practical steps in securing a UNIX/Linux system

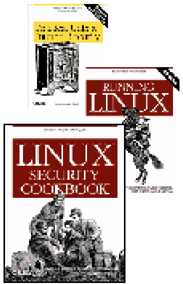
Don Murdoch, CISSP
GCWN, GCUX, GCIH, GCIA,
MCSE & MCSD
Information Systems Security Officer
Old Dominion University, Norfolk, VA

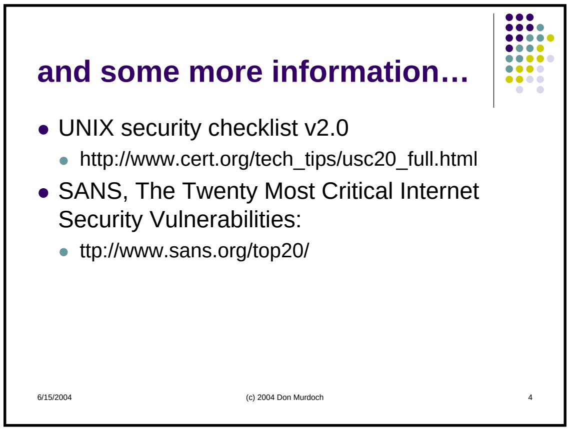
agenda

- o.s. hardening principles
- hardware
- o.s. install and updates
- managing services
- file system
- sudo and syslog
- system banners
- additional topics (if we have time)

for more information …

- O'Reilly! (I think there are some other companies?)
- Linux Security Cookbook
  - By Daniel J. Barrett, Richard Silverman, Robert G. Byrnes
- Running Linux, 4th Edition
  - By Matt Welsh, Matthias Kalle Dalheimer, Terry Dawson, Lar Kaufman
- Practical Unix & Internet Security, 3rd Edition
  - By Simson Garfinkel, Gene Spafford, Alan Schwartz
- SANS GCUX Course – Excellent.
- GIAC GCUX Certification papers.

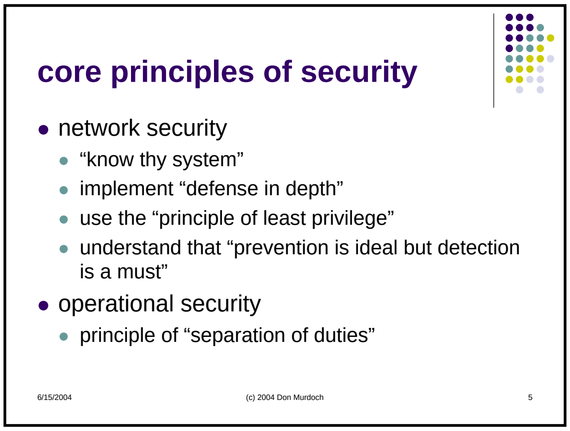




and some more information…

- UNIX security checklist v2.0
  - http://www.cert.org/tech_tips/usc20_full.html
- SANS, The Twenty Most Critical Internet Security Vulnerabilities:
  - ttp://www.sans.org/top20/

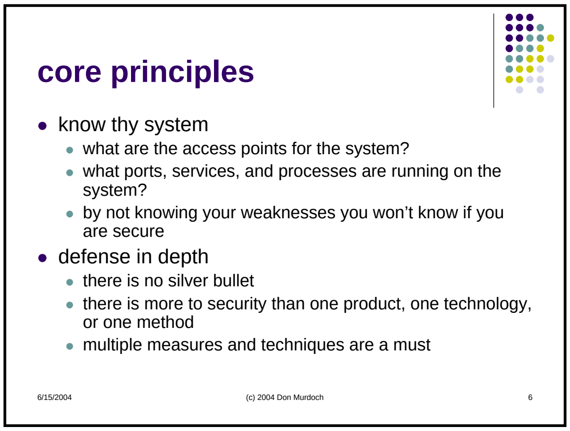
6/15/2004 (c) 2004 Don Murdoch 4



core principles of security

- network security
  - “know thy system”
  - implement “defense in depth”
  - use the “principle of least privilege”
  - understand that “prevention is ideal but detection is a must”
- operational security
  - principle of “separation of duties”

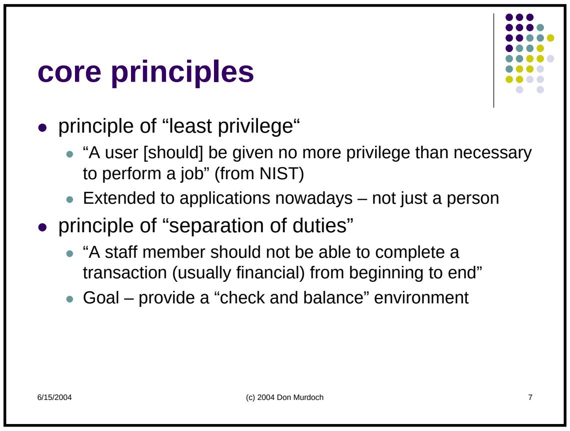
6/15/2004 (c) 2004 Don Murdoch 5



core principles

- know thy system
  - what are the access points for the system?
  - what ports, services, and processes are running on the system?
  - by not knowing your weaknesses you won’t know if you are secure
- defense in depth
  - there is no silver bullet
  - there is more to security than one product, one technology, or one method
  - multiple measures and techniques are a must

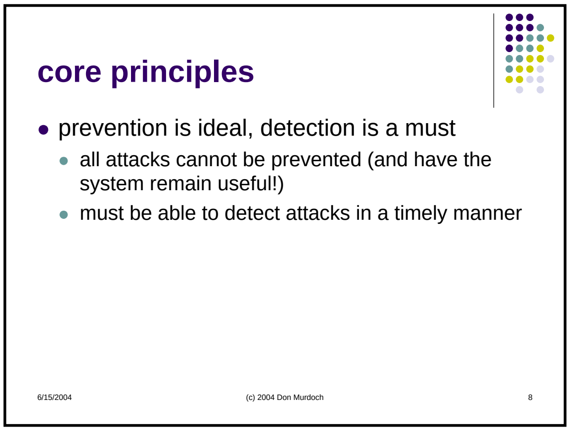
6/15/2004 (c) 2004 Don Murdoch 6



core principles

- principle of “least privilege“
  - “A user [should] be given no more privilege than necessary to perform a job” (from NIST)
  - Extended to applications nowadays – not just a person
- principle of “separation of duties”
  - “A staff member should not be able to complete a transaction (usually financial) from beginning to end”
  - Goal – provide a “check and balance” environment

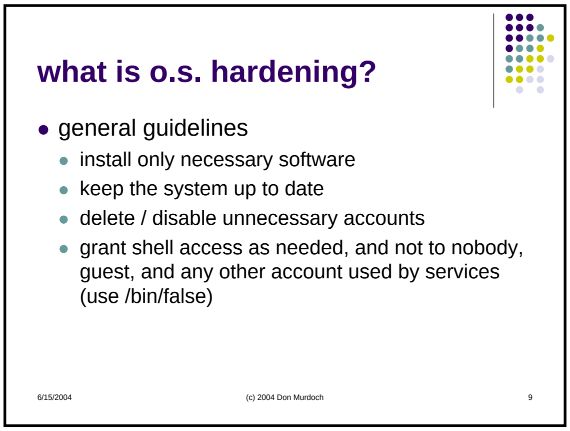
6/15/2004 (c) 2004 Don Murdoch 7



core principles

- prevention is ideal, detection is a must
  - all attacks cannot be prevented (and have the system remain useful!)
  - must be able to detect attacks in a timely manner

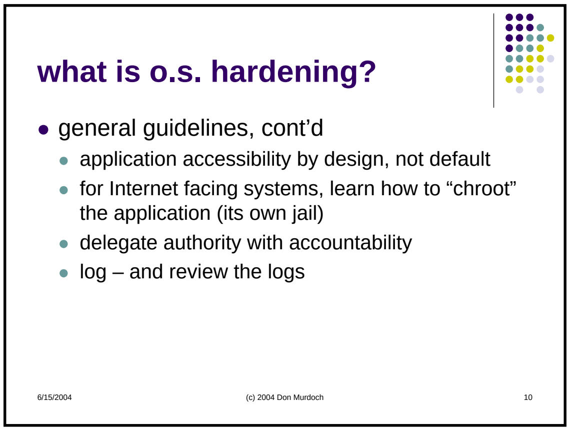
6/15/2004 (c) 2004 Don Murdoch 8



what is o.s. hardening?

