COMP 175

System Administration and Security

PACKAGES AND APPLICATIONS

Packages and Applications

- Objectives
- Upon completion you will:
  - Understand the concept of package tools
  - Be able to install packages on a system
  - Understand the concept of tuning
  - Understand the security risk potential from misconfigured and unpatched applications

Implementing A Web Server

Upon completion you should be able to:

- Install and configure a web server
- Monitoring the server's load and performance
- Configure Maximum requests, servers
- Restricting client user access
- Configure support for scripting languages

Basic Utilities

- Directory/File management: cd, ls, pwd, mkdir, rmdir, cp, mv, rm, find, du, file
- File viewing/editing: touch, more, less, ed, vi, emacs
- User management: passwd, chmod, chown, su, who
- Process management: kill, killall, ps
- Documentation: man, info, /usr/share/doc

Applications: X11, KDE, Gnome, OpenOffice, Apache, Sendmail, Gimp, Mozilla, Firefox

Security Software: gpg, ssh, iptables, ACID, snort, prelude, tcpdump, ethereal, nmap, nessus, tcpspy, tiger, ClamAV, spamassassin

Fuel to the Fire

Adding More Software to the System?

- Old school method
  - Download source, make, compile
    - gcc captures
- New school method - Package Managers
  - Lowers the skillsets needed
  - Easier for support
  - Fewer problems with libraries
    - Static libraries
    - Shared libraries - dynamic linking

Packages Lessen Library Issues

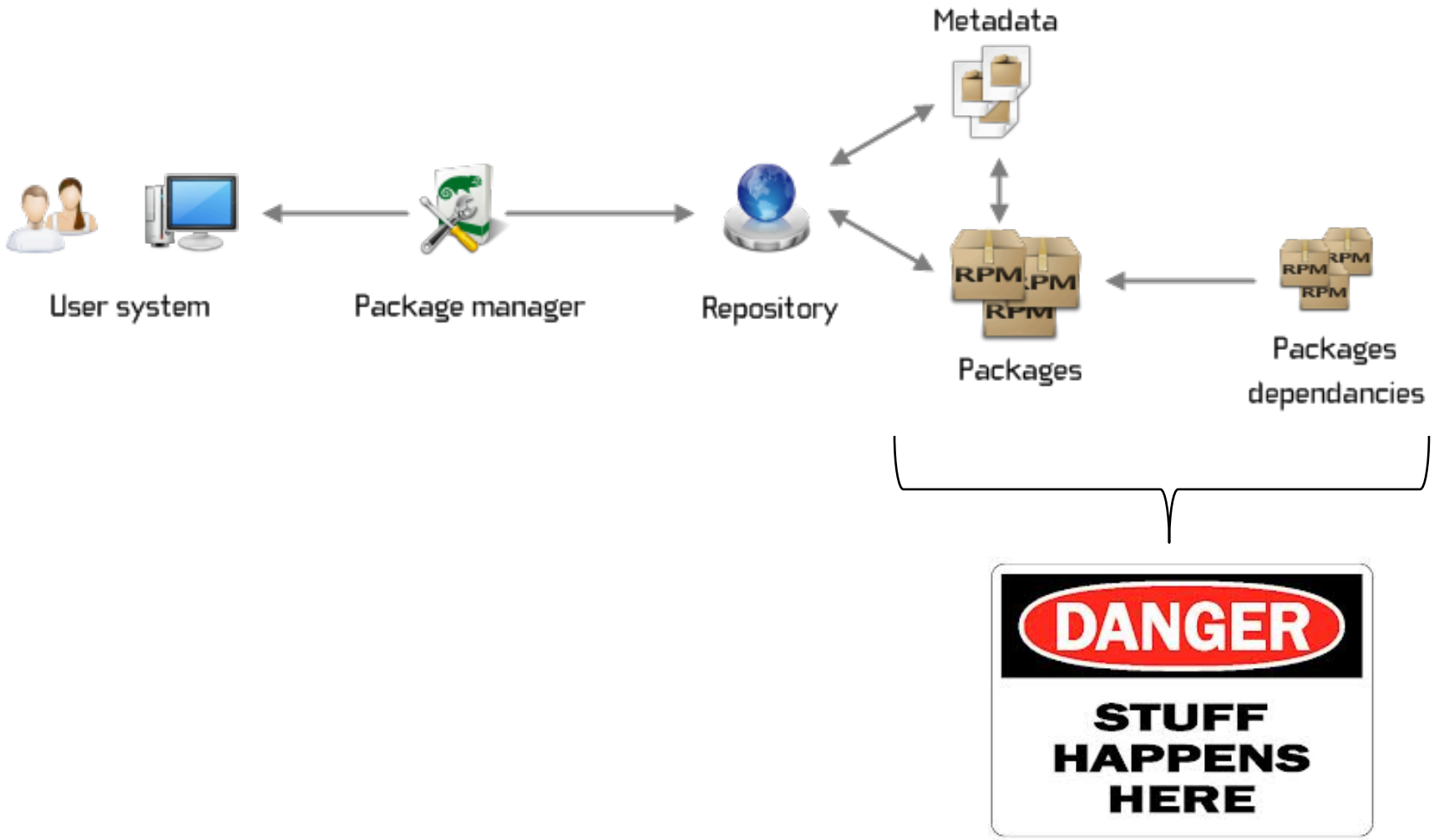
- *Note: Windows equiv. issue caused = DLL hell*
- Applications
  - Program code + static libraries
  - Program code + dynamic link to shared object libraries
- Managing shared library paths
  - set the LD_LIBRARY_PATH (sub-optimal)
- Linux
  - Edit `/etc/ld.so.conf` run `ldconfig`
- Solaris
  - `crle` Configure Runtime Linking Environment
  - Named after clueless Stooge?

Package Management

Package Management Features

- Tools to install, update, remove, and manage
- Install and upgrade software across network
- Indicate what package a file is in, or the files a package contains, e.g., where is /bin/ls
- Maintain a database of packages and their status
- Manage dependency checking
- Signature verification with GPG, PGP, MD5, etc.
- Tools to build packages

Package Managers



Package Tools

Ubuntu (Debian)

- Creating Packages – See online documentation
- Package Installers – from repositories
  - apt-get - Advanced Packaging Tool
    - commonly used CLI packaging tool
- Front end GIU's to apt
  - Synaptic Package Manager
    - No longer installed by default since 11.10
    - Didn't support ratings and reviews
  - Ubuntu Software Center
- Update Manager – updates/patches software

Major Packaging Systems

- RPM – Red Hat Package Manager
  - Used on Red Hat, SUSE, etc. systems
  - *package-version-release.architecture.rpm*
  - e.g. **coreutils-7.10-18.fc9.i386.rpm**
- Debian GNU/Linux Package Manager dpkg
  - Used on Debian/Ubuntu, others
  - *package_version-revision_architecture.deb*
  - e.g. **coreutils_7.10-5ubuntu_i386.deb**
  - dpkg –i filename.deb
    - -l list of installed packages
    - r remove an installed package

Package Tools

RedHat, Fedora

- rpm – CLI
- *yum* – Yellow dog Updater, Modified

SuSE

- YaST - Yet another Setup Tool
- Zypp - Package manager for YaST

Slackware

- pkgtool
  - "Dependency management is left up to the sysadmin"

Solaris

- Solaris Package Manager

Snappy Package Manager

- Snappy - software deployment and package management system
- Originally designed/built by Canonical for the Ubuntu phone operating system.
- Packages called 'snaps'
- Tool for using them 'snapd'
- Work across a range of Linux distributions
- Allow distro-agnostic software deployment
- Designed to work for phone, cloud, internet of things (IoT)and desktop computing

snapcraft.io

Flatpak

- Flatpak - software deployment, package management, and application virtualization for Linux desktop computers
- Provides a sandbox environment for applications in isolation from the rest of the system
- Requires permission from the user to control hardware devices or access user's files
- Developed by freedesktop.org project (X Desktop Group)
  - Formerly xdg-app

yum

yum does dependency checking

- yum install packages
- yum info
- yum list
- yum remove package
- yum update
- yum upgrade

apt-get

- Does dependency checking and management
  - Avoids dependency hell (MS DLL's)
- /etc/apt sources list, configuration files
- APT relies on the concept of repositories
- Syntax
  - apt-get update
  - apt-get install package
  - apt-get upgrade
  - apt-get remove package
  - apt-get dist-upgrade *non-trivial undertaking*

apt-get in Action

`$traceroute` Command not found?

