U.G. Department of Computer Applications

N.G.M College, Pollachi

16UBC627 & Information Security

K1 & K2 Level Questions

Unit:I

1. **This technology is used to measure and analyze human body characteristics for authentication purposes.**
a. Footprinting b. Biometrics c. JBOD d. Anthropomorphism

2. **_____ is an electronic or paper log used to track computer activity.**
a. Traceroute b. Cookie c. Weblog d. Audit trail

3**. This is a series of messages sent by someone attempting to break into a computer to learn which computer network services the computer provides.**
a. Bit robbing b. Web services description language (WSDL) c. Jabber
d. Port scan

4. **This is the name for a group of programmers who are hired to expose errors or security holes in new software or to find out why a computer network's security is being broken**.
a. ERM group b. Computer emergency response teamc. Tiger team
d. Silicone cockroach

5. **This is a mechanism for ensuring that only authorized users can copy or use specific software applications.**
a. Authorized program analysis report b. Private key c. Service level agreement
d. Dongle

6. **At which two traffic layers do most commercial IDSes generate signatures?**
a. Application layer b. Network layer c. Session layer d. Transport layer

7. **This is a Peripheral Component Interconnect (PCI) card that offloads SSL processing to speed up secure transactions on e-commerce Web sites.**
a. PCMCIA card b. Smart card c. Server accelerator card d. Network interface card

8. **_____is a form of eavesdropping used to pick up telecommunication signals by monitoring the electromagnetic fields produced by the signals.**
a. Reverse engineering b. Magneto resistive head technology
c. Van Eck phreaking d. Electronic data processing (EDP)

9**. This enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.**
a. Security Identifier (SID) b. Public key infrastructure (PKI)
c. Internet Assigned Numbers Authority (IANA) d. Private Branch Exchange (PBX)

10. **This is an assault on the integrity of a security system in which the attacker substitutes a section of cipher text (encrypted text) with a different section that looks like (but is not the same as) the one removed.**
a. Trojan horse b. Hashing c. Switching fabric d. Cut and paste attack

Unit:II

11. **Which of the following is an advantage of anomaly detection?**
a. Rules are easy to define. b. Custom protocols can be easily analyzed.
c. The engine can scale as the rule set grows. d. Malicious activity that falls within normal usage patterns is detected.

12**. A false positive can be defined as…**
a. An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior.
b. An alert that indicates nefarious activity on a system that is not running on the network.
c. The lack of an alert for nefarious activity.
d. Both a. and b.

13**. This is an encryption/decryption key known only to the party or parties that exchange secret messages.**
a. E-signature b. Digital certificate c. Private key d. Security token

14. **What is the purpose of a shadow honeypot?**
a. To flag attacks against known vulnerabilities
b. To help reduce false positives in a signature-based IDS.
c. To randomly check suspicious traffic identified by an anomaly detection system.
d. To enhance the accuracy of a traditional honeypot.

15. **This is is the hiding of a secret message within an ordinary message and the extraction of it at its destination.**
a. Secret key algorithm b. Message queuing c. Spyware d. Steganography

16. **An IDS follows a two-step process consisting of a passive component and an active component. Which of the following is part of the active component?**
a. Inspection of password files to detect inadvisable passwords
b. Mechanisms put in place to reenact known methods of attack and record system responses
c. Inspection of system to detect policy violations
d. Inspection of configuration files to detect inadvisable settings

17**. When discussing IDS/IPS, what is a signature?**
a. An electronic signature used to authenticate the identity of a user on the network
b. Attack-definition file
c. It refers to "normal," baseline network behavior
d. None of the above

18. **"Semantics-aware" signatures automatically generated by Nemean are based on traffic at which two layers?**
a. Application layer b. Network layer c. Session layer d. Both a and c

19. **It is OK to put sensitive information in HIDDEN form fields; after all, they are hidden.**
a. True b. False

20**. In what type of attack does an intruder manipulate a URL in such a way that the Web server executes or reveals the contents of a file anywhere on the server, including those lying outside the document root directory?**
a. Cross-site scripting b. Command injection c. SQL injection
d. Path traversal attacks

Unit:III

21. **Which of the following is true of improper error handling?**
a. Attackers can use error messages to extract specific information from a system.
b. Attackers can use unexpected errors to knock an application off line, creating a denial-of-service attack.
c. Unexpected errors can provide an attacker with a buffer or stack overflow condition that sets the stage for an arbitrary code execution.
d. All of the above.

