CTF课程

原创

m0_47528454 已于 2022-01-18 21:00:09 修改 2027 收藏 1
文章标签： 安全
于 2021-10-22 10:53:53 首次发布

ctf:（capture the flag）夺旗赛，是网络安全技术人员之间进行技术竞赛的一种比赛形式，题目类型包括但不限于WEB,MISC（杂项）,Crypto（密码学），PWN,Android，Reverse（逆向）

传统CTF：web渗透，密码学，流量分析，信息隐藏，二进制逆向分析，安卓逆向分析，溢出漏洞分析

团队攻防赛（awd））：web，pwn（堆溢出，栈溢出）

运维赛：模拟漏洞的业务场景，进行黑盒或白盒测试，进行修补漏洞

应急响应赛：

破解大赛：针对windows操作系统，应用程序，vmware虚拟化软件等进行破解

智能家居：

机器人对抗：

web：sql注入，文件上传，文件包含，命令执行，任意文件下载或读取

密码学：常见的有凯撒密码，栅栏密码，base64，unicode，js编码等

团队攻防(AWD)：web代码审计，漏洞挖掘，楼顶修补，漏洞利用，攻击技巧（获取权限，权限维持，不死马），防守技巧（流量分析，攻击溯源，文件监控），以及AWD攻防框架的使用

