

QQ



Blog





Q: 你们这个主要是做什么的啊 ? ? ? ?

Q: 我是零基础 , 啥也不懂能加吗 ? ?



Hello SUSers

By SUS: Xu



01

社团简介

02

什么是网络安全

03

萌新赛

04

如何踏上黑客之道（预）

Part 1

社团简介

Part 1 社团简介



SUS Team

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。

Part 1 社团简介



SUS Team

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—2015	杨梦源	Kamael
2014—2015	印明亮	ymlbright
2015—2016	刘延栋	Laputa
2016—2017	杨青	Young

Part 1 社团简介



SUS Team

老前辈们

- Oldjun
- Flyh4t
- 日辰
- 幽游
- 夕草
- edge
- Allen
- Tcpper
- 风卷
- do9gy
- Aragorn
-

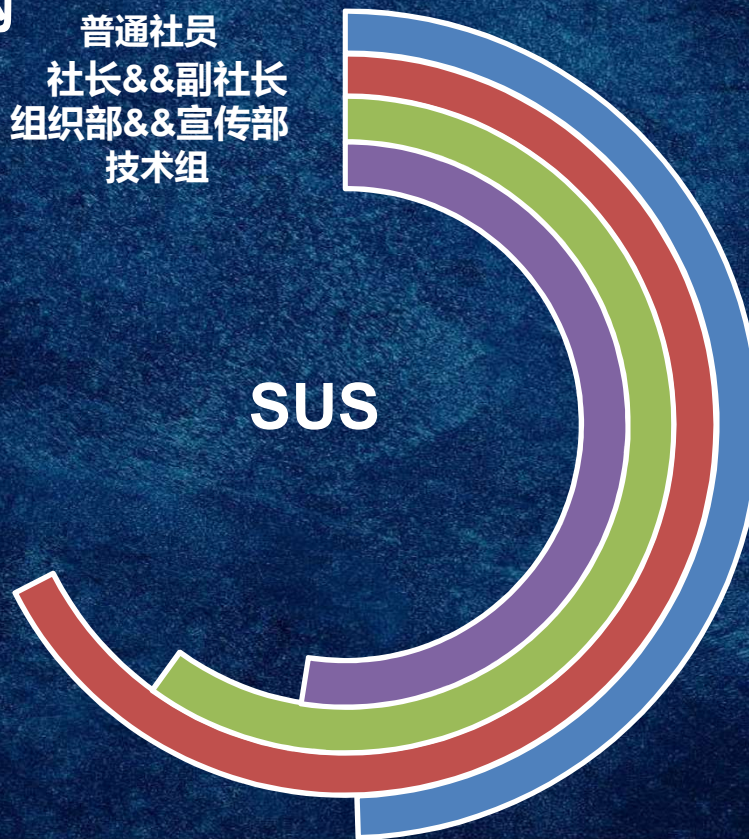
Part 1 社团简介



SUS Team

现在的社团架构

普通社员
社长&&副社长
组织部&&宣传部
技术组



Part 1 社团简介



SUS Team

技术组

隐写取证

徐诚

移动安全

肖贻杰
张林樾

网站攻防

杨青
马凌涛

漏洞利用

徐诚

逆向工程

肖贻杰
张林樾

Else :
胡金涛 , 高语伦

Part 1 社团简介



SUS Team

组织部&&宣传部

组织部：



李玥琚

宣传部：



樊梦颖

Part 1 社团简介



SUS Team

社长&&副社长

社长：



徐诚

副社长：



莫少煌

Part 1 社团简介



SUS Team

Blog

SUS


SUS

秉承古典黑客精神，引领一流网络安全体验

- About
- Notice
- Archives
- Course
- OJ
- CTF-Wiki

通知：新人赛

Posted on 2017-09-24 | 分类于 [Notice](#)



Susers

7	5	6
Posts	Categories	Tags

GitHub

Links

[BXS Team](#)

Part 1 社团简介



SUS Team

Blog:CTF-wiki

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。

CTF-wiki

CTF Wiki是一个免费开放且持续更新的知识整合站点，你可以在这里学到关于CTF竞赛及网络安全相关的有趣知识，我们为你准备了CTF竞赛中的基础知识、常见题型、解题思路以及常用工具等，帮助你更快速地了解CTF竞赛以及网络安全。