- Ubuntu Desktop lacks `traceroute` !
  - Even *Windows* includes `tracert`
  - "Desktop users don't need network debugging tools"
  - Yet it includes traceroute6 for IPv6
  - `tracepath` is *not* `traceroute` (try)
  - `mtr` – mytraceroute is nice – *but*..... (try)
- Standards are standards
- Use `apt install net-tools`
- P.S. Upgrade from 11.04 to 11.10 removed it
  - Distro update *removes* added packages?

apt-get in Action

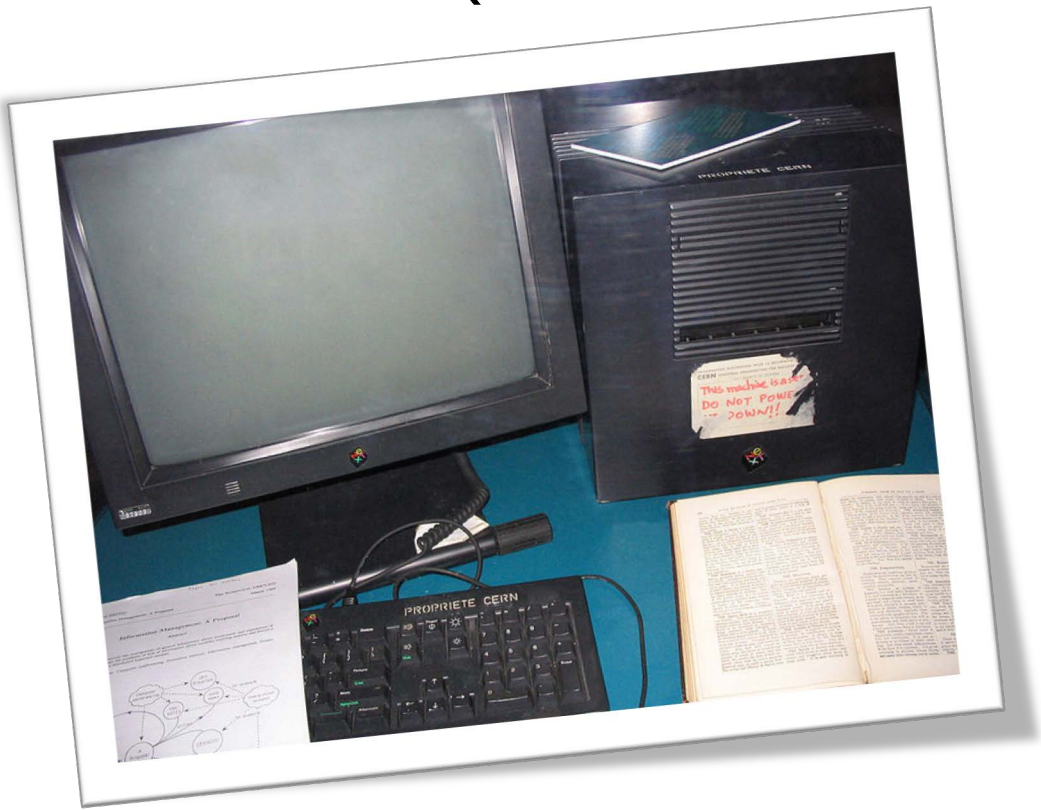
```
mmaxwell@ubuntu:~$ traceroute www.treacle.com
The program 'traceroute' is currently not installed.  You can install it by typi
ng:
sudo apt-get install traceroute
mmaxwell@ubuntu:~$ sudo apt-get install traceroute
[sudo] password for mmaxwell:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 341 not upgraded.
Need to get 52.8kB of archives.
After this operation, 180kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/ maverick/universe traceroute i386 1:2
.0.14-1 [52.8kB]
Fetched 52.8kB in 1s (32.0kB/s)
Selecting previously deselected package traceroute.
(Reading database ... 119499 files and directories currently installed.)
Unpacking traceroute (from .../traceroute_1%3a2.0.14-1_i386.deb) ...
Processing triggers for man-db ...
Setting up traceroute (1:2.0.14-1) ...
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute
 (traceroute) in auto mode.
```

Installing Packages

- Simple Package Installation
- Complex Package Installation
  - Design Considerations
  - Performance Considerations
- Installing and configuring a webserver
- Webservers can be found running on webcams, printers, power strips, switches, routers, etc.
- A webserver provides a platform for distribution, documentation, web applications, monitoring, etc. whether it's for a local Intranet, the global Internet, or your home

Install a Web Server

- In 1989 Tim Berners-Lee proposed a new project at CERN with the goal of easing the exchange of information between scientists by using a hypertext system (a subset of SGML). He wrote the world's first web server (it ran on NeXTSTEP)

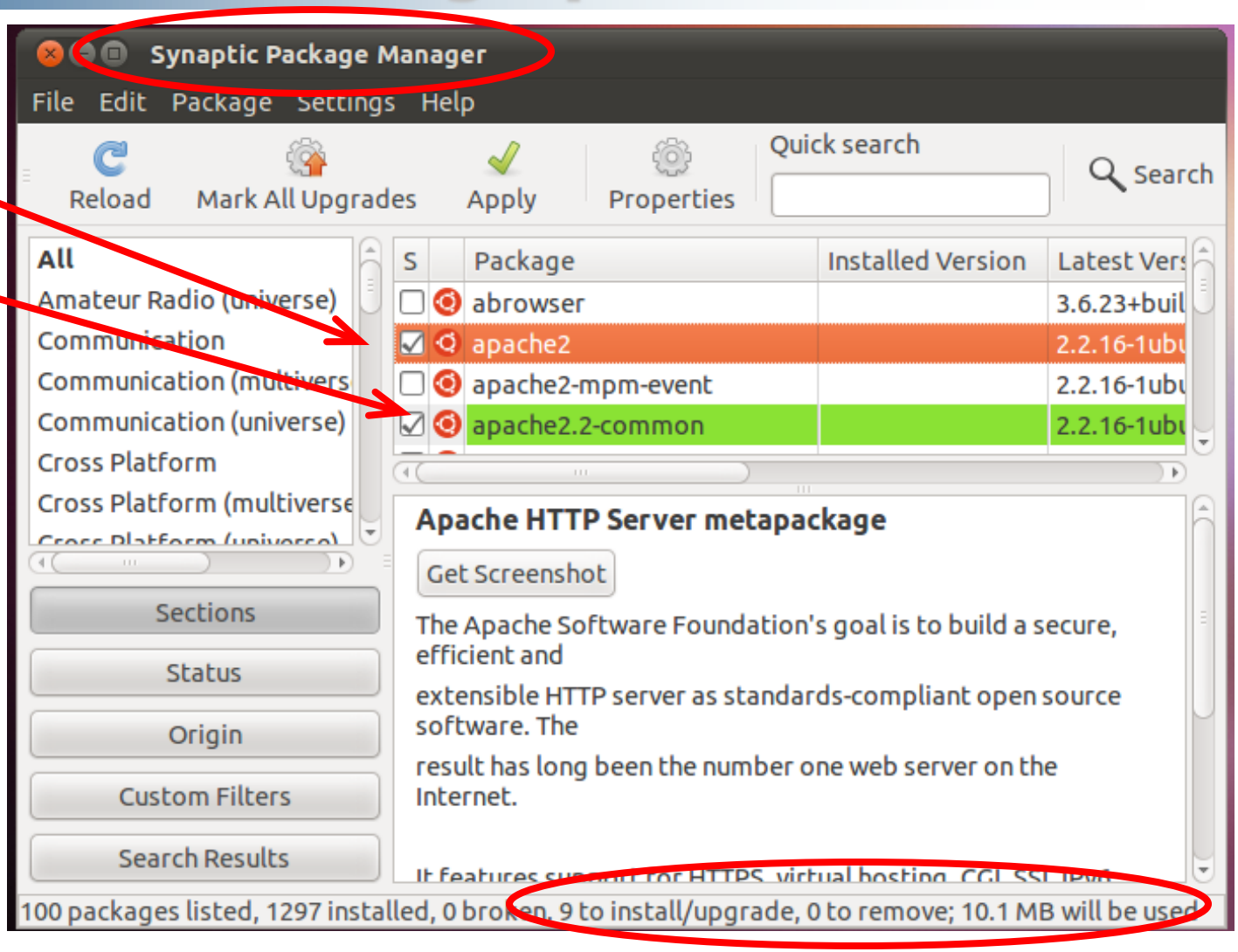


Install a Web Server

- Apache has been the most popular HTTP (Hyper Text Transport Protocol) server software in use since April 1996. As of May 2011 Apache was estimated to serve 63% of all websites and 66% of the million busiest.
- Installing and running a webserver is a routine task for a sysadmin, and by way of example – the test plan is:
  - Install Apache 2.2
  - Confirm Apache is running
  - Replace the default index.html

