**《渗透测试》**

W1:

任务1：简述题，简要阐述渗透测试项目的生命周期。  
任务2：简述题，列举常用渗透测试工具。  
任务3：实践题，在自己的电脑上安装Kali Linux，提交安装完成后的界面截图，要求全屏截图（能看到虚拟机、真机任务栏、真机系统时间）。

W2:

任务1、简述扫描技术的分类  
任务2、简述nmap的主要功能  
任务3、操作题（2张截图），1-配置kali虚拟机可以访问外网，2-查看物理机（真机）的IP地址，使用kali扫描物理机所在网段的所有存活主机。  
任务4、操作题（截图），启动数据包捕获软件wireshark，将任务3的数据通信过程记录下来。  
任务5、操作题（截图），使用wireshark捕获下面的数据包（kali虚拟机去 ping 8.8.8.8）

W3:

任务1，操作题，切换到Kali虚拟机，使用nmap工具扫描本网段所有存活主机；  
任务2，操作题，切换到Kali虚拟机，使用nmap工具扫描真机所在网段所有存活主机；  
任务3，操作题，切换到Kali虚拟机，使用nmap工具扫描本网段所有开放了445端口的主机；  
任务4，操作题，切换到Kali虚拟机，使用nmap工具扫描真机所在网段所有开放了80端口的主机；  
任务5，简答题，简述nmap探测主机存活的技术有哪些？  
任务6，简答题，nmap如下选项具体用途（-sn，-p-，-sV，-O，-sT，-sS，-sU）

W4:

渗透测试和黑客的区别

渗透测试和黑客之间的区别是：渗透测试是一种通过模拟黑客攻击的方式来评估计算机网络系统的安全性能，评估计算机网络系统工作的方法。渗透测试是经过客户授权，采用可控制、非破坏性质的方法和手段发现目标和网络设备中存在弱点，帮助管理者知道自己网络所面临的问题，同时提供安全加固意见帮助客户提升系统的安全性。而黑客则是指那些利用自己在计算机方面的技术，设法在未经授权的情况下访问计算机文件或网络的人。这类人群对社会是具有危害性的。

W5:

部署MoneyBox靶场，完成渗透测试工作（获得3个FLAG），并撰写WriteUP。

W6:

本地搭建实验环境，使用kali中的hydra工具对目标计算机的SSH（或SMB、或FTP服务）进行口令爆破，将主要实验过程截图

W7:

搭建实验环境，实现SSH免密登录（密钥认证），将主要过程界面截图

W8:

SQL注入漏洞的原理是（）

A.  允许用户上传任意类型的文件

B.  允许用户执行系统命令

C.  允许客户端启用javascript脚本

D.  黑客将一段精心构造的代码拼接在正常查询语句的后面，并代入到数据库中执行，从而获取数据库的信息甚至是进行提权

正确答案： D

MySQL元数据库是指以下哪个库（）

A.  master数据库

B.  mysql数据库

C.  Test数据库

D.  Information\_schema数据库，记录mysql自身数据的数据库

正确答案： D

SQL注入的最直接目标是（）

A.  内网控制

B.  修改网页内容

C.  获取网站后台管理员账号和密码

D.  远程控制服务器

正确答案： C

W9:

期中考试复习

W10:

期中考试

W11:

SQL注入需要判断是哪种数据库才好进一步下手测试，一般来说，如果这个网站是PHP的，那么数据库一般是（）？

A.  MySQL

B.  Oracle

C.  SQL Server

D.  Microsoft SQL Server

正确答案： A

张若欣是一家安全公司的技术人员，她对于SQL注入技术有较为深入的了解。一天，她接到一个任务对网站进行渗透测试，她发现网站的URL地址为：http://target/news.php?ID=1 ，她敏锐的感觉到ID这个地方极有可能是一个SQL漏洞的注入点。于是她准备分别输入（）和（）用条件表达式判断有没有异常。

A.  ID=1 and 1=1

B.  ID=5 union select user from database(); #

C.  ID=1 and 1=2

D.  ID=’

正确答案： AC

sqlmap要想注入一个需要登录的网站时，需要加上什么参数？（）

A.  –cookie

B.  --file-read

C.  –dbs

D.  --id

正确答案： A

我们说一个网站有SQL注入漏洞需要满足以下几个条件（）。

A.  用户输入的数据被传递给后台的SQL服务器加以解析并执行

B.  可以输入单引号

C.  肯定要有可以让用户输入的点

D.  可以输入长串儿字符串

正确答案： AC

sqlmap要想列出所有数据库，需要加上什么参数？（）

A.  --file-read

B.  –id

C.  –dbs

D.  --cookie

正确答案： C

菲菲鱼是一个喜欢信息安全技术的中学生，她喜欢到一些公益的SRC平台做渗透。一天，她接到一个任务对网站进行渗透测试，她发现网站的URL地址为：http://target/news.php?ID=1 ，她敏锐的感觉到ID这个地方极有可能是一个SQL漏洞的注入点。那么她可以输入（），用一些异常的数据看有没有异常。

A.  ID=1 and 1=1

B.  ID=1 and 1=2

C.  ID=’

D.  ID=5

正确答案： C

W12:

撰写Hackademic.RTB1靶场渗透测试writeup

W13:

结合owaspbwa靶机的DVWA环境，实现SQL注入漏洞利用（使用自动化注入工具SQLMAP，低级别），主要过程界面截图

W14:

结合owaspbwa靶机中的DVWA环境，实践文件上传漏洞（低级别和中级别），将漏洞利用过程主要界面截图

基于DVWA靶场环境，实现文件包含漏洞利用（低级别和中级别），将主要实现过程截图

基于DVWA靶场环境，实现命令执行漏洞利用，将主要过程截图

W15:

撰写Potato-suncsr靶场Writeup

W16:

撰写靶场DC-1的writeup

W17:

撰写靶场DC-2的writeup