262 Past Year Paper
Part A

1. Three types of malware are viruses, Trojan horses and worms These malwares are categorized based on the way the malwares are activated and propagated. Virus propagates by manual transferring of infected files; worm propagates using only network connection; and Trojan horses are disguised as legitimate software to gain access to computers, once activated, Trojan horses can enable cyber-criminals to spy on the victim, steal sensitive data, and gain backdoor access to the system .

2. Lamport's one-time password scheme relies on using hash functions that are one-way and collision resistant. One-way means the hash function takes in any input and produces a hash digest, and there is no way one can obtain the input from the hash digest. Collision resistant means there is no possibility (very small) that a hash function can product the same hash digest from two different input.

3. Each row of the authorization table of Sandhu & Samarti contains access triplet (Subject, Object, Action). It is also known as the capabilities which is from the point of view of the subject's action on the various objects.

4. A least upper bound for a lattice implies Domination, in other words, there exists at least one level that dominates the rest.

5. Data perturbation can be used in statistical database to change the values in the database such that the statistical information is accurate, but the inferential data is inaccurate to provide protection against inference attack.

6. Spear phishing differs from general phishing in that Spear phishing is targeting a specific person while general phishing is targeting all the people and expecting some to be fooled.

7. Firewalls are assumed to be trusted and invulnerable. There are two other main assumptions, access to the firewall should be through firewall and only authorized traffic should be allowed through the firewall.

8. Syncookies provide protection against connection based denial of service by not dropping connection when the SYN queue fills up until the server receives a "correct" ACK from the client. At this time, the server can reconstruct the SYN queue entry and then connection proceeds as usual.

9. The two primary bases for intrusion detection agents are Host based and Network base.

10. The purpose of sanitization in the context of auditing is to remove any information for which there is a user who is not allowed to see that information.

11. In multilevel access control every subject and object is given clearances and classification or sensitivity and access is determined by a set of rules, for example, Bell-La Padula rules.

12. Treating programs as data until verified provides protection against malware as if a program is treated as data, it would not be executed and the virus will not take effect.

13. Persistent and non-persistent XSS differ in that in persistent XSS, data provided by Web client stays (is stored) on the server, while non-persistent XSS, the data provide by a web client is used immediately, usually without proper sanitisation by server-site scripts to generate result for the user.

14. One major role of a honeypot is to divert attackers from a critical system, and/or collect information about the attacker's activities.

15. A master password is typically used to protect sensitive information such as other passwords and certificates.

16. Units are relevant in digital forensics and logging because

17. The Biba model is for the purpose of Integrity Control while BLP is for the purpose of access control.

18. Phishing emails are typically sent in bulk because The attacker cannot expect to fool most people; the attacker just hopes to fool some.

19. PAT(Port Address Translation) hides internal network addresses (TCP/IP) from the outside world by mapping the external addresses to multiple internal addresses.

20. DNS-based phishing infers with poisoning of hosts file or polluting the user's DNS cache with incorrect information resulting in incorrectly configured DNS or corrupted DNS.

21. Two primary properties used in malware classification are based first on how it spreads or propagates to reach the desired targets, and then on the actions or payloads it performed once a target is reached.

22. Aggregate functions provide computed/aggregated data, which is likely to be less sensitive than individual values.

23. The three primary components of a virus are infection mechanism, which spread the payload, which is what besides spreading the virus, and trigger which is the condition to be met before the payload is activated.

24. Two applications of reverse engineering are malware and Digital rights management.

25. Two channel authentication uses two separate channels to accomplish targeted authentication. One channel is from the client to the server and the second channel is from the server to the client using a different channel (eg telephone or a device etc) to give targeted authentication.

26. A pseudonymising sanitizer removes information from the log such that the originator of the log can reconstruct the deleted information but preserves information and the relationship relevant for the analysis.

27. The C library function strcpy() is considered unsafe because it doesn't check for array boundary, so it may result in buffer overflow.

28. Two classes of intruder than an intrusion detection system may attempt to find are:

    Clandestine, who try to avoid the intrusion detection or auditing system and

    Masquerader, who pretend to be a legitimate user.

29. An event being “Not known to be bad” likely refers to not being on an event description of activities considered to be violating security policies in the context of Intrusion detection system.

30. “Online” and “offline” attacks differ in that online require that connection to be active which may impose certain restrictions while attempting to break the password while offline attack has unlimited changes to break the password.

31. Two resources that can be targeted in a DOS attack is network bandwidth (for network) or memory storage and processor capacity (for computer).

32. Examples of each of the main authentication bases are Single sign-on, multiple factor authentication and biometric.

33. CAPCHA can be used to provide protection against DOS (Denial of Services) attacks because bot(zombies) or automated systems cannot read the distorted image and hence this can be used to differentiate between a human (person) or a zombie accessing a system.

34. Obfuscation and reverse engineering are related in that reverse engineering is trying to produce the source code from the executable, but code obfuscation makes it difficult to reverse engineer and obtain the code. In short, obfuscation is trying to prevent reverse engineering.

35. Two methods of grouping entities for access control are Group based access control, where users are assigned to groups and Role based access control (RBAC), where access control are done based on the roles that users assume in a system rather than the user’s identity.

36. A timing based side channel attack attempts to __ by __.

37. The use of external variables in languages such as PHP or Bash is dangerous because PHP registers all kinds of external variables in the global namespace, hence there is really no way to ensure that those external variables contain authentic data that can be trusted. As a result, injection attacks are possible.