web安全：底层协议，常见漏洞，编程语言，编写poc-->（漏洞复现脚本）

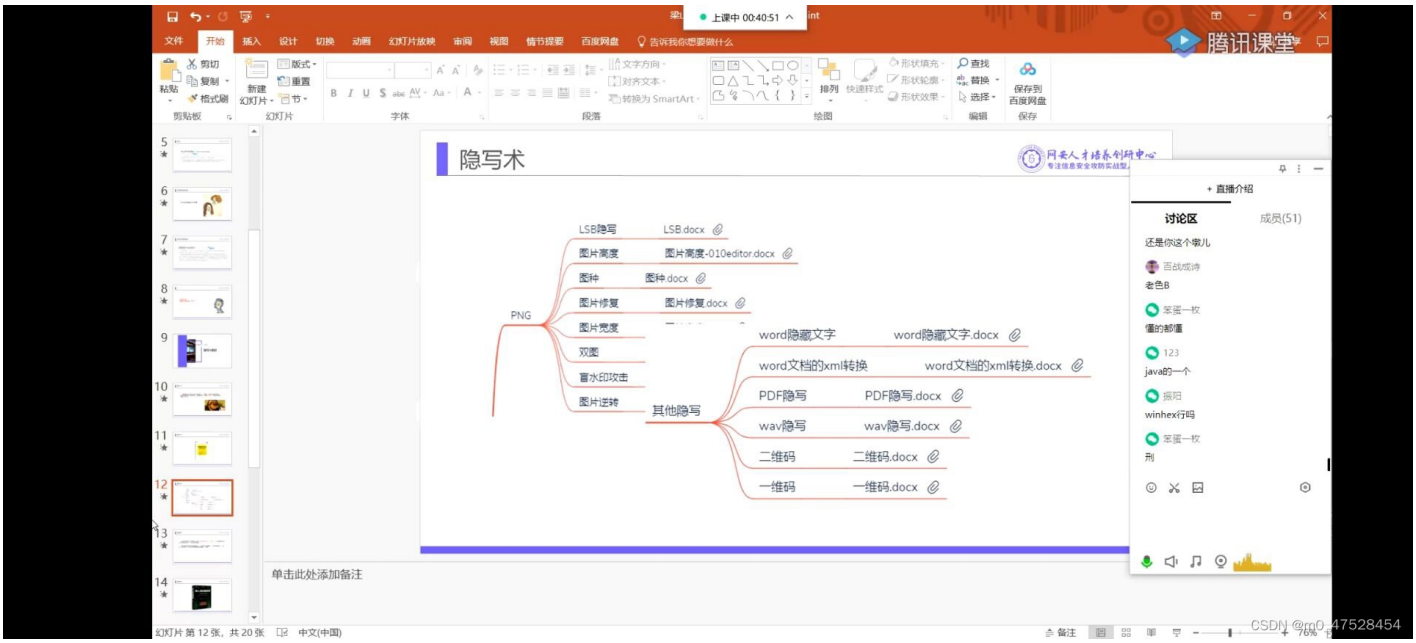
xss漏洞：javascript，传视频（内容安全策略）

SQL注入：报错注入sqli—labs　反序列化RCE

推荐网站：pwnhub，code—breaking，安全客，Freebuf，先知，云演

代码审计

信息隐写：起源于密写术，被用于恶意软件或间谍攻击，也被用于泄密中，泄密人员把信息隐藏到图片，音频等文件中传出

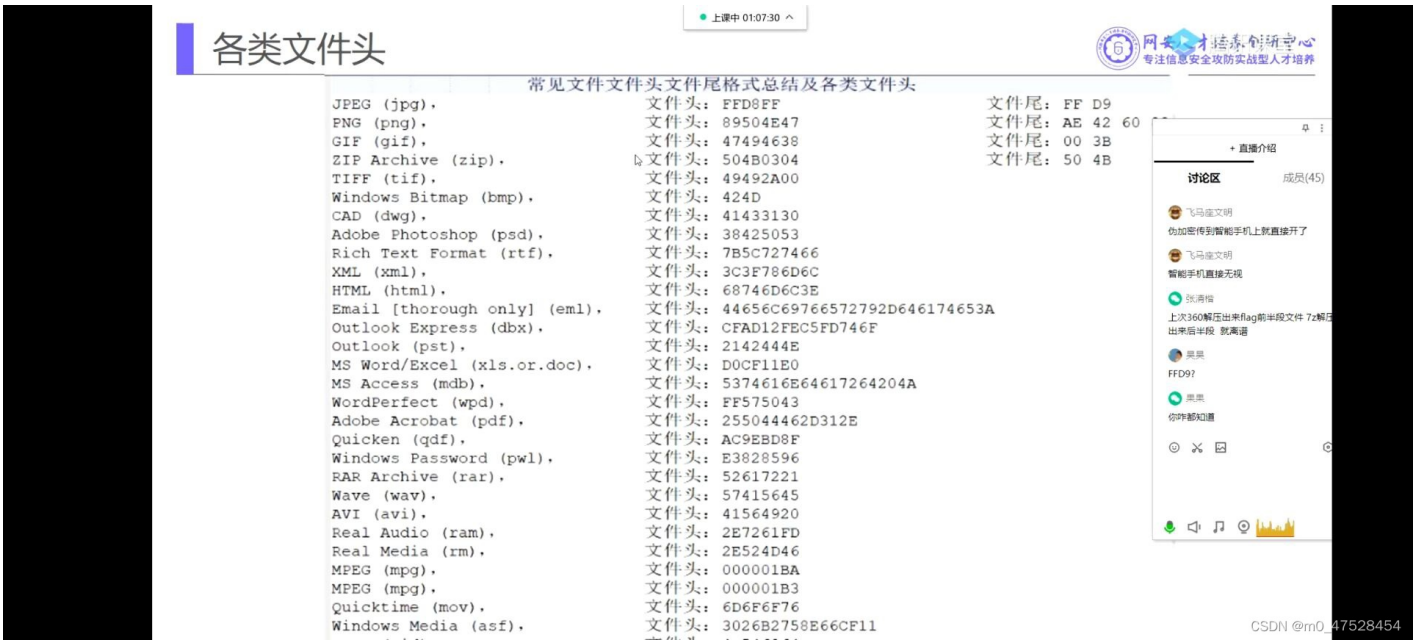


winhex：德国，做取证，数据恢复，磁盘编辑器，

binwalk：binwalk —e 名字

foremost：foremost 名字

010：



信息隐藏技术:隐藏是为了信息不被发现，密码学是为了信息不让破译

隐写术的举例说明：隐形墨水，缩影隐写术，水印

ctf中常见图片类隐写，比如PNG,JPG,GIF,BMP,

隐写术的出题思路：1.破坏文件结构

2.隐去文件后缀

3.结合编码

4.不同的承载文件类型

5.结合二维码

6.结合隐写算法

7.结合搜索引擎

8.和其他MSIC类题目相结合

常见文件格式的分析：ctrl+f查找

1.图片类：png，其文件头位置总是由位固定的字节来描述的 89 50 4E 47 0D 0A 1A 0A

PNG文件结构主要由数据块组成，最少包含4个数据块

PNG标识符---PNG数据块（HDR）--PNG数据块（其他类型数据块）...PNG结尾数据块（IEDN）

JPEG属于有损压缩格式，相对于原始图像，能够得到1/8的压缩比通常能够得到1/8的压缩比,JPEG图片也有相对应的图片头和尾部，以及定义图片高度和宽度的数据块并且JPG图片在有所得时候一般采用DCT变换，有学者在研究DCT域信息隐藏的一些算法。

图像互换格式GIF图片：位图图图形文件格式，以8位色（即256种颜色）重现真彩色的图像，实际上是一种压缩文档，采用LZW压缩算法进行编码，有效地减少了图像文件在网络上传输的时间，是目前广泛应用于网络传输的图像格式之一。

BMP图片：·又称Bitmap（位图）或是DIB(设别无关位图），是windows中广泛使用的图像格式，是不做任何变换的保存图像像素域的数据，是取得原始数据的来源

BMP图片格式组成部分：BMP文件头（14 bytes）+位图信息头（40 bytes）+调色板（由颜色索引数决定）+位图数据（由图像尺寸决定），比如：钱2bytes（0,1）是‘BM’(Windows）

改变动图速率工具（分离动图）：GifSplitter,

隐写总结(步骤）：

1.打开图片查看

2.右键属性

3.用0101editor打开查看文件头，数据块等

4.尝试修改图片宽，高度

5.工具打开（分离）--gif,jpg,png,zip...

（所给图片相同）stegsolve 可以查看图片的通道，xor异或算法

QR Research：二维码扫描工具

第二节课：**压缩包隐写**

是指在ctf比赛中以压缩包为载体文件，或者和压缩包相关的题目类型，压缩包本身不具备隐藏信息的能力，但可以和其他隐写的相关技术相结合，再加上压缩包特有的属性形成这类压缩包隐写

