



## 课程导论（补充）

---



# Outline - I

---

- 问卷情况反馈
- 作业与评分



# 问卷情况反馈

知会一些关键数据：

- windows 仍然是主流！
- 大家都学过 C 了！
- 大家许多还是会 python 的！
- 有 35% 左右是没接触过汇编的
- 有小部分高年级同学
- 70% 左右已有逆向基础、70% 左右已有密码学基础、50% 左右已有 pwn 基础、20% 左右已有 web 基础
- hacker dream
- 担心跟不上



这该死的群友  
CTF 基础竟  
如此扎实



# 作业与评分

- 基础培训 (60%)
  - 第一周 六次课的实验分别占 10%
  - 实验手册会标注考点与关键思路
- 专题拔高 (40%)
  - 第二周分选的两个专题各占 20% (如果超出2个不溢出满分)
  - 专题部分细分会根据作业量届时给出
  - 真题演练

*Relax*, 无论是实验还是真题，都会分【基础】和【挑战】两部分，完成【基础】即可拿满分，可以根据兴趣和时间完成【挑战】部分



# Outline - II

---

- CTF比赛简介
- AAA战队介绍



---

Security CTFs, or Capture-The-Flag competitions have nothing to do with paintball or shooter games, but they are awesome to learn hacking.

by liveoverflow



let's watch two videos

---





---

# What is CTF? An introduction to security Capture The Flag competitions



# 真正的 CTFER 和虚假的 CTFER





# 所以，this is CTF

---

- 真实漏洞利用场景的复现：

构建 real world 环境，分析在野攻击威胁

- **Game of Hackers**

Hacker 们锻炼技术、分享技巧和工具的游戏

- 高自闭性竞技项目

Jeopardy Style + AWD Style

做得出就是做得出，做不出就是做不出



# CTF奥林匹克: DEFCON CTF





# 国际上鼎鼎有名的CTFs

## DEF CON CTF



### Official URL

Total events: 12

Avg weight: 82.60

Vegas finals.

Binjitsu by ddtek (... – 2012)

Legitimate Business Syndicate (2013 – 2017)

## OCTF



### Official URL

Total events: 14

Avg weight: 72.79

Open for everyone. Hope all of you can enjoy it:)

## PlaidCTF



### Official URL

Total events: 12

Avg weight: 89.17

Plaid CTF :: Hosted by Plaid Parliament of Pwning

## Codegate CTF Finals



### Official URL

Total events: 9

Avg weight: 59.17

## Google Capture The Flag



### Official URL

Total events: 10

Avg weight: 63.64

Annual Capture The Flag hosted by the Google Security Team.

形式多数是

- 战队自己的 CTF
- 会议等活动过程的伴随 CTF
- 一些企业主办的 CTF



# 国内著名的CTF比赛



## 强网杯：

在中央网信办、河南省人民政府指导下，由信息工程大学、河南省委网信办、郑州市人民政府联合主办

## XCTF联赛：

多企业（华为、陌陌、天融信）联合赞助，多战队参与配合

## TCTF：

由腾讯安全发起、腾讯安全学院、腾讯安全联合实验室主办，腾讯安全科恩实验室承办，0ops安全团队协办的腾讯信息安全争霸赛

还有XNUCA、国赛CTF、字节CTF、百度CTF、各个队伍举办的自己的CTF等等等



# 一些 CTF 队伍介绍

---

<https://ctftime.org/stats/>

<https://www.xctf.org.cn/ctfs/xctf/>



# 经典 CTF 赛题方向

- MISC: 兼容并包、广泛收罗、脑洞绞尽
- CRYPTO: 优雅，实在太优雅了
- REVERSE: 安全问题之基
- PWN: 我常称研究二进制的人为气宗，因其根基是在逆向工程上的熟练程度和对漏洞利用思想的领悟，在掌握这两门法宝之后，任何二进制类的问题都有一定办法可以搞定 —— 岳不群
- WEB: 我常称 Web 类问题为剑宗，因为 Web 类问题非常繁多，恰如一招一式无穷无尽的剑法，有很多很多的小技巧 —— 风清扬
- others



# everything you want can be CTF challenge

---

看个题板

[https://adworld.xctf.org.cn/match/contest\\_challenge?event=186&hash=ba9b2b4c-7265-45ce-aa4b-c917bc5ce1bc.event](https://adworld.xctf.org.cn/match/contest_challenge?event=186&hash=ba9b2b4c-7265-45ce-aa4b-c917bc5ce1bc.event)

P.S.

