

黑客指南(v0.7.4) 原帖

关于破解系统, 游戏基础, 提示和游戏小技巧的指南

老工具

sshrack, sshguest, shellmail, sshnuke, shellweb, sshescale, ftpnuke, web3xploit 这些先前的工具已经被**移除**. 你需要使用新的工具, 或者自己写你自己的工具

你将需要的工具

预装工具

- **whois**: 你可以用这个来获取一个服务器拥有者的联系方式和其他信息
- **nslookup**: 获取一个域名的IP地址
- **scanlan.exe**: 查看你所连接的网络下的其他设备
- **ssh**: 通过远程机器的用户名和密码来链接远程主机的ssh服务
- **ftp**: 通过远程机器的用户名和密码来链接远程主机的ftp服务
- **logviewer**: 查看和清除电脑的log
- **ping**: 检查远程主机是否可以连接

普通商店的工具

- **nmap**: 获取特定IP的开放端口情况
- **smtp-user-list**: 获取特定IP在SMTP服务器
- **ConfigLan**: 用来管理你租的服务器或者配置网络

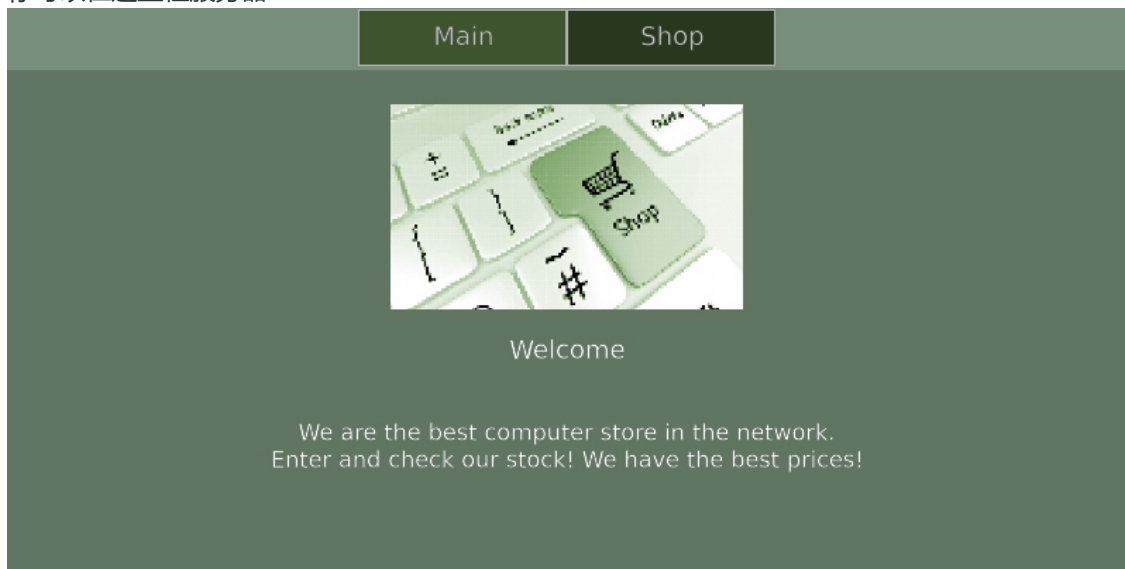
黑客商店的工具

- **AdminMonitor.exe**: 当管理员上线和开始主动追踪你的时候发出警告. 以防万一, 尽量一直在后台挂着.
 - **decipher**: 用来破解密码
 - **scanlib**: 如果你不想写你自己的破解工具, 不要下载(分析一个库(library), 展示该库的弱点 -- 译者注)
 - **scanrouter**: 用来扫描kernal_router.so库. 必要
 - **metasploit.so**: 所有的**破解**都需要这个库, 让它保持在最新版本.
 - **crypto.so**: 所有的**解密**都需要这个库, 让它保持在最新版本.
 - **Sniffer**: 在路由器上运行并等待, 可以截获密码
 - **rshell-server** 和 **rshell-interface**: 你需要在你租的服务器上安装rshell-server来运行rshell-interface(自己的服务器也可以, 但不建议这样做, 会留漏洞 --译者注). 这两个工具能够在你和你的受害者之间建立连接, 然后你就可以为所欲为. 这个需要配合社工使用, 参见社工部分
 - 如果你不知道在**exploits**下你需要什么, 点开在右边的服务列表并好好读读(在上面的select library 下拉菜单中 -- 译者注)
-

商店在哪里

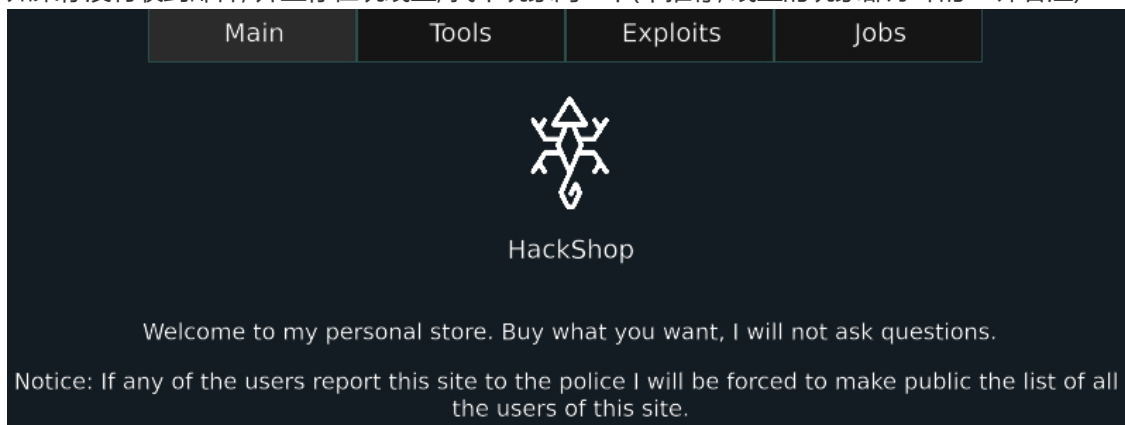
普通商店

- 打开**Browser**, 在搜索框里输入shop.
- 随便找一个网址点进去
- 你可以找到**nmap**, **smtp-server-list**, **http-server**, **ssh-server**, **ftp-server** 和 **电脑配件**.
- 你可以在这里租服务器



