

实验四 网络攻击与防范实验

一 实验目的

通过对 ICMP Flood 攻击、UDP Flood 攻击等 DoS 攻击的过程，了解网络攻击的一般原理和方法，加强对网络攻击的防范意识。了解扫描的概念，能应用工具对主机漏洞进行扫描。

二 实验原理

DoS 攻击的原理

拒绝服务（DoS）攻击利用系统或协议的缺陷，采用欺骗的策略进行网络攻击，目的是使目标主机因为资源全部被占用而不能处理合法用户提出的请求，即对外表现为拒绝提供服务。

常见的 DoS 攻击方法：

（1）UDP Flood 主要通过利用服务器响应发送到其中一个端口的 UDP 数据包所采取的攻击方式。正常情况下，当服务器在特定端口接收 UDP 数据包时，服务器会检查是否有程序在监听相应的端口，如果没有程序在该端口监听，则服务器使用 ICMP 数据包进行响应。在这种攻击中，攻击者通常不会使用真实 IP 地址，而是采用伪造的 UDP 数据包源地址，从而阻止攻击者的真实位置被暴露，由于密保服务器利用资源检查并响应每个接收的 UDP 数据包结果，当接收到大量 UDP 数据包时，目标的资源就会迅速耗尽，导致对正常流量的拒绝服务。

（2）Synflood:该攻击以多个随机的源主机地址向目的主机发送 SYN 包，而在收到目的主机的 SYN ACK 后并不回应，这样，目的主机就为这些源主机建立了大量的连接队列，而且由于没有收到 ACK 一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务。

（2）Land-based：攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过 IP 欺骗的方式发送给被攻击主机，被攻击主机与自己建立空连接并保留连接，从而很大程度地降低了系统性能。

（3）UDP 洪水(UDP flood)：echo 服务会显示接收到的每一个数据包，而 chargen 服务会在收到每一个数据包时随机反馈一些字符。UDP flood 假冒攻击就是利用这两个简单的 TCP/IP 服务的漏洞进行恶意攻击，通过伪造与某一主机的 Chargen 服务之间的一次的 UDP 连接，回复地址指向开着 Echo 服务的一台主机，通过将 Chargen 和 Echo 服务互指，来回传送毫无用处且占满带宽的垃圾数据，在两台主机之间生成足够多的无用数据流，这一拒绝服务攻击飞快地导致网络可用带宽耗尽。

（4）Smurf、UDP-Flood、Teardrop、PingSweep、Pingflood、Ping of Death 等。

DDoS 的原理

分布式拒绝服务（DDoS）是基于 DoS 攻击的一种特殊形式。攻击者将多台受控制的计算机联合起来向目标计算机发起 DoS 攻击。

DDoS 攻击分为 3 层：攻击者、主控端、代理端。1）攻击者：攻击者所用的计算机是攻击主控台，攻击者操纵整个攻击过程，它向主控端发送攻击命令。2）主控端：主控端是攻击者非法侵入并控制的一些主机，这些主机还分别控制大量的代理主机。主控端主机的上面安装了特定的程序，因此它们可以接受攻击者发来的特殊指令，并且可以把这些命令发送到代理主机上。3）代理端：代理端同样也是攻击者侵入并控制的一批主机，它们上面运行攻击器程序，接受和运行主控端发来的命令。代理端主机是攻击的执行者，真正向受害者主

机发送攻击。

攻击者发起 DDoS 攻击的第一步，就是寻找在 Internet 上有漏洞的主机，进入系统后在其上面安装后门程序，攻击者入侵的主机越多，他的攻击队伍就越壮大。第二步在入侵主机上安装攻击程序，其中一部分主机充当攻击的主控端，一部分主机充当攻击的代理端。最后各部分主机各司其职，在攻击者的调遣下对攻击对象发起攻击。

