**第 二 次 实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程名称 | **网络安全实验** | | | | |
| 学生姓名 | 应晓宇 | 学号 | 2021302181140 | 指导老师 | 陈治宏 |
| 专业 | 网安 | 班级 | 7 | 实验时间 | 24.4.3 |

1. **实验介绍**
   * + 1. **实验名称：漏洞侦查实验 实验任务：**

任务一 使用nmap、MSF和Metasploit进行漏洞挖掘和利用；

任务二 使用nikto、crunch和burpsuit进行网站渗透和控制；

任务三 任务三获取webshell权限并拿到目标机开放的远程桌面端口号；

任务四 向目标机添加新用户并控制目标机。

* + - 1. **实验目的：**

了解网络安全漏洞、漏洞挖掘和利用的基本概念以及常用的安全漏洞扫描工具，认知常见的企业网络安全漏洞。

掌握nmap、MSF、Metasploit、nikto这样的网络级扫描工具的功能和操作方法，并能够分析检侧结果，能够运用这些工具解决目标网络信息探测、漏洞挖掘的常见安全问题。

熟悉网站wenshell的概念，理解上传webshell、获取webshell权限的意义和方法，掌握获取webshell权限基础上控制目标机的方法。

了解nikto工具的基本功能，掌握常用的网页服务器扫描和探测命令。

了解crunch的基本功能，掌握利用crunch生成密码字典文件的方法。

了解burpsuit工具的基本功能，掌握其暴力破解密码的基本方法。

通过nmap、MSF、Metasploit、nikto、crunch和burpsuit等工具的学习和使用，能够融会贯通，掌握web漏洞挖掘、渗透、攻击和利用的原理和方法，掌握自主学习和实践主流企业网络扫描工具的功能、操作技巧、检测结果分析、漏洞挖掘的常用方法，具备企业复杂网络信息安全管理的职业能力和终身学习能力。

* + - 1. **实验工具：**

Nmap（集成于kali linux）

MSF（集成于kali linux）

Metasploit（集成于kali linux）

Burp Suite v1.7.26

nikto（集成于kali linux）

crunch（集成于kali linux）

* + - 1. **实验环境：**



1. **实验内容**
2. **任务一**

**【任务描述】**

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用kali集成的扫描工具nmap，对网络进行探测，收集目标网络存活主机信息，并利用主机开放的服务器，获取目标主机的root权限。

利用kali集成的MSF和Metasploit两个工具，实现对目标主机的漏洞探测和利用，并成功攻击目标机。

通过完成本实验任务，要求学生掌握利用nmap进行网络探测并获取目标主机root权限等关键信息的方法；掌握通过MSF和Metasploit实现对目标主机的漏洞探测和漏洞模块利用的流程、方法和技巧，为完成后续漏洞挖掘实验任务奠定坚实的网络探测技术基础。

**【实验目标】**

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

了解扫描工具nmap的基本使用方法，掌握常用的网络扫描和探测命令。

掌握利用nmap进行网络探测并获取目标主机root权限等关键信息的方法。

了解Metasploit工具的基本功能，掌握常用的漏洞探测和利用命令。

掌握通过Metasploit实现对目标主机的漏洞探测和漏洞模块利用技术和方法。

通过nmap、Metasploit等工具的学习和使用，能够融会贯通，掌握自主学习和实践主流企业级网络扫描工具功能、操作技巧、检测结果分析、漏洞挖掘的常用方法，最终具备企业复杂网络漏洞挖掘的职业能力。

