Penetration Testing Interview Questions

General

- What are the phases in the penetration testing lifecycle? (recon,scan,..)
- What types of penetration testing assessments are there? (Internal/External Infrastructure Penetration Testing / Wireless/Web/mobile)
- Difference between active and passive reconnaissance ?
- How are penetration tests classified?
- What types of penetration testing teams are there and what are their responsibilities?
- What are some of the types of attackers? (Script kiddie/ APT/ Malicious insider)
- What are the most common types of malware?
- What are some of the most common vulnerability databases? (NVD/CVE/exploit db/packetstorm/vulnhub)
- What is the Common Vulnerability Scoring System?
- How would you rate vulnerabilities during a penetration test? (risk matrix)
- At what point of an assessment would you start performing testing?
- What are some of the most common vulnerabilities?
- What is the principle of least privilege?

Infrastructure/Operating Systems

- What is the OSI model and what are its layers?
- What is the difference between TCP and UDP?
- What are some of the most common services and what ports do they run on?
- What is DNS?
- What is ARP?
- What is RDP?
- What is a MAC address?
- What is a firewall and how does it work?
- What is the difference between an IDS and an IPS?
- What are honeypots?
- What is the difference between encoding, hashing and encrypting?
- Name a few type of encoding, hash and encryption
- What is salting and what is it used for

- What is the fastest way to crack hashes?
- Difference between symmetric and asymmetric encryption
- In what format are Windows and Linux hashes stored
- Where are Windows and Linux hashes stored, how can you retrieve them?
- What are cron jobs/scheduled tasks?
- Where are cron jobs stored in Windows and Linux?
- What are the different package managers used in Linux and where are they used?
- Describe the permission system used in Linux file systems
- What are SUID and sudo?
- What is Kerberos and how does it perform authentication?
- What is the difference between WEP, WPA and WPA2
- What is WPS? Why is it insecure?

Common Techniques & Attacks

- How can DNS and ARP be exploited by attackers?
- What is DDoS?
- What is buffer overflow?
- What is packet inspection?
- What is privilege escalation? Provide a few examples
- What is the difference between bruteforce and dictionary attacks?
- What is a golden ticket attack?
- What is a common misconfiguration of FTP and SMB? (anonymous login/ null session)

Web Application Vulnerabilities & Attacks

- what is XSS, what types of XSS are there, what are the consequences of a successful attack and how do you prevent XSS?
- What is SQL Injection, different types and examples, how to prevent ?
- Secure and HTTPOnly flags
- What is CSRF, what does it entail and how can it be prevented?
- What is IDOR, what are its consequences and how can you prevent it?
- What are LFI and RFI and what are the consequences of these attacks? How can they be prevented?
- How can you secure data in transit?

Penetration Testing Tools

- What tool would you use to perform a port scan?
- What tools would you use to inspect network packets?
- What tool would you use to bruteforce passwords, online and offline?
- What tool would you use to automate SQL injection attacks?
- What tool would you use to perform an ARP spoofing attack? (Ettercap)
- What tools would you use to perform testing against WiFi networks
- What tool can help generate malicious executables?
- What tools would you use to scan a network for known vulnerabilities?
- What tool would you use to inspect the route between a host and a destination?

Scenario-Based

- How would you remotely access a service that can only be accessed from within an internal network?
- How would you allow regular users to run bash scripts as root and which way is most secure? (cron jobs)
- If you were able to obtain an NTLM hash but could not decrypt it, how would you use this knowledge to obtain access to the target host? (pHT)
- What measures would you put in place to prevent brute forcing?

refrences

- Penetration Testing Interview