Brian Cullinan

11/8/2010

Computer Security – HW 3

Task 1:

I have already created a user account. I used the command “useradd” instead of “adduser” intentionally so that it would not create a home directory and I would not be discovered. I did this the first day root was obtained on the box. I have used a non-standard password for me, and I added myself to the admin group so I could use “sudo”. “pwconv” converts a “passwd” file in to a shadow file by removing the passwords from the “passwd” file and putting them in a differently formatted “shadow” file.

Task 2:

“daemon” is used for all programs that run servers in the background. “nobody” is a user and group that allows to run programs without being associated with any account, this has very limited permissions and is useful for securing webservers. “dhcp” is for running a dhcp server under that user and group, it allows users to query the dhcp server, but not necessarily make changes to the system. “uucp” is used for copying files between unix based systems. “gdm” is the user account the desktop manager runs under. These default accounts are not necessarily needed, but they add a level of abstraction to process control. When a process runs as these users, it is generally not able to make changes to other parts of the system. If used properly these accounts are helpful, but just like anything else that it highly configurable, they can be abused.

Task 3:

Set user ID and set group ID bits are used for forcing the user and group for newly created files. When a file is created the user and/or group will be changed from the creator to the same user or group that is set on the directory it is created in. There are no files on this system with the SUID or SGID bits set, according to the “find” command.

Sticky bit is used on executable and is for forcing commonly used programs between many system users be stored in memory permanently. The SUID and SGID bits would be useful to set on /tmp/ and /var/tmp/ to prevent users from modifying or deleting temporary files created automatically by running applications.

Task 4:

“ps –A” would show everything that is currently running on the machine. "netstat -an | grep LISTEN" shows all the web services that are listening. “nmap localhost” could be used to map out which ports are open from the outside of the machine. “chkconfig serviceName off” can be used to disable services like the ones listed.

Services:

bjc76@kefei1:/home$ ps aux

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND

root 1 0.0 0.0 2536 1512 ? Ss Oct30 0:04 /sbin/init

root 2 0.0 0.0 0 0 ? S< Oct30 0:00 [kthreadd]

root 3 0.0 0.0 0 0 ? S< Oct30 0:00 [migration/0]

root 4 0.0 0.0 0 0 ? S< Oct30 0:00 [ksoftirqd/0]

root 5 0.0 0.0 0 0 ? S< Oct30 0:00 [watchdog/0]

root 6 0.0 0.0 0 0 ? S< Oct30 0:00 [events/0]

root 7 0.0 0.0 0 0 ? S< Oct30 0:00 [cpuset]

root 8 0.0 0.0 0 0 ? S< Oct30 0:00 [khelper]

root 9 0.0 0.0 0 0 ? S< Oct30 0:00 [netns]

root 10 0.0 0.0 0 0 ? S< Oct30 0:00 [async/mgr]

root 11 0.0 0.0 0 0 ? S< Oct30 0:00 [kintegrityd/0]

root 12 0.0 0.0 0 0 ? S< Oct30 0:00 [kblockd/0]

root 13 0.0 0.0 0 0 ? S< Oct30 0:00 [kacpid]

root 14 0.0 0.0 0 0 ? S< Oct30 0:00 [kacpi\_notify]

root 15 0.0 0.0 0 0 ? S< Oct30 0:00 [kacpi\_hotplug]

root 16 0.0 0.0 0 0 ? S< Oct30 0:40 [ata/0]

root 17 0.0 0.0 0 0 ? S< Oct30 0:00 [ata\_aux]

root 18 0.0 0.0 0 0 ? S< Oct30 0:00 [ksuspend\_usbd]

root 19 0.0 0.0 0 0 ? S< Oct30 0:00 [khubd]

root 20 0.0 0.0 0 0 ? S< Oct30 0:00 [kseriod]

root 21 0.0 0.0 0 0 ? S< Oct30 0:00 [kmmcd]

root 22 0.0 0.0 0 0 ? S< Oct30 0:00 [bluetooth]

root 23 0.0 0.0 0 0 ? S Oct30 0:00 [khungtaskd]

root 24 0.0 0.0 0 0 ? S Oct30 0:00 [pdflush]