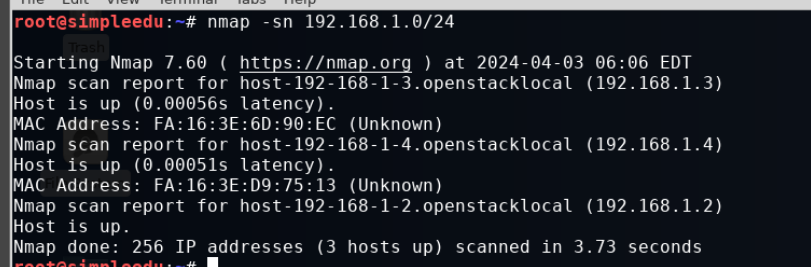
**【实验工具】**

Nmap（集成于kali linux）

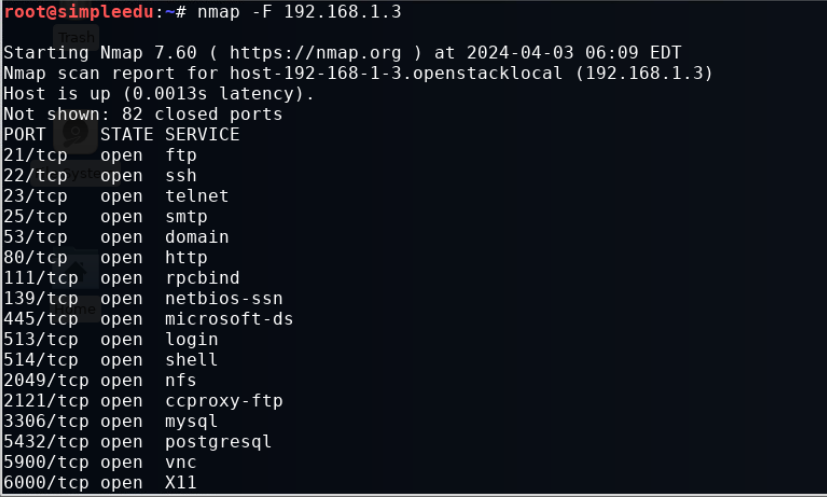
Metasploit（集成于kali linux）

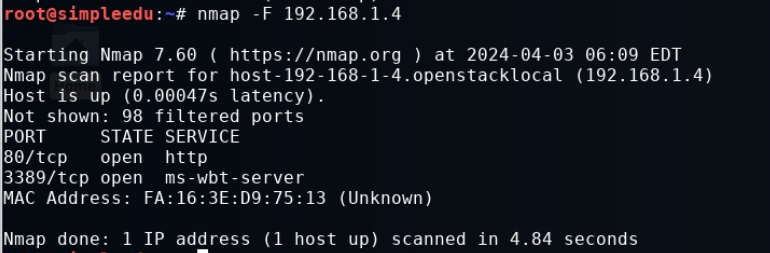
**【操作步骤】**

1.使用nmap扫描网段内存活主机

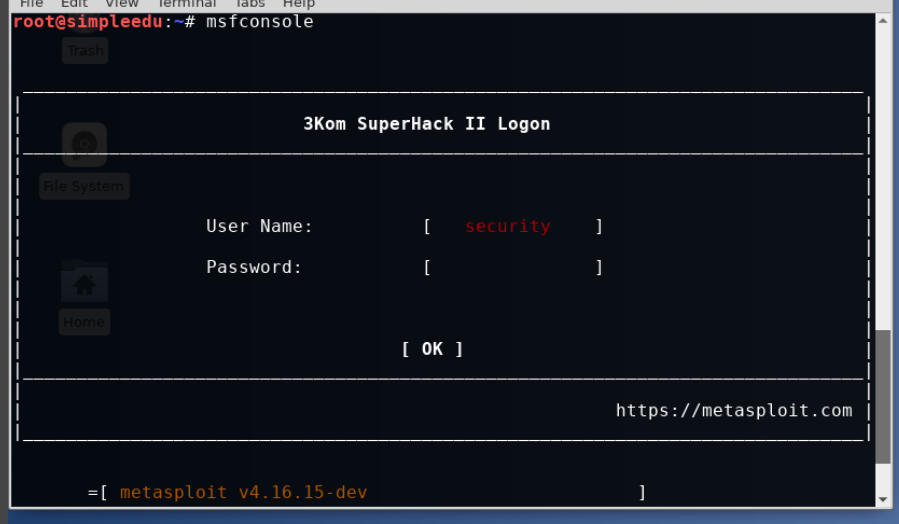


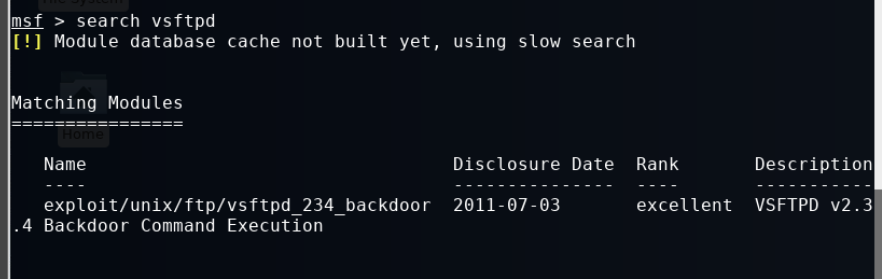
2.分别扫描上一步扫描到的主机的服务，在192.168.1.3中扫描到ftp



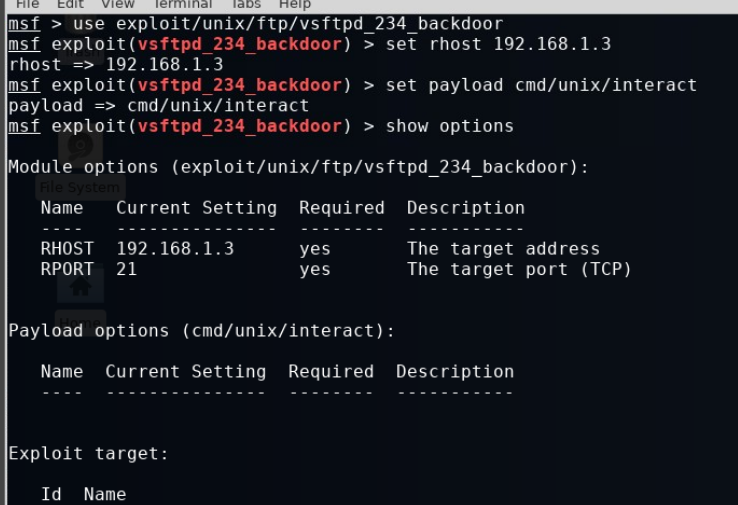


1. 使用msfconsole启动，并搜索vsftpd FTP服务器程序的相关工具和攻击载荷





1. 使用脚本并设定攻击载荷和目标ip



4.攻击，并寻找1.key





发现1.key内容为Metasploit

