COMP3052 Computer Security

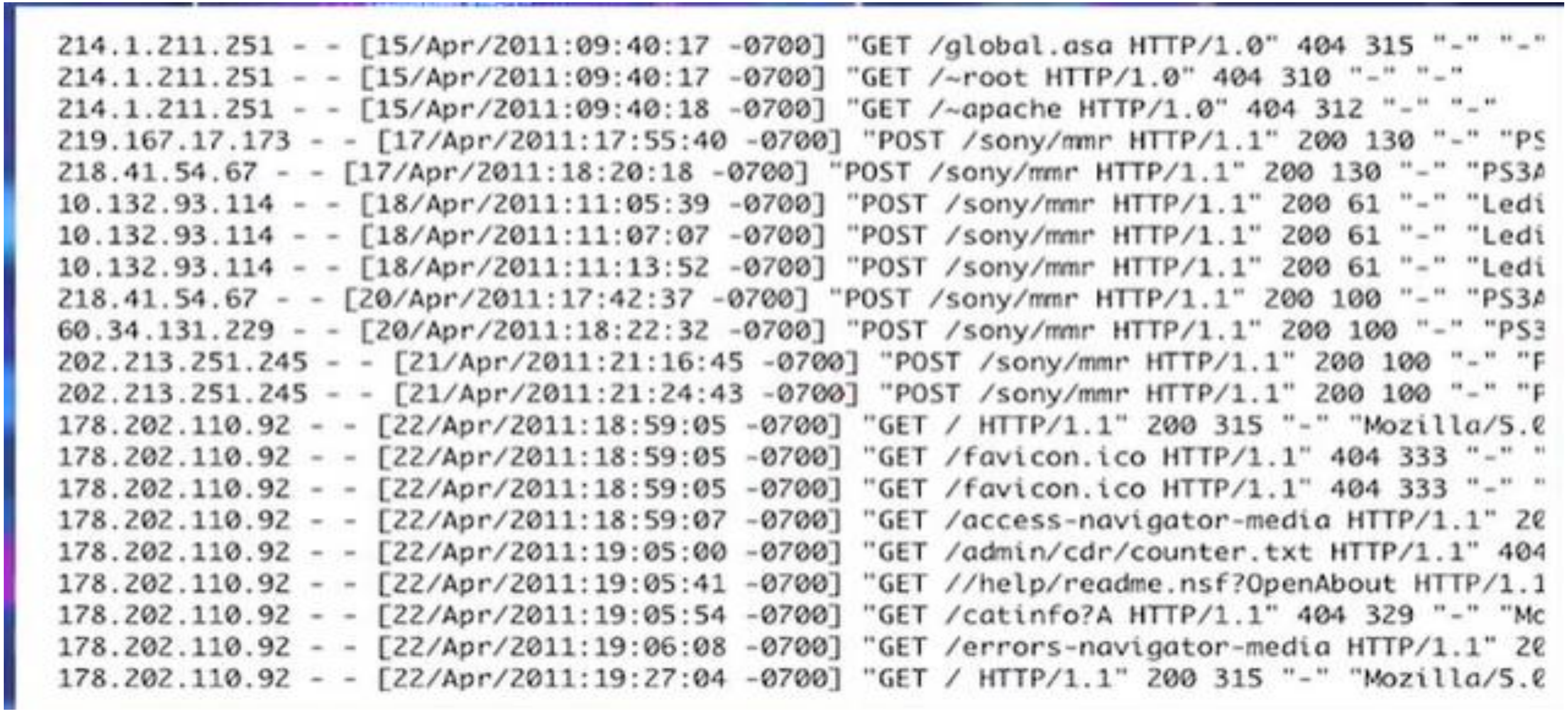
Session 06: Firewalls

Videoclip: What is Firewall? Simplilearn

https://www.youtube.com/watch?v=9GZlVOafYTg

Videoclip: What is a Firewall? PowerCert Animated Videos

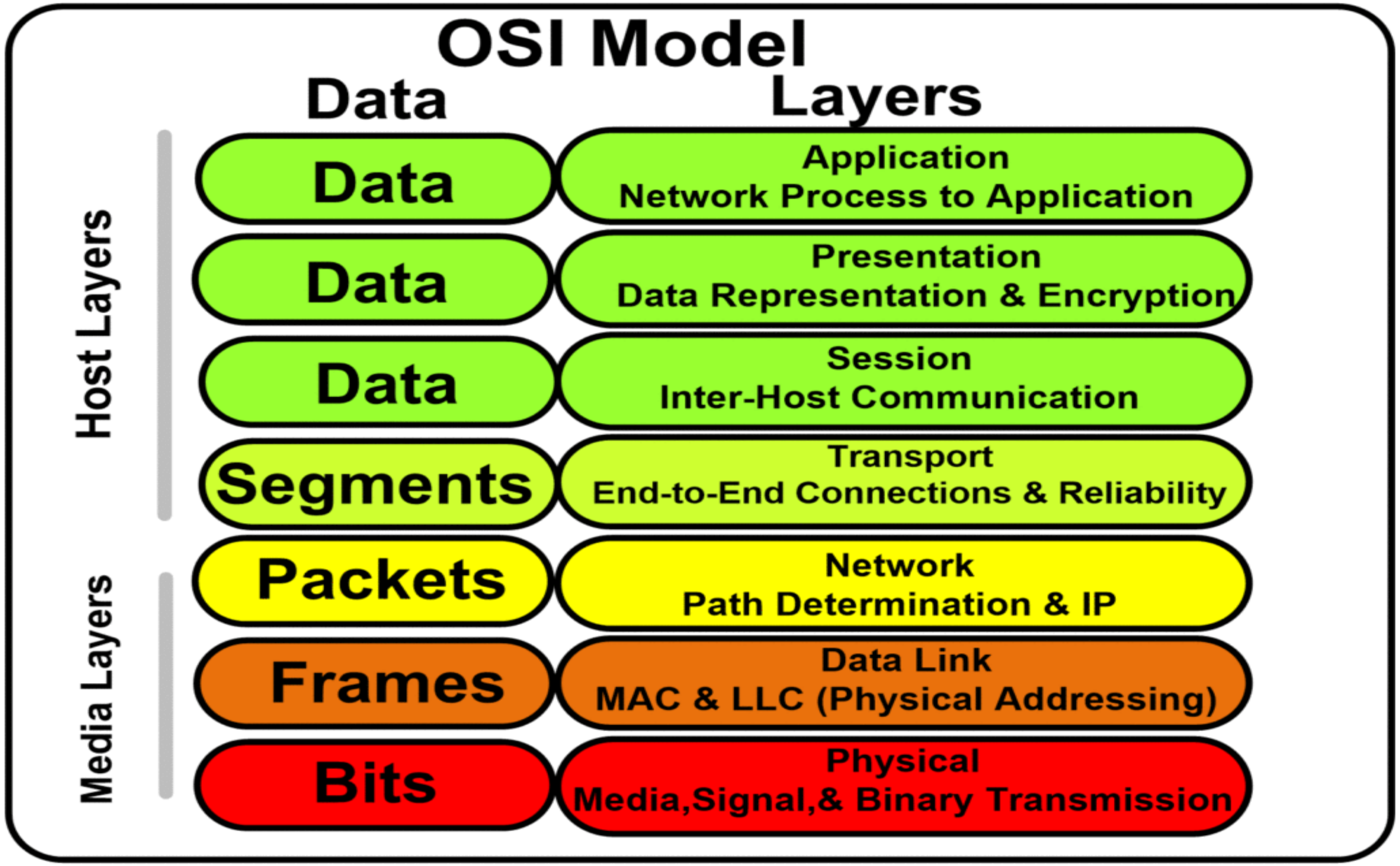
https://www.youtube.com/watch?v=kDEX1HXybrU



```
214.1.211.251 - - [15/Apr/2011:09:40:17 -0700] "GET /global.asa HTTP/1.0" 404 315 "-" "-"
214.1.211.251 - - [15/Apr/2011:09:40:17 -0700] "GET /~root HTTP/1.0" 404 310 "-" "-"
214.1.211.251 - - [15/Apr/2011:09:40:18 -0700] "GET /~apache HTTP/1.0" 404 312 "-" "-"
219.167.17.173 - - [17/Apr/2011:17:55:40 -0700] "POST /sony/mmr HTTP/1.1" 200 130 "-" "PS
218.41.54.67 - - [17/Apr/2011:18:20:18 -0700] "POST /sony/mmr HTTP/1.1" 200 130 "-" "PS3A
10.132.93.114 - - [18/Apr/2011:11:05:39 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
10.132.93.114 - - [18/Apr/2011:11:07:07 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
10.132.93.114 - - [18/Apr/2011:11:13:52 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
218.41.54.67 - - [20/Apr/2011:17:42:37 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "PS3A
