

CTF学习及团队建设浅谈

Author : Venenof7@Nu1L



目录

CONTENTS



1

CTF方向简介

2

高校学生如何从0学习

3

高校社团建设及管理浅谈

4

Nu1L战队的成长史

1.

CTF方向简介

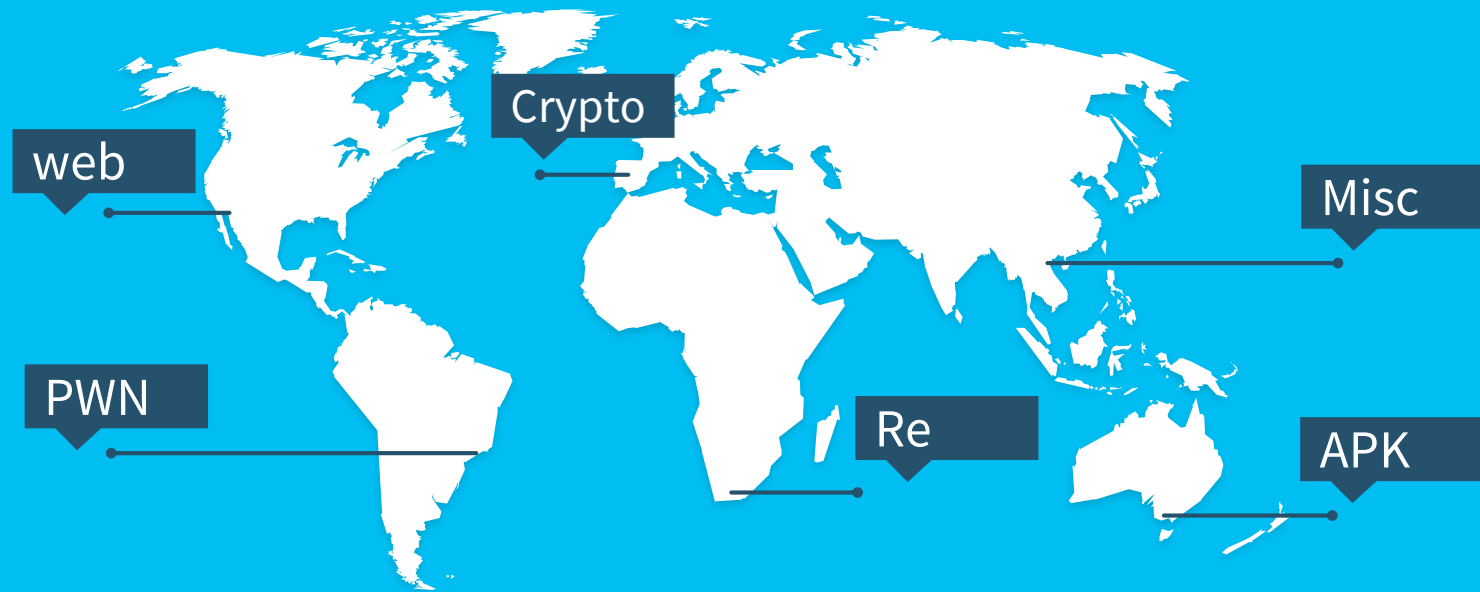
CTF?