**2.任务二**

【**任务描述**】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用kali集成的扫描工具nikto和crunch，对目标网站进行探测，根据收集的信息进行渗透(提交网站后台管理员登陆密码)，获取网站的webshell。

使用burpsuit工具软件暴力破解目标网站管理员登陆密码，以完全控制目标主机系统。

通过完成本实验任务，要求学生掌握对网站进行探测和渗透的技术和工具使用方法，具体包括：利用nikto进行网页服务器探测扫描的方法；掌握使用crunch生成密码字典文件的方法；掌握burpsuit工具软件暴力破解登陆密码的方法，具备更为夯实的漏洞挖掘和利用、信息系统安全防范的职业能力。

【**实验目标**】

了解网络漏洞渗透、webshell的概念，认知常用的安全漏洞扫描工具。

了解nikto工具的基本功能，熟悉其常用的网页服务器扫描和探测命令。

了解crunch的基本功能，掌握利用crunch生成密码字典文件的方法。

了解burpsuit工具的基本功能，掌握其暴力破解密码的基本方法。

通过nikto、crunch和burpsuit等工具的学习和使用，掌握对网站进行渗透、获取webshell、破解密码等常用的漏洞挖掘和利用技术，领会预防漏洞攻击的方法，具备丰富的漏洞挖掘和防攻击能力。