做 ACM 的人打 CTF 就是砍瓜切菜



# 为什么要打 CTF 呢

---



# 你需要经验





此外

---

1. 竞赛保研有加分

大学生信息安全竞赛 —— 创新实践赛、创新作品赛

<http://www.ciscn.cn/home>

2. 可以锤炼实战技术

课堂的内容可能太书面太枯燥，通过实战不仅可以实践知识，还能加深理解

3. 可以认识最前沿的安全关注

漏洞挖掘领域，工业圈要领先于学术圈



# AAA战队介绍

重要的事情说三遍

我们不是社团，  
不是社团，  
不是社团

AAA 战队是由浙江大学信息安全爱好者自发组织，浙江大学计算机学院支持建立的团队（民间组织），队伍中每一位成员都对信息安全有无与伦比的热爱，因此对 CTF 比赛总是充满了激情。



# 天青刺客联盟的历史(1)

而这支战队，一开始也只是个“草台班子”，甚至连固定队名都没有。2012年杭州电子科技大学组织了一次校园CTF比赛，何淇丹通过初赛，结果复赛要求以战队形式参加，他就在浙大校园论坛上发文求组队。“我们几个人就这么认识了，建了个群互相交流。”他说，“后来认识了蓝莲花战队（国际知名战队，源自清华大学的网络安全技术竞赛和研究团队。记者注）的杨坤，建议我们可以一起去参加一些国际级比赛，必须得起个正式队名了，AAA是那时候定下来的。”

“我们这一批人聚得太晚了。”何淇丹觉得遗憾，当浙大AAA与清华蓝莲花组成刘耕铭口中的“陆上最强联队”征战DEFCON黑客大会并成为首支成功闯入总决赛的华人战队的时候，已经是2013年，团队中的一半人即将面临毕业。



.....



# 天青刺客联盟的历史 (2)

在第二期，AAA的重担交到了刘耕铭肩上，一度，整个AAA战队只有刘耕铭一个人。“那时候我大二，接触信息安全的时间也不长，也没打过几场比赛，但战队的元老们都毕业了，忙着工作、创业，不可能经常参加比赛。那段时间在国内的CTF比赛上，浙大AAA战队几乎再没有打进过前二十，可以用“惨烈”来形容，比赛往往“惨”到小白老师得亲自上阵做题。



**Gengming Liu**

@dmxcsnsbh

Security Researcher at [@SingularSecLab](#)  
Pwnium.

[dmxcsnsbh.github.io](https://github.com/dmxcsnsbh) Joined Nov 2018



# 天青刺客联盟的历史 (2)

在第二期，AAA的重担交到了刘耕铭肩上，一度，整个AAA战队只有刘耕铭一个人。“那时候我大二，接触信息安全的时间也不长，也没打过几场比赛，但战队的元老们都毕业了，忙着工作、创业，不可能经常参加比赛。那段时间在国内的CTF比赛上，浙大AAA战队几乎再没有打进过前二十，可以用“惨烈”来形容，比赛往往“惨”到小白老师得亲自上阵做题。



**Gengming Liu**

@dmxcsnsbh

Security Researcher at [@SingularSecLab](#)  
Pwnium.

[dmxcsnsbh.github.io](https://github.com/dmxcsnsbh) Joined Nov 2018



# 天青刺客联盟的历史 (3)

当跌倒谷底之时，任何成长都是进步。得益于白老师在宣传上的努力，战队从单人队伍成长为近**20**人的强队

- 2016年3月，**XCTF**国际联赛郑州站浙大AAA战队逆转夺冠
- 2016年 Mobile Pwn2Own 在日本东京落幕，战队元老何淇丹与时任战队队长刘耕铭摘得桂冠，震惊世界
- ...