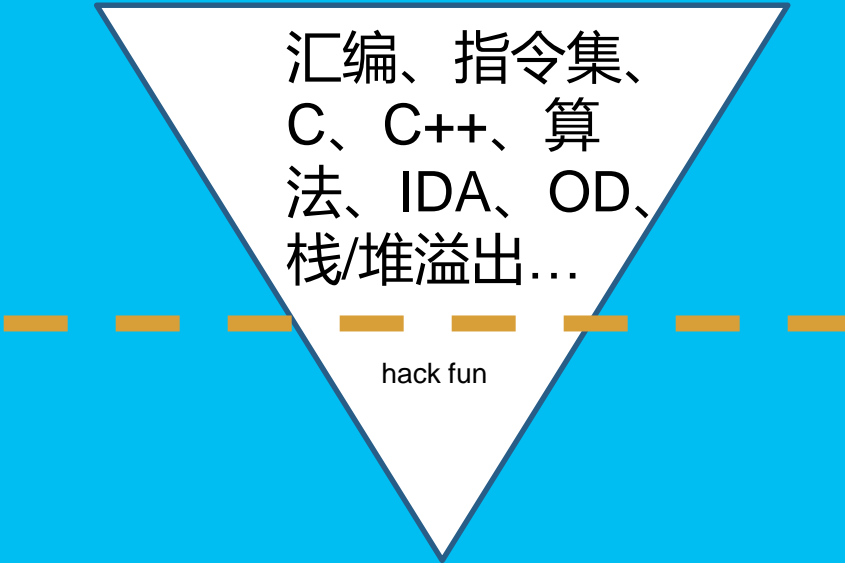
4

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有哪些分类?

5

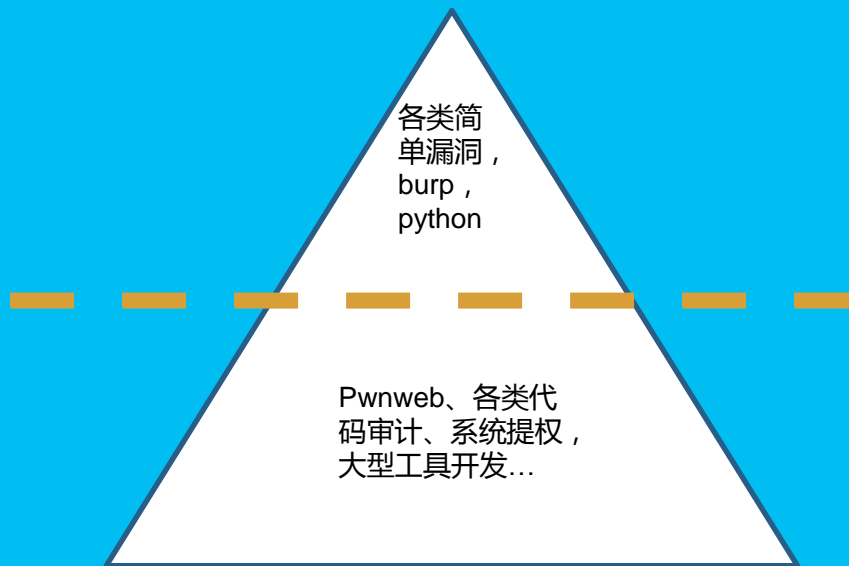




汇编、指令集、
C、C++、算
法、IDA、OD、
栈/堆溢出...

hack fun

WEB



WEB入门最简单

学二进制觉得WEB很简单

学RE的一定能学好二进制

2.

高校学生如何从0学习（以web为例）

>> 01 个人如何入门



■ CTF总是不会做怎么办



■ 为什么别人能秒题我却不能



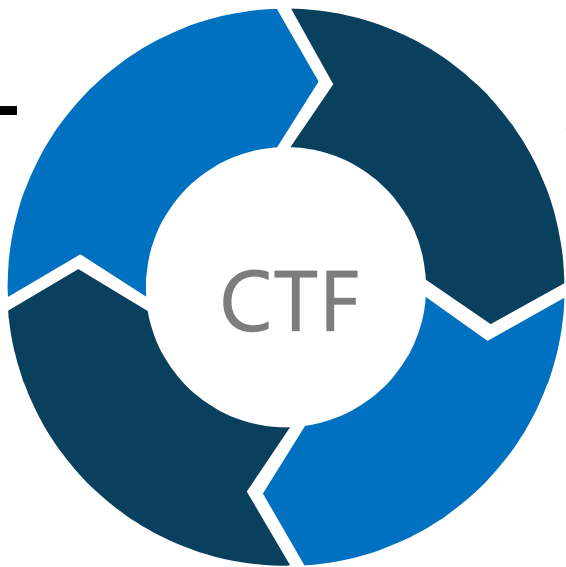
■ 高质量的CTF



■ 如何打好一场线上CTF

➤ 01 CTF总是不会做怎么办

不要把CTF当做一个必需品



对它要有亲切感而不是恐惧感

以赛促练，摸清套路

➤ 02 为什么别人能秒题我却不能

出题人角度：

1. 找点最近新出的漏洞吧
2. 我最近看了个paper，拿来出个题
3. 上次碰到一个实际案例，正好拿过来复现下XD

PS：一切以脑洞为原则的出题人都不是好出题人：)

