
东南大学网络安全联盟
扫一扫二维码，加入群聊。


网络安全联盟博客


Hello SUS
Presented by SUS.Imagemlt

CONTENT

1 社团简介

社团简介

东南大学网络安全联盟(Security Union of SEU)成立于2005年，是一个以促进网络安全爱好者交流为目的，普及网络安全知识为宗旨的社团。

多年来，网安一直坚持“秉承古典黑客精神，引领一流网络安全体验”的宗旨，活跃在学校的各个角落，致力于信息安全技术研究，为对信息安全感兴趣的同学提供技术交流和学习的平台。

社团战队参加各类信息安全竞赛，在各类全国比赛乃至国际比赛中赢得优异成绩；社团内也走出了数位百度、阿里巴巴、腾讯、绿盟等著名互联网公司网络安全团队的技术人才。

社团简介

历届会长

2005—2006	符东辉	Fu
2006—2007	符东辉	Fu
2007—2008	肖剑	单克隆抗体
2008—2009	程岩	暗夜潜风
2009—2010	丁杨	dingo
2010—2011	高岳	我有一把刷子
2011—2012	徐昊	High Power
2012—2013	王迪	Hemlso
2013—2014	杨梦源	kamael
2014—2015	印明亮	ymlbright
2015—2016	刘延栋	Laputa
2016—2017	杨青	Young
2017—2018	徐诚	Xu

社团简介

老前辈们

- Oldjun
- Flyh4t
- 日辰
- 幽游
- 夕草
- Edge
- Allen
- Tcpper
- 风卷
- Do9gy
- Aragorn
- ……

社团简介

现在的社团架构

社团简介

组织部&&宣传部

- 组织部：
  - 协助社团各个部门开展工作，使各部门的作更好的完成，协助安全实验室的成员为各个活动提供技术支持
  - 积极参与社团各个活动的组织策划

- 宣传部
  - 为社团举办的各类活动进行前期、后期宣传，并在举办活动时进行实时宣传
  - 整理社团资料，协助技术组维护练习平台、社团技术博客等
  - 为社团成员，全校同学第一时间传递社团活动信息

