



**Adetti** Networking and Information Security ITIL research and development

## 2 Linux systems security – II

line

Characteristics  
Threats  
Tools  
Opportunities

- user mode / kernel mode separation
- POSIX 2.0
- Monolithic kernel
- 32-bit architecture (with existent 64 bit port)
- multitask / multiprocessing / multiuser

Linux.org/Security/Threats,ToolsAndOpportunities  
[Patch:ThreatsAndToolsAndOpportunities]

Adetti - 435 27 7020047 - 435 27 702000

http://www.adetti.it  
Adetti - 435 27 7020047 - 435 27 702000

5

**Adetti** Networking and Information Security ITIL research and development

## 2 Linux systems security – III

line

Characteristics  
Threats  
Tools  
Opportunities

- Linux functional features
- source code freely available
- centralized development team
- support: commercial and community

Linux.org/Security/Threats,ToolsAndOpportunities  
[Patch:ThreatsAndToolsAndOpportunities]

Adetti - 435 27 7020047 - 435 27 702000

http://www.adetti.it  
Adetti - 435 27 7020047 - 435 27 702000

6

**Adetti** Networking and Information Security ITIL research and development

## 2 Strengths

line

Characteristics  
Threats  
Tools  
Opportunities

- robustness
- price
- flexibility
- security
- lifetime
- hardware reuse
- connectivity
- Unix based

Linux.org/Security/Threats,ToolsAndOpportunities  
[Patch:ThreatsAndToolsAndOpportunities]

Adetti - 435 27 7020047 - 435 27 702000

http://www.adetti.it  
Adetti - 435 27 7020047 - 435 27 702000

7

**Adetti** Networking and Information Security ITIL research and development

## 2 Operating system robustness

line

Characteristics  
Threats  
Tools  
Opportunities

	Open Source	Closed Source
Fast bugs detection	Good	Good
Bug reporting	Good	Poor
Quick issue of patches	Good	Medium
Spotic development	Good	Good
Good architectural design	Medium	Medium

Linux.org/Security/Threats,ToolsAndOpportunities  
[Patch:ThreatsAndToolsAndOpportunities]

Adetti - 435 27 7020047 - 435 27 702000

http://www.adetti.it  
Adetti - 435 27 7020047 - 435 27 702000

Linux ROPhat: 11 days  
Microsoft: 16,1 days  
Sun: 50 days  
Security Portal

8

**Adetti** Networking and Information Security ITIL research and development

**2** line

Characteristics  
Threats  
Tools  
Opportunities

**Part II - Threats**

http://www.adetti.it  
Adetti - +39 02 7620047 - fax 02 7620000  
Linux and security threats, tools and opportunities  
(Part II: Threats) slides 09-10

**9**

**Adetti** Networking and Information Security ITIL research and development

**2** line

Characteristics  
Threats  
Tools  
Opportunities

**Weakness**

- non-supported hardware
- available software
- system administration

http://www.adetti.it  
Adetti - +39 02 7620047 - fax 02 7620000  
Linux and security threats, tools and opportunities  
(Part II: Threats) slides 10-11

**10**

**Adetti** Networking and Information Security ITIL research and development

**2** line

Characteristics  
Threats  
Tools  
Opportunities

**Some other points ...**

- trojans danger
- remote access to the machine
- 'open' services by default
- lack of maintenance and technical aid

http://www.adetti.it  
Adetti - +39 02 7620047 - fax 02 7620000  
Linux and security threats, tools and opportunities  
(Part II: Threats) slides 09-10

**11**

**Adetti** Networking and Information Security ITIL research and development

**2** line

Characteristics  
Threats  
Tools  
Opportunities

**Part III - Tools**

http://www.adetti.it  
Adetti - +39 02 7620047 - fax 02 7620000  
Linux and security threats, tools and opportunities  
(Part II: Threats) slides 11-12

**12**

**Adetti** Networking and Information Security ITIL research and development

## 2 Available tools for Linux II

### Main open-source advantages?

Reduced cost of application development or acquisition	93%
Reduced development or deployment time	72%
Reduced cost of maintaining applications	52%
Superior software quality	45%
Ability to customise and reuse software code	45%
Timely updates/patches	34.2% <small>INFOCIBUILD 2001</small>