Installing Apache

Executables
+
Support files



This is almost *too* easy... it failed

Synaptic Package Manager

- Revised test plan
  - ✓ Patch the operating system
  - ✓ Install Apache 2.2
  - ✓ Confirm Apache is running
  - ✓ Performance considerations
  - ✓ Replace the default index.html
- Synaptic failed during the install process
  - 404 Error was not overly helpful
  - SysAdmin sorted it out
- Later made system update to 11.10 to get even
  - traceroute deleted in return

Installing Apache

ps –ef shows parent and child processes running

4?

```
mmaxwell@ubuntu: ~
File  Edit  View  Search  Terminal  Help
mmaxwell  1988     1  0 00:49 ?        00:00:00 /usr/lib/gnome-panel/clock-apple
mmaxwell  1989     1  0 00:49 ?        00:00:00 /usr/lib/gnome-panel/notificatio
mmaxwell  1990     1  0 00:49 ?        00:00:00 /usr/lib/indicator-applet/indica
mmaxwell  2008     1  0 00:49 ?        00:00:00 /usr/lib/gvfs/gvfsd-metadata
mmaxwell  2014     1  0 00:49 ?        00:00:00 /usr/lib/indicator-sound/indicat
mmaxwell  2015     1  0 00:49 ?        00:00:00 gnome-screensaver
mmaxwell  2017     1  0 00:49 ?        00:00:00 /usr/lib/indicator-messages/indi
mmaxwell  2021     1  0 00:49 ?        00:00:00 /usr/lib/indicator-application/i
mmaxwell  2024     1  0 00:49 ?        00:00:00 /usr/lib/indicator-me/indicator-
mmaxwell  2026     1  0 00:49 ?        00:00:00 /usr/lib/indicator-session/indic
mmaxwell  2031     1  0 00:49 ?        00:00:00 /usr/lib/gvfs/gvfsd-burn --spawn
mmaxwell  2037  1792  0 00:50 ?        00:00:00 /usr/lib/gnome-disk-utility/gdu-
mmaxwell  2039  1792  0 00:50 ?        00:00:00 /usr/bin/python /usr/share/syste
mmaxwell  2040  1792  0 00:50 ?        00:00:00 update-notifier
root      2238     2  0 00:56 ?        00:00:00 [flush-0:20]
root      2593     1  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2596  2593  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2598  2593  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2599  2593  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
mmaxwell  2665     1  4 00:57 ?        00:00:00 gnome-terminal
mmaxwell  2668  2665  0 00:57 ?        00:00:00 gnome-pty-helper
mmaxwell  2669  2665  3 00:57 pts/0    00:00:00 bash
mmaxwell  2688  2669  0 00:57 pts/0    00:00:00 ps -ef
mmaxwell@ubuntu:~$
```

Apache Processes

Building a scalable web server

- Handling an HTTP request
  - Map the URL to a resource
  - Check if client has rights to access resource
  - Choose a handler and generate a response
  - Transmit the response to the client
  - Log the request
- Must handle many clients simultaneously
- Must do this as fast as possible

Apache Processes

Apache Resource Pools

- The OS is one bottleneck to server performance
  - System calls (allocate memory, access a file, create child process) take significant amounts of time
  - Caching is one solution to scaling issues
- Resource pool: application-level data structure to allocate and cache resources
  - Allocate and free memory in the application instead of using a system call
  - Cache files, URL mappings, recent responses
  - Limits critical functions to a small, well-tested part of code

Apache Performance

Multi-Processor Architectures

- A critical factor in web server performance is how each new connection is handled
  - Common optimization strategy: identify most commonly-executed code and make fast
  - Common case: accept a client and return several static objects
  - Make this run fast: pre-allocate a process or thread, cache commonly-used files and the HTTP message for the response

Apache Performance

Connections to a web server

- Must multiplex handling many connections simultaneously
  - select(), poll(): event-driven, singly-threaded
  - fork(): create a new process for a connection
  - pthread create(): create a new thread for a connection
- Handle synchronization among processes/threads
  - Shared memory: semaphores
  - Message passing

Approach 1

Process Driven Architecture

- Devote a separate process/thread to each event
  - Master process listens for connections
  - Master creates a separate process/thread for each new connection
- Performance considerations
  - Creating a new process involves significant overhead
  - Threads less expensive, but still have overhead
- May create too many processes/threads on a busy server

Approach 2

Process/Thread Pool Architecture

- Master thread
  - Creates a pool of threads
  - Listens for incoming connections
  - Places connections on a shared queue
- Processes/threads
  - Take connections from shared queue
  - Handle one I/O event for the connection
  - Return connection to the queue
  - Live for a certain number of events
    - Prevents long-lived memory leaks
- Need memory synchronization

Approach 3

Hybrid Architectures

- Each process can handle multiple requests
  - Each process is an event-driven server
  - Must coordinate switching among events/requests
- Each process controls several threads
  - Threads can share resources easily
  - Requires some synchronization primitives
- Event driven server that handles fast tasks but spawns helper processes for time-consuming requests

Not a Theoretical Question

What are attributes of a good Web Server?

In order, for a production host are:

1. Correctness
2. Reliability
3. Scalability
4. Stability
5. Speed

Attributes

Correctness? Correctness!

- Does it conform to the HTTP specification?
  - It must!
- Does it work with every browser?
- Does it handle erroneous input gracefully
  - Should be flexible with input
  - Strict with output

- RFC's - Internet Engineering Task Force ietf.org
- W3C - World Wide Web Consortium w3.org

Attributes

Reliability

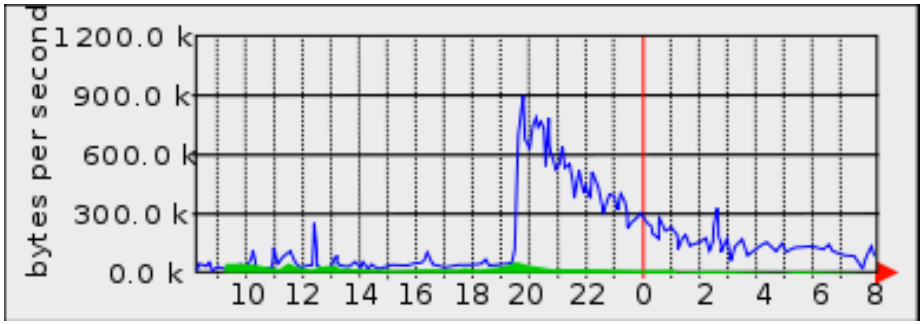
- Can you sleep at night?
- Are you being paged during dinner?
- It is an appliance?

We don’t want our web servers waking us up in the middle of the night, or requiring constant attention. We want a web server that we set up once and rarely touch again. It should behave like an appliance, never breaking down.

Attributes

Scalability

- Does it handle nominal load?
- Have you been *Slashdotted*?
  - Did you survive?
- What is your peak load?



Often systems are deployed without significant scalability testing. These sites tend to fail when uptime is most critical. Healthcare sites?

Attributes

Speed (Latency)

- Does it *feel* fast?
- Do pages snap in quickly?
- Do users often reload pages?

As a site gains viewers, the time for each page to be served will increase. One critical point is when users begin to hit stop on their browsers and reload the page. This places even more load on an already strained system, causing further service denial. Ads, animations, etc. don't help.

Installing Apache

ps –ef shows parent and child processes running

4?

