Networked Services - End of week quizzes

> 18/12/2019

Contents

EOWQ 1

Question 1 - File Permissions

Given the following:

$ chmod 345 test $ chmod og-w,u=rx test What are the resulting permissions? Show the answer in numeric notation.

```
345 to start
og-w tries to take away 2 (010) from 4 (100) for group and from 5 (101) for
other. But the middle bit is not set anyway so this makes no change.
Remains 345.
u=rx sets the user permission to 5 (101) regardless of what it was
previously.

Answer is 545
```

Question 2 - LVM

Logical Volume management, LVM, offers additional features in comparison to fixed partitioning strategies. Reflect on the challenges of dynamic partitioning strategies when compared to traditional partitions.

> Dynamic partitioning allows partitions and disks to be added to existing partitions at runtime, allowing filesystems to be grown or shrunk. But this is complex and error-prone, and careful partitioning at the start is probably safer and more effective.

Question 3 - System Updates

Keeping systems patched and up to date is good practice, but fraught with difficulties. When maintaining a critical server, discuss how such a system can be kept up to date safely.

> Rebooting machine which have been running a while may result in electrical failures. New updates may render currently functioning systems unusable, introduce incompatibilities, or change current behaviours. Keeping backups is valuable, but testing changes on a mirror may be helpful.

Question 4 - XINETD

XINETD follows a different philosophy in comparison to traditional schemes like init.d in the way they handle service daemons. Discuss any negative issues about the approach used by XINETD, i.e. reasons for not wanting to use this approach.

> XINETD may be slower, and more complex, and harder to debug, and has a harder to predict effect on system resources.

Question 5 - find

Write a 1 line statement, using a pipe, which reports how many directories in /home have a group ownership of “people”. Make sure it checks subdirectories too.

> find /home –group people –type d | wc -l

Question 6 - `/etc/passwd`

Given that all the passwords in Linux are hashed, speculate on why it was felt important to move the hashed passwords from /etc/passwd into /etc/shadow. As part of your answer, comment on the need to regularly change the hashing algorithm used in password hashing.

> /etc/passwd is readable by everyone, so that UID and GID can be translated into names, and so everyone has access to hashed passwords. This was considered dangerous, and hashes were moved to shadow. Through hacking techniques it may still be possible to get the hashes, so making hashes difficult to break is important. Thus the reason for updating the hashing technique with changes to current security thinking.

EOWQ 2

Question 1 - IPtables

You are given the following iptables rules:

```
iptables –A INPUT –s 10.3.4.0/24 –j DROP
iptables –A INPUT –s 10.3.5.0/24 –j DROP
iptables –A INPUT –s 10.3.6.0/24 –j ACCEPT
iptables –A INPUT –s 10.3.7.0/24 –j DROP
```

Optimise these four rules into just 2 rules which achieve the same results using VLSM to help.

> iptables –A INPUT –s 10.3.6.0/24 –j ACCEPT iptables –A INPUT –s 10.3.4.0/22 –j DROP

Question 2 - IP route add

Consider a scenario with one machine acting as a router. This machine has 2 interfaces, eth0 and eth1, where eth0 (10.0.0.1/24) is to the intranet and eth1 (10.0.1.1/24) to the internet.

Only one other machine (10.0.0.2/24) is connected to eth0, and only one other machine (10.0.1.2/24) is connected to eth1.

Provide the appropriate ip route commands to get this router operational.

> ip route add 10.0.0.0/24 dev eth0 ip route add 10.0.1.0/24 dev eth1 ip route add default via 10.0.1.2

Question 3 - TIME_WAIT

Consider this entry in the /proc/net/nf_conntrack

```
ipv4     2 tcp      6 52 TIME_WAIT src=146.176.166.1 dst=146.176.166.9
sport=43755 dport=80 src=146.176.166.9 dst=146.176.166.1 sport=80
dport=43755 [ASSURED] mark=0 secctx=system_u:object_r:unlabeled_t:s0 zone=0
use=2
```

Explain what the state of the connection shown here means in terms of what has happened to this TCP stream.

> TIME_WAIT means the stream has closed and exchanged FIN packets.

Question 4 - IPtables

Consider the following firewall rules:

```
$ iptables –A INPUT –s 5.0.0.4 –j ACCEPT
$ iptables –A INPUT –s 5.0.0.5 –j ACCEPT
$ iptables –A INPUT –s 5.0.0.6 –j ACCEPT
$ iptables –A INPUT –s 5.0.0.7 –j DROP
```

A colleague has converted this into the following rules:

```
$ iptables –A INPUT –s 5.0.0.4/30 –j ACCEPT
$ iptables –A INPUT –s 5.0.0.7    –j DROP
```

This new firewall is not functioning in the same way as the previous firewall rules. Fix this new firewall in the simplest way possible so that it is functionally equivalent to the previous firewall rules. The answer should still have only 2 rules.

