CIS551: Computer and Network Security

Jonathan M. Smith

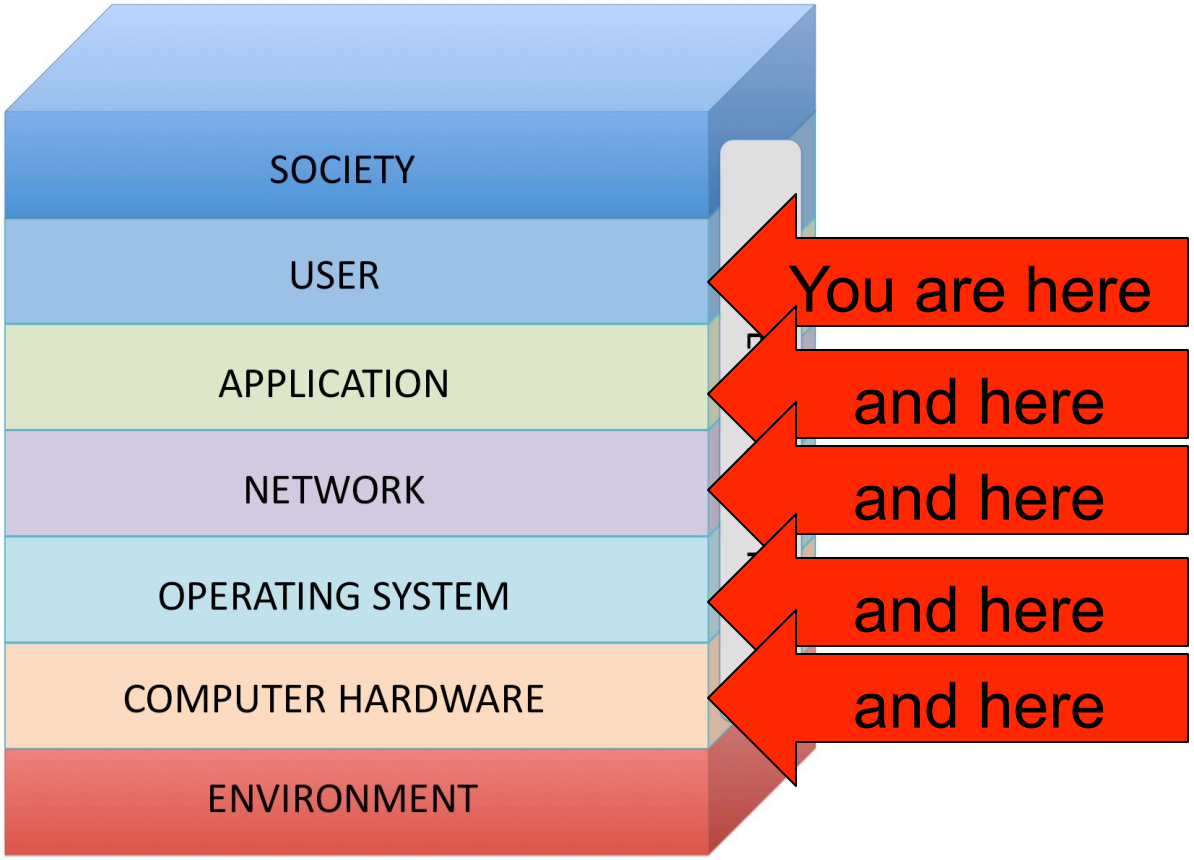
jms@cis.upenn.edu

03/03/2014

CIS551 Topics

- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems Viewpoint
  - Users, social engineering, insider threats

Sincoskie NIS model



W.D. Sincoskie, *et al.* “Layer Dissonance and Closure in Networked Information Security” (white paper)

System Administration

- SysAdmin is a key part of security
- Automated systems amplify effects
- But there is no substitute for “eyeballs”
  - Automation is not yet capable enough
- Two major goals
  - Correct configuration
  - Maintenance (and “firefighting”)

Correct configuration

- Varies, of course, by user
- Two primary contexts
  - Personal machine (e.g., laptop)
  - Shared servers (e.g., speclab, eniac)
- Use access control, user authorizations to control confidentiality and integrity
  - E.g., access to home directory, e-mail folders, personal programs

Things to consider (server)

- User accounts and privileges
  - E.g., administrator/administrative group
- Default “umask” on UNIX
- Initial user setups
- Setuid programs
- Insulating against insider threats
- Logging
- System configuration (firewalls, network interfaces up such as WiFi, Bluetooth)

