Securing your Linux Server: Racing against the attacker

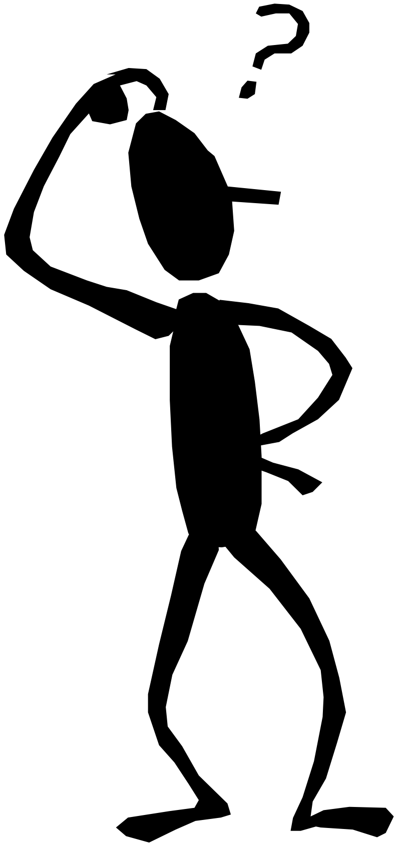
Nigel Edwards
Hewlett-Packard
<nigel_edwards@hp.com>

HP WORLD 2002
Conference & Expo

Agenda

- The major source of security vulnerabilities
- Security strategies
  - Patching
  - Layered utilities (Nessus, Snare, Snort..)
  - Kernel hardening (HP Secure OS Software for Linux or hp-lx (se))

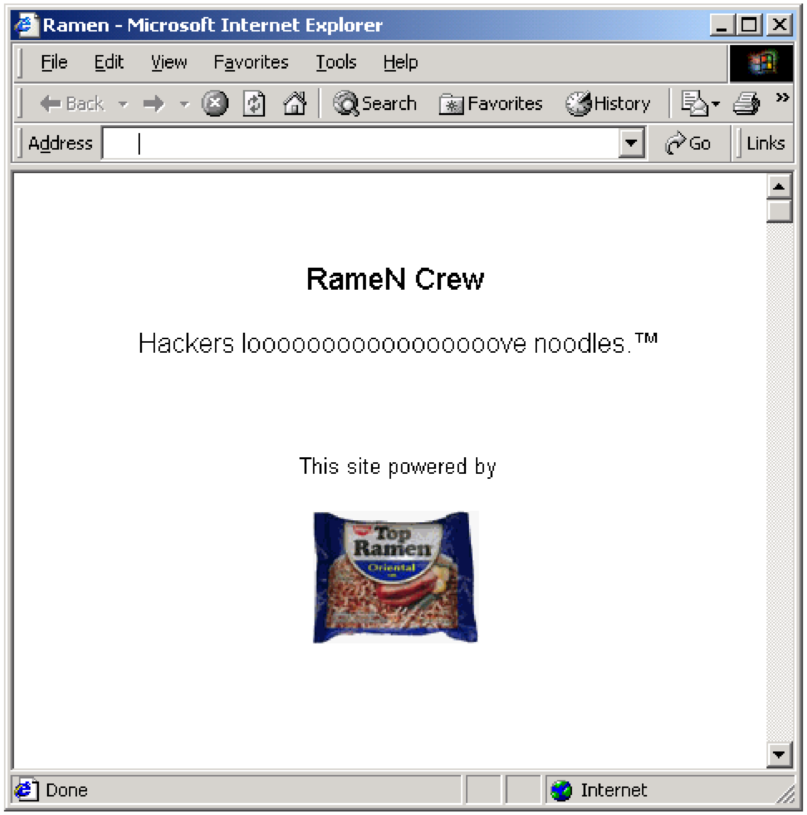
What's the nature of the problem?



- Bugs are the major source of vulnerabilities
  - Application bugs account for about 80%
- CERT issued 37 security advisories in 2001
  - http://www.cert.org/advisories/
  - 30 concerned bugs in applications
  - 4 concerned bugs in "appliances"
  - 2 did not concern bugs
  - Only 1 general purpose kernel bug

An example of a bug exploit in Linux

- The Ramen worm
- Expoited (buffer overflow) bugs in:
    - Rpc.statd
    - Wu-ftpd
    - LPRng
- Root access gained
- Executables overwritten
- Web pages defaced
- Network probed for other vulnerable hosts



RameN Crew

Hackers looooooooooooooooove noodles.™

This site powered by

Root Kits

- Hide the attackers presence
- Allow repeated use of the system by attackers
- Two variants
  - Updated system binaries
  - Loadable kernel module

Patching

- Security Alerts
  - Vendor security bulletins
  - Bugtraq, CERT, etc, …
  - Managed services e.g. Security Focus
- Automated services
  - Aduva - http://www.aduva.com/
  - Red Hat - https://rhn.redhat.com/

Problems with Patching

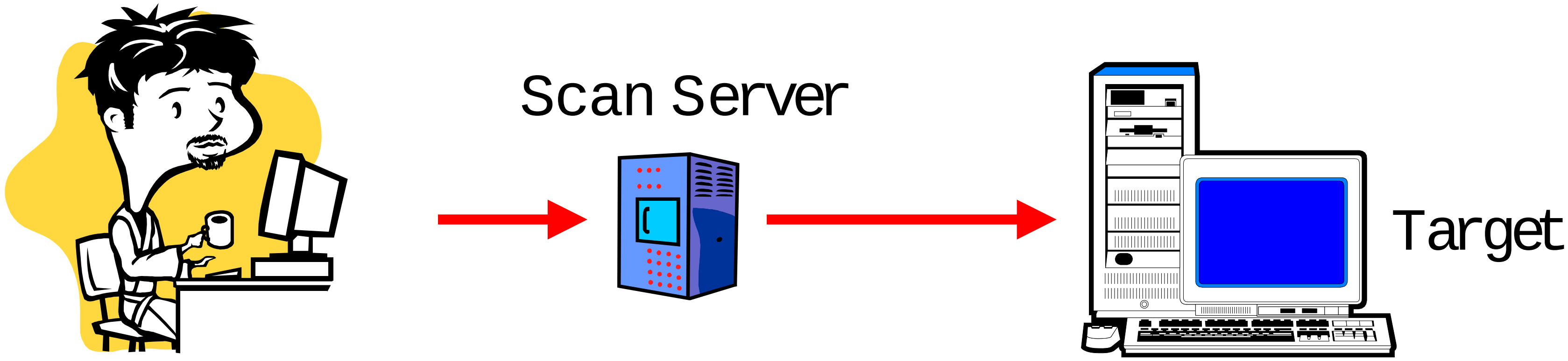
- Not all problems are known – you may be victim before the patch is available or before you can apply the patch
- The attackers are reading the same information sources
  - who is going to win…..?

