
Hacking in the Old-School way
_c757 | Www.HackShell.Net

本次分享的形成

由某次活动影响，想写个Hacking on Linux的简介

开始考虑有几个原因使用Linux以及为何如此地使用Linux

由此PPT从开始的技术简介，演变到有价值观输出

至此PPT就和技术以及Linux无关了

关于价值观

个人选择的价值观，意味着和你的不同意见之间的问题可能会有好坏之分，但不是正确与否；
这里阐述它不代表其具备指导意义，只是在表明世界上存在一个如此的想法或观点。

Outline

- Hacking是啥
- Why the old-school way

之前把题目定为old-school way主要想讨论以下几方面：CLI & scriptized/ Security tools under linux / Secure exchange and communication network / Home-made weapon
现ppt和the old-school way已经没多少联系，保持标题未改，仅为了标注分享形成的原因

Part I:
Hacking 是啥

数据驱动的攻击：

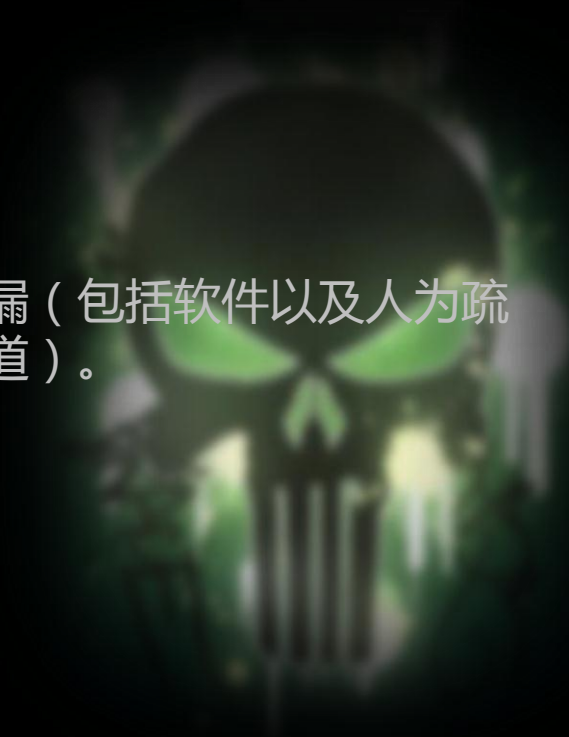
攻击某个程序的一个前提是需要有与该程序进行数据交互的渠道：

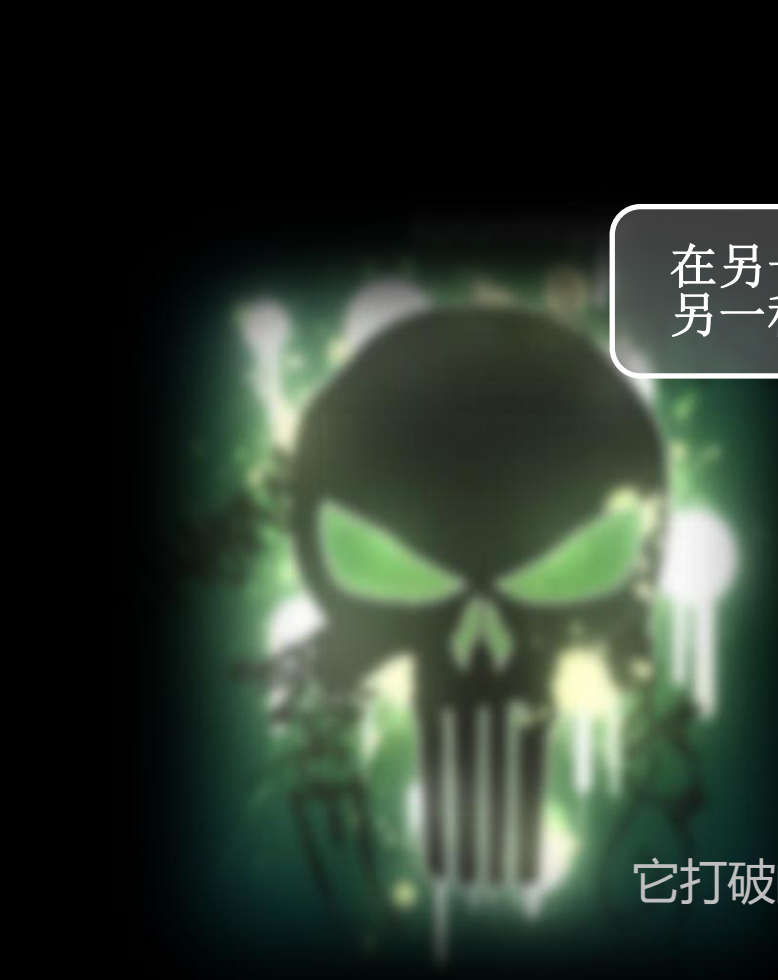
- 可以与目标进行各种本地进程间的通信；
- 可以与目标程序进行网络间进程通信（以**tcp/ip**、以太网为例）：
  1. 目标在监听一个本地可达的端口 （攻击服务器软件）；
  2. 目标会主动发起对本地的链接请求 （攻击浏览器）；
  3. 可路由到对方所在冲突域，而目标对应的网卡处在混杂模式（攻击**IDS**、流量审计软件）。

