首先说说 BT3 跟 BT4 的区别吧! BT4 比 3 支持的网卡多, 破解的网络路由也多。他们就好比 WIN98 和 WINXP 的区别,应该说 BT4 操作比 BT3 好。各自使用感觉吧!

BT4 下用 spoonwep+spoonwpa 破解 wep 或 wpa 加密的无线网络

一、首先下载这三个工具:

1、BT4 正式版 ISO 镜像文件

下载地址: <u>http://www.offensive-security.com/blog/backtrack/backtrack-pre-final-public-release-and-download/</u>

2、U盘启动制作工具: unetbootin

下载地址: http://www.onlinedown.net/soft/88566.htm

3、spoonwep-wpa 破解工具用于 BT4 下的 deb 安装包

下载地址: http://u.115.com/file/f2e57c776c

二、运行 unetboot in 制作 BT4 的 U 盘启动系统。

UNetbootin	
⑦ 发行版 ① 次询访问 INterhootin.	== Select Distribution == 🔽 == Select Version == 🔽
<ol> <li>1. 任列表里选择=</li> <li>2. 选择一种安装类</li> </ol>	"个尖型版本下载,或者于动载入指定又许。 型,然后单击 OK 开始安装。
◎ 光盘镜像 ①	ISO 🔽 G:\ISO文件夹\bt4-pre-final.iso
◎ 自定义 ©	内核 低: [] Ini trd (图): []
	选项 @:
📄 显示所有驱动器(值	用) (4)
类型(T): USB 驱动器	<ul> <li>▼ 驱动器 (V):</li> <li>● 确定 取消</li> </ul>

点确定就开始制作了。在这里需要等几分钟吧,因为从 ISO 文件里提取文件拷贝到 U 盘里需要一段时间。 完成之后,不要重启, 再把刚刚下到的"spoonwep-wpa 破解工具用于 BT4 下的 deb 安装包" 拷贝到 U 盘根目录下面, 自己记好它好的名字,方便到 BT4 下找到它。

## 三、启动 BT4

在 BIOS 里面设置从 U 盘启动。

1.进入主板 bios 设置界面的方法

进入 bios 设置的方式基本都是在开机时按"Del"键,不过有些品牌的主板比较特殊,笔记本则是按 F2 的居多,也有按 F1、ES 设置完毕保存退出则基本都是按 F10。

2.设置 U 盘启动的 bios 菜单项.

A、无需进入 bios 设置的 现在好多名牌大厂主板无需进入 bios 界面就可以用快捷键选择 USB 启动,像华硕和联想的 F8 的 F11、IBM 笔记本的 F12 等等,只要按下这些快 捷键,再选择 USB 设备就可以顺利启动,根本无需在意 U 盘的启动,HDD 还是 ZIP,应该说是比较方便的。

B: 较新的主板 bios 中往往没有 USB-hdd 的选项,这种 bios 设置 U 盘启动都需要同时设置两个项目,下面是几个具体例 1.精英 RS482-M 主板,先把硬盘设为第一启动设备,然后再到上面那个"hard disk boot priority"的项目,里面可以同时看 和 U 盘的型号,把 U 盘调到第一位即可。



C: 常见的新情况是, bios 中根本不出现类似 USB-???的项目,这是主板把 U 盘当硬盘对待,设置 U 盘启动大多涉及两项目,名称基本上就是"1st boot device"、"boot sequece"、"Hard disk boot priority"之类。设置思路基本就是先把硬盘设为动设备,再到硬盘选择项目中把 U 盘提到首位。提供几个图片供大家参考,AWARD 和 AMI 都 有,大同小异.

CPU Feature	Press Enter	Iten He
First Boot Device Second Boot Device	CBRON Renovable	Henu Level 🕨
Third Boot Device Boot Other Device	First Boot Device	s parameter to specify
Security Option HDD S.M.A.R.T. Ca	Renovable [ ] Hard Disk 先这里 . [ ]	uence. The k ID are li
Show Logo On Scre Bypass Vivid BIOS	CURON [#] LAN [ ]	ON:
	DisabledLJ	ovable: Flo LS1 ZIP
	14:Nove ENTER:Accept ESC:Abo	t boot ROM