黑客商店

- 在完成教学任务后你会收到包含黑客商店IP的邮件
- 如果你没有收到邮件, 并且你在玩线上, 找个玩家问一下(不推荐, 线上的玩家都好坏的 -- 译者注)



黑客商店是空的

你的打开方式不对. 你需要点**exploits**然后里面是一些预先准备好的工具(新版本需要点libraries的下拉菜单来找到某个漏洞需要的破解 -- 译者注).

如果你还是不知道你需要什么破解工具, 参见[你需要的工具](#)

入侵工具在哪里

去到黑客商店并进入**exploits**部分, 你需要用一些游戏自带的破解去进行入侵.

如果你不知哪里有黑客工具, 参见[老工具](#)(已弃用 -- 译者注)

如果你还是不知道你需要什么破解工具, 参见[你将需要的工具](#)

破解wifi密码

- 打开终端, 输入如下命令

```
airmon start wlan0
```

- 现在输入如下指令来查看可连接的WiFi

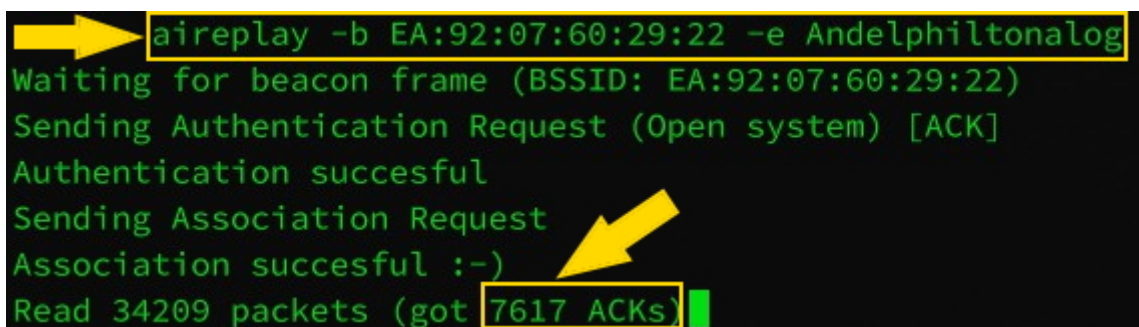
```
iwlist wlan0
```

- 选一个信号最强的(抓包最快)

BSSID	PWR	ESSID
EA:92:07:60:29:22	41%	Andelphiltonalog
C9:84:EB:51:49:42	27%	Yukoshkoshko_04UTT
DA:51:3E:DE:82:0F	19%	Stee
25:87:FB:FE:C0:95	25%	Woodyea
20:51:0D:8D:F5:6A	27%	Iture_1CA

- 现在像图片中这样输入aireplay命令

```
aireplay -b bssid -e essid
```



```
➡ aireplay -b EA:92:07:60:29:22 -e Andelphiltonalog
Waiting for beacon frame (BSSID: EA:92:07:60:29:22)
Sending Authentication Request (Open system) [ACK]
Authentication succesful
Sending Association Request
Association succesful :-)
Read 34209 packets (got 7617 ACKs)
```

- 当它收集到足够的ack包之后使用ctrl+c来停止抓包(所需的ack包参见[WiFi信号强度所对应需要的ack包数量](#))
- 现在输入如下指令

```
aircrack file.cap
```

它会告诉你密码

- 现在你可以在右上角输入密码链接WiFi了

WiFi信号强度所对应需要的ack包数量

Signal Power	Required ACKs	Signal Power	Required ACKs	Signal Power	Required ACKs	Signal Power	Required ACKs
1%	300000	26%	11538	51%	5882	76%	3947
2%	150000	27%	11111	52%	5769	77%	3896
3%	100000	28%	10714	53%	5660	78%	3846
4%	75000	29%	10345	54%	5556	79%	3797
5%	60000	30%	10000	55%	5455	80%	3750
6%	50000	31%	9677	56%	5357	81%	3704
7%	42857	32%	9375	57%	5263	82%	3659
8%	37500	33%	9091	58%	5172	83%	3614
9%	33333	34%	8824	59%	5085	84%	3571
10%	30000	35%	8571	60%	5000	85%	3529
11%	27273	36%	8333	61%	4918	86%	3488
12%	25000	37%	8108	62%	4839	87%	3448
13%	23077	38%	7895	63%	4762	88%	3409
14%	21429	39%	7692	64%	4688	89%	3371
15%	20000	40%	7500	65%	4615	90%	3333
16%	18750	41%	7317	66%	4545	91%	3297
17%	17647	42%	7143	67%	4478	92%	3261
18%	16667	43%	6977	68%	4412	93%	3226
19%	15789	44%	6818	69%	4348	94%	3191
20%	15000	45%	6667	70%	4286	95%	3158
21%	14286	46%	6522	71%	4225	96%	3125
22%	13636	47%	6383	72%	4167	97%	3093
23%	13043	48%	6250	73%	4110	98%	3061
24%	12500	49%	6122	74%	4054	99%	3030
25%	12000	50%	6000	75%	4000	100%	3000

可能需要比图片所需ack更多的包数量

第一个任务

(由于原帖中是一个YouTube的视频链接所以说这里采用语言描述的形式来进行指导)

- 把邮件中的decipher下载到本地bin文件夹下(/bin)
- 在普通商店中下载nmap, 下载到本地bin文件夹下
- 收到邮件后往下翻看到邮件中的IP地址. 拷贝下来.(以下的[IP]都指这个IP)
- 在命令行中输入.

```
whois [IP]
```

来获取IP地址的管理员的信息, 记住其中的"name".