root 25 0.0 0.0 0 0 ? S Oct30 0:00 [pdflush]

root 26 0.0 0.0 0 0 ? S< Oct30 0:00 [kswapd0]

root 27 0.0 0.0 0 0 ? S< Oct30 0:00 [aio/0]

root 28 0.0 0.0 0 0 ? S< Oct30 0:00 [ecryptfs-kthrea]

root 29 0.0 0.0 0 0 ? S< Oct30 0:00 [crypto/0]

root 33 0.0 0.0 0 0 ? S< Oct30 0:28 [scsi\_eh\_0]

root 34 0.0 0.0 0 0 ? S< Oct30 0:00 [scsi\_eh\_1]

root 36 0.0 0.0 0 0 ? S< Oct30 0:00 [kstriped]

root 37 0.0 0.0 0 0 ? S< Oct30 0:00 [kmpathd/0]

root 38 0.0 0.0 0 0 ? S< Oct30 0:00 [kmpath\_handlerd]

root 39 0.0 0.0 0 0 ? S< Oct30 0:00 [ksnapd]

root 40 0.0 0.0 0 0 ? S< Oct30 0:00 [kondemand/0]

root 41 0.0 0.0 0 0 ? S< Oct30 0:00 [kconservative/0]

root 42 0.0 0.0 0 0 ? S< Oct30 0:00 [krfcommd]

root 230 0.0 0.0 0 0 ? S< Oct30 0:00 [mpt\_poll\_0]

root 231 0.0 0.0 0 0 ? S< Oct30 0:00 [mpt/0]

root 234 0.0 0.0 0 0 ? S< Oct30 0:00 [scsi\_eh\_2]

root 313 0.0 0.0 0 0 ? S< Oct30 0:02 [kjournald]

root 374 0.0 0.0 2156 752 ? S Oct30 0:00 upstart-udev-bridge --daemon

root 376 0.0 0.0 2520 936 ? S<s Oct30 0:00 udevd --daemon

root 449 0.0 0.0 0 0 ? S< Oct30 0:00 [kpsmoused]

root 504 0.0 0.0 2516 880 ? S< Oct30 0:00 udevd --daemon

root 517 0.0 0.0 2516 924 ? S< Oct30 0:00 udevd --daemon

111 623 0.0 0.0 3024 1296 ? Ss Oct30 0:01 dbus-daemon --system --fork

root 625 0.0 0.0 1856 552 ? Ss Oct30 0:00 dd bs=1 if=/proc/kmsg of=/var/run/rsyslog/kmsg

syslog 632 0.0 0.0 33428 1380 ? Sl Oct30 0:12 rsyslogd -c4

114 636 0.0 0.1 6008 2844 ? Ss Oct30 0:01 hald --daemon=yes

avahi 638 0.0 0.0 3104 1780 ? Ss Oct30 0:35 avahi-daemon: registering [kefei1.local]

root 639 0.0 0.1 8972 3732 ? Ss Oct30 0:00 gdm-binary

root 647 0.0 0.2 9212 4300 ? Ss Oct30 0:00 NetworkManager

avahi 650 0.0 0.0 2828 528 ? Ss Oct30 0:00 avahi-daemon: chroot helper

root 657 0.0 0.1 3912 2148 ? S Oct30 0:00 /usr/sbin/modem-manager

root 662 0.0 0.1 19764 3300 ? Ssl Oct30 0:02 /usr/sbin/console-kit-daemon

root 727 0.0 0.0 3348 1200 ? S Oct30 0:00 hald-runner

root 731 0.0 0.0 4788 1660 ? S Oct30 0:00 /sbin/wpa\_supplicant -u -s

root 741 0.0 0.1 8528 3340 ? S Oct30 0:00 /usr/lib/gdm/gdm-simple-slave --display-id /org/gnome/DisplayManager/Display1

root 762 0.0 0.4 15624 9788 tty7 Ss+ Oct30 0:18 /usr/bin/X :0 -br -verbose -auth /var/run/gdm/auth-for-gdm-a047jE/database -nolisten tcp vt7

root 845 0.0 0.0 3424 1132 ? S Oct30 0:03 hald-addon-storage: no polling on /dev/fd0 because it is explicitly disabled

root 848 0.0 0.0 3424 1144 ? S Oct30 0:38 hald-addon-storage: polling /dev/sr0 (every 2 sec)

