1. The following was typed at the shell prompt:

```
# mkdir a
# mkdir a/b
# mkdir a/b/c
# cal > today
# date > a/today
# cd a
# ln –s ../today b/c/thelink
# cat b/c/thelink
```

What is “thelink” linked to and explain your answer?

Your answer:
The link file is linked to today which is under /. The current working directory is in a and ../ change the working directory to /. And link the today file.

2. Argue two reasons why a prompt-based interface is better than a GUI interface.

Your answer:
In terms of speed, command line users only need to utilize a keyboard to navigate the interface, often resulting in faster performance.
In terms of resources, a computer that is only using command takes a lot less of the computer’s system resources than a GUI.

3. Write a 1 line statement which shows a long listing of all directories in /home created in Jan, sorted by size. In a long listing you can assume that the size is in column 5 of the output:

Your answer:

```
ls -ld /home | grep Jan | sort -nk5
```

4. The following commands are typed on a Unix computer.

   # ls –l b
   -rwxr-xr-x 1 gordon users 11 Oct 22 12:27 2008

   What is the name of this file, and how big is it in bytes?

   Your answer:
   The name of this file: 2008
   The size in bytes 11 bytes

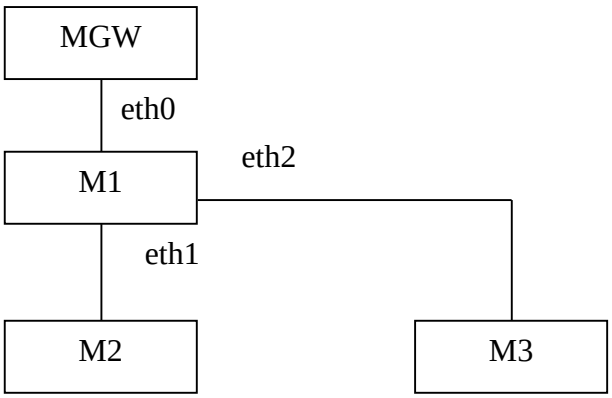
5. You are to set a service httpd running from init.d each time the system reaches runlevel 5 at a startup priority of 30. What would you expect to see in rc5.d? Explain your answer.

   Your answer:
   It means it can kill the process in runlevel 5 (Full multi-user graphical mode) and will start the scripts at the priority 30.

6. User frank is in group smith (gid 40). He has changed jobs and now has to be in group 50. Document the steps to remove him from group 40 and insert him into group 50.

   Your answer:
   # usermod -g 50 frank

7. Consider the following topology:



The ethernet devices shown are from the point of view of M1.
Assume MGW is the gateway machine for this cluster of machines.
All machines (MGW,M1,M2,M3) are Linux machines.

Also from the viewpoint of M1, the following is known:

Eth0 : 10.2.1.20/16
Eth1 : 10.1.25.254/24
Eth2 : 10.3.25.254/24

MGW is 10.2.1.1
M2 is 10.1.25.4
M3 is 10.3.25.10

Supply ifconfig lines for this scenario for use on M3.

Your answer:
ip addr add 10.3.25.10/24 broadcast 10.3.25.255 dev …
ip route append 10.3.25.0/24 dev … table main
ip route append default via 10.3.25.254

8. Continuing from the previous question, supply ip route commands for M2.

Your answer:
ip route append 10.1.25.4/24 dev eth2 table main
ip route append default via 10.3.25.254

9. Show the iptables commands for the OUTPUT table only, which clear out the OUTPUT table, make the policy REJECT, and to only allow access to external telnet servers, for the local system to ping the outside world at rates of less than or equal to 5 per second, and which permits ongoing sessions. Assuming the INPUT table is properly configured.

Your answer:
iptables -F OUTPUT
iptables -P OUTPUT DROP
iptables –A OUTPUT -j REJECT
iptables –A OUTPUT –p tcp --dport telnet –j ACCEPT
iptables –A OUTPUT –p icmp --icmp-type echo-request –m limit --limit 5/second –j ACCEPT
iptables –A OUTPUT –p icmp --icmp-type echo-request -j DROP

10. Consider the following iptables configuration:

    iptables –P INPUT DROP
    iptables –A INPUT –m state --state RELATED,ESTABLISHED –j ACCEPT
    iptables –A INPUT –p tcp --dport httpd –j ACCEPT
    iptables –A INPUT –p icmp --dport ping –j ACCEPT

    Assuming the OUTPUT chain is correctly configured. Your junior administrator produced the above rules but cannot seem to get the rules loaded. Identify and fix all errors.

    Your answer:

    Iptables -A INPUT -m conntrack –ctstate RELATED, ESTABLISHED -j ACCEPT

    Iptables -A INPUT -p tcp –dport http -j ACCEPT
    Iptables -A INPUT -p icmp –icmp-type echo-request -j ACCEPT

11. You have been given the class C network 200.10.40.0/24. Partition this using VLSM to support 3 networks of 40 hosts each, plus 3 /30 networks. Keep the size of each network as small as possible.

    Your answer:

12. Write a virtual host entry to handle www.tester.com, web.tester.com, and tester.com, so that the request is directed to the document root /home/jim, the admin email address is boss@tester.com, and the server name is set to www.tester.com?

Your answer:

```
<VirtualHost *:80>
ServerAdmin  boss@tester.com
DocumentRoot         /home/jim
ServerName   www.tester.com
ServerAlias    web.tester.com tester.com
ErrorLog       logs/sql-error_log
CustomLog    logs/sql-access_log combined
</VirtualHost>
```

13. Supply mod_rewrite instructions for the above virtual host entry such that a request for a host which is not tester.com gets rewritten to tester.com. Do not do the rewrite if the request refers to the URI /~testuser.