社团简介

技术组

目前技术组成员：



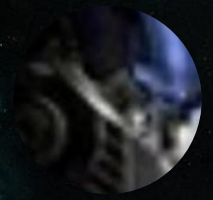





社团简介

社长&&副社长

社长：



马凌涛

副社长：

张林樾

社团简介

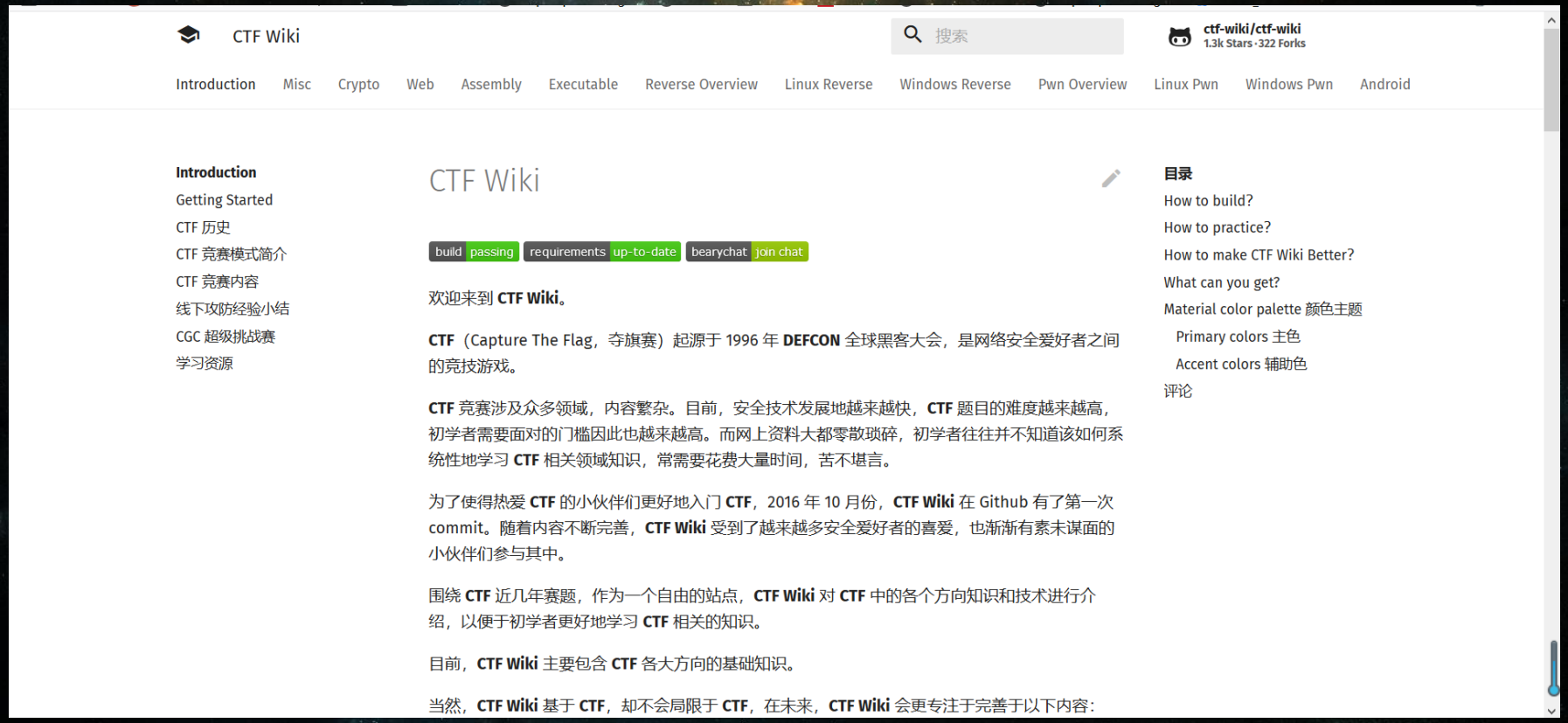