114 852 0.0 0.0 3268 1136 ? S Oct30 0:00 hald-addon-acpi: listening on acpid socket /var/run/acpid.socket

root 865 0.0 0.0 3424 1144 ? S Oct30 0:00 hald-addon-input: Listening on /dev/input/event2 /dev/input/event0

root 868 0.0 0.0 1708 548 tty4 Ss+ Oct30 0:00 /sbin/getty -8 38400 tty4

root 870 0.0 0.0 1708 548 tty5 Ss+ Oct30 0:00 /sbin/getty -8 38400 tty5

root 875 0.0 0.1 8704 2788 tty9 Ss+ Nov07 0:00 passwd

root 877 0.0 0.0 1708 552 tty2 Ss+ Oct30 0:00 /sbin/getty -8 38400 tty2

root 878 0.0 0.0 1708 544 tty3 Ss+ Oct30 0:00 /sbin/getty -8 38400 tty3

root 881 0.0 0.0 1708 552 tty6 Ss+ Oct30 0:00 /sbin/getty -8 38400 tty6

root 885 0.0 0.0 1980 884 ? Ss Oct30 0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket

daemon 889 0.0 0.0 1964 424 ? Ss Oct30 0:00 atd

root 890 0.0 0.0 2092 888 ? Ss Oct30 0:01 cron

root 1048 0.0 0.0 1756 544 ? S Oct30 0:00 /bin/sh /usr/bin/mysqld\_safe

mysql 1168 0.0 0.8 145300 18064 ? Sl Oct30 3:36 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/my

root 1169 0.0 0.0 1672 588 ? S Oct30 0:00 logger -t mysqld -p daemon.error

root 1192 0.0 0.0 2148 576 ? Ss Oct30 0:00 dhclient3 -e IF\_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp3/dhclient.eth0.l

root 1345 0.0 0.0 5364 1108 ? Ss Oct30 0:17 /usr/sbin/sshd

root 1348 0.0 0.0 8628 1864 ? Ss Oct30 0:44 /usr/sbin/nmbd -D

root 1369 0.0 0.1 15172 3156 ? Ss Oct30 0:01 /usr/sbin/smbd -D

root 1380 0.0 0.0 15172 1344 ? S Oct30 0:00 /usr/sbin/smbd -D

root 1404 0.0 0.0 11644 1972 ? Ss Oct30 0:01 /usr/sbin/winbindd

root 1408 0.0 0.0 11756 1652 ? S Oct30 0:00 /usr/sbin/winbindd

root 1431 0.0 0.0 2428 876 ? Ss Oct30 0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd\_compat -inetd\_ipv6

root 1466 0.0 0.1 6668 2456 ? Ss Oct30 0:00 /usr/sbin/cupsd -C /etc/cups/cupsd.conf

root 1561 0.0 0.3 29896 7516 ? Ss Oct30 0:04 /usr/sbin/apache2 -k start

gdm 1578 0.0 0.0 3388 728 ? S Oct30 0:00 /usr/bin/dbus-launch --exit-with-session

gdm 1580 0.0 0.0 2716 892 ? Ss Oct30 0:00 /bin/dbus-daemon --fork --print-pid 5 --print-address 7 --session

gdm 1581 0.0 0.2 26720 5660 ? Ssl Oct30 0:00 /usr/bin/gnome-session --autostart=/usr/share/gdm/autostart/LoginWindow/

root 1600 0.0 0.1 5128 2444 ? S Oct30 0:00 /usr/lib/devicekit-power/devkit-power-daemon

gdm 1614 0.0 0.2 7592 4532 ? S Oct30 0:05 /usr/lib/libgconf2-4/gconfd-2

gdm 1660 0.0 0.4 37744 9688 ? Ssl Oct30 0:34 /usr/lib/gnome-settings-daemon/gnome-settings-daemon --gconf-prefix=/apps/gdm/simple-greeter