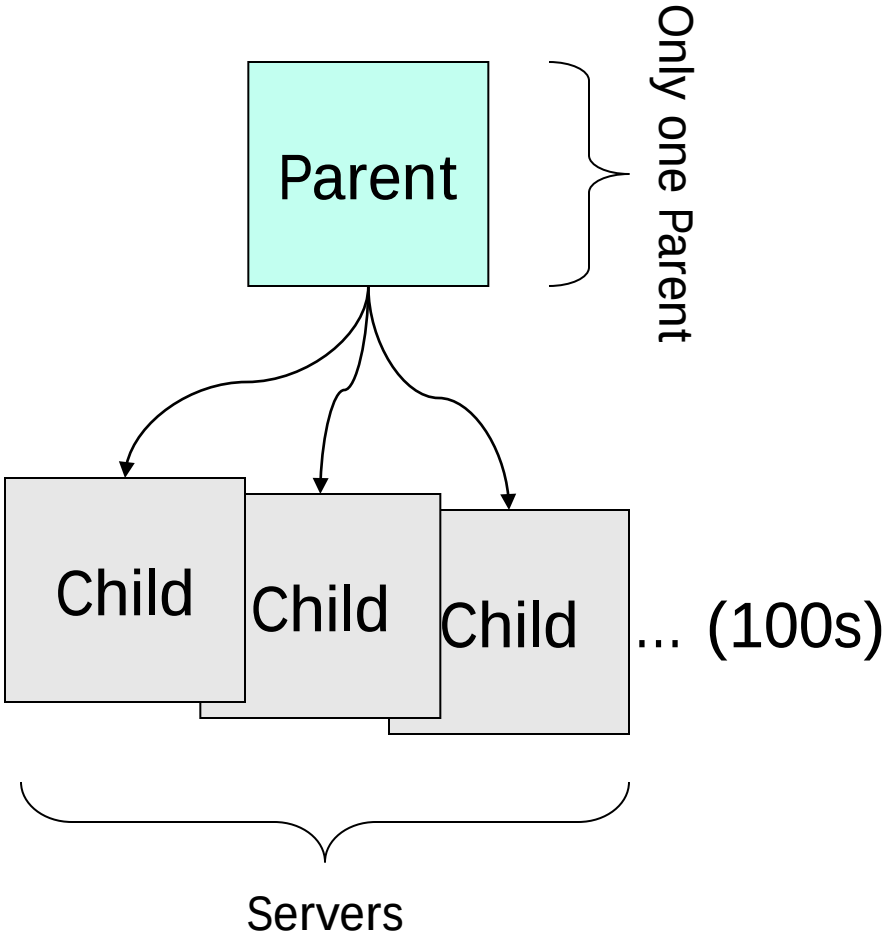
```
mmaxwell@ubuntu: ~
File  Edit  View  Search  Terminal  Help
mmaxwell  1988     1  0 00:49 ?        00:00:00 /usr/lib/gnome-panel/clock-apple
mmaxwell  1989     1  0 00:49 ?        00:00:00 /usr/lib/gnome-panel/notificatio
m                                                                              a
m
m                                                                              t
m
m                                                                              i
m                                                                              i
mmaxwell  2024     1  0 00:49 ?        00:00:00 /usr/lib/indicator-me/indicator-
mmaxwell  2026     1  0 00:49 ?        00:00:00 /usr/lib/indicator-session/indic
mmaxwell  2031     1  0 00:49 ?        00:00:00 /usr/lib/gvfs/gvfsd-burn --spawn
mmaxwell  2037  1792  0 00:50 ?        00:00:00 /usr/lib/gnome-disk-utility/gdu-
mmaxwell  2039  1792  0 00:50 ?        00:00:00 /usr/bin/python /usr/share/syste
mmaxwell  2040  1792  0 00:50 ?        00:00:00 update-notifier
root      2238     2  0 00:56 ?        00:00:00 [flush-0:20]
root      2593     1  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2596  2593  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2598  2593  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2599  2593  0 00:56 ?        00:00:00 /usr/sbin/apache2 -k start
mmaxwell  2665     1  4 00:57 ?        00:00:00 gnome-terminal
mmaxwell  2668  2665  0 00:57 ?        00:00:00 gnome-pty-helper
mmaxwell  2669  2665  3 00:57 pts/0    00:00:00 bash
mmaxwell  2688  2669  0 00:57 pts/0    00:00:00 ps -ef
mmaxwell@ubuntu:~$
```

INSTANT REPLAY

Classic Apache Model

Parent Process

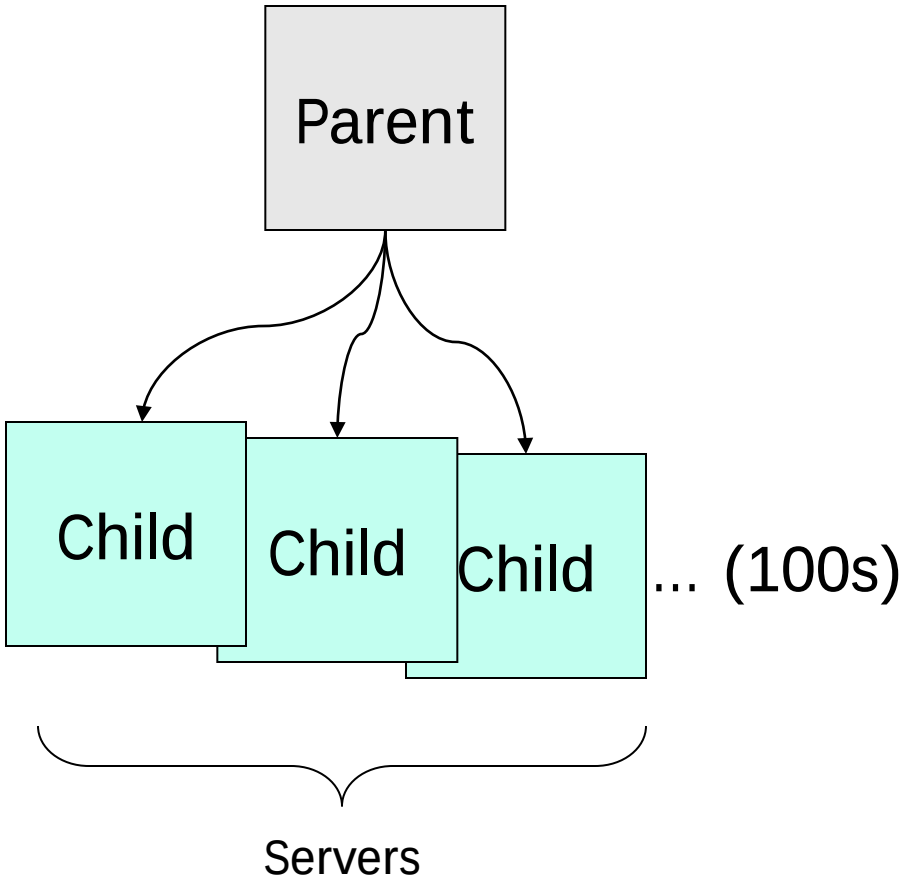
- Main httpd process
- Does not handle connections itself
- Only creates and destroys children
- Has many children
- Shared memory scoreboard to determine who handles connections



Classic Apache Model

Child Process

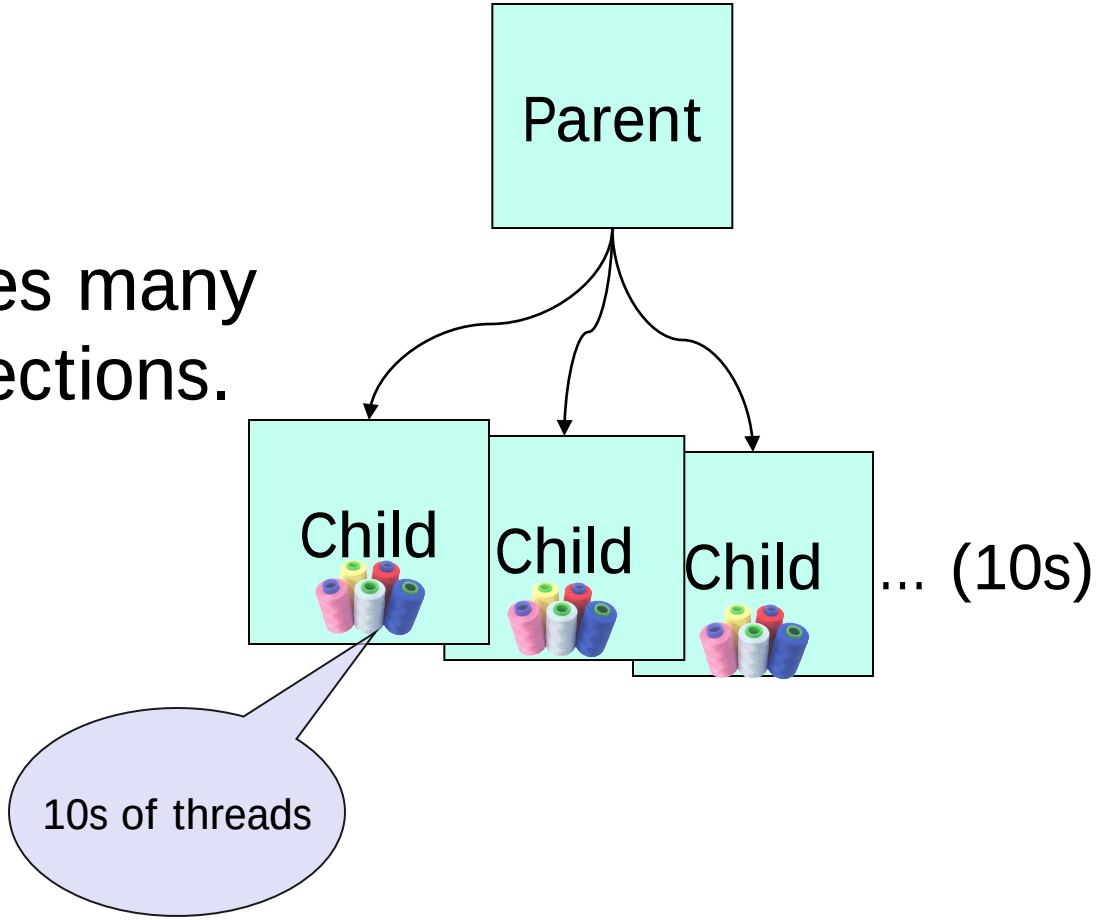
- Called a server in the httpd.conf file
- A single httpd process
- Each child handles one connection at a time
  - High memory requirements
  - Run out of memory before CPU
- *Note: Default install was one parent and three child processes*



Multithreaded Apache

- Apache 2.x Multithreaded

- Few Children
- Each child handles many concurrent connections.