- general guidelines
  - install only necessary software
  - keep the system up to date
  - delete / disable unnecessary accounts
  - grant shell access as needed, and not to nobody, guest, and any other account used by services (use /bin/false)

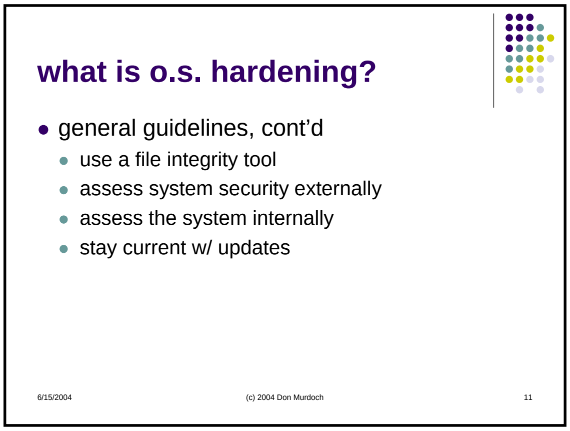
6/15/2004 (c) 2004 Don Murdoch 9



what is o.s. hardening?

- general guidelines, cont’d
  - application accessibility by design, not default
  - for Internet facing systems, learn how to “chroot” the application (its own jail)
  - delegate authority with accountability
  - log – and review the logs

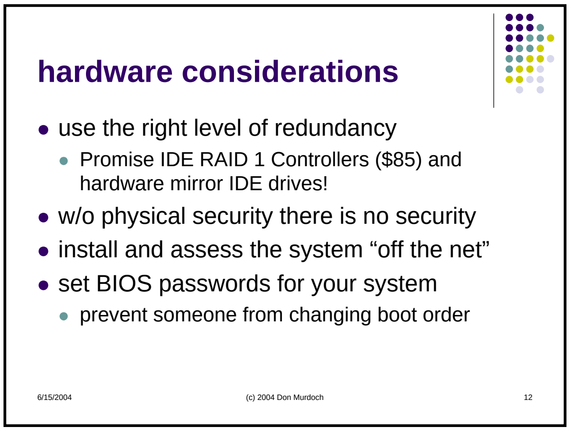
6/15/2004 (c) 2004 Don Murdoch 10



what is o.s. hardening?

- general guidelines, cont’d
  - use a file integrity tool
  - assess system security externally
  - assess the system internally
  - stay current w/ updates

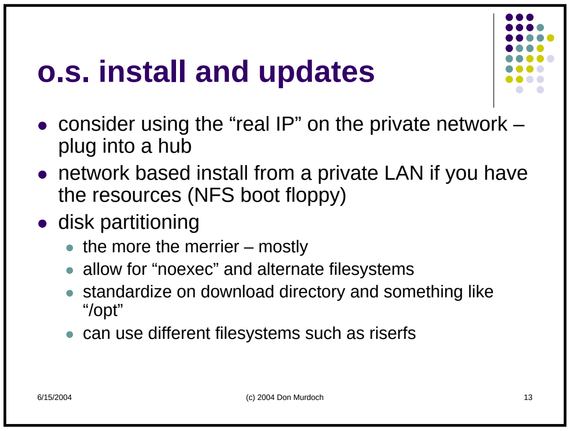
6/15/2004 (c) 2004 Don Murdoch 11



hardware considerations

- use the right level of redundancy
  - Promise IDE RAID 1 Controllers ($85) and hardware mirror IDE drives!
- w/o physical security there is no security
- install and assess the system “off the net”
- set BIOS passwords for your system
  - prevent someone from changing boot order

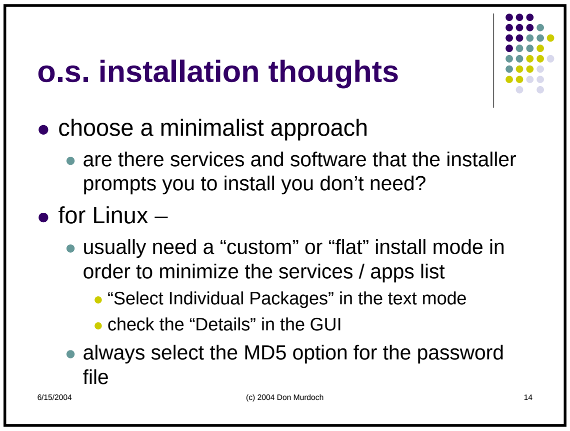
6/15/2004 (c) 2004 Don Murdoch 12



o.s. install and updates

- consider using the "real IP" on the private network – plug into a hub
- network based install from a private LAN if you have the resources (NFS boot floppy)
- disk partitioning
  - the more the merrier – mostly
  - allow for "noexec" and alternate filesystems
  - standardize on download directory and something like "/opt"
  - can use different filesystems such as riserfs

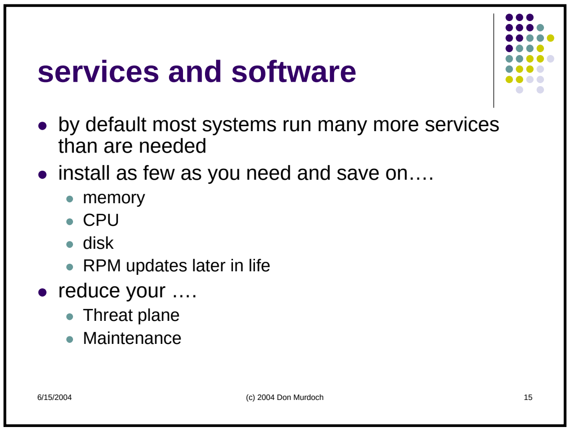
6/15/2004 (c) 2004 Don Murdoch 13



o.s. installation thoughts

- choose a minimalist approach
  - are there services and software that the installer prompts you to install you don't need?
- for Linux –
  - usually need a "custom" or "flat" install mode in order to minimize the services / apps list
    - "Select Individual Packages" in the text mode
    - check the "Details" in the GUI
  - always select the MD5 option for the password file

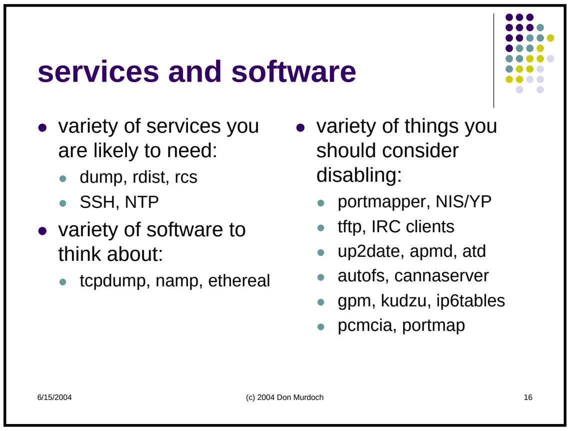
6/15/2004 (c) 2004 Don Murdoch 14



services and software

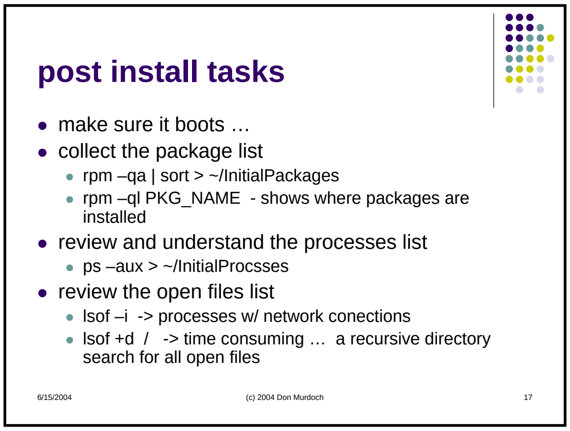
- by default most systems run many more services than are needed
- install as few as you need and save on….
  - memory
  - CPU
  - disk
  - RPM updates later in life
- reduce your ….
  - Threat plane
  - Maintenance