程序的疏漏：

- 程序逻辑可被滥用（可上传任意类型文件、微软**wmf**远程代码执行），可能影响程序逻辑的途径：
  - 程序代码（开发人员），
  - 程序配置（运维人员）；
- 对可能的动态数据考虑不周，导致执行逻辑可被控制（各种代码注入，堆栈溢出，格式化字符串）；

渗透的过程：
利用已有的数据交互渠道，找到交互秩序中的疏漏（包括软件以及人为疏漏），进而去获得其他的数据交互权限（交互渠道）。





在另一种秩序下发生的
另一种漏洞。

漏洞概要

缺陷编号： WooYun-2012-04157
漏洞标题： 深圳地铁 带票出站漏洞
相关厂商： 深圳地铁
漏洞作者： 网络骑士
提交时间： 2012-02-02 17:20
公开时间： 2012-02-02 17:20
漏洞类型： 设计不当
危害等级： 中
自评Rank： 10
漏洞状态： 未联系到厂商或者厂商积极忽略

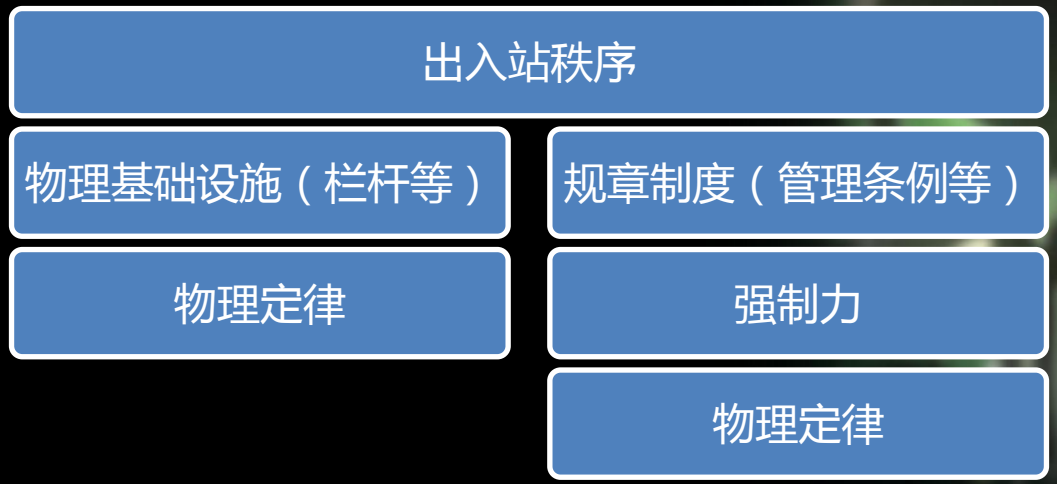
漏洞证明：

从东门站买到深大站的票，
进站，
坐到深大站不下车，到桃园站下。
到出口闸机，将票投入闸机并取回来3次，

它打破的是一个由一些外在强制力维持的、看似一成不变
总是按照预期方式运作的秩序。

秩序

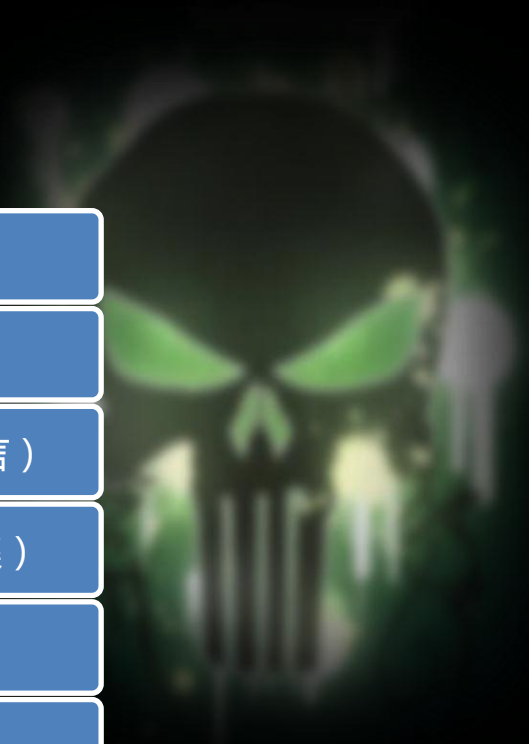
地铁出入站秩序的 维护栈：



秩序

计算机秩序的 维护栈：

- 计算机秩序
- 程序员的意愿/逻辑
- 与编译器/解释器的协定（编程语言）
- 与CPU制造者的协定（CPU指令集）
- CPU制造工艺（物理级别）
- 物理定律