60.34.131.229 - - [20/Apr/2011:18:22:32 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "PS3
202.213.251.245 - - [21/Apr/2011:21:16:45 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "P
202.213.251.245 - - [21/Apr/2011:21:24:43 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "P
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET / HTTP/1.1" 200 315 "-" "Mozilla/5.0
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET /favicon.ico HTTP/1.1" 404 333 "-" "
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET /favicon.ico HTTP/1.1" 404 333 "-" "
178.202.110.92 - - [22/Apr/2011:18:59:07 -0700] "GET /access-navigator-media HTTP/1.1" 20
178.202.110.92 - - [22/Apr/2011:19:05:00 -0700] "GET /admin/cdr/counter.txt HTTP/1.1" 404
178.202.110.92 - - [22/Apr/2011:19:05:41 -0700] "GET //help/readme.nsf?OpenAbout HTTP/1.1
178.202.110.92 - - [22/Apr/2011:19:05:54 -0700] "GET /catinfo?A HTTP/1.1" 404 329 "-" "Mo
178.202.110.92 - - [22/Apr/2011:19:06:08 -0700] "GET /errors-navigator-media HTTP/1.1" 20
178.202.110.92 - - [22/Apr/2011:19:27:04 -0700] "GET / HTTP/1.1" 200 315 "-" "Mozilla/5.0
```