【**实验目标**】

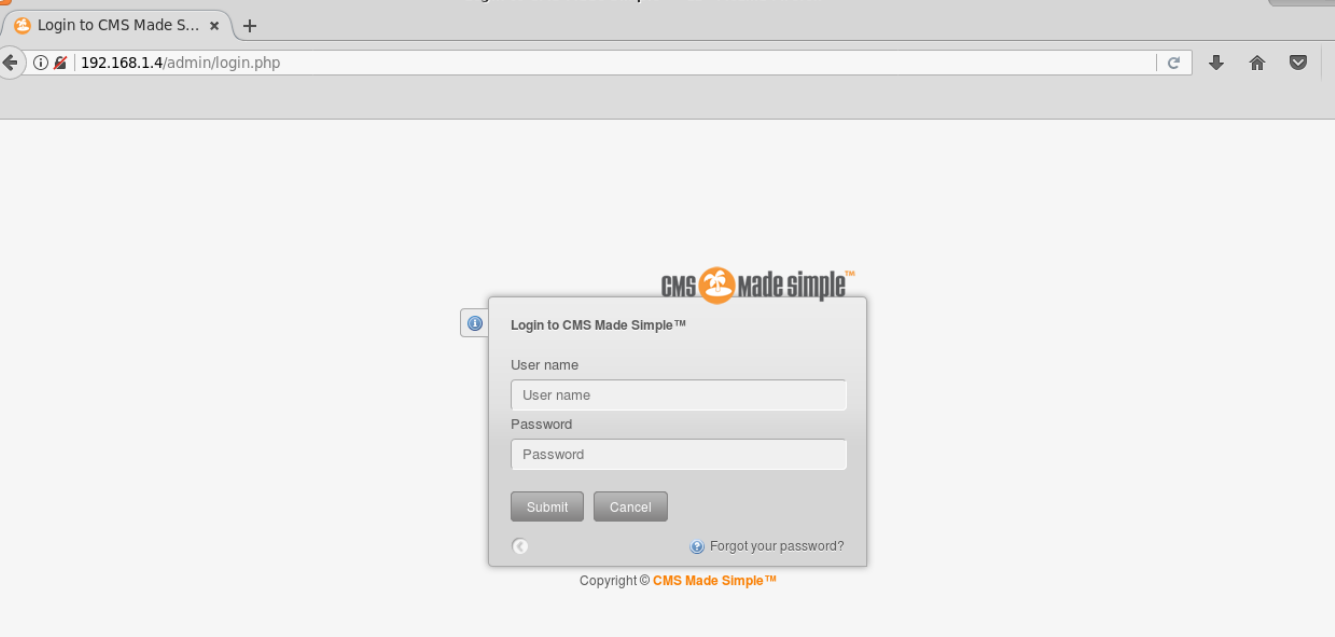
nikto（集成于kali linux）

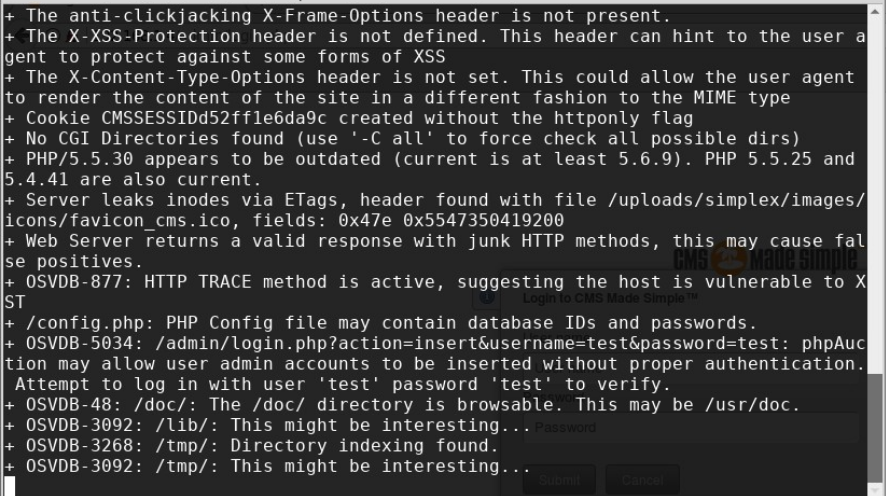
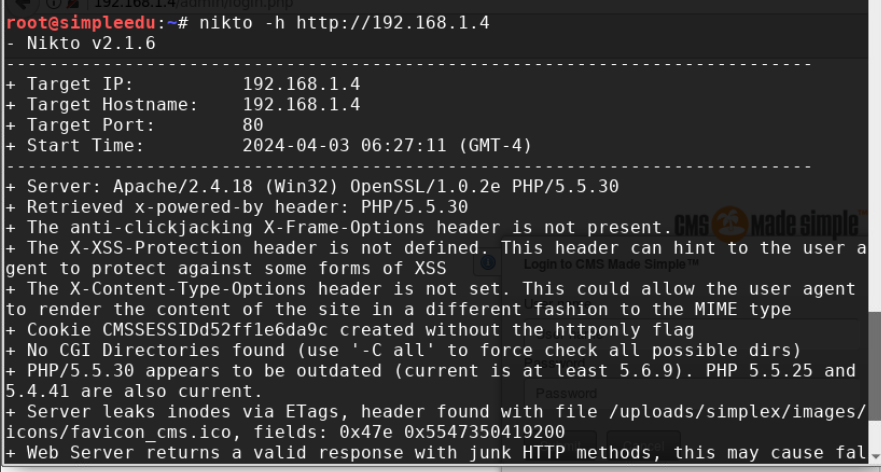
crunch（集成于kali linux）

