Please have a look at our new Website! Now with the newest Information to download!

www.elaman.de

elaman
GERMAN SECURITY SOLUTIONS

Newsletter 3/07

December 2007

ELAMAN works closely with clients to develop a total system solution to their needs and to ensure that they are equipped, trained and manned to meet the formidable challenges in the field of communication.

Adding new products solutions to our portfolio is an ongoing process. Therefore from now on ELAMAN provides a Newsletter whenever important innovations are coming up.

Kind regards
Your Elaman Team

IT Intrusion: Elaman's new Finfisher Products

Elaman has started its own development for IT - Intrusion (Hacking) products and training as we think this area will become more and more important and effective and is a very valuable add on to the classical IP-Monitoring systems provided by e.g. Siemens, ATIS, ETI, etc.

This range of new IT-Intrusion products we named FinFisher.

The FinFisher kit includes certain types of Hardware products like **USB sticks** to extract from a PC all passwords, Logins, E-Mails, files, etc., **Trojan horse** to control remotely a target PC, **software and methods** to get the Trojan on a target PC, **WLAN and Bluetooth hacking** as well as also different kind of **Training** courses.

These kind of methods and applications allow to widen the capabilities in the field of IP-Monitoring in addition to an existing classical IP-Monitoring system where it is limited to plain not encrypted IP-communications. As the FinFisher products are directly placed on the target PCs, encryption is not an issue anymore and also identifying the target is also easy especially comparing to normal IP-Monitoring where decoding and identifying is always difficult.

The experience shows having 100% of IP traffic, the classical IP Monitoring system will give the capability to monitor 40%, FinFisher gives another 40%. The remaining 20% is very difficult to get.

Maybe authorities are already working internally on such methods but even in this case FinFisher will widen such an approach and specially the training will improve the capabilities of the staff and users.

The philosophy behind the FinFisher IT Intrusion package is to provide the government end-user with today's advanced hacking tools and techniques. This enables Intelligence Agencies to use such hacking components to obtain Intelligence information that cannot be obtained in any other way.

The Intrusion tools can be used by Government Departments for internal introduction / training to the hacking threats being faced today.

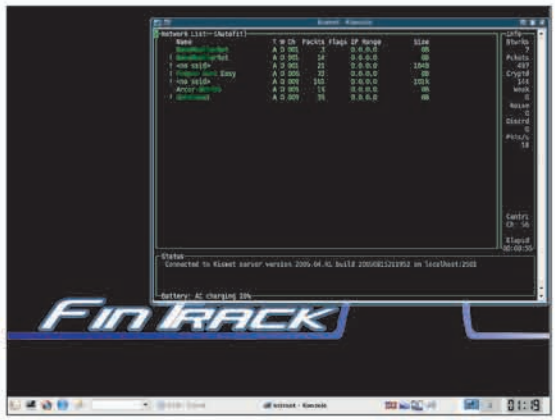
Features
- Information Gathering
- Sniffing
- Exploitation

News

First Information about our new FinFisher IT Intrusion Products!

GOVERNMENTAL SECURITY SOLUTIONS

elaman GmbH • German Security Solutions
Seitzstraße 23 • 80538 Munich • Germany
Tel: +49-89-24 20 91 80 • Fax: +49-89-24 20 91 81 • info@elaman.de • www.elaman.de
HRB München 153662 • Ust-IdNr.: DE814086265 • Geschäftsführer: Holger Rumscheidt



FinFisher WLAN Scanner

FinFisher Products

FinFisher IT Intrusion Programe consists of the following FinFisher Products:

- *FinFisher HQ*

Graphical user interface HQ software for FinFisher 1 and 2.

- *FinFisher 1*

Extracts locally stored user accounts, system and network information from the target PC.

- *FinFisher 2*

Makes a copy of all locally stored e-mails and get a copy of all local files with given file-extensions.

- *FinFisher 3*

2 bootable CD-ROMs to:
a) Clear the Windows Administrator account password and
b) Wipe all local hard-disks.

- *FinSpy*

A trojan-horse-like software for remote surveillance of one or multiple target systems.

