Linux灾难恢复：

Root密码修复

Centos single

Filesystem是硬盘文件根目录，无法再cd ..就像macitosh 硬盘图标

Pwd：显示绝对路径

MBR修复

模拟MBR被破坏和修复

C语言死循环程序

#include<stdio.h>

int main(void)

{

Int a;

While(1)

{printf(“please input your number”);

Scanf(“%d”,&a);

Printf(“your input is %d、n”,a);

}

{挂载：mount [-参数][设备名称][挂载点]

挂载点是一个目录

BIOS包含post加电自检

Basic input output system

一组固化到计算机主板上ROM芯片上的程序，保存着输入输出程序、加电自检程序、自启动程序

Cmos

Bios分为三部分

第一部分：加电自检：硬件检查

第二部分：初始化

第三部分：引导程序：引导操作系统从开始扇区（第一个扇区）读取引导记录，把电脑控制权转给引导记录。

本机子进入bios：Fn+F2（狂按）

Bios—MBR—boot loader—kernel、initrel？

Web安全：

Webshell

一句话木马

提权

后门

跳板

弱口令：

社工

很low的password

http

ftp

ssh

远程拒绝服务：损人不利己的攻击

远程溢出：业界最凶残，最暴力的KO方法

跨站漏洞

窃取用户cookie/影响用户体验

<script>alert(“xss”)</script>

网页挂马

<iframe src=”mm.html”width=”0”height=”0”></iframe>

上传漏洞

双文件、后缀、解析

目录遍历/文件下载

信息泄露

测试文件：  
<http://10.0.0.111/test.php>

站点绝对路径——DOCUMENT\_ROOT

操作系统类型

应用版本信息——SERVER\_SOFTWARE

错误处理：

<http://10.0.0.111/cmseasy/index.php?case=archive>

解析漏洞

Apache

Test.php.xx

IIS

Test.asp/test.jpg

Test.asp;1.jpg

编辑器漏洞

Fckeditor

Ewebeditor

<http://10.0.0.8/ewebeditor/db/ewebeditor.mdb>

本地文件包含

用户文件

http://10.0.0.111/index .php?lang=../../../../../../../etc/password

万能密码：

1’ or ‘1’=’1

Select \* from user where n=1’ or ‘1’=’1

认证绕过/SQL注入漏洞/写权限漏洞

框架漏洞

Struts2远程命令执行

<http://10.0.0.6:8080/ims/ims/userLogin.action>

ThinkPHP任意代码执行漏洞

<http://10.0.0.6:99/index.php?s>=

【常见的攻击密码】

口令猜解/暴力破解

XSS盲打

SQL注入

远程溢出

文件上传

敏感文件泄露

解析漏洞攻击

拒绝服务攻击

本地提权

逻辑漏洞

命令

Whoami

Ifconfig

Nutstat –ntlp

Ls

Cat

Service\_\_\_\_\_ start/stop

Wget

Apt-get

Curl

Ipython

作业：

网上下载一份php源代码

放在/var/www/html目录下

使用拼接方式形成SQL语句

Sql\_login=”select password from user where username=”.$\_post[user]

Information schema

1.判断注入点：数值+- 字符’ “

2.order by (十二分法) 猜列数

3.union select 1,2,3,4,5（id name age - - ）

找到网页上输出位置

4.在输出位置填入敏感函数测试

5. 利用information\_schema库读出目标库名称

6. 利用information\_schema库读出表名称

7. 利用information\_schema库读出列名称

8. 利用information\_schema库读出敏感数据

1.spl-u(urt)—dbs

-D库—tables

-D库-T关心表—columns

-D库-T表-C关心列—dump

-V 1-7

Where id=.$\_GE[id’]

二次注入