burpsuit

【**操作步骤**】

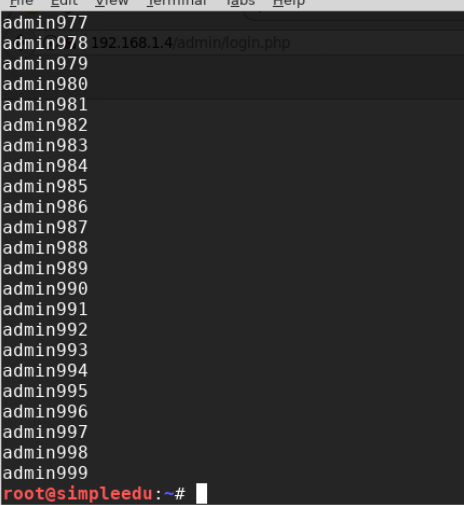
1.扫描目标网站，查看其后台管理界面



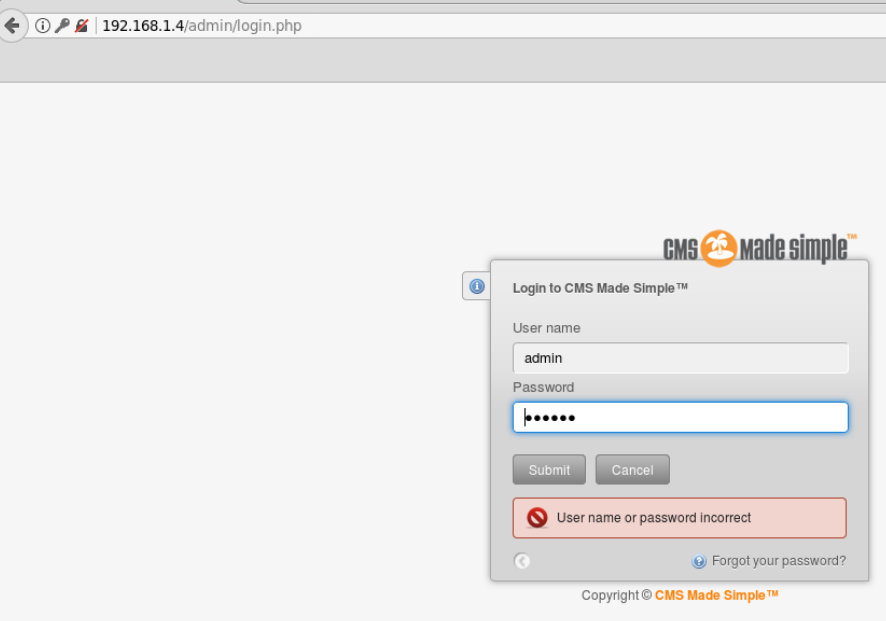


1. 在目标机/root目录下创建password.txt文件准备暴力破解

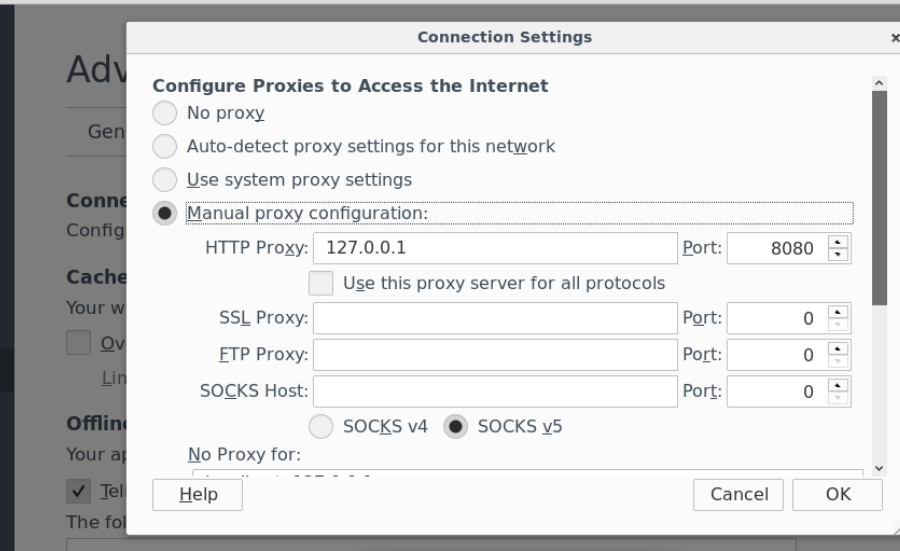
使用命令crunch 8 8 /root/password.txt -t admin%%%