Tools and utilities

- Bastille
  - (http://www.bastille-linux.org/)
- Local system scanners (e.g. Tiger)
  - (http://savannah.gnu.org/projects/tiger/)
- Remote system scanners (e.g. Nessus)
- Intrusion detection (Snort)
- Audit (Snare)
- Psionic PortSentry, HostSentry and LogCheck
  - (http://www.psionic.com/)
- Tripwire

(Remote) System Scanners

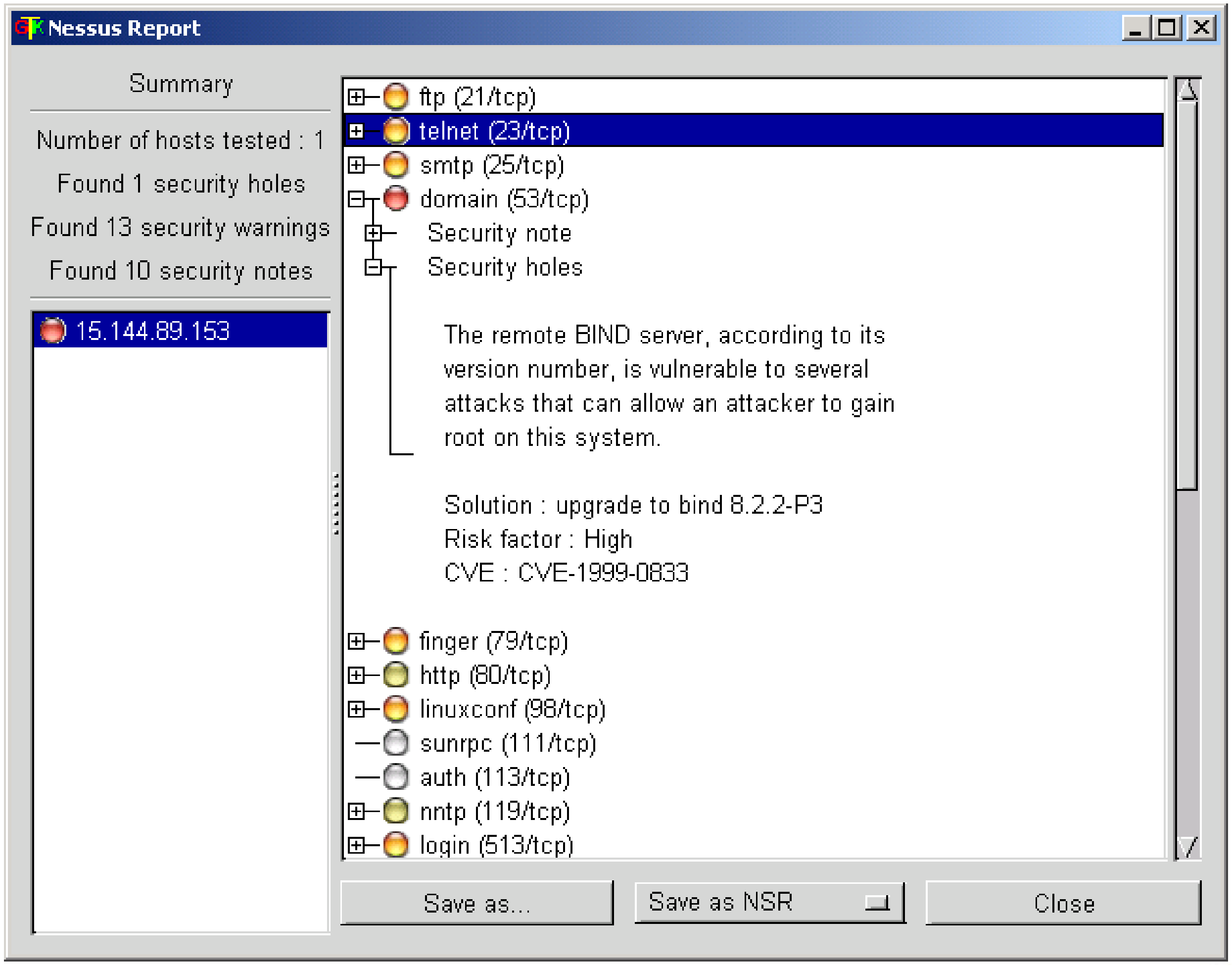
- Nessus
  - http://www.nessus.org/
- Internet Security Systems System Scanner
  - http://www.iss.net/
- And many more