- *FinFly*

A transparent HTTP proxy that can modify executables while they are being downloaded.

- *FinFisher Hacking PC*

Robust notebook including FinTrack and Windows system which both are loaded with all up-to-date hacking tools including scripts for easier usage and automatism. This package also includes special hardware like a high-power Wireless LAN adapter, a modified Bluetooth dongle and 2 wireless antennas for WLAN and Bluetooth hacking.

Finfisher Training

Basic Hacking Course
1 or 2 week basic hacking course covering up-to-date hacking
tools and techniques (using the FinFisher Hacking PC).
Topics included: Profiling, Attacking and many more.

- *Exploiting Software 1*

week course covering techniques to discover and exploit bugs in software.
Topics included: Software bugs, Shellcode, Exploit archives / frameworks, writing custom exploits, etc.

- *Root kits*

1 week course covering root kit / trojan horse techniques.
Topics included: Analysis, usage and development of professional
root kits.

- *Hacking VoIP*

1 week course covering various techniques to eavesdrop Voiceover-IP communication, get access to accounts and more.
Topics included: RTP sniffing, RTP injection, SIP account bruteforcing,
SIP password cracking, etc.

- *Wireless Hacking*

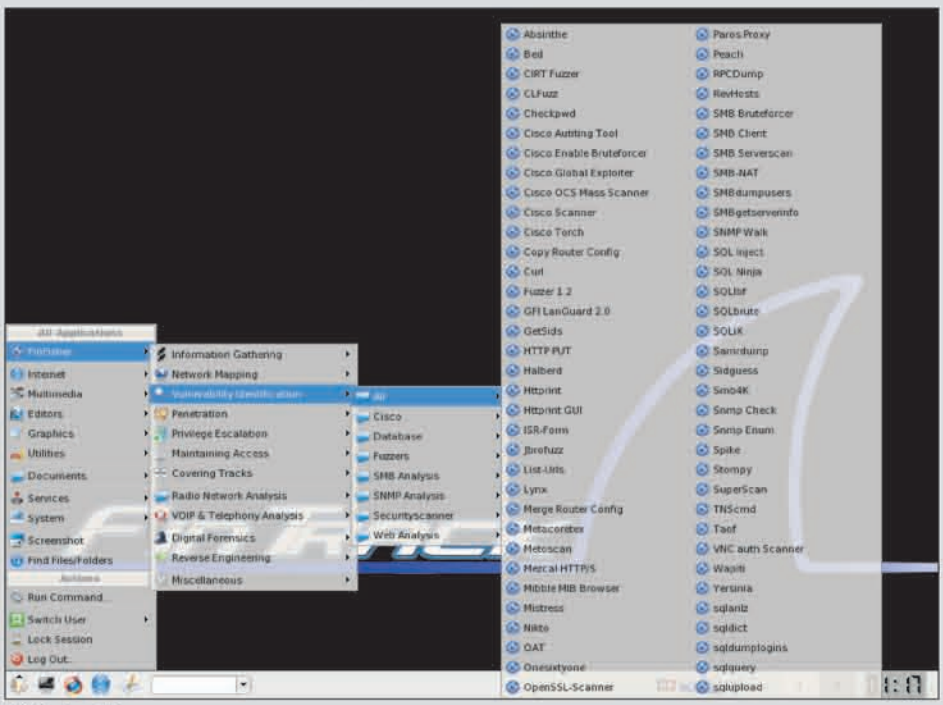
1 week course covering different Wireless hacking techniques including Wireless LANs, Bluetooth and wireless keyboards.
Topics included: WEP / WPA cracking, Bluetooth Sniffing and Link-
Key cracking, etc.

- *Covert Communication*

1 week course covering covert communication techniques and programs.
Topics included: Steganography, cryptography, network protocols, etc.

- *FinFisher Services*

FinAudit Professional 1 or 2 week penetration testing of local network to discover possible attack vectors and ensure the security of the network. Optional Alternatively, ask to join our restricted to government only oneday intrusion seminar.



