**Encryption and Authentication**

* What is a three-way handshake?
* How do cookies work?
* How do sessions work?
* Explain how OAuth works.
* What is a public key infrastructure flow and how would I diagram it?
* Describe the difference between synchronous and asynchronous encryption.
* Describe SSL handshake.
* How does HMAC work?
* Why HMAC is designed in that way?
* What is the difference between authentication vs authorization name spaces?
* What’s the difference between Diffie-Hellman and RSA?
* How does Kerberos work?
* If you're going to compress and encrypt a file, which do you do first and why?
* How do I authenticate you and know you sent the message?
* Should you encrypt all data at rest?
* What is Perfect Forward Secrecy?

**Network Level and Logging**

* What are common ports involving security, what are the risks and mitigations?
* Which one for DNS?
* Describe HTTPs and how it is used.
* What is the difference between HTTPS and SSL?
* How does threat modeling work?
* What is a subnet and how is it useful in security?
* What is subnet mask?
* Explain what traceroute is.
* Draw a network, then expect them to raise an issue and have to figure out where it happened.
* Write out a Cisco ASA firewall configuration on the white board to allow three networks unfiltered access, 12 networks limited access to different resources on different networks, and 8 networks to be blocked altogether.
* Explain TCP/IP concepts.
* What is OSI model?
* How does a router differ from a switch?
* Describe the Risk Management Framework process and a project where you successfully implemented compliance with RMF.
* How does a packet travel between two hosts connected in same network?
* Explain the difference between TCP and UDP.
* Which is more secure and why?
* What is the TCP three way handshake?
* What is the difference between IPSEC Phase 1 and Phase 2?
* What are biggest AWS security vulnerabilities?
* How do web certificates for HTTPS work?
* What is the purpose of TLS?
* Is ARP UDP or TCP?
* Explain what information is added to a packet at each stop of the 7 layer OSI model.
* Walk through a whiteboard scenario for your environment of choice (Win/Linux) in which compromising the network is the goal without use of social engineering techniques (phishing for credential harvesting, etc).
* Explain how you would build a web site that could secure communications between a client and a server and allow an authorized user to read the communications securely.
* How does an active directory work?
* Do you know how Single Sign-On works?
* What is a firewall?
* How does it work?
* How does it work in cloud computing?
* Difference between IPS and IDS?
* How do you build a tool to protect the entire Apple infra?
* How do you harden a system?
* How to you elevate permissions?
* Describe the hardening measures you've put on your home network.
* What is traceroute? Explain it in details.
* How does HTTPS work?
* What would do if you discovered an infected host?
* What is SYN/ACK and how does it work?
* You got the memory dump of a potentially compromised system, how are you going to approach its analysis?
* How would you detect a DDOS attack?
* How does the kernel know which function to call for the user?
* How would you go about reverse-engineering a custom protocol packet?

**OWASP Top 10, Pentesting and/or Web Applications**

* Differentiate XSS from CSRF.
* What do you do if a user brings you a pc that is acting 'weird'? You suspect malware.
* What is the difference between tcp dump and FWmonitor?
* Do you know what XXE is?
* Explain man-in-the-middle attacks.
* What is a Server-Side Request Forgery attack?
* Describe what are egghunters and their use in exploit development.
* How is pad lock icon in browser generated?
* What is Same Origin Policy and CORS?

**Databases**

* How would you secure a Mongo database?
* Postgres?
* Our DB was stolen/exfiltrated. It was secured with one round of sha256 with a static salt.
  + What do we do now?
  + Are we at risk?
  + What do we change?
* What are the 6 aggregate functions of SQL?

**Tools and Games**

* Have I played CTF?
* Would you decrypt a steganography image?
* You're given an ip-based phone and asked me to decrypt the message in the phone.
* What CND tools do you knowledge or experience with?
* What is the difference between nmap -ss and nmap -st?
* How would you filter xyz in Wireshark?
* Given a sample packet capture - Identify the protocol, the traffic, and the likelihood of malicious intent.
* If left alone in office with access to a computer, how would you exploit it?
* How do you fingerprint an iPhone so you can monitor it even after wiping it?
* How would you use CI/CD to improve security?
* You have a pipeline for Docker images. How would you design everything to ensure the proper security checks?
* How would you create a secret storage system?
* What technical skill or project are you working on for fun in your free time?
* How would you harden your work laptop if you needed it at Defcon?
* If you had to set up supply chain attack prevention, how would you do that?

**Programming and Code**

* Code review a project and look for the vulnerability.
* How would you conduct a security code review?
* How can Github webhooks be used in a malicious way?
  + If I hand you a repo of source code to security audit what’s the first few things you would do?
    - Can I write a tool that would search our Github repos for secrets, keys, etc.?
  + Slack?
    - <https://arstechnica.com/security/2016/04/hacking-slack-accounts-as-easy-as-searching-github/>
  + AWS?
  + Etc.
* Given a CVE, walk us through it and how the solution works.
* Tell me about a repetitive task at work that you automated away.
* How would you analyze a suspicious email link?

**Compliance**

* Can you explain SOC 2?
  + What are the five trust criteria?
* How is ISO27001 different?
* Can you list examples of controls these frameworks require?
* What is the difference between Governance, Risk and Compliance?
* What does Zero Trust mean?
* What is role-based access control (RBAC) and why is it covered by compliance frameworks?
* What is the NIST framework and why is it influential?
* What is the OSI model?