6/15/2004 (c) 2004 Don Murdoch 15



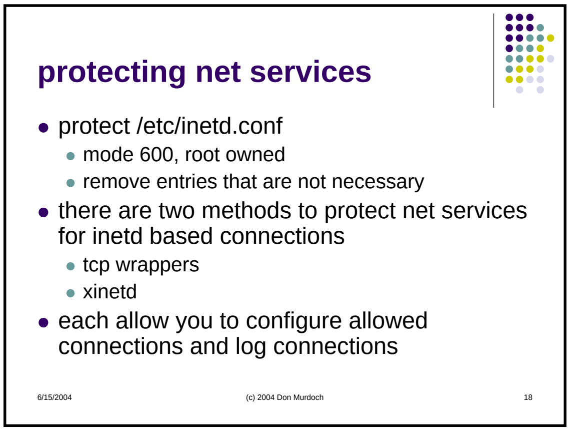
services and software

- variety of services you are likely to need:
  - dump, rdist, rcs
  - SSH, NTP
- variety of software to think about:
  - tcpdump, namp, ethereal
- variety of things you should consider disabling:
  - portmapper, NIS/YP
  - tftp, IRC clients
  - up2date, apmd, atd
  - autofs, cannaserver
  - gpm, kudzu, ip6tables
  - pcmcia, portmap



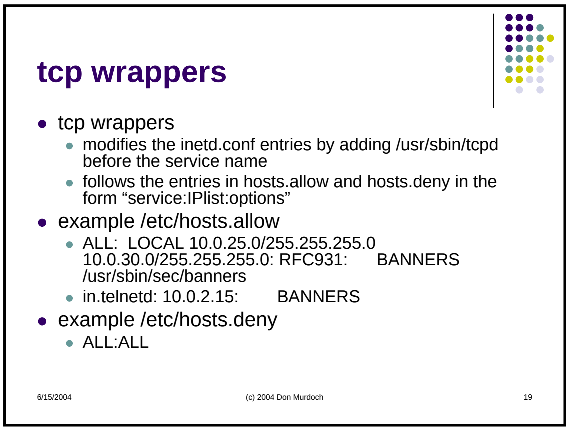
post install tasks

- make sure it boots …
- collect the package list
  - rpm –qa | sort > ~/InitialPackages
  - rpm –ql PKG_NAME - shows where packages are installed
- review and understand the processes list
  - ps –aux > ~/InitialProcsses
- review the open files list
  - lsof –i -> processes w/ network conections
  - lsof +d /   -> time consuming … a recursive directory search for all open files



protecting net services

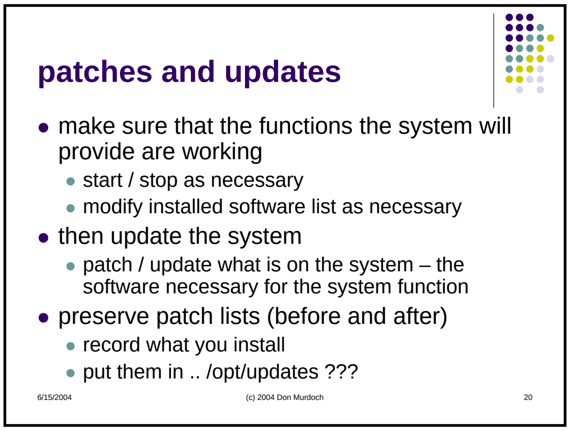
- protect /etc/inetd.conf
  - mode 600, root owned
  - remove entries that are not necessary
- there are two methods to protect net services for inetd based connections
  - tcp wrappers
  - xinetd
- each allow you to configure allowed connections and log connections



tcp wrappers

- tcp wrappers
  - modifies the inetd.conf entries by adding /usr/sbin/tcpd before the service name
  - follows the entries in hosts.allow and hosts.deny in the form “service:IPlist:options”
- example /etc/hosts.allow
  - ALL: LOCAL 10.0.25.0/255.255.255.0 10.0.30.0/255.255.255.0: RFC931:   BANNERS /usr/sbin/sec/banners
  - in.telnetd: 10.0.2.15:   BANNERS
- example /etc/hosts.deny
  - ALL:ALL

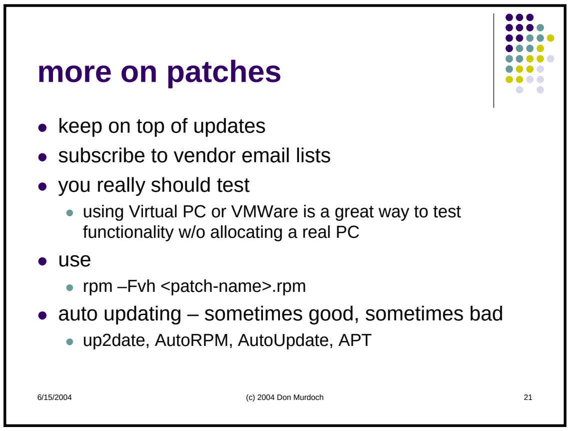
6/15/2004 (c) 2004 Don Murdoch 19



patches and updates

- make sure that the functions the system will provide are working
  - start / stop as necessary
  - modify installed software list as necessary
- then update the system
  - patch / update what is on the system – the software necessary for the system function
- preserve patch lists (before and after)
  - record what you install
  - put them in .. /opt/updates ???

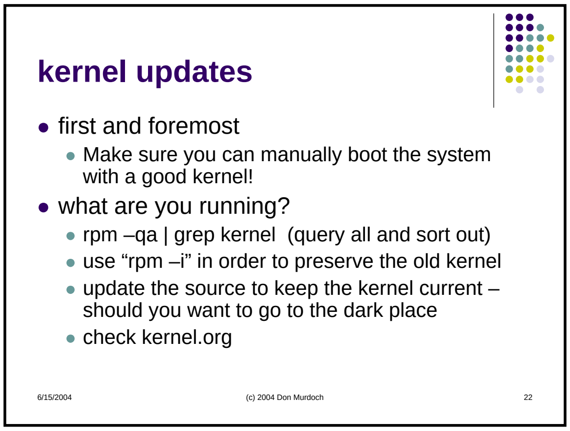
6/15/2004 (c) 2004 Don Murdoch 20



more on patches

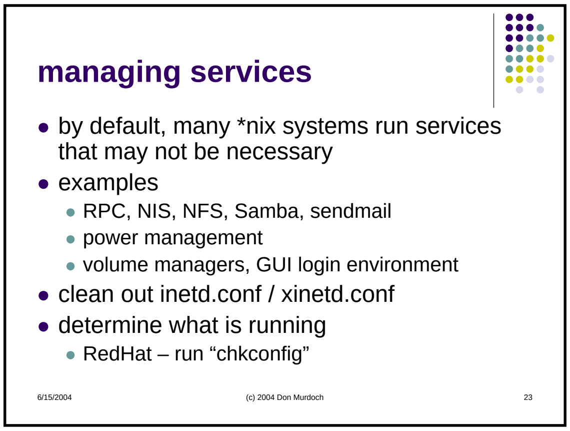
- keep on top of updates
- subscribe to vendor email lists
- you really should test
  - using Virtual PC or VMWare is a great way to test functionality w/o allocating a real PC
- use
  - rpm –Fvh <patch-name>.rpm
- auto updating – sometimes good, sometimes bad
  - up2date, AutoRPM, AutoUpdate, APT