Scan Server

Target

Nessus



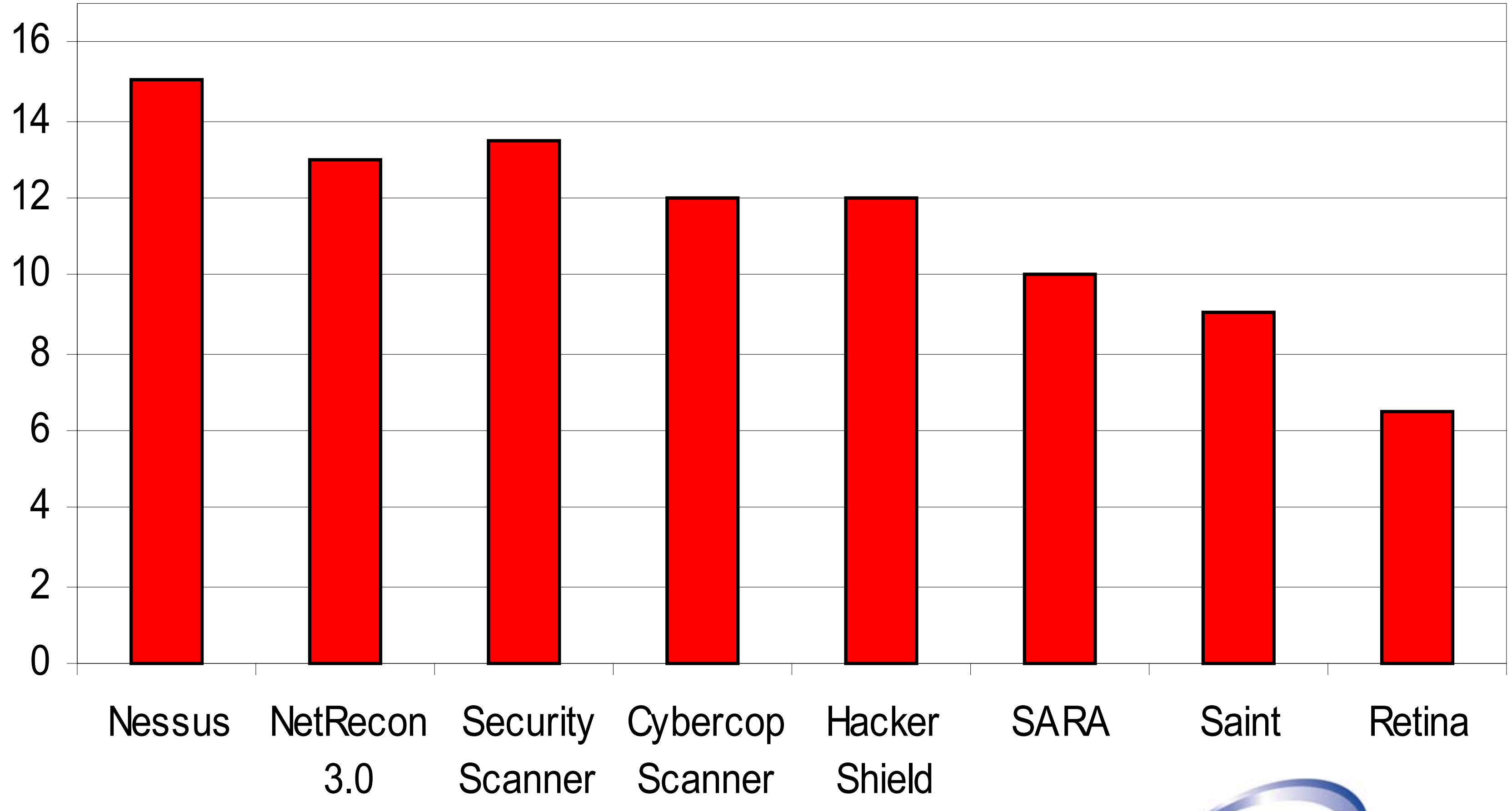
```
Summary

Number of hosts tested : 1
Found 1 security holes
Found 13 security warnings
Found 10 security notes

15.144.89.153
```

```
ftp (21/tcp)
telnet (23/tcp)
smtp (25/tcp)
domain (53/tcp)
  Security note
  Security holes

    The remote BIND server, according to its
    version number, is vulnerable to several
    attacks that can allow an attacker to gain
    root on this system.

    Solution : upgrade to bind 8.2.2-P3
    Risk factor : High
    CVE : CVE-1999-0833

finger (79/tcp)
http (80/tcp)
linuxconf (98/tcp)
sunrpc (111/tcp)
auth (113/tcp)
nntp (119/tcp)
login (513/tcp)
```

Scanner effectiveness

100% = 17

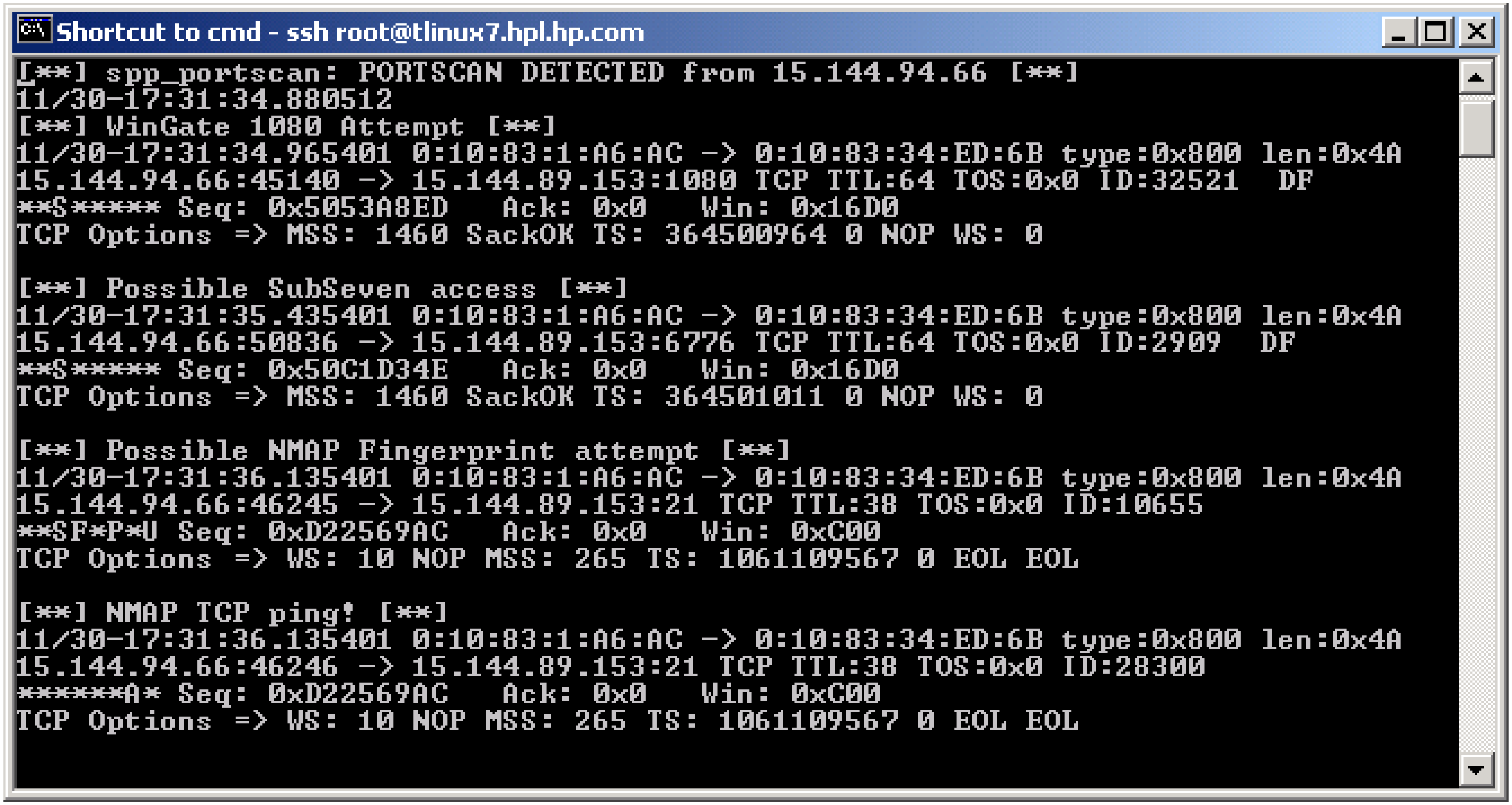
Source: Network Computing January, 2001
http://www.networkcomputing.com/



