

---

# 网络攻防实战

---

第一周

陈健

[chenj@nju.edu.cn](mailto:chenj@nju.edu.cn)

---

# 准备工作

---

本课程QQ群号 301264016

进群请修改群昵称为：学号 姓名

# 课程简介

---

- 课程名称-《网络攻防实战》
  - 教学目标
    - 通过实验进一步巩固和加深对计算机网络安全、信息安全基本概念的理解与掌握
    - 掌握网络渗透攻击实战所需的基本能力
    - 掌握安全漏洞的独立分析、挖掘与验证所需的基本能力
    - 培养学生对网络安全领域的兴趣
-

# 注意事项

---

## □ 法律红线

- 所有知识技能仅限在授权的合法环境中使用。未经明确许可，对任何系统进行探测、渗透或攻击均属违法

## □ 审慎负责

- 仅在课程要求的实验环境和自有设备上使用工具，不访问、不干扰、不破坏任何非授权目标

## □ 专业操守

- 牢记技术应用的道德边界，所学应用于防御、研究和促进安全，绝不用于恶意目的、个人炫耀或非法牟利

# 怎么学习网络安全



# 怎么学习网络安全

---

- 对于安全入门来说，宽度比深度更重要！
  - 切入点：渗透测试

# 怎么学习网络安全

---

- 网络安全的核心能力：攻击和防御
  - 网络攻击：非法使用或获取网络中的信息或破坏网络正常运行的行为
  - 网络防守：保护计算机网络的各种技术
- 学习安全从攻击手段入门！

# CTF夺旗赛简介

---

- CTF (Capture The Flag) 夺旗赛是网络安全领域中网络安全技术人员之间进行技术竞技的一种比赛形式
  - 起源于1996年DEFCON全球黑客大会
  - 参赛团队之间通过攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这串内容称为“flag”

# CTF夺旗赛简介

---

- 竞赛模式
  - 解题模式
    - 参赛队伍通过互联网在线参与，题目主要包含六个类别：**RE**逆向工程、**Pwn**漏洞挖掘与利用、**Web**渗透、**Crypto**密码学、**Mobile**移动安全和**Misc**安全杂项
  - 攻防模式
    - 参赛队伍在网络空间互相进行攻击和防守，通过挖掘网络服务漏洞并攻击对手服务来得分，通过修补自身服务漏洞进行防御来避免丢分
  - 混合模式
    - 参赛队伍通过解题获取一些初始分数，然后通过攻防对抗进行得分增减，最终以得分高低分出胜负

# 网络安全竞赛简介

□ ctftime.org

The screenshot shows the homepage of ctftime.org. At the top, there's a navigation bar with links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, Contact us, and About. There's also a 'Sign in' button. Below the navigation is a search bar with the placeholder 'Search CTFs, teams, news...'. The main content area has two main sections: 'Team rating' and 'Past events'.

**Team rating**

This section displays a table of the top 10 teams based on their rating. The columns are Place, Team, Country, and Rating. The teams listed are: 1. d33f0g, 2. kummuunien, 3. Infiltrate, 4. ..., 5. Project Selen, 6. justdialTheRisk, 7. theblackzenome, 8. The Flat Network Society, 9. L33k, and 10. Never Stop Exploiting.

**Past events**

This section lists three past events with their results:

- idekCTF 2025** (July 04, 2025 08:00 UTC | On-line | Write-up voting in progress)  
Top 3 teams: 1. FluFingers (Germany), 2. CyberSquad (Hungary), 3. Team Greece.
- justCTF 2025** (June 03, 2025 19:00 UTC | On-line | Write-up voting in progress)  
Top 3 teams: 1. Project Sekai (Hungary), 2. Infiltrate (Hungary), 3. kummuunien (Finland).
- World Wide CTF 2025** (July 26, 2025 12:00 UTC | On-line)  
Top 3 teams: 1. r00tdeaf0l (Hungary), 2. Rubyball (Hungary), 3. D33f0g (Hungary).

**Upcoming events**

This section lists two upcoming events:

- WHY2025 CTF** (On-line) - Date: July 08, 16:00 — July 11, 16:00 UTC | Duration: 3d 0h | 179 tasks.
- Bartown CTF 2025** (On-line) - Date: July 08, 16:00 — July 08, 19:00 UTC | Duration: 1d 3h | 181 tasks.

