An Intrusion Detection System (IDS) is like a digital security guard for computer networks. Its job is to monitor and analyze the activities happening on a network or a computer system to identify any unusual or suspicious behavior that could indicate a potential security threat.

Normal Behavior vs. Anomalies:

- Normal Behavior: Think of normal behavior as the usual patterns of activity on a computer network. It's like the routine actions and interactions that happen regularly.
- Anomalies: Anomalies are deviations from this normal behavior. They're like unexpected or unusual activities that might signal a security problem.

Difficulty in Anomaly Detection:

- Diverse Activities: Networks have a wide range of activities happening all the time, and it can be challenging to distinguish between regular and suspicious actions.
- Changing Patterns: Normal behavior can change over time, making it tricky to define a fixed set of rules for what is considered normal.
- False Positives: Anomaly detection systems may sometimes mistakenly flag normal behavior as suspicious, leading to false alarms.
- Adaptation by Intruders: Smart attackers can adapt and change their tactics to avoid detection, making it difficult for the IDS to keep up.

Related posts:

- 1. Explain briefly computer security. How you will design the policies for information security within an organization?
- 2. Which components of the computer system need to be secure?

- 3. Discuss the goals of computer security system.
- 4. Describe the problems related with computer security.
- 5. Explain security measure taken to protect the system.
- 6. How can an organization protect its computer system hardware?
- 7. What are the advantages and disadvantages of computer security?
- 8. Write short note on security policy used for computer systems.
- 9. Discuss different security models in details.
- 10. What are the advantages and disadvantages of Biba Model?
- 11. Discuss the security mechanism used to provide security in computer system.
- 12. What are the components of security policy?
- 13. Discuss various attacks in computer security.
- 14. Write short note on server-side attack and insider attack.
- 15. Differentiate between active and passive attack.
- 16. Write a short note on marketplace for vulnerabilities.
- 17. How can we defend zero-day vulnerabilities?
- 18. Discuss error 404 hacking digital India part 1 chase.
- 19. Discuss control hijacking in computer security.
- 20. Describe briefly buffer overflow attack.OR What is control hijacking with an example ? Explain the term of buffer overflow in control hijacking.
- 21. How to prevent buffer overflow attack?
- 22. Explain integer overflow attack.
- 23. How can we prevent integer overflow attack?
- 24. What do you understand by format string vulnerabilities?
- 25. How can we prevent format string vulnerabilities?
- 26. How can we control hijacking attack?
- 27. Define and explain the term confidentiality policy.
- 28. What is Data breach?

- 29. What are the issues related Bell-LaPadula model?
- 30. Explain Discretionary Access Control (DAC).
- 31. Explain the issues related with DAC.
- 32. Describe Mandatory Access Control (MAC).
- 33. What are the problems related with MAC?
- 34. What are the advantage and disadvantages of DAC and MAC?
- 35. Differentiate between DAC and MAC.
- 36. Describe confinement principle in brief.
- 37. Describe detour used in Unix user ids and process ids.
- 38. Explain basic permission bits on non-directories and directories files.
- 39. Define SUID, SGID and sticky bits with basic difference.
- 40. Discuss confinement techniques in details.
- 41. Explain error 404 digital hacking in India part 2 chase.
- 42. What do you understand by VM based isolation?
- 43. Describe the types of VM based isolation.
- 44. Discuss briefly the term rootkit.
- 45. Explain the purpose of rootkit. What are the examples of rootkits?
- 46. Explain various types of rootkits.
- 47. How can we prevent rootkits?
- 48. What is Intrusion Detection System (IDS)?
- 49. Explain the types of intrusion detection system.
- 50. Discuss the need of intrusion detection system.
- 51. Explain advantages and disadvantages of different types of IDS.
- 52. What are the features of intrusion detection system?
- 53. What are the components of IDS?
- 54. Why is security hard?
- 55. What is Access Control list (ACL) and also define what are the technologies used in

access control?