# 插播历史趣闻

Melody

2015年10月01日

Melody 17:40:58  
我是来自蓝田材化15级大一新生，陈建瑜

Melody 17:41:33  
今天来杭电找ak才知道浙大有这个组织，  
不知道还纳新吗

刘耕铭 17:42:09  
你想做安全？

Melody 17:42:14  
嗯

刘耕铭 17:42:15  
我们不纳新

Melody

2015年10月01日

Melody 22:24:05  
学长

Melody 22:30:36  
我到学校了

Melody 22:30:38  
你还在实验室吗

刘耕铭 22:30:45  
我们没有实验室



## 天青刺客联盟的历史 (4)

接着2017， 2018年， 贵队继续打遍天下

“

我们当年就是从**2017年深圳 RisingStar 夺冠开始，开启了 AAA 黄金一代的光辉。**

接连拿到 SECCON 世界第二， 打进 CodeGate 决赛， 强网杯第二惜败于 eee 战队， 国内除了 eee 基本没有能匹敌的

”



# 天青刺客联盟的历史 (5)

---

然后，像股票一样又到了低谷

“2019年是黑暗的一年”，“我们甚至没有进入XCTF的决赛”，“一场比赛完全靠crypto”，“当时做出一个题目就是胜利了”，“学长是没有学长的” .....



# 天青刺客联盟的历史 (6)

---

然后，像股票一样又到了低谷

“2019年是黑暗的一年”，“我们甚至没有进入XCTF的决赛”，“一场比赛完全靠crypto”，“当时做出一个题目就是胜利了”，“学长是没有学长的” .....



# 天青刺客联盟的历史 (now)

感谢前任队长朱梦凡，黄山在ACTF 19/20 的努力，感谢网安学院在各方面的支持，AAA如今终于再出江湖

新人们站出来取得的成就

全国大学生信息安全竞赛实践赛决赛全国第六名

XNUCA 2020 线上第一名

TCTF/OCTF 2020 新星赛决赛第二名

Plaid CTF 2020 线上世界第一名 (A\*0\*E)

DEFCON CTF 2020 线上世界第一名 (A\*0\*E)

DEFCON CTF 2020 线上世界第一名 (A\*0\*E)

第五届强网杯（2021）线下决赛全国第三名

第五届强网杯（2021）线上赛全国第四名

.....



## 战队当前

---

核心还是打CTF比赛，其他如科研、SRC、护网等也有参加

现役成员可以前往官网或者微信进行查看，活跃参赛选手近20人，还有其他的如科研大佬、币圈大佬等等

还是不够打，还是不够打，*We need more*



# 战队日常



## 比赛比赛比赛

战队会持续地关注由大厂、兄弟队伍组织以及国家官方的比赛，如

- 信息安全创新实践赛（保研赛）
- 由腾讯/华为/字节/阿里举办的比赛 (TCTF/HCTF/AliCTF...)
- XCTF联赛 (今年甚至是出题方)
- 国际赛如SECCON CTF, Codegate, BalsnCTF...
- 联队赛如Plaid CTF, DefCon CTF...



# 战队日常

## 研创性活动

大厂如阿里、华为、腾讯都非常乐于邀请我们参加相关讨论以及分享的活动。

同时借助曾经学长以及网安学院的资源，我们可以蹭到各种讲座以及夏令营。

相关活动包含但不限于

**企业参观：** 蚂蚁安全应急响应中心参观、光年实验室参观、  
华为杭研所参观等

**研讨讨论：** “华为印象”博士茶思会

**夏令营及网课：** 系统组/AI组夏令营





# 战队日常



夜宵撸串

顺便聊聊感情问题



正经吃饭

学期首末的工作安排



不正经吃饭

听说有人得了奖学金



几代同堂吃饭

与真正的大佬同桌battle

还有很多很多如企业吃饭，老师请饭 blabla



# 新鲜分享，周末过去的 ACTF

由于最近发展的较好，XCTF联赛于去年年底邀请AAA为第七届XCTF比赛分站赛最后一场进行出题

时隔七年的再次合作

好的CTFer不仅要做题，还得会出题，还得能保证题目可以正常运行

o! are bots in poorui working correctly?  
Yesterday at 11:08 PM

lemonz 06/25/2022  
is web challenge down?  
3

rgolab 06/25/2022  
gogogo is down again?  
devgianlu Yesterday at 6:01 PM  
<http://124.71.180.254:10022/> is dead