38. Two things that packet filtering firewalls would typically filter based on are Collection of rules and default security policy.

39. SQL rand in a mechanism for protecting a database against SQL injection by adding a random key to SQL keyword (internally). Before the keywords are actually sent to the database, the random key is removed.

40. A maximum time between password changes is specified so that the user is forced to change his/her password.

41. The principle of least privilege implies we should give a subject the lowest security level to access a higher security level object.

42. The Chinese Wall Model is designed to handle conflict of interest, a concept that is used to control access to objects that might conflict the interest of the subject. The main idea in this concept is to use a logical wall (barrier) to prevent a subject that accesses data from one side of the wall from accessing data on the other side which has conflict of interest.

43. Role hierarchies in RBAC support hierarchical structure of roles in an organization. It makes use of the concept of inheritance to enable one role to implicitly include access rights associated with a subordinate role.

44. The common ground between misfeasors and masqueraders is that both have the password for a legitimate account.

45. Pharming involves modification of hosts file, perhaps through a virus, or by compromising or “poisoning” DNS servers that translate URL’s into IP addresses.

46. DOS amplification is characterized by Making use of several intermediaries, e.g zombies and reflectors.

47. One advantage of using roles, in databases for example, is to organize the granting of privileges based on least (minimal) required privileges by job scope or functional activities.

48. To be stateless means a server has not committed any resources and is relevant in the context of client puzzle connection protocol.

49. Sub puzzles allow the average number of operations to remain the same while reducing the standard deviation.

50. Examples of each of the main authentication bases are password, PIN, or a secret for what a subject knows, a card, badge, or device for what a subject has, biometrics such as fingerprints or retinal characteristics for what a subject is and in front of a particular terminal or in a specific room for where an entity is.

51. Two security properties of a cryptographic hash function are one-way, that is, it is infeasible to generate the preimage from the hash digest, and collision resistance, that is, it is infeasible to have two different messages with the same hash value.

52. Two possible consequences of a buffer overflow are exploitation by an attacker to inject malware to cause an attack against availability such as denial of service and running some arbitrary code to modify data (attack data integrity) as well as stealing information (attack on data confidentiality).

53. The principle of least privilege is reflected via a partial order $\leq$ (generally a reflexive, antisymmetric, and transitivity relation), so that for every two elements $a, b \in L$ there exists a least upper bound $u \in L$ and a greatest lower bound $l \in L$ in a lattice.

54. Random seeding a password generator with time alone is a bad idea because if an attacker knows the time, the attacker can use the same time as the seed to the random generator to regenerate the same sequence of password.

55. Inference is the derivation of Sensitive information from non-sensitive, typically aggregate data.

56. Error-based SQL injection uses Error messages thrown by the database server to obtain information about the structure of the database.

57. A chain of custody provides assurances that evidences collected during digital forensics are un-altered.

58. The phrase “Something you have, something you know, or something you are” refers to the bases of authentication. In authentication, something you have, something you know or something you are refers to the three factors used in authentication. An example of something you have is a staff card, something you know is a password, and something you are is a fingerprint.

59. Stack randomization is used to protect against buffer overflow attacks and works by randomizing the new buffer location, the new instance of the program run is probably in a different memory location and hence make the overflow attack difficult.

60. Salt is used in the UNIX based password system, where the password and salt are hashed to hide the relationship between a user and the password used. In the event an intruder is able to get the password file, the intruder will not be able to establish the association of the password to its user because the salt is a value that is randomly generated.

61. XSS is an abbreviation for cross site scripting. It is a type of injection attack in which an attacker can use it to send a malicious script to an unsuspecting user and exploits vulnerabilities of the dynamic web pages, in particular, it involves the use of those vulnerabilities to gather data from a user that should not be gathered.

62. Sanitisation in the context of logs involves removing information from the log that a user should not be able to see to provide confidentiality of the log.

63. The purpose of sanitization in the context of auditing is to remove any information for which there is a user who is not allowed to see that information.

64. Cohen’s undecidability theorem states “It is undecidable whether an arbitrary program contains a computer virus”.

65. A firewall cannot protect against internal attackers or services that by-pass the firewall, eg dial-up connection.

66. Single sign-on has a single point of entry as a gateway to multiple systems, using a master password, necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and authentication information.

67. A minimum time between password changes is specified so users are able/forced to change the password and to make sure that the passwords are secured from the attacker who may be trying to hack their passwords.

68. The channels used in two channel authentication are different between each other where one channel is between the client and the server, and the other is between the server and the client and must be independent.

69. The BLP ds-property provides permission may be passed from an authorized subject to another, level authorized subject.

70. The two primary aims of digital forensics are to gather evidence from computer devices to investigate a crime or to recover lost data.

71. Pharming is more technical and less social engineering than deceptive phishing because it involves technology to perform the phishing act. It is carried out by modifying the hosts file through virus or “poison” DNS servers.

72. Consider that file A is infected with a virus and that file B is not currently infected. File B can be directly infected by the actions of Carol if she executes file A and writes file B after that. By executing file A, Carol will be infected with the virus and by writing file B, the virus will spread to infect file B.

73. An advantage of stateless puzzles over stateful puzzles is that the answer to stateless puzzles is nothing.