Blog

- https://susers.github.io/

社团简介

CTF-wiki

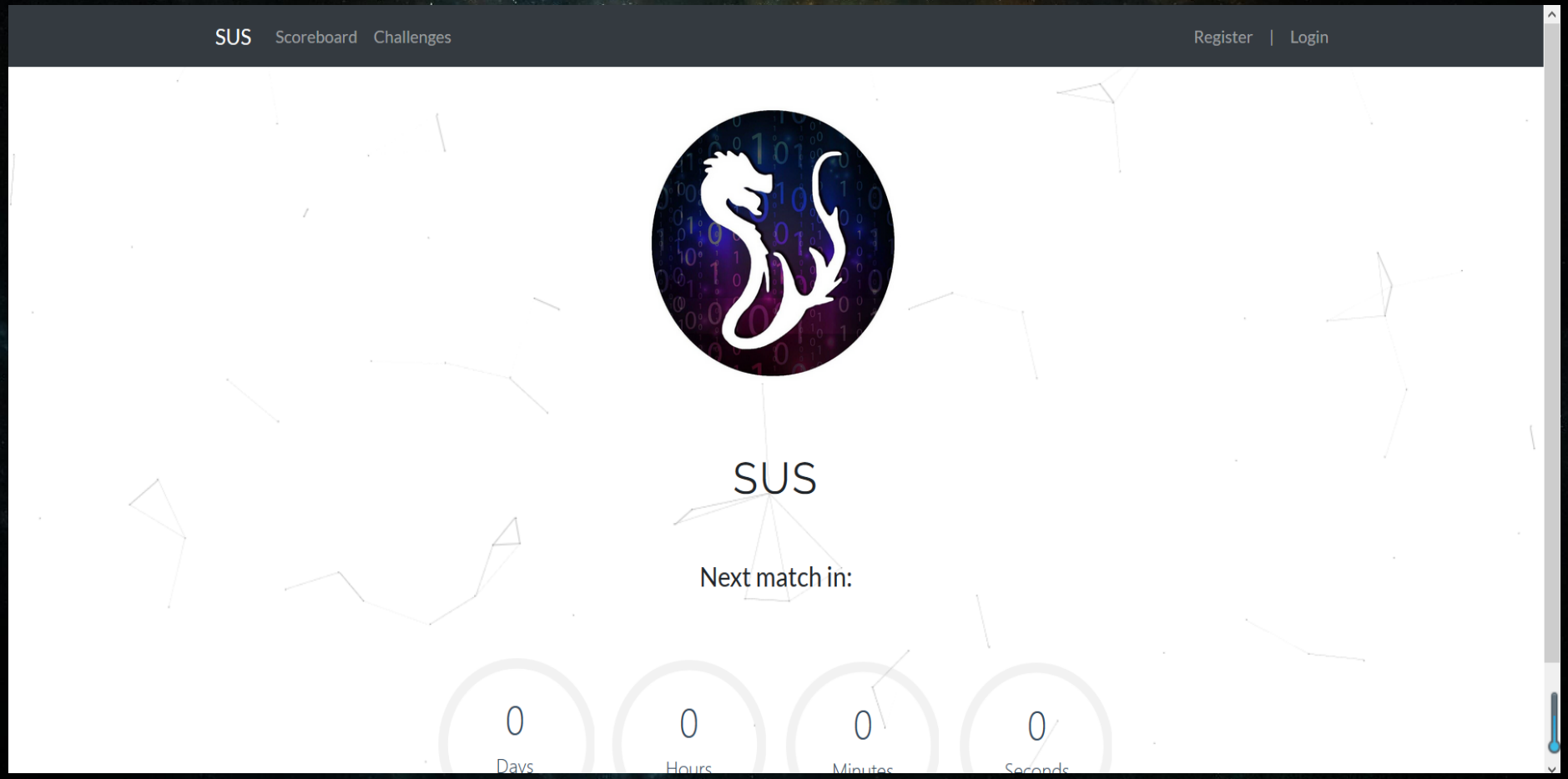
- https://ctf-wiki.github.io/ctf-wiki/#/



