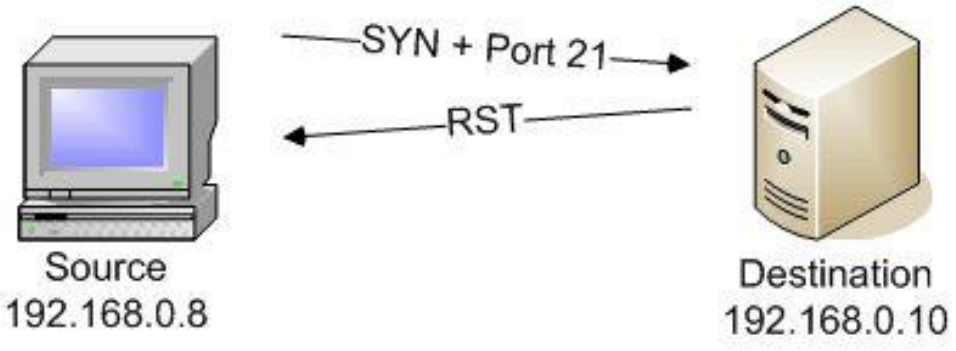


图3 tcp connect 检测到端口关闭

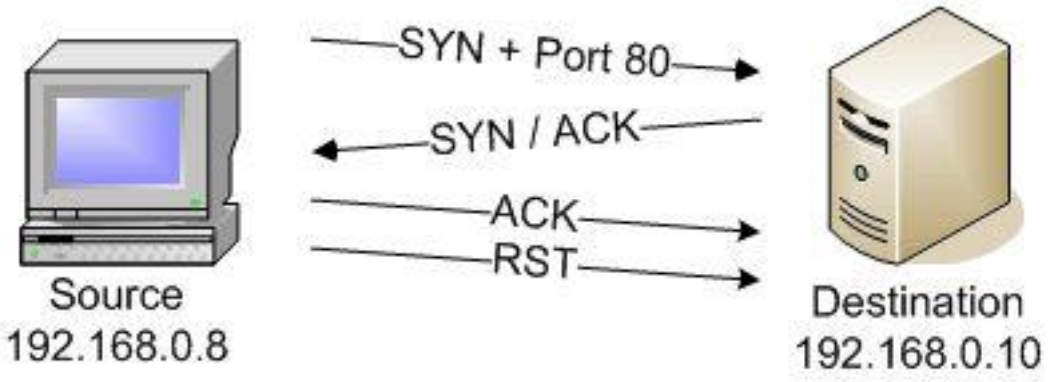


图4 Tcp connect 检测到端口打开

2.TCP SYN scanning：这是 Nmap 默认的扫描方式，通常被称作半开放扫描（Half-open scanning）。该方式发送 SYN 到目标端口，如果收到 SYN/ACK 回复，那么判断端口是开放的；如果收到 RST 包，说明该端口是关闭的。如果没有收到回复，那么判断该端口被屏蔽（Filtered）。

nmap –sS target

3.TCP ACK scanning：

向目标主机的端口发送 ACK 包，如果收到 RST 包，说明该端口没有被防火墙屏蔽；没有收到 RST 包，说明被屏蔽。该方式只能用于确定防火墙是否屏蔽某个端口，可以辅助 TCP SYN 的方式来判断目标主机防火墙的状况。