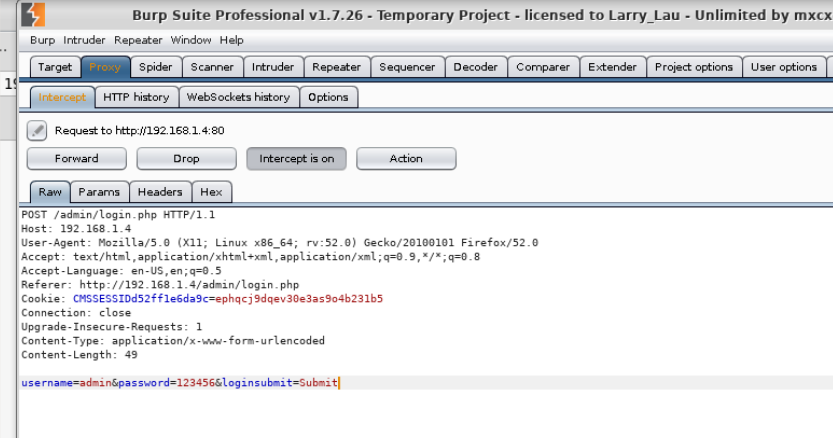
1. 在网站中输入用户名admin密码123456



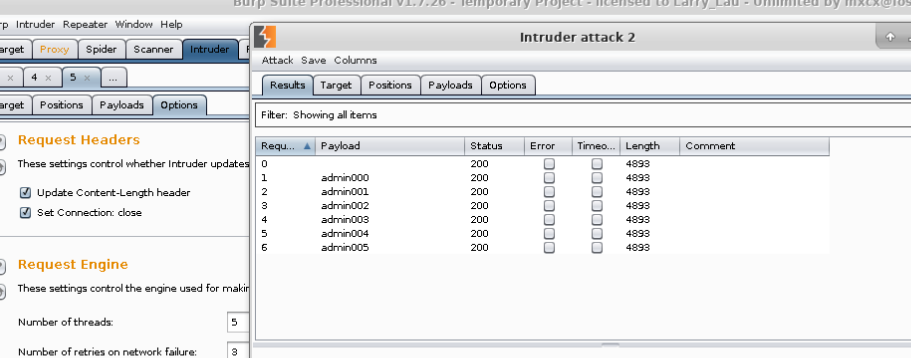
1. 配置manual proxy

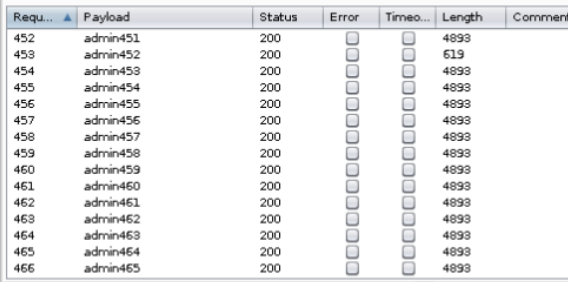


1. 在网页中提交账户密码，使用burpsuit拦截数据包



1. 在burpsuit中使用之前创建的password.txt作为字典，暴力破解password





破解出密码为admin452

**3.任务三**

【**任务描述**】

本实验任务在任务二操作完成的基础上，上传目标机网站的webshell,然后利用获取的网站webshell权限，查看目标主机信息,提交目标主机远程桌面端口号，为下一任务添加用户，完全控制目标主机系统做环境准备。