Snort intrusion detection system

- Packet sniffer and logger
- Potentially can detect various attacks including:
  - Port scans
  - Buffer overflows…
- http://www.snort.org/
- See also tcpdump

Snort – example output



```
[**] spp_portscan: PORTSCAN DETECTED from 15.144.94.66 [**]
11/30-17:31:34.880512
[**] WinGate 1080 Attempt [**]
11/30-17:31:34.965401 0:10:83:1:A6:AC -> 0:10:83:34:ED:6B type:0x800 len:0x4A
15.144.94.66:45140 -> 15.144.89.153:1080 TCP TTL:64 TOS:0x0 ID:32521  DF
**S***** Seq: 0x5053A8ED   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 364500964 0 NOP WS: 0

[**] Possible SubSeven access [**]
11/30-17:31:35.435401 0:10:83:1:A6:AC -> 0:10:83:34:ED:6B type:0x800 len:0x4A
15.144.94.66:50836 -> 15.144.89.153:6776 TCP TTL:64 TOS:0x0 ID:2909  DF
**S***** Seq: 0x50C1D34E   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 364501011 0 NOP WS: 0

[**] Possible NMAP Fingerprint attempt [**]
11/30-17:31:36.135401 0:10:83:1:A6:AC -> 0:10:83:34:ED:6B type:0x800 len:0x4A
15.144.94.66:46245 -> 15.144.89.153:21 TCP TTL:38 TOS:0x0 ID:10655
**SF*P*U Seq: 0xD22569AC   Ack: 0x0   Win: 0xC00
TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] NMAP TCP ping! [**]
11/30-17:31:36.135401 0:10:83:1:A6:AC -> 0:10:83:34:ED:6B type:0x800 len:0x4A
15.144.94.66:46246 -> 15.144.89.153:21 TCP TTL:38 TOS:0x0 ID:28300
******A* Seq: 0xD22569AC   Ack: 0x0   Win: 0xC00
TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL
```

Tripwire(& friends)

- Intrusion detection
- Periodically (e.g. daily) scans files to detect changes
- Email notification to administrator
  - Update tripwire database or…
  - Manually revert file
- Included in some distributions (e.g. Red Hat 7.1)
  - http://www.tripwire.org/
- Chkrootkit
  - http://www.chkrootkit.org/

Limitations of patching and layered security utilities

- Not all vulnerabilities and bugs are known
  - A patch may not be available
  - You may not apply the patch in time

- Two types of layered utilities
  - Signature based
    - Not 100% of known vulnerabilities
    - Useless against unknown vulnerabilities

  - State monitoring
    - Detection not prevention
- Kernel root kits are extremely difficult to detect

Agenda

- The major source of security vulnerabilities
- Security strategies
  - Patching
  - Layered utilities (Nessus, Snare, Snort..)
  - Kernel hardening (HP Secure OS Software for Linux or hp-lx (se))