出题方向：

1.图种类题目

2.与压缩包加密破解相关的题目类型

（1）和密码学相结合，需要我们破解密码

（2）爆破密码，字典攻击，掩码攻击

（3）明文攻击

（4）CRC32爆破

文件格式：504B0304:头文件标记　　14 00：解压文件所需的pkware版本

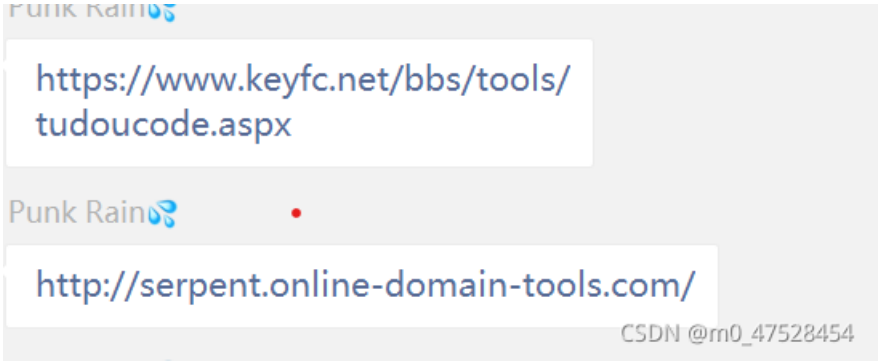
00 00：全局方式位标记（有无加密）　08　00：压缩方式

50 4B 01 02：目录文件文件头标记（0x02014b50）　3F 00:压缩使用的pkware版本

14 00：解压文件所需pkware版本　00 00：全局方位式标记（有无加密）　08 00：压缩方式

加密方式：brainfuck 所用工具Brainfuck

总结：图片隐写的步骤，使用到的工具：



文本隐写：

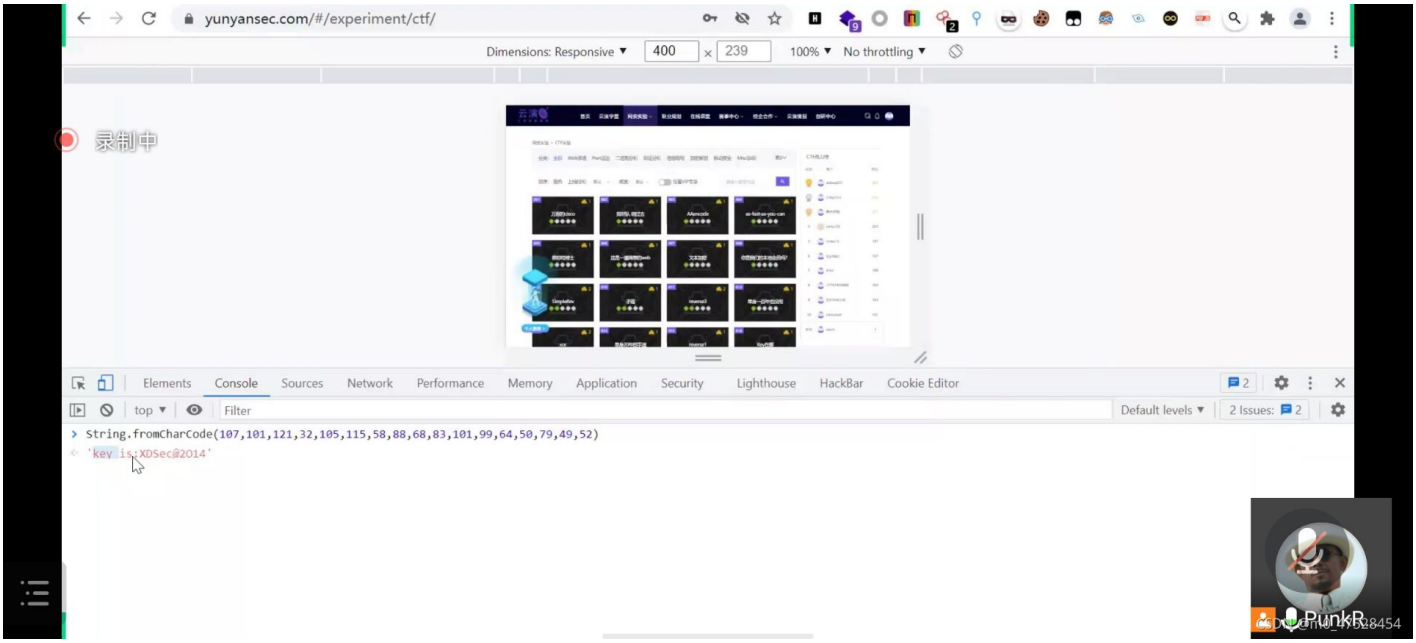
1.word隐写：包括批注，个人信息，水印，不可见内容，

excel隐写：（1）颜色，通过欺骗我们肉眼所见得颜色来隐写信息，包括单元格颜色，字体颜色等

（2）xml转换 （使用010editor）

PDF：工具wbstego4open，可以把文件隐写到BMP,TXT,HTM和PDF文件中，

解密ASCII码：

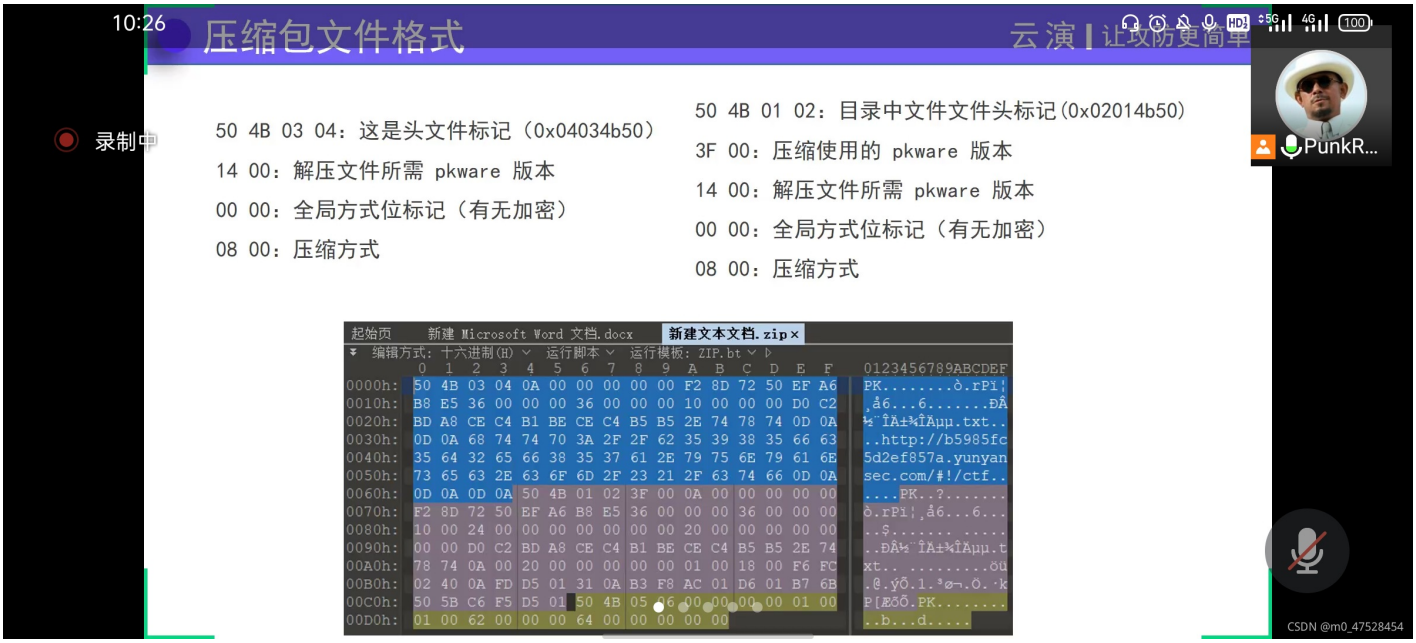


课前回顾：

隐写：文本类（隐藏文字），音频类，压缩包类，

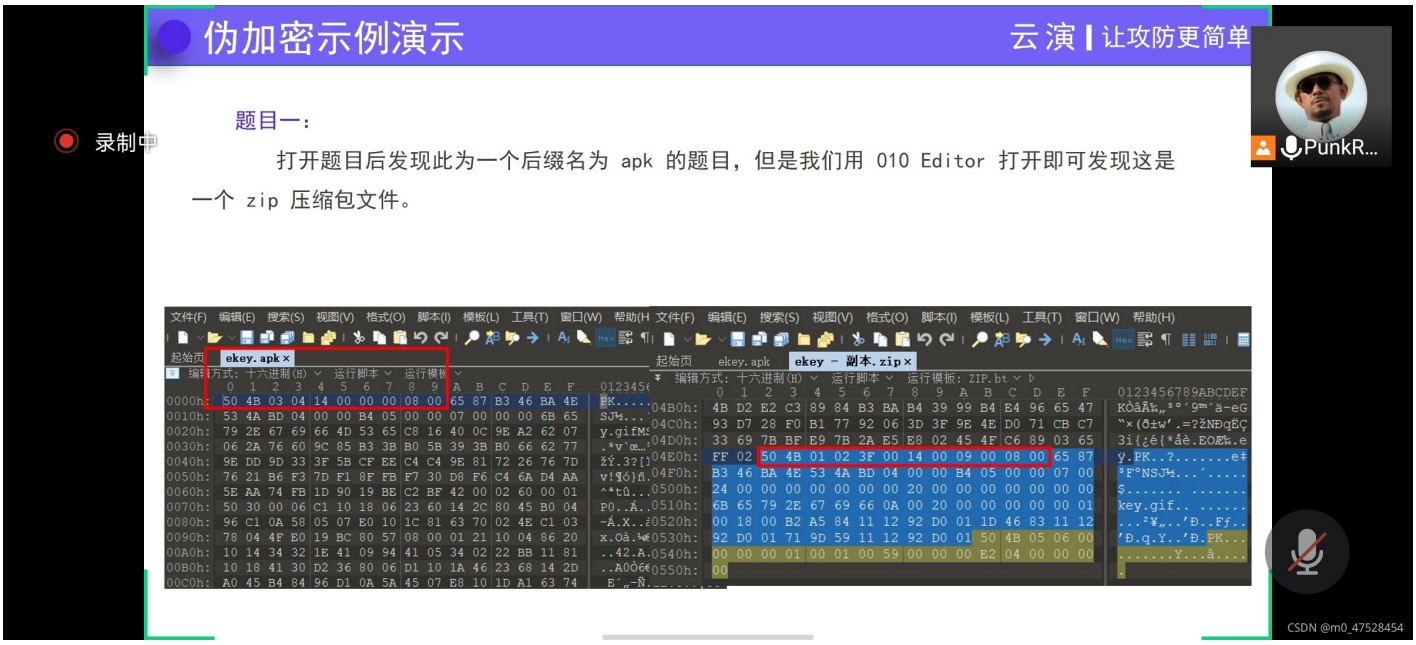