22. **The "NO-CACHE" cache-control response header prohibits documents from being stored on the client.**
a. True b. False

23. **Which of the following is NOT recommended for securing Web applications against authenticated users?**
a. Client-side data validation
b. Filtering data with a default deny regular expression
c. Running the application under least privileges necessary
d. Using parameterized queries to access a database

24**. In which of the following exploits does an attacker insert malicious coding into a link that appears to be from a trustworthy source?**
a. Cross-site scripting b. Command injection
c. Path traversal attack d. Buffer overflow

25. **Encrypted data is not at risk by key loggers.**
a. True b. False

26**. In which of the following exploits does an attacker add SQL code to a Web form input box to gain access to resources or make changes to data?**
a. Cross-site scripting b. Command injection
c. SQL injection d. Buffer overflow

27. **Which of the following is characteristic of spyware?**
a. Blocking access to antivirus and antispyware updates
b. Aggregating surfing habits across multiple users for advertising
c. Customizing search results based on an advertiser's needs
d. All of the above

28. **Web application variables can still be manipulated even when both client and server are using digital certificates to authenticate themselves and establish an SSL connection.**
a. True b. False

29. **One of the most obvious places to put an IDS sensor is near the firewall. Where exactly in relation to the firewall is the most productive placement?**
a. Inside the firewall b. Outside the firewall c. Both d. None

30. **This was commonly used in cryptography during World War II.**
a. Tunneling b. Personalization c. Van Eck phreaking d. One-time pad

Unit: IV

31. **Today, many Internet businesses and users take advantage of cryptography based on this approach.**
a. Public key infrastructure b. Output feedback
c. Encrypting File System d. Single sign on

32. **This is the name for the issuer of a PKI certificate**.
a. Man in the middle b. Certificate authority
c. Resource Access Control Facility d. Script kiddy

33. **Developed by Philip R. Zimmermann, this is the most widely used privacy-ensuring program by individuals and is also used by many corporations**.
a. DSS b. OCSP c. Secure HTTP d. Pretty Good Privacy

34. **This is the encryption algorithm that will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years as the new standard encryption algorithm**.
a. Rijndael b. Kerberos c. Blowfish d. IPsec

35. **This is the inclusion of a secret message in otherwise unencrypted text or images**.
a. Masquerade b. Steganography c. Spoof d. Eye-in-hand system

36. **In password protection, this is a random string of data used to modify a password hash**.
a. Sheepdip b. Salt c. Bypass d. Dongle

37. **This is a mode of operation for a block cipher, with the characteristic that each possible block of plaintext has a defined corresponding cipher text value and vice versa.**
a. Foot printing b. Hash function c. Watermark d. Electronic Code Book

38. **This is a trial and error method used to decode encrypted data through exhaustive effort rather than employing intellectual strategies**.
a. Chaffing and winnowing b. Cryptanalysis c. Serendipity d. Brute force cracking

39**. An intruder might install this on a networked computer to collect user ids and passwords from other machines on the network.**
a. Passphrase b. Root kit c. Ownership tag d. Token

40. **This type of intrusion relies on the intruder's ability to trick people into breaking normal security procedures.**
a. Shoulder surfing b. Hijacking c. Brain fingerprinting d. Social engineering

Unit:V

41**. The developers of an operating system or vendor application might issue this to prevent intruders from taking advantage of a weakness in their programming.**
a. Cookie b. Key fob c. Watermark d. Patch

42**. This is an attack on a computer system that takes advantage of a particular vulnerability that the system offers to intruders.**
a. Port scan b. Denial of service c. Exploit d. Logic bomb

43**. This is a program in which harmful code is contained inside apparently harmless programming or data**.
a. Snort b. Honeypot c. Blue bomb d. Trojan horse

44. **This is the modification of personal information on a Web user's computer to gain unauthorized information with which to obtain access to the user's existing accounts.**
a. Identity theft b. Cookie poisoning c. Shoulder surfing d. Relative identifier

