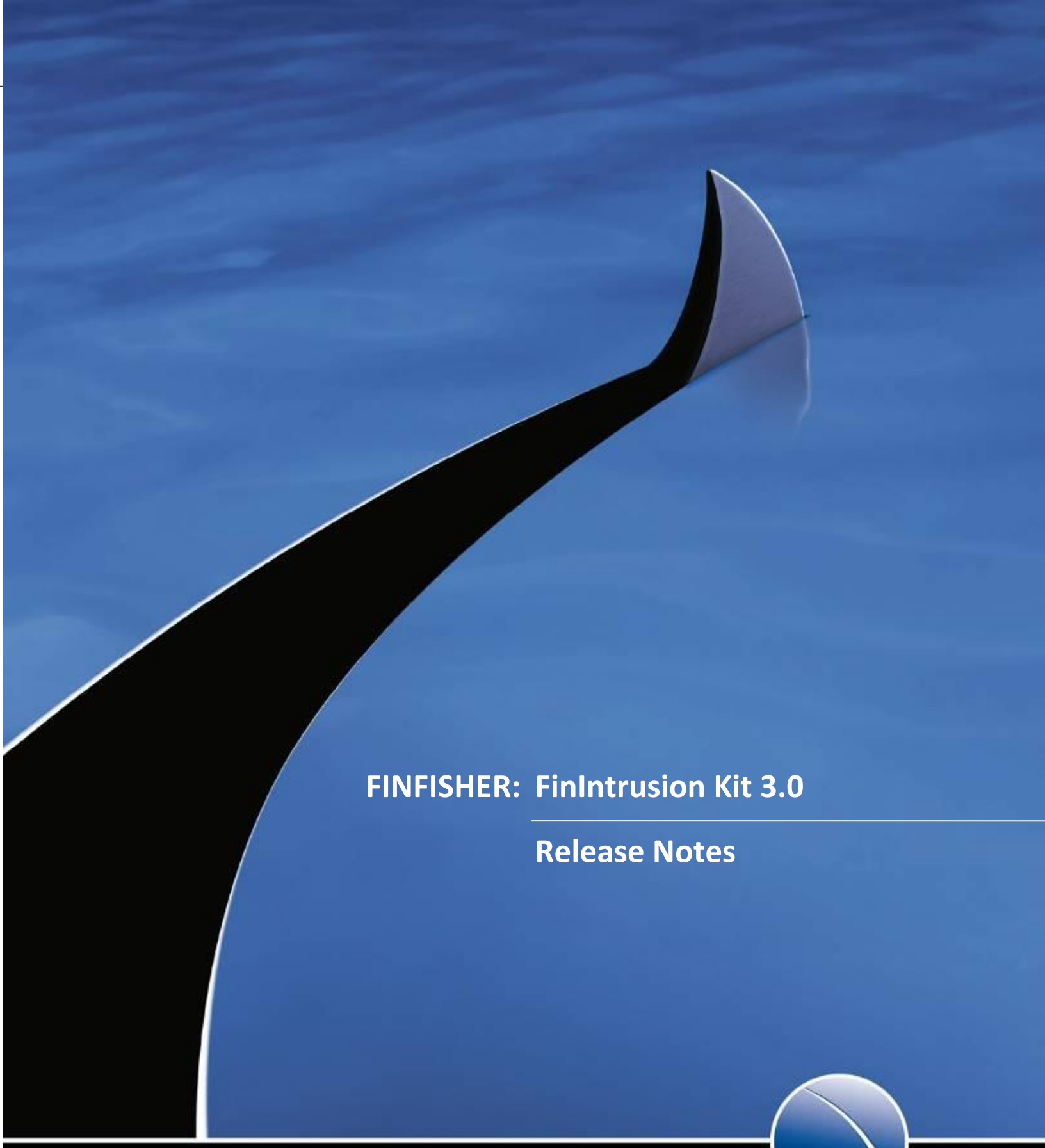


FINFISHER: FinIntrusion Kit 3.0

Release Notes

FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM

Date 2013-02-08

Release information

Version	Date	Author	Remarks
1.0	2010-06-29	ht	Initial version
2.0	2011-05-26	Pk	Changes for FinIntrusion Kit Version 2.0
2.2	2011-09-23	Pk	Changes for FinIntrusion Kit Version 2.2
2.3	2011-11-02	PK	Changes for FinIntrusion Kit Version 2.3
2.4	2011-11-30	PK	Changes for FinIntrusion Kit Version 2.4
3.0	2013-02-08	PK	Changes for FinIntrusion Kit Version 3.0