> Move line 2 and put it into line 1

Question 5 - IProute and ping

Consider the following configuration:

```
ip route add 20.0.0.0/24 dev eth1
ip route add 20.1.6.0/24 dev eth0
ip route add 20.1.0.0/16 dev eth2
ip route add default via 20.0.0.254
```

If a user on this machine typed:

```
$ ping 20.0.1.5
```

which interface would the ping packet leave on? Explain your answer.

> It would leave on eth1, as no local Ethernet route matches and thus it would be delivered via the gateway 20.0.0.254.

Question 6 - `ip addr`

Write the “ip address” line needed to define 53.17.5.1/25 for use with device eth0, including the broadcast configuration.

> ip addr add 53.17.5.1/25 broadcast 53.17.5.127 dev eth0

Question 7 - IPtables

Consider the following iptables configuration:

```
iptables –P INPUT DROP
iptables –A INPUT –m conntrack --ctstate RELATED,ESTABLISHED –j ACCEPT
iptables –A INPUT –p udp --dport 80   –s 9.2.0.0/24 –j DROP
iptables –A INPUT –p tcp --dport http –s 9.2.0.0/16 –j ACCEPT
iptables –A INPUT –p tcp --dport 80   –s 9.2.4.0/24 –j DROP
iptables –A INPUT –p tcp --dport 80   –s 9.2.4.0/8  –j DROP
iptables –A INPUT –j REJECT
```

Which of ACCEPT, REJECT, or DROP would be applied to each of the following new packets:

a) incoming tcp packet, ip 9.2.3.51, heading to port 80. b) incoming tcp packet, ip 9.2.4.52, heading to port 80. c) incoming tcp packet, ip 9.2.0.53, heading to port 80. d) incoming tcp packet, ip 9.0.3.54, heading to port 80.

> a) ACCEPT, b) ACCEPT, c) ACCEPT, d) DROP

EOWQ 3

Question 1 - Apache lightweight process model

The Apache web server uses by default a heavyweight forking process model. Other process models also exist. Reflect on the implications of switching to a process model which uses a lightweight threaded model in a single heavyweight process for Apache.

> Lightweight process models do not offer inter-thread memory protection, or other security measures which protect processes from each other. Thus errors or hacking from one thread could affect another. It does however offer the possibility of higher performance.

Question 2 - Apache ReWrite rules

An apache configuration file currently has no mod_rewrite commands. The following is added to the correct virtual host area

RewriteEngine on RewriteCond %{HTTP_HOST} magic.org$ [NC] RewriteRule .* http://magic.uk/ [L,R=permanent] What would the results be of handling the following URLs? Briefly explain your answers. You will score 0 if you do not include an explanation.

a) http://magic.org.uk/test1.html b) http://webmagic.ORG/test2.html

> A) HOST does not match so no rewrite, B) everything matches due to NC.

Question 3 - `.htaccess` file

Write a .htaccess file to stop 146.176.10.10 and any IPs in the range 10.0.1.0 to 10.0.1.255 from accessing your website.

```
<RequireAll>
    require not ip 146.176.10.10
    require not ip 10.0.1.0/24
</RequireAll>
```

Question 4 - webserver logfile

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 /here.html HTTP/1.1" 404 200 "http://linuxzoo.net/index.html" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

What is (a) the error code, (b) the address of the client machine making the request, (c) the transfer size, and (d) the page requested.

> (a) 404 (b) 70.227.105.100 (c) 200 (d) /here.html

Question 5 - ReWrite rules

Consider the following mod_rewrite rules:

```
RewriteEngine On
RewriteCond ${HTTP_HOST} linuxzoo.net
RewriteCond ${REQUEST_URI} test
RewriteRule (.*) http://host1.com/$1
RewriteRule /mine/(.*) http://host2.com/$1
```

What would happen if a browser request was processed by these rules, given the urls:

(a) http://www.linuxzoo.net/retest.html (b) http://www.napier.ac.uk/test.html

Explain your answer or you will score 0.

> (a) Matches the first rewritecond, as there are no anchors. Similarly for condition 2. As both match the first rewriterule is done, redirecting the request to http://host1.com/retest.html (b) No match to first cond, but does match second cond. However, both conditions are ANDed together, so first rewriterule is passed over. Second rule does not match, so the original URL is left unchanged.

Question 6 - `Options -Indexes` (Apache webserver config)

Discuss why:

`Options -Indexes`

may provide an element of security in an Apache webserver configuration.

> This option stops the web browsers being able to see a directory listing if the browser provides a URL which is a directory in the document root. By blocking this, users will not be able to see the names of files and directories in the document root, and thus entries they should not be able to know about will not be easily identified. Instead, the user would have to use guesswork to find files which were not part of the navigation tree of the site. Such files may include password information, development code, logs, etc, and so hiding them has some benefit.

Question 7 - Apache weblog referer field and marketing

In an Apache weblog, discuss what sort of benefit can be obtained in terms of marketing from the referrer field?