图片类：与其他类型相结合

第三节课：压缩包伪加密

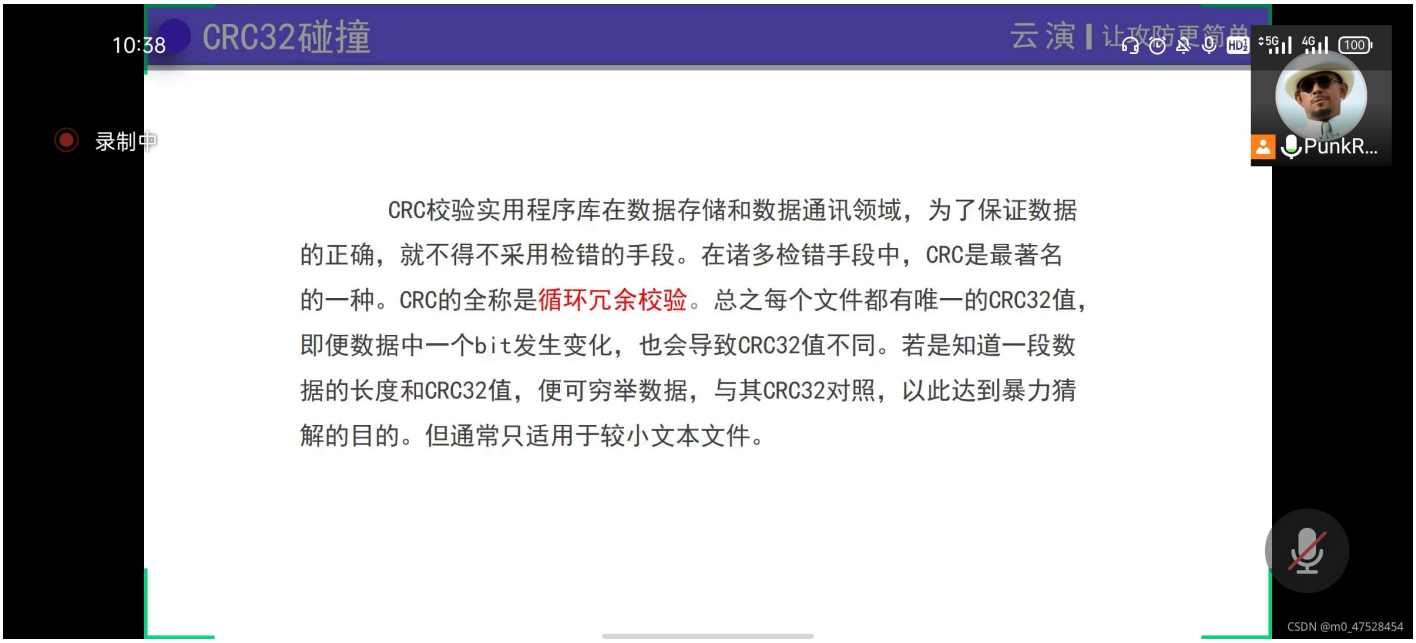

10:26
压缩包文件格式
云演 | 让攻防更简单
录制中
50 4B 03 04：这是头文件标记（0x04034b50）
14 00：解压文件所需 pkware 版本
00 00：全局方式位标记（有无加密）
08 00：压缩方式
50 4B 01 02：目录中文件文件头标记(0x02014b50)
3F 00：压缩使用的 pkware 版本
14 00：解压文件所需 pkware 版本
00 00：全局方式位标记（有无加密）
08 00：压缩方式
起始页 新建 Microsoft Word 文档.docx 新建文本文档.zip
编辑方式：十六进制(H) 运行脚本 运行模板：ZIP.bt
0000h: 50 4B 03 04 0A 00 00 00 00 00 F2 8D 72 50 EF A6 PK.....ò.rPï¦
0010h: B8 E5 36 00 00 00 36 00 00 00 10 00 00 00 D0 C2 ¸å6...6.....ÐÂ
0020h: BD A8 CE C4 B1 BE CE C4 B5 B5 2E 74 78 74 0D 0A ½¨ÎÄ±¾ÎÄµµ.txt..
0030h: 0D 0A 68 74 74 70 3A 2F 2F 62 35 39 38 35 66 63 ..http://b5985fc