现代CTF竞赛

由专业队伍承担比赛平台、命题、赛事组织以及自动化积分系统。参赛队伍需提交参赛申请，由 DEFCON 会议组织者进行评选。



Susers

7
Posts

5
Categories

6
Tags

GitHub

Links

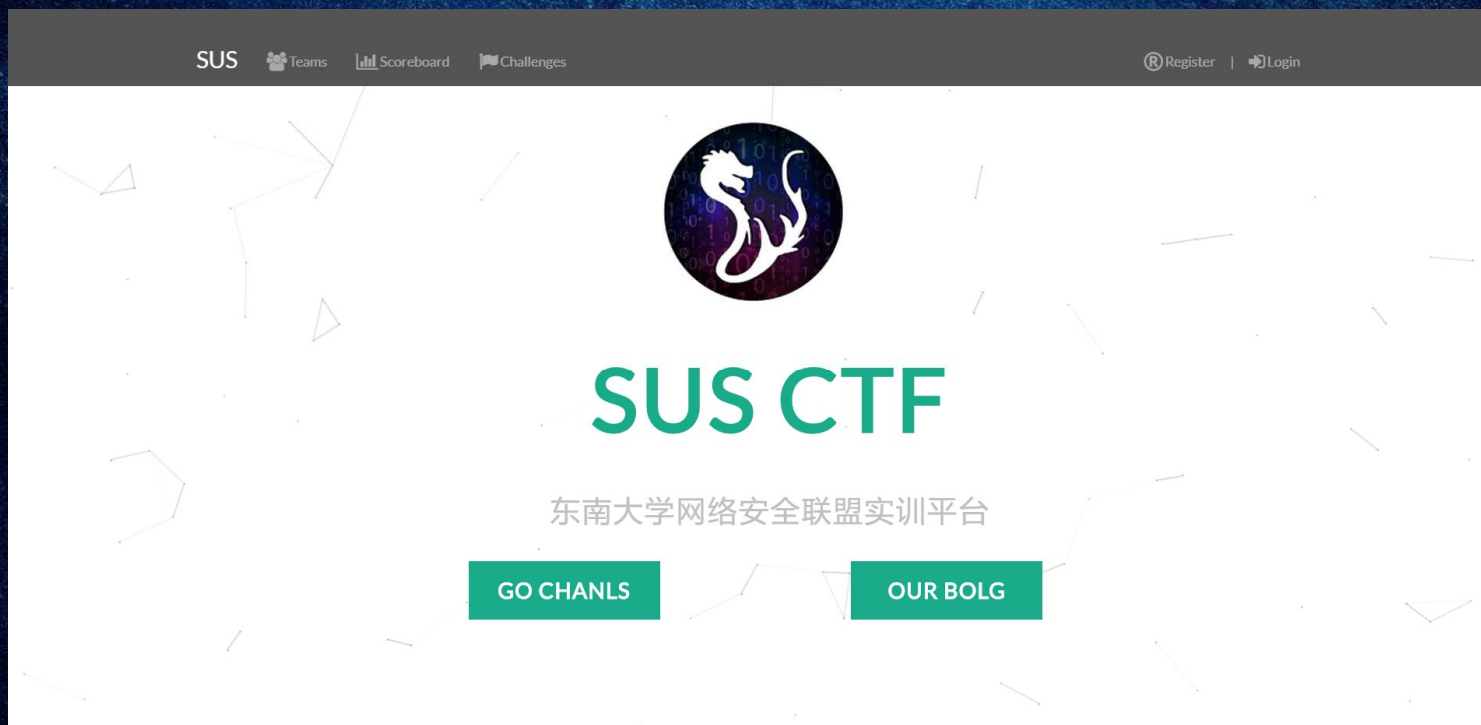
BXS Team

Part 1 社团简介



SUS Team

实训平台





社团战队Hydr4g0n(SUS)

- 第一届xctf总积分第十五名
- 2015ACTF第二名
- 第四届江苏省信息安全技能竞赛第四名
- 第五届江苏省信息安全技能竞赛第五名
- 全国高校网络安全运维挑战赛华东赛区二等奖
- 上海市全国大学生网络安全技能竞赛三等奖
- ISG-2017教育组三等奖