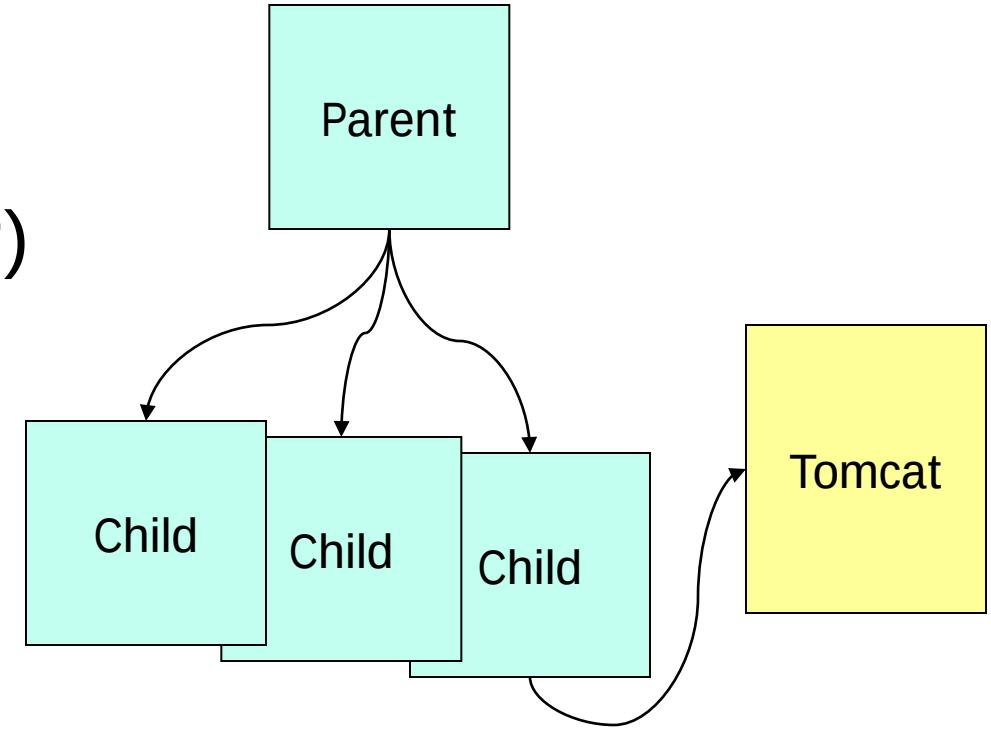
Apache Design

- **Dynamic Content: Modules**
  - Extensive API
  - Pluggable Interface
  - Dynamic or Static Linkage
- **In-process Modules**
  - Run from inside the httpd process
    - CGI (mod_cgi)
    - mod_perl
    - mod_php
    - mod_python
    - mod_tcl

Apache Design

Out-of-process Modules

- Processing happens outside of httpd (eg. Application Server)
- Tomcat
  - mod_jk/jk2, mod_jserv
- mod_proxy
- mod_jrun



Apache Tomcat

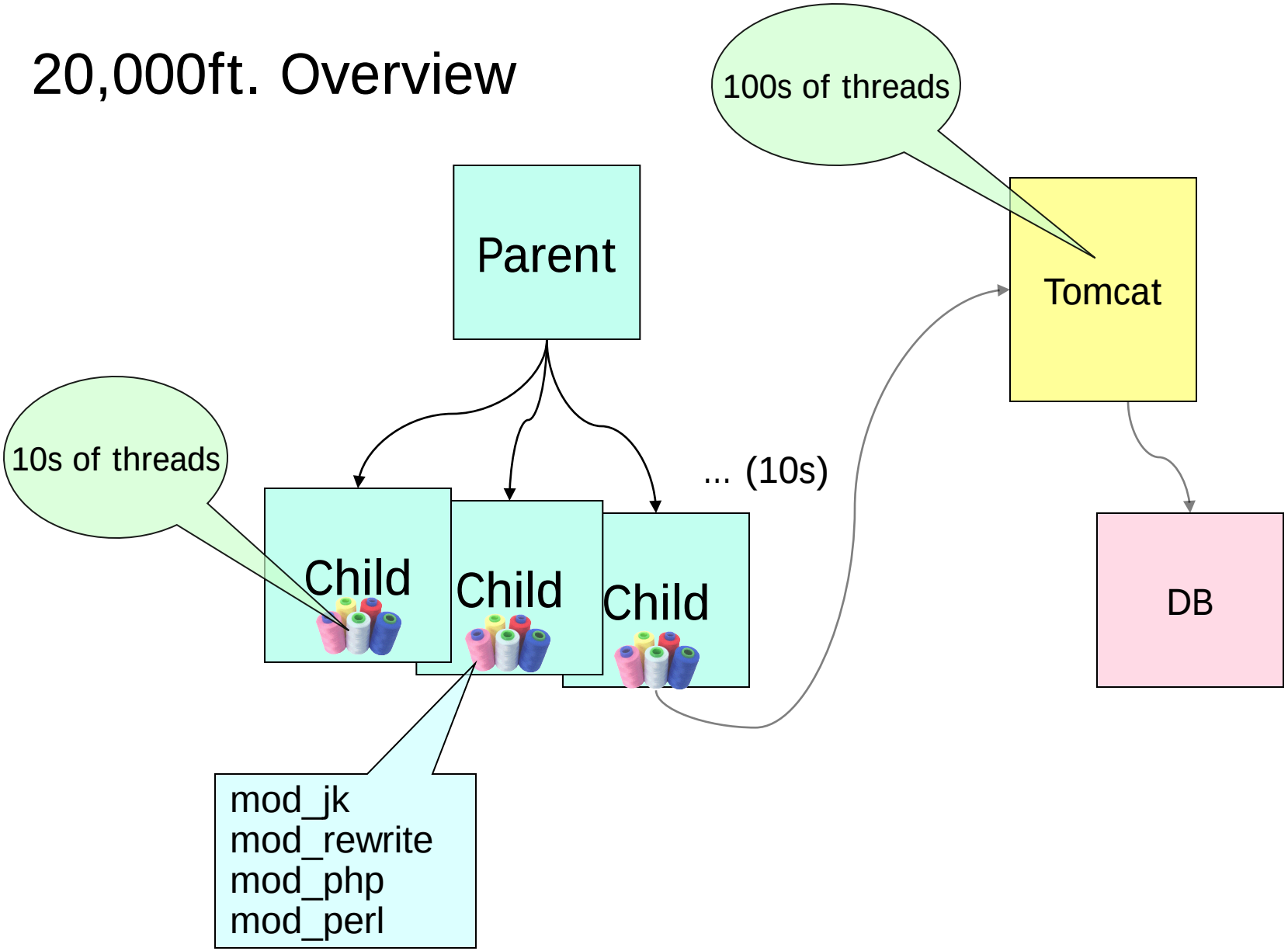
- Apache Tomcat is an open-source web server developed by the Apache Software Foundation (ASF)
- Tomcat implements several Java EE specifications including Java Servlet, JavaServer Pages (JSP), Java EL, and WebSocket, and provides a "pure Java" HTTP web server environment for Java code to run in

Apache Tomcat

The Apache Software Foundation
http://www.apache.org/

Apache Design

20,000ft. Overview



Apache Design

- Multi-Processing Module
- An *MPM* defines how the server will receive and manage incoming *requests*
- Allows OS-specific optimizations
- Allows vastly different server models (eg. threaded vs. multiprocess)

- In multi-threaded MPMs (eg. Worker)
- Each thread handles a single connection
- Allows child to handle many connections at once

Apache 1.3

Standard Directives

- StartServer: Number of child processes to create at startup
- MinSpareServer: Minimum idle children to have at any time
- MaxSpareServer: Maximum idle children to have at any time
- MaxClients: Maximum concurrent client connections to allow
- MaxRequestsPerChild: Maximum requests that each child is allowed to serve before it must terminate and be replaced. Clears out things , good for buggy 3rd party modules that leak system resources.