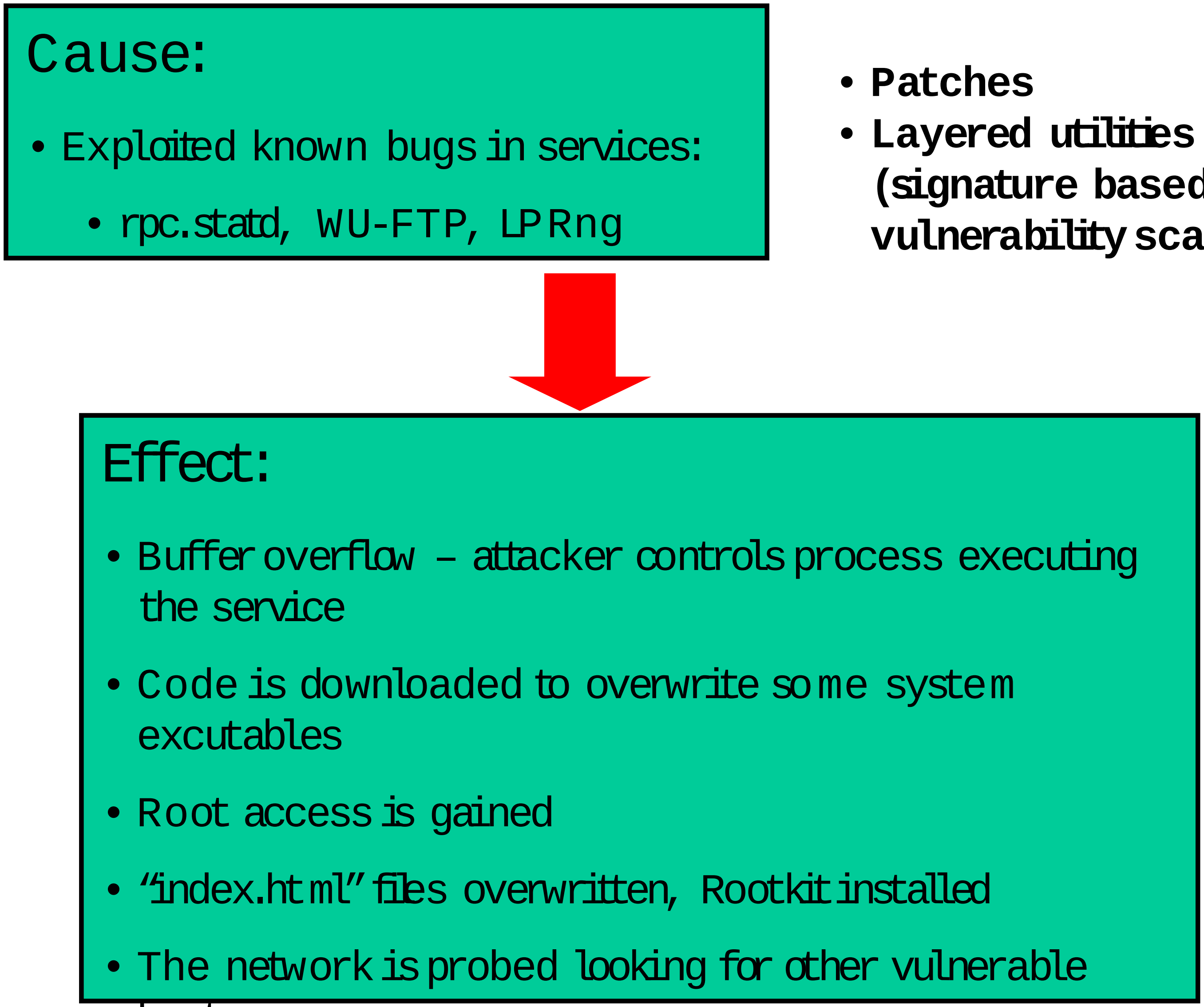
Kernel hardening – “The philosophy of Containment”

- Bugs are inevitable
- You cannot not know what a program will do until it runs
- Misconfiguration and administration errors are inevitable
- Attempt to contain the damage
  - “A sandbox” limits access to system and network resources
  - Control access to privilege (e.g. root)

Kernel hardening – historical challenges

- Can require extensive integration work to “port” an application or service
- Administration complexity
- Kernel code changes
- Recent newer models such as hp-lx (se) have improved the situtation

An Attack Pathology



Cause:

- Exploited known bugs in services:
  - rpc.statd, WU-FTP, LPRng

Effect:

- Buffer overflow – attacker controls process executing the service
- Code is downloaded to overwrite some system excutables
- Root access is gained
- “index.html” files overwritten, Rootkit installed
- The network is probed looking for other vulnerable hosts

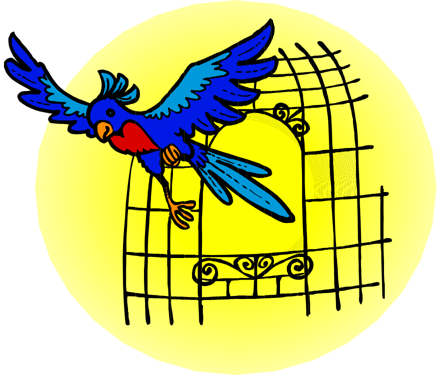
- **Patches**
- **Layered utilities (signature based IDS, vulnerability scanners,..)**

- **Detection:**
  - **Audit**
  - **Non-signature base IDS**
- **Prevention:**
  - **Kernel hardening**

Discretionary access control (DAC)

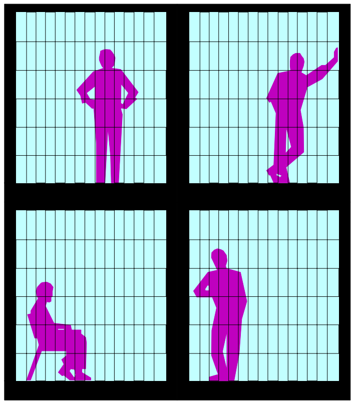
```
-rw-r--r--   1 nje        users      3083399 Nov 18  1998 BellLaPadula.pdf
-rw-r--r--   1 nje        users      8082702 Nov  1  2000 ande72.pdf
-rw-r--r--   1 nje        users      1580903 Nov  1  2000 ande80.pdf
-rw-r--r--   1 nje        users       433265 Nov  1  2000 dod85.pdf
```

- File owner can grant access to anybody
- DAC does not give good containment properties
  - Users can change who gets access to different parts of the system
  - Users can be tricked into updating files which they own to introduce “Trojan Horses”



CONTAINMENT ✗

Mandatory Access Control (MAC)



CONTAINMENT

- Mandatory Access Control
  - Access control beyond the discretion of the owner
  - Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December, 1985
- Important for protecting sensitive files
  - Web pages, executables, …
  - Important for protecting other system resources
  - E.G. communication channels
- Important for constraining the user/process to a known part of the system - CONTAINMENT

What is hp-lx (se)?