0040h: 35 64 32 65 66 38 35 37 61 2E 79 75 6E 79 61 6E 5d2ef857a.yunyan
0050h: 73 65 63 2E 63 6F 6D 2F 23 21 2F 63 74 66 0D 0A sec.com/#!/ctf..
0060h: 0D 0A 0D 0A 50 4B 01 02 3F 00 0A 00 00 00 00 00 ....PK..?.....
0070h: F2 8D 72 50 EF A6 B8 E5 36 00 00 00 36 00 00 00 ò.rPï¦¸å6...6...
0080h: 10 00 24 00 00 00 00 00 00 00 20 00 00 00 00 00 ..$..... .....
0090h: 00 00 D0 C2 BD A8 CE C4 B1 BE CE C4 B5 B5 2E 74 ..ÐÂ½¨ÎÄ±¾ÎÄµµ.t
00A0h: 78 74 0A 00 20 00 00 00 00 00 01 00 18 00 F6 FC xt.. ....öü
00B0h: 02 40 0A FD D5 01 31 0A B3 F8 AC 01 D6 01 B7 6B .@.ýÕ.1.³ø¬.Ö.·k
00C0h: 50 5B C6 F5 D5 01 50 4B 05 06 00 00 00 00 01 00 P[ÆõÕ.PK........
00D0h: 01 00 62 00 00 00 64 00 00 00 00 00 ..b...d.....
PunkR...
CSDN @m0_47528454