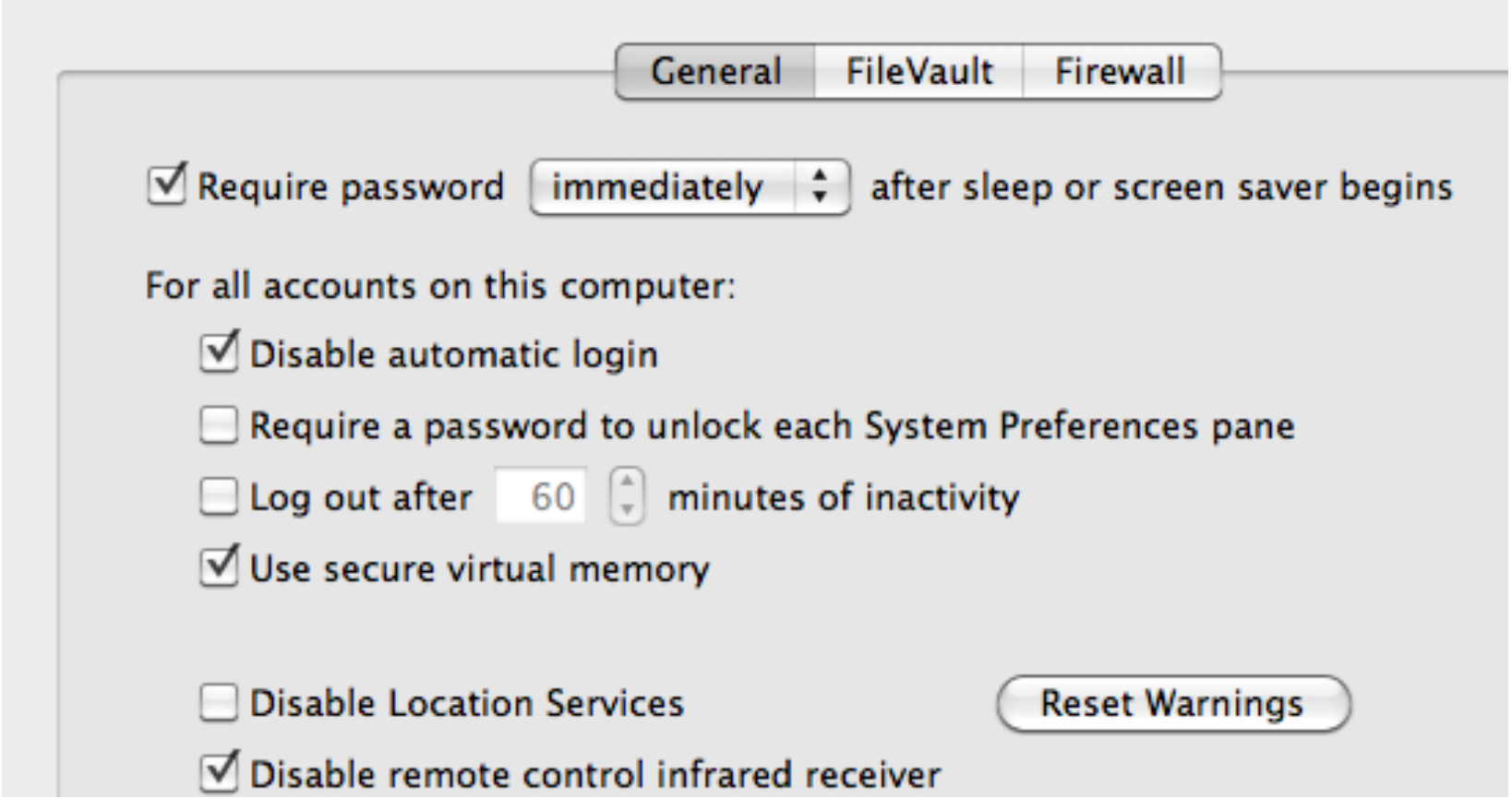
Things to consider (personal)

- Permissions on files
- Browser configurations
- System configuration (services, network interfaces, etc.)
- Visibility / responsiveness to entities
  - Which ports are open? (use nmap tool)
- Logging and Monitoring

