minidwep-gtk 的 WEP 加密安全性研究

启动 CDlinux 后在桌面的 minidwep-gtk 图标上点击鼠标的右键选择执行

Home	Spoonwep2			
》 垃圾箱	S			
CDLINUX	X minidwep-gt	 ▲ 执行(E) ※ 编辑启动器(F) 		
软盘驱动器	minidwep	 □ 如有加令加(2) □ 用 "Mousepad" 打开(<u>0</u>) ☆ 用 "AbiWord 字处理" 打开 ■ 用其它应用程序打开(<u>A</u>) 		
		↓ 复制(C) 参 剪切(I) ⑦ 删除(D)		
Spoonwpa		重命名(<u>R</u>)		
& 🖷 🍃	2 🔘 🕥	• • • • • • • • • • • • • • • • • • •	4)	Anywlan

执行后跳出一个警告的对话框,点 OK 就可以了!

Home	Spoonwep2			
运 垃圾箱	feedingbottle			
	ininidwep-gtk	■ minidwep-gtk ▲ 軟件是家用无线路由器安全审计之工具 切勿用于非法行为 盗用他人无线网络涉嫌违法 丢弃WEP加密,使用WPA2加密		
软盘驱动器 Spoonwpa	minidwep			
	2 🗐 🕥 -	minidwep-gtk	4))	风云007 Anywlan

启动完成

lomi	dwep-gtk	(
无线	网卡	路由MAC	名称	强度	信道 加密方式	客户端MAC		
wlan0	-							S扫描
wlan0 RTL	.8187							
rti8187 - [p	ohy0]							
	200							
	方式							
WEP	×							
方式选择	¥	11:18:10>等待	持命今中				1	山白田
📕 🖌 Airepla	iy-ng -2		9 m 4 1					
🛿 🗵 🗹 Airepla	iy-ng -3						11	A停止
🗌 Airepla	iy-ng -4							
Airepla	iy-ng -5							
Airepla	iy-ng -6							
Airepla	iy-ng -7							
注入;	速率							
500	-							<u>E</u> 退出
				IV	S数量:			

点击扫描开始搜索 WEP 加密的无线信号

lom minidwep	-gtk				
无线网卡	路由MAC	名称	强度 信道 加密方式	客户端MAC	
wlan0	Scanning				S扫描
参J wlan0 RTL8187 rtl8187 - [phy0] 2坂洋					
信道					
LIN 加密方式	-				
Aireolau ng 2					上启动
awzī IV Aireplay-ng -3					
Aireplay-ng -4					
Aireplay-ng -5					
Aireplay-ng -6					
Aireplay-ng -7					
注入速率					
500	•				<u>E</u> 退出
Charles IV			11/5数量:0		

片刻后扫描到2个 wifi 信号

📄 minidwep-g	K	
om) 无线网卡	路由MAC 名称 强度 信道 加密方式 客户端MAC	:
wlan0 🔻	00:16:01:2D:2D:3E_TP-LINK466WEP	<u>S</u> 扫描
wlan0 RTL8187 rtl8187 - [phy0] 坂弁	00:0F:B5:E9:88:54wireless336WEP	
信道		
方式选择 → Aireplay-ng -2 → Aireplay-ng -3 Aireplay-ng -3 Aireplay-ng -4 → Aireplay-ng -5 Aireplay-ng -6 Aireplay-ng -7 ○ Aireplay-ng -7	11:19:18>等待命令中	上启动
500	D/C##	上退出

信号强度为负数显示,选择信号强度高的一个准备破解,攻击方式默认-2、-3、-5,注入速度设置到最高 800, 最后点击启动开始自动破解.......!