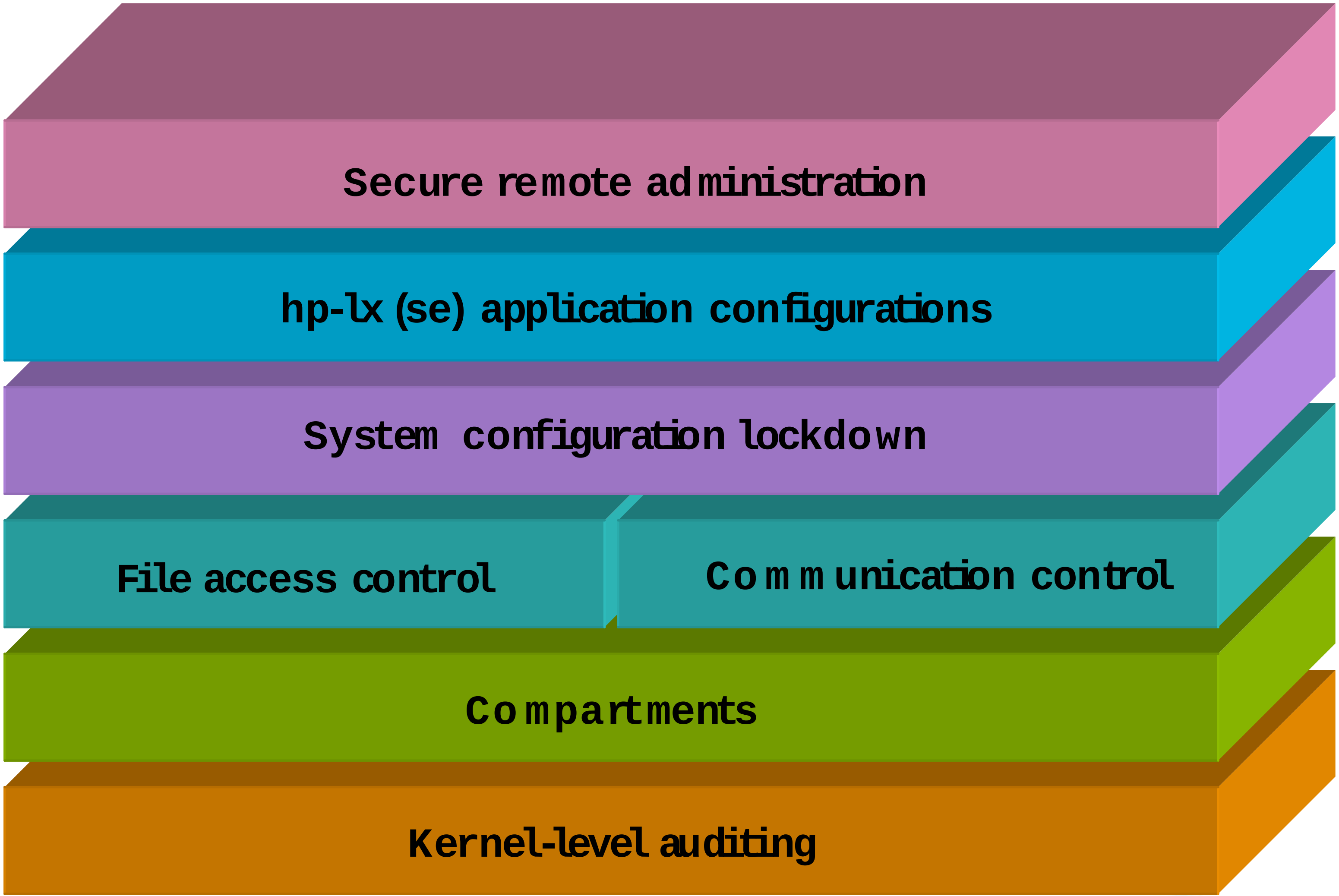
- A highly secure version of Linux for running applications and services
- Service provider focus
- Building on the success of HP Virtualvault
  - Balance ease of use with security
- A new security model focused on Internet services and applications
- Minimal kernel changes
  - Binary compatible with Red Hat 7.1
- HP will deliver:
  - Example services (e.g. Apache)
  - SDK and (eventually) integration tools

hp-lx (se) breakthrough manageability

"We chose HP Secure OS for Linux because of its ease of use and administration and for its superior security features.“

Konstantin Agouros
Manager, Competence Team Security
NetAge Solutions
http://www.netage.de/