Configuration tool examples

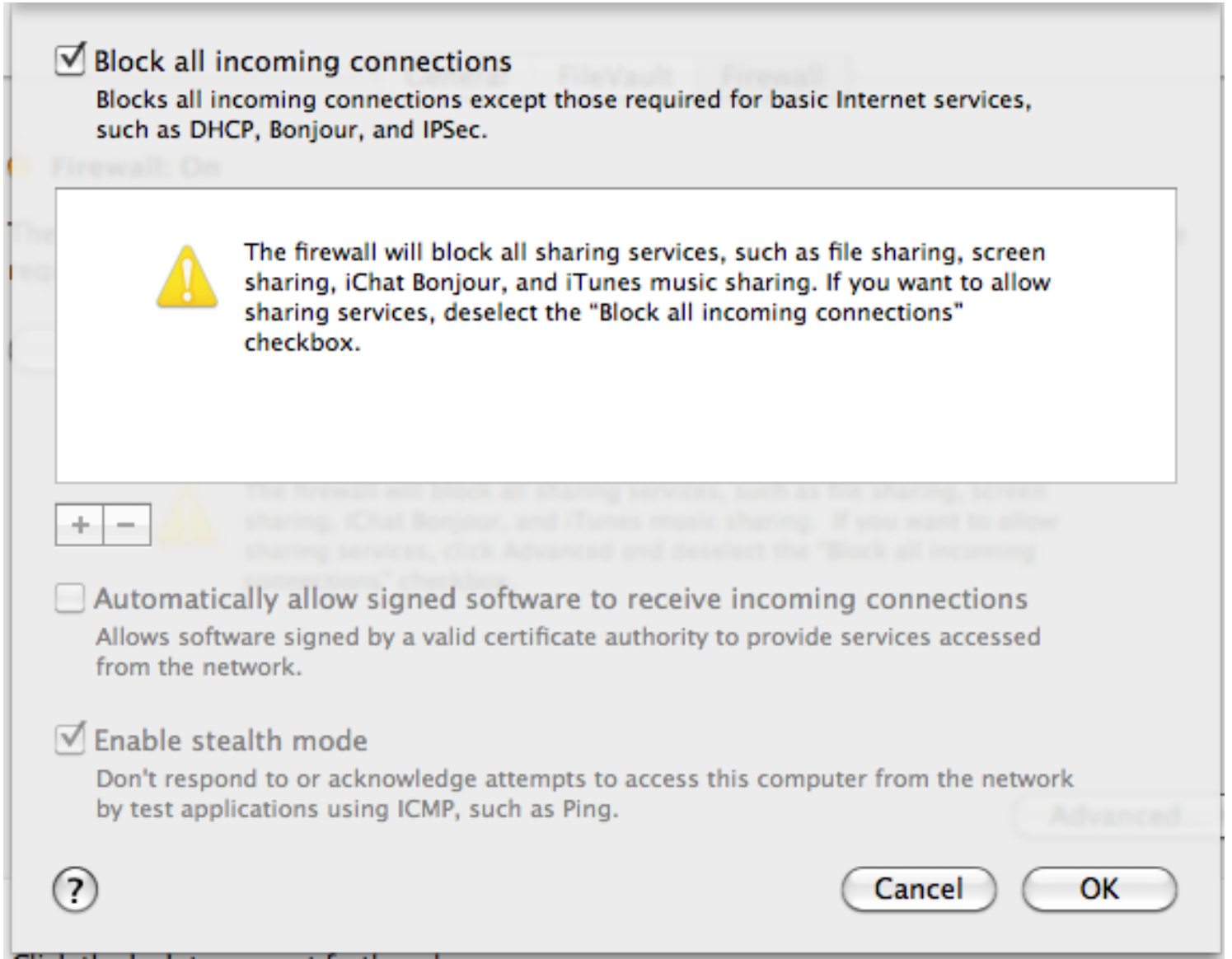
- nmap 127.0.0.1 – check your ports
- ifconfig or netstat –i
- Various configuration UIs (*e.g.*, “System Preferences” or application “Preferences” on Mac)
- “ps” or “Activity Monitor”

