

超级用户指南(SUPERUSER GUIDE)

0.7.2585a) [原帖](#)

译注: 这个manual有些许过时, 内部过时的命令我会标出来, 但整体还是具有参考意义的

by DrDerpenstein

这个指南不是来解释特定任务的指令的, 而是为了演示如何相互配合使用这些命令. 参见手册和命令的提示来获取更多信息.

在现实中你不可能问一个人"这个服务器我该怎么黑? 因为我这样的时候, 它就会变成这样那样的..." 你必须要了解如何正确地使用指令, 并且仔细解读**非常基础**的手册(Manual)

该指南的下一部分会涉及到具体命令的使用. 为了表述方便, 我们令目标IP为"123.123.123.123", 用户名为"person", 密码为"abcd".

剧透警告

这个游戏的很大一个乐趣就是你盯着屏幕, 抓耳挠腮地尝试解决在真实的渗透测试或黑客行动中会遇到的谜题. 阅读该指南的时候, 你在游戏中会失去很多学习, 挫折, 和获得成就感的机会. 尽量少看攻略

开始

当你开始游戏的时候, 你需要创建如下账号:

- Browser.exe > 搜索 "bank" > 创建一个银行账户
- Browser.exe > 搜索 "mail" > 创建一个邮箱账户
- Browser.exe > 搜索 "shop" > 将所有的工具下载到你的/bin文件夹中

你会收到一封任务邮件. 完成任务后, 你会收到一封带有IP地址的邮件, 在浏览器中输入IP. 这是通往真正的应用商店和任务信息的链接.

如果你在线上模式, 你可以打开"Chat.exe". 即便你不打开这个应用, 别的玩家也可以看到你在线.

通用(部分过时)

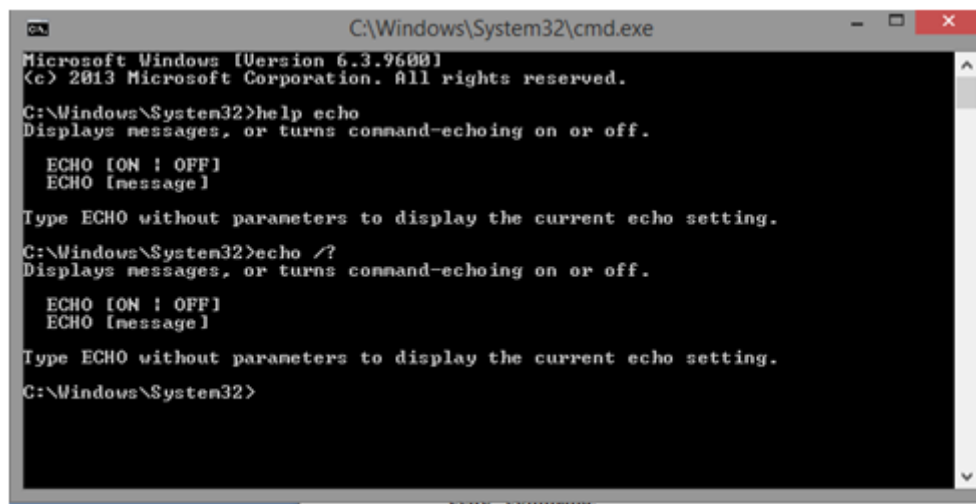
总是在你的电脑上保存一个字典文件"dictionary.txt". 在里面存储你所有遇见过的密码. 每一个密码换一行, 你也应该从别的电脑上获取字典文件. 你可以利用这个来进行暴力破解.

(译注: 在最新版本中不内置字典暴力破解, 但你可以自己写一个字典暴力破解程序)
但其实没有必要, 效率非常低

你可以, 也应该, 打开多个终端窗口, 方便你来运行那些需要你整合很多信息的命令.

除了查看manual.exe的帮助文档来获取命令的更多信息, 你也可以通过在命令后输入help来获取命令的更多信息. 在真实终端中, 你可以这样输入, 比如说这是一个使用echo指令的样例:

- Linux: "man echo"
- DOS: "help echo"
- DOS: "echo /?"



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>help echo
Displays messages, or turns command-echoing on or off.

    ECHO [ON | OFF]
    ECHO [message]

Type ECHO without parameters to display the current echo setting.
C:\Windows\System32>echo /?
Displays messages, or turns command-echoing on or off.

    ECHO [ON | OFF]
    ECHO [message]