Review of major features



Secure remote administration

hp-lx (se) application configurations

System configuration lockdown

File access control

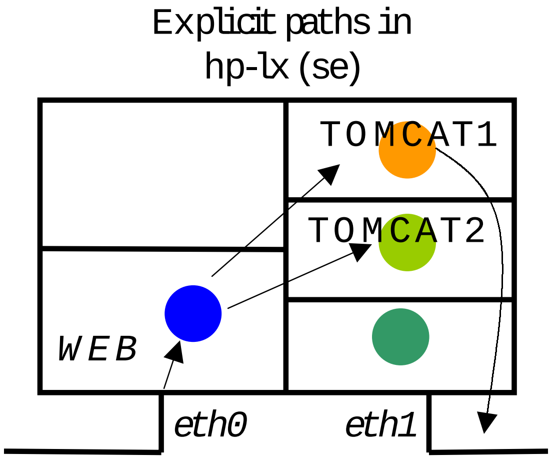
Communication control

Compartments

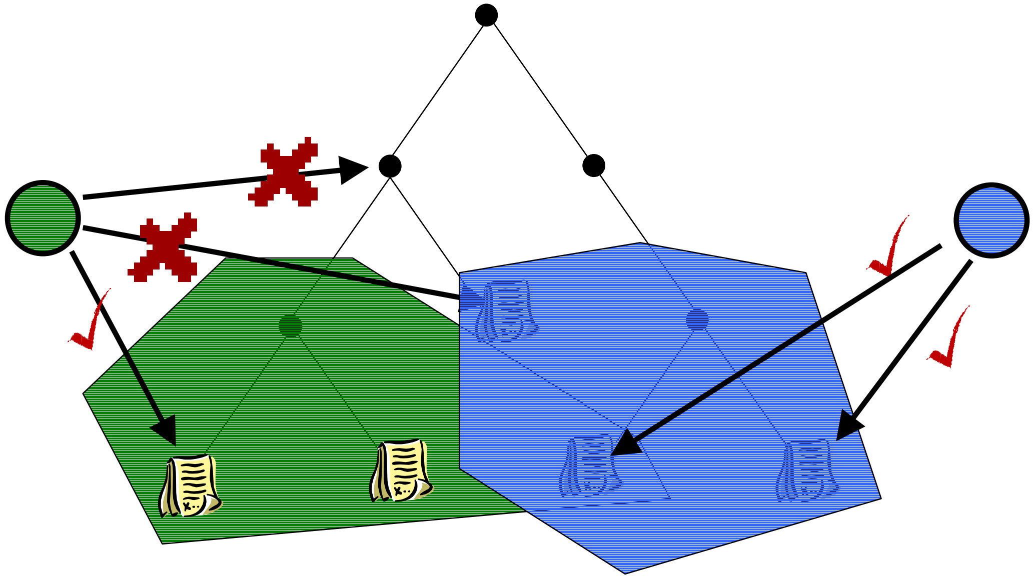
Kernel-level auditing

HP-LX compartment communication rules

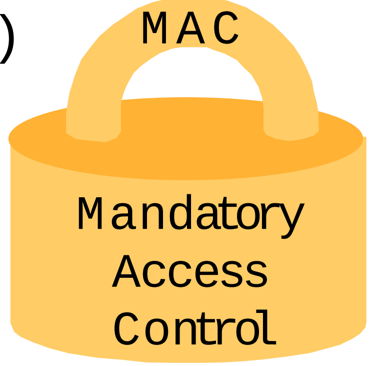
```
HOST:* -> COMPARTMENT:WEB
                    METHOD TCP PORT 80 NETDEV eth0

COMPARTMENT:WEB -> COMPARTMENT:TOMCAT1
                    METHOD TCP PORT 8007 NETDEV lo

COMPARTMENT:WEB -> COMPARTMENT:TOMCAT2
                    METHOD TCP PORT 8008 NETDEV lo

COMPARTMENT:TOMCAT1 -> HOST:SERVER1
                    METHOD TCP PORT 8080 NETDEV eth1
```



HP-LX file system protection

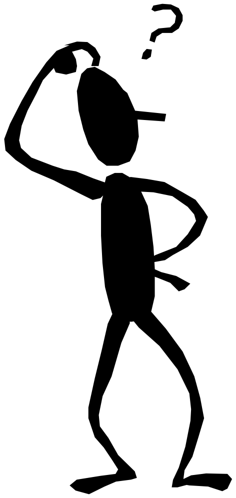


- File Control Table specifies compartment access: read, write, append
- Fine-grain control and coarse grain (per file, per directory)



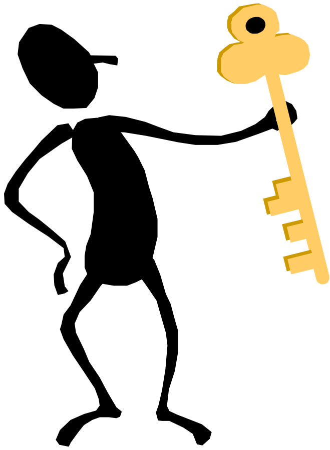
```
web /compt/web                read
web /compt/web/tmp            read,write
web /compt/web/dev            read,write
web /compt/web/apache/logs    read,write
```

- Tripwire – Integrity protection

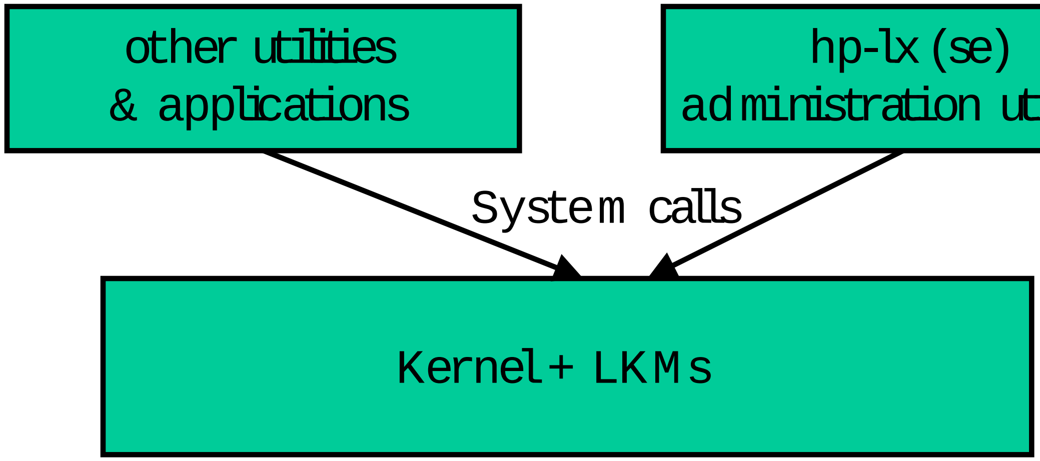


Why is kernel-level Auditing important?

Answer: it is very hard to by-pass



A secure administration model (1/2)