Part 1 社团简介



SUS Team

社团荣誉





Part 2

什么是网络安全

Part 2 什么是网络安全



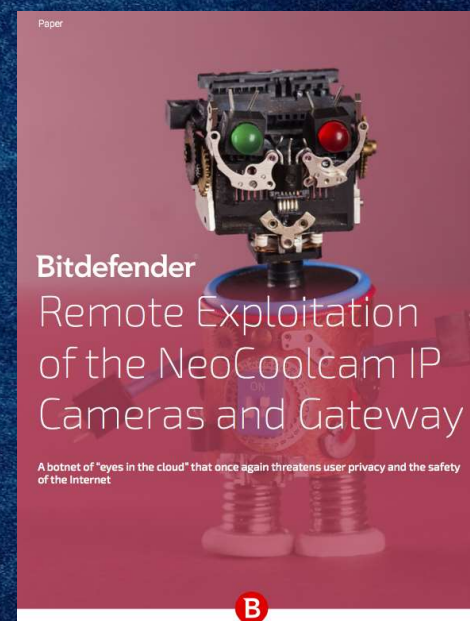
SUS Team





安全大事件

- 2017.3.7 Strust 漏洞
- CIA/NSA网络军火库泄露
- WananCry勒索病毒席卷全球
- 物联网Mirai僵尸网络
-





信息泄露 && 社会工程学

- 【小实验】照片发微信朋友圈真的会泄露位置吗？
- 个人信息泄露的危害到底离你有多远？
- 微信聊天记录定位物理地址
- 社工字典

Part 2 什么是网络安全



SUS Team

通信安全---无线安全

```
root@kali: ~  
File Edit View Search Terminal Help  
CH 7 ][ Elapsed: 1 min ][ 2016-07-14 07:06  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
78:A3:51:12:A6:A8 -80 30 2 0 1 54e WPA2 CCMP PSK LaFaLink-2.4G-12A6A8  
80:89:17:CC:F7:26 -82 34 0 0 1 54e WPA2 CCMP PSK TP-LINK_F726  
BSSID STATION PWR Rate Lost Frames Probe  
(not associated) 7C:1D:D9:A5:55:47 -92 0 - 1 0 4  
(not associated) 0C:91:60:81:89:AD -92 0 - 1 0 4  
78:A3:51:12:A6:A8 C4:8E:8F:61:18:DB -74 0 - 1 0 140 LaFaLink-2.4G-12A6A8
```


Part 2 什么是网络安全



SUS Team

通信安全---无线安全

```
jikefeng — -bash — 113x24
Q 1 handshake
Aircrack-ng 1.2 rc3

[00:00:00] 57 keys tested (3561.89 k/s)

KEY FOUND! [ 12344321 ]

Master Key      : 0E F4 DC CE 4A C6 8E E4 34 8A 22 79 5A 89 07 61
                  CD 58 01 D2 2D D7 60 5F 7A AC A8 93 C4 71 86 3D

Transient Key   : 85 2B C0 20 F7 CA 33 6D 7B FA 1E 27 F2 3D 52 C0
                  B7 AA F7 65 1C 56 B2 83 82 77 A9 DC 0D CC 39 FD
                  EA 79 5F 0B D8 AA CE C2 02 6A 45 BC A3 59 F7 6B
                  A5 CF 14 22 3C 4C 1F 1C 07 BF 95 7F E8 33 6E 4D

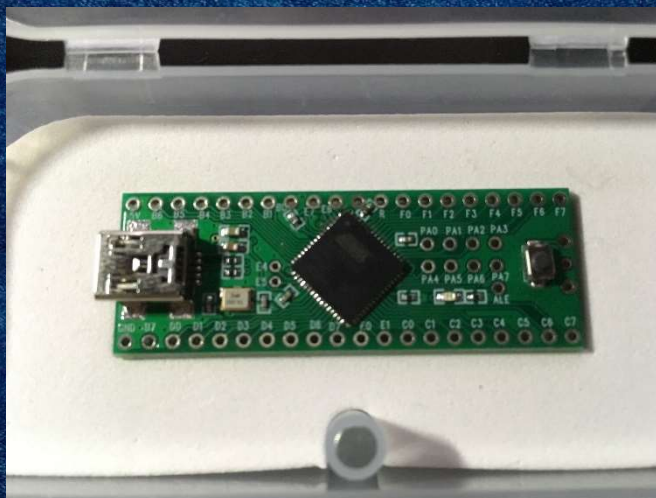
EAPOL HMAC     : 0B EC 57 B4 64 88 E1 B0 EB EA 10 3C D5 E2 5A 81
lifengfengdeMacBook-Pro:jikefeng lifengfeng$
```


Part 2 什么是网络安全



SUS Team

硬件安全





内网渗透

Currently scanning: 192.168.29.0/16 | Screen View: Unique Hosts

18 Captured ARP Req/Rep packets, from 5 hosts. Total size: 1080

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.23.1	00:50:56:c0:00:08	14	840	Unknown vendor
192.168.23.2	00:50:56:e3:97:3d	1	60	Unknown vendor
192.168.23.146	00:0c:29:5c:20:3c	1	60	Unknown vendor
192.168.23.147	00:0c:29:d0:35:cb	1	60	Unknown vendor
192.168.23.254	00:50:56:e7:cf:28	1	60	Unknown vendor