Your answer:

```
RewriteEngine on
RewriteCond %{HTTP_HOST} !^tester\.com$
RewriteCond %{REQUEST_URI} !^/~testuser
RewriteRule ^/(.*)$    tester.com$1 [L,R]
```

14. Consider the following DNS zone information.

```
$ORIGIN tester.com.
$TTL    86400
@                   1D IN SOA       ns1 admin.tester.com. (
                        2004101701              ; serial
                        3H                      ; refresh
                        15M                     ; retry
                        1W                      ; expiry
                        1D )                    ; minimum
                    1D IN NS      ns1
                    1D IN A       50.1.1.1
www.                CNAME         tester.com.
ns1                 1D IN A       50.1.1.10
web                 CNAME tester.com
```

Spot 2 errors with this configuration.

Your answer:

www. CNAME tester.com.

Web CNAME ***tester.com.***

15. An apache configuration file currently has no mod_rewrite commands. If the following is added to a virtual host area, what would the result be and why of handling the URL
    http://www.napier.ac.uk/~gordon/hello.html

```
RewriteEngine on
RewriteCond %{HTTP_HOST}    ^www\.napier\.ac\.uk [NC]
RewriteCond %{REQUEST_URI}  !^/~gordon
RewriteRule ^/(.*)          http://www.live.napier.ac.uk/$1 [L,R=permanent]
RewriteRule ^/(.*)          http://www.soc.napier.ac.uk/$1 [L,R=permanent]
```

Your answer:

16. Write a .htaccess file to permit only 146.176.1.5 and 10.0.0.1 from accessing your website.

Your answer:

```
<RequireAny>
        Require     ip      146.176.1.5
        Require     ip      10.0.0.1
</RequireAny>
```

17. Briefly discuss the effectiveness of SPF in fighting spam email.

Your answer:
Setting up an SPF record for your domain can help prevent the emails you send out from being flagged as spam and can reduce attempts by spammers to spoof your domain. SPF is a special type of DNS record that designates the servers and hosts that are authorized to send email from a particular domain. When you implement an SPF record for your domain, spammers are less likely to "spoof" the domain, or use the domain in the FROM address of their spam emails. Since the SPF record identifies only the servers or hosts you use as authorized to send email for your domain, emails sent from a spammer's unauthorized host is far more likely to be captured by spam filters and far less likely to reach their intended audience. This makes your domain less attractive to spammers. As a result, your legitimate email is less likely to be identified as spam and your domain is less likely to be blacklisted by spam filters.

18. Consider the following virtual hosts table entry for sendmail:

gordon jim@internet.com
jim jim@internet.com

Explain what this means.

Your answer:

It does the virtual host mapping for outgoing email. It match the user Gordon with jim@internet.com.

19. Below is a line from a webserver logfile and relates to the virtual host linuxzoo.net:

    70.227.105.100 - - [15/Oct/2008:04:45:29 +0100] "GET /20.20.20.4 HTTP/1.1" 404 4405 "http://25.25.25.5/page2.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

    Explain the meaning of 70.227.105.100, 20.20.20.4, 25.25.25.5, and 4405.

    Your answer:

    70.227.105.100 = IP address (%h)
    20.20.20.4 = resource request
    25.25.25.5 – the site that client reports having been referred from.
    4405 = the size of the object. If "0" for no content, use %b7.

20. Consider the following output from "ifconfig eth0".

```
eth0      Link encap:Ethernet  HWaddr 00:E0:81:26:30:E4
          inet addr:146.176.166.1  Bcast:146.176.166.255  Mask:255.255.255.0
          inet6 addr: fe80::2e0:81ff:fe26:30e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:500  Metric:1
          RX packets:228989464 errors:265780 dropped:0 overruns:0 frame:0
          TX packets:288311148 errors:0 dropped:0 overruns:0 carrier:0
          collisions: 0 txqueuelen:1000
          RX bytes:1548063009 (1476.3 Mb)  TX bytes:1954165244 (1863.6 Mb)
          Base address:0xd800 Memory:fe980000-fe9a0000
```

    Discuss any problems shown in this output of ifconfig.

    Your answer:

    There is CRC error in received packets.

Total Marks [40]

21. After the following command is executed what will be the permissions set on any new file created?

    # umask 226

Your answer:

File => 666-226= 440 (This is asked only.)

Directory => 777-226 = 551

22. In a typical linux filesystem, which two directories are the most likely directories to hold the commands that normal users would commonly execute?

Your answer:
/usr/sbin - Used to store user commands. The directory `/usr/bin/` also stores user commands.
/bin - Location of many system commands, such as `shutdown`. The directory `/usr/sbin/`also contains many system commands.

23. Show the commands you would use to create a file called “file6” which contains a listing of the user’s home directory followed by a listing of the directory /bin.

    Note the list of the user’s home directory should include hidden files but the listing of the /bin directory should not.

Your answer:

 # ls -al /home/ > file6
 # ls -l /bin/ >> file6

24. The following commands are typed on a Unix computer.

    # ls –ld b
    drwxr-xr-x 3 root root 16 Oct 24 13:53 b

    What is the name of this directory, and how many bytes does the directory contain?