FinFisher Menu

Recommended Finfisher Kits

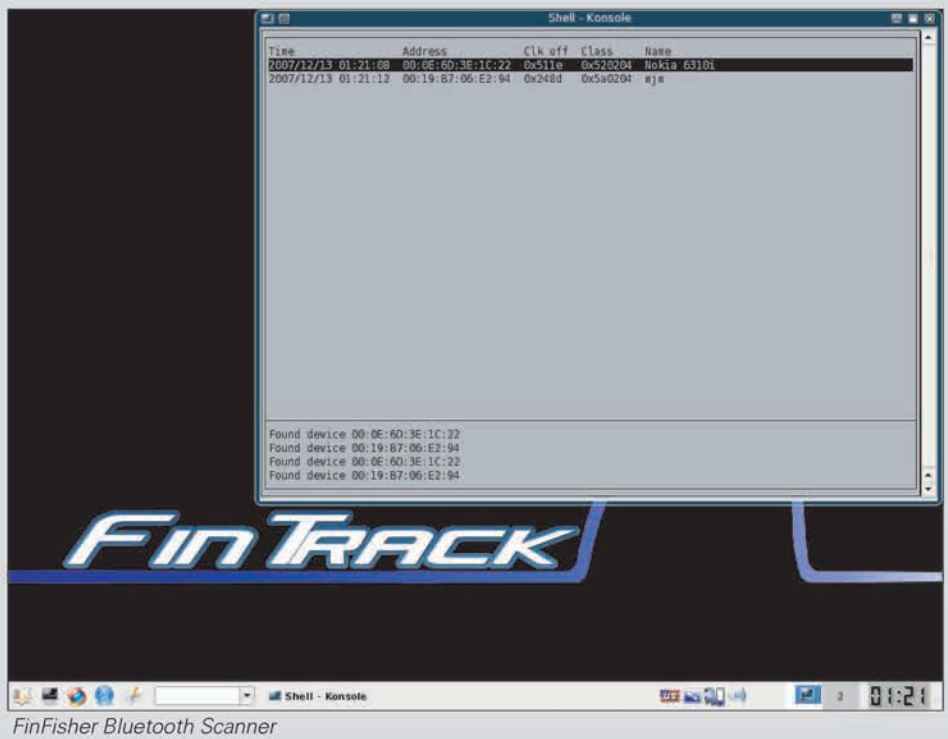
FinFisher Starter Kit
This kit includes FinFisher 1, 2, 3, HQ and the FinFisher Hacking PC kit.

FinFisher Software Kit
This kit includes only FinFisher 1, 2, 3 and HQ.

The FinFisher Project - Function and Purpose

In essence, it is an aggressive IT hacking component. It utilizes and incorporates Black Hat Hacking tactics to enable Intelligence Agencies to be able to gather information from target systems that would otherwise be extremely difficult to obtain legally.

The FinFisher Project operates on the understanding that there is a need for "authorized" Agencies to obtain information, using such methods, as they need to be pro-active against the strategies and tactics employed by their Targets. They can then alert the appropriate Law Enforcement or Military units and organizations within their country to intercept and prevent an incident, as opposed to reacting after. The System has also been developed with operational simplicity in mind, so that Intelligence operators require the minimum of technical ability and skill when using the tactical components within the FinFisher Project. The FinFisher Project is scalable, thus becoming more complex in capability and operation as the objectives of the user become more complex, and their knowledge and understanding of the Systems they are attacking become more advanced.



FinFisher Bluetooth Scanner

Appropriate Note

The FinFisher System has been developed to assist Intelligence Agencies obtaining information from civilian individuals and groups.
It is not intended, or has it been tested, to see if it has the capability to break into advanced complex government or military security systems with secret, or above security, classification.
Also, while every effort has been made to ensure the FinFisher Project can get past known Anti-Virus and Anti-Spyware Products and local Firewalls and Security, no guarantees are given in this area as these products are continuously being developed on a daily basis.

For further Information please don't hesitate to contact us under:

elaman GmbH
German Security Solutions

Seitzstraße 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81

info@elaman.de
www.elaman.de

HRB München 153662
Ust-IdNr.: DE814086265

Managing Director:
Holger Rumscheidt