通过完成本实验任务，要求学生理解webshell的概念，掌握webshell上传方法，以及通过webshell查看目标机信息的方法。

【**实验目标**】

熟悉网站wenshell的概念，理解上传webshell、获取webshell权限的意义和方法。

掌握通过网站webshell信息获取其用户及密码信息的方法。

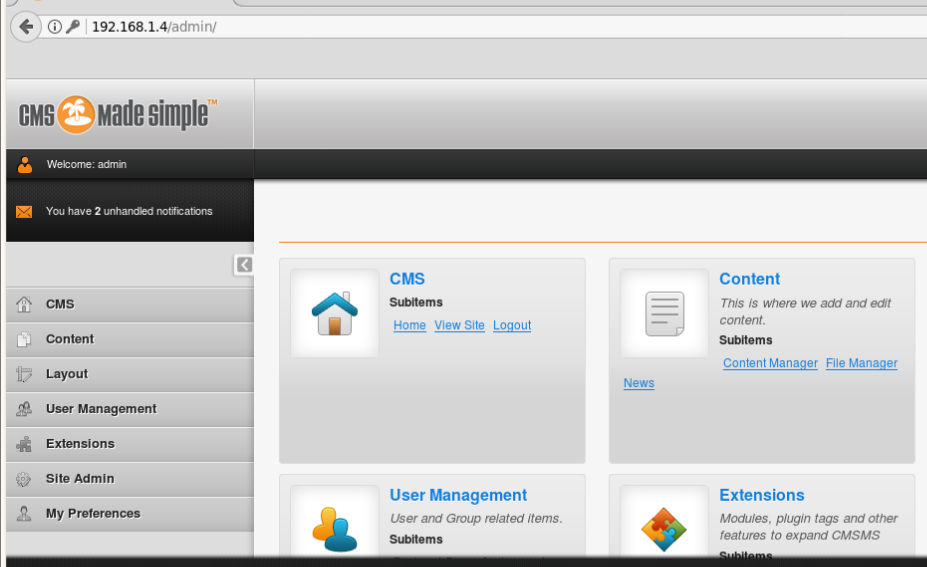
掌握通过webshell查看目标机关键信息的方法。

【**实验工具**】

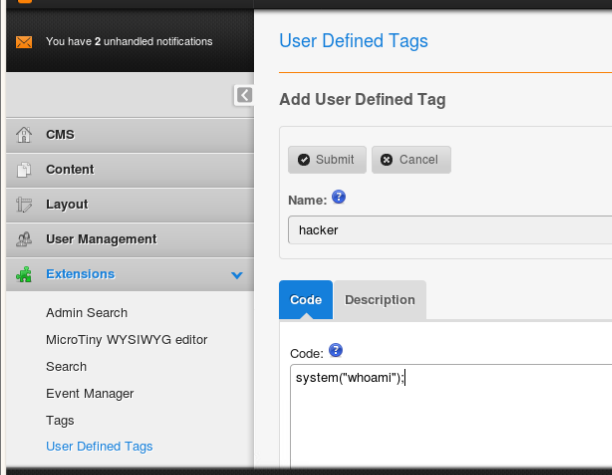
Firefox（火狐浏览器）

【**操作步骤**】

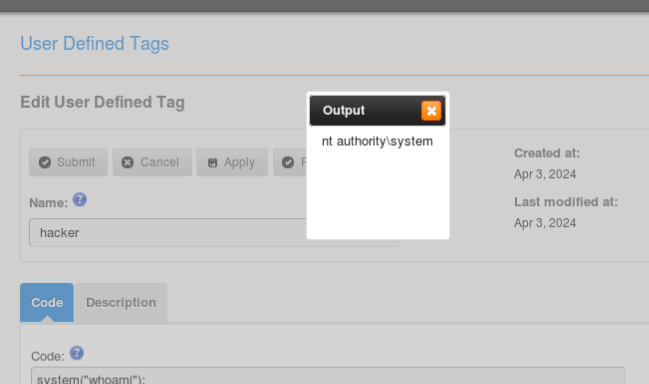
1. 登录目标网站



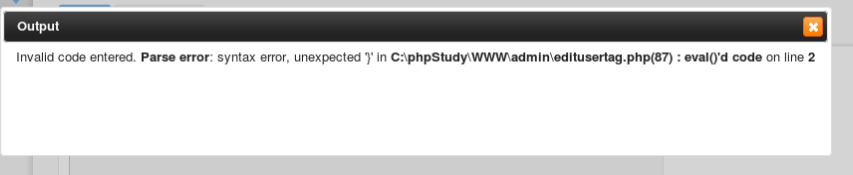
1. 设置用户自定义标记



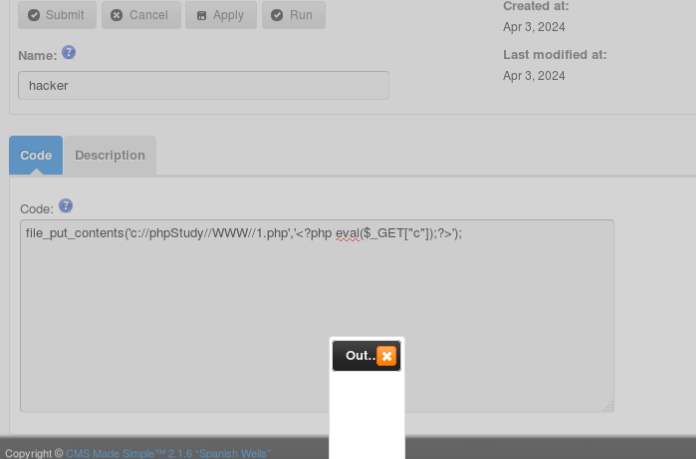
1. 点击Run后返回结果



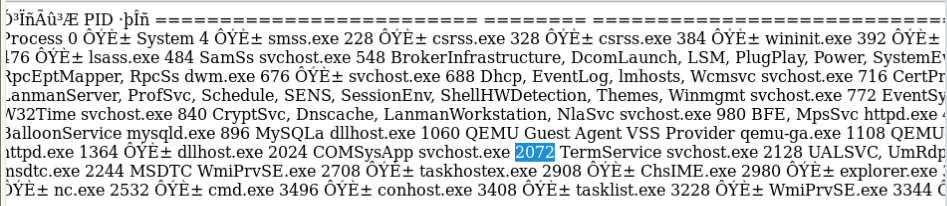
1. 通过随便在code中写入东西触发错误获得目录



1. 上传一句话木马

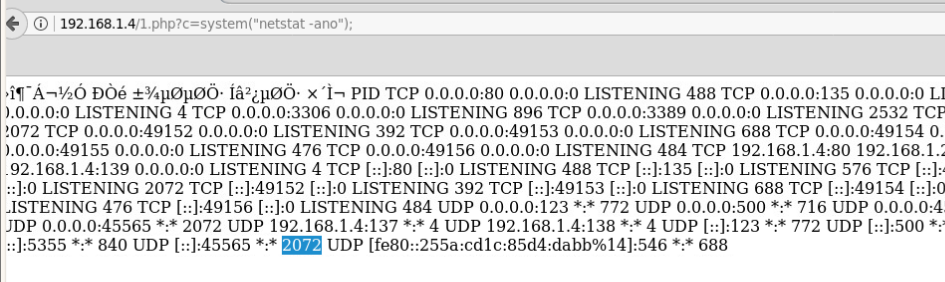


1. 查看目标主机开放的远程桌面端口，命令：192.168.1.4/1.php?c=system(“tasklist -svc”);



发现端口为2072

7.使用system(“netstat -ano”);查看端口号



可以看到是45565

**4.任务四**

【**任务描述**】

本实验任务在任务三操作完成的基础上，向目标机添加新用户，并完全控制目标主机系统。

通过完成本实验任务，要求学生在掌握webshell上传及权限获取方法的基础上，掌握向目标机添加新用户，设置用户权限并实现目标机控制的方法，进而掌握企业级复杂网络webshell相关的高级漏洞挖掘和利用方法，具备高级漏洞挖掘和利用、信息系统安全管理的职业能力。