社团简介

实训平台

- http://sus.njnet6.edu.cn/



社团简介

社团战队SUS(Hydr4g0n)

- 2017.9 SU 战队WHCTF 第四名
- 2017.9 ISG-2017 教育组三等奖
- 第四届“问鼎杯" 优胜奖
- 江苏省第六届信息安全技能竞赛 二等奖
- 2017 高校网络信息安全管理运维赛 华东区二等奖，全国三等奖
- 2017 中国智能汽车挑战赛初赛第六,优秀奖
- 2017 XNUCA全国总决赛第五，二等奖
- 2017 HCTF国际赛 第十六名
- 2017 厦门大学“全国网络安全精英邀请赛" 全国第?四名
- I春秋 “2017赛季网络安全竞赛排名” 第四名
- 2017 NCTF-2017 ?校组三等奖|XCTF国际联赛组委会
- 2018 西湖论剑 团体三等奖
- 2018 CISCN全国大学生信息安全竞赛技能赛 全国三等奖

社团简介

社团荣誉

2 什么是网络安全

什么是网络安全

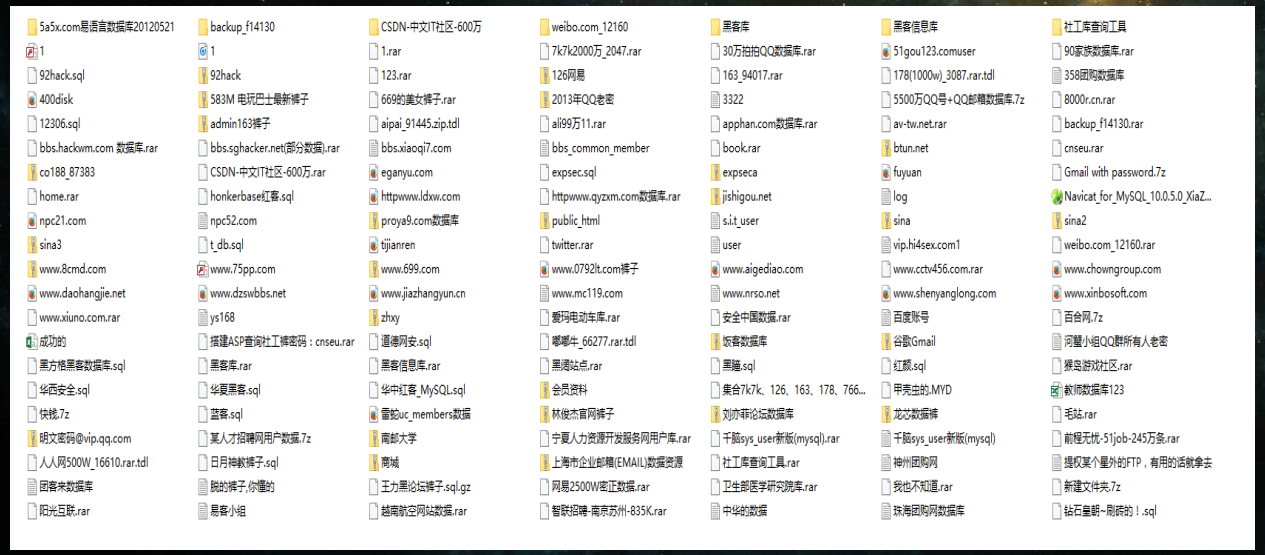
近年网络安全大事件

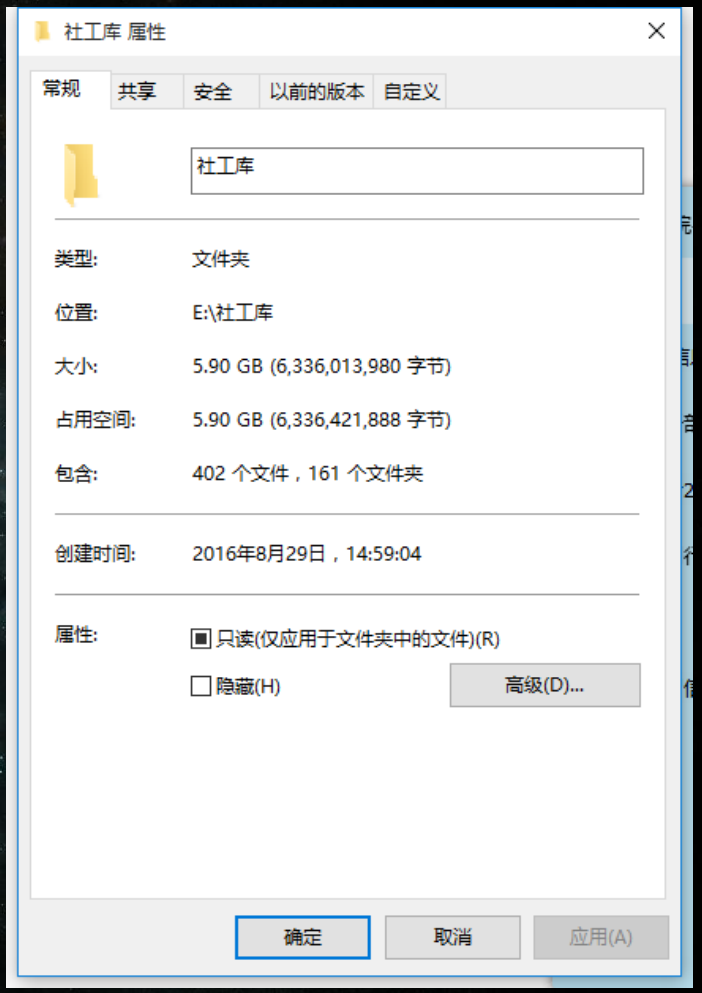
- 2017 Struts漏洞
- 2017 NSA武器库泄露
- 2017 WannaCry勒索病毒
- 2018.1 meldown与Spectre漏洞 影响所有Intel CPU
- Facebook深陷丑闻 千万用户信息遭泄露
- 2018.6 Acfun遭受黑客攻击泄露近千万条用户数据
- 2018.5 区块链平台EOS现史诗级系列高危安全漏洞
- 2018.8 华住大量数据泄露