- 给邮件中的邮箱地址发消息, 在social engineering中找到"administrative Action(行政行为)".
- 按照提示给的空档填入即可(administrator name 用之前whois获得的name, 第一个名字用邮件中提供的名字)
- 如果正确的话, 对方应该会回复密码
- 执行以下命令:

```
nmap [IP]
```

来检查IP的开放端口(一般就只有一个ssh)

- 执行以下命令, 用ssh链接服务器

```
ssh [name]@[IP]
```

其中[name]是邮箱@符号前面的名字

- 如果连接成功的话终端会变色.
- 在变色的终端输入

```
FileExplorer.exe
```

来打开图形化的文件管理器

- 找到Config文件夹, 把其中的mail.txt拷贝到本地(拖到桌面上)
- 新打开一个终端, 输入如下命令:

```
decipher ../Desktop/Mail.txt
```

- 等进度条走完, 给原邮件回复获取到的密码, 他会给你回复一个IP, 即黑客商店的IP

权限等级

- **Guest:** 就像它的名字一样, 如果你拥有的是guest权限, 你不能访问一些我非常重要的系统文件和文件夹, 并且只能运行特定的命令. 但是你可以访问 `/home/guest` 下的文件和一些未经保护的用户文件和文件夹
- **非root(non-root):** 一个non-root用户是一个在这台计算机上注册了的用户. 你可以访问你的用户文件夹和其他大多数系统文件夹, 执行大多数命令.
- **root:** 拿到root权限至关重要. 如果你是root用户, 你可以在机器上为所欲为. 所以说, 如果你想要在被入侵机器上进行你想要的操作, 你必然需要root权限.

apt-get

什么是apt-get

apt-get是一个包管理器. 它让你能够使用命令行下载程序或运行库.

官方的repository默认被开启.

你也可以把黑客商店作为repository添加.

你也可以设置你自己的repository, 细节参见[如何搭建特定服务器](#)

apt-get相关命令

在你开始使用apt下载, 升级或搜索包之前, 永远记住先运行这个命令:

```
sudo apt-get update
```

如果你想要升级你的系统或安装的包, 使用这个

```
sudo apt-get upgrade
```

使用这个来下载

```
sudo apt-get install [package or lib name]
```

使用例:

```
sudo apt-get install init.so
```

使用这个来搜索包

```
sudo apt-get search [package or lib name]
```

使用例:

```
sudo apt-get search kernel
```

使用这个来查看某个repository的所有包

```
sudo apt-get show [address]
```

使用例:

```
sudo apt-get show 182.182.9.21
```

使用这个来添加一个repository

```
sudo apt-get addrepo [address]
```

使用例:

```
sudo apt-get addrepo 182.182.9.21
```

注意: 在在线模式中添加其他玩家的repo时请小心

CHMOD速查表

+	添加权限
-	移除权限
-R	应用到子文件
u	用户(拥有者)
g	组
o	其他人和游客
r	读
w	写
x	执行

永远使用sudo运行该命令

使用例

移除拥有者的读权限

```
chmod u-r /home/user/document.txt
```

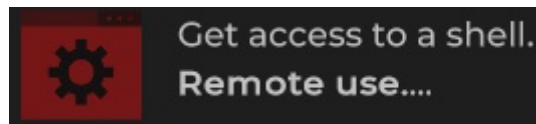
向除了拥有者所有人(包括)给予写入和执行权限, 并应用到所有子文件夹和文件

```
sudo chmod -R o+wx /home/user/myfolder
```

HTTP

- 你需要libhttp的破解来破解http服务
- **你需要获得shell来进行连接**
- 如果描述说的是"get access to a shell", 那么就可以用来连接

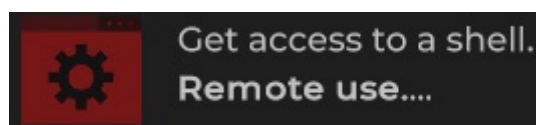
样例破解



SSH

- 你需要libssh来破解ssh服务
- 如果你知道用户名和密码, 你可以通过ssh连接. 你也可以用提供shell access的破解来建立连接
- 阅读在hackshop中的描述. 如果它提到了"获取shell", 那么你就可以用它来连接. 或者如果你知道用户名和密码, 你就可以使用ssh直接连接.

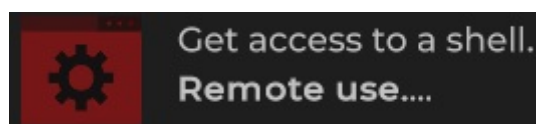
样例破解



FTP

- 你需要libftp漏洞来入侵一个ftp服务
- 如果你知道用户名和密码, 可以使用ftp命令来连接. 你也可以使用提供shell权限的漏洞来连接.
- 阅读在hackshop中的描述. 如果它提到了"获取shell", 那么你就可以用它来连接. 或者如果你知道用户名和密码, 你就可以使用ftp直接连接.

