Chapter W26 Advanced System Administration

In-Chapter Exercise Solutions

W26.1 Yes

W26.2 **lpadmin [ -E ] [ -U username ] [ -h server[:port] ] -x destination**

In this form of the lpadmin command, -x deletes the printer or class named as the destination argument. Any jobs that are pending for the destination will also be removed, and any job that is currently printed will be aborted.

W26.3 The HP\_Laserjet\_P1006 has been deleted on the Black\_Dragon, the print server.

W26.4 through 13 No answers required.

W26.15 No answer required.

W26.16 No.

W26.17 Default ACLs for non-directories don’t make sense, because no other file system objects can be created “inside” a file that isn’t a directory!

W26.18 The qualifier for Entry types Owner, Owning group, mask, and others. That’s because qualifiers for the user is the Owner, group is the Owning group, the mask applies to no named entity, and other is Others.

W26.19

# file: somefile

# owner: bob ---------→ Owner class rw-

# group: bob

user::rw-

masked----- | user:mansoor:rw-

masked----- | group::r--

mask::rw- ---------→ Group class rw-

other::--- ---------→ Other class ---

W26.20 The original permissions can be restored with **chmod g+w acltest**

W26.21 No answer required.

W26.22 No answer required.

W26.23 No answer required.

W26.24 Because the aclmode setting is “discard” on file objects whose permissions have been modified with the chmod command, and/or because the user has been denied all permissions with the mode bit 7. To determine which case is true, chmod the file test5.dir to give the user access, not dent the user all access.

W26.25 **chmod 744** deletes x permission for group and others.

W26.26 No answer required, but either by executing them directly in a terminal window on the TrueOS system, or via ssh, both methods will yield the same results.

W26.27 Intrusion detection, for example, you can monitor logs in real time (as shown in Section W26.8, and in Chapter W22 covering systemd at the book website, with the **journalctl –f** command) to see what ufw firewall rules are being tested.

W26.28 **sudo ufw insert 2 deny from 192.168.0.31 to any port 22**

W26.29 **sudo ufw delete** [all three rules seen in the last ufw status command output.

W26.30 No answer required.

W26.31 No answer required.

W26.32 No answer required.

W26.33 No answer required.