➤ 02 为什么别人能秒题我却不能

做题人角度：

功夫下在平时
追踪新鲜漏洞

不要期望出题人的点你都遇到过

充足的耐心，仔细观察每一个点

高质量赛事

国际赛事：

defcon、HITCON、OCTF、RWCTF等...

国内赛事：

各类赛事（参与度好，但是质量参差不齐）

➤ 04 如何打好一场CTF

四点，逐一介绍：

一颗不放弃的心

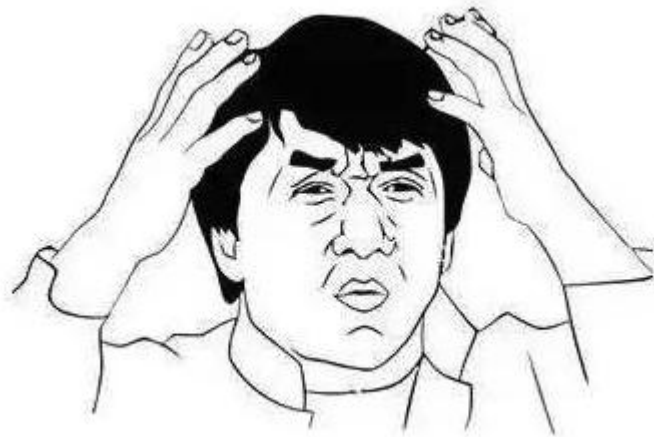
平常积累的一些trick

不要期望着出题人的出题点你都见过

仔细观察每一个点

➤ 04 一颗不放弃的心：

态度问题，不用多说，大家都懂。

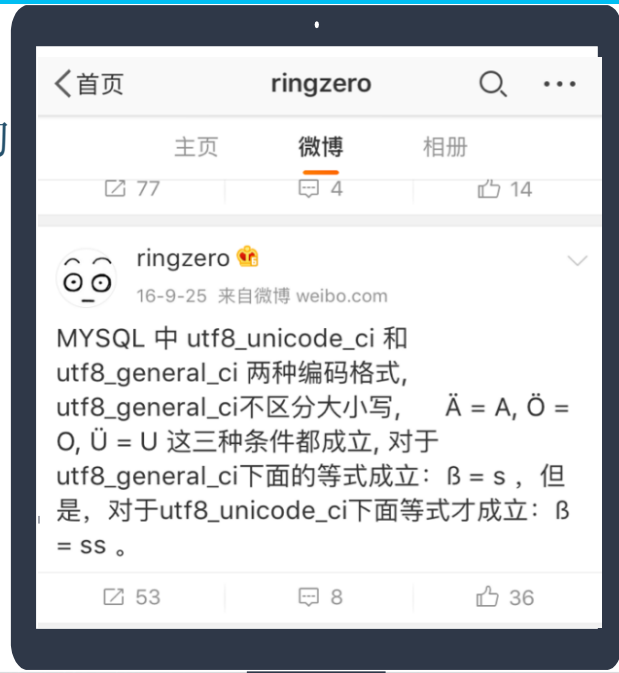


平常积累的一些trick

» 大佬weibo:

» 以HITCON2016为例，Orange的审计题为例，绕过方法就是在猪猪侠微博上提过的：

```
if ( $username == 'orange' || strpos($sql, 'orange') != false ) {  
    $this->__die("Orange is so shy. He do not want to see you.");  
}  
$obj = $this->__query($sql);  
if ( $obj != false && $obj->role == 'admin' ) {  
    $this->__die("Hi, Orange! Here is your flag: " . $FLAG);  
} else {  
    $this->__die("Admin only!");  
}
```