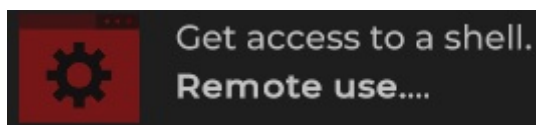
样例破解



SMTP

- 你需要libsmtp漏洞来入侵smtp服务
- 使用smtp-user-list来获取机器的用户列表
- 你需要获取shell来连接
- 阅读黑客商店的漏洞描述. 如果它说获得访问shell的权限, 就可以用来连接

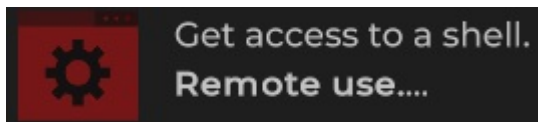
样例破解



聊天室(chat room)

- 你需要libchat漏洞来入侵聊天室
- 你需要shell权限来连接运行聊天室的服务器
- 阅读黑客商店的漏洞描述. 如果它说获得进入shell的权限, 你可以用它来连接

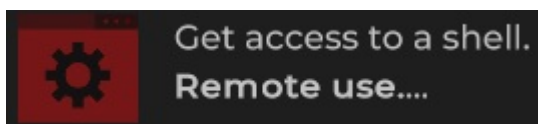
样例破解



未开放的端口(closed ports)

- 你需要libsql漏洞来入侵一个未开放的端口
- 你需要在同一个网络中才能连接到未开放的端口
- 你需要shell权限来连接
- 阅读黑客商店的漏洞描述. 如果它说获得对shell的访问权, 你可以用它来连接

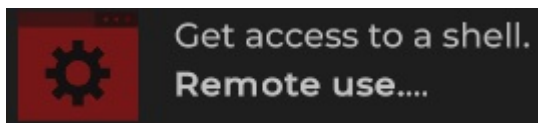
样例破解



监控摄像头(cams)

- 你需要libcam漏洞来入侵一个安全摄像头
- 你需要shell权限来连接
- 阅读黑客商店的漏洞描述. 如果它说获得对shell的访问权, 你可以用它来连接
- 安全码(security code)是root用户密码

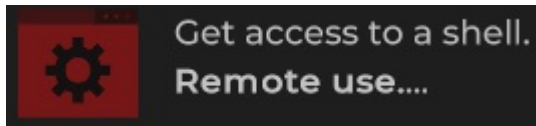
样例破解



反向shell(rshell server)

- 你需要librshell漏洞来入侵rshell服务。
- 阅读黑客商店的漏洞描述. 如果它说获得对shell的访问权, 你可以用它来连接。

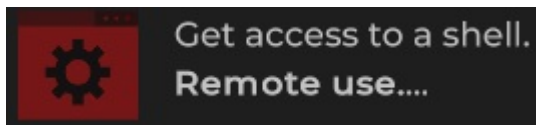
样例破解



students学生 / employees雇员 / criminals罪犯

- 你需要libsql的漏洞来入侵。
- 如果它是封闭端口，你需要在该网络中才能连接。
- 你需要shell权限来连接。
- 阅读黑客商店的漏洞描述。如果它说获得对shell的访问权，你可以用它来连接。

样例破解



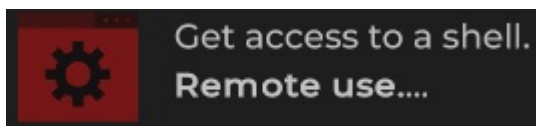
无开放端口

- 如果你没有看到任何端口，请连接路由器。点击[如何连接](#)获取详细信息。
- 你可以试试反向shell，你可以在邮件中使用"有趣的游戏Funny Game"模板来发送反向shell给NPC。点击 [社会工程学](#)并阅读 "有趣的游戏Funny Game"。
- 点击 [如何入侵本地的其他主机](#)查看更多信息。

路由器(routers)

- 你需要kernel_router的漏洞来入侵路由器。
- 你需要利用漏洞来连接路由器。
- 使用scanrouter工具来了解版本号。

样例破解



防火墙(firewalls)

- 你需要kernel_router的漏洞来禁用防火墙。

样例破解



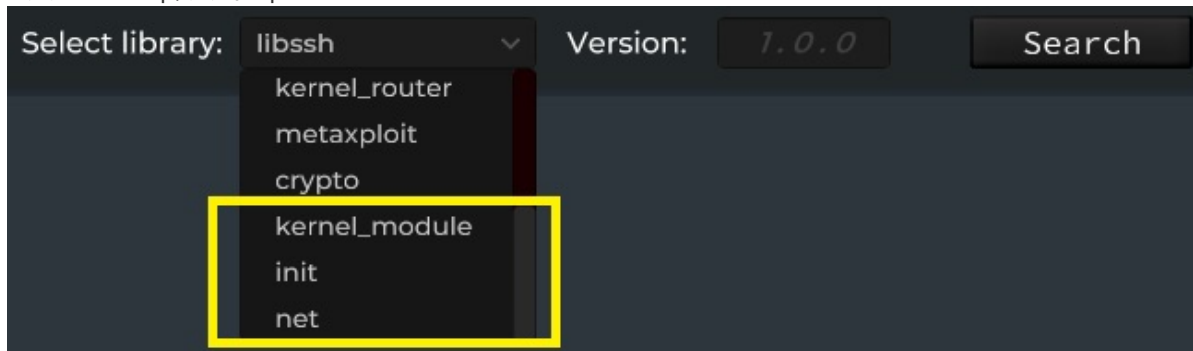
本地库(local libraries)

- 默认的本地库有：
 - kernal_module.so

- net.so
- init.so
- 在hackshop中, 本地库的名字对应着相应的破解
- 如果你不知道版本号, 参见[如何确定库的版本号](#)