秩序

社会秩序的 维护栈：

WYBH是“我也不会”的简写。

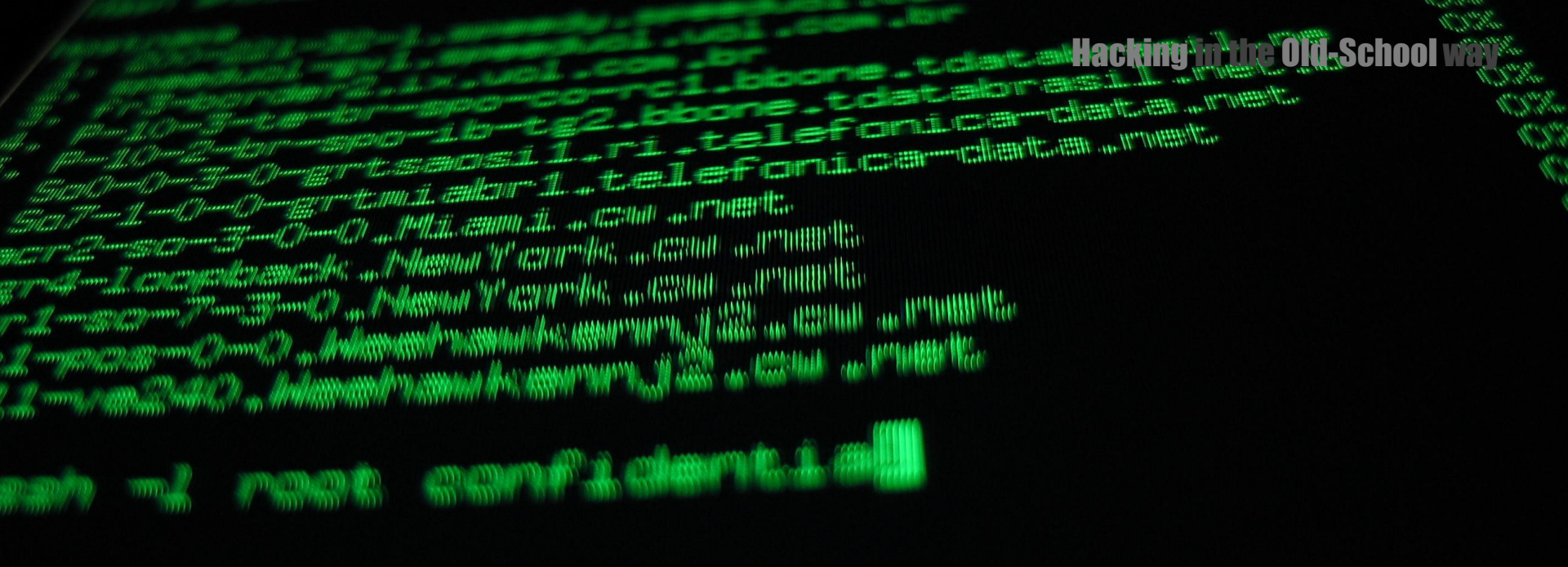
Hacking是啥

Hacking是一种思考方式：
不基于（信任）任何既得结论，从 根本 出发考虑问题，
以批判的角度审视秩序的思考方式。

以期找到颠覆现有秩序的方法。

从最根本的角度去尝试理解问题的行为也有助于引导自己去了解事物本质

Hack the planet 不是特指物联网络的突破，也不是入侵城市基础设施。
而是指以Hacking的批判性思维看待生活中包括计算机和计算机之外的一切事物。
它们不一定就是按照“看上去”、“显而易见的方式”去发生。
Hacking是一种思考方式，甚至于一种生活方式。



Part II:

<Programming from the Ground Up> by Jonathan Bartlett, Chapter 1, page 1:

I enjoy the challenge to not only make a working program, but to do so **WITH STYLE**. Programming is like poetry.

HACKER

我们做的原因，决定着我们做的方式。
Why we Hack

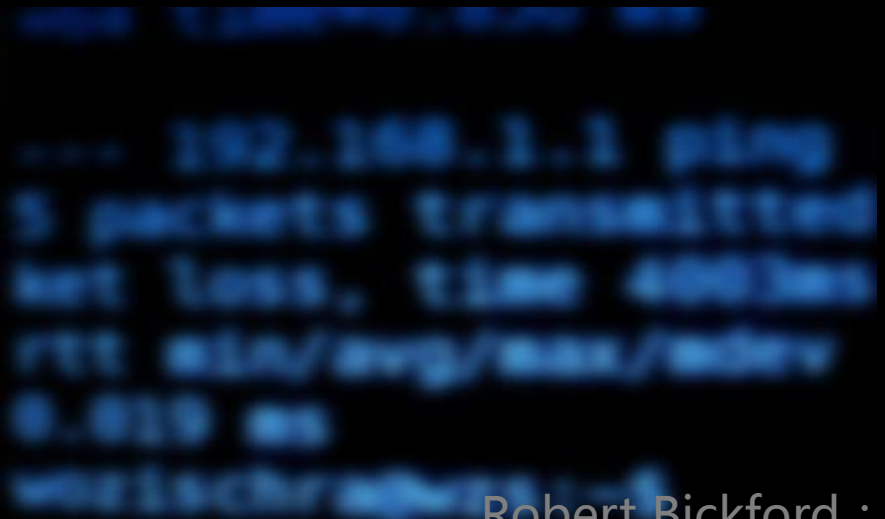
- 杀人
- 杀人者的行为艺术

二级谋杀/激情杀人 与 《电锯惊魂》式杀人

He enjoy the challenge to not only make a man dead, but to do so **WITH STYLE**.
Killing is like poetry.