root 1679 0.0 0.0 1708 552 tty1 Ss+ Oct30 0:00 /sbin/getty -8 38400 tty1

gdm 1683 0.0 0.0 5536 1908 ? S Oct30 0:00 /usr/lib/gvfs/gvfsd

gdm 1685 0.0 0.3 19908 7096 ? S Oct30 0:00 /usr/lib/notification-daemon/notification-daemon

gdm 1689 0.0 0.4 25992 9356 ? S Oct30 0:02 metacity

gdm 1690 0.0 0.4 26064 9188 ? S Oct30 0:08 gnome-power-manager

gdm 1691 0.0 0.6 28880 14172 ? S Oct30 1:10 /usr/lib/gdm/gdm-simple-greeter

root 1693 0.0 0.1 7928 2264 ? S Oct30 0:00 /usr/lib/gdm/gdm-session-worker

gdm 1697 0.0 0.1 86584 3116 ? Ssl Oct30 0:00 /usr/bin/pulseaudio --start --log-target=syslog

gdm 1699 0.0 0.1 10640 2868 ? S Oct30 0:00 /usr/lib/pulseaudio/pulse/gconf-helper

root 1822 0.0 0.0 11640 1232 ? S Oct30 0:00 /usr/sbin/winbindd

root 1823 0.0 0.1 11976 2400 ? S Oct30 0:00 /usr/sbin/winbindd

root 6040 0.0 0.2 13004 4400 ? Ss 11:16 0:00 sshd: kw236 [priv]

kw236 6094 0.0 0.0 13004 1976 ? S 11:17 0:00 sshd: kw236@pts/4

kw236 6095 0.0 0.1 6128 3396 pts/4 Ss+ 11:17 0:00 -bash

root 6425 0.0 0.2 13024 4496 ? Ss 12:32 0:00 sshd: root@pts/0

root 6479 0.0 0.0 4380 1900 pts/0 Ss+ 12:32 0:00 -bash

root 6542 0.6 0.1 10516 3140 ? Ss 12:39 0:00 sshd: at89 [priv]

sshd 6543 1.0 0.0 6708 1268 ? S 12:39 0:00 sshd: at89 [net]

bjc76 6544 0.0 0.0 2648 1024 pts/3 R+ 12:40 0:00 ps aux

root 7349 0.0 0.0 1756 492 ? S Nov01 0:00 /bin/sh ./trace\_kw236/apache2

root 7350 0.0 0.0 1756 492 ? S Nov01 0:00 /bin/sh ./trace\_root/apache2

root 7351 0.0 0.0 1756 496 ? S Nov01 0:00 /bin/sh ./trace\_test1/apache2

root 7352 0.0 0.0 2984 700 ? S Nov01 0:03 tail -F /root/.bash\_history

root 7353 0.0 0.0 2984 660 ? S Nov01 0:03 tail -F /jail/home/test1/.bash\_history

root 7354 0.0 0.0 2984 700 ? S Nov01 0:04 tail -F /home/kw236/.bash\_history

www-data 23916 0.0 0.2 30056 4288 ? S Nov07 0:00 /usr/sbin/apache2 -k start

www-data 23917 0.0 0.2 29896 4124 ? S Nov07 0:00 /usr/sbin/apache2 -k start

www-data 23919 0.0 0.2 29896 4252 ? S Nov07 0:00 /usr/sbin/apache2 -k start

www-data 23920 0.0 0.1 29896 3704 ? S Nov07 0:00 /usr/sbin/apache2 -k start

www-data 23921 0.0 0.1 29896 3704 ? S Nov07 0:00 /usr/sbin/apache2 -k start

root 27785 0.0 0.2 12912 4536 ? Ss Nov07 0:00 sshd: bjc76 [priv]

bjc76 27840 0.0 0.1 13044 2236 ? S Nov07 0:01 sshd: bjc76@pts/3

bjc76 27841 0.0 0.1 4840 2116 pts/3 Ss Nov07 0:00 -bash

www-data 32207 0.0 0.1 29896 3704 ? S Nov07 0:00 /usr/sbin/apache2 -k start