    Your answer:

    The directory name : ***b***

    The directory contains ***16 bytes***

25. The following command was typed in:

    # ls -l /etc/rc5.d/*sshd*
    lrwxrwxrwx 1 root root 14 Oct 25 2006 /etc/rc5.d/S55sshd -> ../init.d/sshd

    What does this tell you about sshd? Explain your answer.

    Your answer:

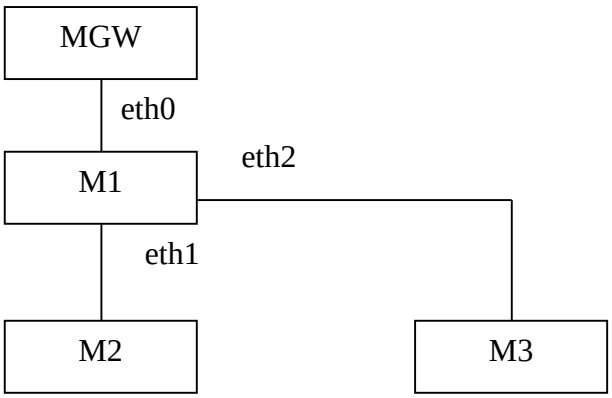
    2006 /etc/rc5.d/S55sshd is the file that has been softlinked.
    ../init.d/sshd is the original file.

26. Your trainee administrator has added the “date” command to all new users login details, so that new users get today’s date printed when they log in. Users created before this change are unaffected. What file did he edit to do this, and how to we get rid of this effect for all users.

Your answer:

/home/user/.bash_profile
.$i

27. Consider the following topology:



The ethernet devices shown are from the point of view of M1.
Assume MGW is the gateway machine for this cluster of machines.
All machines (MGW,M1,M2,M3) are Linux machines.

Also from the viewpoint of M1, the following is known:

Eth0 : 10.2.1.20/24
Eth1 : 10.1.25.254/16
Eth2 : 10.3.25.254/24

MGW is 10.2.1.1
M2 is 10.1.25.4
M3 is 10.3.25.10

Supply ifconfig lines for this scenario for use on M1.

Your answer:

ip addr add 10.2.1.20/24 broadcast 10.2.1.255 dev eth0
ip addr add 10.1.25.254/16 broadcast 10.1.255.255 dev eth1
ip address add 10.3.25.254/24 broadcast 10.3.25.255 dev eth2

ip route append 10.2.1.0/24 dev eth0 table main
ip route append 10.1.0.0/16 dev eth1 table main
ip route append 10.3.25.0/24 dev eth2 table main

ip route append default via 10.2.1.1

28. Continuing from the previous question, supply ip route commands for M2.

Your answer:

ip addr add 10.1.25.4/16 broadcast 10.1.255.255 dev eth1
ip route append 10.1.0.0/16 dev eth1 table main
ip route append default via 10.2.25.254

29. Write iptables commands for the FORWARD chain, clearing the chain, setting the default to DROP, and allowing connections in the established and connected state to work for both eth0->eth1 and eth1->eth0. Permit new http traffic to be forwarded from eth0 to eth1 only if the destination machine is 10.1.2.3.

Your answer:

iptables -F FORWARD
iptables -P FORWARD DROP
iptables –A FORWARD -m conntrack –ctstate RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -m conntrack - - ctstate NEW -p tcp - - dport http -d 10.1.2.3 -j ACCEPT

30. Consider the following iptables configuration:

    iptables –P INPUT DROP
    iptables –A INPUT –m state --state NEW –j ACCEPT
    iptables –A INPUT –o eth0 –p tcp --dport ssh –j ACCEPT

    Assuming the OUTPUT chain is correctly configured. Your junior administrator produced the above rules for a new server which runs an sshd service. The server has only 1 network card. However, packets are not being handled correctly and the ssh server is not processing ssh requests properly. Spot any errors and fix them.

    Your answer:

    -o must be -i

31. In terms of security, explain why it would be very unwise for a system administrator to allow a normal user to run the “tcpdump” command?

    Your answer:

    tcpdump clients can run analysis on the traffic which can be used to get important information of the network

32. Consider the following:

```
<VirtualHost tester.com:800>
        ServerAlias www.tester.com web.tester.com
        ServerAdmin root@tester.com
        DocumentHome /home/here/
        ServerName tester.com
 <VirtualHost>
```

The virtualhost entry shown above is not working. It should support tester.com, www.tester.com, web.tester.com, with a server name of tester.com. Identify 2 faults and fix them.

Your answer:

DocumentRoot and
/VirtualHost

33. Supply mod_rewrite instructions for the above virtual host entry such that a request for web.tester.com or tester.com will be redirected externally and permanently to http://www.tester.com. You may use RewriteCond only once.

Your answer:

RewriteCond %{HTTP_HOST} ^web\.tester\.com$ [OR]
RewriteCond %{HTTP_HOST} ^test\.com$
RewriteRule . http://www.test.com [L,R]*

RewriteCond %{HTTP_HOST} !^www\.test\.com$
RewriteRule ^/(.)$ http://www.test.com$1 [L]*

34. You find the following .forward file:

```
> cat /home/andrew/.forward
\gordon
andrew
```

Explain the .forward file as shown.

Your answer:

Every line in this file is treated as an alias for the user Gordon and Andrew. In this case email for this user would go to both Gordon and Andrew. And thus, the '\' is to prevent from infinite loop for the user Gordon.

This appear to suggest delivery as normal to Andrew, but also a copy of the email to Gordon. However, for each name the whole alias process is redone, so that aliases for andrew will also be processed.