➤ 04 平常积累的一些trick

各类技术网站：

freebuf

360安全播报

Sec-news

先知

国外各类技术博客

Ctftime的wp（往往会有意外的学习经验）

大佬的blog：

- 1.ph-<https://www.leavesongs.com/>
 - 2.lemon-<http://www.cnblogs.com/iamstudy/>
 - 3.lr-<http://lorexxar.cn/>
 - 4.bendawang-<http://bendawang.site/>
 - 5.smile: <https://www.smi1e.top/>
 - 6.wupco- <http://www.wupco.cn/>
- etc...

善于学习他人思路，往往一个题目会有不同的解，借鉴学习提升功力

不要期望着出题人的出题点你都见过

Pwnhub-大物必须过 Writeup

写在最前

这回认真写一次wp，我会尽量写的完整一点，用狼人杀的话说就是把心路历程讲明白。主要两个目的，第一是给做题人一个参考，我在做这题的时候并不知道RPO是啥（看了别人的wp才知道），然而最终还是能做出来，我想这个过程还是值得新人借鉴的，也就是遇到一道新题应该怎么去入手，打CTF遇到自己没见过的知识点太多了，不能期待着撞知识点；第二其实更重要的是给出以后的出题人提一个醒，应该怎么出题。



具体可以看一下firesun的wp过程，自行扫描

仔细观察每一个点

- » 护网杯2019决赛为例
 - » 某thinkphp案例
 - » 没有0day的情况下
 - » 网上所有的exp都不可以
 - » 曲线救国：
 - Runtime目录会泄露session
 - 伪造登录后台getshell
 - 目录遍历的妙用

仔细观察每一个点

- » N1CTF Old Attack
 - » Cookie base64解码发现不同
 - » ECB-128, 伪造cookie获取权限

➤ 05 个人的一点经验

从15月接触信息安全一直到现在。

- 1-学到东西才是关键。
- 2-日常看的点，不要局限于仅仅看过，尽量去复现XD。
- 3-有的时候不是你不会，只是没去研究下去。

BCTF2017-firecms=>基本完全复现Uber-selfxss案例

- 4-多研究，以赛代练
- 5-扩大知识面（常见漏洞，学习开发，复现题目代码等）

➤ 05 个人的一点经验

如何学习WEB

- 1-前期书籍+刷题
- 2-巩固所学的各类基础漏洞知识
- 3-尝试利用PHP、Python这些入门层级低的语言去编写exp、工具、平台等
- 4-现实漏洞的复现（各类CVE、CMS漏洞等等）
- 5-从做题人尝试转变为出题人

➤ 05 个人的一点经验

Web选手如何去打AWD

AWD考察的是什么：

- 漏洞的审查能力
- 快速编写脚本的能力
- 权限维持的能力

WEB选手需要什么：

- 丰富的代码审计技巧
- 熟练运用python
- 一整套自己的权限维持流程

➤ 05 个人的一点经验

举例：中关村比赛

PHP题目：

```
grep "file_get_contents" -r *
```

>发现根目录下images文件存在任意文件读取

JAVA题目：

Tomcat弱口令

本身的war包

=>没你想的那么难其实

3.

高校社团建设及管理浅谈

04 社团需要什么

- 一个灵魂人物
- 团结、一致
- 学校、老师的支持

No.1

需要什么

No.2

- 定期的训练
- 不气馁，相信自己以及队友
- 总结分享

➤ 02 提高效率的方法

- ❑ 比赛过程中人员太多怎么办
- ❑ 不知道解题进度怎么办（想在宿舍）
- ❑ 不想翻墙

No.1

notion

No.2

- ❑ Notion解决你的一切烦恼
- ❑ 高度饱和的ui
- ❑ 各种畅快的功能
- ❑ 不用翻墙



CodeBlue

Click on a card to view details.

Click on 'Board by Status' to toggle between views.