Type ECHO without parameters to display the current echo setting.
C:\Windows\System32>
```

译注: 这个在现在版本的GH中已经被弃用, 想要获得一个命令的帮助, 请使用:

[命令] help

或直接输入命令名, 不带参数

其实很多命令在购入的时候都会拥有说明.

厌倦了每次入侵新机器时都要破译root密码吗?

试试Root Spoofing!

译注: 已弃用

保存一个已经被破译的账户的完整root哈希值, 并将其复制粘贴到你当前目标的位置。将这个新的哈希值复制并保存到 "passwd" 文件中, 然后用已知的密码 "sudo -s"。下面是一个例子。

假设这个哈希值被解码为 "hello" root:sa4sda9f8as7fd3asdf21s6d8f41

将整个行从你的电脑复制到受害者的passwd文件中并保存. 它必须是文件中唯一的哈希值 (所以记得覆盖其他的) 。

输入 "sudo -s"

输入你已知的密码: "hello"

被动防御

不要

- 分享你的IP
- 分享你的账户信息
- 分享你的密码

要

- 每个账户使用不同的密码
- 备份你的文件和程序

你可以通过删除你"/home/\$USER/Bank.txt"和"/home/\$USER/Mail.txt"的内容来防止数据泄露, 系统会在你登陆相应账户的时候重新恢复数据, 确保这些文件中不包含你密码的哈希值.

如果你想要加强的安全, 你可以把重要的文件系统文件夹(像是/boot, /sys, /lib, /usr)的权限改掉.

冷知识, usr不是"user"的缩写, 而是"Unix System Resources"的缩写

"chmod [u,g,o]-rwx" 会**移除**相应用户\组\游客的读, 写, 执行权限, 因为用的是减号

"chmod [u,g,o]+x" 会**添加**相应用户\组\游客的执行权限, 因为用的是加号

你可以按照你的意愿来调整权限. 但chmod命令只能在root权限下执行(通过sudo -s或sudo chmod...来使用)

如果你被其他玩家追踪或入侵, 你的所有资料会被全部移除. 但是你可以通过一些小准备来减轻危害. 找一个较为不安全的IP, 黑入并在机器内保存一个隐藏的很深的文件. 把你认为重要的东西都放在那个文件下. 在这种情况下, 如果你被黑了, 唯一的损失就是你需要入侵你的个人存储服务器来找回你的文件

如果你的备用储存服务器也被黑了怎么办? 多交些朋友嘛. 在线上聊天室交一些朋友, 当你发现一个能够协商并且信得过的朋友, 你可以让他们拥有你的个人存储库的IP, 他们就会获取并保管你的文件. 作为交换, 他们可能也会让你保存他们的文件

译注: 在现在的版本不会删档, 你受到伤害的严重程度取决于入侵你的玩家心情的好坏和他们的恶趣味程度.

里面提到的个人备用存储库可以使用, 但交朋友极其不推荐, 现在线上就是黑暗森林

在端口暴露的情况下, 运营服务器风险非常大. 只在你电脑上开放你必须要开放的端口. 理想状态下, 你会把你之前入侵的机器当作你的服务器. 游戏的后期版本可能具有你可以从一个单独的托管公司租用的服务器.

译注: 租赁服务器已经有了

通过更改你链接的wifi, 你可以更改你的IP地址. 在你黑过一堆网站和机器并留下log之后, 你可以换个wifi, 让那些想要被动追踪的人去到一个死掉的IP.

主动防御

行动之前

确认你的 AdminMonitor.exe 在运行

初次接触

运行PS命令, 产生一个正在执行的命令的列表. 在这个列表中, 如果你发现在列表中有名为"dsession"的进程, 代表系统管理员在线.

现在能够减缓管理员追踪速度的方法只有:

- 删除在"/boot"和"/sys"下的所有文件.
- 利用reboot重启目标电脑
- 进行越快越好, 因为你在过程中仍在被追踪

在之后的版本可能能够通过杀掉管理员进程来阻止追踪

译注: 不可用, 会显示"受保护的进程"

入侵中

确保你经过很多跳板机, 参见[跳板连接](#)

行动结束

在你离开目标机器之前, 你必须检查log. 目前来说, 没有在不重复连接到机器的情况下清除断连日志的方法. 所以说, 你**不应该**删掉显示你连接到系统的log - 如果管理员发现一个没有相对应连入条目的断连条目, 他们就会认为有人在搞破坏. 知道这一点之后, 你必须只删掉那些说明你IP"获取shell(shell obtained)" 和那些可能会能够证明你在干坏事的记录. 比如说显示"连接改道(connection rerouted)" 和"文件删除(file

deleted)"的日志条目.

在之后的游戏版本中可能会添加这种情况的解决方案. 可能会以Fork炸弹(fork bomb)的形式出现. 在这种情况下, 你的断连log **应该** 不会留下, 因为在这种情况下你通过fork炸弹断连, 而不是常规方式.

包嗅探/破解wifi(部分过时)

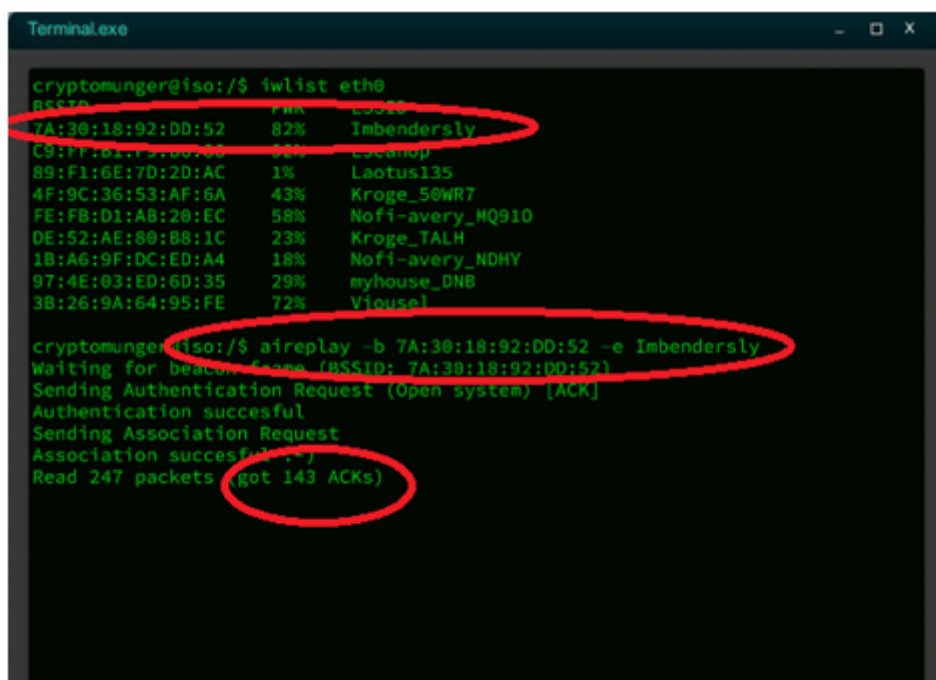
译注: 老版本的方法和新版本有差异, 这里贴新版本的教程, 但教程原图是老版本

终端输入 "iwlist wlan0"

找到信号强度"PWR"最高的WiFi的ESSID和BSSID

输入 "airmon start wlan0".

输入"aireplay -b"并加上你刚才iwlist出来的信息, 如图:



```
cryptomunger@iso:/$ iwlist eth0
BSSID              PWR  ESSID
7A:30:18:92:DD:52   82%  Imbendersly
C8:FF:81:13:00:00   50%  Oceanop
89:F1:6E:7D:2D:AC    1%  Laotus135
4F:9C:36:53:AF:6A   43%  Kroge_50WR7
FE:FB:D1:AB:20:EC   58%  Nofi-avery_MQ910
DE:52:AE:80:88:1C   23%  Kroge_TALH
1B:A6:9F:DC:ED:A4   18%  Nofi-avery_NDHY
97:4E:03:ED:6D:35   29%  myhouse_DNB
3B:26:9A:64:95:FE   72%  Vhouse1

cryptomunger@iso:/$ aireplay -b 7A:30:18:92:DD:52 -e Imbendersly
Waiting for beacon frame (BSSID: 7A:30:18:92:DD:52)
Sending Authentication Request (Open system) [ACK]
Authentication succesful
Sending Association Request
Association succesful (??)
Read 247 packets (got 143 ACKs)
```

在这个命令执行后, 等待生成足够数量的ACK包. 如果信号足够强的话, 至少7000个ACK包就足够了. 对于信号弱的网络, 你可能需要多达20000个ACK包.

按"ctrl + c"

输入"aircrack file.cap"

终端就会返回对应的wifi密码

查找IP和目标

下面是一些你寻找你黑客目标的方法, 排名不分先后

NSLOOKUP

找任何一个游戏内的域名, 方便表示起见, 这里使用"www.shop.com"

终端输入"nslookup www.shop.com"

*注意输入必须带有www和.com

系统日志