Characteristics  
Threats  
Opportunities

<http://www.adetti.it>  
 Adetti - +39 02 7620047 - +39 02 7620000  
Linux and security threats, tools and opportunities  
(Patch Threats and tools in use)

13

**Adetti** Networking and Information Security ITIL research and development

## 2 Available tools for Linux I

- PGP and public key cryptography
- SSL, S-HTTP and S/MIME
- IPSEC implementation
- SSH (Secure Shell) and stunnel

Characteristics  
Threats  
Opportunities

<http://www.adetti.it>  
 Adetti - +39 02 7620047 - +39 02 7620000  
Linux and security threats, tools and opportunities  
(Patch Threats and tools in use)

14

**Adetti** Networking and Information Security ITIL research and development

## 2 Available tools for Linux II

- PAM – Pluggable Authentication Modules
- Kerberos
- CFS - Cryptographic File System
- StackGuard

Characteristics  
Threats  
Opportunities

<http://www.adetti.it>  
 Adetti - +39 02 7620047 - +39 02 7620000  
Linux and security threats, tools and opportunities  
(Patch Threats and tools in use)

15

**Adetti** Networking and Information Security ITIL research and development

## 2 Network administration platform

- Secure
- Not-expensive
- Complete from origin

Web site	63%
Server monitoring system	60%
Web site administration	60%
Application development testing	55%
Desktop configuration	40%
Event monitoring, configuration	37%
Web site index of pages to use on your website	33%
Database management	32%
Network security	25%
Storage management	10%
Customer applications	8%
Other	8%

Characteristics  
Threats  
Opportunities

<http://www.adetti.it>  
 Adetti - +39 02 7620047 - +39 02 7620000  
Linux and security threats, tools and opportunities  
(Patch Threats and tools in use)

16

**Adetti** Networking and Information Security ITIL research and development

## 2 Available Software I

### line Firewall

- Kernel iptables
- Frontends

Linux and security threats, tools and opportunities  
<http://www.adetti.it>  
 +39 02 7600641 - fax 02 7600600  
 (Photos: Trend Micro)

**Adetti** Networking and Information Security ITIL research and development

## 2 Available software II

### line Security auditing tools

- Nessus
- Saint

Linux and security threats, tools and opportunities  
<http://www.adetti.it>  
 +39 02 7600641 - fax 02 7600600  
 (Photos: Trend Micro)

**Adetti** Networking and Information Security ITIL research and development

## 2 Nessus

Linux and security threats, tools and opportunities  
<http://www.adetti.it>  
 +39 02 7600641 - fax 02 7600600  
 (Photos: Trend Micro)

**Adetti** Networking and Information Security ITIL research and development

## 2 Nessus

Linux and security threats, tools and opportunities  
<http://www.adetti.it>  
 +39 02 7600641 - fax 02 7600600  
 (Photos: Trend Micro)



**Adetti** Networking and Information Security ITIL research and development

**2** linux

Characteristics  
 Threats  
 Tools  
 Opportunities  
 Other sources

**Other sources (distributions)**

- <http://www.suse.com> | <http://www.redhat.com>

**Security**

- <http://www.linuxsecurity.com>
- <http://www.securityfocus.com>

**Software Tools**

- <http://www.freshmeat.net>

Linux and Security articles, books and opportunities  
 © Paulo Trezentos (adetti@isc.te.pt)

**Adetti** ITIL research and development  
 +351 21 7920047 - 21 12 735530

**25**

**Adetti** Networking and Information Security ITIL research and development

**2** linux

Characteristics  
 Threats  
 Tools  
 Opportunities

**Questions ?**

**Some security tools examples...**

**Paulo.Trezentos@adetti.iscte.pt**

**<http://paulo.trezentos.gul.p/articles/>**

Linux and Security articles, books and opportunities  
 © Paulo Trezentos (adetti@isc.te.pt)

**Adetti** ITIL research and development  
 +351 21 7920047 - 21 12 735530

**26**