比赛网址: <https://bullseye.ctf.codeblue.jp/>



 Board by Status ▾

Properties Group by Status Filter Sort 🔍 Search ... New ▾

 No Status 5 ... +

In Progress 3 ... +

Cancelled 1 ... +

+ Add a Group



flute

Misc Reverse



Wire Hetimarl

Pwn



Key_check

Pwn



playground



InvisibleMemo

Pwn

In Progress

Need a leak



Snippet

Web

 Smi1e Smi1e  Q 7

In Progress



火狐 -Higitsune-

Pwn

Cancelled

+ New

03 人太多怎么办

- 不好管理
- 摸鱼选手
- 利益纷争

No.1

人太多？

No.2

- 社长的责任
- 定期筛选
- 老选手的传承

- 前期定期培训
- 选拔赛
 - 特长
 - 全面

No.1

标准

No.2

- 面试环节
 - 乐于分享
 - 可以傲但人品要好
 - 不是一个利益选手

其实最重要的还是社长

压力/责任

不一定技术能力最强

但一定要有为大家着想的心

4.

Nu1L战队的成长史

➤ 01 关于Nu1L

- ❑ 15年10月成立
- ❑ 国内顶尖CTF战队
- ❑ 多企业/高校联合

No.1

Nu1L

No.2

- ❑ 征战于国内外各类CTF赛事
- ❑ 10月单月获得全国3个冠军
1个亚军
 - ❑ 护网杯2019冠军
 - ❑ 中关村某比赛冠军
 - ❑ 字节跳动CTF亚军
 - ❑ 第五届XCTF国际联赛总决赛冠军

- ❑ 15年10月成立
- ❑ 初始赛果比较好
- ❑ 尝试扩大知名度

No.1

Nu1L

No.2

- ❑ 内部选手引荐
 - ❑ 南邮
 - ❑ 电科大
- ❑ 侧面迂回招人
- ❑ 官网
 - ❑ <https://nu1l-ctf.com>

- 主流安全公司内推
- 比赛差旅报销
- 每年的聚餐

No.1

战队福利

- 各类赚外快机会
 - 培训
 - 出题
 - 安服

No.2

5.

我们在做的一些事

《从0到1 CTFer的成长之路》

- » 马上发行
- » 配套的在线平台
- » 电子工业出版社



“巅峰极客”线下赛场景



为了更好地分享，我们建设了小密圈

» 完全免费

 知识星球



星主: Nu1L Team

CTFWP@Nu1L



长按扫码预览社群内容
和星主关系更近一步

N1CTF

- » 源于2018
- » 2019年CTFTIME权重满分，获得好评

Organized CTF events

Name	Weight
N1CTF 2019	36.00
N1CTF 2018	24.38

➤ 开源题目以及平台

» <https://github.com/Nu1LCTF>

The screenshot shows the GitHub repository page for Nu1LCTF. The repository is owned by Nu1LCTF and is located at <https://github.com/Nu1LCTF>. The page displays a list of repositories, including Nu1L-Team-Page, n1ctf-2019, nu1html, and n1ctf-2018. The n1ctf-2018 repository is highlighted as the official repository containing files related to N1CTF 2018. The page also features a sidebar with top languages (JavaScript, C++, Python) and a list of people (20) who have contributed to the repository.

github.com/Nu1LCTF

Search or jump to... Pull requests Issues Marketplace Explore

Nu1LCTF
<https://nu1l-ctf.com>

Repositories Packages People Teams Projects Settings

Find a repository... Type: All Language: All Customize pins New

Nu1L-Team-Page
JavaScript 0 stars 0 forks Updated 5 days ago

n1ctf-2019
Python MIT 7 stars 0 forks Updated 24 days ago

nu1html
JavaScript 0 stars 0 forks Updated on 17 Aug

n1ctf-2018
Official repository containing files related to N1CTF 2018.
ctf writeup n1ctf

Top languages
JavaScript C++ Python

People 20
Invite someone



THANKS!

提问时间！

hack fun😊