# 实验报告模板

华南理工大学

《网络攻防原理与技术》课程实验报告

实验题目： 网络侦察与网络扫描

|  |
| --- |
| **实验概述** |
| 【实验目的及要求】  实验目的：   1. 熟悉网络侦察技术的几种常用方法和作用 2. 掌握常见扫描技术（主机扫描、端口扫描、操作系统检测）   实验要求：  【实验环境】  操作系统：Windows XP |
| **实验内容** |
| 【实验方案设计】   一：利用搜索引擎搜索“北京师范大学”   1. 获取“北京师范大学”的网站地址 2. 获取网络相关信息 3. 搜索密码文件、搜索管理员后台URL、搜索CGI漏洞、搜索黑客留下的后门……    二：利用whois数据库查询   1. 查询目标域名的注册机构 2. 查询目标域名详细的注册资料 3. 查询IP地址分配和拥有机构   三：网络扫描   1. 熟悉nmap命令 2. 对靶机metasploitable 3进行扫描（端口，os，漏洞） 3. 防火墙关闭 4. 防火墙打开   【实验过程】（实验步骤、记录、数据、分析）  实验内容一：利用搜索引擎搜索“北京师范大学”   1.通过关键字搜索“北京师范大学”获得网络地址  屏幕快照 2018-10-17 下午7.10.52  2.通过intext：to parent directory搜索  屏幕快照 2018-10-17 下午7.16.48屏幕快照 2018-10-17 下午7.09.34   1. 在Shodan中搜索   屏幕快照 2018-10-17 下午7.47.22屏幕快照 2018-10-17 下午7.47.39  屏幕快照 2018-10-17 下午7.53.20屏幕快照 2018-10-17 下午7.53.47屏幕快照 2018-10-24 下午7.15.05  timg  实验内容一：利用WHOIS数据库查询<baidu.com>  屏幕快照 2018-10-17 下午7.27.11  **实验内容二：网络扫描**   1. nmap scanme.nmap.org扫描结果   屏幕快照 2018-10-21 下午4.38.53  结论：扫描到scanme.nmap.org IP地址是45.33.32.156，1个主机开启，22、80、9929、31337端口开启，996个端口关闭   1. nmap –sV scanme.nmap.org 扫描结果   屏幕快照 2018-10-21 下午4.45.42  结论：查到端口服务版本信息和服务器信息（Linux操作系统）   1. nmap -p22,80 scanme.nmap.org扫描端口22,80：   屏幕快照 2018-10-21 下午4.56.51  结论：两个端口均开启  4.nmap -p1-1024 scanme.nmap.org扫描端口号在1-1024范围内所有开启的端口：  屏幕快照 2018-10-21 下午5.00.50  结论：1-1024范围内只有22,80端口开启，1022个端口关闭  5.nmap 192.168.1.0/24  屏幕快照 2018-10-21 下午5.22.42屏幕快照 2018-10-21 下午5.24.02  结论：主机都开启了，但是所有端口扫描都被过滤了。   1. namp 1.2.3.4和nmap 1.2.3.5和nmap 1.2.3.6   屏幕快照 2018-10-21 下午5.25.11屏幕快照 2018-10-21 下午5.26.33屏幕快照 2018-10-21 下午5.26.53  结论：主机都开启，端口扫描都被过滤  7.nmap -sV --reason scanme.nmap.org  屏幕快照 2018-10-21 下午5.08.42  扫描结果的根据   1. Nmap –sL 202.38.193.50-60   屏幕快照 2018-10-21 下午5.35.32   1. Nmap –sn –n 192.168.56.1-254   屏幕快照 2018-10-21 下午5.42.14  结论：IP地址在192.168.56.1-254范围内的主机都在线   1. Nmap –Pn -n mmsec.science   屏幕快照 2018-10-21 下午5.51.37   1. Nmap –sn –PS mmsec.science   屏幕快照 2018-10-21 下午5.59.08   1. Nmap –sn –PS8080 mmsec.science   屏幕快照 2018-10-21 下午5.59.14   1. Nmap –sn –PA mmsec.science   屏幕快照 2018-10-21 下午6.04.04   1. Nmap –sn –PA8080 mmsec.science   屏幕快照 2018-10-21 下午6.07.50   1. Nmap –sn –PU mmsec.science   屏幕快照 2018-10-21 下午6.09.21   1. Nmap –sn –PU53 mmsec.science   屏幕快照 2018-10-21 