Program: BE Computer Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VI

Course Code: CSC604 and Course Name: Cryptography and System Security

Time: 1 hour Max. Marks: 50

==============================================================================

=============================================================================

Note to the students:- All the Questions are compulsory and carry equal marks .

|  |  |
| --- | --- |
| Q1. | Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm. |
| Option A: | 882 |
| Option B: | 770 |
| Option C: | 1078 |
| Option D: | 1225 |
|  |  |
| Q2. | Use Caesar’s Cipher to decipher the following HQFUBSWHG WHAW |
| Option A: | ABANDONED LOCK |
| Option B: | ENCRYPTED TEXT |
| Option C: | ABANDONED TEXT |
| Option D: | ENCRYPTED LOCK |
|  |  |
| Q3. | The RSA signature uses which hash algorithm? |
| Option A: | MD5 and SHA-1 |
| Option B: | MD5 |
| Option C: | SSL |
| Option D: | SHA-1 |
|  |  |
| Q4. | DES follows |
| Option A: | Hash Algorithm |
| Option B: | Caesars Cipher |
| Option C: | Feistel Cipher Structure |
| Option D: | SP Networks |
|  |  |
| Q5. | How is IP address spoofing detected? |
| Option A: | Comparing the TTL values of the actual and spoofed addresses |
| Option B: | Installing and configuring a IDS that can read the IP header |
| Option C: | Identify all TCP sessions that are initiated but does not complete successfully |
| Option D: | Implementing a firewall to the network |
|  |  |
| Q6. | Which cryptographic algorithm is used in CMAC? |
| Option A: | RC-4 |
| Option B: | AES |
| Option C: | Triple DES and AES |
| Option D: | DES |
|  |  |
| Q7. | How many rounds does the AES-192 perform? |
| Option A: | 10 |
| Option B: | 12 |
| Option C: | 14 |
| Option D: | 16 |
|  |  |
| Q8. | What is the block size in the Simplified AES algorithm? |
| Option A: | 8 bits |
| Option B: | 14 bits |
| Option C: | 20 bits |
| Option D: | 36 bits |
|  |  |
| Q9. | In RSA, Ф(n) = \_\_\_\_\_\_\_ in terms of p and q. |
| Option A: | (p)/(q) |
| Option B: | (p) \* (q) |
| Option C: | (p-1)(q-1) |
| Option D: | (p+1)(q+1) |
|  |  |
| Q10. | SSM stands for |
| Option A: | Secure Security Module |
| Option B: | Session Security Module |
| Option C: | Service Session Module |
| Option D: | Session Service Module |
|  |  |
| Q11. | What is the PGP stand for? |
| Option A: | Permuted Gap Permission |
| Option B: | Permuted Great Privacy |
| Option C: | Pretty Good Permission |
| Option D: | Pretty Good Privacy |
|  |  |
| Q12. | The issuer unique identifier of the X.509 certificates was added in which version? |
| Option A: | 1 |
| Option B: | 2 |
| Option C: | 3 |
| Option D: | 4 |
|  |  |
| Q13. | What is the full-form of CMAC? |
| Option A: | Code-based MAC |
| Option B: | Cipher-based MAC |
| Option C: | Construct-based MAC |
| Option D: | Collective-based MAC |
|  |  |
| Q14. | In an IP packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet? |
| Option A: | 16 |
| Option B: | 32 |
| Option C: | 12 |
| Option D: | 14 |
|  |  |
| Q15. | The full form of SSL is |
| Option A: | Serial Session Layer |
| Option B: | Secure Socket Layer |
| Option C: | Session Secure Layer |
| Option D: | Series Socket Layer |
|  |  |
| Q16. | In SSL which protocol consists of only 1 bit? |
| Option A: | Alert Protocol |
| Option B: | Handshake Protocol |
| Option C: | Upper-Layer Protocol |
| Option D: | Change Cipher Spec Protocol |
|  |  |
| Q17. | URL stands for – |
| Option A: | Universal Remote Locator |
| Option B: | Universal Resource Language |
| Option C: | Uniform Resource Locator |
| Option D: | Uniform Resource Language |
|  |  |
| Q18. | Which of the stored procedure is used to test the SQL injection attack? |
| Option A: | xp\_write |
| Option B: | xp\_regwrite |
| Option C: | xp\_reg |
| Option D: | xp\_Read |
|  |  |
| Q19. | In a \_\_\_\_\_\_\_\_\_\_\_\_\_ attack, the extra data that holds some specific instructions in the memory for actions is projected by a cyber-criminal or penetration tester to crack the system. |
| Option A: | Phishing |
| Option B: | MiTM |
| Option C: | Buffer-overflow |
| Option D: | Clickjacking |
|  |  |
| Q20. | Packet sniffers involve \_\_\_\_\_\_\_\_\_\_\_\_ |
| Option A: | Active receiver |
| Option B: | Passive receiver |
| Option C: | Legal receiver |
| Option D: | Partially-active receiver |
|  |  |
| Q21. | Firewalls are often configured to block \_\_\_\_\_\_\_\_\_\_\_ |
| Option A: | UDP traffic |
| Option B: | TCP traffic |
| Option C: | Sensitive traffic |
| Option D: | Best-effort traffic |
|  |  |
| Q22. | What is one advantage of setting up a DMZ with two firewalls? |
| Option A: | You can control where traffic goes in three networks |
| Option B: | You can do stateful packet filtering |
| Option C: | You can do load balancing |
| Option D: | You can do stateless packet filtering |
|  |  |
| Q23. | What is the major drawback of anomaly detection IDS? |
| Option A: | These are very slow at detection |
| Option B: | It generates many false alarms |
| Option C: | It doesn’t detect novel attacks |
| Option D: | These are very fast at detection |
|  |  |
| Q24. | What are the strengths of the host based IDS? |
| Option A: | Attack verification |
| Option B: | System specific activity |
| Option C: | No additional hardware required |
| Option D: | Attack verification, System specific activity, No additional hardware required |
|  |  |
| Q25. | \_\_\_\_\_\_\_ are used as the base of the Public Key Infrastructure. |
| Option A: | SSL certificates |
| Option B: | TLS certificates |
| Option C: | X.509 certificates |
| Option D: | HAS certificates |