6/15/2004 (c) 2004 Don Murdoch 21



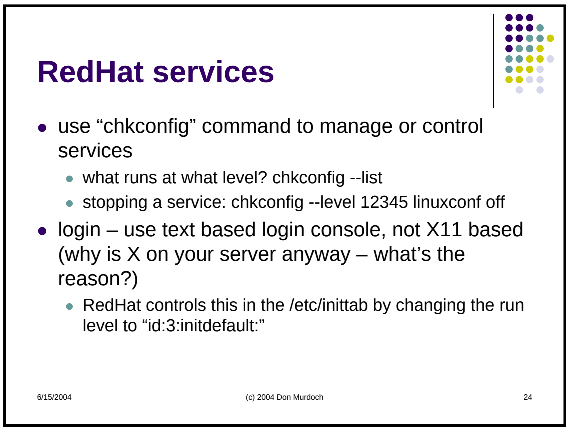
kernel updates

- first and foremost
  - Make sure you can manually boot the system with a good kernel!
- what are you running?
  - rpm –qa | grep kernel (query all and sort out)
  - use “rpm –i” in order to preserve the old kernel
  - update the source to keep the kernel current – should you want to go to the dark place
  - check kernel.org



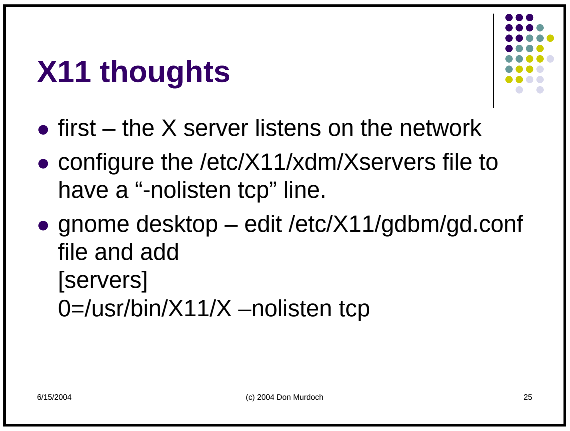
managing services

- by default, many *nix systems run services that may not be necessary
- examples
  - RPC, NIS, NFS, Samba, sendmail
  - power management
  - volume managers, GUI login environment
- clean out inetd.conf / xinetd.conf
- determine what is running
  - RedHat – run “chkconfig”



RedHat services

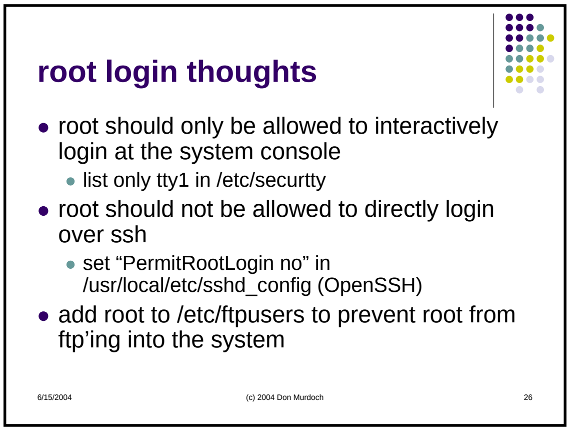
- use “chkconfig” command to manage or control services
  - what runs at what level? chkconfig --list
  - stopping a service: chkconfig --level 12345 linuxconf off
- login – use text based login console, not X11 based (why is X on your server anyway – what’s the reason?)
  - RedHat controls this in the /etc/inittab by changing the run level to “id:3:initdefault:”



X11 thoughts

- first – the X server listens on the network
- configure the /etc/X11/xdm/Xservers file to have a "-nolisten tcp" line.
- gnome desktop – edit /etc/X11/gdbm/gd.conf file and add
  [servers]
  0=/usr/bin/X11/X –nolisten tcp

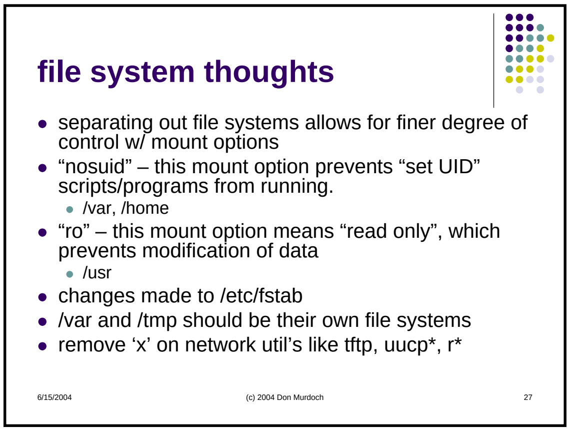
6/15/2004 (c) 2004 Don Murdoch 25



root login thoughts

- root should only be allowed to interactively login at the system console
  - list only tty1 in /etc/securtty
- root should not be allowed to directly login over ssh
  - set "PermitRootLogin no" in /usr/local/etc/sshd_config (OpenSSH)
- add root to /etc/ftpusers to prevent root from ftp'ing into the system

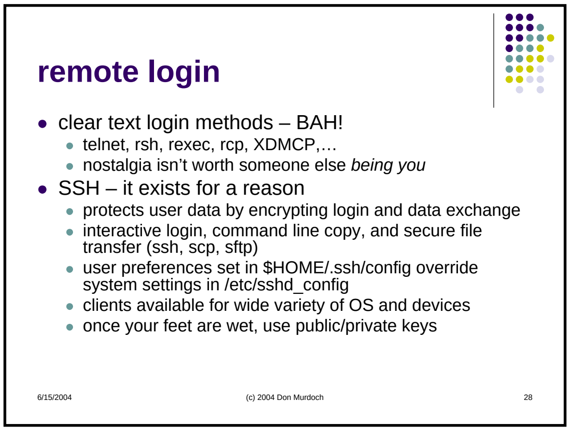
6/15/2004 (c) 2004 Don Murdoch 26



file system thoughts

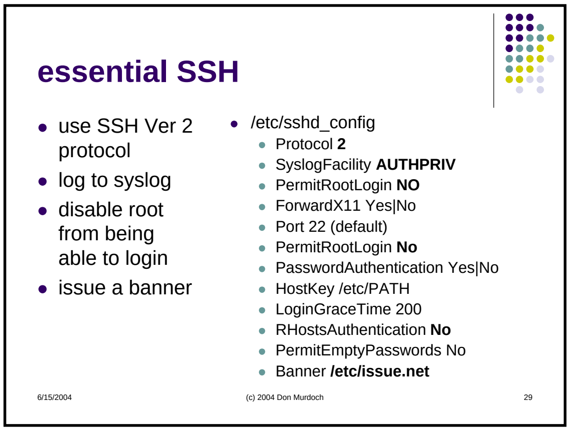
- separating out file systems allows for finer degree of control w/ mount options
- "nosuid" – this mount option prevents "set UID" scripts/programs from running.
  - /var, /home
- "ro" – this mount option means "read only", which prevents modification of data
  - /usr
- changes made to /etc/fstab
- /var and /tmp should be their own file systems
- remove 'x' on network util's like tftp, uucp*, r*