Apache 2.0 and later

Apache MPM (Multi-Processing Modules)

- Multithreaded within each child
- Dramatically reduced memory footprint
- Fewer children

Apache Directives

- MinSpareThreads – Minimum idle threads to allow at any time across all children
- MaxSpareThreads – Maximum idle threads to allow at any time across all children
- ThreadsPerChild - Threads within each child
- MaxClients – Maximum concurrent client connections to allow at any time
- MaxRequestsPerChild – Maximum requests that each child is allowed to serve before it must terminate and be replaced

Performance Characteristics

Prefork

- High memory usage
- Highly tolerant of faulty modules
- Highly tolerant of crashing children
- Fast
- Well-suited for 1 and 2-CPU systems
- Tried-and-tested model from Apache 1.3
- “You’ll run out of memory before CPU.”

Performance Characteristics

Worker

- Low to moderate memory usage
- Moderately tolerant to faulty modules
- Faulty threads can affect all threads in child
- Highly-scalable
- Well-suited for multiple processors
- Requires a mature threading library (Solaris, AIX, Linux 2.6 and others work well)
- Memory is no longer the bottleneck

Performance Considerations

Always test and document

MEMORY

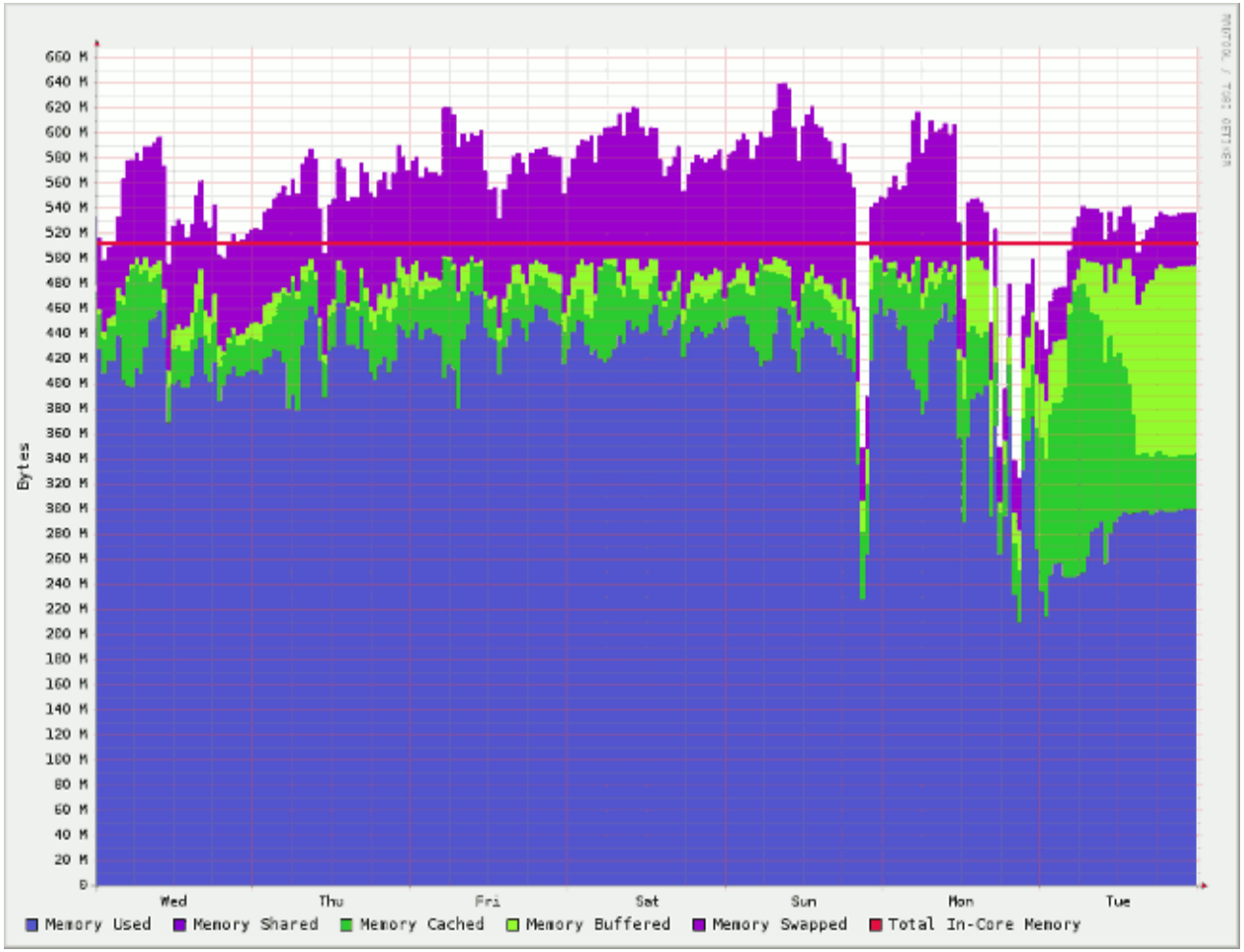
USED

CACHED

BUFFERED

SWAPPED

PHYSICAL



Performance Considerations

- sendfile() support – serving static content (html pages, images, etc.) is faster if OS supports this
- Eliminates Double-copy: when a process reads data from a file and sends it to a network device, the first copy happens when the kernel reads the file into the userspace process memory area. The second copy happens when the kernel copies the data back out of userspace into kernel space, forms a full data packet, and then copies that to the network card. With sendfile() the process instructs the kernel to send a particular file out to a network.

Performance Considerations

- sendfile() support in both the OS and NIC
- Zero-copy - best-case scenario. The kernel and NIC cooperate together to read and assemble data directly from a disk straight to the network.
- The data passes to a network socket without ever having to be copied into main memory.
- Dramatic improvement for static files 50%+

The point of this....

- Advantage of awareness and some understanding of:
  - Hardware characteristics and features
  - Operating System internal workings
  - Application configurations with respect to OS, hardware

Performance Considerations

Load balancing via RoundRobin DNS

```
; <<>> DiG 9.5.1b1 <<>> yahoo.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58299
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 13, ADDITIONAL: 11

;; QUESTION SECTION:
;yahoo.com.                IN    A

;; ANSWER SECTION:
yahoo.com.          2433   IN    A     67.195.160.76
yahoo.com.          2433   IN    A     72.30.2.43
yahoo.com.          2433   IN    A     98.137.149.56
yahoo.com.          2433   IN    A     98.139.180.149
yahoo.com.          2433   IN    A     209.191.122.70
```

Performance Considerations

RoundRobin DNS also provides Geographical redundancy

```
; <<>> DiG 9.5.1b1 <<>> www.dot.ca.gov
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24179
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.dot.ca.gov.                IN    A

;; ANSWER SECTION:
www.dot.ca.gov.      259    IN    A     149.136.36.11
www.dot.ca.gov.      259    IN    A     149.136.20.66
```