10:26
伪加密原理
云演 | 让攻防更简单
录制中
无加密
50 4B 03 04 14 00 00 00 08 00
50 4B 01 02 14 00 00 00 08 00
伪加密：
50 4B 03 04 14 00 00 00 08 00
50 4B 01 02 14 00 09 00 08 00
无加密
50 4B 03 04 14 00 02 00 08 00
50 4B 01 02 14 00 02 00 08 00
加密：
50 4B 03 04 14 00 01 00 08 00
50 4B 01 02 14 00 01 00 08 00
根据左图，我们来看下下图中是否为真加密呢？
文件头：
50 4B 03 04 14 00 00 00
文件内容头
50 4B 01 02 14 00 14 00 09 00
起始页 1.jpg 1.zip
编辑方式：十六进制(H) 运行脚本 运行模板：ZIP.bt
0000h: 50 4B 03 04 14 00 00 00 00 00 22 71 88 4E 86 A6 PK......"q^N†¦
0010h: 10 36 05 00 00 00 05 00 00 00 05 00 00 00 31 2E .6..............1.
0020h: 74 78 74 68 65 6C 6C 6F 50 4B 01 02 14 00 14 00 txthelloPK.....
0030h: 09 00 00 00 22 71 88 4E 86 A6 10 36 05 00 00 00 ...."q^N†¦.6....
0040h: 05 00 00 00 05 00 24 00 00 00 00 00 00 00 20 00 ......$....... .
0050h: 00 00 00 00 00 00 31 2E 74 78 74 0A 00 20 00 00 ......1.txt.. ..
0060h: 00 00 00 01 00 18 00 85 89 C0 90 D1 ED D4 01 85 ....…‰À.Ñíô.…
0070h: 89 C0 90 D1 ED D4 01 4E 30 E0 8C D1 ED D4 01 50 ‰À.Ñíô.N0à.Ñíô.P
0080h: 4B 05 06 00 00 00 00 01 00 01 00 57 00 00 00 28 K..........W...(
0090h: 00 00 00 00 00 .....
PunkR...
CSDN @m0_47528454

（改后缀为.zip用360压缩或7z解压）



CRC:线性结构



流量分析：CTF题型主要为流量包修复，web流量包分析，usb流量包分析和其他流量包分析

日志分析：

方法：1.特征字符分析：：根据攻击者利用的漏洞的特征，进行判断攻击者使用的是哪一种攻击，常见的类型：sql注入，xss跨站脚本攻击，恶意文件上传，一句话木马连接等

2.访问频率分析：通过查看攻击者访问的频率来判断攻击者使用的是哪一种攻击，常见的类型：SQL盲注，敏感目录爆破，账号爆破，web扫描

特征字符分析：

内存&磁盘取证：

密码学：

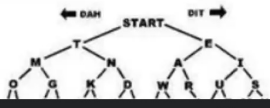
10:39

腾讯会议
01:05:18
离开

录制中

密码学根据其研究的范畴可分为密码编码学和密码分析（破解）学。密码编码学和密码分析学是相互对立、相互促进发展的。

密码编码学是研究密码体制的设计、对信息进行编码表示、实现信息隐藏的一门科学。密码分析学，是研究如何破解被加密信息的一门科学。



PunkR...

解除静音　开启视频　共享屏幕　成员(34)　更多

录制中

解密原理与方法

云演 | 让攻防更简单

在计算机领域，密码加密主要用于两方面：一是登录口令；二是文件加密。密码破解要认真分析检材的加密类型和算法，这样才能有的放矢进行解密工作。通常情况下，一个密码可能会包含如下符号：26个小写字母、26个大写字母、10个数字和33个其他字符，用户可以使用这95个字符的任意组合作为密码。

PunkR...

录制中

密码破解的基础理论

云演 | 让攻防更简单

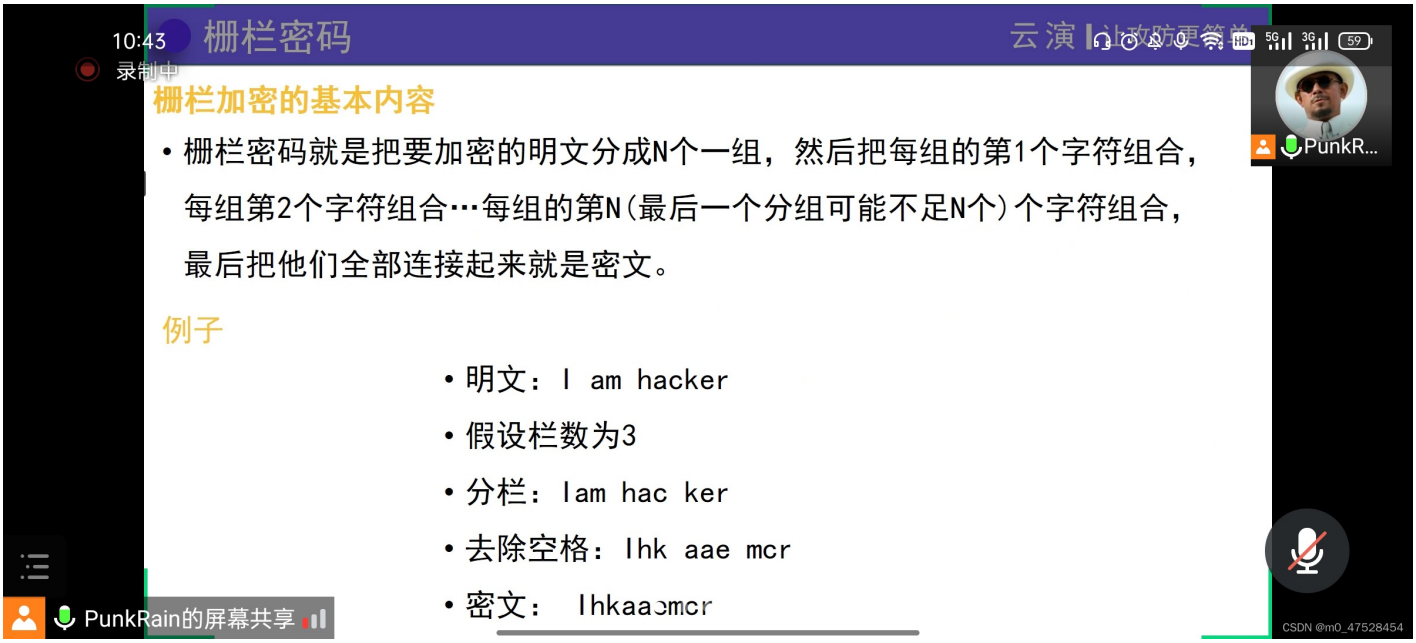
目前计算机中通用的加密算法有DES、RSA、MD5、SHA1、AES等，这些加密算法都是公开的标准，甚至连密钥也公开。一方面，互联网的本质是为了资源共享，因此标准是要统一，方便数据交换。另一方面，由于这些加密算法很强壮，按当时的技术环境，即使公开发布也不会对数据的安全性产生太大影响。