nmap –sA target

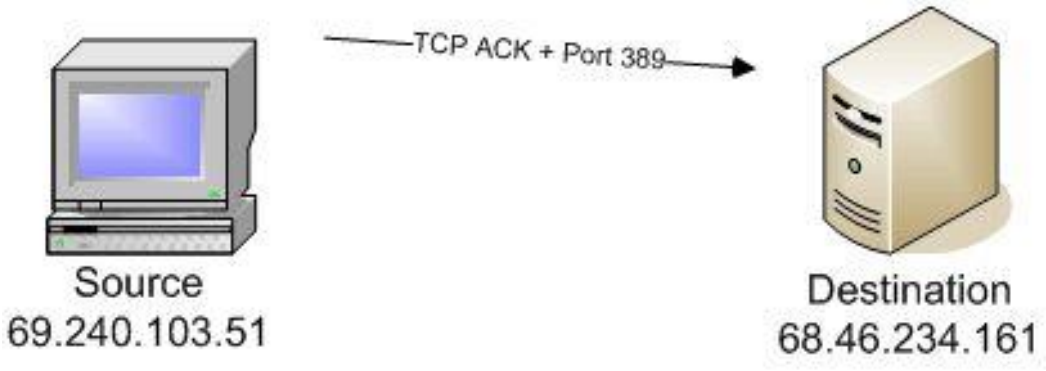


图 5 TCP ACK 监测到端口被屏蔽

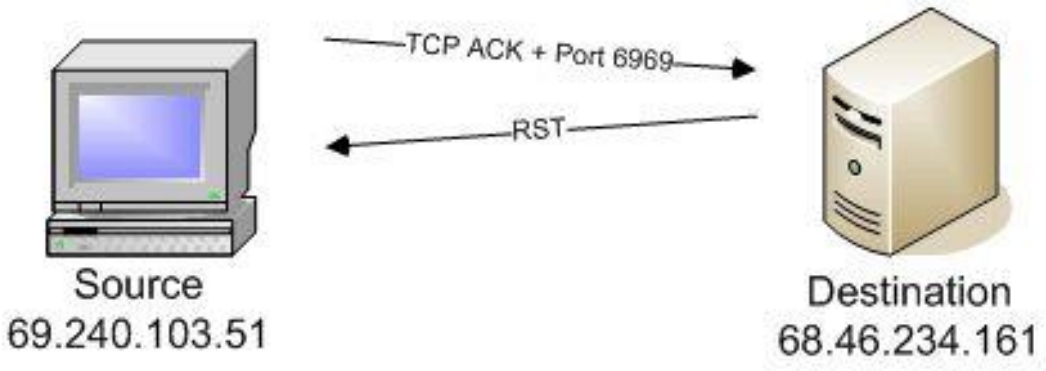


图 6 TCP ACK 检测到端口未被屏蔽

4.TCP FIN/Xmas/NULL scanning:

这三种扫描方式被称为秘密扫描（Stealthy Scan），因为相对比较隐蔽。FIN 扫描向目标主机的端口发送的 TCP FIN 包或 Xmas tree 包/Null 包，如果收到对方 RST 回复包，那么说明该端口是关闭的；没有收到 RST 包说明端口可能是开放的或被屏蔽的（open|filtered）。

