使用 minidwep 工具研究 WEP 加密的安全性

在 minidwep 上面点鼠标右键选择执行,也可以在不能启动到桌面时输入 minidwep 命令执行。

1		
Home	Spoonwen2	
》 垃圾箱	 ※ 编辑启动器(E) ◎ 用 "Mousepad" 打开(Q) ◇ 用 "AbiWord 字处理" 打开 ✓ 申其它应用程序打开(<u>A</u>) 	
@	 2 复制(C) 参 剪切(I) ·	
CDLINUX	minidw 重命名(R)	
	▲ 应用程序(A)	
软盘驱动器	minidwep	
Spoonwpa		
& 🗑	<u>/ 🔘 🕥 -</u>	Anywlan

启动中并自动识别到网卡的端口

📄 sudo				
	Detectir	winidwep g Wireless card on PC		
Wireless Card Interface	Selected:wlanO Chipset	Driver		
wlan0	RTL8187	rt18187 - [phy0]		
40				
Spoonwpa				
	2 🙆 🕥	▲ 🗖 sudo	()	风云007 Anvwlan

sudo				
Scan a	ninidwep ps encrypted by WEP or WPA encry WPA	tion?		
Spoonwpa	Concerv		X	
? 7	🕅 🎧 🔺 🗖 sudo			云007 Anywia

选择是破解 WEP 还是 WPA 加密的信号后点击 OK



📜 sudo				
winidwep Scanning AP,please wait 20 seconds! Press Enter to finish scanning 18 <☐ OK >				
Spoonwpa	<u> </u>		风云の	07
🕂 🦟 🖉 🏹 🗕 sudo		4))	Any	wlan

搜索到2个WEP加密的信号

负数越小信号越强,随便选择一个进行破解!

📄 sudo				
	Choose one ap AP wac Essid PWR Ch Privacy Client			
	00:16:01:20:20:3ETP-LINK506WEP 00:0F:B5:E9:88:54wireless336WEP			
	< OK > <cancel></cancel>			
		Ø		
dp				
Spoonwpa				
0				凤云007
7 🗇 🥖	🥘 🕥 🔺 🗖 sudo		۲)	Anyw

选中要破解的信号,点 OK 进行下一步设置!



100.00			
📄 sudo			
	winidwep Select Mode:		
	<pre>[*] a aireplay-ng -2(Interactive mode) [*] b aireplay-ng -3(ARP-request mode) [] c aireplay-ng -4(Chopchop mode) [*] aireplay-ng -5(Fragment mode) [] e aireplay-ng -6(Caffe-latte mode) [] f aireplay-ng -7(Fragments against a client)</pre>		
Encor			
spoon	мра		
			凤云007
21	〒 🥖 🥘 🌢 🗖 sudo	()	Anywlan

一般选择 -2、-3、-5 模式后点 OK 同时开始攻击.....

这个默认 500 的攻击速度,最后点 OK 进入全自动攻击模式!

sudo	
Inject Rate, 500 is normal Select inject rate 000 1 400 2 300 3 200 4 100 5 50 6 20 7 10 8	
<mark>< DK ></mark> ⟨Cancel>	
ϕ	
Spoonwpa	
	风云007
 // // // // // // // // // //////////	Anywic

自动开始发动攻击中.....

sudo				
F	■inidwep Take Authentication successful!			
aireplay-ng -F -2 :19 -× 500 mon0 aireplay-ng -3 -k aireplay-ng -F -m For information,	2 -p 0841 -c fffffffffffff -b 00:0F:B ⊃ 00:0F:B5:E9:88:54 -h 00:E0:4C:03:3 ■ 144 -5 -b 00:0F:B5:E9:88:54 -h 00: no action required: Using gettimeof	5:E9:88:54 -h 00:E0:4C:03:33 3:19 -× 500 mon0 E0:4C:03:33:19 mon0 day() instead of /dev/rtc		
<i>dp</i>				
Spoonwpa				
				凤云007
-} 🛒 🍃	🥐 🔯 🕥 🔺 🗖 sudo	[airodump-ng]	()	Anywlan

得到 cap 注入包并开始注入,可以看到 IVS 数值开始快速增加!



IVS 数据继续快速增加



超过 5000 后自动开始搜寻密码.....



密码还没有出来, IVS 数值继续快速增加中......



IVS 已经 14000 多了, 耐心等待密码一定会出来的!



终于得到密码了

Key	found	后面的	1234567890	就是密码
/				

A Home	Spoonwep2					
》 垃圾箱	🍋 feedingbottle					
CDLINUX	aninidwep-gtk		dialog			
■ 软盘驱动器	minidwep	J	ap name: wireless ap mac: 00:0F:B5:E9:6 Hex key found ! 12345	nini 18:54 167890	днер	
Spoonwpa						
-}	2 🚳 🕥 • 🛙] dialog			4))	风云007 Anywlan

欢迎假如QQ技术交流群 114705111