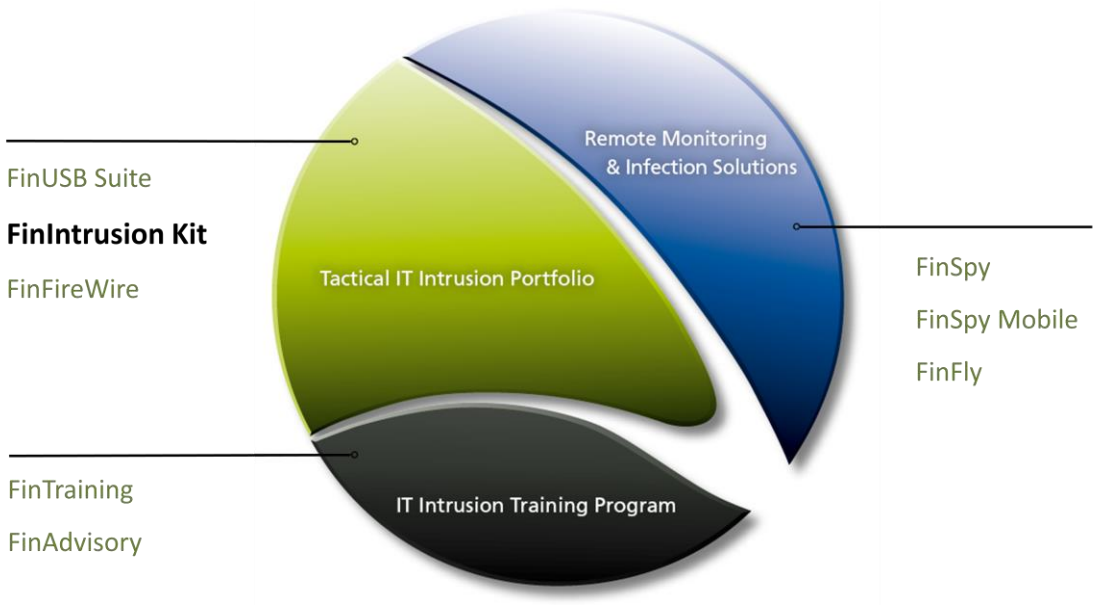
Table of Content

1 OVERVIEW

The *FinIntrusion Kit* is a multi-purpose IT Intrusion kit that has been built specifically for nowadays operations by Law Enforcement and Intelligence Agencies. It can be utilized in a wide-range of operational scenarios like:

- Breaking into- and monitoring Wireless and Wired Networks
- Remotely breaking into E-Mail Accounts
- Performing security assessments of Servers and Networks

The full capabilities are shown in several training courses, each focusing on different operational use-cases.



2 CHANGELOG

Version: 3.0		
Component	**Change**	**Description**
GUI	Improvement / Bugfix	A new design and some fixes to prevent crashes or freezing of the GUI component.
Network / Scanner	Update	Improved the scan speed by 50% and implemented an optional OS fingerprinting.
Network / Scanner	New Feature	Possibility to update Fingerprinting Database to detect newer Operating Systems or Hardware Vendors.
Network / Scanner	New Feature	Based on the network mask the possible target range will be automatically detected. In an older version only a class c-network was supported.
Network Jammer /Sniffer	Bugfix	Some gateway settings could trigger a problem with these modules and they stopped working.
Wireless / Scanner	New Feature	It is possible to refresh the client list of a selected AP without losing old entries.
Wireless / Mass Jammer	New Module	Implement a newer and faster WLAN mass jammer which can disconnect all Wireless Networks on all or dedicated Channels. Black- and white list support is implemented.
Wireless / Breaking Encryption	Update / Improvement	To increase the possibility to capture more packages or WPA handshakes.
Wireless / Multiple Interface Handling	Update / Improvement	Multiple Wireless Adapter and Process handling is supported now. The change was necessary to run a Wireless Jammer and Fake AP at the same time.
Wireless / Fake AP	New Feature	A dedicated channel can be selected, otherwise a random channel will be chosen.
Password / Meta Information	New Module	It is possible to extract “hidden” meta-information from files and to generate customized password list.
Password / Hash Finder	New Module	This module can be used to search for known hashes and send back the clear-text password. An auto detection of the hash type is implemented.