什么是网络安全

社会工程学

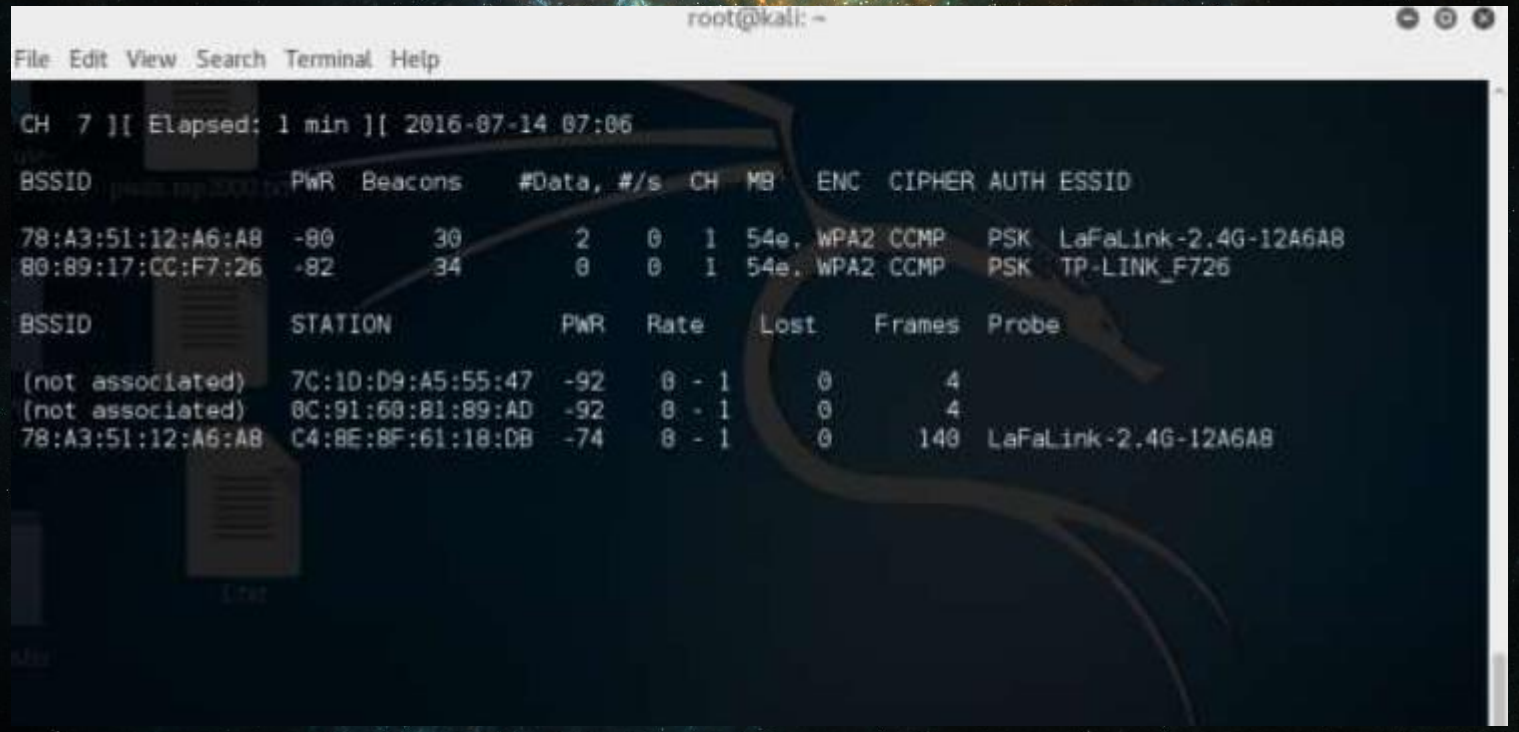
- [看我如何社工Xiaoba并且冻结他的财付通]