NorCal Circuit

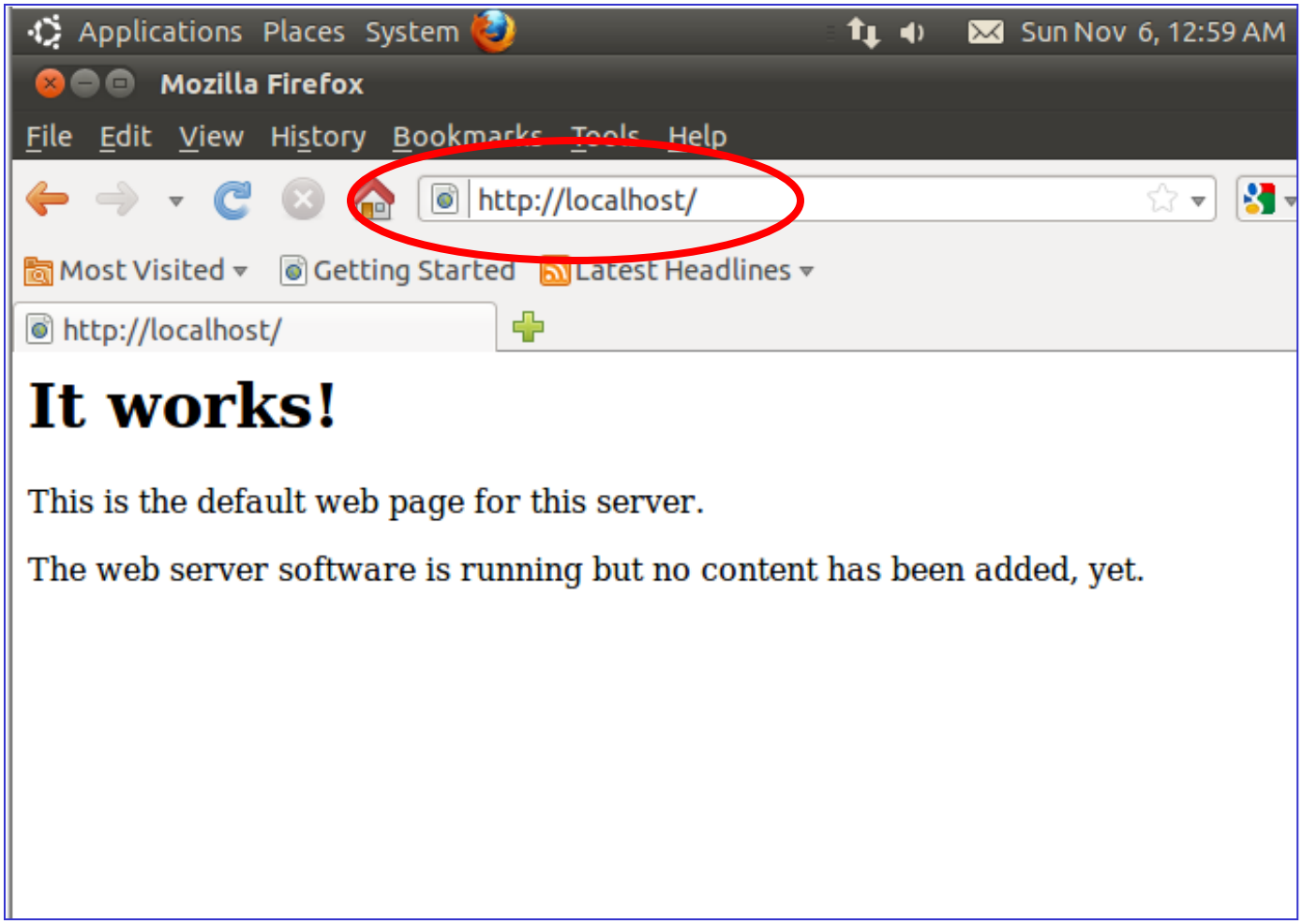
SoCal Circuit

After the web server is configured and restarted, what does it look like on the web?

Installing Apache

- Default index.html page viewed in Firefox
- Never leave this page visible on Internet

Poor browser menu to content ratio



Installing Apache

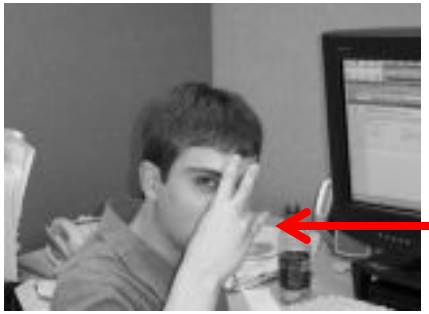
Some quick content is added – HTML + CSS

Editing in vi
:wq!

mmaxwell@ubuntu: /var/www

File Edit View Search Terminal Help

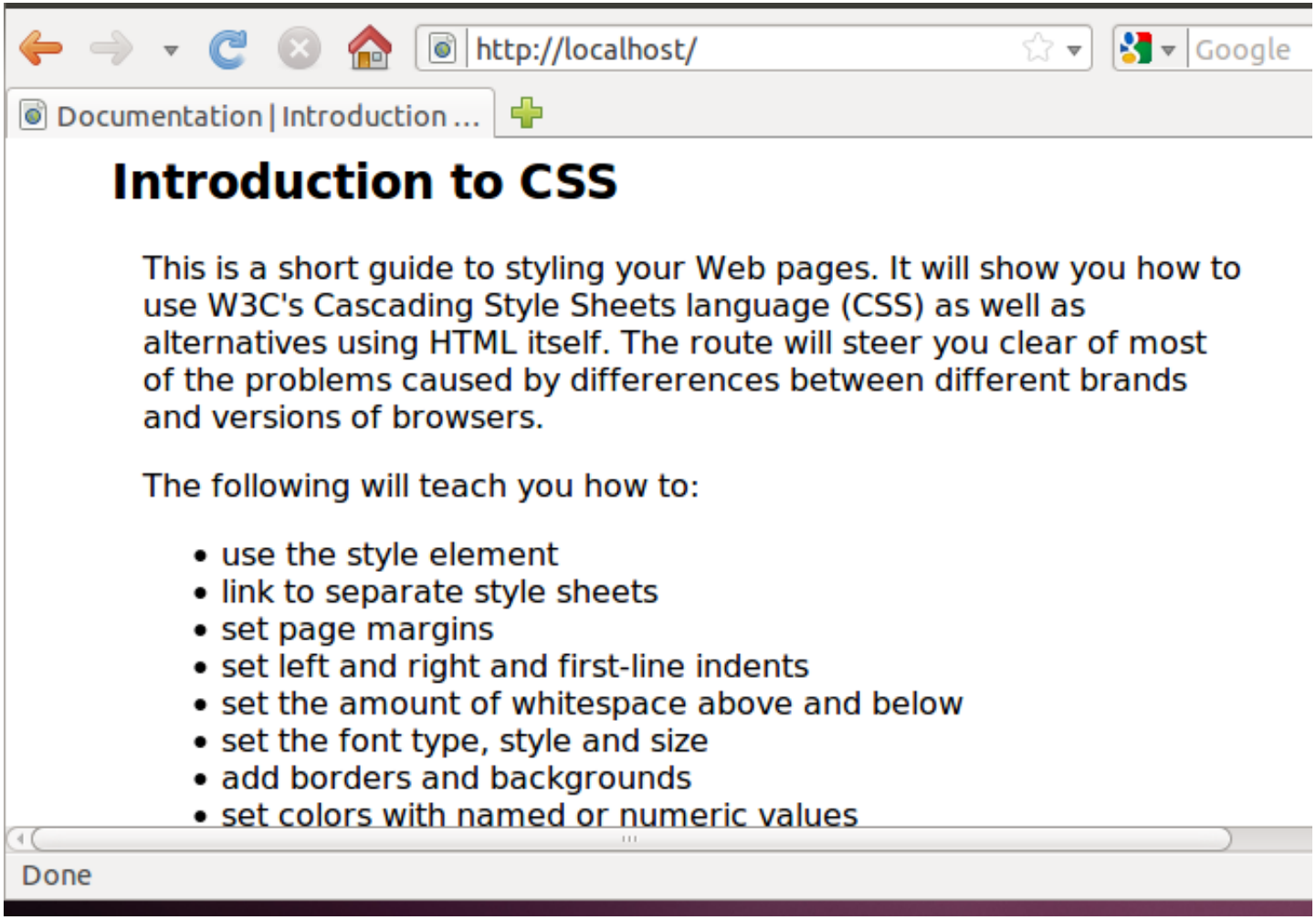
```
</pre>

<p>The <em>size</em> attribute can be used to select the font size
as a number from 1 to 6. If you place a - or + sign before the
number it is interpreted as a relative value. Use size="+1" when
you want to use the next larger font size and size="-1" when you
want to use the next smaller font size, e.g.</p>

<pre>
&lt;font size="+1" color="maroon"
  face="Garamond, Times New Roman"&gt;some text ...&lt;/font&gt;
</pre>

<p>There are a couple of things you should avoid: Don't choose
color combinations that make text hard to read for people who are
color blind. Don't use font to make regular text into headings,
which should always be marked up using the h1 to h6 tags as
appropriate to the importance of the heading.</p>

</body>
</html>

:wq!
```



vi gangstas

Installing Apache

- Viewing the new index.html file
  - Improved content to menu browser setting



Installing Apache

- Apache configuration files are in /etc/apache2

mmaxwell@ubuntu: /etc/apache2

File Edit View Search Terminal Help

```
mmaxwell@ubuntu:/etc/apache2$ ls -al
total 84
drwxr-xr-x   7 root root  4096 2011-11-06 00:56 .
drwxr-xr-x 132 root root 12288 2011-11-06 00:56 ..
-rw-r--r--   1 root root  7994 2011-09-01 03:25 apache2.conf
drwxr-xr-x   2 root root  4096 2011-11-06 00:56 conf.d
-rw-r--r--   1 root root  1169 2011-09-01 03:25 envvars
-rw-r--r--   1 root root     0 2011-11-06 00:56 httpd.conf
-rw-r--r--   1 root root 31063 2011-09-01 03:25 magic
drwxr-xr-x   2 root root  4096 2011-11-06 00:56 mods-available
drwxr-xr-x   2 root root  4096 2011-11-06 00:56 mods-enabled
-rw-r--r--   1 root root   750 2011-09-01 03:25 ports.conf
drwxr-xr-x   2 root root  4096 2011-11-06 00:56 sites-available
drwxr-xr-x   2 root root  4096 2011-11-06 00:56 sites-enabled
mmaxwell@ubuntu:/etc/apache2$
```