35. An apache configuration file currently has no mod_rewrite commands. If the following is added to a virtual host area, what would the result be and why of handling the URL
http://www.napier.ac.uk/~gordon/hello.html

```
RewriteEngine on
RewriteCond %{HTTP_HOST}    !^www\.napier\.ac\.uk [NC]
RewriteCond %{REQUEST_URI}  ^/~gordon
RewriteRule ^/(.*)          http://www.live.napier.ac.uk/$1 [L,R=permanent]
RewriteRule ^((.*)          http://www.soc.napier.ac.uk/$1 [L,R=permanent]
```

Your answer:

In the first condition that the host that does not start with www and the condition is false and the case is insensitive. And the 2nd condition is correct which the path is correct and that does not need the full path because of the "{REQUEST_URI}". So, the URL will be http://www.live.napier.ac.uk/~gordon/hello.html.

36. The following is an .htaccess file of a fictitious student on a student's web account.

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /home/test/.www-password
Required user any
```

The password file was built using:

```
$ passwd –c /home/test/.www-password user1
$ passwd /home/test/.www-password user2
```

Spot 2 errors with this approach and fix the errors.

Your answer:

Required ---- Require
Any ----- user1 user2

37. Consider the following zone file:

```
$TTL    86400
$ORIGIN tester.com.
@                   1D IN SOA       ns1 me.tester.com. (
                        2004101701              ; serial
                        3H              ; refresh
                        15M             ; retry
                        1W              ; expiry
                        1D )            ; minimum

                    1D IN NS      ns1
                    1D IN A       10.10.10.1
```

Write the remaining part of the zone file so that:

- www.tester.com has an ip of 10.10.10.2
- ns1.tester.com is an alias for tester.com
- web.tester.com is 10.10.10.10 and 10.10.10.11, allocated using a round-robin allocation method.
- mail to www.tester.com is directed to web.tester.com

Your answer:

```
www     IN A        10.10.10.2
        IN MX       10      web.tester.com.
ns1     CNAME       tester.com.
web     IN A        10.10.10.1
        IN A        10.10.10.11
```

38. Detail the effect of the “-m state --state NEW” part of the following firewall rule.

    # /sbin/iptables -A INPUT -m state --state NEW -p tcp --dport http -j ACCEPT

Your answer: The firewall rule is defined in INPUT chain. It will accept the new tcp connections from HTTP.

39. Below is a line from a reverse zone and relates to the IP range 1.1.1.0/24:

    1 PTR grussell.org

    Explain the line shown.

Your answer: The IP address of grussell.org is 1.1.1.1. The IP address indicates to grussell.org

40. Consider the following output from “ifconfig eth0”.

```
eth0      Link encap:Ethernet  HWaddr 00:E0:81:26:30:E4
          inet addr:146.176.166.1  Bcast:255.255.166.1  Mask:255.255.0.0
          inet6 addr: fe80::2e0:81ff:fe26:30e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:228989464 errors:0 dropped:0 overruns:0 frame:0
          TX packets:288311148 errors:0 dropped:23422 overruns:0 carrier:0
          collisions: 2342340 txqueuelen:1000
          RX bytes:1548063009 (1476.3 Mb)  TX bytes:1954165244 (1863.6 Mb)
          Base address:0xd800 Memory:fe980000-fe9a0000
```

Discuss any problems highlighted as a result of this output.

Your answer:

The broadcast address is wrong. The address should be 146.176.255.255. That’s why transmit packet are dropped.

Total Marks [40]

1. $ chmod 547 file1
   $ chmod ou+x file1
   $ chmod g-w file1
   $ chmod u=rw file1
   Show NUMERIC notation

Answer: 647

2. $ ls -l
   -rw-rw-r--. 3 root root 14 Sep 28 15:15 file1
   -rw-rw-r--. 3 root root 14 Sep 28 15:15 file2
   -rw-rw-r--. 3 root root 14 Sep 28 15:15 file3
   $ ln file3 file4
   $ ls -l
   -rw-rw-r--. 3 root root 14 Sep 28 15:15 file1
   -rw-rw-r--. 4 root root 14 Sep 28 15:15 file2
   -rw-rw-r--. 4 root root 14 Sep 28 15:15 file3
   -rw-rw-r--. 4 root root 14 Sep 28 15:15 file4
   What does the link count tell you about the nature of the files in this directory.

Answer: file2 and file3 made hard link file. After that file3 and file4 make hard link from command so the number change from 3 to 4.

3. Consider the following hash information:

```
817ea56a11b3f9b476e0940f353c782a  file1
a456756a11b3f9b476e0940f353c782a  file2
817ea56a11b3f9b476e0940f353c3431  file3
817ea56a11b3f9b476e0940f353c782a  file4
817ea56a11b3f9b476e0940f353c782a  file5
```

   Look at the following file metadata:

```
-rw-rw-r--. 1 gordon staff     689 Dec 15  2015 file1
-rw-rw-r--. 1 gordon gordon    689 Dec 15  2015 file2
-rw-rw-r--. 1 gordon gordon    689 Dec 15  2015 file3
-rw-rw-r-x. 2 tony   gordon    689 Dec 16  2015 file4
-rw-rw-r--. 1 gordon gordon    941 Dec 15  2015 file5
```

   Which files are likely to contain the same data?

Answer: File1 and file4. Used md5 datahash.

4. Search the /home directory and all the subdirectories for a DIRECTORY owned by the user "mtk" and with PERMISSIONS rwx for owner, and rx for group and other. When it finds a match it should do an ls on the directory and display the information about the directory itself (and not the contents of each directory).

Answer: find /home -type d -user mtk -perm 755 -exec ls -d {}\;

5. $ ls -l
   -rw-r---w-. 1 root root 196641 Jan 27 2017 file1
   drwxr-x-w-. 2 root root 6 Jul 27 2004 directory1
   What umask would have been needed to get those permissions on both the file and directory by default?

Answer: umask 025
(if directory has x permission, the file umask must be taken.)

6. Here "file1" contains the height in feet and inches of a number of students. For example, here zawye is described as 5 feet and 9 inches. Give a one line shell command, using pipes as necessary, to display a list of the names of the students in increasing order of height (so shortest student first). Only the names should be displayed.

Answer: sort -k1 -k2 -n file1 | cut -f3 -d" "

7. $umask 472
   $touch file
   $mkdir dir
   Using symbolic notation, what would be resulting permissions be on the file called "file" and directory called "dir"? **Briefly explain your answer**.

Answer: **dir 194**
file 305
The default permission of directory is 777 and the default permission of file is 666. I want to get actual permission. So it needs to reduce from default permission to umask.
`

8. $pwd
   /home/tom/public_html/web
   $ls –l
   lrw-r-r-. 1 tom tom 19 Feb 16 14:30 index.html -> ../../hello.html
   Show the command required to reform this link using an ABSOLUTE pathname instead of the relative one shown.

Answer: ln -s index.html /home/tom/hello.html

9. Write the regular expression to match these words in /usr/dict/words.
   a5ca1aa5c
   abc14azaabc
   aZcMAGICa1aaZc

Answer: grep -E '(a.c).*a.a\1/usr/dict/words

10. You need a regular expression to find all the words in the dictionary /usr/dict/words which start with "a", then some characters later either have any three characters then sometime later have these three characters again once. The "z" must be the last character in the word.

Answer: grep -E '^a.*(...).*\1.*z$' /usr/share/dict/words

11. Write the regular expression to matches all lines that consist of only the letters a,b,c.

Answer: grep -w '^[abc]*$' /usr/share/dict/words

12. Consider the layout you get from an ls -l /home/gordon command:

```
-rwxr-xr-x. 1 gordon gordon  128 Mar 15  2013 index.html
```

With this in mind, and using grep with ls -l and any other commands you think fit, write a one line set of piped commands to find the owner of any files or directories in the current directory which have rwx for user, r-- permissions for other.

Answer: ls -l | grep -E '^.rwx…r--' | cut d" " -f3

13. Find the login shell for "gordon" using grep and cut. Here is a snip from the appropriate file.

```
apache:x:48:48:Apache:/var/www:/sbin/nologin
```

Answer: grep -E '^gordon' /etc/passwd | cut -f7 -d":"

14. Consider the following:

```
$ tail -3 /etc/group
gdm:x:1:
dovecot:x:2:
mysql:x:3:
```

Write the possible command to find user include group name is dovecot.

Answer: grep -E ".*:.*:.*:2:.*" /etc/passwd | cut -d":" -f1

15. Consider the following:

```
$ cat /etc/passwd
root:x:0:1:root:/root:/bin/bash
bin:x:1:2:bin:/bin:/sbin/nologin
daemon:x:2:3:daemon:/sbin:/sbin/nologin
```

Find the group of user daemon using appropriate command.

Answer: get "^.*:.*:3:.*" /etc/group | cut -f1 -d":"

16. Examine some of the lines of the following file, named "demo" in /home/gordon/:

```
gordon,r,200
petra,l,120
gill,j,100
```

This file shows how many miles each member of staff lives from work. Now, write a 1 line linux command using pipes which will show only the mile column, restricted to those staff members with the surname "l". The query should not show any other rows, and only the miles information.

Answer: grep ‘,l,’ /home/gordon/demo | cut -d”,” -f3

17. Run a command which shows which users have the group called “andrew” as secondary groups.

Answer: grep -E ‘^andrew:’ /etc/group | cut -d”:” -f4
(secondary group is at 4th col /etc/group)

18. Consider the following command chain:

```
$ touch file
$ ls -l file
-rw-r--r--. 1 root root 0 Mar 14 16:09 file
$ chown bin.users file
$ chgrp root file
$ ls -l file
```

What is the owner and group of this file after the last command?

19. Consider the following command chain:
$chmod 541 file
$chmod o=rw, gu-x file
What is the symbolic value of the permissions for file?
20. Consider the following commands:
$chmod 644 file
$chmod og-r file
$chmod ug+w, o=w file
What umask would be needed so that the command "touch newfile" or "mkdir dir" would create a file or directory with the same permissions as "file".
21. Consider the following set of commands acting on a file called "new".
$ chmod 746 new
$ chmod ou+x new
$ chmod g-w new
What is the resulting permissions in NUMERIC notation? Show your workings.
22. Consider the following:
$ ip route show table main
default via 10.0.32.22 dev ens3
10.0.32.16/29 dev ens3
10.0.32.0/23 dev ens2
10.0.32.0/24 dev ens1
If you ping each of the following IP numbers, which device in each case do the packets get transmitted on, if any?
(1) 10.0.32.19 – **through ens3 , because the least range /29 will take place to transmit.**
(2) 10.0.128.11 – **ens3 , default route**
(3) 10.0.33.56 – **ens2**
(4) 10.0.32.77 – **ens1**
23. $ ip route show
default via 192.168.0.1 dev ens3
192.168.100.0/24 dev ens1
192.168.0.0/16 dev ens2
192.168.0.0/24 dev ens3

192.168.100.64/22 dev ens4

If you ping each of the following IP numbers, which device in each case do the packets get transmitted on, if any?

(1) 192.168.100.129 – ens1

(2) 192.168.100.1 - ens4

(3) 192.155.100.64 - ens3

(4) 192.168.0.15 – ens2

(5) 192.168.2.64 – ens2

(6) 192.168.101.57 – ens4

24. A linux machine is connected to two networks, and is acting as a router. The internal network is ens1 and the external network is ens2. The ens1 network is IP 172.156.1.1/24, and ens2 is IP 172.156.2.1/24. This Linux machine's gateway is 172.156.2.254. A machine in the internal network, with IP 172.156.1.2, is unable to access machines in the internet, such as IP 172.100.1.50. The following commands were executed and their output collected:

$ip addr show

1: ens1: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000

Link/ether fe:37:da:98:ec:cd brd ff:ff:ff:ff:ff:ff

Inet 172.156.1.1/24 brd 172.156.1.255 scope global ens1

1: ens2: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000

Link/ether ab:cd:ef:34:46:67 brd ff:ff:ff:ff:ff:ff

inet 172.156.2.1/24 brd 172.156.2.255 scope global ens2

$ ip route show

Default via 172.156.1.254 dev ens2

172.156.1.0/24 dev ens1

172.156.2.0/24 dev ens2

$ cat /proc/net/arp

IP address	HW type	Flags	HW address	Mask	Device
172.156.1.2	0x1	0x2	12:00:ab:cd:ef:5f	*	ens1

Pings to 172.100.1.50 fail from 172.156.1.2. What is the error and supply all commands needed to fix the issue?

Answer: ip route append 172.156.2.0/24 dev ens2 table main
ip route append default via 172.156.2.254

25. Consider the following DNS configuration. A server is connected to a network, but has connectivity issues. Things seem fine when talking to the local network, but you cannot make contact with machines beyond this network. The local machine has an IP of 100.101.10.1/24. The gateway router is 100.101.10.254. A machine outside your network has the IP 100.101.11.10, and is confirmed up and able to handle pings.

$ ip addr show

1: em1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000

link/ether d4:ae:52:ad:9d:a4 brd ff:ff:ff:ff:ff:ff

inet 100.101.10.1/24 brd 100.101.10.255 scope global em1

$ ip route show

100.101.10.0/24 dev em1

$ cat /proc/net/arp

IP address	HW type	Flags	HW address	Mask	Device
100.101.10.1	0x1	0x2	00:26:b9:5d:25:5e	*	em1
100.101.10.254	0x1	0x2	00:26:b9:5d:25:5f	*	em1

Pings to 100.101.11.10 fail. 100.101.11.10 never appears in the arp table. Explain the error and supply all commands needed to fix the issue?

Answer: ip addr add 100.101.11.10/24 broadcast 100.101.11.255 dev em0
ip route append default via 100.101.10.254 dev em1

26. $ ip route show
    default via 10.0.0.1 dev em1
    10.0.1.0/24 dev em2
    10.0.0.0/16 dev em1
    10.0.4.0/22 dev em3
    10.1.0.0/24 dev em4
    If you ping the following IP numbers, which device do they get transmitted on, if any?

    (1) 10.1.0.1 – **em4**
    (2) 10.0.5.4 – **em3**
    (3) 10.0.1.254 – **em2**
    (4) 10.1.1.1 – **em1 (default)**

27. Consider the following DNS configuration.

```
$TTL    86400
$ORIGIN imc.com.mm.
@                   1D IN SOA       dns1 www.google.com. (
                                2004101701      ; serial
                                3H              ; refresh
                                15M             ; retry
                                1W              ; expiry
                                1D )            ; minimum
                    1D IN NS    dns1.imc.com.mm.
                    1D IN A     10.2.2.1
www                     A       10.2.2.10
dns1  1D IN A       10.2.2.5
```

    Using the information from this forward zone, identify the origin name of the reverse zone for this example, and show the configuration entries needed in a matching reverse zone file to translate 10.2.2.5 and 10.2.2.1 back to their hostnames.

Answer:

28. Consider the following DNS configuration.

```
$TTL 1D
$ORIGIN advanced.com.
@       IN SOA  @       me.advanced.com. (
```

```
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
@       IN      NS      advanced.com.
        IN      A       172.16.1.1
        IN      MX      10      mail.advanced.com.
        IN      MX      20      mail.offsite.com.
;;Round Robin
www     IN      A       172.16.1.10
www     IN      A       172.16.1.11
www     IN      A       172.16.1.12
```

Your web browser visited www.advanced.com and used the IP 172.16.1.10. It then visited the page 5 minutes later. What IP number would likely be used on that second visit? Use that example to briefly critically discuss the load balancing offered by this configuration.

Answer: On the second visit, 172.16.1.10 will reply until the connection is down or the cache has TTL.

29. Consider the following reverse zone with an origin of 0.0.12.in-addr.arpa.