3 LIMITATIONS

This chapter covers current known limitations within the FinIntrusion Kit Software.

Feature	Description
Backtrack	Backtrack includes a wide-range of publicly available IT Intrusion tools within the Toolset. As most of them are proof-of-concept tools, their functionality cannot be guaranteed in every scenario.
FinIntrusion Kit	The software is an approach to automate complex attacks with a simple user interface. Due to the wide-range of different networks and scenarios, the implemented operations cannot be guaranteed to work in all scenarios without more advanced user interaction.
WEP - Cracking	The automated WEP cracking technique requires the Access-Point to be vulnerable to the fragmentation attack.
USB Hard-Disk	The rainbow tables and default word lists provide a selection of possible passwords. It is not guaranteed that the Target's passwords are contained within these lists. Currently the FinIntrusion Kit has no support to crack WPA-PSK with rainbow tables.
Password Generator from Websites	Only HTTP/HTTPS pages without pre-authentication could be scanned. No Proxy support at the moment. Only "pure" HTTP Websites are supported. Password List could still have some useless Entries (e.g. script code), which must be removed manually.
WPA Cracking	Only WPA/WPA2-PSK mode could be attacked. WPA/WPA2 in Enterprise mode couldn't be attacked. There is no possibility to identify "from outside" in which mode the Wireless Network runs (PSK / Enterprise). The success to crack a WPA-PSK depends on the password list and CPU power and could take days / weeks / years.
Wireless Cracking	The Wireless environment is highly flexible. It could happen that Wireless Clients / Networks cannot be detected (depends on the channel hopping and the frequency which is used). Some Access-Points have intrusion detection and prevention or make

	active network / cracking attacks very difficult.
HTTPS emulation	Some browser like Google Chrome prevent a HTTPS → HTTP break down for their (non-)commercial services e.g. Gmail. These can only be bypassed if the Target is using a different browser. In the case a SSL break down isn't possible, the target system will get a certificate warning!
Fake Access Point Setup	Currently we strongly recommend to us a cable network interface as Uplink interface, otherwise the bandwidth / network performance could trigger a lot of packages lost.
OS detection	OS fingerprinting cannot guarantee that the result is the actual OS. In most of the cases a specific fingerprint can only be generated if at least one TCP port is open. If a target is using a personal firewall which blocks all incoming connections, an OS fingerprint cannot be done. An active OS fingerprint can also trigger an alert on target system.
Jammer	Some systems, especially SOHO environment, can be vulnerable for DoS attacks based on jamming the (wireless) network or dedicated connected Clients. In some cases the equipment needs a reboot or must be switched off/on. There exists no indication which helps us to detect it before the attack will be done. If you're not sure, please feel free to contact our support team.
Wireless Client / Network detection.	Currently we're only supporting 802.11bgn networks which run in a 2.4Ghz frequency.
MAC Spoofing	FinIntrusion Kit has support to spoof the MAC address of the current used Network Adapter. This feature is only working for Network Intrusion Attacks. For Wireless Intrusion attacks, the MAC address for a virtual monitoring interface cannot be spoofed and will be all the time the real MAC address of the wireless adapter (even if this MAC address of the wireless adapter is spoofed!).
ARP Spoofing / Sniffing / Jammer failed	The FinIntrusion Kit tries to do an ARP spoofing attacks for different scenarios. In some cases the default gateway or some firewalls are detecting and blocking ARP spoofing attacks. If the target system or default gateway has static MAC address

	entries, the attack will also fail. In these cases the Network Sniffer and Jammer will not work.
Client Isolation	Wireless client devices can be isolated from each other either within an SSID or between 2 SSIDs. In this case all target systems will be listed with one identical MAC address. In these cases the Network Sniffer and Jammer will not work.

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

WWW.GAMMAGROUP.COM