6/15/2004 (c) 2004 Don Murdoch 27



remote login

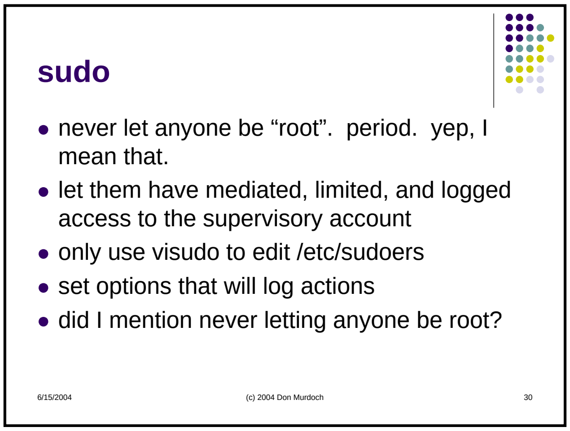
- clear text login methods – BAH!
  - telnet, rsh, rexec, rcp, XDMCP,…
  - nostalgia isn’t worth someone else *being you*
- SSH – it exists for a reason
  - protects user data by encrypting login and data exchange
  - interactive login, command line copy, and secure file transfer (ssh, scp, sftp)
  - user preferences set in $HOME/.ssh/config override system settings in /etc/sshd_config
  - clients available for wide variety of OS and devices
  - once your feet are wet, use public/private keys



essential SSH

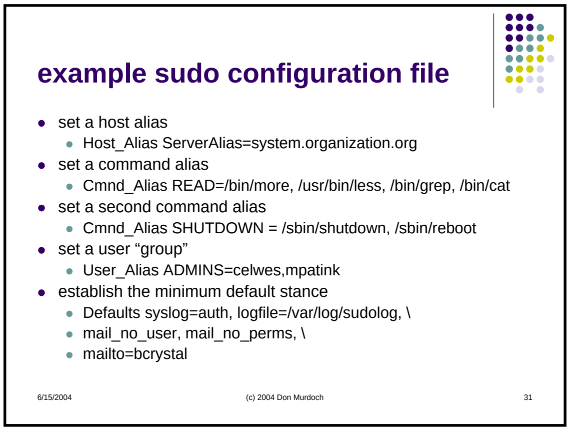
- use SSH Ver 2 protocol
- log to syslog
- disable root from being able to login
- issue a banner

- /etc/sshd_config
  - Protocol **2**
  - SyslogFacility **AUTHPRIV**
  - PermitRootLogin **NO**
  - ForwardX11 Yes|No
  - Port 22 (default)
  - PermitRootLogin **No**
  - PasswordAuthentication Yes|No
  - HostKey /etc/PATH
  - LoginGraceTime 200
  - RHostsAuthentication **No**
  - PermitEmptyPasswords No
  - Banner **/etc/issue.net**



sudo

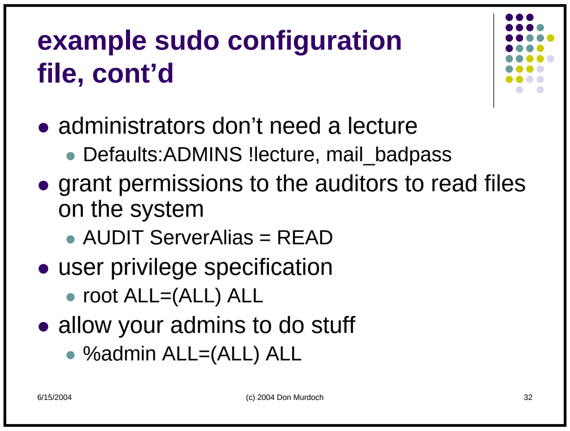
- never let anyone be “root”. period. yep, I mean that.
- let them have mediated, limited, and logged access to the supervisory account
- only use visudo to edit /etc/sudoers
- set options that will log actions
- did I mention never letting anyone be root?



example sudo configuration file

- set a host alias
  - Host_Alias ServerAlias=system.organization.org
- set a command alias
  - Cmnd_Alias READ=/bin/more, /usr/bin/less, /bin/grep, /bin/cat
- set a second command alias
  - Cmnd_Alias SHUTDOWN = /sbin/shutdown, /sbin/reboot
- set a user “group”
  - User_Alias ADMINS=celwes,mpatink
- establish the minimum default stance
  - Defaults syslog=auth, logfile=/var/log/sudolog, \
  - mail_no_user, mail_no_perms, \
  - mailto=bcrystal

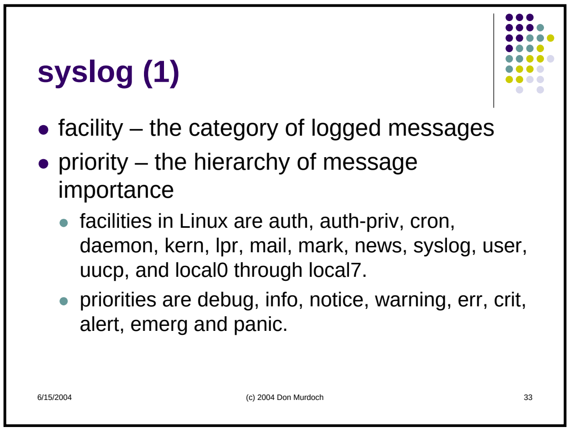
6/15/2004 (c) 2004 Don Murdoch 31



example sudo configuration file, cont’d

- administrators don’t need a lecture
  - Defaults:ADMINS !lecture, mail_badpass
- grant permissions to the auditors to read files on the system
  - AUDIT ServerAlias = READ
- user privilege specification
  - root ALL=(ALL) ALL
- allow your admins to do stuff
  - %admin ALL=(ALL) ALL

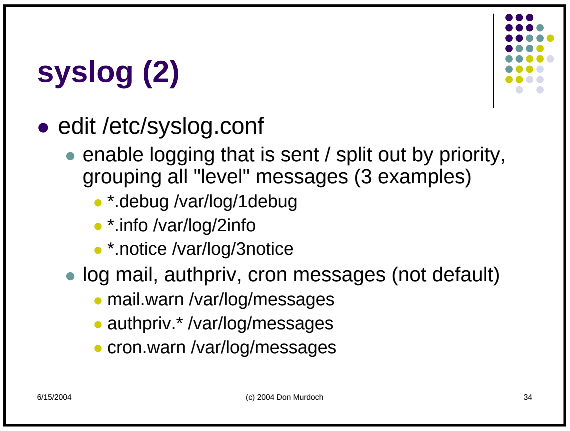
6/15/2004 (c) 2004 Don Murdoch 32



syslog (1)

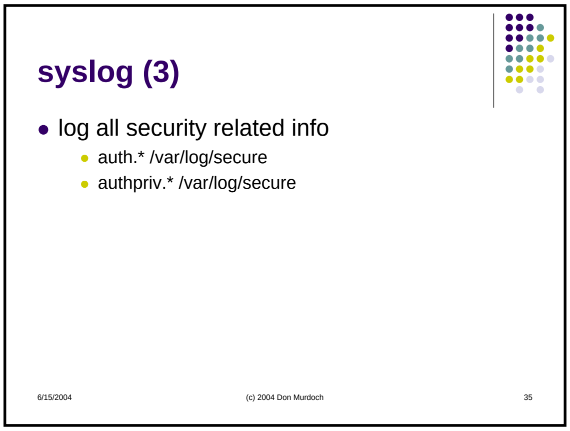
- facility – the category of logged messages
- priority – the hierarchy of message importance
  - facilities in Linux are auth, auth-priv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, and local0 through local7.
  - priorities are debug, info, notice, warning, err, crit, alert, emerg and panic.