nmap –sN/sF/sX target

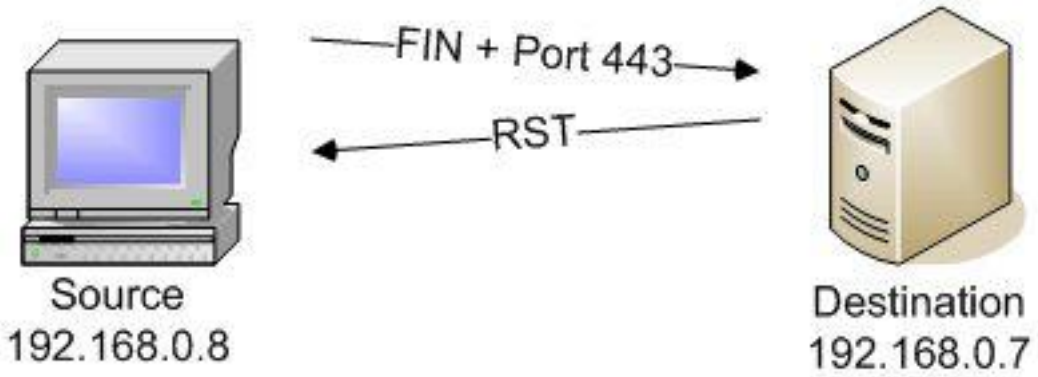


图 7 TCP FIN 探测主机端口关闭

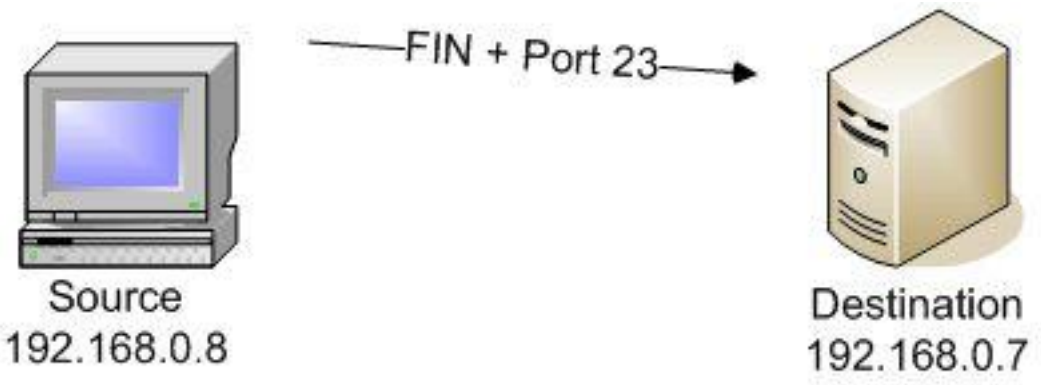


图8 TCP FIN 探测主机端口可能开启可能屏蔽

5.UDP scanning：

UDP 扫描方式用于判断 UDP 端口的情况。向目标主机的 UDP 端口发送探测包，如果收到回复“ICMP port unreachable”就说明该端口是关闭的；如果没有收到回复，那说明 UDP 端口可能是开放的或屏蔽的。

nmap –sU target

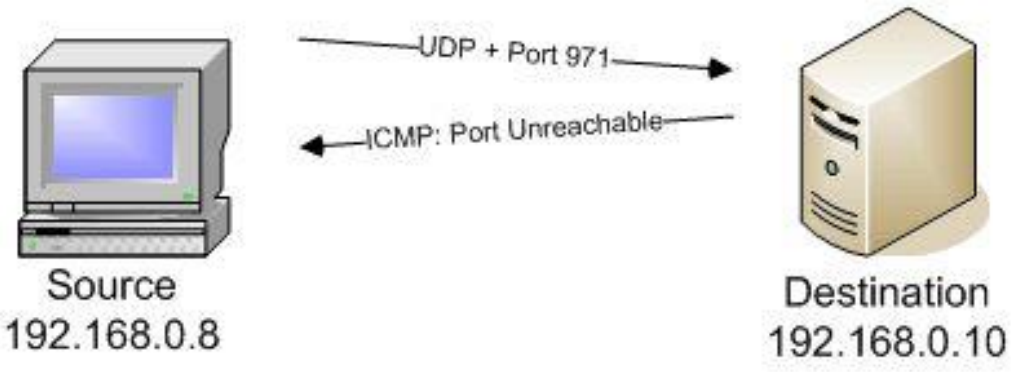


图9 UDP 端口关闭

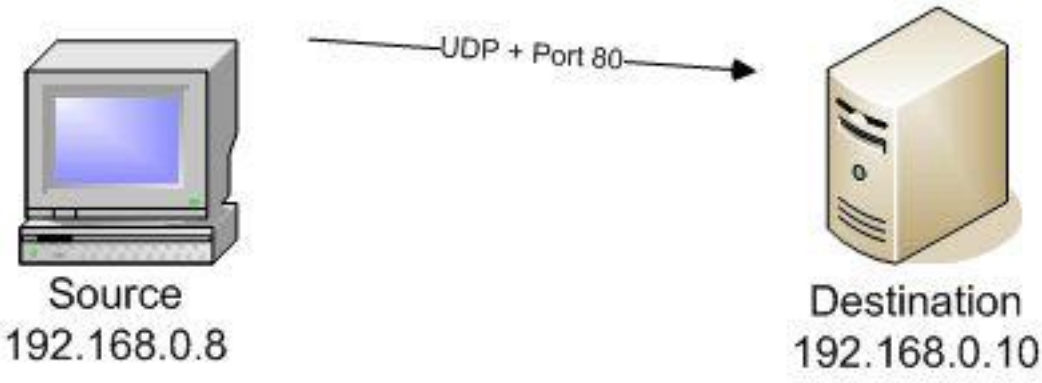


图10 UDP 端口开放或被屏蔽

三． 版本侦测原理：

版本侦测，用于确定目标主机开放端口上运行的具体的应用程序及版本信息。如果是 TCP 端口，尝试建立 TCP 连接。尝试等待片刻。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。

nmap –sV target

四． 操作系统侦测原理：

Nmap 使用 TCP/IP 协议栈指纹来识别不同的操作系统和设备。在 RFC 规范中，有些地方对 TCP/IP 的实现并没有强制规定，由此不同的 TCP/IP 方案中可能都有自己的特定方式。Nmap 主要是根据这些细节上的差异来判断操作系统的类型的。具体做法：分别挑选一个 open 和 closed 的端口，向其发送经过精心设计的 TCP/UDP/ICMP 数据包，根据返回的数据包生成一份系统指纹。将探测生成的指纹与 nmap-os-db 中指纹进行对比，查找匹配的系统。如果无法匹配，以概率形式列举出可能的系统。

nmap –O target

4. 怎么完成防火墙 / IDS 逃逸：

1.碎片化:

