

Black Hole

Wireless Traffic Intercept, Reconstruction & Analysis Tool

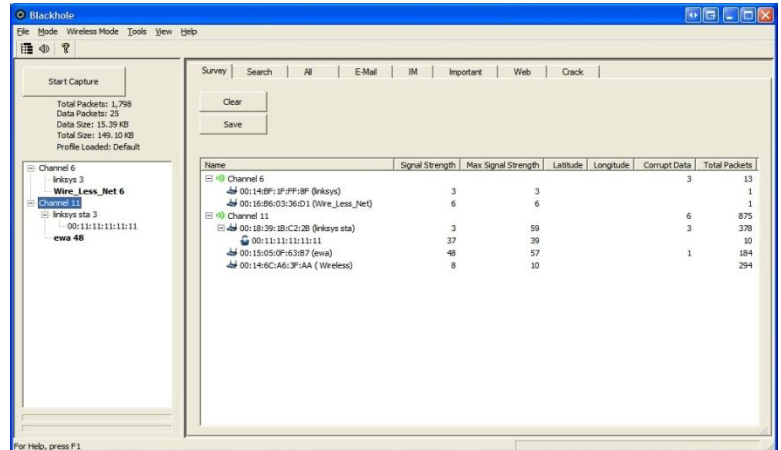
Applications

- Network Survey
- Intelligence Operations
- Network Testing

System Description

Black Hole is a MS Windows based solution that requires only a commercially available wireless access card and a standard PC host. The user is able to **Scan** all 802.11 a/b/g channels, and target any

channel to **Capture** and **Reconstruct** the internet traffic that is occurring. The user can view, in near real-time, the Instant Messages, E-Mails and Web pages on the target channel. The user can save this captured data in a file for later analysis by either using Black Hole's **Review** function or transporting the file to another host. The user can also use the **Crack** function to determine the WEP/WPA encryption key being used by a target. Once a key is known, either by using Black Hole's internal capability or from other sources, the key can be exploited by Black Hole to create clear text from an encrypted source. Because Black Hole uses the standard MS Window's interface to control all of its functions, operator training is simplified.



Features

LAN Protocols: 802.11 a/b/g
 Operational Modes: Passive & Active (when the system is creating traffic)

Key Functions

Capture: Defines channel of interest and scans the environment for all activity on the channel. Selected activity is recorded to a file, for later review, or reconstructed and reviewed in real-time. Black Hole's E-mail, Instant Message, and Web tabs provide the ability to filter, display, and reconstruct e-mail messages (POP3, SMTP, IMAP), instant messaging (Yahoo, ICQ, AOL, MSM), or web page (HTTP) activity. Once a tab is selected, a simple double-click will reconstruct e-mail messages, web pages, and instant message conversations.

Review: Review and reconstruct previously recorded files.

Search: Searches traffic for key words. For example, if the user searches for "bat", it will display anywhere the letters "bat" appear, including bat, battle, combat, etc. More than one keyword can be searched at a time.

Key Functions (continued)

Crack: Attack WEP and WPA (TKIP/PSK) encrypted networks. All encrypted access points (AP) currently in range will be shown in the list and all clients connected to an encrypted AP are listed below their associated AP. The user can then initiate an attempt to determine the encryption key. An active statistical attack against WEP can be performed with results usually in 10 minutes or less. A successful passive attack depends on network traffic. An attack against WPA is a dictionary attack.

Survey: Shows all AP/Clients that are within range and basic traffic analysis such as signal strength, number of data packets and number of corrupt data packets. When a GPS unit is attached, the LAT, and LONG of the strongest signal from each AP will be kept. This function can write the captured data in HTML or KML format, which can be used with a mapping program to give the user a graphical image of the locations where the strongest signal strengths for each AP and Client are detected.

Recommended Host CPU Configuration:

OS:	Windows XP Pro
CPU Clock:	2 GHz min
RAM:	1 GB min
Hard Drive:	50 GB
WLAN Card:	Proxim ORiNOCO a/b or a/b/g
GPS:	Serial, NMEA

For more information contact:

Tom Bonazza
Phone: 304.333.2510
tbonazza@ewa.com