6/15/2004 (c) 2004 Don Murdoch 33



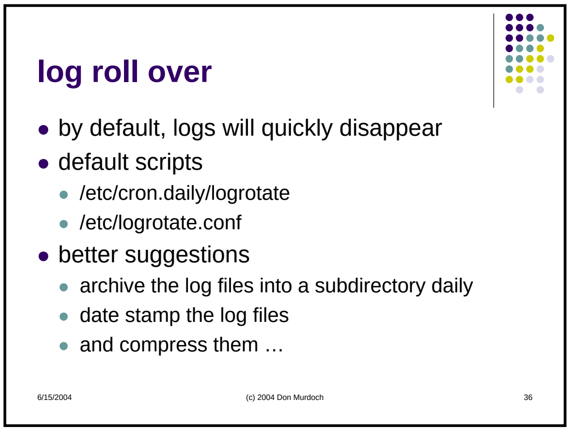
syslog (2)

- edit /etc/syslog.conf
  - enable logging that is sent / split out by priority, grouping all "level" messages (3 examples)
    - *.debug /var/log/1debug
    - *.info /var/log/2info
    - *.notice /var/log/3notice
  - log mail, authpriv, cron messages (not default)
    - mail.warn /var/log/messages
    - authpriv.* /var/log/messages
    - cron.warn /var/log/messages



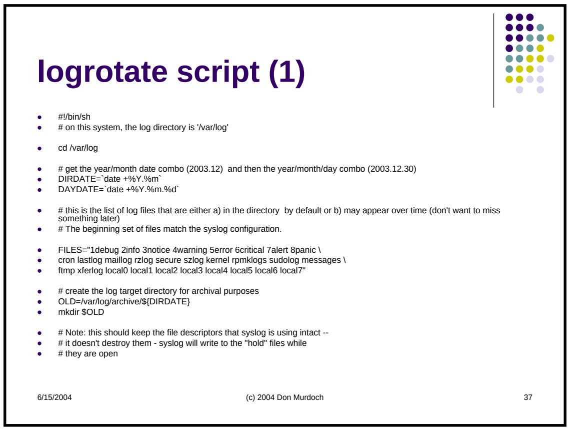
syslog (3)

- log all security related info
  - auth.* /var/log/secure
  - authpriv.* /var/log/secure



log roll over

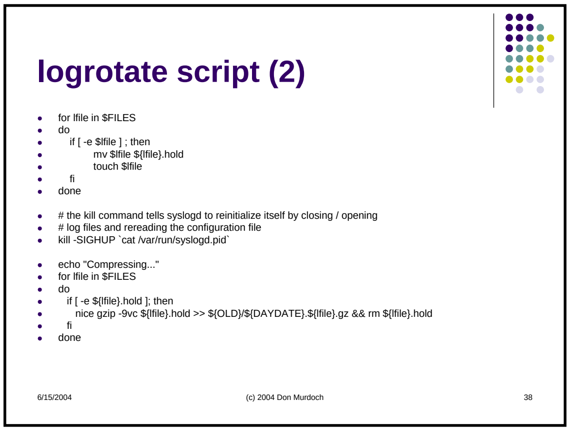
- by default, logs will quickly disappear
- default scripts
  - /etc/cron.daily/logrotate
  - /etc/logrotate.conf
- better suggestions
  - archive the log files into a subdirectory daily
  - date stamp the log files
  - and compress them …



logrotate script (1)

```
#!/bin/sh
# on this system, the log directory is '/var/log'

cd /var/log

# get the year/month date combo (2003.12)  and then the year/month/day combo (2003.12.30)
DIRDATE=`date +%Y.%m`
DAYDATE=`date +%Y.%m.%d`

# this is the list of log files that are either a) in the directory  by default or b) may appear over time (don't want to miss
something later)
# The beginning set of files match the syslog configuration.

FILES="1debug 2info 3notice 4warning 5error 6critical 7alert 8panic \
cron lastlog maillog rzlog secure szlog kernel rpmklogs sudolog messages \
ftmp xferlog local0 local1 local2 local3 local4 local5 local6 local7"

# create the log target directory for archival purposes
OLD=/var/log/archive/${DIRDATE}
mkdir $OLD

# Note: this should keep the file descriptors that syslog is using intact --
# it doesn't destroy them - syslog will write to the "hold" files while
# they are open
```

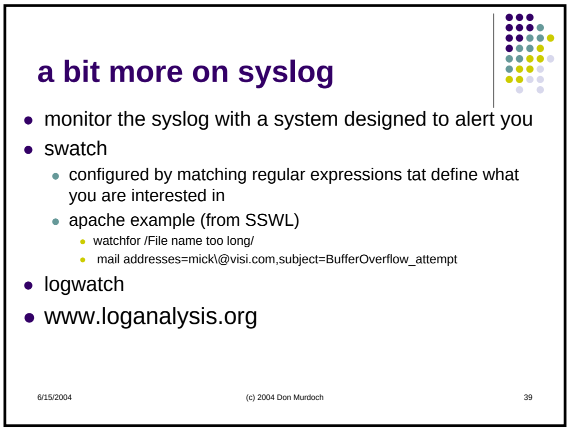
6/15/2004 (c) 2004 Don Murdoch 37



logrotate script (2)

```
for lfile in $FILES
do
   if [ -e $lfile ] ; then
            mv $lfile ${lfile}.hold
            touch $lfile
   fi
done

# the kill command tells syslogd to reinitialize itself by closing / opening
# log files and rereading the configuration file
kill -SIGHUP `cat /var/run/syslogd.pid`

echo "Compressing..."
for lfile in $FILES
do
  if [ -e ${lfile}.hold ]; then
     nice gzip -9vc ${lfile}.hold >> ${OLD}/${DAYDATE}.${lfile}.gz && rm ${lfile}.hold
  fi
done
```

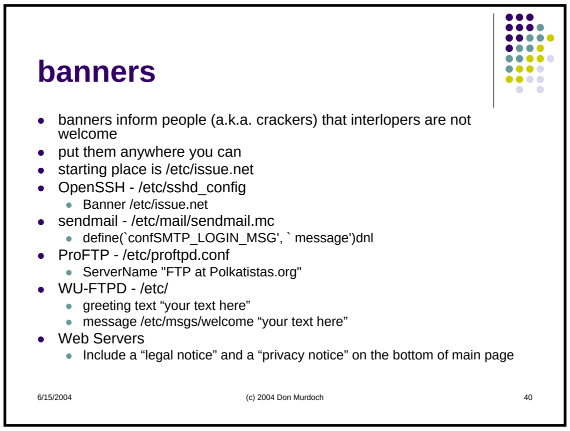
6/15/2004 (c) 2004 Don Murdoch 38



a bit more on syslog

- monitor the syslog with a system designed to alert you
- swatch
  - configured by matching regular expressions tat define what you are interested in
  - apache example (from SSWL)
    - watchfor /File name too long/
    - mail addresses=mick\@visi.com,subject=BufferOverflow_attempt
- logwatch
- www.loganalysis.org

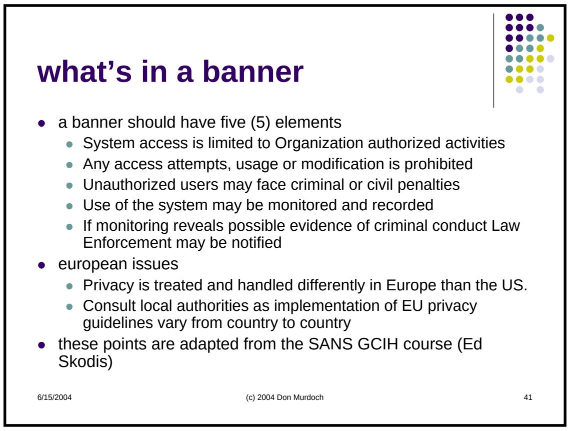
6/15/2004 (c) 2004 Don Murdoch 39



banners

- banners inform people (a.k.a. crackers) that interlopers are not welcome
- put them anywhere you can
- starting place is /etc/issue.net
- OpenSSH - /etc/sshd_config
  - Banner /etc/issue.net
- sendmail - /etc/mail/sendmail.mc
  - define(`confSMTP_LOGIN_MSG', ` message')dnl
- ProFTP - /etc/proftpd.conf
  - ServerName "FTP at Polkatistas.org"
- WU-FTPD - /etc/
  - greeting text “your text here”
  - message /etc/msgs/welcome “your text here”
- Web Servers
  - Include a “legal notice” and a “privacy notice” on the bottom of main page