# 网络安全竞赛简介

---

## □ DEFCON CTF

- 起源于1996年DEFCON全球黑客大会
- 全球最有影响力的黑客竞赛 - “黑客世界杯”
- 1996年开始，已成功举办29届
- 中国战队成绩
  - 2015年：blue-lotus 第4名
  - 2016年：blo0p 第2名
  - 2017年：hitcon 第2名
  - 2020、2021年：A\*0\*E、kazebin分别获得第1名

# 网络安全竞赛简介

---

## □ Pwn2Own

- 黑客界的奥林匹克
- Pwn2Own的目标是四大浏览器IE、Chrome、Safari和Firefox的最新版
- 中国战队成绩
  - 2016年：腾讯安全Sniper战队 第1名
  - 2017年：360安全团队、Sniper科恩实验室、长亭安全团队分获前三名

# 网络安全竞赛简介

---

- CGC
  - 旨在推进自动化网络攻防技术的发展
- XCTF联赛
- 全国大学生信息安全竞赛
- 强网杯全国网络安全挑战赛
- HITCON CTF
- OCTF/TCTF

# DEFCON CTF 拉斯维加斯决赛现场

---



# Linux发行版排名

## GNU/Linux Distributions Listed by Google Trends Scores

Ranked by average weekly scores over a one year period between January 2023 - January 2024

#	Name	Score	#	Name	Score	#	Name	Score	#	Name	Score
1	Ubuntu	6	21	Parrot	46	41	KDE neon	14	61	Archman	88
2	Debian	4	22	Lubuntu	43	42	Slax	79	62	PureOS	52
3	Kali	18	23	Kubuntu	34	43	Solus	32	63	ClearOS	57
4	CentOS	50	24	Xubuntu	54	44	Vanilla	23	64	Endless	78
5	Arch	63	25	OpenSUSE	9	45	Nobara	18	65	LXLE	91
6	Linux Mint	2	26	MX Linux	1	46	Knoppix	276	66	Rosa	105
7	Fedor	7	27	Elementary	13	47	Ubuntu Studio	92	67	Ubuntu Kylin	151
8	RHEL	62	28	Endeavour	3	48	Bodhi	41	68	SmartOS	37
9	Manjaro	5	29	Deepin	77	49	Q4OS	29	69	BunsenLabs	111
10	RasPi OS	122	30	Linux Lite	11	50	LinuxFX	51	70	PCLinuxOS	22
11	Alpine	27	31	Puppy Linux	19	51	Mageia	17	71	Kodachi	88
12	Pop!_OS	6	32	Slackware	42	52	ArcoLinux	26	72	SparkyLinux	20
13	Rocky	48	33	Garuda	12	53	Artix	78	73	Archcraft	49
14	Oracle Linux	87	34	Qubes	53	54	Peppermint	31	74	XeroLinux	56
15	Tails	38	35	Void	93	55	Ubuntu Budgie	107	75	AV Linux	103
16	Zorin	10	36	Ubuntu MATE	82	56	Ultimate Linux	152	76	Athena	66
17	NixOS	26	37	ALT Linux	64	57	wattOS	69	77	SystemRescue	332
18	AlmaLinux	21	38	antiX	15	58	Clear Linux	67	78	Voyager	40
19	Gentoo	59	39	BlackArch	182	59	Devuan	38	79	Nitrx	61
20	SteamOS	175	40	Tiny Core	75	60	blendOS	45	80	EuroLinux	74

# KALI Linux

---

- 官网地址 [www.kali.org](http://www.kali.org)
- 基于Debian的Linux发行版本
- 前身是BackTrack, 2013年3月发布
- 用于渗透测试和安全审计
- 包含600+安全工具
- 支持ARM和手机平台

# 使用Linux

---

- 通过虚拟化软件安装/导入Linux
    - virtualbox
      - [www.virtualbox.org](http://www.virtualbox.org)
    - vmware
      - [www.vmware.com](http://www.vmware.com)
  - 通过微软的WSL
  - 申请公有云上的Linux虚拟机
  - 在mini主机、树莓派等小型主机上安装Linux系统
  - Live USB
-