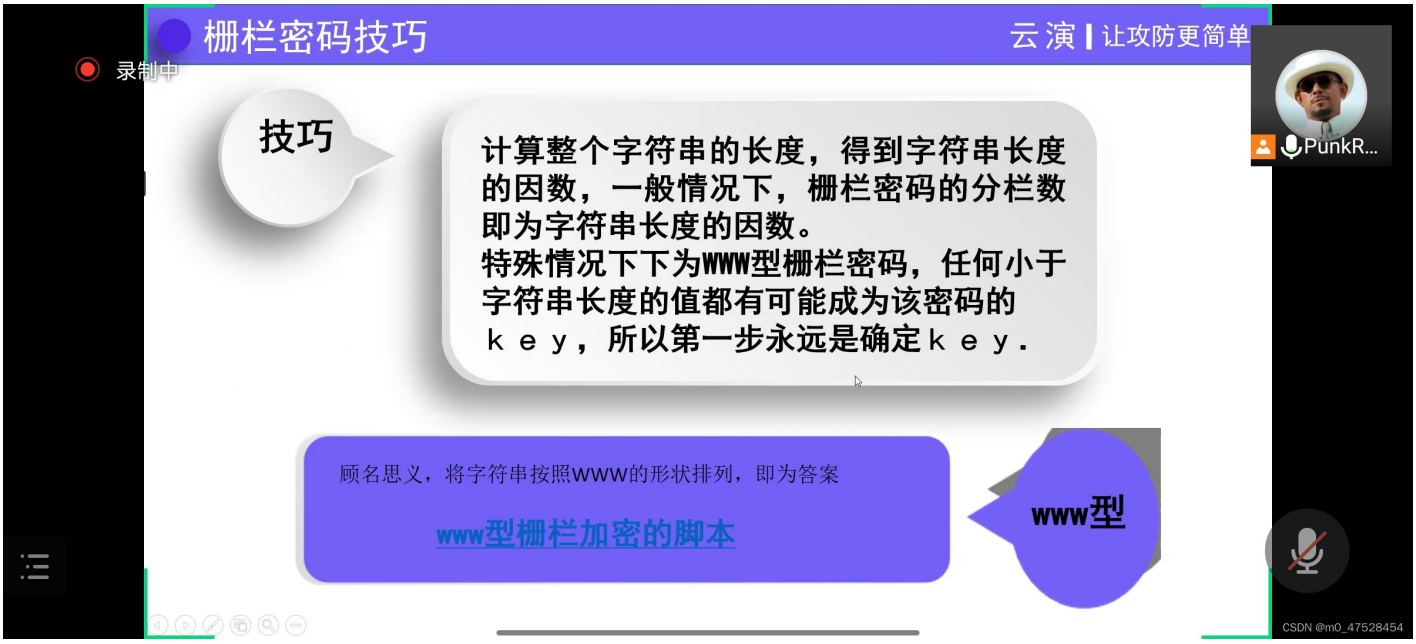
PunkR...

密码编码学：是研究密码体制的设计，对信息进行编码表示，实现信息隐藏的一门科学

密码分析（破解）学：研究如何破解被加密信息的一门科学

栅栏加密的基本内容：





工具：ctfcrak

11:27 录制中

培根密码

云演 | 让攻防更简单

PunkR...

培根密码(Baconian Cipher)是一种替换密码，每个明文字母被一个由5字符组成的序列替换。

原理：最初的加密方式就是由‘A’和‘B’组成序列替换明文，比如字母‘D’替换成“aaabb”。

CSDN @m0_47528454

11:16 录制中

凯撒密码

云演 | 让攻防更简单

PunkR...

其他的解密技巧：词频分析

在一些CTF中，借助字符统计
其对应的明文字符是e。

词频分析网站

```
strings = open('flag.txt').read()

result = {}
for i in alpha:
    counts = strings.count(i)
    i = '{0}'.format(i)
    result[i] = counts

res = sorted(result.items(),key=lambda item:item[1
for data in res:
    print(data)

for i in res:
    flag = str(i[0])
```

CSDN @m0_47528454

录制中

凯撒密码

云演 | 让攻防更简单

PunkR...