他在制造自己想要享受的：
- 艺术家：制造/表现美
- 欣赏者：发现/享受美

诗歌的美不仅仅在于它尝试表达的内容，
更多的在于它的表达方式/风格。
他的目标不仅仅是结果，他的每一个动作和设计，是构成整首诗的每一句话。他要的不仅仅是谋杀，他在表达他的观点，以一种华丽的方式。



为啥Hacking
怎么样去Hacking

Robert Bickford：
A hacker is “any person who derives joy from discovering ways to circumvent limitations”

```
=64 time=0.850 ms

--- 192.168.1.1 ping
5 packets transmitted
ket loss, time 4003ms
rtt min/avg/max/mdev
0.019 ms
wozischra@wzs:~$
```

为啥Hacking
怎么样去Hacking

- 结果很可能是失败的，但是经历一定是一次奇妙的探险。
- 在其间我们享受着我们的行为，享受着过程带来的快乐。

Not only for the goal, for the Experience, for the Art.
结果固然需要在意，
但更重要的是 我们在做，以及我们做的方式。

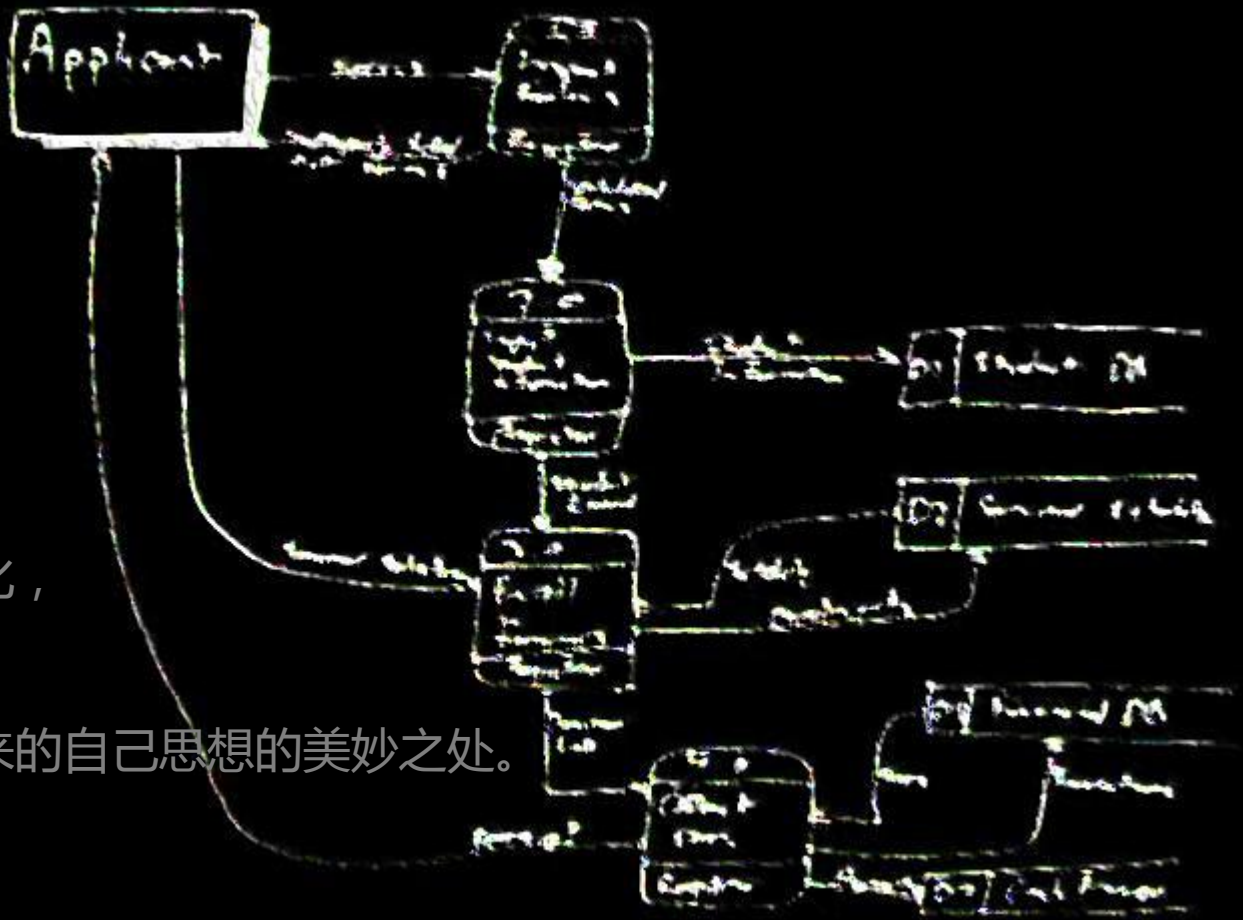
过程

Hacking中：

- 实施框架/步骤
- 问题分析
- 背景音乐的选取

过程是对思想的实例化，
是价值观输出的产物；

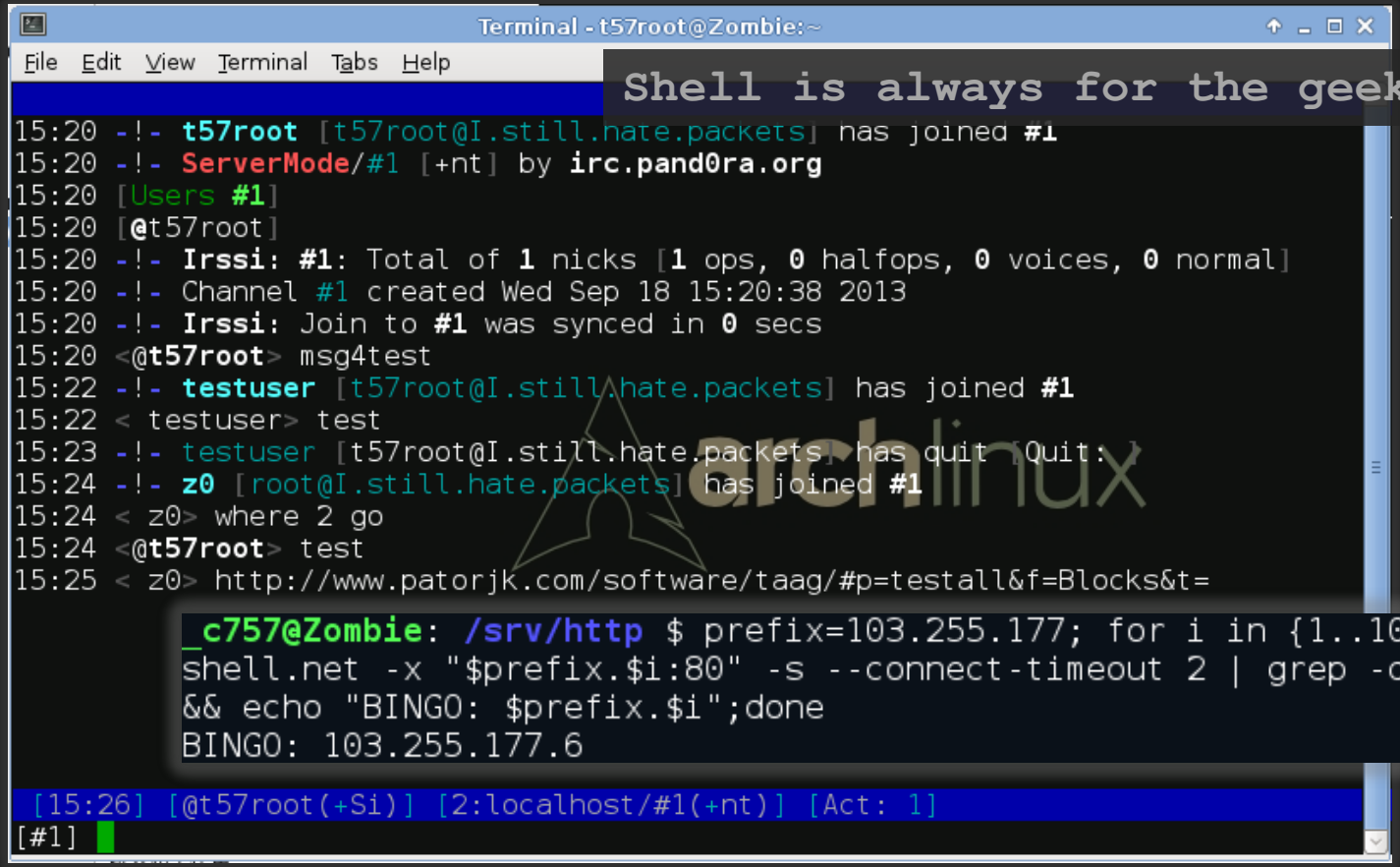
体验过程中所展现出来的自己思想的美妙之处。



虽然可能无助于命令执行的成功率，
但是同样可以尝试调整你的终端配色，向历史致敬，
享受手指在命令行上跳舞时透出的神秘。

"But we are hackers and hackers have black terminals with green font colors!"