— 06/25/2022  
site not loading

beWhatYouWannaBe is down, fixing it

rgolab 06/25/2022  
again problem with gogogo  
RONIT NARAYANAN IVI Yesterday at 7:52 PM  
<http://124.71.205.170:10047/index.php> (myclient) says connection error

parrot 06/25/2022  
tolesion down?



# 用力过猛

## “20万逆向题”

NutCracker

大家好，我是ARealBug这道逆向题的作者，也是AAA的指导老师，此题花了我一个月时间，难度有点大的是正常的，希望有人能够挑战成功。

NutCracker

大家早上好，刚才有同学来问ARealBug这道逆向题本身会不会有什么问题，我这里明确回复一下，这道题是由C和汇编两种语言混合编程，代码量大约6000行，每行代码我都做过严格调试，程序完成后在3台物理机上做过测试，一台是thinkpad T43，一台是amd cpu的机器，一台是thinkpad x1c 2018。祝各位在比赛结束前能攻破此题。



不过

---

既然现在不是纳新，那就不多叨叨这些了



# Outline – III 回到这门课上

---

- 安全攻防远在身边，近在眼前
- Linux 操作系统 101
- 一些课程的 TIPS



# 发生在身边的安全事件



游戏外挂





# 发生在身边的安全事件

## 恶意、流氓应用

如何看待最近大学生传播的app关不掉声音的“给我O泡”？



### 1013事件

未分类 ▾

今天 傍晚5:07

1013事件

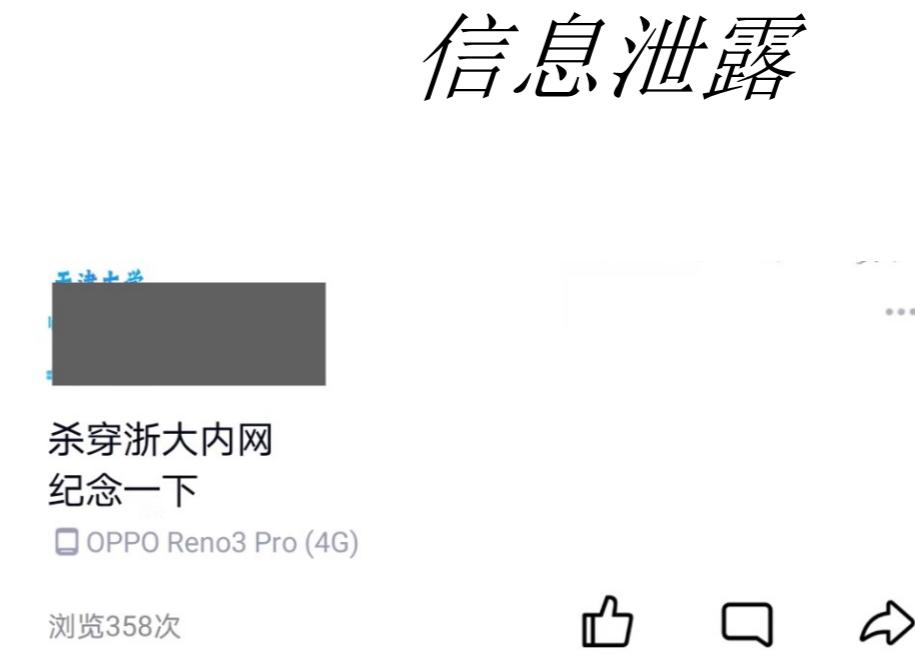
指大学生上课时因莫名软件而散发出的“O泡果奶”广告声，中招者会因该原因产生社会性死亡。

今天在课堂上听到好多次给我O泡，请问大家最近有没有这样的经历



# 发生在身边的安全事件

学习通被曝信息泄露：超 1.7 亿条隐私数据售卖 1.2 万元，甚至包含密码！



什么都不会的话唠萌新、lance1z、0xCaner、一颗好桃、雪高要贾心GGJ、Z、仰望天空却被星星砸到了、浮槎、桢、Ricky Gao等98人觉得很赞

大佬tql  
理看化！: 大佬tql  
: 大佬太强了  
ql  
话唠萌新: 大佬tql



# 后续？

<首页

微博正文

...



