Tails - Feature #5769
Applications audit

07/18/2013 07:46 AM - Tails

Status: Confirmed
Priority: Normal
Assignee:
Category:
Target version:
Feature Branch:
Type of work: Security Audit
Blueprint:

Start date:
Due date:
% Done: 80%
Estimated time: 0.00 hour
Spent time: 0.00 hour
Starter: No
Affected tool:

Description
Any included networked application needs to be analyzed for possible information leakages at the protocol level, e.g. if email clients leak the real IP address through the EHLO/HELO request etc.

This could be limited to applications whose protocol allows for such leakages.

General issues
The "claws with torsocks leaks hostname bug was fixed, but the fact that torsocks behaves worse than tssocks in this respect is worrying and should be investigated further. Perhaps other applications using torify are also affected?

Per-software sub-pages:

Resources
- iSECPartners' LibTech-Auditing-Cheatsheet

Subtasks:
Feature # 6117: Audit Pidgin
Feature # 6118: audit iceweasel config
Feature # 6115: Audit polipo
Feature # 6121: Audit Liferea
Feature # 6119: audit claws mail

History
#1 - 10/04/2013 06:36 AM - intrigeri
- Starter set to No

#2 - 10/04/2013 06:37 AM - intrigeri
- Type of work changed from Research to Audit

#3 - 06/09/2014 11:05 AM - BitingBird
- Subject changed from applications audit to Applications audit

#4 - 02/19/2016 12:43 AM - intrigeri
- Type of work changed from Audit to Security Audit