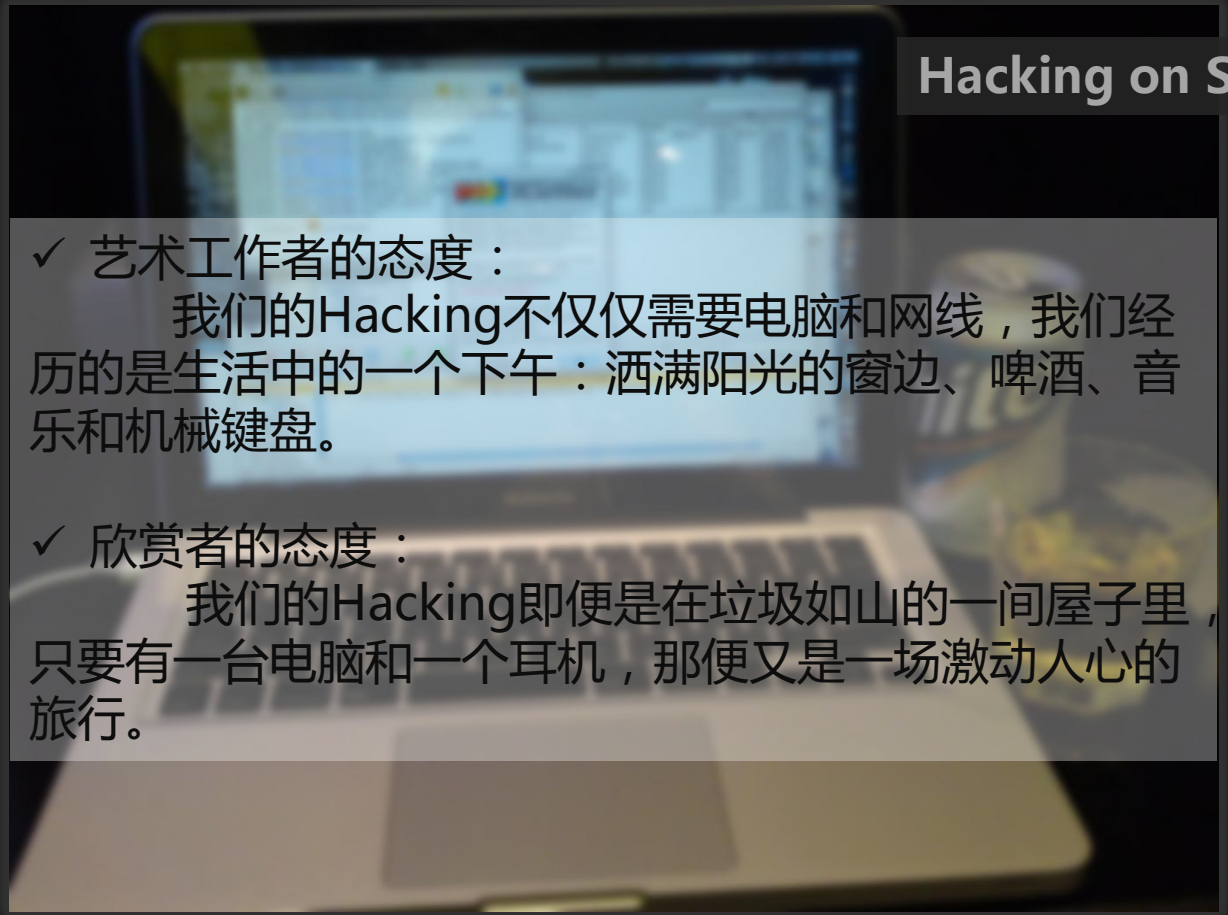
- John Nunemaker



Part II: Do it with YOUR STYLE.

Hacking on Sunday afternoon

Part II: Do it with YOUR STYLE.



Hacking on Sunday afternoon

✓ 艺术工作者的态度：

我们的Hacking不仅仅需要电脑和网线，我们经历的是生活中的一个下午：洒满阳光的窗边、啤酒、音乐和机械键盘。

✓ 欣赏者的态度：

我们的Hacking即便是在垃圾如山的一间屋子里，只要有一台电脑和一个耳机，那便又是一场激动人心的旅行。

既然结果我们左右不了，那么就让我们忠于过程吧

过程是对思想的展现；
享受过程意味着“享受现在”；

结果可能是令人喜悦的，
而令人感到美好的只能是过程。

- 看过那个画
- 看画

- 听过那个歌
- 听歌

- 曾经活过
- 活着

- 我有一段美好的回忆
- 我在回忆我的回忆

每个人都是艺术工作者，工程师也是。

http://www.hackshell.net/blog/index.php/archives/562/

每一次过程都是在对自己心中的“酷”和“理想状态”的造就与展现。按照心中所想去构建并实践整个过程。
即便没人在看，我们也应懂得享受我们想享受的，体验这件事本身的过程。
做其他事也应这样，赋予生活更多的意义。
生活不缺少美好，而是缺少制造美好和享受美好的意识。美是一种意义。

就像做这个PPT一样，形式无伤大雅，但是我喜欢以我认为“美”的方式去展现它（效果另说）。

每个人都是艺术工作者，只要你在表达自己对美的理解和感受。

Life is like poetry. Living with style!
生活是一首诗。