腾讯QQ



6-27 11:42 腾讯QQ官方微博 已编辑

+关注

6月26日晚上10点左右，我们收到部分用户反馈QQ号码被盗。QQ安全团队高度重视并立即展开调查，发现主要原因系用户扫描过不法分子伪造的游戏登录二维码并授权登录，该登录行为被黑产团伙劫持并记录，随后被不法分子利用发送不良图片广告。

确认原因后，我们第一时间组织安全技术力量，积极对抗黑产作恶，目前受影响范围已得到控制，受此事件影响的用户帐号也于今日凌晨陆续恢复正常使用。

对于给用户带来的不便，我们深表歉意！目前我们正在收集整理黑产团伙的犯罪证据，后续将根据需要配合有关部门开展工作，保护平台及用户的正当权益。在此，也提醒广大用户，不要扫描来源不明的二维码。在非常用环境下登录帐号时要提高安全警惕，防范帐号被盗风险。

#QQ回应盗号为黑产行为# #QQ盗号#



# 发生在身边的安全事件

小白求教：实验室服务器被挖矿软件攻占怎么办

① 2022-04-17 22:53:03 ② 682 收藏 收起所有图片

电脑医院  
13 / 20568



## 病毒、木马

今天打算上去炼丹发现服务器显卡被占了一半，看了一下后台连接到了nanopool.org,查了一下是个矿池

Processes:						GPU Memory Usage
GPU ID	GI ID	CI	PID	Type	Process name	GPU Memory Usage
0	N/A	N/A	39630	C	./python	5069MiB
1	N/A	N/A	39630	C	./python	5069MiB
2	N/A	N/A	39630	C	./python	5069MiB
3	N/A	N/A	39630	C	./python	5069MiB

```
(base) hztt@hztt-SYS-7049GP-TRT:~$ ps -ef|grep pyt
root      1817      1  0 11:36 ?
root      1898      1  0 11:36 ?
root     39627      1  0 19:57 ?
root    39630  39627  0 19:57 ?
```

【求助】电脑里所有文件都被恶意加密并勒索收费解密，怎么办？

① 2022-02-18 15:19:33 ② 3743 收藏 收起所有图片

电脑医院  
13 / 20568



救救！电脑中了勒索病毒，然后应该怎么办

① 2022-03-23 15:04:16 ② 1373 收藏 收起所有图片

电脑医院  
13 / 20568

救救！电脑中了勒索病毒，所有的文件都被加密了，然后应该怎么办，里面都是我的实验报告



更新：联系了360解密大师的客服，正在解决问题。

期间，360解密大师还远程访问了我的电脑，三下五除二搞定。

那几个文件测试了一下，方法有效！！！

现在正在把所有的盘符的所有文件都解密，速度很慢，预计要几天。密，已是万幸！！！

360真牛逼！！！决定永远不删360软件了。我是普通的免费会员，这个地步真心服了。



# SO 安全攻防离我们真的很近

---

在开始学习所谓的安全实践之前  
一些显而易见的“安全”你做好了么？

- 可千万别用默认密钥和弱密钥了
- 可千万别随便打开邮件和消息中的文件了
- 可千万别瞎下载盗版软件了
- 可千万别再嫌弃频繁的软件和系统更新了
- 可千万别随便浏览XXX网站了 😜



# Suppose 这门课程结束后

概括来说

- 自学能力的提升 
- 通过入门 CTF 从而为后续的课程研究打开不一样的视角

细节来说

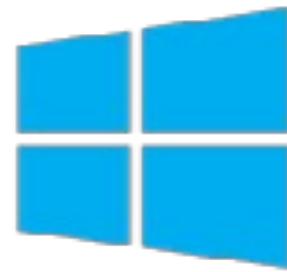
- 学会各方向 CTF 赛题基础部分的求解
- 在所选的专题方向上完成拔高
- 完成作业，取得一个好绩点



# Linux 操作系统 101

---

**Linux** (/ˈli:nʊks/ (listen) LEE-nuuks or /'lɪnʊks/ LIN-uuks) is a family of open-source ***Unix-like*** operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991, by ***Linus Torvalds***.