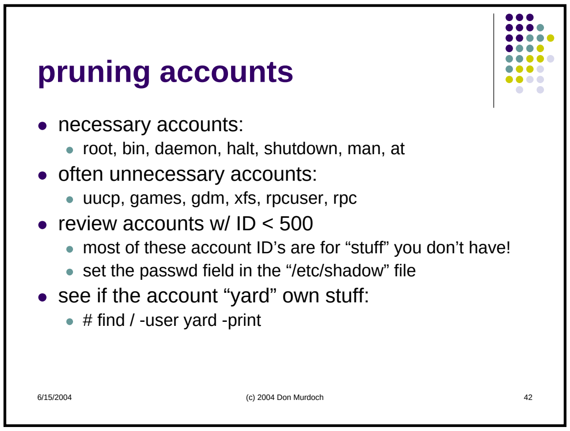
6/15/2004 (c) 2004 Don Murdoch 40



what’s in a banner

- a banner should have five (5) elements
  - System access is limited to Organization authorized activities
  - Any access attempts, usage or modification is prohibited
  - Unauthorized users may face criminal or civil penalties
  - Use of the system may be monitored and recorded
  - If monitoring reveals possible evidence of criminal conduct Law Enforcement may be notified
- european issues
  - Privacy is treated and handled differently in Europe than the US.
  - Consult local authorities as implementation of EU privacy guidelines vary from country to country
- these points are adapted from the SANS GCIH course (Ed Skodis)

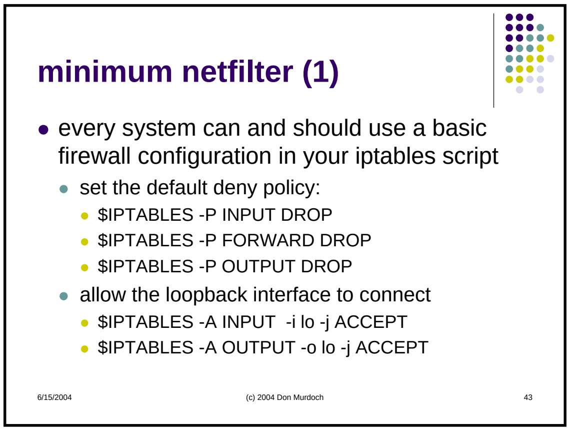
6/15/2004 (c) 2004 Don Murdoch 41



pruning accounts

- necessary accounts:
  - root, bin, daemon, halt, shutdown, man, at
- often unnecessary accounts:
  - uucp, games, gdm, xfs, rpcuser, rpc
- review accounts w/ ID < 500
  - most of these account ID’s are for “stuff” you don’t have!
  - set the passwd field in the “/etc/shadow” file
- see if the account “yard” own stuff:
  - # find / -user yard -print

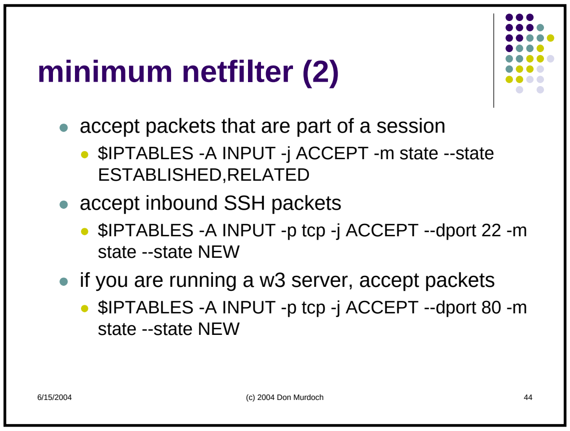
6/15/2004 (c) 2004 Don Murdoch 42



minimum netfilter (1)

- every system can and should use a basic firewall configuration in your iptables script
  - set the default deny policy:
    - $IPTABLES -P INPUT DROP
    - $IPTABLES -P FORWARD DROP
    - $IPTABLES -P OUTPUT DROP
  - allow the loopback interface to connect
    - $IPTABLES -A INPUT -i lo -j ACCEPT
    - $IPTABLES -A OUTPUT -o lo -j ACCEPT

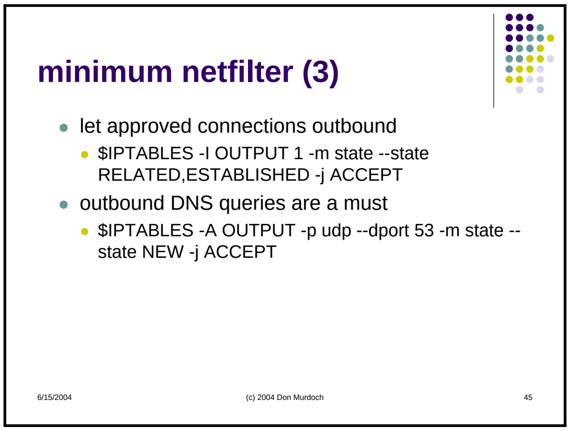
6/15/2004 (c) 2004 Don Murdoch 43



minimum netfilter (2)

- accept packets that are part of a session
  - $IPTABLES -A INPUT -j ACCEPT -m state --state ESTABLISHED,RELATED
- accept inbound SSH packets
  - $IPTABLES -A INPUT -p tcp -j ACCEPT --dport 22 -m state --state NEW
- if you are running a w3 server, accept packets
  - $IPTABLES -A INPUT -p tcp -j ACCEPT --dport 80 -m state --state NEW

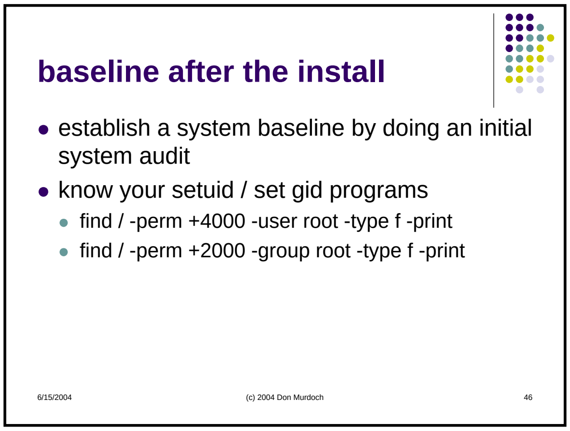
6/15/2004 (c) 2004 Don Murdoch 44



minimum netfilter (3)

- let approved connections outbound
  - $IPTABLES -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT
- outbound DNS queries are a must
  - $IPTABLES -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

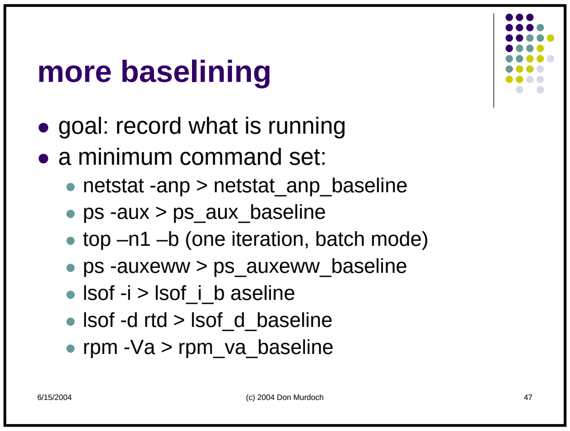
6/15/2004 (c) 2004 Don Murdoch 45



baseline after the install

- establish a system baseline by doing an initial system audit
- know your setuid / set gid programs
  - find / -perm +4000 -user root -type f -print
  - find / -perm +2000 -group root -type f -print