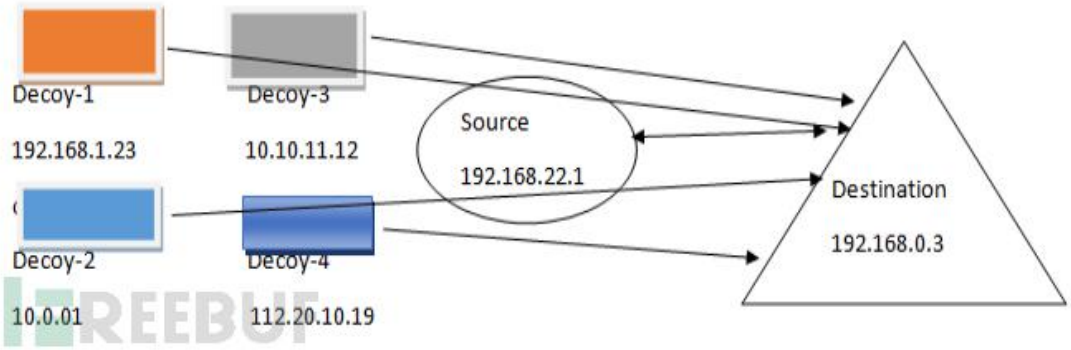
将可疑的探测包进行分片处理（例如将 TCP 包拆分成多个 IP 包发送过去），某些简单的防火墙为了加快处理速度可能不会进行重组检查，以此避开其检查。

nmap –f target

nmap --mtu 16 target

2.诱饵：

这种类型的扫描是非常隐蔽且无法察觉。目标由多个假冒或伪造 IP 地址进行扫描。这样防火墙就会认为攻击或扫描是通过多个资源或 IP 地址进行，于是就绕过了防火墙。



这实际上在目标看来是由多个系统同时扫描，这使得防火墙更难追查扫描的来源。

nmap –D RND:10 target

nmap –D decoy1,decoy2,… target

3、空闲扫描

攻击者将首先利用一个空闲的系统并用它来扫描目标系统。

扫描的工作原理是利用某些系统中采用可预见的 IP 序列 ID 生成。为了使空闲扫描成功，僵尸主机的系统必须是在扫描时间处于闲置状态。在这种技术中会隐藏攻击者的 IP 地址。

nmap –P0 –sI zombie target

4、选择特定原端口

每个 TCP 数据包带有源端口号。默认情况下 Nmap 会随机选择一个可用的传出源端口来探测目标。该–source-port 选项将强制 Nmap 使用指定的端口作为源端口。这种技术是利用了盲目地接受基于特定端口号的传入流量的防火墙的弱点。端口 21（FTP），端口 53（DNS）和 67（DHCP）是这种扫描类型的常见端口。

nmap –source-port port target

5、随机数据长度：

附加随机数据长度，我们也可以绕过防火墙。许多防火墙通过检查数据包的大小来识别潜伏中的端口扫描。这是因为许多扫描器会发送具有特定大小的数据包。为了躲避那种检测，我们可以使用命令–data-length 增加额外的数据，以便与默认大小不同。

nmap –data-length target

6、 MAC 地址欺骗：

每台机器都有自己独特的 mac 地址。因此这也是绕过防火墙的另一种方法，因为某些防火墙是基于 MAC 地址启用规则的。特别是–spoof-MAC 选项使您能够从一个特定的供应商选择一个 MAC 地址，选择一个随机的 MAC 地址，或者设定您所选择的特定 MAC 地址。 MAC 地址欺骗的另一个优点是，你让你的扫描隐蔽，因为你的实际 MAC 地址就不会出现在防火墙的日志文件。

nmap –Pn –spoof-mac mac_address target

7、发送错误校验

在某些防火墙和 IDS / IPS，只会检查有正确校验包的数据包。因此，攻击者可以通过发送错误校验欺骗 IDS / IPS。

nmap --badsum target