> The referrer field indicates the webpage on which a browser user was on when they clicked a link which took them to the site related to this weblog. This effectively indicates how the user came to this site. Seeding links to the site across other webpages is common when trying to improve the popularity of a site, and may be done as part of search engine optimisation (SEO). Knowing which locations are effective and which are poor sources of users helps to guide where best to advertise links, and to better understand client demographics.

EOWQ 4

Question 1 - Email header validity

Consider the following email and its associated headers.

```
From user@gmail.com Sun Nov 15 11:12:30 2018
Received: from freemail.ru [160.150.1.4]
   by gmail.com (8.22.15) id PDQ666
   Sun Nov 15 11:12:21 2018 -0000
Received: (payments@hmrc.gov.uk)
   by host4454.hmrc.gov.uk (8.22.11) id LXY123
   Sun Nov 15 21:12:00 2018 +1000
Date: Sun Nov 15 11:12:21 2018
From: payments@hmrc.gov.uk
To: user@gmail.com
Message-Id: <20181115111215.LXY123@hmrc345677111>
Subject: You are overdue for your tax
You have been detected buying ripple currency, making a
profit, and not declaring this as income. Please click the
link below and supply a credit card to make the payment
immediately
http://hmrc.gov.uk@thegardenshop.co.uk/finaldemand.html
```

Discuss the validity of this email in terms of the its headers.

> There is a mismatch between hop 1 and hop2. Hop1 could be plausible for HMRC, but the email actually appears to originate from a free email server in russia, and suggests the first hop might have been inserted by the original sender. It is also unclear why HMRC emails might need to traverse such a far away timezone.

Question 2 - MTA node

In terms of email delivery, how does an MTA node know where to send an email? In your explanation, you should use the following example:

Email envelope:

helo host1.com mail from: me@host2.com rcpt to: me@host3.com

> As the rept to is host3.com, the MTA would look up the MX record of host3.com, and try the entries from lowest priority to highest. For each entry, the hostname could be translated from the MX record into an A record, and then the email would be sent there. If there were no MX records, then the A record of host3.com would be used instead.

Question 3 - `newaliases`

Your /etc/aliases file has been updated by your junior aministrator, but it does not seem to be working correctly. When an email is sent to "group", the email is rejected with an error.

```
test: gordon,andrew@gmail.com
group: test,brian
group2: /dev/null
```

Discuss the most likely reason why the error may be occurring.

> Maybe the junior has not yet rebuild the aliases.db file by running newaliases?

Question 4 - `.forward`

Consider the following scenario

```
$ cat /etc/aliases
email1: jim,john
brian: peter,email1
$ cat /home/jim/.forward
\brian
```

There is no .forward defined for either john or peter.

> Email to email1 would go to both jim and john, but jim has a .forward for brian. As brian is escaped as \brian, no alias lookup will take place and instead email will be delivered as if brian is a local user. In short, the email will go to john and brian.

Question 5 - `genericstable` config

In a sendmail configuration for mysite.net, you are aware of the following genericstable information

```
bill    bill@asecuritysite.com
brain brian@napier.ac.uk
```

Then bill sends email out via this server, what happens?

> As the email leaves the server, the from address is rewritten from bill@mysite.net to bill@asecuritysite.com

Question 6 - Faking hostnames

For fighting email spam, a company as set up a database of the domain names associated with emails containing fake news articles. The intention is that domains on the list should be blocked from sending emails. Discuss the effectiveness of this idea.

> As domain and hostnames can be easily faked, this would only be useful if the IP number of the sender also matched the A record of that domain's email server, or is somehow validated in some other way such as SPF. Otherwise the spammers would just randomly choose domain names, and innocent domain owners could be blocked.

Question 7 - Social Engineering

A company is concerned that social engineering might be employed to obtain passwords from employees. Briefly discuss 2 possible options in tackling or mitigating this issue.

1. Training for users
2. Passwords based on biometrics
3. logins based on something other than passwords
4. two factor logins
5. login anomaly detection, e.g. spotting logins from new locations.
6. Social engineering monitoring to detect when staff discuss things which may result in them being targeted for attacks.

Question 8 - DOS and the attack multiplier

In a Denial of Service attack, discuss how an attack multiplier works and why it is important to perform an effective attack.

> An attack multiplier increases the traffic size in comparison to the original attack traffic. So, if an attacker sends a 10 byte message, the multiplier would be 100 if the attack becomes an 1000 byte message by the time it arrives at the target. Multipliers allow sources with bandwidth much lower than the target to perform an effective attack.

Question 9 - Server update issues

Discuss the risks involved in keeping a production server up to date with the latest patches?

> It is possible that patches will stop the server working properly, leading to server down time. It is also possible that the servers need to be rebooted for the patches to take effect, which again can lead to downtime due to patching issues, as well as machines which may have problems which only come to light when their power is cycled (such as hardware faults or a reliance on non-persistent data).