凯撒密码的替换方法是通过排列明文和密文字母表，密文字母表示通过将明文字母表向左或向右移动一个固定数目的位置。例如，当偏移量是左移3的时候（解密时的密钥就是3）：

明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ ；
密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC。

使用时，加密者查找明文字母表中需要加密的消息中的每一个字母所在位置，并且写下密文字母表中对应的字母。需要解密的人则根据事先已知的密钥反过来操作，得到原来的明文。例如：

明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG ；
密文：WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ。

恺撒密码的加密、解密方法还能够通过同余的数学方法进行计算。首先将字母用数字代替，A=0，B=1，...，Z=25。此时偏移量为n的加密方法即为：

$$E_n(x) = (x + n) \mod 26.$$

解密就是：

$$D_n(x) = (x - n) \mod 26.$$

CSDN @m0_47528454

11:07
录制中

Base编码

云演 | 让攻防更简单

PunkR...

Base编码的常见种类

- base16:16进制（包含数字0-9，大写字母A-F）
- base32:在base16的基础上增添了大写字母G-Z
- base64:在base32的基础上增加小写字母a-z

- 注意：当编码位数不足时，会使用“=”填充

PunkRain的屏幕共享

录制中

Base编码

云演 | 让攻防更简单

PunkR...

- base58：将base64的编码除去可能产生歧义的字符，例如数字0和大写字母O，大写字母I和小写字母L，以及影响双击选择的字符/和+，一共是58个字符，由于不是2的整数次幂，所以采用辗转相除法进行转换
- 将数字不断对58取余，直到商为0，将每一步的余数都查表（base64除去上面的歧义字符之后的表），如果待转化的数字前面有0，直接附加编码1来代表，有多少个就加多少个（在编码表中1代表0）解码时需要将长度传入
- base36：包含0~9的数字，加上所有26个字母，不区分大小写，不包含任何标点，所有的字母要不全大写，要不全小写
- base62:26个字母的大小写再加上0-9，一共62个字符.base62 编码在短地址服务中用的比较多
- Base91、base92、base85

录制中

云演 | 让攻防更简单

PunkR...

字母

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
A	.-	B	-...	C	-.-.	D	-..
E	.	F	..-.	G	--.	H	....
I	..	J	.---	K	-.-	L	.-..
M	--	N	-.	O	---	P	.--.
Q	--.-	R	.-.	S	...	T	-
U	..-	V	...-	W	.--	X	-..-
Y	-.--	Z	--..				

数字

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
0	-----	1	.----	2	..---	3	...--
4	....-	5	.....	6	-....	7	--...
8	---..	9	----.				

标点符号

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
.	.-.-.-	:	---...	,	--..--	;	-.-.-.
?	..--..	=	-...-	'	.----.	/	-..-.
!	-.-.--	-	-....-	_	..--.-	"	.-..-.
(	-.--.	)	-.--.-	$	...-..-	&	....

是由美国的摩尔斯在
码（Morse code）。
促的点信号“ . ”，
读“答 —”（Da）。

PunkRain的屏幕共享

CSDN @m0_47528454

11:09

录制中

Base编码

云演 | 让攻防更简单

PunkR...

Base64加密：

- string=“abc”
- 每个字母的ASCII值为：97 98 99
- 二进制为：1100001 1100010 1100011
- 011000 010110 001001 100011
- 转成10进制：24 22 9 35
- 加密结果为：YWJj

Base64加密表：

A	0	Q	16	g	32	w	48
B	1	R	17	h	33	x	49
C	2	S	18	i	34	y	50
D	3	T	19	j	35	z	51
E	4	U	20	k	36	0	52
F	5	V	21	l	37	1	53
G	6	W	22	m	38	2	54
H	7	X	23	n	39	3	55
I	8	Y	24	o	40	4	56
J	9	Z	25	p	41	5	57
K	10	a	26	q	42	6	58
L	11	b	27	r	43	7	59
M	12	c	28	s	44	8	60
N	13	d	29	t	45	9	61
O	14	e	30	u	46	+	62
P	15	f	31	v	47	/	63

CSDN @m0_47528454

11:05
录制中

列位移密码(Columnar Transposition Cipher)

列移位密码是一种比较简单，易于实现的换位密码，通过一个简单的规则将明文打乱混合成密文

例子：
明文 The quick brown fox jumps over the lazy dog
密钥 how are u

填入5行7列表(事先约定填充的行列数，如果明文不能填充完表格可以约定使用某个字母进行填充)

按how are u在字母表中的出现的先后顺序进行编号，我们就有a为1,e为2，h为3，o为4，r为5，u为6，w为7，所以先写出a列，其次e列，以此类推

密文： qoury inpho Tkool hbxva uwmtd cfseg erjez

11:03
录制中

曲路密码(Curve Cipher)

一种换位密码，需要事先双方约定密钥(也就是曲路路径)。
明文： The quick brown fox jumps over the lazy dog
填入5行7列表(事先约定填充的行列数)

11:06 录制中

摩尔斯电码(Morse)

电报通信的语言是由电码符号组成的。电报通信最早是由美国的摩尔斯在１８４４年发明的，所以电码符号也被叫做摩尔斯电码（Morse code）。电码 符号由两种基本信号和不同的间隔时间组成：短促的点信号“ . ”，读“ 的 ”（Di）；保持一定时间的长信号“—”，读“答 —”（Da）。

11:05 录制中

敲击码(Tap code)

敲击码是一种以非常简单的方式对文本信息进行编码的方法。因该编码对信息通过使用一系列的点击声音来编码而命名，敲击码是基于5×5方格波利比奥斯方阵来实现的，不同点是是用K字母被整合到C中。

	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

源文本	F	O	X
位置	2,1	3,4	5,3
敲击码	.. .	... .	....