缓冲区溢出原理

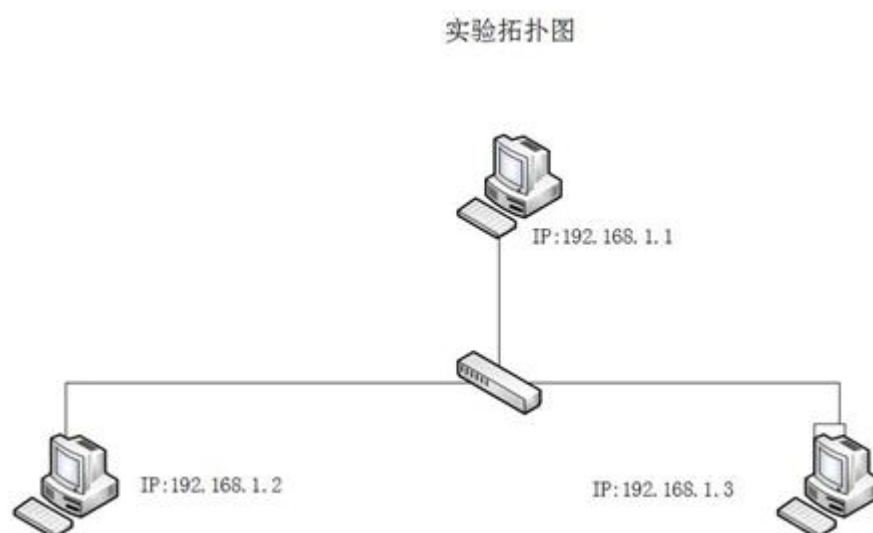
缓冲区是内存中存放数据的地方。在程序试图将数据放到计算机内存中的某一位置，但没有足够空间时会发生缓冲区溢出。

缓冲区溢出指的是一种系统攻击的手段，通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达到攻击的目的。

IPC\$漏洞攻击：445 端口是个毁誉参半的端口，可以通过这个端口在局域网中进行共享文件和打印机共享，但通过这个端口黑客可以入侵服务器，2017 年 10 月，由于病毒“坏兔子”来袭，国家互联网应急中心等安全机构建议用户及时关闭计算机上的 445 端口和 139 端口。勒索病毒也是基于 445 端口进行攻击。

三 实验环境

实验环境中要求如下网络拓扑：



四 实验内容和任务

任务一、Fakeping 攻击。

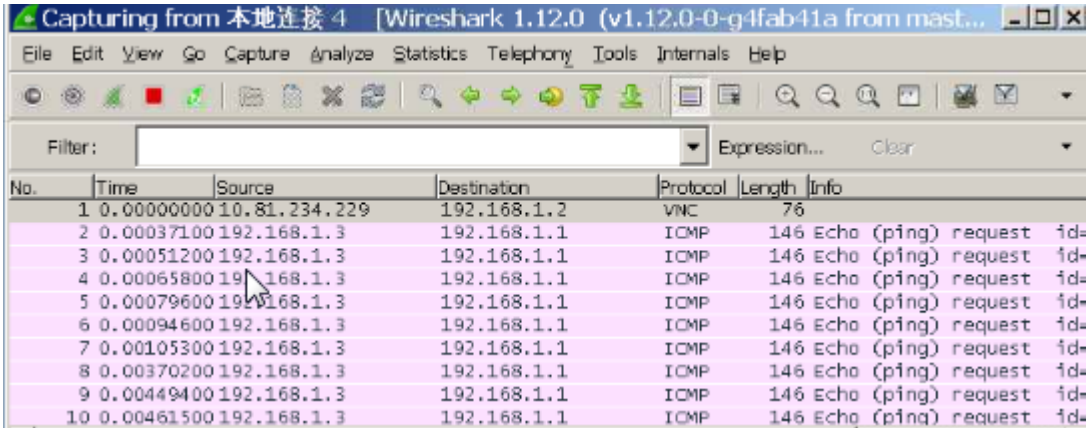
步骤 1：在命令行模式下，进入 fakeping 目录，输入命令

Fakeping 192.168.1.3 192.168.1.1 100

(该命令用于在操作机上向 192.168.1.1 发送伪装 icmp 请求信息，请求信息的伪装源地址为 193.168.1.3。注：fakeping 命令格式：fakeping 伪装源 目的地址 数据包大小)



