Part I - Characterization

Linux systems security

- Critical since:
  - growth on the number of Linux servers
  - critical role of those servers
  - one compromised server, one compromised network
Linux systems security – II

- Linux technical features
  - user mode / kernel mode separation
  - POSIX 2.0
  - Monolithic kernel
  - 32 bit architecture (with existent 64 bit port)
  - multi tasking / multiprocessing / multiuser

Linux systems security – III

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

Strengths

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

Operating system robustness

<table>
<thead>
<tr>
<th>Feature</th>
<th>Open Source</th>
<th>Proprietary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast bug detection</td>
<td>Good</td>
<td>Poor</td>
</tr>
<tr>
<td>Bug reporting</td>
<td>Good</td>
<td>Poor</td>
</tr>
<tr>
<td>Quick issue of patches</td>
<td>Good</td>
<td>Medium</td>
</tr>
<tr>
<td>Total development</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Open architecture design</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Part II - Threats

- non-supported hardware
- available software
- system administration

Part III - Tools

- trojans danger
- remote access to the machine
- 'open' services by default
- lack of maintenance and technical aid
Available tools for Linux I
- PGP and public key cryptography
- SSL, S-HTTP and S/MIME
- IPSEC implementation
- SSH (Secure Shell) and telnet

Available tools for Linux II
- PAM – Pluggable Authentication Modules
- Kerberos
- CFS - Cryptographic File System
- StackGuard

Network administration platform
- Secure
- Not-expensive
- Complete from origin
Available Software I

Firewall
- Kernel iptables
- Frontends

Available Software II

Security auditing tools
- Nessus
- Saint
Part IV - Opportunities

Linux as platform for critical services
- secure and robust
- demanding in human resources concern
- commercial support already effective

Linux as security tool
- complete
- non-expensive
- good commercial offer (solutions, software,...)
Characterization

Threats

Tools

Opportunities

Other sources

Vendors (distributions)


Security

http://www.linuxsecurity.com

Software Tools

http://www.freshmeat.net

Questions?

Some security tools examples...

Some other sources...

http://paulo.trezentos.gul.pt/articles/