```
$TTL 86400
@       IN SOA  sillynet.net. admin.sillynet.net. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
        IN      NS      sillynet.net.
20      IN      PTR     sillynet.net.
30      IN      PTR     www.sillynet.net.
```

Using dig -x on 20.0.0.12, the DNS server is returning no information. Diagnose the problem based on the information you can see in the question.

Answer: should be dig -x 12.0.0.20

30. Write mod_rewrite rules for an Apache virtual host called "here.com", which has an alias "mail.here.com". These rules should rewrite "mail.here.com" to "here.com", and should also additionally redirect any request from IP 172.16.10.1 involving any of the virtual hosts to the file "/var/www /html/byebye.html". You can assume the virtualhost definition already exists and is correct. Make sure any regular expressions you use match only the exact conditions listed.

Answer:

```
RewriteEngine On
RewriteCond  %{HTTP_HOST}  ^mail\.here\.com
RewriteRule  ^(.*)$  http://here.com$1
RewriteCond %{REMOTE_ADDR}  ^172\.16\.10\.1
```

RewriteRule ^(.*) /var/www/html/byebye.html [L,R]

31. For an Apache setup, use Require and associated .htaccess commands to allow access from 192.168.10.1 and 192.168.10.2 without any additional authentication, as well as access from 192.168.10.10 if they have already Basic Authenticated themselves as group merit. You can assume all Basic Authentication setup and configuration has already been provided.

Answer:

```
<RequireAny>
        Require ip 192.168.10.1
        Require ip 192.168.10.2
        <RequireAll>
                Require ip 192.168.10.10
                Require group merit
        </RequireAll>
</RequireAny>
```

32. For an Apache setup, use Require and associated .htaccess commands to allow access from 192.168.10.1 for user jim and 192.168.10.2 for user dave without any additional authentication, as well as can't access from 192.168.10.10 if they have already Basic Authenticated themselves as group gordon and can't access form 192.168.10.5 and from 192.168.10.6 . You can assume all Basic Authentication setup and configuration has already been provided.

Answer:

```
<RequireAny>
        <RequireAll>
                Require ip 192.168.10.1
                Require user jim
        </RequireAll>
        <RequireAll>
                Require ip 192.168.10.2
                Require user dave
        </RequireAll>
        <RequireAll>
                Require not ip 192.168.10.10
                Require group gordon
        </RequireAll>
        <RequireNone>
                Require ip 192.168.10.5
                Require ip 192.168.10.6
        </RequireNone>
</RequireAny>
```

33. Write mod_rewrite rules for an Apache virtual host called "there.com", and the path is "/here.dat", then redirect externally to http://fool.org. , and should also additionally redirect any request from IP 172.16.10.1 involving any of the virtual hosts to the file

"/var/www /html/byebye.html". You can assume the virtualhost definition already exists and is correct. Make sure any regular expressions you use match only the exact conditions listed.

Answer:

```
RewriteEngine On
RewriteCond  %{HTTP_HOST}  ^there\.com$
RewriteCond  %{REQUEST_URI}  ^/here\.dat$
RewriteRule  ^(.*)$  http://fool.org  [R]
RewriteCond  %{REMOTE_ADDR}  ^172\.16\.10\.1$
RewriteRule  ^(.*)$  /var/www/html/byebye.html  [L,R]
```

34. Write a virtualhost entry for a virtual host, defining a virtual host called google.com, which has two aliases called www.google.com and srv.google.com. Administrative emails should be delivered to admin@google.com. All the site's webpages are held in a directory called /home/myat/public_html. Access logfiles need to be stored in /var/log/httpd/google.log, while error logs should be in /var/log/httpd/google.error. The access log should be in the default "combined" style.

Answer:

```
<VirtualHost *:80>
        ServerAdmin admin@google.com
        DocumentRoot  /home/myat/public_html
        ServerName  google.com
        ServerAlias  www.google.com srv.google.com
        ErrorLog  /var/log/httpd/google.error
        CustomLog  /var/log/httpd/google.log combined
</VirtualHost>
```

35. All hostnames used in the Apache definition will have these rules applied to them.
    [1] RewriteEngine on
    [2] RewriteCond %{REMOTE_IP} 192.168.1.10
    [3] RewriteCond %{HTTP_HOST} www.last.org
    [4] RewriteRule index.html index.txt
    [5] RewriteRule ^/www/(.*) http://there.com/$1
    What happens if Apache is asked to process the following URLs?
    (1) A request from IP 100.120.111.50 for http://www.last.org/web/index.html
        - As original URL
    (2) A request from IP 192.168.1.10 for http://www.lasttest.com/www/index.dat
        - As rule will be changed as RewriteRule

36. Require rules from a .htaccess file also contains appropriate Basic Authentication configuration to make the rules work.

