1. Explain risk, vulnerability and threat?

TIP: A good way to start this answer is by explaining vulnerability, and threat and then risk. Back this up with an easy to understand example.

Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat e.g. Default username and password for a server – An attacker can easily crack into this server and compromise it (Here's a resource that will navigate you through cyber security attacks).

2. What is the difference between Asymmetric and Symmetric encryption and which one is better?

Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption.

Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel.

Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using symmetric process.

3. What is an IPS and how does it differs from IDS?

IDS is an intrusion detection system whereas an IPS is an intrusion prevention system. IDS will just detect the intrusion and will leave the rest to the administrator for further action whereas an IPS will detect the intrusion and will take further action to prevent the intrusion. Another difference is the positioning of the devices in the network. Although they work on the same basic concept but the placement is different.

4. What is XSS, how will you mitigate it?

Cross site scripting is a JavaScript vulnerability in the web applications. The easiest way to explain this is a case when a user enters a script in the client side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client side.

Countermeasures of XSS are input validation, implementing a CSP (Content security policy) etc (Also consider checking out this career guide for cissp certification).

TIP: Know the different types of XSS and how the countermeasures work.

5. What is the difference between encryption and hashing?

Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.
Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity.

6. Are you a coder/developer or know any coding languages?

TIP: You are not expected to be a PRO; understanding of the language will do the job.

Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to automate tasks, exploit development etc. A little knowledge of the three can be of great advantage - both in the interview and on the floor.

7. What is CSRF?

Cross Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples and countermeasures.

8. What is a Security Misconfiguration?

Security misconfiguration is a vulnerability when a device/application/network is configured in a way which can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

9. What is a Black hat, white hat and Grey hat hacker?

TIP: Keep the answer simple.

Black hat hackers are those who hack without authority. White hat hackers are authorised to perform a hacking attempt under signed NDA. Grey hat hackers are white hat hackers which sometimes perform unauthorised activities.

10. What is a firewall?

TIP: Be simple with the answer, as this can get complex and lead to looped questions.

A firewall is a device that allows/blocks traffic as per defined set of rules. These are placed on the boundary of trusted and untrusted networks.

11. How do you keep yourself updated with the information security news?

TIP: Just in case you haven't followed any: the hacker news, ThreatPost, Pentest mag etc.

Be sure to check and follow a few security forums so that you get regular updates on what is happening in the market and about the latest trends and incidents.

12. The world has recently been hit by ……. Attack/virus etc. What have you done to protect your organisation as a security professional?

Different organisations work in different ways, the ways to handle incident is different for all. Some take this seriously and some not. The answer to this should be the process to handle an incident. Align this with one you had and go on… just don’t exaggerate.

13. CIA triangle?

Confidentiality: Keeping the information secret.

Integrity: Keeping the information unaltered.

Availability: Information is available to the authorised parties at all times.

14. HIDS vs NIDS and which one is better and why?

HIDS is host intrusion detection system and NIDS is network intrusion detection system. Both the systems work on the similar lines. It’s just that the placement in different. HIDS is placed on each host whereas NIDS is placed in the network. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes processing power of the host as well.

Level 02 - Learners (Experienced but still learning)

15. What is port scanning?

Port scanning is process of sending messages in order to gather information about network, system etc. by analysing the response received.

16. What is the difference between VA and PT?

Vulnerability Assessment is an approach used to find flaws in an application/network whereas Penetration testing is the practice of finding exploitable vulnerabilities like a real attacker will do. VA is like travelling on the surface whereas PT is digging it for gold.

17. What are the objects that should be included in a good penetration testing report?

A VAPT report should have an executive summary explaining the observations on a high level along with the scope, period of testing etc. This can be followed by no of observations, category wise split into high, medium and low. Also include detailed observation along with replication steps, screenshots of proof of concept along with the remediation.

18. What is compliance?

Abiding by a set of standards set by a government/Independent party/organisation. E.g. An industry which stores, processes or transmits Payment related information needs to be complied with PCI DSS (Payment card Industry Data Security Standard). Other compliance examples can be an organisation complying with its own policies.

19. Tell us about your Personal achievements or certifications?

Keep this simple and relevant, getting a security certification can be one personal achievement. Explain how it started and what kept you motivated. How you feel now and what are your next steps.

20. Various response codes from a web application?

1xx - Informational responses
2xx - Success
3xx - Redirection
4xx - Client side error
5xx - Server side error

You may also like: Cybersecurity: What's next in 2018?

21. When do you use tracert/traceroute?

In case you can't ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is firewall, ISP, router etc.

22. DDoS and its mitigation?

DDoS stands for distributed denial of service. When a network/server/application is flooded with large number of requests which it is not designed to handle making the server unavailable to the legitimate requests. The requests can come from different not related sources hence it is a distributed denial of service attack. It can be mitigated by analysing and filtering the traffic in the scrubbing centres. The scrubbing centres are centralized data cleansing station wherein the traffic to a website is analysed and the malicious traffic is removed.

23. What is a WAF and what are its types?
TIP: This topic is usually not asked in detail.

WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud based.

24. Explain the objects of Basic web architecture?
TIP: Different organisations follow different models and networks. BE GENERIC.

A basic web architecture should contain a front ending server, a web application server, a database server.

Level 03 - Master (Entered into a managerial position or sitting for one)
25. How often should Patch management be performed?

Patch should be managed as soon as it gets released. For windows – patches released every second Tuesday of the month by Microsoft. It should be applied to all machines not later than 1 month. Same is for network devices, patch as soon as it gets released. Follow a proper patch management process.

26. How do you govern various security objects?

Various security objects are governed with the help of KPI (Key Performance Indicators). Let us take the example of windows patch, agreed KPI can be 99%. It means that 99% of the PCs will have the latest or last month’s patch. On similar lines various security objects can be managed.

27. How does a Process Audit go?

The first thing to do is to identify the scope of the audit followed by a document of the process. Study the document carefully and then identify the areas which you consider are weak. The company might have compensatory controls in place. Verify they are enough.

28. What is the difference between policies, processes and guidelines?

As security policy defines the security objectives and the security framework of an organisation. A process is a detailed step by step how to document that specifies the exact action which will be necessary to implement important security mechanism. Guidelines are recommendations which can be customised and used in the creation of procedures.

29. How do you handle AntiVirus alerts?

Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

30. What is a false positive and false negative in case of IDS?

When the device generated an alert for an intrusion which has actually not happened: this is false positive and if the device has not generated any alert and the intrusion has actually happened, this is the case of a false negative.

You may also like: What are the Top 7 Security certifications?

31. Which one is more acceptable?

False positives are more acceptable. False negatives will lead to intrusions happening without getting noticed.

32. Software testing vs. penetration testing?

Software testing just focuses on the functionality of the software and not the security aspect. A penetration testing will help identify and address the security vulnerabilities.

33. What are your thoughts about Blue team and red team?

Red team is the attacker and blue team the defender. Being on the red team seems fun but being in the blue team is difficult as you need to understand the attacks and methodologies the red team may follow.

34. What is you preferred - Bug bounty or security testing?

Both are fine, just support your answer like Bug Bounty is decentralised, can identify rare bugs, large pool of testers etc.