35 Questions Every PENETRATION TESTER Must Know.

scspcommunity SCSP Community scsp-community scsp-community CommunityScsp

1. Define the difference between netNTLM and NTLM hashed.

2. When a connection is sent from your web browser to the web server certain steps take place. Map these onto each OSI Layers.

3. While conducting an application pentest, explain when would you use a Null Byte?

4. What will the command be for an Nmap Scan, which doesn't ping the host nor does any DNS lookups and only returns the results for port tcp/139 and tcp/445?

5. During a pentest you found a Local File Inclusion vulnerability in a *.php* file on a web server. Using this you want to read the *config.php* file, on the server but the code is being interpreted. What work around will you do to access the *config.php* file?

6. Can a SQLi vulnerability lead to Remote Code Execution? If so, explain how?

7. Define the following attack vectors with their preventions: SQLi, XSS, Denial of Service, DDoS, MITM, Phishing, SSTI, Buffer overflow, ARP poisoning, hybrid attacks, URL Manipulation, SSRF, XXE, Brute forcing.

8. What is a webshell? If some protection mechanism is implemented how can you bypass the uploader protections to upload the webshell?

9. Define the Same Origin Policy in relation with the Document Object model.

10. You want to bypass firewall rules when running an nmap scan. Which source port can you specify to scan from to achieve this?

11. Considering there is unlimited budget and resources, draw an optimally secure cooperate network for an organization. It must have the major components including but not limited to, for e.g. the Internet, an Active Directory Server, a user subnet, a web server with a backend database, a human resource server, Wi-Fi access for users, a VPN etc.

12. During an on-site pentest, how will you gather credentials without the use of any active scanning?

13. User authentication is a sensitive action, how can we make it more secure?

14. Define the concept of session hijacking, and explain its various methods.

15. Define kerberoasting.

16. Suppose you have gained physical access to a machine on a corporate domain, it is connected to the network but you don't have credentials for either the domain or the local machine. However, you do have your own laptop. How will you begin testing?

17. A database lies behind a jump server, whose IP address is unknown. How will you target this?

18. During a pentest you gained unprivileged Windows credentials, how can you escalate your privileges?

19. During an application pentest you find a Java applet, what might you do with it?

20. You want to get the Windows host to send you the victim's password hash. What payload would you inject in a HTML page to do so?

21. An application is scoping an authorization cookie to the parent domain. Is this a security concern?

22. During an application pentest you come across a forget password page consisting of 3 steps, (i) Enter your name (ii) Answer 3 security questions (iii) Set a new password. What tests would you perform here?

23. You are Pentesting a Windows host, and you have successfully gained a meterpreter session, what type of post exploitation will you perform next?

24. Define a golden ticket and a silver ticket.

25. At the end of a pentest, you are requested to advise the client some of the top network controls to implement. What would they be?

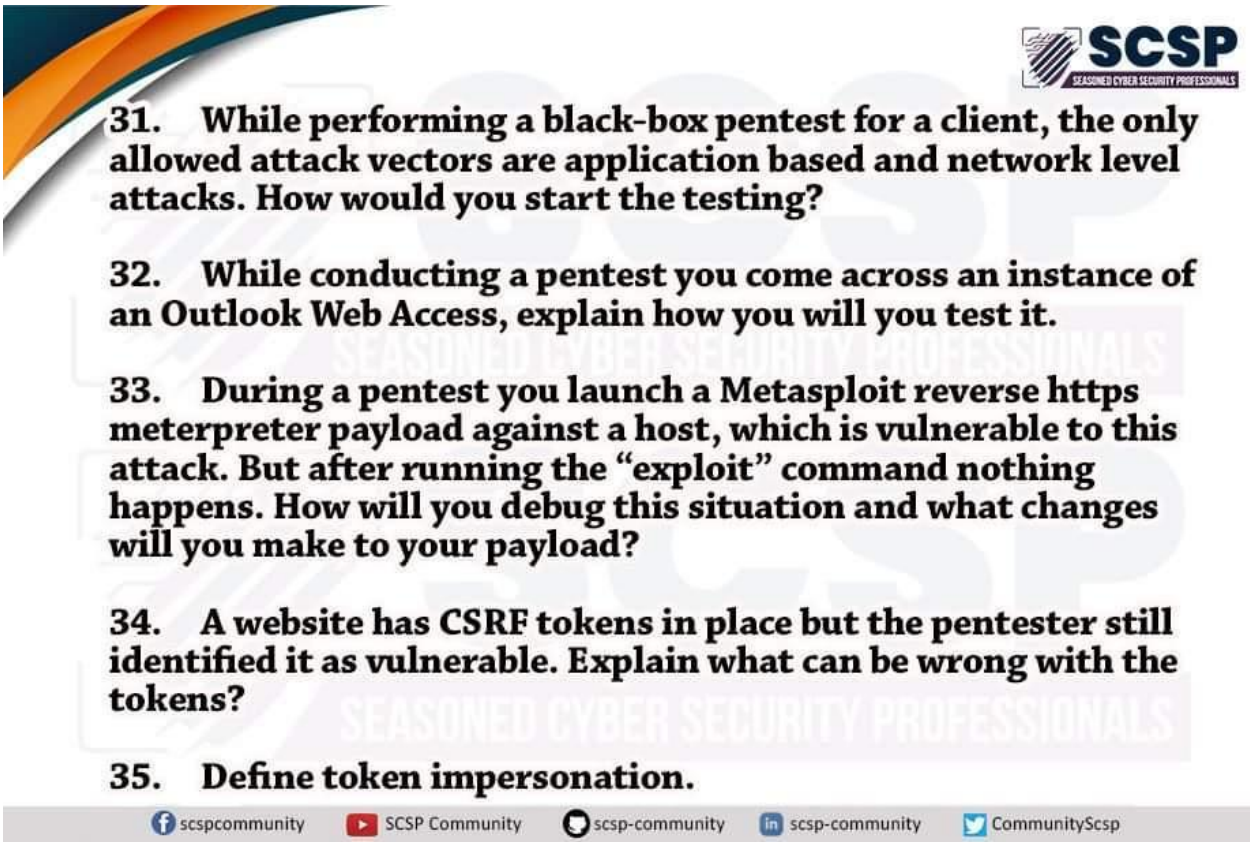
26. Define the most common network vulnerabilities that a pentester may come across.

27. At the end of a pentest, the final findings are presented in front of the C-level executives. They may not possess a strong technical knowledge. Explain how you would show them the impact and criticality of your findings.

28. Identity theft is a rising issue, how can this be prevented?

29. What does the term residual risk mean? And what are ways to deal with risk?

30. You want to extract Active Directory hashes from the AD server, and you only have a compromised Mac OS X laptop in the corporate user subnet. How will you accomplish this?


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
31. While performing a black-box pentest for a client, the only allowed attack vectors are application based and network level attacks. How would you start the testing?
32. While conducting a pentest you come across an instance of an Outlook Web Access, explain how you will you test it.
33. During a pentest you launch a Metasploit reverse https meterpreter payload against a host, which is vulnerable to this attack. But after running the "exploit" command nothing happens. How will you debug this situation and what changes will you make to your payload?
34. A website has CSRF tokens in place but the pentester still identified it as vulnerable. Explain what can be wrong with the tokens?
35. Define token impersonation.
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp