Networked Services - Week two quiz

> 05/12/2019

- Networked Services - Week two quiz
  - Question 1
    - Answer 1
    - Revision 1
      - VLSM table
  - Question 2
    - Answer 2
    - Revision 2
      - IP command cheat sheet
        - addr
        - link
        - route
  - Question 3
    - Answer 3
    - Revision 3
  - Question 4
    - Answer 4
    - Revision 4
  - Question 5
    - Answer 5
    - Revision 5
  - Question 6
    - Answer 6
    - Revision 6
  - Question 7
    - Answer 7
    - Revision 7

Question 1

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.

Answer 1

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

Revision 1

VLSM table

Slash Notation	Subnet Mask	Hosts
.../16	255.255.0.0	65534
.../17	255.255.128.0	32766
.../18	255.255.192.0	16382
.../19	255.255.224.0	8190
.../20	255.255.240.0	4094
.../21	255.255.248.0	2046
.../22	255.255.252.0	1022
.../23	255.255.254.0	510
.../24	255.255.255.0	254
.../25	255.255.255.128	126
.../26	255.255.255.192	62
.../27	255.255.255.224	30
.../28	255.255.255.240	14
.../29	255.255.255.248	6
.../30	255.255.255.252	2

There are four IP ranges that need to be dropped apart from one that will need to be accepted. Therefore we accept this range first and drop the rest. The IP ranges can be concatinated into one subnet `10.3.4.0/22` as this allows for four usable /24 address spaces.

Question 2

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.

Answer 2

```
$ 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
```

Revision 2

IP command cheat sheet

addr

Display IP Addresses and property information.

```
$ ip addr # Show information for all addresses.
$ ip addr show dev eth1 # Display information only for device eth1.
$ ip addr add # Add an address.
$ ip addr add 192.168.1.1/24 dev em1 # Add address 192.168.1.1 with netmask
24 to device em1.
$ ip addr del # Delete an address.
$ ip addr del 192.168.1.1/24 dev em1 # Remove address 192.168.1.1/24 from
device em1.
```

link

Manage and display the state of all network interfaces.

```
$ ip link # Show information for all interfaces.
$ ip link show dev eth1 # Display information only for device eth1.
$ ip -s link # Display interface statistics.
```

route

Display and alter the routing table.

```
$ ip route # List all of the route entries in the kernel.
$ ip route add # Add an entry to the routing table.
$ ip route add default via 192.168.1.1 dev em1 #Add a default route (for
all addresses) via the local gateway 192.168.1.1 that can be reached on
device em1.
$ ip route add 192.168.1.0/24 via 192.168.1.1 # Add a route to
192.168.1.0/24 via the gateway at 192.168.1.1.
$ ip route add 192.168.1.0/24 dev em1 # Add a route to 192.168.1.0/24 that
can be reached on device em1.
$ ip route delete 192.168.1.0/24 via 192.168.1.1 # Delete the route for
192.168.1.0/24 via the gateway at 192.168.1.1.
```

Question 3

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.

Answer 3

TIME_WAIT means the stream has closed and exchanged FIN packets.

Revision 3

Question 4

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.

Answer 4

Revision 4

Question 5

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.

Answer 5

Revision 5

Question 6

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

Answer 6

Revision 6

Question 7

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:

1. incoming tcp packet, ip 9.2.3.51, heading to port 80.
2. incoming tcp packet, ip 9.2.4.52, heading to port 80.
3. incoming tcp packet, ip 9.2.0.53, heading to port 80.
4. incoming tcp packet, ip 9.0.3.54, heading to port 80.

Answer 7

Revision 7