Security preferences 1



Security preferences 2

Security preferences 3



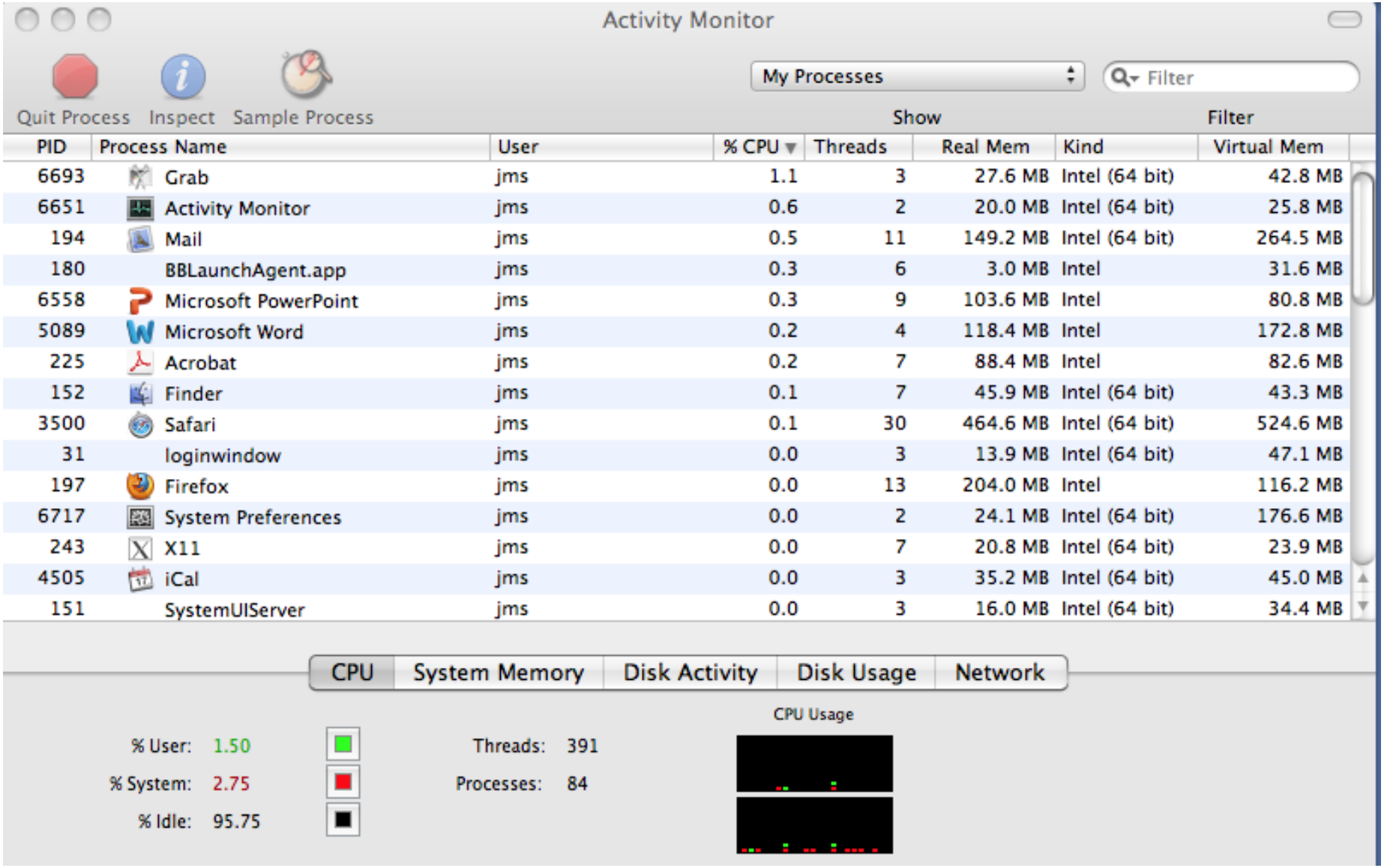
netstat -i

```
bash-3.2$ netstat -i
Name  Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16384 <Link#1>                        10697     0    10696     0     0
lo0   16384 localhost   ::1                 10697     -    10696     -     -
lo0   16384 localhost   fe80:1::1           10697     -    10696     -     -
lo0   16384 127           localhost         10697     -    10696     -     -
gif0* 1280  <Link#2>                            0     0        0     0     0
stf0* 1280  <Link#3>                            0     0        0     0     0
en0   1500  <Link#4>    00:26:4a:18:e6:86   404376   728   253000 11662     0
en0   1500  158.130.50/23 seasnet-50-11.c    404376     -   253000     -     -
fw0   4078  <Link#5>    00:26:4a:ff:fe:18:e6:86      0     0        0     0     0
en1   1500  <Link#6>    00:26:bb:02:af:fb        0     0        0     0     0
bash-3.2$
```