本地破解

去到hackshop, 点击Exploits



- 选择一个本地库, 输入版本号来搜索.
- 找一个破解, 阅读描述
 - 如果你不知道找哪些库, 参见
- 参见 ["如何本地入侵"](#)

如何确定库的版本号

- 社工
- 如果你不知道社工的名字或者邮箱, 参见[如何找到社工所需的名字和邮箱](#)
- 如果你想要知道你的版本号, 使用如下代码(复制到codeeditor中, 编译, 存储到home文件夹, 运行):

```
metasploit = include_lib("/lib/metasploit.so")
if not metasploit then metasploit =
include_lib(get_shell.host_computer.current_path+"/metasploit.so")
if not metasploit then exit("Can't find metasploit.so in /lib folder or current
folder.")
if params.len == 0 then exit("You have to specify full path.\nTarget file must
be library.\nusage: "+program_path.split("/")[-1]+" /folder/filename.so")
lib = metasploit.load(params[0])
if not lib then exit("You have to specify full path.\nTarget file must be
library.\nusage: "+program_path.split("/")[-1]+" /folder/filename.so")
print(lib.lib_name+" = "+lib.version)
```

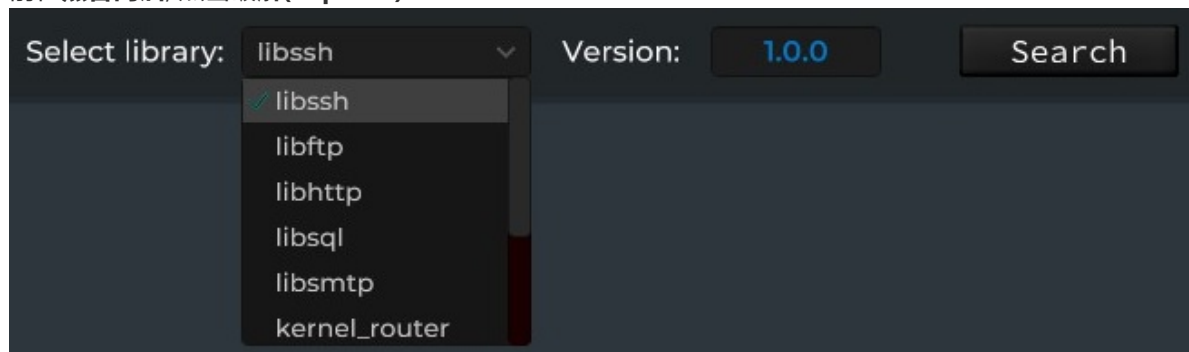
如何远程入侵

使用nmap, 查看结果

PORT	STATE	SERVICE	VERSION	LAN
80	open	http	1.0.0	192.168.0.2
3306	closed	employees	1.0.0	192.168.0.3

你可以看到**服务名称(service)**和 **版本号(version)**

前往[黑客商店](#), 点击[破解\(exploits\)](#):



- 在下拉菜单中选择**服务对应的库(library name)**, 输入版本号, 点击搜索.
- 在出现的破解中选一个, 读一读描述. 你就会知道这个破解能够干什么, 需要什么样的先决条件.
- 下载其中一个并运行

如果你不知道选哪一个, 参见前文对应的服务名

如果先决条件没有被满足, 破解不会生效

如果破解没有生效

- 换一个破解
- 尝试其他端口
- 如果你收到了用户/管理员在线(active user/root)的警告, 尝试社会工程学让他们上线
- 如果你收到了破解版本不符(**mismatched version numbers**)的警告, 尝试另外一破解
- 如果没有端口开放, 尝试使用路由器(router)破解.
- 还是不行的话, 换个任务或者换个目标去入侵

如果你黑入了远程机器, 参见[如何本地入侵](#)

如果你尝试获得了一个非root用户的密码

- 确定你连接到了远程服务器且拥有shell. 如果你没有连接, 参见[如何连接](#)
- 如果你是guest, 使用**sudo -u**来切换用户或者**sudo -s**来成为root.
- 如果你是非root用户, 使用**sudo -s**来成为root

你必须清除你的log. 如果你不知道怎么清除log, 参见[如何清除记录\(log\)](#)

如何本地入侵

如果你拿到了shell, 但不是root用户...

- 找一个本地破解(local exploit)
 - 如果你不知道在哪里找, 参见[本地破解](#)
- 确定你已经拿到了shell
- 在你找本地破解之前, 利用社工来获得本地 **kernal_module.so**, **init.so**, **net.so**库的版本号
 - 社工邮件标题选择 "**system information**"
- 如果你不知道如何找到社工所需的邮件, 参见[如何找到社工所需的名字和邮箱](#)
- 从hackshop找一个kernal_module, init或net库的破解
 - 优先选择给root权限的, 如果没有, 选择给非root用户权限的

- 在你连接的机器上, 运行Browser.exe来下载破解, 或者从你的电脑上传到远程的/home/guest目录下
- 如果收到了缺失metasploit.so或者crypto.so, 从你的电脑的/lib下找到他们并放到你破解的目录下
- 如果你改动了一个用户的密码, 你可以使用 `sudo -u` 来切换到那个用户
- 如果你获得了一个用户的权限, 把/etc/passwd拷贝到本地, 用 `decipher` 破解, 然后 `sudo -s` 变为root权限
- 你可以使用 `scp -d` 来下载文件, 或者是使用图形化的FileExplorer.exe(没人会用scp的 -- 译者注)
- 如果你通过ftp连接, 通过 `get /etc/passwd` 来下载密码文件
- 如果你获得了root密码, 运行 `sudo -s`

