◇ EASY (Q1–Q10)

Q1. iptables is a user-space utility that interfaces with which Linux kernel framework?
A. SELinux
B. netfilter
C. systemd
D. AppArmor

Q2. Which netfilter table is used by default for packet filtering?
A. nat
B. mangle
C. raw
D. filter

Q3. Which iptables target allows a packet to pass through the firewall?
A. DROP
B. REJECT
C. ACCEPT
D. LOG

Q4. Which iptables target silently discards packets?
A. ACCEPT
B. REJECT
C. LOG
D. DROP

Q5. Stateful Packet Inspection (SPI) relies on which kernel feature?
A. NAT
B. conntrack
C. routing table
D. DNS cache

Q6. Which command-line tool is primarily used to analyze captured packets visually?
A. tcpdump
B. Wireshark
C. traceroute
D. nmap

Q7. Which protocol version introduces mandatory IPsec support?
A. IPv4
B. IPv5
C. IPv6
D. IPv7

Q8. Which iptables chain processes packets destined for the local system?
A. OUTPUT

B. FORWARD
C. INPUT
D. POSTROUTING

Q9. Fail2ban primarily protects against:
A. Malware infection
B. Brute-force attacks
C. DDoS floods
D. Packet sniffing

Q10. Which Wireshark feature allows filtering of displayed packets?
A. Capture filter
B. Display filter
C. Routing filter
D. Protocol mapper

◇ MEDIUM (Q11–Q25)

Q11. In netfilter processing, which hook is triggered before routing decisions?
A. INPUT
B. OUTPUT
C. PREROUTING
D. POSTROUTING

Q12. Which iptables table is mainly used for address translation?
A. filter
B. nat
C. mangle
D. raw

Q13. Which chain is evaluated for packets generated locally?
A. INPUT
B. FORWARD
C. OUTPUT
D. PREROUTING

Q14. How does SPI improve firewall security?
A. Encrypts traffic
B. Tracks connection states
C. Blocks all inbound traffic
D. Uses application signatures

Q15. Which connection state allows return traffic for an established session?
A. NEW

B. INVALID
C. ESTABLISHED
D. DROPPED

Q16. Which iptables match is commonly used with SPI?
A. -m owner
B. -m time
C. -m state / -m conntrack
D. -m mac

Q17. Why is IPv6 firewalling more critical than IPv4 in some cases?
A. IPv6 uses NAT by default
B. IPv6 has globally routable addresses
C. IPv6 blocks ICMP
D. IPv6 disables routing

Q18. Which command-line tool complements Wireshark for live packet capture?
A. nmap
B. tcpdump
C. netstat
D. ss

Q19. Which Wireshark statistic helps analyze traffic distribution by protocol?
A. Follow TCP stream
B. Protocol hierarchy
C. Expert info
D. Packet bytes

Q20. Which Fail2ban component defines actions on detection?
A. Filter
B. Jail
C. Action
D. Rule chain

Q21. In iptables, what happens if no rule matches and default policy is DROP?
A. Packet is accepted
B. Packet is logged
C. Packet is silently dropped
D. Packet is forwarded

Q22. Which netfilter hook handles packets leaving the system after routing?
A. INPUT
B. FORWARD
C. POSTROUTING
D. PREROUTING

Q23. Which Wireshark filter displays only HTTP traffic?
A. tcp
B. port 80
C. http
D. ip.addr

Q24. Which Fail2ban log source is commonly monitored for SSH attacks?
A. /var/log/syslog
B. /var/log/messages
C. /var/log/auth.log
D. /var/log/kern.log

Q25. Which iptables target sends an ICMP error to the sender?
A. ACCEPT
B. DROP
C. REJECT
D. LOG

△ HARD (Q26–Q40)

Q26. Which netfilter hook combination allows NAT to occur before routing?
A. INPUT + OUTPUT
B. PREROUTING + POSTROUTING
C. FORWARD + INPUT
D. OUTPUT + INPUT

Q27. Why is the raw table processed before conntrack?
A. To encrypt packets
B. To bypass connection tracking if needed
C. To modify TTL
D. To log packets

Q28. Which scenario best demonstrates SPI using iptables?
A. Blocking all inbound traffic
B. Allowing ESTABLISHED,RELATED packets
C. Filtering based on MAC address
D. Dropping ICMP packets

Q29. In IPv6 firewalling, which tool replaces iptables?
A. nftables
B. ip6tables
C. arptables
D. ebtables

Q30. Why ICMPv6 must be allowed in IPv6 firewalls?
A. For encryption
B. For Neighbor Discovery and routing functions
C. For NAT traversal
D. For application filtering

Q31. Which Wireshark feature reconstructs application-level conversations?
A. Capture filter
B. Packet bytes pane
C. Follow TCP Stream
D. Expert info

Q32. Which Fail2ban workflow is correct?
A. Attack → Firewall → Log → Ban
B. Log entry → Filter match → Action executed
C. Packet drop → Log → Alert
D. IDS alert → Fail2ban ban

Q33. Which iptables rule best prevents SSH brute-force attacks?
A. Allow all port 22 traffic
B. Rate-limit new SSH connections
C. Drop ESTABLISHED traffic
D. Disable conntrack

Q34. Which netfilter component maintains state information?
A. Routing engine
B. conntrack table
C. filter table
D. mangle table

Q35. Why SPI firewalls are more secure than stateless ones?
A. Faster processing
B. Awareness of session context
C. Encryption support
D. MAC filtering

Q36. Which Wireshark analysis helps identify suspicious retransmissions?
A. Protocol hierarchy
B. TCP stream graph
C. Packet length
D. Display filter

Q37. What is a common pitfall when configuring IPv6 firewalls?
A. Over-filtering ICMPv6
B. Enabling IPsec

C. Using global addresses
D. Logging enabled

Q38. Which Fail2ban feature reduces false positives?
A. Permanent bans
B. Adjustable retry and time windows
C. Disabling logs
D. Blocking entire subnets

Q39. Which iptables concept ensures rules are evaluated sequentially?
A. Rule priority
B. First-match policy
C. Random evaluation
D. Hash-based lookup

Q40. Which integrated approach provides the strongest host-level protection?
A. iptables only
B. Fail2ban only
C. iptables + SPI + Fail2ban
D. Wireshark + tcpdump