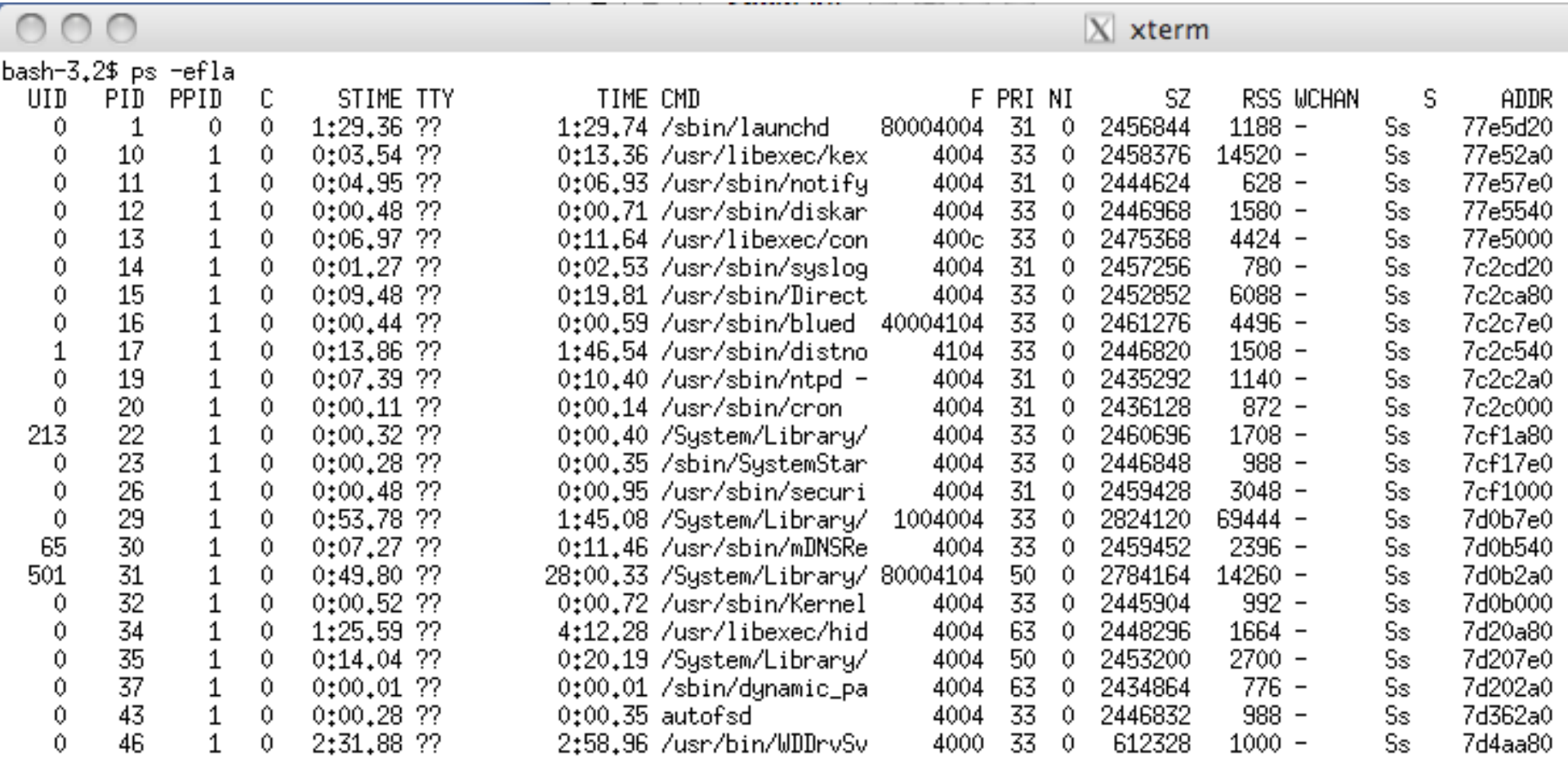
nmap

```
bash-3.2$ nmap 127.0.0.1

Starting Nmap 4.76 ( http://nmap.org ) at 2011-03-15 08:40 EDT
Interesting ports on localhost (127.0.0.1):
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds
bash-3.2$ grep 631 /etc/services
ipp             631/udp     # IPP (Internet Printing Protocol)
ipp             631/tcp     # IPP (Internet Printing Protocol)
```