📄 minidwep-g	tk			_			
无线网卡	路由MAC	名称	强度	信道力	加密方式	客户端MAC	
wlan0 🔻	00:16:01:2D:2D:3E	TP-LINK	44	_6_	_WEP	4	<u>S</u> 扫描
wlan0 RTL8187 rtl8187 - [phy0]	00:0F:B5:E9:88:54	wireless_	33	_6	_WEP		
在 信道							
	k -						
WEP V	r I						
方式选择							
Aireplay-ng -2	11:22:03>等待命	令中					
Z Aireplay-ng -3							A停止
Aireplay-ng -4							
Aireplay-ng -5							
Aireplay-ng -6							
12 注入速率							
800 -	10 -						E退出
Contraction Contraction			IVS₹	x₩:0			

自动开始进行虚拟连接......后面的事情就不需要我们参与了!

omi minidwep-g	tk	
无线网卡	路由MAC 名称 强度 信道 加密方式 客户端MA	c
🧊 wlan0 🔻	00:16:01:2D:2D:3ETP-LINK446WEP	S扫描
ジ wlan0 RTL8187 rtl8187 - [phy0] 扱余	00:0F:B5:E9:88:54wireless336WEP	
夏 次 信道		
LIN 加密方式		
WEP		
方式选择	44.22.47 。 長柳さなさなます」	
Aireplay-ng -2	11:22:46> 虚拟连接成功! 11:22:44> 岩洋WEPilitic语或	
अ∑z 💌 Aireplay-ng -3	The second secon	A停止
Aireplay-ng -4		
Aireplay-ng -5		
Aireplay-ng -6		
Aireplay-ng -7		
onw 注入速率		
800 -		<u>E</u> 退出
Laster Co	1/2 初二・	

同时发动-2、-3、-5的攻击.....

m	tk	
无线网卡	路由MAC 名称 强度 信道 加密方式 客户端MAC	
wlan0 🔻	00:16:01:2D:2D:3E_TP-LINK446WEP	S扫描
wlan0 RTL8187 rtl8187 - [phy0]	00:0F:B5:E9:88:54wireless336WEP	
信道		
IN 加密方式		
- 方式选择 ✓ Aireplay-ng -2 ✓ Aireplay-ng -3 Aireplay-ng -4 ✓ Aireplay-ng -5 Aireplay-ng -6	11:22:47>启动aireplay-ng -5 11:22:47>启动aireplay-ng -3 11:22:47>启动aireplay-ng -2 11:22:46>虚拟连接成功! 11:22:44>发送WEP认证请求	<u>L</u> 启动 <u>A</u>停止
Aireplay-ng -7		

-2 攻击注入成功,IVS 的数值开始快速增长,这个时候破解密码就是时间的问题了。

lomu	vep-gt	k	
无线网	ŧ	路由MAC 名称 强度 信道 加密方式 客户端MA	.c
wlan0	-	00:16:01:2D:2D:3E_TP-LINK446WEP	<u>S</u> 扫描
参J wlan0 RTL81 rtl8187 - [phy	87 '0]	00:0F:B5:E9:88:54wireless336WEP	
信道			
	-		
LIN 加密方:	式		
-方式选择 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1 ● Aireplay-1	ng -2 ng -3 ng -4 ng -5 ng -6 ng -7	11:22:54>Aireplay-ng -2 成功,开始注入 11:22:47>启动aireplay-ng -5 11:22:47>启动aireplay-ng -3 11:22:47>启动aireplay-ng -2 11:22:46>虚拟连接成功! 11:22:44>发送WEP认证请求	<u>」</u> 启动 <u>A</u> 停止
注入速	*		
800	-		E退出

IVS 的数值继续快速增长,并且在超过 6000 后就自动启动 aircrack-ng 搜寻密码。

lomi minidw	vep-gtk				
无线网	卡 路由MAC	名称 强度	信道 加密方式	客户端MAC	
wlan0	▼ 00:16:01:2D:2	D:3E_TP-LINK4	146WEP		S扫描
参J wlan0 RTL81 rtl8187 - [phy	87 00:0F:B5:E9: 0]	38:54wireless3	36WEP		
6道					
All					
LIN 加密方: WEP	et				
方式选择 ✓ Aireplay-r ✓ Aireplay-r ✓ Aireplay-r ✓ Aireplay-r Aireplay-r Aireplay-r Aireplay-r Aireplay-r 2 Aireplay-r 2 Aireplay-r	ng -2 11:23:04>启 11:23:04>用 11:22:54>启 11:22:47>启 11:22:47>启 11:22:47>启 11:22:47>启 11:22:46>虚 11:22:46>虚	动aircrack-ng搜寻密码 始寻找密码 replay-ng -2 成功,开始 动aireplay-ng -5 动aireplay-ng -3 动aireplay-ng -2 拟连接成功! 送WEP认证请求	3 注入		<u>」</u> 启动 ▲停止
000		IVC	教書·0174		<u>Lastra</u>

密码还没有计算出来继续搜集 IVS 数值.....