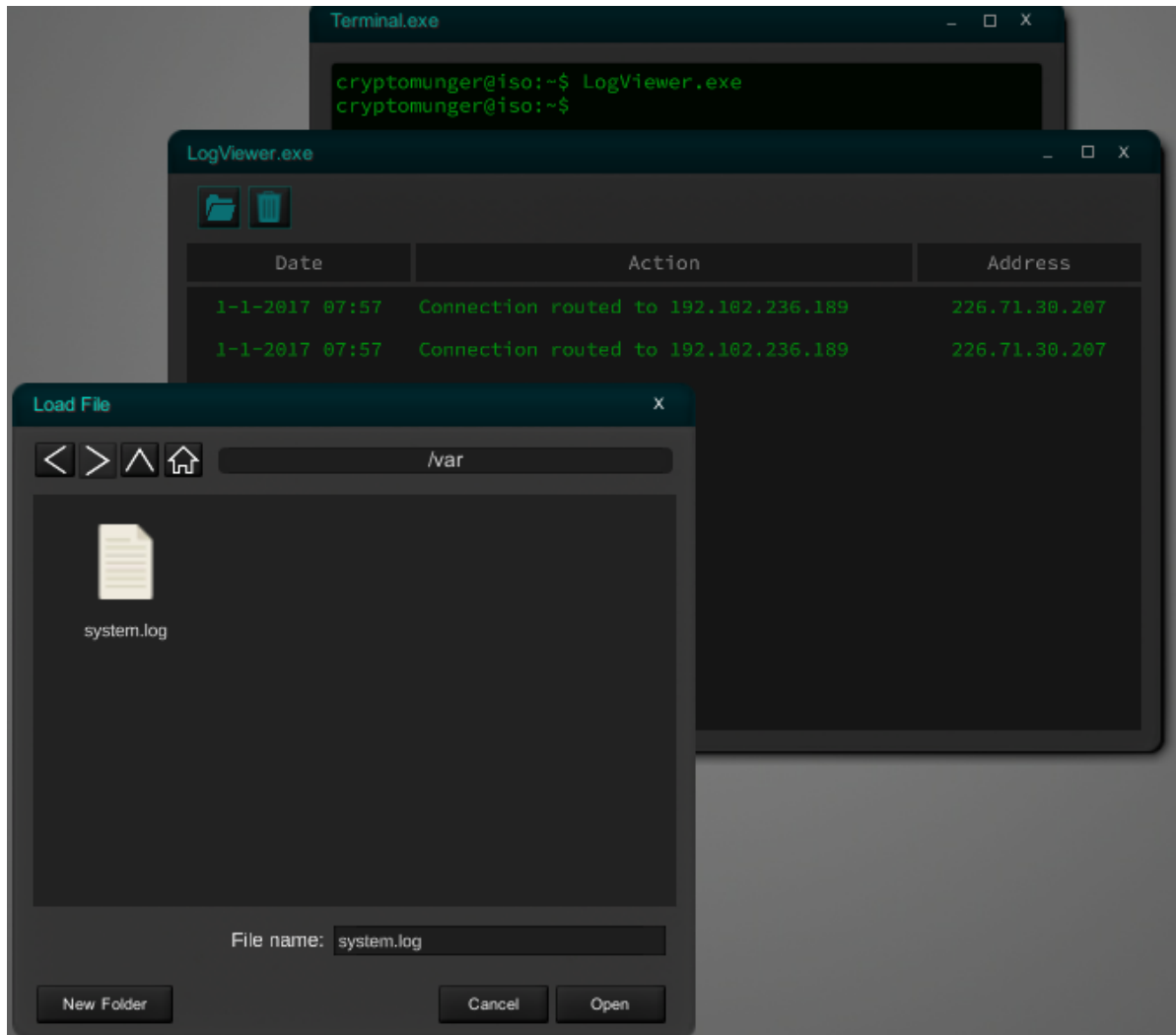
当你成功入侵一个机器之后, 你可以阅读在/var下的系统日志

终端输入LogViewer.exe或者打开system.log

这个会展示所有连接过或连接到过的IP, 包括NPC和玩家的IP

在你黑入其他机器之前, 考虑考虑这件事: **你不能删除你的断连日志,你也会留下日志.曾经成就了你的东西现在毁灭了你**

尝试去黑入那些NPC, 或者那些粗心的, 留下了"获取到shell"日志或者光删掉了连接日志的人



CHAT.exe

读一读多人模式的聊天记录, 全都是等待被黑入的机器

译注: 因为这个游戏玩的人不多, 可能聊天不是那么活跃

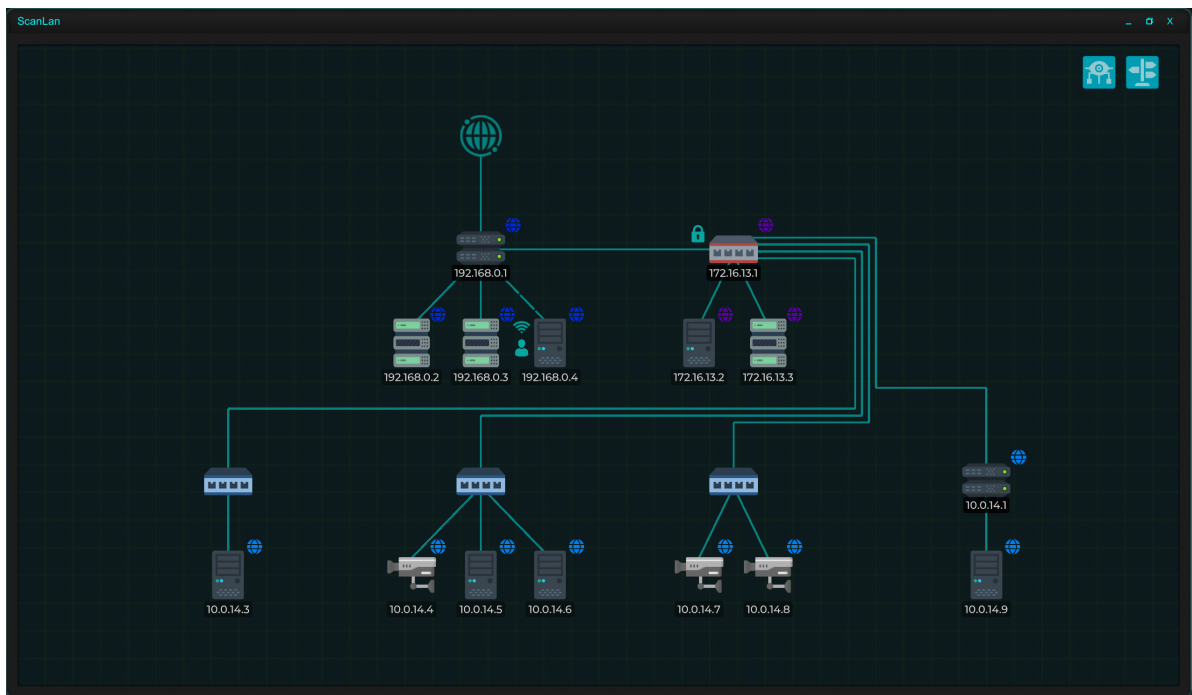
SCANLAN.exe

如果你已经连接到一个机器, 并且认为内网中肯定有其他的设备:

译注: 在老版本中scanlan以命令形式存在, 现在版本以scanlan.exe存在, 请先将scanlan.exe放入你黑入的机器的目录下

输入ScanLan.exe, 你会获得其他本地机器的IP. 对于如何黑入本地IP, 参见[FAQ](#).

译注: 在最新版本中scanlan会直接显示网络结构



任务

参见黑客商店的"job"界面

阅读领取任务之后发给你的邮件

译注: 接下来四个部分原教程所给的解释皆已过时, 故不翻译

FTP(常用端口21)(过时)

SSH(常用端口22)(过时)

SMTP(常用端口25)(过时)

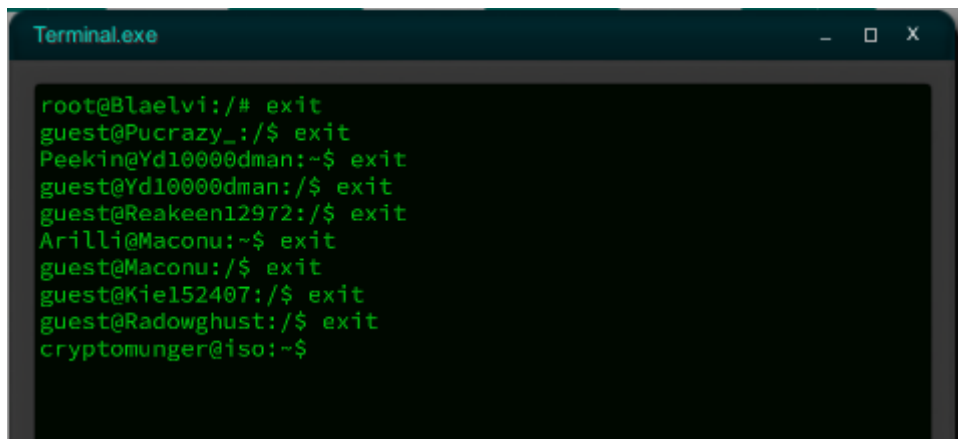
HTTP(常用端口80)(过时)

跳板链接

跳板链接是指你通过多台计算机重新路由你的连接的操作. 这能够很好地隐藏你的真正IP, 因为你入侵时使用的是你最后一个跳板机的IP. 想想看, 如果你在大街上带了很多层面罩...人们在寻找真正在面罩下的人这件事上又能够走多远呢?

想要建立你自己的跳板链接:

1. 黑入任何服务器, 并获取root权限
2. 上传你的入侵工具, 因为大部分的电脑都不会拥有这些工具
3. 从你获得root权限的机器入侵其他机器
4. 重复以上步骤, 直到你认为你拥有足够多次连接