Activity monitor



ps


xterm
bash-3.2$ ps -efla
UID PID PPID C STIME TTY TIME CMD F PRI NI SZ RSS WCHAN S ADDR
0 1 0 0 1:29.36 ?? 1:29.74 /sbin/launchd 80004004 31 0 2456844 1188 - Ss 77e5d20
0 10 1 0 0:03.54 ?? 0:13.36 /usr/libexec/kex 4004 33 0 2458376 14520 - Ss 77e52a0
0 11 1 0 0:04.95 ?? 0:06.93 /usr/sbin/notify 4004 31 0 2444624 628 - Ss 77e57e0
0 12 1 0 0:00.48 ?? 0:00.71 /usr/sbin/diskar 4004 33 0 2446968 1580 - Ss 77e5540
0 13 1 0 0:06.97 ?? 0:11.64 /usr/libexec/con 400c 33 0 2475368 4424 - Ss 77e5000
0 14 1 0 0:01.27 ?? 0:02.53 /usr/sbin/syslog 4004 31 0 2457256 780 - Ss 7c2cd20
0 15 1 0 0:09.48 ?? 0:19.81 /usr/sbin/Direct 4004 33 0 2452852 6088 - Ss 7c2ca80
0 16 1 0 0:00.44 ?? 0:00.59 /usr/sbin/blued 40004104 33 0 2461276 4496 - Ss 7c2c7e0
1 17 1 0 0:13.86 ?? 1:46.54 /usr/sbin/distno 4104 33 0 2446820 1508 - Ss 7c2c540
0 19 1 0 0:07.39 ?? 0:10.40 /usr/sbin/ntpd - 4004 31 0 2435292 1140 - Ss 7c2c2a0
0 20 1 0 0:00.11 ?? 0:00.14 /usr/sbin/cron 4004 31 0 2436128 872 - Ss 7c2c000
213 22 1 0 0:00.32 ?? 0:00.40 /System/Library/ 4004 33 0 2460696 1708 - Ss 7cf1a80
0 23 1 0 0:00.28 ?? 0:00.35 /sbin/SystemStar 4004 33 0 2446848 988 - Ss 7cf17e0
0 26 1 0 0:00.48 ?? 0:00.95 /usr/sbin/securi 4004 31 0 2459428 3048 - Ss 7cf1000
0 29 1 0 0:53.78 ?? 1:45.08 /System/Library/ 1004004 33 0 2824120 69444 - Ss 7d0b7e0
65 30 1 0 0:07.27 ?? 0:11.46 /usr/sbin/mDNSRe 4004 33 0 2459452 2396 - Ss 7d0b540
501 31 1 0 0:49.80 ?? 28:00.33 /System/Library/ 80004104 50 0 2784164 14260 - Ss 7d0b2a0
0 32 1 0 0:00.52 ?? 0:00.72 /usr/sbin/Kernel 4004 33 0 2445904 992 - Ss 7d0b000
0 34 1 0 1:25.59 ?? 4:12.28 /usr/libexec/hid 4004 63 0 2448296 1664 - Ss 7d20a80
0 35 1 0 0:14.04 ?? 0:20.19 /System/Library/ 4004 50 0 2453200 2700 - Ss 7d207e0
0 37 1 0 0:00.01 ?? 0:00.01 /sbin/dynamic_pa 4004 63 0 2434864 776 - Ss 7d202a0
0 43 1 0 0:00.28 ?? 0:00.35 autofsd 4004 33 0 2446832 988 - Ss 7d362a0
0 46 1 0 2:31.88 ?? 2:58.96 /usr/bin/WDDrvSv 4000 33 0 612328 1000 - Ss 7d4aa80

SysAdmin: logs

- Often neglected
- On *nixes usually in /var/log
- Applications, services, hardware, topical
- Best used to detect anomalies
  - To create “that’s funny….” reaction
- Malware tries not to get logged
- Crackers will delete or edit logs

/var/log

```
bash-3.2$ ls /var/log
CDIS.custom              cups                     install.log.5.bz2        monthly.out              system.log.2.bz2
DiagnosticMessages       daily.out                ipfw.log                 ppp                      system.log.3.bz2
alf.log                  dpd.log                  kernel.log               privoxy                  system.log.4.bz2
apache2                  fax                      kernel.log.0.bz2         sa                       system.log.5.bz2
appfirewall.log          fsck_hfs.log             kernel.log.1.bz2         samba                    system.log.6.bz2
appfirewall.log.0.bz2    hdiejectd.log            kernel.log.2.bz2         secure.log               system.log.7.bz2
appfirewall.log.1.bz2    install.log              kernel.log.3.bz2         secure.log.0.bz2         uucp
appfirewall.log.2.bz2    install.log.0.bz2        kernel.log.4.bz2         securityproxy            weekly.out
appfirewall.log.3.bz2    install.log.1.bz2        krb5kdc                  snort                    windowserver.log
appfirewall.log.4.bz2    install.log.2.bz2        launchd-shutdown.log     system.log               windowserver_last.log
appfirewall.log.5.bz2    install.log.3.bz2        launchd-shutdown.log.1   system.log.0.bz2
asl                      install.log.4.bz2        mail.log                 system.log.1.bz2
bash-3.2$
```