Windows 8

X  
Mac OS X





# kernel.org

Protocol	Location
HTTP	<a href="https://www.kernel.org/pub/">https://www.kernel.org/pub/</a>
GIT	<a href="https://git.kernel.org/">https://git.kernel.org/</a>
RSYNC	<a href="rsync://rsync.kernel.org/pub/">rsync://rsync.kernel.org/pub/</a>

Latest Release

5.18.5 

mainline:	5.19-rc3	2022-06-19	<a href="#">[tarball]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>	<a href="#">[browse]</a>
stable:	5.18.5	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
stable:	5.17.15 [EOL]	2022-06-14	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
longterm:	5.15.48	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
longterm:	5.10.123	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
longterm:	5.4.199	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
longterm:	4.19.248	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
longterm:	4.14.284	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
longterm:	4.9.319	2022-06-16	<a href="#">[tarball]</a>	<a href="#">[pgp]</a>	<a href="#">[patch]</a>	<a href="#">[inc. patch]</a>	<a href="#">[view diff]</a>
linux-next:	next-20220621	2022-06-21					<a href="#">[browse]</a>



# 为什么这节课中要使用 Linux

---

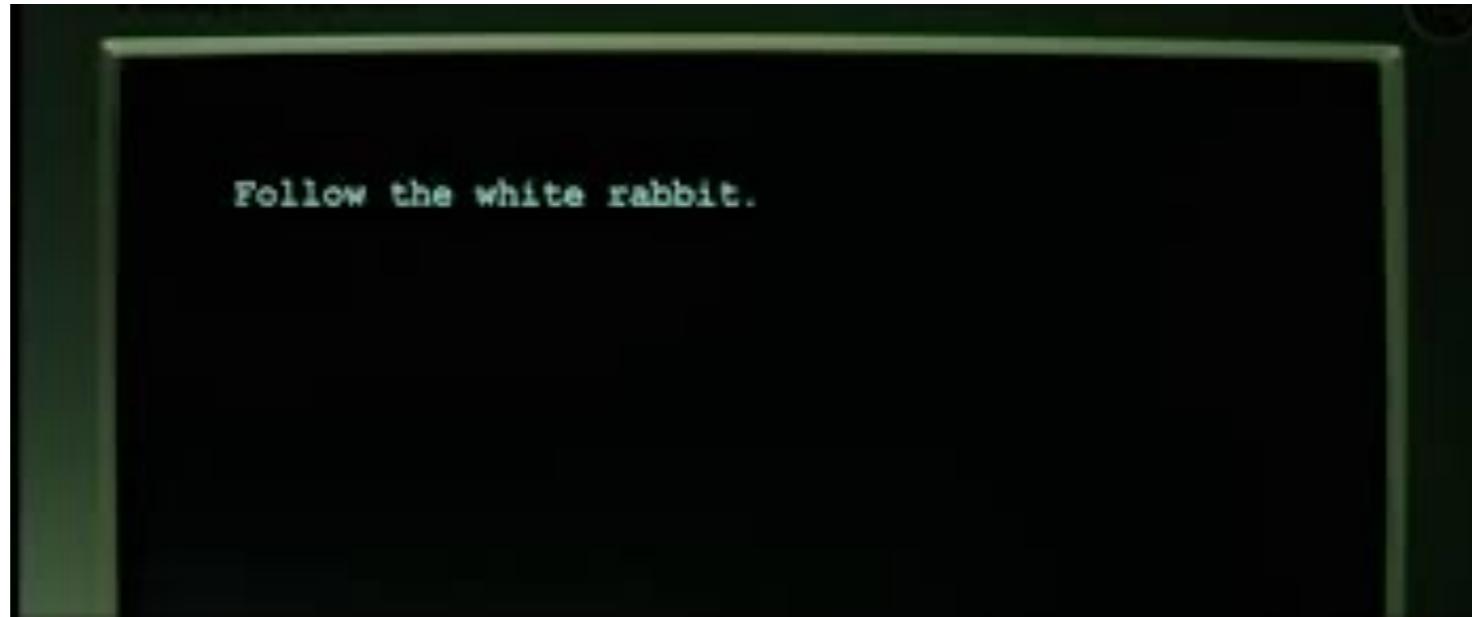
1. Linux上环境搭建、工具安装都相对称手
2. 对于 reverse 和 pwn 而言，从 Linux 出发的门槛要低很多
3. 早点熟悉 Linux is not a bad choice
4. 部分工具仅支持 Linux 端构建