```
Terminal.exe
root@Blaelvi:/# exit
guest@Pucrazy_:/ $ exit
Peekin@Yd10000dman:~$ exit
guest@Yd10000dman:/ $ exit
guest@Reakeen12972:/ $ exit
Arilli@Maconu:~$ exit
guest@Maconu:/ $ exit
guest@Kiel152407:/ $ exit
guest@Radowghust:/ $ exit
cryptomunger@iso:~$
```

*注意你可以通过exit来退出连续的shell界面

你也可以通过手动往Map.exe中添加服务器信息的方式来进行跳板连接

log清理

每一次跳板连接都会创建一个"获取shell"日志条目, 你必须要删除这些log.

并且, 这些你作为跳板的机器都会留下一个"连接重新路由(connection rerouted)"的日志条目.

在你清楚你的踪迹的时候, 你也必须删除这个日志条目. 在断开连接之前检查LogViewer.exe.

当然, 灾难性的后果最终会降临到你的电脑上... 所以说, 在你黑入你的第一个(第一群)跳板机之后, 你必须立马删掉你的"连接重新路由"日志条目, 让可能会追踪你的有关部门的线索断掉

不受支持的端口(过时)

下列端口在当前游戏版本内不可被入侵

译注: 现在皆可通过sql黑入

- 6233 Students
- 3692 Employees
- 141 Bank
- 6344 Dpreports
- 6578 Crimestats

获取密码文件

想要从你的目标电脑上获取密码文件(比如Bank.txt, Mail.txt, passwd), 你可以把这些文件复制到你电脑上

这些文件的默认位置在 `"/home/USER/"` 中, USER代表用户名

终端输入decipher + 包含密码的文件名

你可以通过FileExplorer.exe或mv命令来将文件复制到你的电脑上.

这些文件都是以[用户名:密码哈希值]的形式来排布的, 查看冒号前的值来确定用户名

在现在的版本中, 如果文件包含多个 用户-密码 对, decipher将不会正确解密. 你必须将所有的 用户-密码 对复制到一个空白的Notepad.exe文件中, 并分别decipher原始文件中的每个账户

译注: 在最新版本中, 当有多个 用户-密码 对的时候, decipher会弹出一个选择界面, 所以说可以将所有的 用户-密码 对放在一个文件中

电脑配件

购买电脑配件来升级你的电脑不便宜, 但很简单. 为了最高的性价比, 你需要拥有足够的钱, 并且对你需要什么硬件拥有一个大致的概念(哪种配件对你来说最重要)

为了做出明智的决定, 事先知道所有的电脑配件在电脑上拥有什么角色非常重要:

- 机械硬盘(HDD) - 这个决定你的电脑的储存容量是多少(你能够存下多少文件)
- RAM(内存) - 这个决定你同时能够打开多少个程序, 如果你总是收到"没有足够的内存"的警告, 这就是罪魁祸首.
- CPU - 通俗来讲, 这是电脑的"大脑", 对机器处理任务的速度和同时处理多项不同任务的能力拥有很大影响.
