Linux and security: threats, tools and opportunities

Guide Share Europe 6th Technical Symposium

Paulo Trezentos
(Paulo.Trezentos@adetti.iscte.pt)

UNIDE / ISCTE Lisbon University

Berlin, 7-8 October 2002
Outline

- Linux characterization
- Threats
- Tools
- Opportunities
Part I - Characterization
**Linux systems security I**

- **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)
  - multitask / multiprocessing / multiuser
Linux systems security – III

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

Strengths

- robustness
- price
- flexibility
- security
- lifetime
- hardware reuse
- connectivity
- Unix based
## Operating system robustness

<table>
<thead>
<tr>
<th>Characterization</th>
<th>Open Source</th>
<th>Closed Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast bugs detection</td>
<td>Good</td>
<td>Good</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>Solid development</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Good architectural design</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

- **Linux RedHat**: 11 days
- **Microsoft**: 16.1 days
- **Sun**: 90 days

*Security Portal*
Part II - Threats
Weakness

- non-supported hardware
- available software
- system administration
Some other points ...

- **trojans danger**
- remote access to the machine
- 'open' services by default
- lack of maintenance and technical aid
Part III - Tools
Main *open-source* advantages?

<table>
<thead>
<tr>
<th>Characterization</th>
<th>Threats</th>
<th>Tools</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced cost of application development or acquisition</td>
<td>93%</td>
<td>Reduced development or implementation time</td>
<td>72%</td>
</tr>
<tr>
<td>Reduced cost of maintaining applications</td>
<td>52%</td>
<td>Superior software quality</td>
<td>45%</td>
</tr>
<tr>
<td>Ability to customize and reuse software code</td>
<td>45%</td>
<td>Timely updates/patches</td>
<td>34%</td>
</tr>
</tbody>
</table>

INFOWORLD 2001
www.infoworld.com
Available tools for Linux I

- PGP and public key cryptography
- SSL, S-HTTP and S/MIME
- IPSEC implementation
- SSH (Secure Shell) and \texttt{stelnet}
Available tools for Linux II

- **PAM** – Pluggable Authentication Modules
- **Kerberos**
- **CFS** - Cryptographic File System
- **StackGuard**
## Network administration platform

- **Secure**
- **Not-expensive**
- **Complete from origin**

### Tools

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server</td>
<td>65%</td>
</tr>
<tr>
<td>Server operating system</td>
<td>61%</td>
</tr>
<tr>
<td>Web-application server</td>
<td>45%</td>
</tr>
<tr>
<td>Application development testing</td>
<td>45%</td>
</tr>
<tr>
<td>Desktop operating system</td>
<td>38%</td>
</tr>
<tr>
<td>E-mail, messaging, or collaboration</td>
<td>30%</td>
</tr>
<tr>
<td>We are not using or planning to use open-source software</td>
<td>28%</td>
</tr>
<tr>
<td>Network management</td>
<td>25%</td>
</tr>
<tr>
<td>Database management</td>
<td>25%</td>
</tr>
<tr>
<td>Network security</td>
<td>25%</td>
</tr>
<tr>
<td>Storage management</td>
<td>10%</td>
</tr>
<tr>
<td>E-commerce applications</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>8%</td>
</tr>
</tbody>
</table>

INFOWORLD: 2001
www.infoworld.com
Available Software I

Firewall

- Kernel iptables
- Frontends
Available software II

Security auditing tools

- Nessus
- Saint
Characterization
Threats
Tools
Opportunities
Linux and security: threats, tools and opportunities
(Paulo.Trezentos@adetti.iscte.pt)
Nessus

Characterization

Threats

Tools

Opportunities

Improperly configured LDAP servers will allow any user to connect the server and query for information.

The LDAP bind function in Exchange 5.5 has a buffer overflow that allows a remote attacker to conduct a denial of service or execute commands in all version prior to Exchange server sp2.

Note: no test was done to see what version of Exchange server is running, nor attempt to verify service pack.

Solution: Disable NULL BIND on your LDAP server
Also see: http://www.microsoft.com/technet/security/bulletin/ms99-0
Risk factor: Medium
CVE: CVE-1999-0385
Available software III

Intrusion Detection Systems

- snort
- tripwire (digital signature), scanlogd

Event logging

- syslogd
- Iplog / Iptraf
Part IV - Opportunities
Conclusion

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,...)
### Other sources

#### Vendors (distributions)
- [http://www.suse.com](http://www.suse.com) | [http://www.redhat.com](http://www.redhat.com)

#### Security
- [http://www.linuxsecurity.com](http://www.linuxsecurity.com)
- [http://www.securityfocus.com](http://www.securityfocus.com)

#### Software Tools
- [http://www.freshmeat.net](http://www.freshmeat.net)
Questions?
Some security tools examples...

Paulo.Trezentos@adetti.iscte.pt

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