BTW，不建议完全以Linux作为host，毕竟连个微信都没有 :(  
（注：此处“微信”指的是一种编程技巧或方法）



# what is shell

---



In computing, a ***shell*** is a computer program which exposes an ***operating system's services to a human user or other programs***. In general, operating system shells use either a ***command-line interface (CLI) or graphical user interface (GUI)***, depending on a computer's role and particular operation. It is named a shell because ***it is the outermost layer around the operating system***.



# demo time

---



# 记住如下 UNIX Shell Command

---

划重点，实验里要用的

- ls
- pwd
- cat
- echo
- cp
- mv



# 记住如下 UNIX Shell Command

记住了么

- ls A. 连接和打印文件
- pwd B. 打印当前目录路径
- cat C. 列举当局目录
- echo D. 输出参数到标注输出
- cp E. 移动文件
- mv F. 拷贝文件



# 记住如下 UNIX Shell Command

记住了么

- ls → A. 连接和打印文件
- pwd → B. 打印当前目录路径
- cat → C. 列举当局目录
- echo → D. 输出参数到标注输出
- cp → E. 移动文件
- mv → F. 拷贝文件



# 划重点

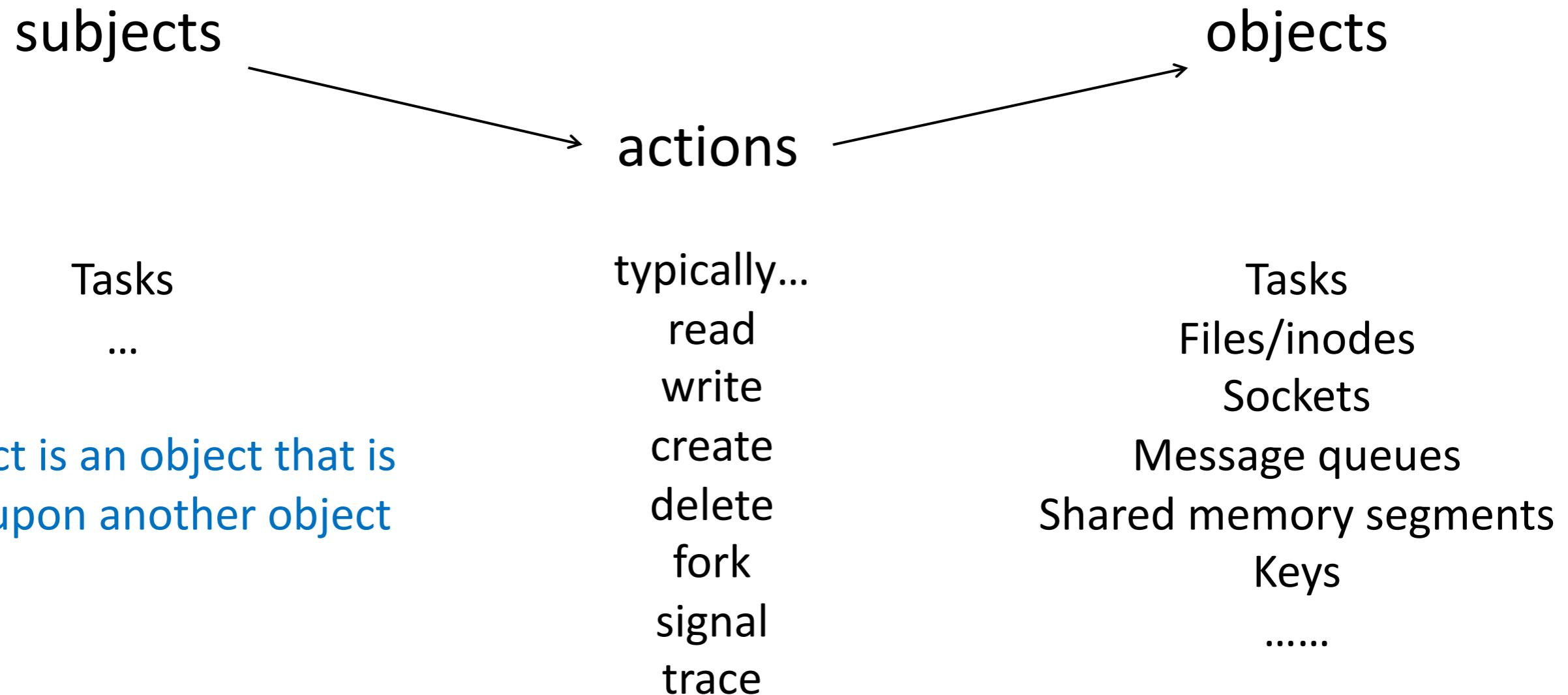
---

chown (change file owner and group)

chmod (change file modes and Access Control List)



# Linux 权限管理 – 基本概念



***When a subject acts upon an object. a security calculation is made***



# Rules

---

- Discretionary access control (DAC)  
自主访问控制  
owner subjective 可以自主决定是否将 objective 的访问权许授予其他 subjective
- Mandatory access control (MAC)  
强制访问控制  
OS 统一约束 subjective 对 objective 的访问



# Rules

---

- **Discretionary access control (DAC)**

自主访问控制

owner subjective 可以自主决定是否将 objective 的访问权许授予其他 subjective

- Mandatory access control (MAC)

强制访问控制

OS 统一约束 subjective 对 objective 的访问



# Since in Linux

---



