FININTRUSION KIT

FinIntrusion Kit was designed and developed by world-class IT Intrusion specialists, who have over 10 years of experience in their area through their work in several Tiger Teams (Red Teams) in the private and government sector assessing the security of different networks and organizations.

The FinIntrusion Kit is an **up-to-date and covert** operational Kit that can be used for most common **IT Intrusion Operations** in defensive and offensive areas. Current customers include **Military CyberWar Departments, Intelligence Agencies, Police Intelligence and other Law Enforcement Agencies**.

QUICK INFORMATION	
Usage:	· **Strategic Operations** · **Tactical Operations**
Capabilities:	· **Break WEP/WPA Encryption** · **Network Monitoring** **(including SSL Sessions)** · **IT Intrusion Attacks**
Content:	· **Hardware/Software**

Usage Example 1: Technical Surveillance Unit

The FinIntrusion Kit was used to break **the WPA encryption** of a Target's home Wireless network and then monitor his **Webmail (Gmail, Yahoo, …) and Social Network (Facebook, MySpace, …) credentials**, which enabled the investigators to **remotely monitor** these accounts from Headquarters without the need to be close to the Target.

Usage Example 2: IT Security

Several customers used the FinIntrusion Kit to successfully **compromise the security** of networks and computer systems for **offensive and defensive** purposes using various Tools and Techniques.

Usage Example 3: Strategic Use-Cases

The FinIntrusion Kit is widely used to remotely gain access to Target Email Accounts and Target Web-Servers (e.g. Blogs, Discussion Boards) and monitor their activities, including Access-Logs and more.

Feature Overview

· Discovers **Wireless LANs (802.11) and Bluetooth® devices**
· Recovers WEP (64 and 128 bit) Passphrases **within 2-5 minutes**
· **Breaks WPA1 and WPA2** Passphrases using Dictionary Attacks
· Actively monitors Local Area Network (Wired and Wireless) and **extracts Usernames and Passwords even for TLS/SSL-encrypted sessions**
· Emulates **Rogue Wireless Access-Point** (802.11)
· Remotely **breaks into Email Accounts** using Network-, System- and Password-based Intrusion Techniques
· **Network Security Assessment** and Validation

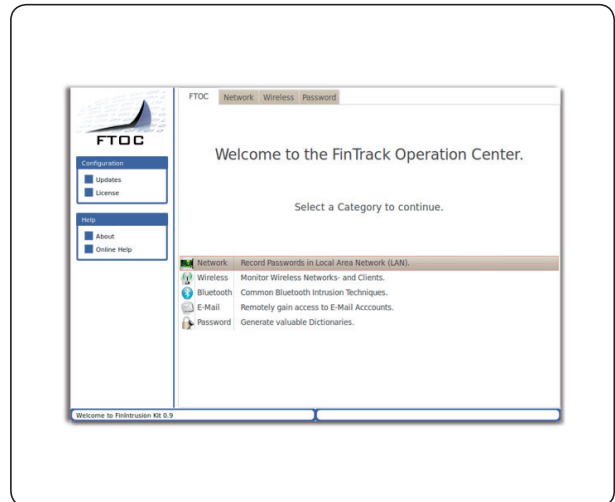**For a full feature list please refer to the Product Specifications.**

FINFISHER™

IT INTRUSION

Product Components

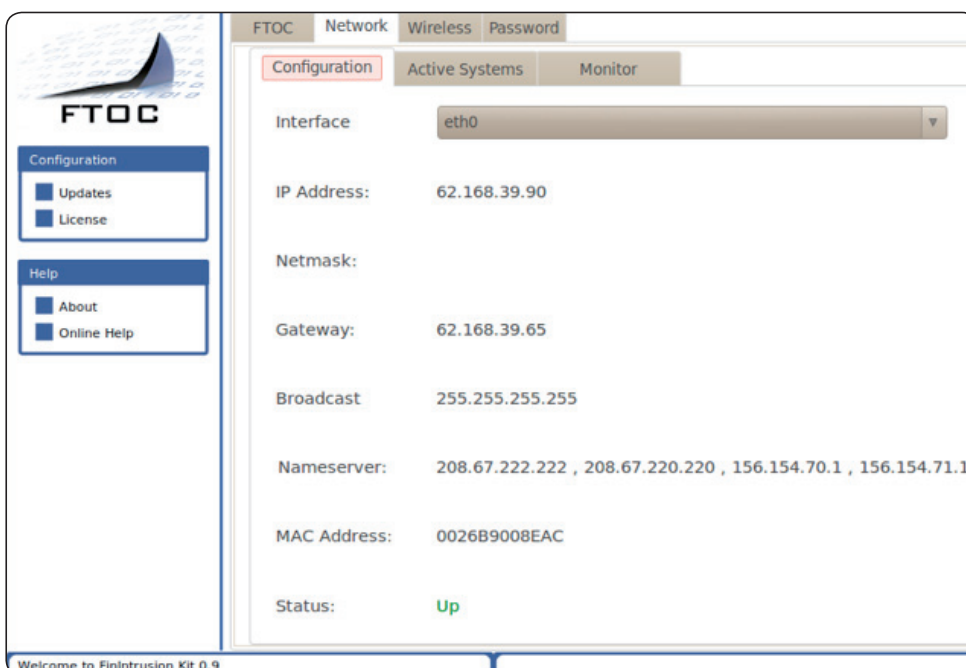**FinIntrusion Kit - Covert Tactical Unit**

Basic IT Intrusion Components:
· High-Power WLAN Adapter
· High-Power Bluetooth Adapter
· 802.11 Antennas
· Many Common IT Intrusion Devices

FinTrack Operation Center
· Graphical User Interface for Automated IT Intrusion
  Attacks

Automated LAN/WLAN Monitoring

LAN/WLAN Active Password Sniffer

Captures even SSL-encrypted data like Webmail, Video Portals, Online-Banking and more

Username	Password	Server	Protocol
dropbox	fr33dom	64.223.183.17	https
ftp	secret1	128.101.240.212	ftp
ftoc	password1	62.84.74.92	pop3

Main Credentials

Start   Delete   Save...