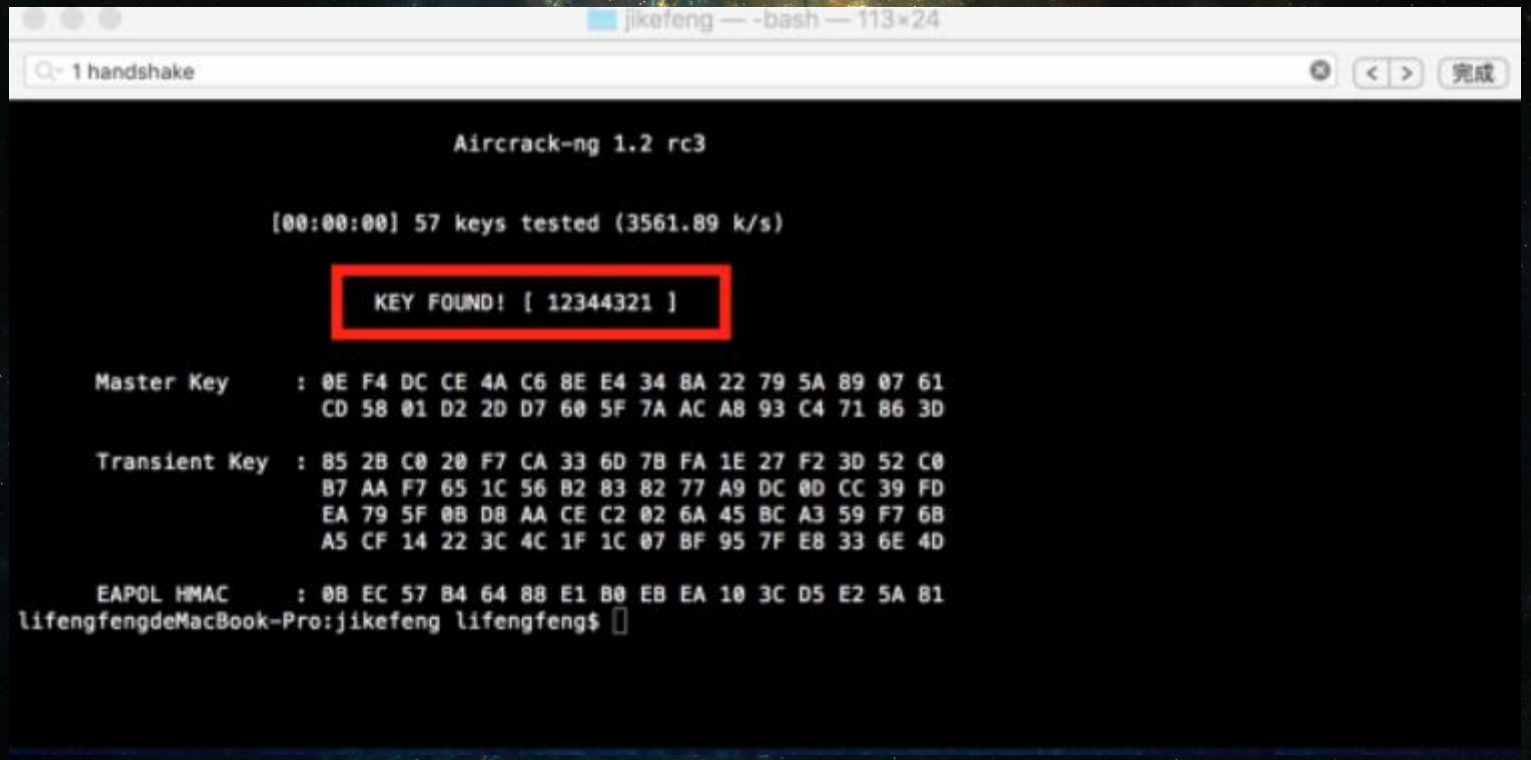
什么是网络安全

- 通信安全——无线安全
  - Kali Linux使用Aircrack破解wifi密码(wpa/wpa2)



什么是网络安全

- 通信安全——无线安全



什么是网络安全

网站攻防

- 小实验——对某个个人博客的一次渗透到获取服务器root权限
  - 文件包含漏洞读取配置文件信息
  - 判断真实ip 利用redis提权
  - 维持权限

什么是网络安全

病毒木马

Metasploit实现木马生成、捆绑、免杀

```
[>] Please enter the base name for output files (default is 'payload'):

Language:           powershell
Payload:            powershell/meterpreter/rev_http
Required Options:   LHOST=192.168.23.142  LPORT=12345  LURI=/  PROXY=N
                    STAGERURILENGTH=4  USER_AGENT=Mozilla/4.0
                    (compatible; MSIE 6.1; Windows NT)
Payload File:       /var/lib/veil-evasion/output/source/payload.bat
Handler File:       /var/lib/veil-evasion/output/handlers/payload_handler.rc

[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)

[>] Press any key to return to the main menu.
```

