实验指南

（补充实验 1）实验目的：主机发现

实验环境：Linux

实验对象：局域网内主机

实验要求：

-用 Ping 命令发现目标网络主机是否活跃，分析命令行中的参数和实验结果；

-用 srp-scan 命令发现目标网络中的活跃主机，分析命令行中的参数和实验结果；

-用 nmap 命令，分别通过发送 ARP，ICMP，TCP 包，发现目标网络中的活跃主机，分析命令行中的参数和实验结果；

-掌握所有 ICMP 消息类型；ICMP 是控制包，分为多种类型，针对这些类型，会有不同的响应方式。了解所有的 ICMP 包类型，是什么功能，用在什么场合等，写入报告；

注意：本实验都用命令行界面进行；

（补充实验 2）实验目的：识别目标主机上运行的服务/端口扫描

实验环境：Linux

实验对象：局域网内主机

实验要求：

之前我们练习了用 nmap 工具发现目标主机运行的服务类型，其实能完成这个功能的工具还有其他，比如 netcat.本实验要求完成以下内容：

-用 nmap 命令进行 TCP SYN 端口扫描，发现目标主机上开放的端口，运行的服务及版本；

-用 nc 命令分别进行 TCP 和 UDP 端口扫描，发现目标主机上运行的服务信息；

-通过 man nc 或者查阅资料掌握 nc 命令，理解各参数的含义和功能，写入报告；

（补充实验 3）实验目的：检测操作系统

实验环境：Linux 命令行界面、Window

实验要求：有三种方式可以用于检测操作系统，本此实验要求练习每一个检测 OS 的方法：

1）通过分析目标主机开放的端口和运行的服务信息来推断 OS；

在上一个实验的基础上，分析端口和运行服务信息，推测 OS；

2）通过分析目标对 ICMP 包的响应信息的方式来探测 OS；

掌握 stack fingerprinting 的原理；

用 nmap -O 命令检测目标主机的 OS；

考虑当检测目标主机后发现没有一个端口打开时，该如何检测 OS；

3）通过 banner-grabbing(标头抓取)的方式探测 OS；

前两种种方法是主动式探测，比较容易被发现；现在我们来实验通过监听网络流量的被动式探测，即抓取标头信息，来分析得出结论。

-通过 telnet 嗅探实现 banner grabbing。Telnet 是 windows 下自带的工具。掌握 telnet 嗅探的原理，TCP/IP 会话的三个因素（TTL，Window size, DF）。用 **telnet** 命令发送正确的请求来探测目标主机，分析得到的结果信息；

-故意用 telnet 向目标发送一个错误的请求，分析其返回信息，能得出什么结论；

-用 netcat 进行 banner grabbing.利用 nc 命令，分析返回结果；

（补充实验 4）实验目的：查找目标公司的邮件服务器和防火墙

公司的邮件服务器通常和防火墙位于同一个系统，或者在同一个网段中。

实验要求：

-用 Host 命令，分析得到的信息；

如：host www.ruc.edu.cn

host ruc.edu.cn

-追踪到目标经过的路径，分析到达目标的前一跳是什么

(UNIX 下)traceroute www.ruc.edu.cn

(Windows 下)tracert

（综合实验）实验目的：对机房网络系统进行探测

实验对象：本实验机房局域网为目标系统

根据本机房 IP 地址范围，使用多种安全工具软件，对机房系统进行探测，撰写探测报告：说明其系统节点分布、端口开放、运行服务及存在漏洞类型等信息，并查阅资料，对漏洞信息进行介绍。**注意**要在实验过程中，掌握所使用的每一个工具的功能和工作原理，写入报告。

目标可以具体细分为：

1）探测目标网络系统存活节点分布情况；（分别使用 cheops-ng/NetworkView 两种工具）得到机房的网络的 IP 地址范围；获得机房网络拓扑图；掌握两种工具的功能；

2）通过当前系统中运行的服务以及版本信息，查阅资料，推测可能存在的漏洞。

3）比如检测出某主机上运行 http 服务，且版本为 Apache 2.0，而查阅资料后可知该版本存在一些漏洞，那我们就可以初步假定，目标主机也可能存在这些漏洞，下一步需要利用专业工具来验证；

3）**扫描目标网络系统存在的漏洞，查阅相关资料，分析漏洞原理；**

-用 Nessus 进行漏洞扫描；熟悉 Nessus 的功能和使用，介绍 Web Interface 上各个标签的含义（如 Policy 等），写入报告；针对扫描出的漏洞，查阅资料，分析原理及危害；

-用 Metaspolit 进行漏洞扫描。认真阅读《Metaspolit 操作手册》，熟悉 Metaspolit 的功能和使用。使用 Web 应用程序测试功能，对测试结果进行分析，写入报告；针对扫描出的

漏洞，查阅资料，分析其原理以及危害，写入实验报告；

-用 X-Scan 对目标进行综合扫描；掌握 X-Scan 的功能以及使用；分析扫描结果；

-比较三者产生的结果，从功能和原理上分析这三个工具的异同，写入报告；

【参考】大家可以参考石老师第 2 章的 PPT ；