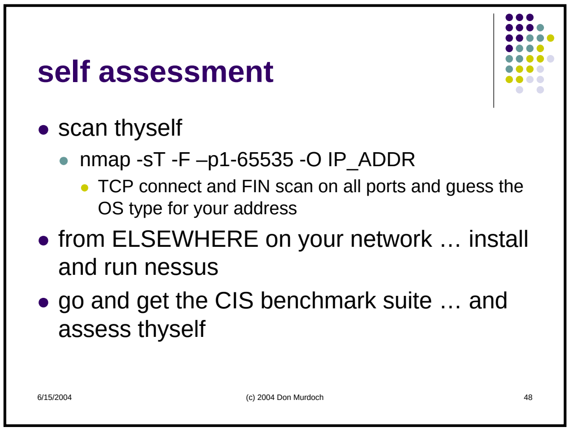
6/15/2004 (c) 2004 Don Murdoch 46



more baselining

- goal: record what is running
- a minimum command set:
  - netstat -anp > netstat_anp_baseline
  - ps -aux > ps_aux_baseline
  - top –n1 –b (one iteration, batch mode)
  - ps -auxeww > ps_auxeww_baseline
  - lsof -i > lsof_i_b aseline
  - lsof -d rtd > lsof_d_baseline
  - rpm -Va > rpm_va_baseline

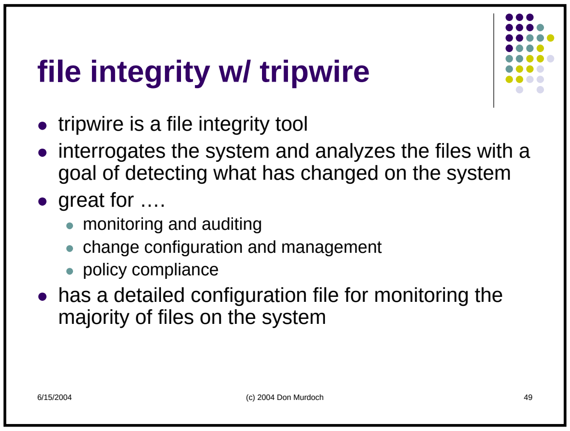
6/15/2004 (c) 2004 Don Murdoch 47



self assessment

- scan thyself
  - nmap -sT -F –p1-65535 -O IP_ADDR
    - TCP connect and FIN scan on all ports and guess the OS type for your address
- from ELSEWHERE on your network … install and run nessus
- go and get the CIS benchmark suite … and assess thyself

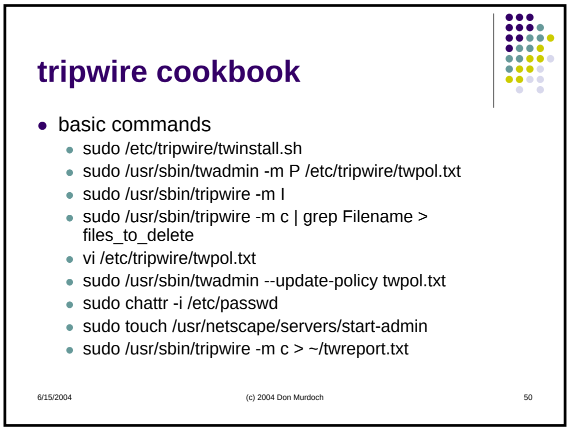
6/15/2004 (c) 2004 Don Murdoch 48



file integrity w/ tripwire

- tripwire is a file integrity tool
- interrogates the system and analyzes the files with a goal of detecting what has changed on the system
- great for ….
  - monitoring and auditing
  - change configuration and management
  - policy compliance
- has a detailed configuration file for monitoring the majority of files on the system

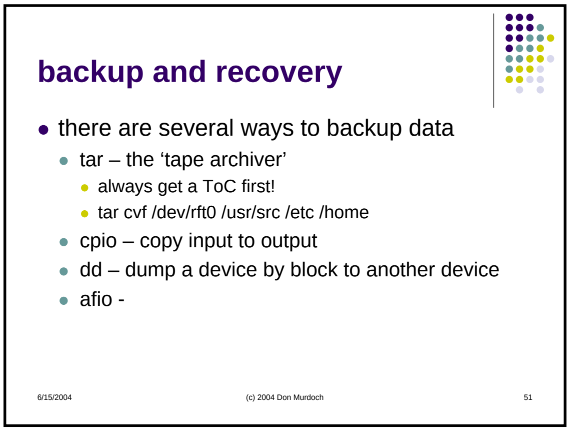
6/15/2004 (c) 2004 Don Murdoch 49



tripwire cookbook

- basic commands
  - sudo /etc/tripwire/twinstall.sh
  - sudo /usr/sbin/twadmin -m P /etc/tripwire/twpol.txt
  - sudo /usr/sbin/tripwire -m I
  - sudo /usr/sbin/tripwire -m c | grep Filename > files_to_delete
  - vi /etc/tripwire/twpol.txt
  - sudo /usr/sbin/twadmin --update-policy twpol.txt
  - sudo chattr -i /etc/passwd
  - sudo touch /usr/netscape/servers/start-admin
  - sudo /usr/sbin/tripwire -m c > ~/twreport.txt

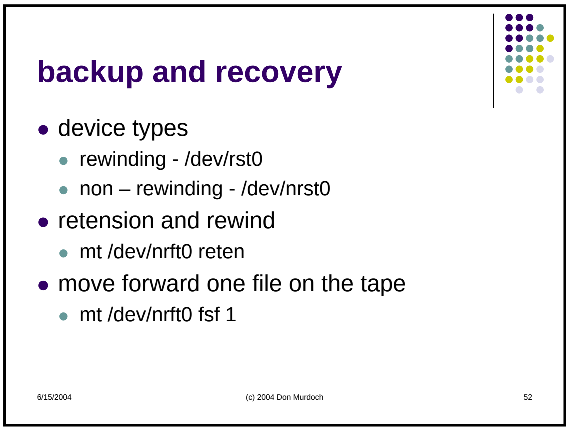
6/15/2004 (c) 2004 Don Murdoch 50



backup and recovery

- there are several ways to backup data
  - tar – the 'tape archiver'
    - always get a ToC first!
    - tar cvf /dev/rft0 /usr/src /etc /home
  - cpio – copy input to output
  - dd – dump a device by block to another device
  - afio -

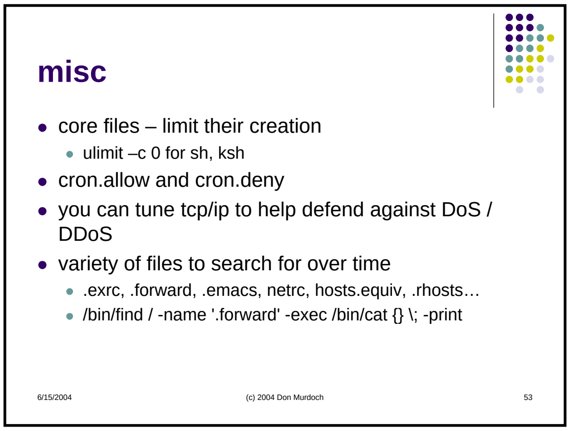
6/15/2004 (c) 2004 Don Murdoch 51



backup and recovery

- device types
  - rewinding - /dev/rst0
  - non – rewinding - /dev/nrst0
- retension and rewind
  - mt /dev/nrft0 reten
- move forward one file on the tape
  - mt /dev/nrft0 fsf 1

6/15/2004 (c) 2004 Don Murdoch 52



misc

- core files – limit their creation
  - ulimit –c 0 for sh, ksh
- cron.allow and cron.deny
- you can tune tcp/ip to help defend against DoS / DDoS
- variety of files to search for over time
  - .exrc, .forward, .emacs, netrc, hosts.equiv, .rhosts…
  - /bin/find / -name '.forward' -exec /bin/cat {} \; -print

6/15/2004 (c) 2004 Don Murdoch 53