配合社会工程学 && arp欺骗



网站攻防

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.212 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.106 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.089 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.054/0.115/0.212/0.059 ms
www-data
```




漏洞利用

```
root in ~/Desktop/tmp λ ./pwn1.bin
welcome to XMAN!
what do you want to do?
1. introduce your self
2. get boy students infomation
3. get girl students infomation
4. Exit
1
1
your name is:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
hello, AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
!
[1] 28357 segmentation_fault ./pwn1.bin
```




病毒木马

```
[>] 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.█
```


Part 2 什么是网络安全



SUS Team

- 移动安全
- 逆向破解
- 加密解密
- 工控安全
-

Part 3

萌新赛

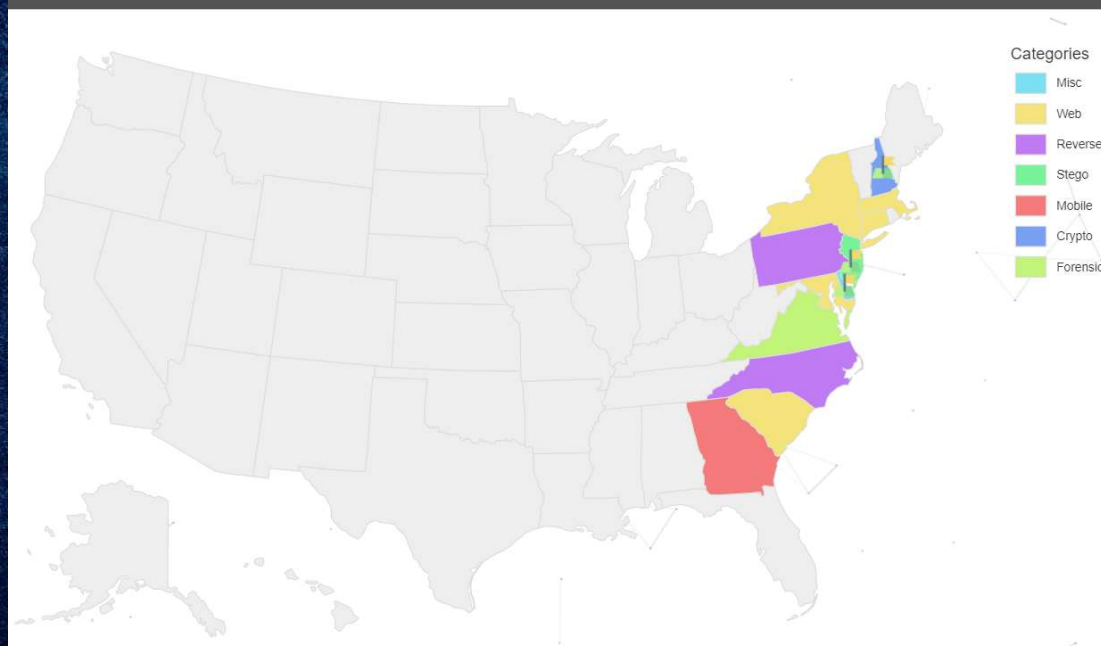
Part 3 萌新赛



SUS Team

<https://susers.github.io/wiki/>

Challenges



Part 4

如何踏上黑客之道(预)

Part 4 如何踏上黑客之道(预)

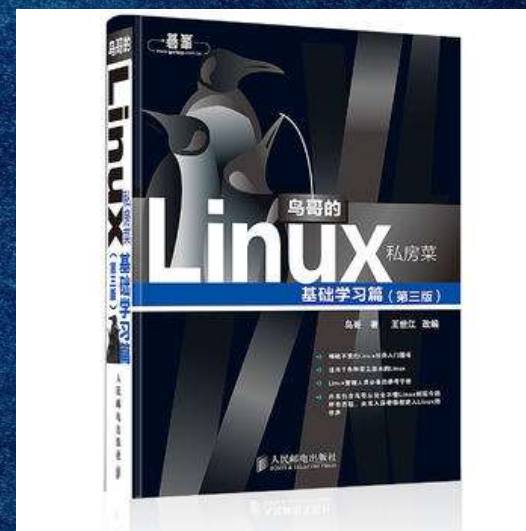


SUS Team

- 学会科学上网
- 学会Google

下次宣讲会前

- 虚拟机
- Linux
- <https://ctf-wiki.github.io/ctf-wiki/#/>
- 萌新赛





Thanks for Watching

QQ



Blog