- 电源(PSU) - 要想为你的硬件提供支持, 机器必须拥有足够的电源输入. 电源功率(W)的多少决定了电源能够提供功率和你能够拥有设备效能的上限.
- 主板(mobo) - 这是你电脑硬件的基础, 连接所有其他硬件的硬件. 想要支持各种不同的硬件, 你的主板必须拥有正确的硬件配置和"兼容性"

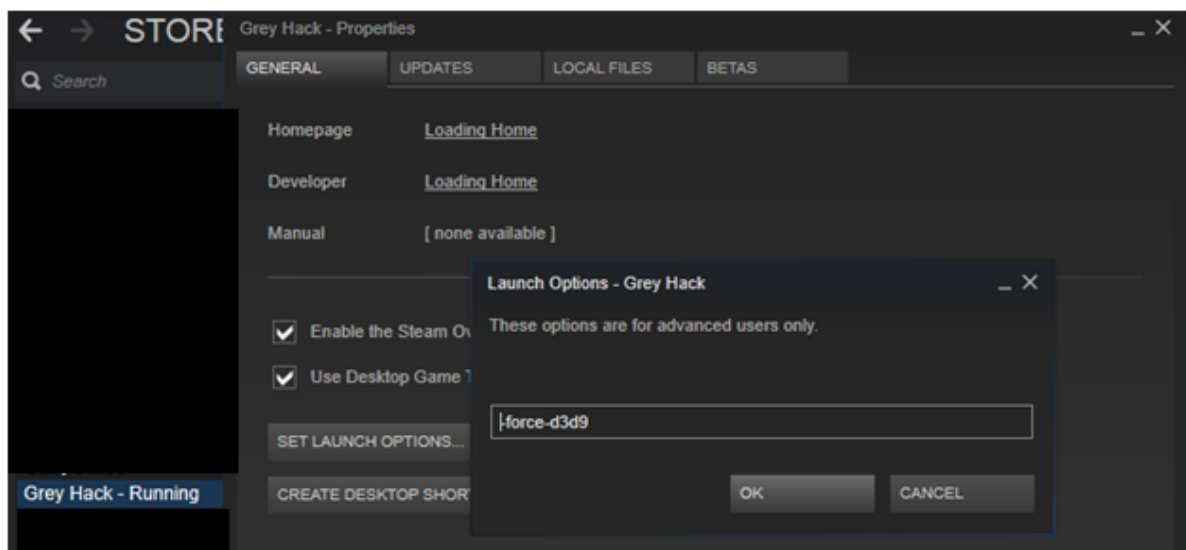
所有的硬件必须拥有正确的配置, 例如:

- LGA的CPU不能安在DGA的主板上
- DDR3内存不会在DDR2主板上工作
- 你不可能在一个只有一个内存插槽的主板上插四条内存

问答

我电脑配置没有问题, 为什么打不开游戏?

可能是DirectX驱动的问题, 在游戏的启动项中添加"-force-d3d9"



我如何迁移我的存档?

前往你的游戏目录文件夹(一般是[你的steam库路径]\common\Grey Hack)

在里面的\Grey Hack_Data文件夹中找到GreyHackDB.db文件夹, 把这个复制到你新电脑的同一目录下.
steam云存储在以后的版本会出现.

当你连接到目标公网IP后如何入侵内网?

1. nmap 123.123.123.123
2. 从黑客商店下载和开放端口相关的工具, 切记要使用相对应服务的破解
3. 参见工具的指引
4. 这个时候你至少应该拥有guest权限了. 在文件系统里转转, 找到可以解密的密码文件. 复制到自己电脑上然后解密
 - 译注: 现在版本你不可能利用游客身份找到可解密的密码文件, 只能使用本地提权命令或sudo -s
5. 当你有了密码之后, sudo -s成为超级管理员

现在你是超级管理员了

6. 拥有root权限的你现在可以向文件系统中上传你的入侵工具了. 将它们上传.
7. nmap对应的本地IP
 - 译注: 建议在nmap之前先使用ScanLan.exe扫描本地网络再进行入侵
8. 在你上一步获取到的终端中入侵本地IP
 - 译注: 可能会遇到其他的阻碍, 像是对方在交换机之后或者防火墙之类的, 需要更多步骤
9. 通过以上的步骤, 你现在应该连接到了目标IP, 做你该做的事情

SUDO是什么?

"以超级管理员身份运行(Super User DO)"- 它让你能够在不受系统保护影响的情况下进行操作. sudo + 命令代表以root身份执行该命令, sudo -s代表进入root身份

IP没有开放端口, 怎么办?

你当前最好的选择是去看一下你所拥有的关于这个IP的资料. 这个在SMTP或社工入侵无效的时候可能会给你更多的机会. 在现在的版本中肯定有那种黑不进去的服务器, 可能你就是不太走运.

- 你需要下载更多的黑客工具吗?
- 你考虑过你所有的提权工具了吗?
- 如果你不能黑入机器, 尝试过社工了吗?
- 你的任务真的需要你入侵系统吗? 有没有在不黑入系统的前提下完成任务的方式?

译注: 现在几乎所有的没有开放端口的机器都可以通过路由器黑入, 如果内网中依旧没有端口开放, 尝试反向shell

我的电脑现在在运行服务, 并拥有开放端口, 我怎么关闭它?

译注: 该部分已过时