Reference: Network Logging: Definition & Tools

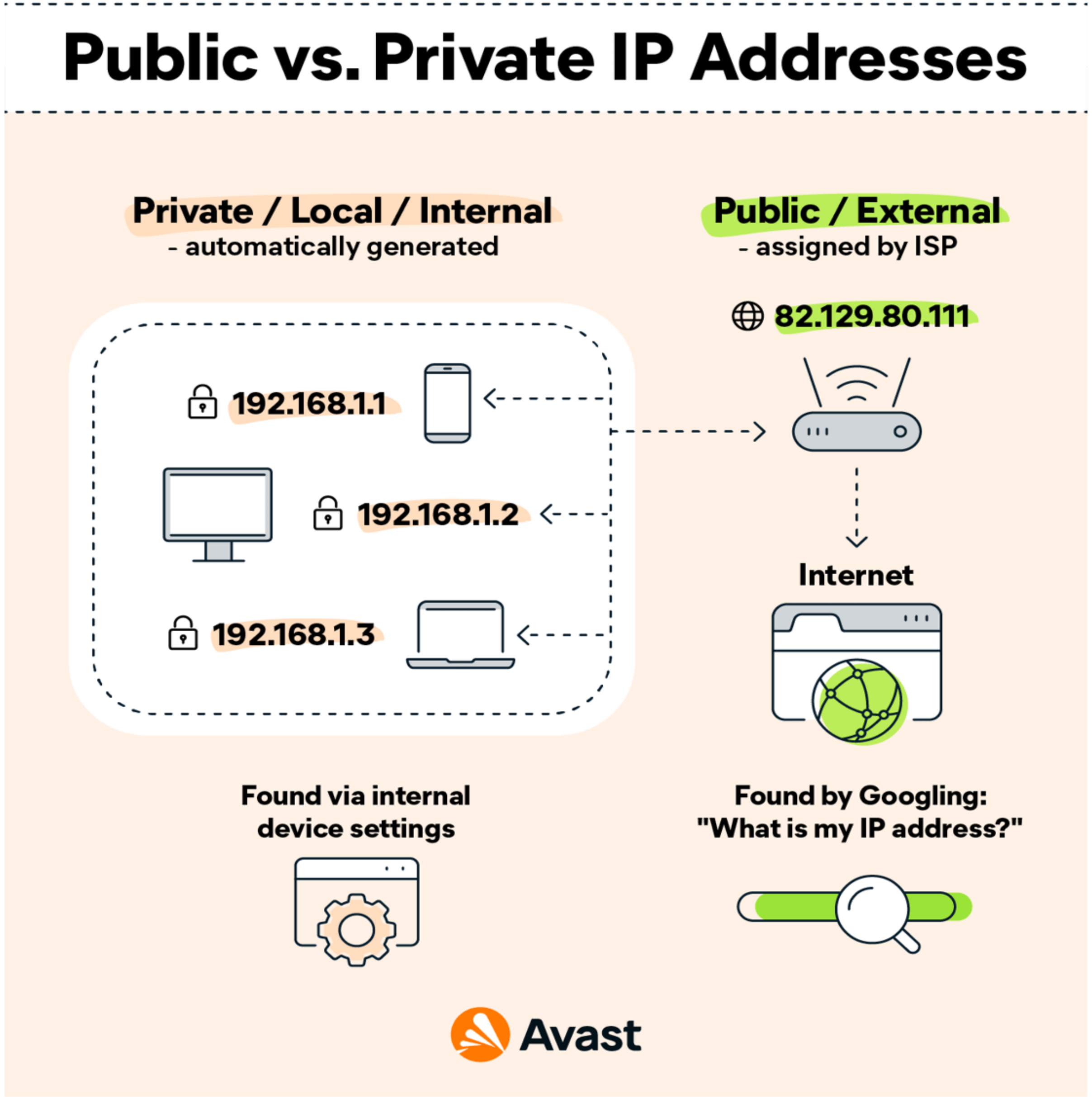
https://study.com/academy/lesson/network-logging-definition-tools.html