# 通过virtualbox导入ubuntu Linux

---

## □ 虚拟机镜像

■ <https://box.nju.edu.cn/d/a51ffa79c40c49e19bc8/>

## □ 虚拟机镜像导入方法

■ <https://www.arysontechnologies.com/blog/how-to-open-vdi-file/>

---

# Virtualbox中虚拟机的网络设置

---

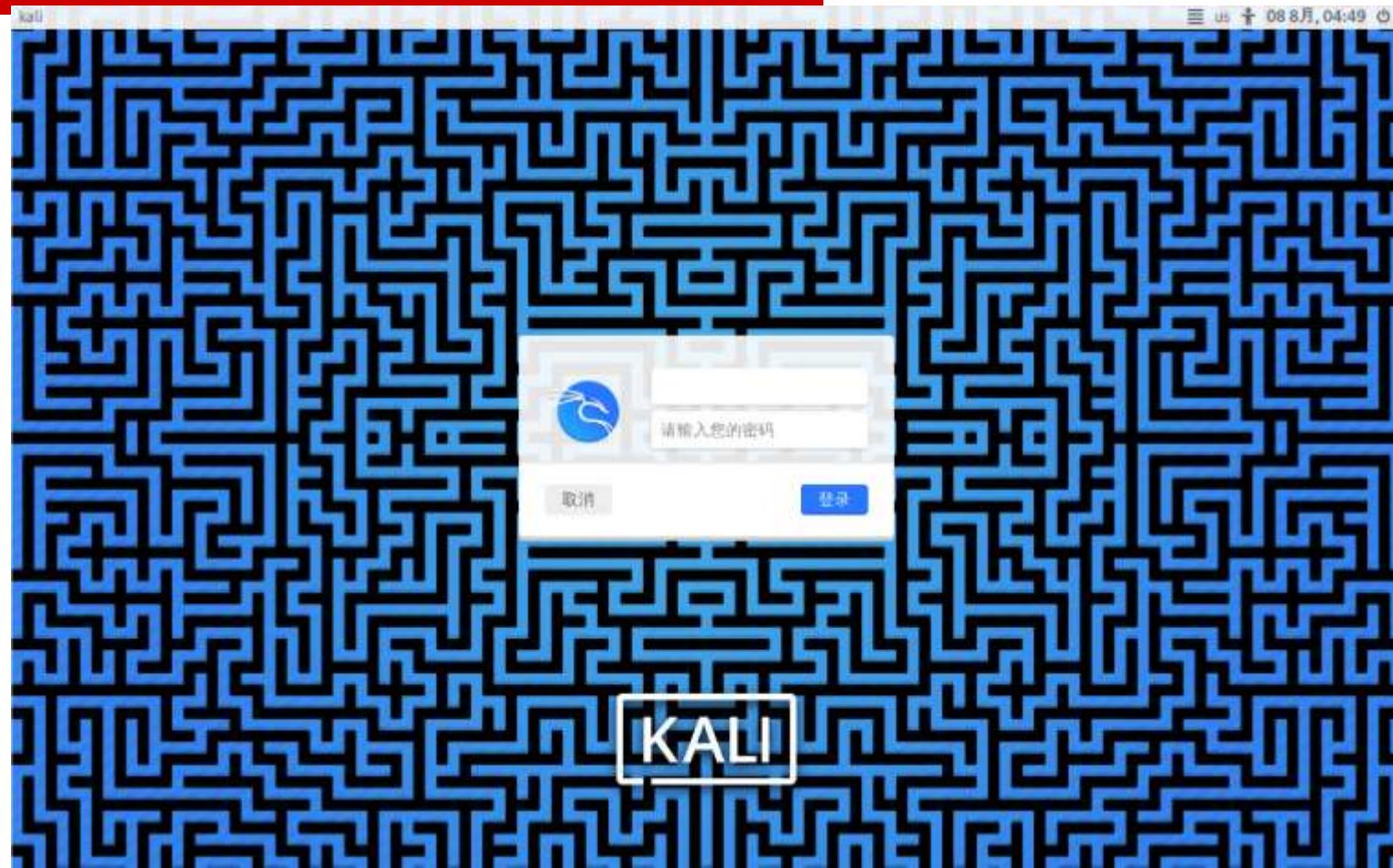
## □添加NAT网络

- 管理->工具->网络管理器->NAT网络->创建

## □虚拟机连接NAT网络

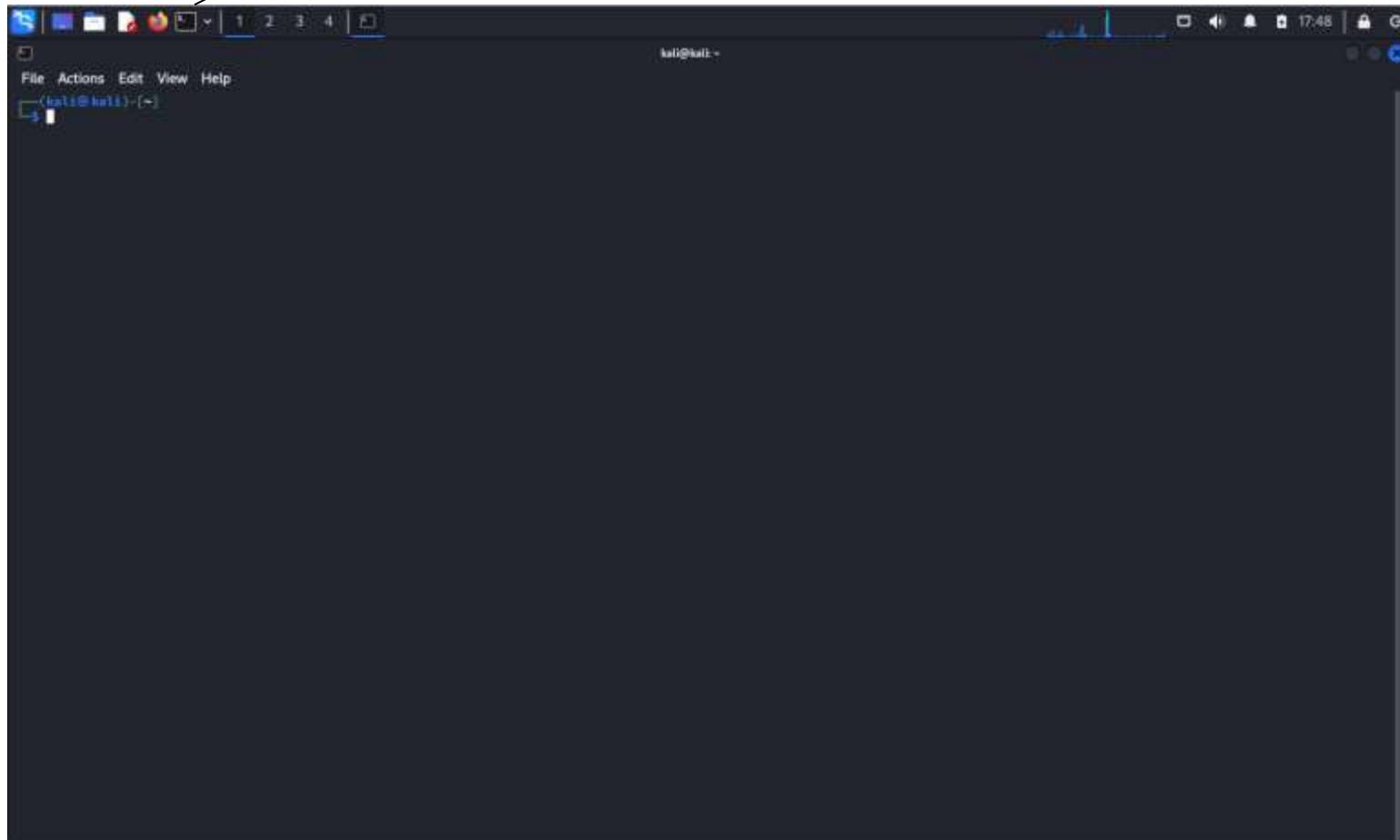
- 选择虚拟机->设置->网络->网卡1->连接方式设置为NAT网络

# Kali Linux登录界面



# 打开终端

点击该图标或按下ctrl-alt-t组合键打开终端



# Shell prompt

---

```
$ date
```

```
Fri Aug 8 08:42:56 PM CST 2025
```

```
$ echo "zone=Asia/Shanghai" | sudo tee -a /usr/share/zoneinfo/Asia/Shanghai
```

```
$ sudo rm /etc/localtime
```

```
$ sudo ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
```

---

# 修改密码

---

```
$ passwd
```