

## Wireless Security Live CD Distributions

Raul Siles (January 08)

<http://www.raulsiles.com/resources/wifi.html>

SANS SEC617 CD	
<b>Author</b>	SANS (Joshua Wright)
<b>URL</b>	SANS Security 617: "Assessing and Securing Wireless Networks" <a href="http://www.sans.org/training/description.php?mid=3">http://www.sans.org/training/description.php?mid=3</a>
<b>Version</b>	20071024
<b>Size</b>	570 MB
<b>Base OS</b>	Backtrack v2
<b>Goal</b>	Wireless security, auditing, and penetration testing
<b>Wireless drivers</b>	See "Backtrack v2"
<b>Wireless tools</b>	See "Backtrack v2" + "Backtrack 2 Final Customization Notes.pdf" (inside CD)

Backtrack v2	
<b>Author</b>	remote-exploit.org (Max Mosser et. al.)
<b>URL</b>	<a href="http://www.remote-exploit.org/backtrack.html">http://www.remote-exploit.org/backtrack.html</a>
<b>Version</b>	20071024
<b>Size</b>	700 MB
<b>Base OS</b>	Slax (Merge of Whax and Auditor Security Collection)
<b>Goal</b>	Linux live distribution focused on penetration testing
<b>Wireless drivers</b>	<a href="http://backtrack.offensive-security.com/index.php?title=HCL:Wireless">http://backtrack.offensive-security.com/index.php?title=HCL:Wireless</a> <a href="http://backtrack.offensive-security.com/index.php?title=Changelog#Wireless_Attacks_.40_their_best">http://backtrack.offensive-security.com/index.php?title=Changelog#Wireless Attacks .40 their best</a>
<b>Wireless tools</b>	<a href="http://backtrack.offensive-security.com/index.php?title=Tools#Radio_Network_Analysis">http://backtrack.offensive-security.com/index.php?title=Tools#Radio_Network_Analysis</a>

Wifiway	
<b>Author</b>	<a href="http://www.seguridadwireless.net">www.seguridadwireless.net</a>
<b>URL</b>	<a href="http://www.wifiway.org">http://www.wifiway.org</a>
<b>Version</b>	0.8
<b>Size</b>	420 MB
<b>Base OS</b>	<a href="http://www.linuxfromscratch.org">www.linuxfromscratch.org</a>
<b>Goal</b>	Wireless with international language support
<b>Wireless drivers</b>	<a href="http://www.wifiway.org/contenido.html">http://www.wifiway.org/contenido.html</a> <a href="http://www.wifiway.org/contenido/drivers.html">http://www.wifiway.org/contenido/drivers.html</a>
<b>Wireless tools</b>	<a href="http://www.wifiway.org/contenido/aplicaciones.html">http://www.wifiway.org/contenido/aplicaciones.html</a>

<b>WiFiSlax (Spanish)</b>	
<b>Author</b>	<a href="http://www.seguridadwireless.net">www.seguridadwireless.net</a>
<b>URL</b>	<a href="http://www.wifislax.com">http://www.wifislax.com</a>
<b>Version</b>	3.1
<b>Size</b>	680 MB
<b>Base OS</b>	Backtrack v2
<b>Goal</b>	Wireless security auditing (Spanish)
<b>Wireless drivers</b>	<a href="http://www.wifislax.com/contenido/drivers.php">http://www.wifislax.com/contenido/drivers.php</a>
<b>Wireless tools</b>	<a href="http://www.wifislax.com/contenido/aplicaciones.php">http://www.wifislax.com/contenido/aplicaciones.php</a>

<b>Russix</b>	
<b>Author</b>	Russ Williams, Steve Armstrong
<b>URL</b>	<a href="http://www.russix.com">http://www.russix.com</a>
<b>Version</b>	-
<b>Size</b>	210 MB
<b>Base OS</b>	Slax (version 5 based upon the Linux 2.6 kernel)
<b>Goal</b>	An up-to-date Wireless Security Assessment Toolkit - ie it gets more frequent updates to tools than Backtrack
<b>Wireless drivers</b>	Atheros
<b>Wireless tools</b>	AircrackNG (PTW), Cowpatty, ASleap, Evil Tiny Twin (based upon aircrack), Kismet, nmap, wireshark, and WEP/WPA breaking scripts

<b>SkyRidr</b>	
<b>Author</b>	Nico Darrow
<b>URL</b>	<a href="http://www.skyridr.net/skyridr_0-9.iso">http://www.skyridr.net/skyridr_0-9.iso</a>
<b>Version</b>	0.9
<b>Size</b>	676 MB
<b>Base OS</b>	Debian base OS, basically Auditor with some scripts
<b>Goal</b>	Automate & script a lot of common wireless hacks in a simple to use menu system: hotspot phishing, wep cracking, DoS, port knocking rogue, custom frame creation, etc
<b>Wireless drivers</b>	Skyridr script only supports the madwifi drivers so an Atheros card is required
<b>Wireless tools</b>	Updated aircrack suite and some custom scapy code

<b>OSWA-Assistant</b>	
<b>Author</b>	ThinkSECURE
<b>URL</b>	<a href="http://oswa-assistant.securitystartshere.org">http://oswa-assistant.securitystartshere.org</a>
<b>Version</b>	0.9.0.2a
<b>Size</b>	500-600 MB
<b>Base OS</b>	KNOPPIX 5.1.1
<b>Goal</b>	Wireless auditing: WiFi, Bluetooth, and RFID. Redesigned with user-friendly menus and a web-based help system called the ActivityMap to help non-technical users perform basic wireless audits of their home networks.
<b>Wireless drivers</b>	Madwifi-ng, IPW2200, RT2570, RT73, RT2500 & LORCON support.
<b>Wireless tools</b>	<a href="http://securitystartshere.org/page-training-oswa-assistant-faq.htm">http://securitystartshere.org/page-training-oswa-assistant-faq.htm</a>

Additionally, there is a small bootable CD (13MB), based on FreeBSD, focused on the 802.11 WEP fragmentation attack. It provides support for Atheros cards and includes aircrack, stumbler, and wesside. It is available at <http://darkircop.org/security/bootable.iso>.