📄 minidwej	o-gtk	
无线网卡	路由MAC 名称 强度 信道 加密方式 客户端MAC	
wlan0	▼ 00:16:01:2D:2D:3E_TP-LINK446WEP	S扫描
刻 rtl8187 - [phy0] 设余	00:0F:B5:E9:88:54wireless336WEP	
· 信道		
All		
LINI 加密方式		
WEP	× .	
方式选择		
Airanlay, no.	11:23:04>启动aircrack-ng搜寻密码	L启动
Aireplay-ng	- 11:23:04>开始寻找密码	A 1981 - 1
Aireplay-ng	- II:22:54>Alreplay-ng-2 放功,开始注入 4 11:22:47、史記bireplay.ng 5	
Aireplay-ng -	5 11-22:47 >户动alreplay-ng -3	
🔄 🗌 Aireplay-ng -	6 11-22:47 >户計airenlay ng 2	
🗌 🗌 Aireplay-ng -	7 11:22:47启幼alleplay-ig-2 11:22:46、唐拟连续成15.1	
onv 注 λ 速率	11·22·44> 发送WEP认证请求	
11/1/14		C C B H
800		<u>E</u> 184

IVS 数值快速增长中.....

om	minidw	ep-gt	<u>k</u>	
	无线网十	ŧ	路由MAC 名称 强度 信道 加密方式 客户端MAC	
	wlan0	-	00:16:01:2D:2D:3E_TP-LINK446WEP	<u>S</u> 扫描
剑 Z圾和	vlan0 RTL818 tl8187 - [phy(87)]	00:0F:B5:E9:88:54wireless336WEP	
	信道			
	All	•		
LIN	加密方式	ť		
	VVEr			_
	方式选择		11:23:04>启动aircrack-no搜寻家码	1.Deft
	Aireplay-n	g -2	11:23:04>开始寻找密码	
3. SZZ	Aireplay-n	g -3	11:22:54>Aireplay-ng -2 成功,开始注入	A停止
	Aireplay-n	g -4	11:22:47>启动aireplay-ng -5	
S.	 Aireplay-n 	g -5	11:22:47>启动aireplay-ng -3	
\mathcal{F}	Aireplay-n	g -6	11:22:47>启动aireplay-ng -2	
	_ Aireplay-n	g -7	11:22:46>虚拟连接成功!	
onv	注入速率	E	11:22:44>发送WEP认证请求	
	000	1-1	2004	E38.44

搜集一定数量的 IVS 密码就会自动就会跳出来,KEY:后面显示的就是密码。这个教材里面的密码比较简单并且是 64 位的加密,所以速度很快。

1	<u>db</u>	1				
Hom	miniowep-gi	CK.				
	无线网卡	路由MAC	minidwep messag	e this last is the	MAC	
	wlan0 💌	00:16:01				S扫描
	wlan0 RTL8187	00:0F:B5	AP MAC: 00:0F:B5:E9:88	:54		
45.48.2	rtl8187 - [phy0]		Essid: wireless			
山山以木			Hex Key: 1234567890			
		8				
Exc	信道					
	All					
CDLIN	加密方式					
	WEP 💌					
					1	
	方式选择	11:23:22			-	L启动
	Aireplay-ng -2	11:23:04				
软盘驱动	Aireplay-ng -3	11:23:04				A停止
	Aireplay-ng -4	11:22:54				
18	Aireplay-ng -5	11:22:47				
dp	Aireplay-ng -6	11:22:47				
-	Aireplay-ng -7	11:22:47				
Spoonv	注入速率	11:22:46		X <u>C</u> lo	ose	
	800 💌	11:22:44				<u>E</u> 退出
	Lesses 1. J		IVS	数量:20576		
	IVS数量: 20576					$\boxed{\mathbf{X}} \neq 0.07$

欢迎假如QQ技术交流群 114705111