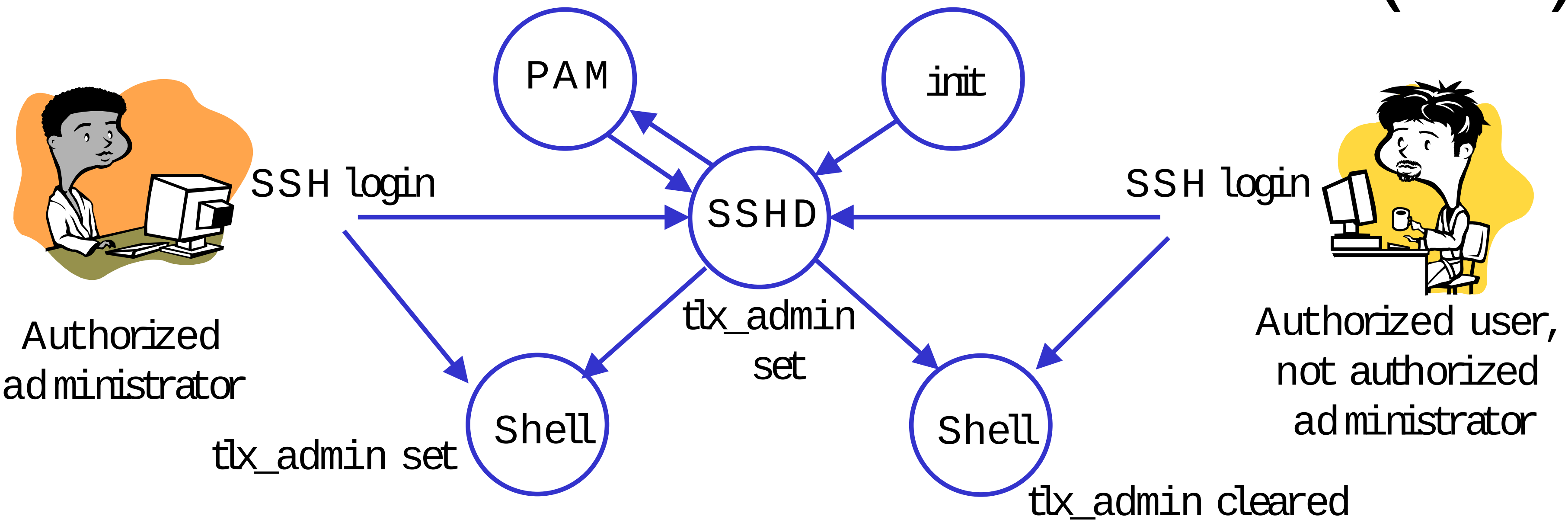


hp-lx (se) management utilities

- Create, destroy, start, stop compartments
- Configure communication rules for compartments
- Manage audit system

How do we stop the abuse of the system calls used for this?

A secure administration model (2/2)



PAM

init

SSHD

SSH login

SSH login

Authorized administrator

Authorized user, not authorized administrator

tlx_admin set

Shell

tlx_admin set

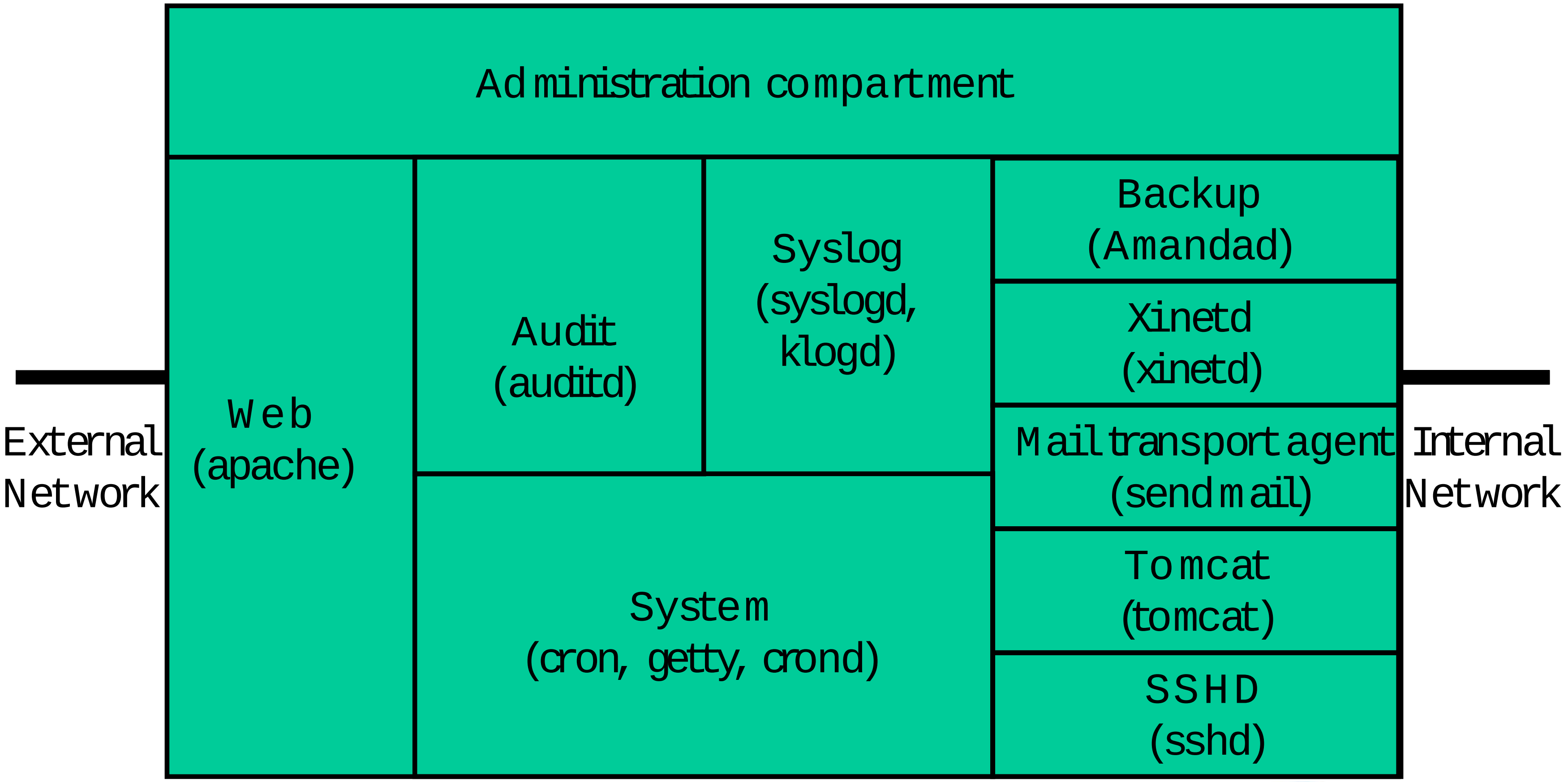
Shell

tlx_admin cleared

Each process has an additional attribute:

- The tlx_admin bit
- Code inside kernel checks for this bit before executing administration functions
- Works in parallel to Linux capability mechanism (which we also use)
- A more restricted management model than capabilities

Typical hp-lx (se) compartment configuration



Administration compartment

External Network

Web (apache)

Audit (auditd)

Syslog (syslogd, klogd)

System (cron, getty, crond)

Backup (Amandad)

Xinetd (xinetd)

Mail transport agent (sendmail)

Tomcat (tomcat)

SSHD (sshd)

Internal Network

Conclusion

- Patching
  - Window of vulnerability leads to race condition
- Application level utilities
  - Signature based
    - Window of vulnerability leads to race condition
    - Not 100% effective
  - State monitoring
    - Detection not prevention
- Kernel hardening e.g. hp-lx (se)
  - Containment prevents known and UNKNOWN attacks