```
[1] <RequireAny>
[2]   <RequireAll>
[3]     Require IP 15.4.4.1
[4]     Require IP 15.4.4.2
[5]   </RequireAll>
```

[6] <RequireAny>
[7] Require IP 15.4.4.10
[8] Require user jim
[9] </RequireAny>
[10] </RequireAny>
Consider the following cases of attempted access, and state whether access is permitted or not. Include an explanation of your reasoning.
1) Access from IP 15.4.4.10 by user tom - **permitted**
2) Access from 15.4.4.2 **- permit**

37. Apache access log extract related to the virtualhost test.com:
192.132.10.10 - example [10/Sep/2012:03:46:14 +0100] "GET /here1.html HTTP/1.1" 405 194 "http://test.net/here2.html" "Mozilla/5.0
(compatible; spider/2.0; +http://www.test.org/here3.html)"
What is the full URL of the page being requested? Was the request successful? If not, also state the response code.

Answer: http://www.test.org/here1.html
4 means error by client (unsuccessful)

38. A server called imc.com, with aliases web.imc.com, www.imc.com, and test.imc.com.

[1] <VirtualHostname *:80>
[2] ServerAdmin me@imc.com
[3] DocumentRoot /home/me/public_html
[4] ServerName imc.com
[5] ServerNames www.imc.com,test.imc.com,web.imc.com
[6] ErrorLog imc.error
[7] AccessLog imc.log combined
[8] <\VirtualHostname>
Spot 4 lines with errors and for those lines with the errors write the correct information.

Ans: <VirtualHost>
ServerAliases
CustomLog (not access log)
</VirtualHost>

39. $ cd /home/tom/public_html
$ cat .htaccess
AuthType Basic
AuthName "By Invitation Only"
AuthUserFile /home/tom/password
Require user jerry
$ htpasswd -c /home/tom/password jerry
New Password: jerry
Retype New Password: jerry
Adding password for user jerry

After configured, the system doesn't work. The error log from Apache suggests that the .htaccess file cannot be accessed. Suggest 4 commands which might fix this issue.

Ans: #chmod 701 /home/tom
 # chmod 751 /home/tom/public_html
 # chown -R tom.tom /home/tom
 # systemctl restart httpd.service

40. A user "dave" wants to arrange for their email to be delivered so that "dave" receives her email normally, but also so that user "demo" receives a copy of her emails automatically. How could this be achieved using a .forward? Include the full .forward pathname as well as the contents of the file in your answer.

Ans: # vi /home/dave/.forward
\dave
demo

Firewall Sir Kaung

Q1: Using Stateful firewall rules, configure a firewall for a linux box acting as a gateway router. This box has two network connections em1 (to the internet) and em2 (to the intranet). Configure only the FORWARD table and then make the default policy DROP. The gateway should allow traffic from the internet to connect to an HTTP server at 25.4.4.10 and allow an SSH server in the intranet at 25.4.5.1 to connect to any machine in the internet.

Ans:

iptables -A FORWARD -j REJECT (if the question asks for drop)

iptables -F INPUT

iptables -F OUTPUT

iptables -F FORWARD

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -A FORWARD -i em1 -m conntrack –ctstate NEW -p tcp –dport 80 -j ACCEPT

iptables -A FORWARD -o em1 -m conntrack –ctstate NEW -p tcp -s 25.4.5.1 -j ACCEPT

Q2: Using stateful iptables firewall rules, configure a firewall for a server which has only one network interface. This server should allow external users to access a local service running on port 53 on tcp and allow local users to access ssh on an external machine with an IP of 10.0.0.1. Configure both ingress and egress rules. Set all default policies to DROP.

Ans:

iptables -F INPUT

iptables -F OUTPUT

iptables -F FORWARD

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -A INPUT -m conntrack –ctstate RELATED, ESTABLISHED -j ACCEPT

iptables -A INPUT -m conntrack --ctstate NEW -p tcp --dport 53 -j ACCEPT

iptables -A OUTPUT -m conntrack –ctstate NEW -p tcp –sport ssh -d 10.0.0.1 -j ACCEPT

Q3: One of your SSH server machines is being attacked from a site with the IP 10.0.0.1. The attack takes the form of hundreds of login attempts per second, lasting minutes at a time. Unfortunately, this site also has legitimate need to access your SSH traffic. Your junior system administrator has written the following firewall:

```
iptables -F INPUT
iptables -P INPUT DROP
iptables -A INPUT -m conntrack –ctstate RELATED, ESTABLISHED -j
ACCEPT
iptables -A INPUT -p tcp –dport ssh -m limit –limit 1/second -j
ACCEPT
```

This has limited new connections to 1 per second for everyone. Propose a better solution so that only SSH connections from 10.0.0.1 is rate limited, and all other machines can connect without limits.

ANS:

iptables -A INPUT -p tcp --dport ssh -s 10.0.0.1 -m limit –limit 1/second -j ACCEPT

iptables -A INPUT -p tcp –dport ssh ! -s 10.0.0.1 -j ACCEPT

Q4: Consider the following information:

```
$ sesearch -T -s label1_t
type_transition label1_t label3_t: process label4_t;
type_transition label1_t executable1 : process label3_t;
$ ls -Z executable1
-rwxr-x---. system_u:object_r:label3_t:s0 executable1
```

Discuss what happens if a process of label1_t executes the executable called executable1?

ANS:

Happens Process type label4 transition (or) the process will become type label4_t.

Q5: `$ps -xZ | grep httpd`

```
       System_u:system_r:httpd_t:s0  32722 ?     Sl 0:22
/usr/sbin/httpd
   $ ls -Z exec.exe
        -rwxr-x---. System_u:object_r:httpd_user_script_exec_t:s0
      exec.exe
```

How could you discover which process type httpd_t would transition to if it executed exec.exe?

ANS:

initrc_t will work out first.

Q6: When running under SELinux, an error was flagged up. After checking the error log, it seems that process p1_t was trying to access f1_t, and this is denied.

On running audit2allow, the systems suggests

Allow p1_t f1_t: file read;

Discuss whether adding this rule to the SELinux database would be the best approach, and if not then what should be the next step?

ANS:

- The error message will be sent back with this, **Allow p1_t f1_t: file read;**

Q7: In terms of a network-based application, such as SSH, explain how SElinux supports the idea that applications can be restricted to just certain ports.

ANS:

semanage port -l

Every process has been assigned with a certain port on SELinux label. Only process types which relate to the port types which define the port numbers requested would be permitted to actually open those ports. Rules in SELinux define which process types relate to which port types, and thus process types which are not linked to particular requested port numbers would be stopped.

Q8: How selinux increases the security of a server in comparison to the standard user/group/other file and directory permissions model.

ANS:

Uses MAC security

- More sensitive
- More detailed
- Flexible