## 四、进入 BT4

登陆的用户名: root, 密码: toor

startx 命令启动图形化界面。

	Ignoning extra sumbols	
/ Fnnone fnom vkhe	ignoring caura symbols	
The XKFYBOARD ke	uman commiler (ykhcomm) remorts:	
$\rightarrow \text{Warning}$ :	Tume "ONE LEVEL" has 1 levels, but (RALT) has 2 sumbols	
>	Ignoring extra sumbols	
Errors from xkbc	comp are not fatal to the X server	
The XKEYBOARD ke	umap compiler (xkbcomp) reports:	
> Warning:	Type "ONE_LEVEL" has 1 levels, but <ralt> has 2 symbols</ralt>	
>	Ignoring extra symbols	
Errors from xkbc	omp are not fatal to the X server	
The XKEYBOARD ke	ymap compiler (xkbcomp) reports:	
> Warning:	Type "ONE_LEVEL" has 1 levels, but <ralt> has 2 symbols</ralt>	
>	Ignoring extra symbols	
Errors from xkbc	omp are not fatal to the X server	
(EE) Grab failed	. Device a fready configured?	
(EE) Preinit ret	urned NULL for MacIntosh Mouse button emulation	
(FF) Coal failed	Deuice alreadu configured?	
(FF) PreInit ret	urned NULL for "AT Translated Set 2 keyboard"	
(EE) config/hal:	NewImmutDeviceRequest failed	
The XKEYBOARD ke	uman compiler (xkbcomn) reports:	
> Warning:	Type "ONE LEVEL" has 1 levels, but <ralt> has 2 symbols</ralt>	
>	Ignoring extra symbols	
Errors from xkbc	comp are not fatal to the X server	
(EE) Grab failed	. Device already configured?	
(EE) PreInit ret	urned NULL for "Macintosh mouse button emulation"	
(EE) config/hal:	NewInputDeviceRequest failed	
(EE) Grab failed	. Device a fready configured?	
(EE) Preinit ret	urned NULL for "HI Iranslated Set 2 Keyboard"	
(LE) Config/nal:	newinputpevicenequest failed	rometo
waiting for Y se	muen to shut down	expl Ait
wareing TOP A Se		U.
1.52.1.57.1.1.1		

五、安装 spoonwep-wpa-rc3. deb 包



点击左下角的开始菜单,点击一个叫 system mune 的弹出菜单,再点击"storeage media",

会打开一个窗口,点击窗口上面有个刷新的按钮,在窗口下面空白的地方会列出你的硬盘和外设,

进入 U 盘, 找到刚才放入的 spoonwep-wpa-rc3. deb, 把这个文件复制到 BT4 的桌面

(其实就是/root),可以直接拖到桌面,打开命令行窗口运行"dpkg -i spoonwep-wpa-rc3.deb"

稍等几秒中,桌面上出现 desktop 的文件夹,里面就有了 spoonwep2+spoonwpa,好了,

直接单击图标就能运行 spoonwep2 或 spoonwpa 了。

也可以输入以下命令执行: spoonwep2 执行:spoonwep2

spoonwpa 执行:spoonwpa

六、开始破解!!!!

## 下面破解称为傻瓜式 不用输入大量的命令。

输入 spoonwpa 回车后就会弹出 spoonwpa 的窗口。

<b>a</b>		Shell - Konsole	e <2>	0		
root@bt:~# spoonw root@bt:~# ]	pa					[]20 ] ▲ []31 []81 []81 []81 []81 []81 []81 []81 []8
	<b>6</b>	SpoonWpa	/ Wpa Cracker / Sha	manVirtuel 2K8		
		OISCOVERY	S HANDSHARE CAPTUR	CRACKING	🕜 HELP	
		I Met ( I Modi See Modi	CARD WLANO ER (NORMAL E UNKNOWN VICTI NEXT			

在 NET CARD 里选 WLANO, 在 DRIVER 里选 NORMAL,

在 MODE 里选 UNKNOWN VICTIM, 再点击 NEXT、点击 LAUNCH 进入搜索, 然后关闭 spoonwpa 再开一下, 点击 SPOONWEP SETTINGS, 在 NET CARD 里选 MONO, 在 DRIVER 里选 NORMAL, 在 MODE 里选 UNKNOWN VICTIM, 再点击 NEXT、点击 LAUNCH 进入搜索后就可以看见好多网卡啦,



选定1个必须有客户端的网卡点击

SELECTION OK, 再点击 LAUNCH AUTOMATED HANDSHAKE CAPTURE, 如抓到握手包, 我这里由于晚上没几个开路由的信号很

就不一一演示了。很难抓到握手包·!

spoonwep2 破解法跟 WPA 和 WEP 一样。:

输入 spoonwep2 回车后就会弹出 spoonwep2 的窗口。 点击 SPOONWEP SETTINGS,在 NET CARD 里选 WLANO,在 DRIVER 里选 NORMAL,在 MODE 里选 UNKNOWN VICTIM,

再点击 NEXT、点击 LAUNCH 进入搜索, 然后关闭 spoonwep2 再开一下, 点击 SPOONWEP SETTINGS,

在 NET CARD 里选 MONO,在 DRIVER 里选 NORMAL,在 MODE 里选 UNKNOWN VICTIM,再点击 NEXT、

点击 LAUNCH 进入搜索后就可以看见好多网卡啦,选定 1 个网卡点击 SELECTION OK,选定

PO841 REPLAY ATTACK (这里有4条命令选择),点击 LAUNCH 后就等待密码的出来

(sata 数据包到 10000 个左右, 跑到 30000 以上就应该放弃了)。