什么是网络安全

硬件安全

- 基于ArduinoLeonardo板子的BadUSB攻击实战

什么是网络安全

- 移动安全
- 逆向破解
- 加密解密
- 工控安全
- 。。。。。。

3 什么是CTF竞赛

CTF竞赛介绍

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

CTF竞赛介绍

一些知名赛事

- 国际赛事
  - 国际赛事大多收录于CTF-TIME中，如DEFCON HITCON 等，其中DEfCON为顶级赛事
  - 其他的不错的比赛：
    - CSAW
    - GoogleCTF
    - 34c3
    - SECCON
- 国内
  - XCTF联赛（包含多个分赛）
  - XNUCA（全国高校网安联赛，中科院举办）
  - HCTF（杭电举办，原属XCTF分站赛后独立举办）
  - CISCN（学校承认的国赛）
  - 省内：天翼杯、领航杯

CTF竞赛介绍

国际知名战队：

- PPP（美国CMU，包括GeoHot等人） Shellfish （美国）Cykor（韩国） 俄罗斯LC&C战队

国内知名战队：

- 蓝莲花（国内CTF先驱，最先打入DEFCON）
- HITCON（台湾一支联合战队）
- Tea Deliverers （蓝莲花核心成员重组的一支战队）
- r3kapig (国内一支新成立的战队，由FlappyPig与Eur3ka组成)
- 其他知名战队：
  - 浙大AAA，腾讯eee,清华Redbud，北邮天枢战队，北航lancet战队，福州大学ROIS战队，多校联合战队Nu1L,SU战队（江苏高校联队），Xlcteam等等

CTF竞赛介绍

SU战队

- SU战队简介：江苏省网络安全联盟

SU战队战绩：2016alictf第十名，XMAN夏令营练习赛第一名、结业赛解题第三名、攻防赛第五名、总排名第三名。2016华山杯初赛第十名，决赛第七名、第三届xctf总决赛、2017 whctf第四名、SCTF第八名等等

•战队目标：努力发展成为国内一流战队，走上国际赛场

CTF竞赛介绍

正题：CTF比赛类型

一般分为两种：

- 解题模式（Jeopardy）
  - 题型分类:web re pwn crypto misc
- 攻防模式（Attack-Defence）
  - 主要为pwn和web

CTF竞赛介绍

战队与技术组招人

我们需要：

- Web手
- 逆向手
- Pwn手
- 密码学
- 每个方向最好兼职Misc

CTF竞赛介绍

选拔方式

- 期中考试后举办校赛，具体时间之后在群里通知
- 下学期大概4月份举办面向南京市各高校的邀请赛，同时也作为对校内的第二次招新
- 录取方式：排名+面试（面试主要用于确定是否存在作弊现象）

CTF竞赛介绍

加入我们的福利：

- 队内技术指导
- 征战各大CTF赛事，以及各大安全会议的免费门票
- 战队内部资源共享
- 各大互联网公司内推机会，部分高校网安方向保研机会（我校网安学院比较重视CTF比赛，CTF比赛在网安学院认可度高于ACM等）
- 学到知识，提升自己的实力（重中之重）

4

如何踏上黑客之道（预告）

如何踏上黑客之道（预告）

下次宣讲会之前希望大家提前掌握：

- 虚拟机
- 虚拟机中运行linux(推荐ubuntu，或者直接Kali)
- https://ctf-wiki.github.io/ctf-wiki/#/
- 活动：
  - 国庆期间萌新试水赛（地址之后另行通知）
  - 萌新赛讲解，礼物发放
  - 各个方向的成员给大家提出学习建议

网站推荐

实验吧：http://www.shiyanbar.com/

i春秋：http://www.ichunqiu.com/

安全客：https://www.anquanke.com/

Freebuf：http://www.freebuf.com/

先知社区：http://xz.aliyun.com/

看雪：http://www.pediy.com/

吾爱破解：http://www.52pojie.cn/

电子书下载：http://www.jb51.net/books/

THANK YOU!

PRESENTED BY OFFICEPLUS


东南大学网络安全联盟
扫一扫二维码，加入群聊。


网络安全联盟博客