步骤 2: 在目标机上打开 Wireshark 软件, 监听本地主机上的 icmp 数据包, 并设置数据包过滤参数。如下图所示:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.81.234.229	192.168.1.2	VNC	76	
2	0.00037100	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
3	0.00051200	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
4	0.00065800	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
5	0.00079600	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
6	0.00094600	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
7	0.00105300	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
8	0.00370200	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
9	0.00449400	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=
10	0.00461500	192.168.1.3	192.168.1.1	ICMP	146	Echo (ping) request id=

可以看到, 192.168.1.3 主机在没有发送 icmp 请求的情况下却收到了大量的 icmp 响应数据包。该数据包即为 192.168.1.2 伪造的源地址为 192.168.1.3 发给 192.168.1.1 的请求数据包的响应 icmp 数据包。

建议进入虚拟机试验环境进行实验。

***任务二、UDP Flood 攻击**

步骤 1: 使用 Htop 查看 CPU 使用率

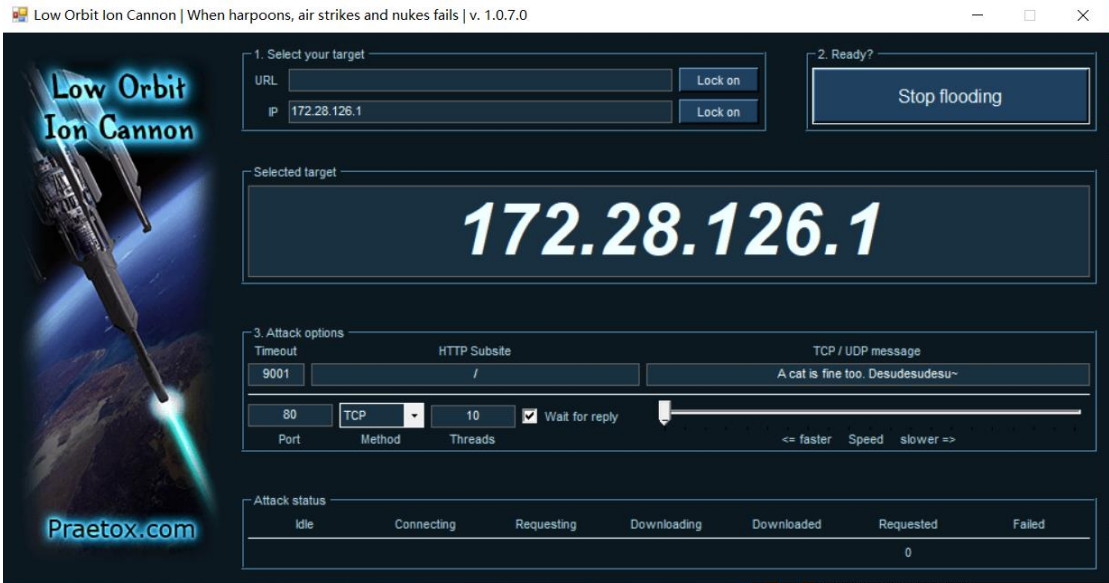
步骤 2: 使用 Hping3 进行 UDP Flood 攻击。

在 Kali 中, 使用 `Hping3 -udp -s 6666 -p 53 -a 8.8.8.8 -flood 182.168.12.130` 进行攻击, 查看攻击的效果。

任务三、基于 LOIC 的攻击

LOIC 代表低轨道离子炮。它是一种免费且流行的工具, 可用于 DDoS 攻击。

步骤 1 使用 LOIC 进行锁定实验用 IP 地址, 实施 Flood 攻击



步骤 2 使用 Htop 查看 CPU 使用率。

任务四 基于 IPC\$漏洞的攻击

步骤 1 通过扫描软件收集服务器信息。（可以利用 Nmap 软件进行扫描）

步骤 2. 尝试使用共享访问服务进行连接。使用 NTscan 扫描器进行暴力破解（具体操作步骤请参考奇安信实验平台中内容。）

五. 实验报告要求

对实验任务中的不同攻击方式进行实验，给出每一步实验结果的截图；

要求每个人实验报告中截图要有自己的特征，不能抄袭。