Printer logs (Mac)

```
localhost - _AUTHREF_ [07/Mar/2011:05:04:46 -0500] "POST /admin HTTP/1.1" 200 209 CUPS-Add-Modify-Printer successful-ok
localhost - - [14/Mar/2011:07:19:52 -0400] "POST /admin HTTP/1.1" 401 199 CUPS-Add-Modify-Printer successful-ok
localhost - _AUTHREF_ [14/Mar/2011:07:19:52 -0400] "POST /admin HTTP/1.1" 200 199 CUPS-Add-Modify-Printer successful-ok
localhost - - [14/Mar/2011:09:21:40 -0400] "POST /admin HTTP/1.1" 401 209 CUPS-Add-Modify-Printer successful-ok
localhost - _AUTHREF_ [14/Mar/2011:09:21:40 -0400] "POST /admin HTTP/1.1" 200 209 CUPS-Add-Modify-Printer successful-ok
localhost - - [14/Mar/2011:09:22:01 -0400] "POST /admin HTTP/1.1" 401 199 CUPS-Add-Modify-Printer successful-ok
localhost - _AUTHREF_ [14/Mar/2011:09:22:01 -0400] "POST /admin HTTP/1.1" 200 199 CUPS-Add-Modify-Printer successful-ok
localhost - - [14/Mar/2011:13:36:10 -0400] "POST /printers/HP_LaserJet_1160_series HTTP/1.1" 200 1313 Create-Job successful-ok
localhost - - [14/Mar/2011:13:36:10 -0400] "POST /printers/HP_LaserJet_1160_series HTTP/1.1" 200 776175 Send-Document successf
ul-ok
localhost - - [14/Mar/2011:16:49:58 -0400] "POST /printers/HP_LaserJet_1160_series HTTP/1.1" 200 1323 Create-Job successful-ok
localhost - - [14/Mar/2011:16:49:58 -0400] "POST /printers/HP_LaserJet_1160_series HTTP/1.1" 200 328499 Send-Document successf
ul-ok
localhost - - [14/Mar/2011:16:58:42 -0400] "POST /admin HTTP/1.1" 401 209 CUPS-Add-Modify-Printer successful-ok
localhost - _AUTHREF_ [14/Mar/2011:16:58:42 -0400] "POST /admin HTTP/1.1" 200 209 CUPS-Add-Modify-Printer successful-ok
localhost - - [15/Mar/2011:08:18:49 -0400] "POST /admin HTTP/1.1" 401 199 CUPS-Add-Modify-Printer successful-ok
localhost - _AUTHREF_ [15/Mar/2011:08:18:49 -0400] "POST /admin HTTP/1.1" 200 199 CUPS-Add-Modify-Printer successful-ok
bash-3.2$ pwd
/var/log/cups
bash-3.2$ ls
access_log      error_log       page_log
bash-3.2$
```

grep “Stealth” Appfirewall.log

```
Mar 15 10:16:18 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:137 from 158.130.50.233:137
Mar 15 10:17:05 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:57118 from 128.91.2.13:53
Mar 15 10:17:48 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:52276 from 128.91.2.13:53
Mar 15 10:18:08 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:137 from 158.130.50.233:137
Mar 15 10:18:09 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:137 from 158.130.50.233:137
Mar 15 10:18:40 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:61661 from 128.91.2.13:53
Mar 15 10:18:58 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:137 from 158.130.50.233:137
Mar 15 10:18:58 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:137 from 158.130.50.233:137
Mar 15 10:19:04 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to TCP 158.130.50.12:5189 from 194.28.157.83:80
Mar 15 10:20:03 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:63767 from 128.91.2.13:53
Mar 15 10:21:10 seasnet-50-11 Firewall[74]: Stealth Mode connection attempt to UDP 158.130.50.12:61166 from 128.91.2.13:53
bash-3.2$ traceroute 194.28.157.83
traceroute to 194.28.157.83 (194.28.157.83), 64 hops max, 52 byte packets
 1  subnet-50-router.seas.upenn.edu (158.130.50.1)  69.545 ms  1.067 ms  0.945 ms
 2  isc-uplink-2.seas.upenn.edu (158.130.128.2)  0.926 ms  1.207 ms  0.886 ms
 3  external3-core2.dccs.upenn.edu (128.91.10.2)  0.824 ms  0.870 ms  0.813 ms
 4  external-core1.dccs.upenn.edu (128.91.9.1)  1.029 ms  0.993 ms  0.889 ms
 5  ge-8-46.car2.philadelphia1.level3.net (4.78.155.1)  1.445 ms  1.943 ms  1.502 ms
 6  ae-6-6.ebr1.newyork1.level3.net (4.69.133.170)  3.506 ms  3.510 ms  3.655 ms
 7  ae-81-81.csw3.newyork1.level3.net (4.69.134.74)  7.455 ms
    ae-91-91.csw4.newyork1.level3.net (4.69.134.78)  12.727 ms
    ae-61-61.csw1.newyork1.level3.net (4.69.134.66)  4.753 ms
 8  ae-13-69.car3.newyork1.level3.net (4.68.16.5)  3.878 ms
    ae-43-99.car3.newyork1.level3.net (4.68.16.197)  4.563 ms
    ae-33-89.car3.newyork1.level3.net (4.68.16.133)  3.911 ms
 9  tiscali-level3-ge.newyork1.level3.net (4.68.110.78)  3.779 ms  3.710 ms  3.598 ms
10  xe-0-1-0.was14.ip4.tinet.net (89.149.185.6)  11.612 ms
    xe-2-0-0.was14.ip4.tinet.net (89.149.185.18)  22.017 ms
    xe-1-1-0.was14.ip4.tinet.net (89.149.182.13)  21.752 ms
11  194-28-156-61.zenprotection.com (194.28.156.61)  8.220 ms  21.929 ms  8.151 ms
12  194-28-156-117.zenprotection.com (194.28.156.117)  21.923 ms  8.189 ms  8.148 ms
13  194-28-156-83.zenprotection.com (194.28.156.83)  21.849 ms  21.917 ms  22.406 ms
14  194-28-156-42.zenprotection.com (194.28.156.42)  19.804 ms  28.133 ms  23.598 ms
15  194-28-157-83.zenprotection.com (194.28.157.83)  22.705 ms  8.464 ms  21.703 ms
bash-3.2$
```