【**实验目标**】

理解webshell权限获取的意义和方法。

掌握获取webshell权限基础上控制目标机的方法。

掌握企业级复杂网络漏洞挖掘和利用方法。

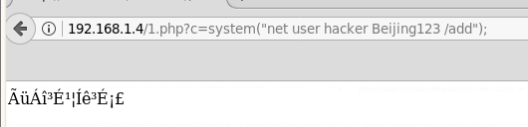
具备高级漏洞挖掘和利用职业能力。

【**实验工具**】

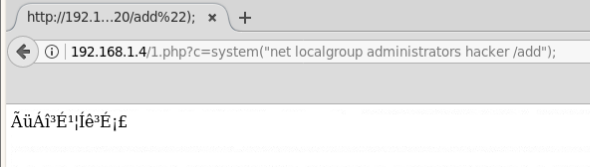
Firefox（火狐浏览器）

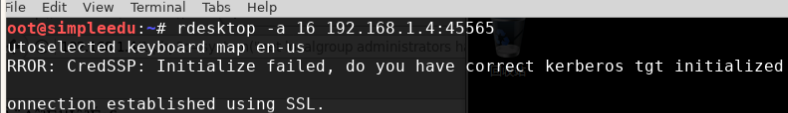
【**操作步骤**】

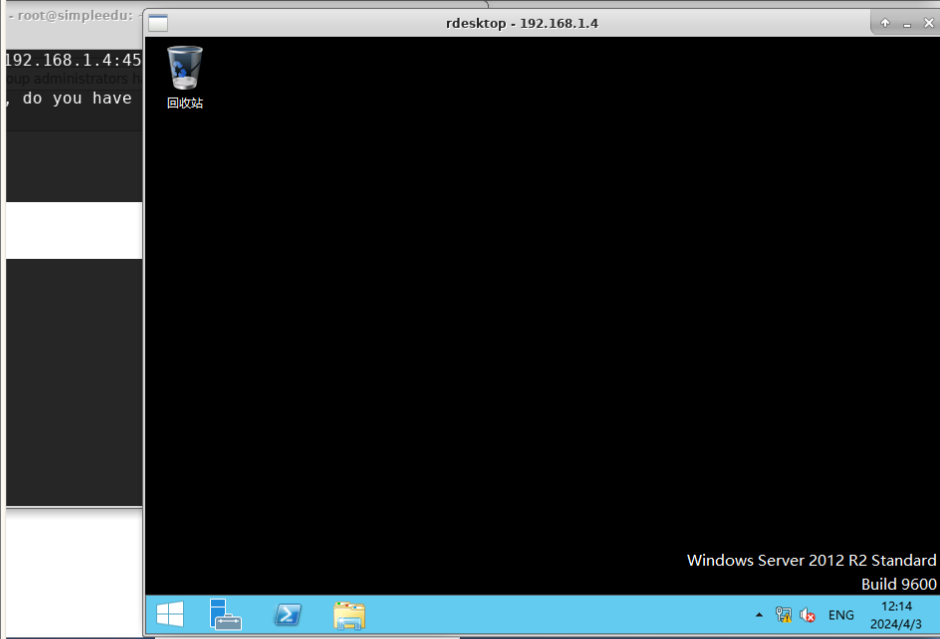
1. 向目标网站添加新用户



1. 将hacker添加进管理员组，并通过刚才的端口远程连接

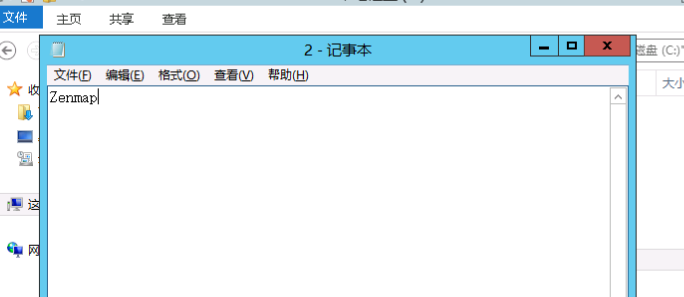






1. 设置目标机C:\2.key可读权限并查阅





可以看到内容是“Zenmap”

三、实验总结

本次实验虽然引入了一些关于metaspoilt的内容，但总体上还是和上次实验强关联，算是对上次实验的深入巩固。除此之外，还掌握了burpsuit工具的基本功能，掌握其暴力破解密码的基本方法，还有通过nikto对网站进行侦查的技术，学到的东西还是很多的，对于php和一句话木马更加熟练了，还有抓包操作，亲自上手进行对于日常的安全思想无疑有着巨大的帮助。