你使用破解重设的密码的用户名会出现在终端的运行结果中

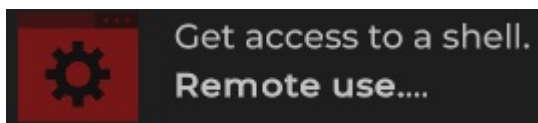
如何入侵本地的其他主机

- 不要断开连接或者使用 `exit` 命令
- 使用 ScanLan.exe 来查看网络中的设备
- 使用 `nmap` 命令扫描目标的lan ip
- 把漏洞上传到你连接的设备上, 并运行漏洞

如何连接

- 如果是ssh, 运行ssh命令。
- 如果是ftp, 运行ftp命令。
- 如果你想直接连接到路由器, 你需要提供shell权限的漏洞。
- 如果你不知道密码, 你必须入侵目标。点击右边的 [如何远程入侵](#)并阅读它。
- 你需要提供shell权限的漏洞来连接任何东西。
- 如果漏洞描述说获得访问shell的权限, 你可以用它来连接。否则, 你不能连接...
- 如果你已经连接了并且不知道该怎么, 点击右边的 [如何本地入侵](#)并阅读它。

样例破解



破解没有达到预期或无法运行

- 获得另一个漏洞。
- 尝试入侵其他端口。
- 如果你得到一个关于'活跃用户'/'root'的警告, 尝试社会工程。
- 如果你得到一个关于版本号不匹配的警告, 尝试另一个漏洞。
- 如果没有剩下的端口可以黑, 试试路由器漏洞或rshell。
- 还是不走运吗? 找另一份job/mission/quest或黑掉另一个东西。

如果不符合要求，漏洞将不工作。

如何完成任务

- 损坏数据 (Corrupt Data)
 - 连接到目标。如果你不知道如何连接，请点击[如何连接](#)并阅读它。
 - 你必须成为root。如果你不知道如何成为root，点击[如何获取root权限](#)并阅读它。
 - 删除 /boot 文件夹。你可以从FileExplorer.exe中找到并删除它，或者直接输入 `rm -r /boot` 并点击回车。
 - 运行 `reboot` 命令。
 - 回复邮件。输入任何东西并发送。
- 找/解密密码 (Credentials)
 - 如果你有passwd密码文件，你不需要连接到目标。你可以找到一个可以破解passwd文件的漏洞，不需要额外的工作。
 - 如果你找不到或者无法破解密码文件，请连接到目标。如果你不知道如何连接，请点击[如何连接](#)并阅读它。
 - 你需要至少获得非root用户的权限。
 - 在目标机上运行FileExplorer.exe。打开 /etc 文件夹，把passwd文件拖到你的电脑上，然后运行解密。
 - 你可以运行 `scp -d /etc/passwd` 命令来下载passwd文件。之后，运行解密。
 - 如果是 FTP 服务器，使用 `get /etc/passwd` 命令来下载 passwd 文件。
 - 如果你获得了密码，只使用密码或user_name:password回复邮件。
- 修改学位 (Academic Changes)
 - 连接到目标。如果你不知道如何连接，请点击[如何连接](#)并阅读它。
 - 你必须至少获得非root用户的权限。如果你不知道如何做，点击[如何远程入侵](#)并阅读它。
 - 在目标上运行FileExplorer.exe并搜索StudentsViewer.exe。
 - 在目标上运行StudentsViewer.exe，找到人并更改记录。它版本必须至少是7.0
 - 回复邮件。输入任何内容并发送。
- 犯罪记录 (Police Records)
 - 连接到目标。如果你不知道如何连接，请点击[如何连接](#)并阅读它。
 - 你必须至少获得非root用户的权限。如果你不知道怎么做，点击[如何远程入侵](#)并阅读。
 - 在目标上运行FileExplorer.exe，搜索PoliceRecord.exe。
 - 在目标上运行PoliceRecord.exe，找到人并更改记录。
 - 回复邮件。输入任何东西并发送。

如果你黑了什么，你必须清除日志。如果你不知道如何清除日志，请点击[如何清除记录log](#)并阅读它。

隐藏任务: 如何找到隐藏任务

什么是隐藏任务？

隐藏任务是一种不能在黑客商店找到的任务类型。有很多隐藏任务，而且这些隐藏任务比黑屋任务更加多样化。

如何找到隐藏任务？

- 黑掉一些东西并四处查看，阅读日志、文本和pdf文件。
- 试着找出正在发生的事情或已经发生的事情。
- 试着解开谜题

社会工程学

管理行动(Administrative action)

- 用这个来获取用户密码。
- 你可以使用 `whois` 命令来获得额外的信息。
- 你可以使用 `smtp-user-list` 来获得额外的信息。
-

登录问题(Login issues)

- 使用这个来获取用户密码。
- 你可以使用 `whois` 命令来获得额外的信息。
- 你可以使用 `smtp-user-list` 来获得额外的信息。

在线用户(Online user)

- 用这个来使非root用户在线。
- 公司名称是域名。
- 你可以使用 `whois` 命令来获得额外的信息。
- 你可以使用 `smtp-user-list` 来获得额外的信息。

在线管理员(Admin online)

- 使用这个命令可以使根用户在线。
- 公司名称是域名。
- 你可以使用 `whois` 命令来获得额外的信息。

系统信息(System information)

- 用这个来了解目标上安装的库的版本号。
- 你必须向一个非root用户发送邮件。
- 你必须在[姓名]栏中输入一个非root用户的名字。
- 你必须写出库的名称。(例如：net.so)

远程登录

- 不言自明

有趣的游戏

- 它是rshell的专属。
- 设置你的rshell服务器
- 如果你不知道如何设置一个服务器。点击[如何搭建特定服务器](#)并阅读它。
- 然后点击附件。
- 填写空字段并点击应用，然后发送。
- 现在运行rshell-interface。