install.log

```
bash-3.2$ tail install.log
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Printer HP_Pdf2Pdf1 does not require an update.
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Connected printer: MANUFACTURER:HP;MODEL:Deskjet F4100 series
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Printer HP_ResourceManager does not require an update.
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Connected printer: MANUFACTURER:HP;MODEL:Deskjet F4100 series
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Printer HP_Scan does not require an update.
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Connected printer: MANUFACTURER:HP;MODEL:Deskjet F4100 series
Mar 14 21:25:12 new-host-2 Software Update[6275]: JS: Printer HP_SmartX does not require an update.
Mar 14 21:25:13 new-host-2 Software Update[6275]: Package Authoring: my.result.title and my.result.message not define
d or empty
Mar 14 21:25:30 new-host-2 Software Update[6275]: Can't load distribution from http://swcdn.apple.com/content/downloa
ds/56/40/061-7230/SnZ47R2KJ5FQG6QGQ3Fksq5mzxt59bhbNH/061-7230.English.dist: Error Domain=NSURLErrorDomain Code=-1001
UserInfo=0x1165c7300 "The request timed out." Underlying Error=(Error Domain=kCFErrorDomainCFNetwork Code=-1001 UserI
nfo=0x116571070 "The request timed out.")
Mar 14 21:25:31 new-host-2 Software Update[6275]: JS: 10.6.6
bash-3.2$
```

Secure.log

```
bash-3.2$ tail secure.log
Mar 15 07:08:19 Macintosh loginwindow[31]: in pam_sm_authenticate(): Failed to determine Kerberos principal name.
Mar 15 07:38:03 Macintosh loginwindow[31]: in pam_sm_authenticate(): Failed to determine Kerberos principal name.
Mar 15 08:18:49 Macintosh com.apple.SecurityServer[26]: Succeeded authorizing right 'system.print.admin' by client '/System/Li
brary/Printers/Libraries/makequeuesagent' for authorization created by '/System/Library/Printers/Libraries/makequeuesagent'
Mar 15 08:18:49 Macintosh com.apple.SecurityServer[26]: Succeeded authorizing right 'system.print.admin' by client '/System/Li
brary/SystemConfiguration/PrinterNotifications.bundle/Contents/MacOS/makequeues' for authorization created by '/System/Library
/SystemConfiguration/PrinterNotifications.bundle/Contents/MacOS/makequeues'
Mar 15 08:18:49 Macintosh com.apple.SecurityServer[26]: Succeeded authorizing right 'system.print.admin' by client '/usr/sbin/
cupsd' for authorization created by '/System/Library/SystemConfiguration/PrinterNotifications.bundle/Contents/MacOS/makequeues
'
Mar 15 08:19:06 seasnet-50-11 loginwindow[31]: in pam_sm_authenticate(): Failed to determine Kerberos principal name.
Mar 15 08:53:31 seasnet-50-11 com.apple.SecurityServer[26]: UID 501 authenticated as user jms (UID 501) for right 'system.pref
erences.security'
Mar 15 08:53:31 seasnet-50-11 com.apple.SecurityServer[26]: Succeeded authorizing right 'system.preferences.security' by clien
t '/Applications/System Preferences.app' for authorization created by '/Applications/System Preferences.app'
Mar 15 08:53:32 seasnet-50-11 com.apple.SecurityServer[26]: Succeeded authorizing right 'system.preferences' by client '/Syste
m/Library/PrivateFrameworks/Admin.framework/Versions/A/Resources/writeconfig' for authorization created by '/Applications/Syst
em Preferences.app'
Mar 15 09:43:03 seasnet-50-11 loginwindow[31]: in pam_sm_authenticate(): Failed to determine Kerberos principal name.
bash-3.2$
```