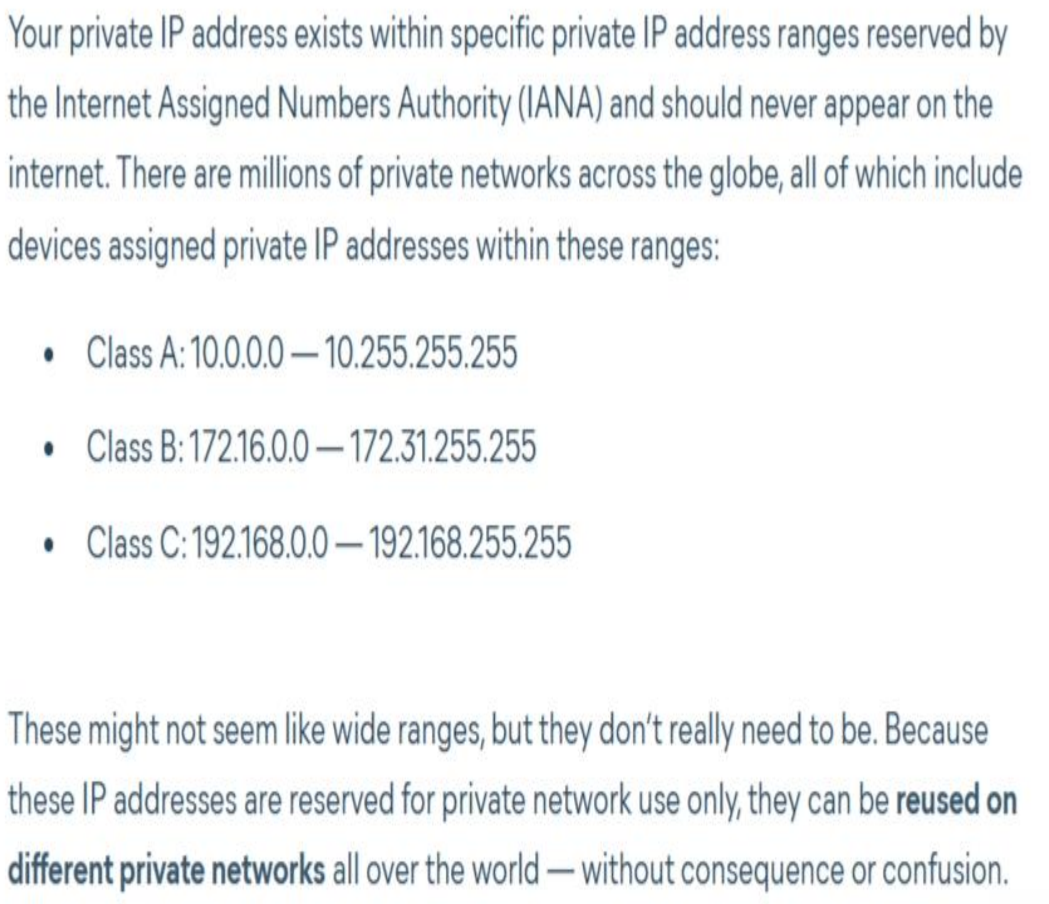


OSI Model

	Data	Layers
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data Representation & Encryption
	Data	Session Inter-Host Communication
	Segments	Transport End-to-End Connections & Reliability
Media Layers	Packets	Network Path Determination & IP
	Frames	Data Link MAC & LLC (Physical Addressing)
	Bits	Physical Media,Signal,& Binary Transmission

Reference: 7 Layers of OSI Model and Their Functions
https://electricala2z.com/cloud-computing/osi-model-layers-7-layers-osi-model/


Public vs. Private IP Addresses
Private / Local / Internal
- automatically generated
Public / External
- assigned by ISP
82.129.80.111
192.168.1.1
192.168.1.2
192.168.1.3
Internet
Found via internal device settings
Found by Googling: "What is my IP address?"
Avast


Your private IP address exists within specific private IP address ranges reserved by the Internet Assigned Numbers Authority (IANA) and should never appear on the internet. There are millions of private networks across the globe, all of which include devices assigned private IP addresses within these ranges:

- Class A: 10.0.0.0 — 10.255.255.255
- Class B: 172.16.0.0 — 172.31.255.255
- Class C: 192.168.0.0 — 192.168.255.255

These might not seem like wide ranges, but they don't really need to be. Because these IP addresses are reserved for private network use only, they can be **reused on different private networks** all over the world — without consequence or confusion.