一句话实际用处的大小在于它文学价值之外的价值。
这句话不仅仅是书本上一句看上去很华丽的形容句*。
它在表述一个含义。

这句话不是为了两个词堆砌在一起看上去很炫而写出来的（我认为现在很多文字的意义就止于此）

Life is like poetry. Living with style!
生活是一首诗。

怎样去做任何一件事/生活：

按照自己的想法，
实践、展现思想，去制造美，并感受美，
以赋予生活更多意义，以更华丽的方式。

Hack your life to live your own style.

Hacking in the Old-School way

Hacking是啥

Hacking是一种思考方式：
不基于（信任）任何既得结论，从根本出发考虑问题。
以批判的角度审视秩序的思考方式。

以期找到颠覆现有秩序的方法。

从最根本的角度去尝试理解问

Part I: Hacking是啥

Hacking in the Old-School way

Life is like poetry. Living with style!
生活是一首诗。

怎样去做任何一件事/生活：

按照自己的想法，
实践、展现思想，去制造美，并感受美，
以赋予生活更多意义，以更华丽的方式。

Part II: Do it with YOUR STYLE.

_c757 | Www.HackShell.Net


Go Hacking,
in your own way.
Enjoy Your Thinking, Enjoy Your Art.
_c757 | Www.HackShell.Net

The play is being continued, so just keep making yourself amazed.
Go ahead, make your day!

Enjoy Your Art

me@ningful.me