Self-assessment questions -Others

1. Compare Packet filtering and stateful inspection firewalls architectures.

2. Explain the concept of proxy firewalls.

3. Discuss the differences between signature-based detection and heuristic detection

4. Explain how Behavior blocking antimalware works

5. Discuss advantages and disadvantages of signature based IDS.

6. Discuss advantages and disadvantages of statistical anomaly based IDS.

7. Discuss advantages and disadvantages of rule based IDS.

8. Briefly describe what is meant by ‘MAC spoofing’ and how such a technique can be leveraged by a malicious user.

9. Briefly describe what is meant by ‘ARP spoofing’ and how such a technique can be leveraged by a malicious user.

10. What is the 802.1X protocol used for? Describe the

communicating entities that participate and the basic flow of the protocol message exchanges.

11. Someone claims that by spoofing the source IP address of your outgoing network packets, you can effectively hide your online 'identity'. Is this true or not? Explain why.

12. Describe a scenario where and how IP spoofing can be employed by a malicious user.

13. Describe a technique where and how the IP fragmentation process can be misused in order to compromise a network's security status.

14. Describe a technique where and how the IP header's TTL value can be misused in order to bypass network defensive mechanisms.

15. Describe two techniques where the ICMP protocol can be misused against the network and/or the connected hosts.

16. What is a network traffic access control list (ACL) and how it can be employed in securing the network?

17. What NAT stands for and under what situations is commonly employed? What are security-related advantages that NAT provides?

18. In cases where the available public IP addresses are less than the internal systems, a technique referred as PAT

(Port Address Translation) or NAPT (Network Address Port Translation) is commonly employed. Describe how it functions.

19. Briefly describe how the TCP handshake process is leveraged by network scanning tools.

20. Briefly describe what is meant by ‘DHCP starvation’ and how such a technique can be leveraged by a malicious user.

21. The DNS protocol specifies the existence of an ID field in the protocol header. Explain why is this needed and how it can be misused by a malicious entity.

22. What are the major benefits of introducing and using IPSec?

23. Enumerate and explain the basic functionalities of IPSec.

24. What are security associations and why are they important?

25. What are the two basic options (reflected in the corresponding headers) in IPSec and how they differ?

26. What does uniquely identify SA and how?

27. Explain the two different modes of IPSec?

28. What is Security Policy Database (SPD) and what is

its usage?

29. What are the elementary entries of the SPD?

30. What are the basic functionalities of the Authentication Header (AH) and its organization?

31. What is the concept of “anti-replay” and how it is being implemented by using AH?

32. What is Message Authentication Code (MAC) and how it is being calculated?

33. Explain the concept of Encapsulating Security Payload (ESP), it structure, organization and functionality.

34. What are transport and tunnel modes and what, if any, are the major differences?

35. What is the best mode to implement Virtual Private Network (VPN): tunnel or transport one?

36. Explain why an RSA key with a small size (<1024 bits) should be avoided.

37. Assume an e-mail client application that is configured to digitally sign all outgoing messages with the user’s private RSA key. However, the application digitally signs only the body of the message but not any possible attachments. Should the recipient trust such an email message or not and why.

38. Describe the process that must be followed in order to SSL-enable a web server with a CA-signed digital certificate.

39. Briefly describe the main characteristics of the SSL protocol.

40. Briefly describe the handshake phase in the SSL protocol.

41. Why is user authentication in the SSL protocol optional?

Last modified: Monday, 14 February 2022, 10:40