- 56. Write short notes on Software Fault Isolation (SFI)i. Goal and solution, ii. SFI approach.
- 57. Explain briefly the term access control.
- 58. Describe different models of access control.
- 59. Discuss implementation of access control ABAC and MAC.
- 60. Briefly explain the uses of access control system.
- 61. What are the components of access control system?
- 62. Discuss access control principle and security principle used for access control.
- 63. What are the characteristics and features of Unix?
- 64. Differentiate between Unix and Windows.
- 65. What are the various issues in access control?
- 66. Describe browser isolation.
- 67. Explain working of browser isolation.
- 68. Define browser isolation technology. What are browser isolation vendors?
- 69. Define web security with its goals.
- 70. Explain threat modelling. What is its purpose?
- 71. Discuss threat modelling methodologies.
- 72. Explain tools used for threats modelling.
- 73. How to create a threat model?
- 74. What is rendering? Discuss rendering engine. List some rendering engine in web browser.
- 75. Explain security interface framework.
- 76. Describe cookies and frame busting.
- 77. Discuss web server threats in details.
- 78. Describe cross-site request forgery in details.
- 79. How can we prevent CSRF attack?
- 80. When does CSRF attack takes place?

- 81. Write short note on cross-site scripting (XSS).
- 82. Explain different ways used to prevent XSS.
- 83. Describe XSS vulnerabilities.
- 84. What is the principle of public key cryptography? Discuss the applications for public key cryptography.
- 85. Difference between symmetric and asymmetric key cryptography.
- 86. What are the advantages and disadvantages of RSA?
- 87. Write a short note on hybrid cryptosystem.
- 88. Describe briefly the term digital envelope.
- 89. Explain the digital signatures.
- 90. Describe the steps used in creating digital signature.
- 91. Write a short note on Message Digest (MD) hash function.
- 92. What are the properties and requirements for a digital signature?
- 93. Explain the variants of digital signatures.
- 94. What is hash function? Discuss SHA-512 with all required steps, round function and block diagram.
- 95. What are the characteristics of SHA function?
- 96. Discuss public key distribution. Describe the various schemes used for public key distribution.
- 97. Discuss X.509 certificates in detail. What is the role of X.509 certificates in cryptography?
- 98. Discuss X.509 digital certificate format.
- 99. What do you mean by PGP? Discuss its application.
- 100. Discuss the steps that are followed for the transmission and reception of PGP messages.
- 101. Explain real world protocols.
- 102. List the basic terminology used in cryptography.

- 103. Discuss the functionality of S/MIME.
- 104. What is email security?
- 105. What is an email certificate?
- 106. What is Transport Layer Security (TLS)?
- 107. What are the components of TLS? Explain the working of TLS.
- 108. Explain internet protocol security (IPSec) in detail.
- 109. Write a short note on the applications of IP security.
- 110. What are the advantages of IPSec?
- 111. What are the uses of IP security?
- 112. Discuss components of IP Security.
- 113. Explain the working of IP Security.
- 114. Describe briefly Domain Name Server (DNS).
- 115. How DNS security works?
- 116. Explain the DNS security threats.
- 117. Discuss measures against DNS attacks.
- 118. Explain SSL encryption. What are the steps involved inSSL server authentication?
- 119. What is DES? Why were double and triple DES created and what are they?
- 120. Write short note on secret key cryptography. Also list its advantages, disadvantages and examples.
- 121. Define internet infrastructure. What are different internet infrastructures?
- 122. Explain the advantages and disadvantages of in TCP/IP model.
- 123. Give a short summary of IP protocol functions.
- 124. Define routing protocols.
- 125. What are the types of routing protocols?
- 126. Discuss the advantages and disadvantages of different routing protocols.
- 127. What do you mean by DNS? Explain DNS rebinding attack.
- 128. How DNS rebinding work?

- 129. Discuss the features of DNS rebinding attack.
- 130. How can we prevent DNS rebinding attack?
- 131. Explain key management protocol
- 132. What are the advantages and disadvantages of key management protocol?
- 133. What are the security and operational requirements forkey management protocol?
- 134. Write a short note on VPN and tunnel mode.
- 135. Discuss link layer connection in TCP/IP model.
- 136. Write short note on firewall.
- 137. What is packet filtering firewall? Explain its advantage and disadvantage.
- 138. Write short note on telnet.
- 139. Explain briefly fragmentation at network layer.
- 140. Write short note on proxy firewall.
- 141. Write short note on intrusion detection.
- 142. What is packet filtering firewall? Explain its advantage and disadvantage.
- 143. What is Cyberethics?