CCTV访问请求

- 这是为网络/安全摄像头准备的。

如果你不知道在哪里可以找到用于社会工程的名字和电子邮件，请点击[如何找到社工所需的名字和邮箱](#)并阅读它。

如何找到社工所需的名字和邮箱

- 如果服务器存在EmployeesViewer.exe, 你可以用它来查看邮箱.
 - 如果你已经拿到了shell, 查看/home文件夹来找名字
 - 如果你没办法查看home文件夹, 使用 `ls /home` 来查看
 - 在/home/[用户名]/config文件夹中会有邮箱(Mail.txt)
 - 如果你没办法查看home文件夹, 使用 `cat /home/[用户名]/Config/Mail.txt` 来查看
 - 如果SMTP服务在运行, 你可以使用 `smtp-user-list` 来查看邮箱
-

如何获取root权限

- 如果你已经连接并知道密码，使用sudo -s命令来获得root权限。
 - 如果你不知道密码，也没有连接，点击[如何远程入侵](#)并阅读它。
 - 如果你已经连接，但不知道密码，点击[如何本地入侵](#)并阅读。
 - 如果你不知道如何连接，点击[如何连接](#)并阅读。
-

如何切换用户或以另外一个用户的身份登录

- 如果你没有连接到目标，但你知道密码并且是ssh，运行 `ssh` 命令。
 - 如果你没有连接到目标，但你知道密码并且是ftp，运行 `ftp` 命令。
 - 如果你已经进入并且知道密码，使用 `sudo -u` 命令。
 - 如果你不知道密码，点击[如何本地入侵](#)并阅读它。
 - 如果你没有连接到目标，或不知道如何连接，或无法连接，点击[如何连接](#)并阅读。
-

如何获取银行账户

- 你不需要与目标连接。你可以找到一个可以破解银行密码的漏洞，不需要额外的工作。
- 如果你找不到或无法破解，请连接到目标。如果你不知道如何连接，请点击[如何连接](#)并阅读它。
- 你可以在目标机上运行FileExplorer.exe，并在 /home/user 文件夹中导航。
- 进入配置文件夹，在你的电脑上拖拽Bank.txt文件并运行解密。
- 你可以使用 `scp -d /home/username/Config/Bank.txt` 命令来下载证书。
- 如果是FTP服务器，使用 `get /home/username/Config/Bank.txt` 命令来下载Bank.txt文件。

- 之后，运行解密
- 如果你不知道任何用户名来使用上述命令，使用 `ls /home` 命令来查看用户名/文件夹。

你现在不能入侵银行系统。你只能单独入侵银行账户。

如何获取电子邮件账户

- 连接到目标。如果你不知道如何连接，请点击[如何连接](#)并阅读它。
你可以在目标机上运行FileExplorer.exe，并在 `/home/user` 文件夹中导航。
进入配置文件夹，在你的电脑上拖拽Mail.txt文件并运行解密。
你可以使用 `scp -d /home/username/Config/Mail.txt` 命令来下载证书。
如果是 FTP 服务器，使用 `get /home/username/Config/Mail.txt` 命令来下载 Mail.txt 文件。
之后，运行解密
如果你不知道任何用户名来使用上述命令，使用 `ls /home` 命令来查看用户名/文件夹。

你可以侵入电子邮件服务/网站。

- 侵入并进入任何邮件服务器。
- 你可以在数据库中找到账户和密码。
- 如果你得到了数据库，你可以打开并查看它或运行破译和破解密码。

如何入侵路由器

- 运行scanrouter来了解目标路由器的版本号。
- 从黑客商店下载一个kernel_router漏洞。
- 运行漏洞。
- 你可以用路由器漏洞入侵服务器/计算机。
- 你可以用路由器漏洞入侵密码/文件/文件夹。

如果一个漏洞不能用，就找另一个漏洞

如何清除记录log

- 你必须是root才能清除日志。
- 在目标上运行LogViewer.exe，清除获得的shell、连接路由和文件删除的条目，点击保存按钮。
- 如果是FTP，使用 `cd /var` 命令进入var文件夹，然后使用 `get system.log` 命令下载日志文件。
打开并编辑下载的日志文件，用 `put system.log` 命令重新上传。

加速破解速度

- 从正规商店购买更好的CPU。
- 更快的CPU会更快地破解密码和扫描其他东西。

FTP中的上传与下载

- 使用put命令来上传东西。
- 使用get命令来下载一些东西。
- 你只能在FTP服务器中运行预定义的命令。

- 运行help命令以获得更多信息。

防火墙设置

- 使用ifconfig命令，了解什么是网关IP。
- 打开浏览器。
- 在地址栏中输入你的网关IP，并添加：8080
- 它应该看起来像这样。



- 单击 "添加条目Add Entry"按钮，并像这样填写空白的文件。
- 单击 "防火墙Firewall"。
- 单击 "添加条目 "按钮。
- 填写空字段，并确保你不阻止你自己的计算机。
- 然后点击 "保存Save Button"按钮，保存你的配置。

如何自保

- 为了保护自己，你需要删除所有文件的访客权限。运行这个命令。

```
sudo chmod -R o-rwx /
```

- 获取1个或多个租用的服务器并一直使用它们。
- 为了保护你的租用的服务器，请输入以下命令。
- (如果你要创建和使用非root用户，这可能不适合你)
- (确保你租用的服务器的当前版本没有办法获得root权限)

```
sudo chmod -R o-rwx /
```

```
sudo chmod -R g-rwx /
```

```
sudo chmod -R u-rwx /
```

- 点击[如何生存](#)，并阅读它。
- 点击[如何防范嗅探器](#)并阅读它。
- 点击[如何防范反向shell](#)并阅读它。

如何生存

- 阅读游戏手册中的整个 "入门 "和 "高级 "部分。
- 如果你不想阅读整个 "入门 "部分，只需阅读 "游戏结束 "和 "高级 "部分。
- 从正规商店租用服务器并使用它们来做任何事情。它们可以隐藏你的真实IP，也是对付NPC的最好方法。
- 不要忘记清除可疑的日志。阅读游戏手册中的 "游戏结束 "或点击右边的 "如何清除日志 "并阅读它。
- 点击[如何自保](#)并阅读它。
- 如果你是在在线模式下，不要运行任何你不信任的东西。

安全模式

什么是安全模式？

- 安全模式是当重要的系统文件被删除、移动或损坏时，你将被转到安全模式。
- 在安全模式下，只有命令行，你不能运行文件资源管理器和其他类似程序，但你总是可以运行基于命令行的程序。
- 安全模式让你有机会恢复你的系统。
- 如果你想手动进入安全模式，运行 `reboot -sm` 这个命令。

如何防范反向shell

- If you are on single player, no need to worry.

如果在在线模式

- 你能做的最好的事情是不安装你不信任的东西。
- 你能做的第二件事是运行ps命令。一旦你运行它，你会看到机器上当前的工作进程。如果你看到一些不寻常的东西，用sudo的kill命令来终止rshell连接。

如何防范嗅探器sniffer

- 如果你是单人游戏，不必担心。

如果你是在在线模式下：

- 用记事本打开/server/conf/sshd.conf，把替换掉
- replace

```
"encryption_enabled": false,
```

with

```
"encryption_enabled": true,
```

- 然后保存它。
- ssh-server带有一个基本的加密算法，但熟练的程序员不难破解它。如果你想获得更好的加密，可以制作你自己的加密方式，或者找一个值得信赖的加密方式。

如何升级本地库

运行这两个命令（点击右边的apt-get，并阅读它以了解更多细节）。

```
sudo apt-get update
sudo apt-get upgrade
```

此外，你可以按照以下步骤作为一个替代的解决方案

- 对于 ssh (libssh), ftp (libftp), http (libhttp), chat (libchat), rshell (librshell), repository (librepository), 当它们更新后再从普通商店下载并运行/安装。

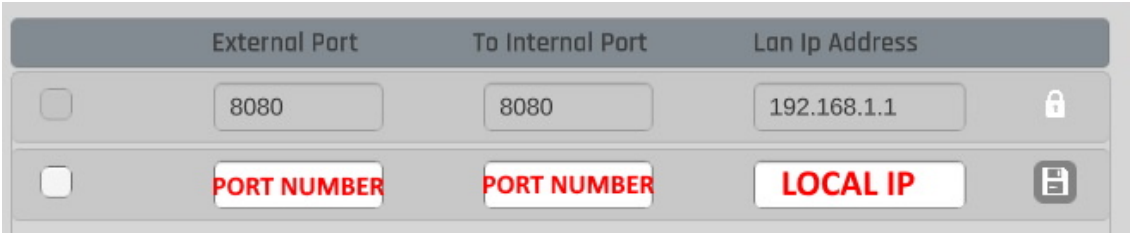
- 对于init.so、kernel_module.so、net.so，在它们更新时从npc服务器下载。
- 对于crypto.so和metasploit.so，当它们更新时，再从黑客商店下载它们。
- 你的网络的kernel_router.so，得到自动更新。
- 你租用的服务器的kernel_router.so不能被更新。

如何升级租赁服务器的硬件

- 登录你租用的服务器。
- 在你租用的服务器上打开Browser.exe，去正规商店购买硬件。
- 在你租用的服务器上打开Settings.exe，更换硬件。

如何搭建特定服务器

- 访问普通商店或黑客商店以找到所需文件。
- 如果你不知道在哪里找到所需的文件，请点击右边的 "设置服务器所需的文件和端口 "并阅读它。
- 找到所需的文件，然后下载它。
- 把它放在你租用的服务器上，并以sudo或root权限在你租用的服务器上运行它
- (你可以使用你自己的电脑，但这是有风险的)
- 使用ifconfig命令，了解什么是网关IP和本地IP。
- 在你租用的服务器上打开浏览器。
- 在地址栏中输入你的网关IP，并添加：8080
- 它应该看起来像这样。



	External Port	To Internal Port	Lan Ip Address	
<input type="checkbox"/>	8080	8080	192.168.1.1	
<input type="checkbox"/>	PORT NUMBER	PORT NUMBER	LOCAL IP	

- 如果你不知道你必须输入什么端口号，请点击右边的 "设置服务器所需的文件和端口 "并阅读它。
- 然后点击 "保存 "按钮，保存你的配置。

设置特定服务器必须的文件和端口

SERVICE NAME	REQUIRED FILE	WHERE TO FIND	PORT NUMBER
FTP	ftp-server	regular shop	21
SSH	ssh-server	regular shop	22
HTTP	http-server	regular shop	80
RSHELL	rshell-server	hack shop	1222
REPOSITORY	repository-server	regular shop	1542
CHAT	chat-server	regular shop	6667

如何使用特定主题

- 打开记事本

- 将主题内容复制并粘贴到记事本中，并将其保存在某处。
 - 打开设置->外观，点击三个点，选择保存的主题文件。
点击应用变化。
-

如何使用自定义壁纸

- 打开设置->外观，将鼠标移到黄色图标上。
 - 它将告诉你在哪里复制你的自定义壁纸和其他细节。
 - 将你的壁纸复制到正确的文件夹后，关闭外观并重新打开它。
 - 点击下拉菜单，选择你的墙纸。
 - 单击 "应用更改"。
-