所以我们简单的讨论 file 的访问控制



# For a traditional Unix User

---

用户进行身份标注为：

- Real User ID
- Real Group ID

注意

- root (uid 0) is the **superuser**
- unprivileged users can use the **su** and **sudo** programs for privilege elevation
- user can be added into an existing group to utilize the **privileged access it grants**



moreover

---

用户的 credentials 还有

- Effective, Saved and FS User ID
- Effective, Saved and FS Group ID



# File Permission - 1

---

*In Linux, each **file** is associated with an **owner** and a **group** and assigned with **permission access rights** for three different classes of users*

非常 coarse 的粒度

- owner user
- group users
- others (every user else)



# File Permission - 2

---

There are **three** file permissions types that apply to each class

- read
- write
- execute



# File Permission - together

```
-rw-r--r-- 12 linuxize users 12.0K Apr  8 20:51 filename.txt
| [-][-][-] [-----] [---]
| | | | | | +-----> 7. Group
| | | | | +-----> 6. Owner
| | | +-----> 5. Alternate Access Method
| | +-----> 4. Others Permissions
| +-----> 3. Group Permissions
+-----> 2. Owner Permissions
+-----> 1. File Type
```

The first two columns of the file permission output are circled in red, highlighting the user and group information.



# Some more interesting stuffs

---

- ssh and remote shell
- setuid
- symbolic link
- environment variable
- ...



# 一些课程的 tips

---

掏心窝子说几句

- 关于这门课程和专题
- 一些学习建议
  - For 小白
  - For 大佬
- 关于CTF和安全方向本身



## Last but not least

---

剑者，心之刃也，既可为杀，亦可为护。杀与护，不过一念之间  
——仙剑奇侠传



你怎么也进来了？