利用拥有管理员权限的Browser.exe连入你的网关地址(通过ScanLan.exe获得), 就会打开一个端口设置界面, 可以调整端口

我黑入了一个IP, 但命令都用不了?

有下列三个可能原因:

1. 你的连接是ftp连接, 所以说只能使用ftp给你的指令, 直到你能够通过其他方法获得shell
2. 另外一个玩家已经蹂躏过这个服务器了, 他可能删掉了/bin和/usr文件夹. 这个服务器大抵是寄了... 这就是黑客工作.
3. 你遇见bug了

我不小心删掉了我的"建立连接"log, 怎么办?

1. 赶快连接回服务器
2. 删掉你的断连, 获取shell和连接重新路由的log
3. 断开连接

我如何入侵其他玩家的机器/我如何知道我入侵了其他玩家的机器?

入侵玩家机器的方法和入侵其他机器几乎一样, 重点和难点是找到他们的IP.

当你入侵了一个玩家的机器, 你会注意到很多NPC机器不会拥有的特征:

- 他们在/bin或/usr/bin中会有入侵用的文件
- 那些一般来说有密码的文件都被修改过了
- 他们留下了一个readme.txt文件等着你去寻找
- 他们拥有一个超级大的字典文件

译注: 现在基本不会

- 他们更改了很多文件夹的权限
- 他们拥有一个看起来就不像NPC的bank.txt

译注: 现在也不会

我如何知道我购买过的工具的版本, 我忘了?

在下载入侵工具之后给它命个名, 记录工具版本

CTRL + C和 CTRL + V 在终端里用不了?

这就是正常终端的用法. 这些组合键其实是在向linux终端发送指令, 而不是用来复制粘贴. 比如说, CTRL + C会终止当前正在执行的命令. 使用右键菜单来复制粘贴, 或者使用ctrl + shift + c

我觉得我找到了个bug, 如何反馈?

1. 首先在chat.exe中间问一问其他人是否遇见了相同的bug
2. 如果别人也有相同的bug, 将触发条件和bug具体信息尽可能清晰并详细地描述. 最好带上截屏
3. 将以上信息提供给游戏的独立开发者 "KuRouZu".

译注: 或在discord上讨论

为什么我在玩多人的时候总是断开连接?

当官方要重启服务器的时候, 一般会有提前的警告.

现在的游戏版本感觉并没有延迟补偿机制 - 如果你现实世界中的网络连接断开了, 你就会从服务器中断开

这个游戏到底有多真实?

这个游戏中的命令, 战术, 用户界面和其他东西都是基于真实世界中的渗透测试的. 显然, 由于这只是个游戏, 为了简洁和易用性, 大部分地方还是没有还原的. 即便你感觉游戏很好玩, 也别以为你能够在现实世界中当个黑客.

我从哪里能够得到游戏中的工具?

找那些ALI领域或者信息科技领域的大牛去要吧.

译注: 非法侵入计算机信息系统罪, 是指违反国家规定, 侵入国家事务, 国防建设, 尖端科学技术领域的计算机信息系统的行为

词汇列表

黑帽子

代词/形容词

一个出于利己主义或者伤害他人的目的而进行黑客行为的黑客或者用户. 他们一般来说会破坏系统或蒙骗他人.

扩展阅读: [白帽子](#), [灰帽子](#)

CLI

名词

"命令行界面(Command Line Interface)"的缩写.

基于文字的交互界面, 像是微软的DOS/powershell或者Linux Shell(Bash, zsh, 等等)