Reference: Public vs. Private IP Addresses: What's the Difference?
https://www.avast.com/c-ip-address-public-vs-private

1. What is an advantage of UDP over TCP?

(A) UDP communication requires less overhead.

(B) UDP communication is more reliable.

(C) UDP reorders segments that are received out of order.

(D) UDP acknowledges received data.

2. When is UDP preferred to TCP?

(A) When a client sends a segment to a server.

(B) When all the data must be fully received before any part of it is considered useful.

(C) When an application can tolerate some loss of data during transmission.

(D) When segments must arrive in a very specific sequence to be processed successfully.

Reference: 15.3.3 Transport Layer Quiz Answers

https://itexamanswers.net/15-3-3-transport-layer-quiz-answers.html

1. What is an advantage of UDP over TCP?

(A) UDP communication requires less overhead.

(B) UDP communication is more reliable.

(C) UDP reorders segments that are received out of order.

(D) UDP acknowledges received data.

2. When is UDP preferred to TCP?

(A) When a client sends a segment to a server.

(B) When all the data must be fully received before any part of it is considered useful.

(C) When an application can tolerate some loss of data during transmission.

(D) When segments must arrive in a very specific sequence to be processed successfully.

Reference: 15.3.3 Transport Layer Quiz Answers

https://itexamanswers.net/15-3-3-transport-layer-quiz-answers.html

1. What are iptables?

Answer: Iptables is a command line utility used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel.

2. What a chain is in context with iptables?

Answer: A chain is a set of rules that determine how a packet should be handled. When a packet arrives, it is compared against the rules in each chain until a match is found. The packet is then handled according to the action specified in that rule. There are three built-in chains in iptables: INPUT, OUTPUT, and FORWARD.

Reference: 20 IPTables Interview Questions and Answers

https://climbtheladder.com/iptables-interview-questions/

3. What are the most commonly used chains in iptables?

Answer: The most commonly used chains in iptables are the INPUT, OUTPUT, and FORWARD chains. The INPUT chain is used to filter incoming traffic, the OUTPUT chain is used to filter outgoing traffic, and the FORWARD chain is used to filter traffic that is being forwarded through the system.

Reference: 20 IPTables Interview Questions and Answers

https://climbtheladder.com/iptables-interview-questions/

4. Can you explain how to set up an iptable rule for allowing traffic from any host on the network?

Answer: You can set up an iptable rule for allowing traffic from any host on the network by using the “iptables -A INPUT -j ACCEPT” command. This will allow all traffic from all hosts on the network to be accepted.

5. How can you allow access to a particular IP address using iptables?

Answer: You can allow access to a particular IP address using iptables by adding a rule that allows traffic from that IP address. For example, if you wanted to allow traffic from the IP address 1.2.3.4, you would add a rule that looks like this: “iptables -A INPUT -s 1.2.3.4 -j ACCEPT”

Reference: 20 IPTables Interview Questions and Answers

https://climbtheladder.com/iptables-interview-questions/

6. Can you explain how to open port 8080/tcp so that web servers running as non-root users can bind to it?

Answer: You can open port 8080/tcp by adding the following rule to your IPTables configuration: “iptables -A INPUT -p tcp --dport 8080 -j ACCEPT”

Reference: 20 IPTables Interview Questions and Answers

https://climbtheladder.com/iptables-interview-questions/

8. How do you limit the number of concurrent connections coming from a single source IP address to 100?

Answer: You can use the following rule in your iptables configuration:

```
“iptables -A INPUT -p tcp –syn --dport 80 -m connlimit --connlimit-above 100 -j REJECT”
```

This rule will limit the number of concurrent connections to port 80 (HTTP) from any single source IP address to 100. If more than 100 connections are attempted, the rule will reject the connection.

9. Can you tell me some disadvantages of iptables?

Answer: Some disadvantages of iptables include the fact that it can be difficult to configure, and it can be resource intensive if you are using it to filter a lot of traffic. Additionally, iptables can be bypassed if an attacker is able to gain access to the server itself, so it is not a perfect security solution.

Reference: 20 IPTables Interview Questions and Answers

https://climbtheladder.com/iptables-interview-questions/