Installing Apache

From the apache2.conf file header!

```
# Do NOT simply read the instructions in here
# without understanding what they do.
# They're here only as hints or reminders.
# If you are unsure consult the online docs.
# You have been warned.
```

1. RTFM - not just the .conf file
2. Test in a test environment
3. Monitor when in production

/etc/httpd/httpd.conf

```
ServerAdmin root@treacle.com
ServerName www.treacle.com:80
DocumentRoot "/srv/httpd/htdocs"
User apache
Group apache
# Default setting is very restrictive
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>
```

/etc/httpd/httpd.conf

```
# Now specify to be less restrictive
<Directory "/srv/httpd/htdocs">
    Options Indexes FollowSymLinks Includes
    IndexOptions FancyIndexing
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

/etc/httpd/httpd.conf

```
# Prevent .htaccess and .htpasswd files from being viewed
<FilesMatch "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy All
</FilesMatch>


# location of log file
ErrorLog "/var/log/httpd/error_log"
LogLevel warn
CustomLog "/var/log/httpd/access_log" common
```

/etc/httpd/httpd.conf

```
<Directory "/srv/httpd/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

/etc/httpd/httpd.conf

```
<VirtualHost treacle.com:80>
  ServerAdmin root@treacle.com
  DocumentRoot "/srv/httpd/htdocs"
  ServerName www.treacle.com
  ServerAlias treacle.com
  ErrorLog "/var/log/httpd/error_log"
  LogLevel warn
</VirtualHost>

<VirtualHost 7sins.com:80>
  ServerAdmin root@treacle.com
  DocumentRoot "/srv/httpd/htdocs/7sins"
  ServerName www.7sins.tk
  ErrorLog "/var/log/httpd/error_log.7sins"
  CustomLog "/var/log/httpd/access_log.7sins" combined env=!dontlog
  LogLevel warn
</VirtualHost>
```

error_log

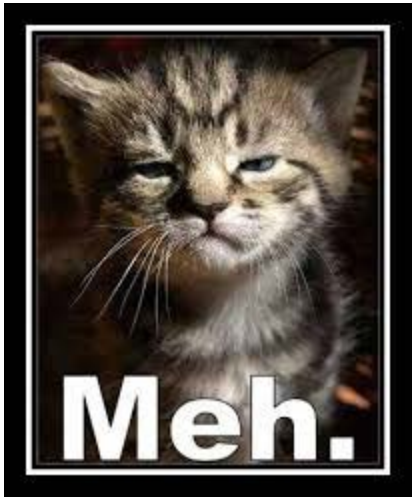
```
[Fri Nov 06 21:08:53 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/manager
[Fri Nov 06 21:08:53 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/packages
[Fri Nov 06 21:08:53 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/scripts
[Fri Nov 06 21:08:53 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/inv
[Fri Nov 06 21:08:53 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/admin
[Fri Nov 06 21:08:54 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/CMS
[Fri Nov 06 21:08:54 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/includes
[Fri Nov 06 21:08:54 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/rte
[Fri Nov 06 21:08:54 2015] [error] [client 67.198.166.59] File does not exist: /srv/httpd/htdocs/admin
[Sat Nov 07 18:01:39 2015] [error] [client 207.46.13.121] File does not exist: /srv/httpd/htdocs/68krmvt
[Sat Nov 07 19:41:46 2015] [error] [client 207.46.13.121] File does not exist: /srv/httpd/htdocs/68krmvt
[Sat Nov 07 23:47:21 2015] [error] [client 94.250.253.129] File does not exist: /srv/httpd/htdocs/wp-login.php
[Sat Nov 07 23:47:23 2015] [error] [client 94.250.253.129] File does not exist: /srv/httpd/htdocs/administrator
[Sun Nov 08 04:38:51 2015] [error] [client 159.203.129.161] File does not exist: /srv/httpd/htdocs/icons
[Sun Nov 08 14:20:45 2015] [error] [client 66.249.79.54] File does not exist: /srv/httpd/htdocs/mogf9s
```

67.198.166.59 Sacramento Cloud host Krypt.com

207.46.13.121 bingbot

94.250.253.129 Russia ISP

66.249.79.54 Googlebot



Apache Security

Responsibility of the System Administrator

- Configuration vulnerabilities
  - Directory browsing
  - Forwarding proxy
- Failure-to-patch vulnerabilities
  - Apache killer tool exploiting DoS flaw (8/2011)
- Add-In vulnerabilities
  - SQL Injection
  - mysql exploits
- Clueless tool/user issues

Want to see what can happen then?

Index of / - NCSA Mosaic

http://geo.dot.ca.gov/

File Edit View Favorites Tools Help

Favorites

Index of /

Index of /

Name	Last modified	Size	Description
probe.png	12-Jan-2011 13:46	103	
wms.html	01-Feb-2011 08:30	1.8K	
wms.html.bak	31-Jan-2011 16:16	1.8K	

Apache/2.2.16 (Ubuntu) Server at geo.dot.ca.gov Port 80

SirVic And #WhiteHat Team @ UnderNet

Proudly Present :

* ANFWD * - (Another Fine Web Defacement)

" And there will be a time, when penguins attack "

That being said, here we go !

1) The Shoutz : From SirVic to all #WhiteHat Team memberz, to all .ro scripto-kiddies, i know i said that i hate you guys, but i don't, i love the fact that you suck, you .. inspire me to achieve perfection :-) ; random greets to tha suppa' duppa' retired h4x0r AccDenied, baftalo phanakot! ; and last but not least, to all the regular members of #WH , teh WhiteHat open-to-the-public channel :-) *AND* to all those who know what it takes to pimp a server ! =)

2) The Phuck-yews: surprise fuckers! - we ran out of enemies :-(; iasi-hack is too gay to be mentioned here, so in teh absence of a worthy enemy, we decided to leave this field blank... well.... almost blank :-)

3) Message to teh sysadmins (as in trstan - Star[redacted] & larry - Larry [redacted]r , with special thanks to teh finger utility) DUDES, you actually get paid for what you "do" ?! ; i kept a close watch to your so called "hunting techniques" (back on www1.) , no offence, but you should REALLY learn some *NIX before attempting to call yourselfs "sysadmins" ;)

Contact zone :

you could try mailing me : SirVic@WhiteHat.ro ; SirVic@SirVic.biz
forum is available of course ! -> http://forum.WhiteHat.ro
oh yeah, almost forgot, you can also join UnderNet on channel #WH =)

Copyright : SirVic Of UnderNet - 19.07.2006

http://www2.dot.ca.gov :)

http://www2.dot.ca.gov/whitehat.jpg
BURN BABY, BURN !!! ;-))

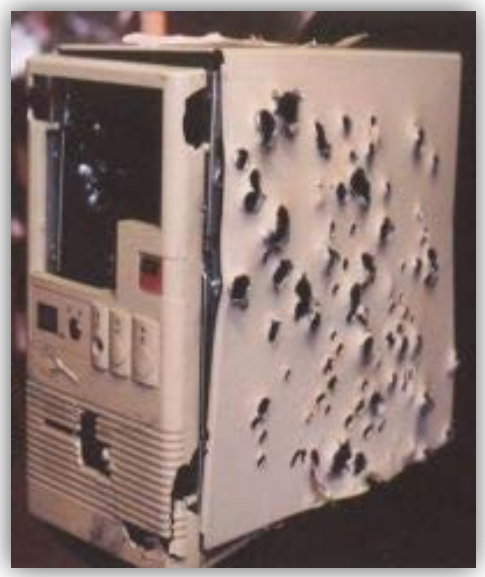

BUTTPIRATEZ
AAAAARRRRRRGGGHHHHHH! !!!!!!

st4ck - h4rv3st - l0rd_byr0n - gridrunk - j0shua - freak - hellsink - losjack - hux0x

Compromised Hosts

- Directory browsing – data disclosure
- Defacements – tough to explain to management

- Worst case is the compromise is not detected



Expended after compromise

Compromised Webservers

- What happens to a vulnerable hosting service?
- Weak/flawed remote management tool
  - 20,000 compromised websites
  - Hidden Iframes for injecting <height=0 width=0>
  - Hidden comments for Black Hat SEO
  - Extra folders for ???? content

Remember

- Package management
  - Manage dependency checking
- CLI Package manager – APT
- Common GUI for APT - Synaptic
- 1989 Tim Berners-Lee wrote first web server
- Apache is currently most common webserver
- Five attributes of a good web server
  - Correctness
  - Reliability
  - Scalability
  - Stability
  - Speed