扩展阅读: [GUI](#)

灰帽子

也被叫做 "灰色黑客(Grey hack)"

代词/形容词

一个一般来说没有恶意, 但并不总是按照规矩行事的黑客, 用户, 或者这样的行为.

扩展阅读: [黑帽子](#), [白帽子](#)

GUI

"图形化用户界面(Graphical User Interface)" 的简写

基于图形化的交互界面. 像是Windows, Mac Os, 和Linux的一些分支

扩展阅读: [CLI](#)

[颜色]帽子

形容词

白帽子, 灰帽子, 黑帽子(暂且不提红帽子)等是描述黑客或者用户的词语. 这个词语源于古老的黑白西部片. 由于是黑白图像, 好人和坏人的身份只能通过通过他们帽子的颜色来区分.

译注: 红帽子一说指专门针对linux系统的黑客. 一说指那些私法制裁者类型的, 在发现黑帽子黑客以后, 代替有关部门执行正义的黑客

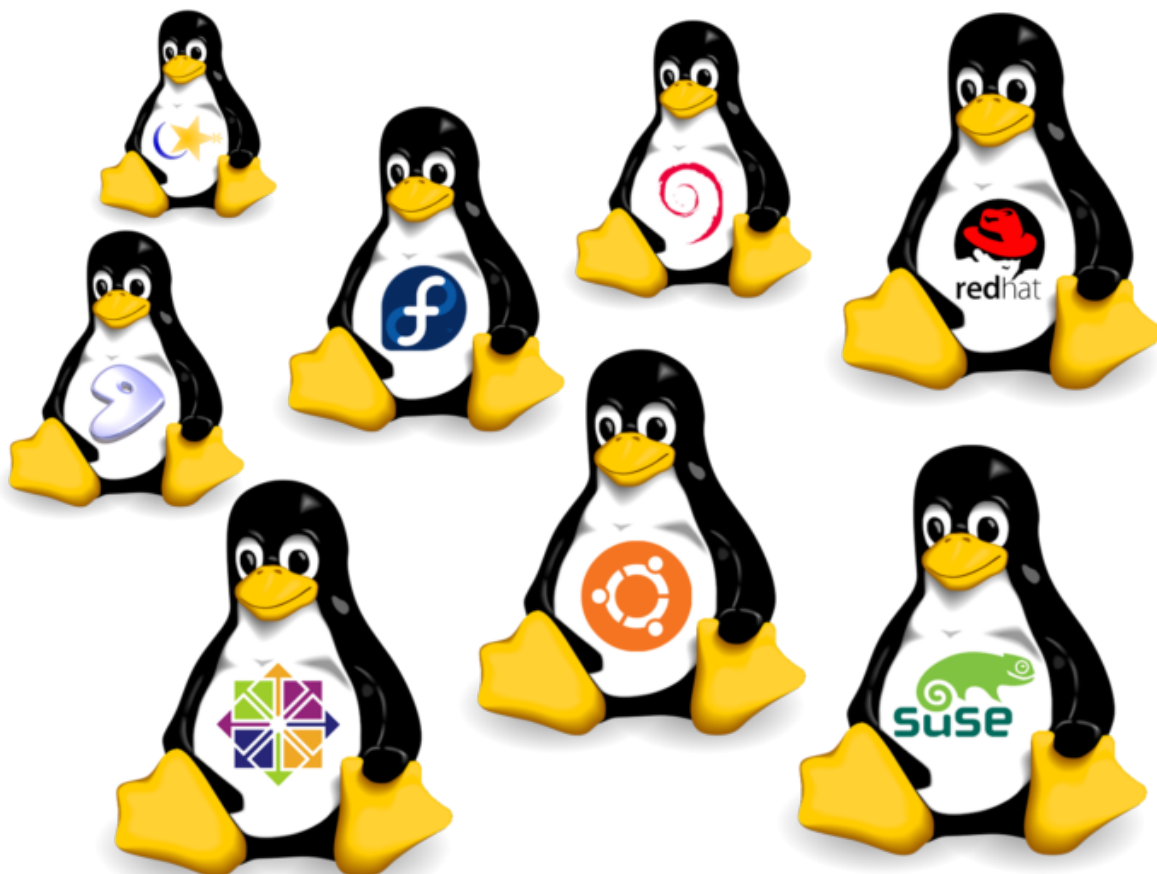


Linux

名词

一个将你从巨硬那些狗屁(bullshit)玩意儿中拯救出来的操作系统. 学着去用它, 爱上它, 做一个自由(free)的人.

译注: 原文就是这么写的



Repo

名词

存储库(repository)的缩写

这是用户在Linux中安装/管理程序的方法. 就这个游戏而言, 它是一个缓存或转储的, 为了共享的自由文件.

Root

名词

基于Linux的系统的管理员账号的名称

RTFM

名词

源于Arch Linux社区, 更多信息详见:

[RTFM](#)

shell

也叫Bash

名词

1. 大多数时候指终端和终端命令
2. 通过远程, 并且大多数时候是以非法方式, 获得别人电脑的root权限

译注: 对于第一条, 并非所有shell都叫bash(字面意思)

skid

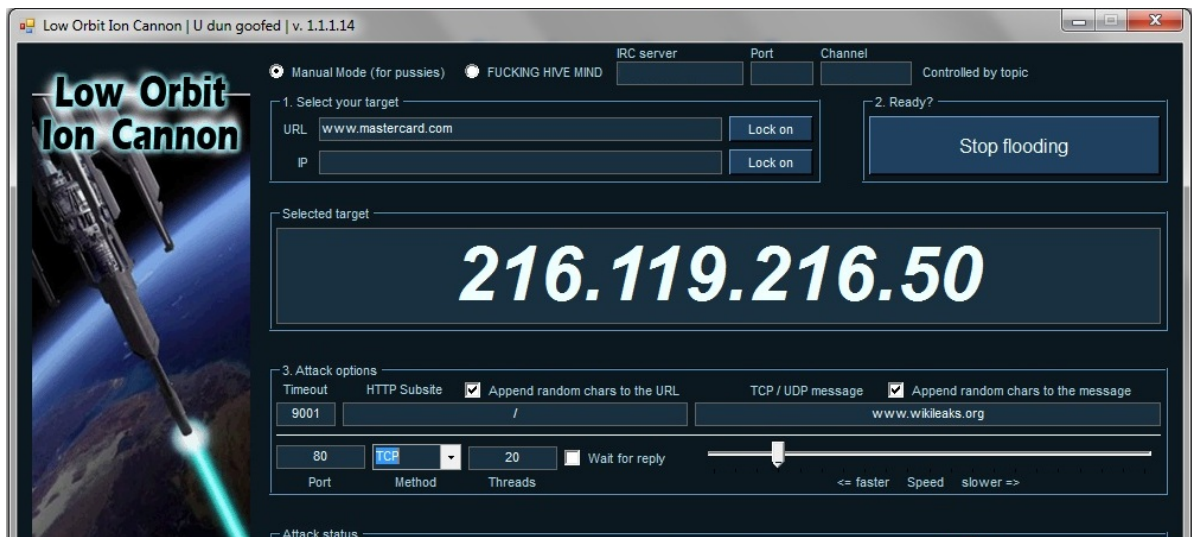
代词(贬义):

脚本小子(script kiddie)的缩写

一个能够通过(大多数时候带GUI)脚本来执行黑客行动, 但离开脚本完全不知道如何达成相同效果的人.

形容词:

一个简单易用的脚本



译注: 图片中的是LOIC, 一个有GUI的DoS软件

白帽子

代词/形容词

一个坚守内心正义的黑客. 正义一般包含举报违法行为和报告安全漏洞

扩展阅读: [黑帽子](#), [灰帽子](#)

后记

我游戏内的ID是 "cryptomunger", 欢迎来问问题!

将会在之后的教程中添加的部分

通过192.168.0.1设置端口转发

作为游戏机制添加的脚本系统

服务器托管(SSH/FTP/HTTP)

- 劫持域名
- 托管可执行程序
- 租用域名

可能会加入的游戏机制

- 相信在某个版本, 玩家可以通过租用的服务器来运行自己的应用商店
- 在某个版本, 玩家可以自己写shell脚本
- 在接下来的版本中, 游戏会拥有更多的应用和终端命令

译注: 基本上都已经加入了

通过[链接](#)加入discord!

感谢 KuRouZu 开发这么一个令人沉迷的, 精妙的和有教育意义的游戏!