下午6.09.28   1. Nmap –sn –PE mmsec.science   屏幕快照 2018-10-21 下午6.11.01   1. Nmap –sn –PP mmsec.science   屏幕快照 2018-10-21 下午6.11.08   1. Nmap –sn –PO mmsec.science   屏幕快照 2018-10-21 下午6.12.30   1. Nmap –sn –PR mmsec.science   屏幕快照 2018-10-21 下午6.12.36   1. Nmap –sU –p53 mmsec.science --reason   屏幕快照 2018-10-21 下午6.14.28   1. Nmap –sS mmsec.science   屏幕快照 2018-10-21 下午6.16.00   1. Nmap –sT mmsec.science   屏幕快照 2018-10-21 下午6.16.41   1. Nmap –sN mmsec.science   屏幕快照 2018-10-21 下午6.17.18   1. Nmap –sF mmsec.science   屏幕快照 2018-10-21 下午6.18.27   1. Nmap –sX mmsec.science   屏幕快照 2018-10-21 下午6.18.34   1. Nmap –sA mmsec.science   屏幕快照 2018-10-21 下午6.19.26   1. Nmap –O mmsec.science   屏幕快照 2018-10-21 下午6.21.03   1. 防火墙关闭时，扫描Metasploitable 3靶机 2. 在靶机终端输入ipconfig得到IP地址172.21.125.225   屏幕快照 2018-10-24 上午11.12.02   1. 关闭防火墙 2. 在kali的终端中输入nmap 172.21.125.225进行扫描，发现有20个端口开启   屏幕快照 2018-10-24 上午11.13.40   1. 在kali的终端中输入nmap -sT 172.21.125.225进行扫描，发现有20个端口开启   屏幕快照 2018-10-24 上午10.53.17   1. 在kali的终端中输入nmap -Pn 172.21.125.225进行扫描，发现有20个端口开启   屏幕快照 2018-10-24 上午11.05.04   1. 在kali的终端中输入nmap -sS 172.21.125.225进行扫描，发现有20个端口开启   sS  （7）通过nmap -O 172.21.125.225命令进行操作系统检测，结果如下  屏幕快照 2018-10-24 上午11.09.32   1. 输入msfconsole   屏幕快照 2018-10-24 上午11.22.42屏幕快照 2018-10-24 上午11.22.51  （6）输入use auxiliary/scanner/portscan/tcp  （7）输入show options查看需要填写的内容  屏幕快照 2018-10-23 上午12.23.39   1. 输入-h命令查看帮助手册   屏幕快照 2018-10-24 上午11.35.58   1. 输入set rhosts 171.21.125.225设置靶机   屏幕快照 2018-10-24 上午11.35.43   1. 输入search cve:2018 app:server 查看漏洞   屏幕快照 2018-10-24 上午11.31.34  输入search port：8080 app:server 查看端口8080的漏洞  屏幕快照 2018-10-24 上午11.45.29屏幕快照 2018-10-24 上午11.45.39   1. 在防护墙开启时对靶机进行扫描 2. 开启防火墙 3. 使用不同技术对靶机进行端口扫描   ~~屏幕快照 2018-10-24 上午11.19.35~~  ~~屏幕快照 2018-10-24 上午10.53.06屏幕快照 2018-10-24 上午11.05.12~~  ~~sS~~   1. 使用nmap -O 172.21.125.225命令进行操作系统检测   屏幕快照 2018-10-24 上午11.34.09   1. 漏洞扫描   输入search cve:2018 app:server 查看漏洞屏幕快照 2018-10-24 上午11.33.08  查看端口8080漏洞  屏幕快照 2018-10-24 上午11.42.28  屏幕快照 2018-10-24 上午11.42.37  【结论】   1. 防火墙关闭时扫描到的开启端口比防火墙打开时扫描到的端口要多，说明防火墙对一些数据包有过滤作用。 2. 防火墙关闭时，直接得出确定结论：探测到的操作系统是win7（与实际不符）。而当防火墙开启时，只能猜测是各个操作系统的概率，其中win8可能性最大（实际上靶机的操作系统是win8）。 3. 防火墙的开启或关闭对漏洞扫描结果没有影响。 |
|  |