45. **This type of attack may cause additional damage by sending data containing codes designed to trigger specific actions - for example, changing data or disclosing confidential information.**
a. Buffer overflows b. Block cipher
c. War dialing d. Distributed denial-of-service attack

46**. This is the forging of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.**
a. Foot printing b. Non repudiation c. E-mail spoofing d. Finger

47. **This is a type of network security attack in which the intruder takes control of a communication between two entities and masquerades as one of them.**
a. Hijacking b. Identity theft c. Smurf attack d. Tunneling

48. **This is a compromised Web site that is being used as an attack launch point in a denial-of-service attack.**
a. Bastion host b. Packet monkey c. Dongle d. Zombie

49.**This electronic "credit card" establishes a user's credentials when doing business or other transactions on the Web and is issued by a certification authority**.
a. Private key b. Digital certificate c. Smart card d. Ownership tag

50.**What "layer" of an e-mail message should you consider when evaluating e-mail security?**
a. TCP/IP b. SMTP c. Body d. All of the above

****

ANSWER KEY: Information Security:

1.b; 2.d; 3.d; 4.c; 5.d; 6.b; 7.c; 8.c; 9.b; 10.d; 11.c; 12.d; 13.c; 14.c; 15.d; 16.b; 17.b; 18.d; 19.b; 20.d; 21.d; 22.b; 23.a; 24.a; 25.b; 26.c; 27.b; 28.a; 29.a; 30.d; 31.a; 32.b; 33.d; 34.a; 35.b; 36.b; 37.d; 38.d; 39.b; 40.d; 41.d; 42.c; 43.d; 44.b; 45.a; 46.c; 47.a; 48.d; 49.b; 50.d

U.G. Department of Computer Applications

N.G.M College, Pollachi

16UBC627 – Information Security

K3-Level Questions

Unit –I

11. List and elaborate the current Security Trends.
12. Discuss the various Security Threats.
13. Distinguish the threat models and give its benefits.
14. Differentiate Authorization and Authentication.
15. Examine the OSI Security architecture.

Unit – II

6. Explain Symmetric encryption with diagram.
7. Discuss about Public key Encryption with appropriate diagram.
8. Examine the Cryptographic protocols in the distributed systems.
9. Explain DES Encryption Algorithm with diagram.

Unit – III

10. Discuss in detail about the types of Intruders.
11. List and explain the various Intrusion techniques.
12. Categorize the Intruders and their behaviour pattern.
13. Discuss the various database management techniques used in trusted systems.

Unit – IV

14. Explain Defensive programming.
15. Discuss in detail about the Security failures.

16. List out the technical trends affecting software security.

17. List the various Implementation flaws.

Unit – V

18. Discuss about Safe languages and sand box testing.

19. Write a survey on Electronic Voting system.

20. Explain trusted devices.

21. List out the various Networks based Attacks.

22. Survey “Privacy in Security”.

K4-Level Questions.

Unit – I

1. Discuss in detail about the Security Attacks and Security Mechanisms.

2. Elaborate Enforcement of Security and Security Evaluation.

3. List the various Security services and explain them.

4. List and elaborate the types of Security attacks with diagram.

Unit – II

5. Give a detailed study on Cryptography and its protocols.

6. Discuss in detail about Hash functions.

7. Give a detailed account on Public key cryptography with diagram.

8. Survey “Cryptographic protocols and their integration into Distributed syetems”.

Unit – III

9. Explain the various Intrusion Detection approaches.

10. Give a detailed account on Password management.

11. List the various Types of Virus and explain them.

12. Discuss in detail about the Firewalls and its types.

Unit – IV

13. Explain in detail about the following:
    (i) Hackers (ii) Crackers (iii) Attackers

14. Discuss in detail about Buffer Overrun.

15. Discuss in detail about Defensive programming and its techniques.

16. Give a detailed account on Secure software engineering.

Unit – V

17. Give a detailed study on Network based Attacks and the Security Laws.

18. Discuss in detail about Digital rights management and copy protection.

19. Analyze the code for Security Errors.

20. Survey “Denial of Service and Availability”.