Written exam in TSIT02 Computer security

14:00–18:00, 13th January 2020

Guilherme B. Xavier
Institutionen för Systemteknik,
Linköpings Universitet

Permitted equipment: General dictionaries between English and another language without personal notes. (Thus not specific scientific dictionaries with or without formulæ.)

Grading: Grade 3 requires at least **22** points, while grade 4 requires **28** and grade 5 **33** points respectively.

Other information: There are 40 multiple choice questions, each being worth one point. **To avoid blind guessing, 3 wrong answers will eliminate one correct one.** Therefore if you are completely unsure of the answer to a question, it is best to leave it blank. You do not need to mark which questions you have done on the examination front page (since there are more than 30 questions).

Answers should be handed in on a single sheet of paper. Try to have the answers provided in numerical order, beginning with the first one, one answer per line. When you run out of space (lines), start a second column close to the top.

1. **What is the purpose of an encryption cipher such as AES?**
   a) To provide integrity to the information.
   b) To protect against denial-of-service attacks.
   c) To authenticate the communicating parties.
   d) To provide confidentiality to the information.

2. **What is the best mitigation strategy for ransomware attacks?**
   a) Paying up the hackers.
   b) Contacting the police.
   c) Encrypting your data.
   d) Having up-to-date backups of the data.

3. **The use of a fingerprint scanner as an authentication method:**
   a) improves security since there is no password involved.
   b) is inconvenient since it still takes a long time to authenticate a user.
   c) is best connected to other authentication methods such as passwords.
   d) is not reliable enough to be used for authentication

4. **Elevation of privileges is when:**
   a) An intruder logs into a server as a guest and by exploiting a bug is able to change his status to root user.
   b) A company's employee has his account upgraded to administrator status since he now needs to dynamically change the access rights of many users working on a new project
   c) When a new system administrator is hired, his account is created with root status.
   d) An intruder is able to gain inside knowledge about the habits of the system administrators of a company.

5. **A hacker is able to gain a user's credentials (login and password) by pretending to be this user's partner on the phone speaking with a customer relations representative of a telecom operator. This type of attack is called:**
   a) Credentials theft
   b) Man-in-the-middle
   c) Node flooding
   d) Social engineering

6. **Diffie-Hellmann is an algorithm designed to:**
   a) Encrypt blocks of data
   b) Authenticate an user
   c) Elevate privileges
   d) Exchange cryptographic keys

7. **If a cryptographic algorithm uses a random 100-bit key, what is the maximum number of brute-force tries that a hacker must attempt to break the scheme?**
   a) 2^{100}
   b) 100
   c) $\log_{10}100$
   d) $\sqrt{100}$

8. **You receive an email saying your LiU email account is full, and it asks you to click on a link to log in to get more space. The email does not address you by your name, merely beginning with "Dear student". What type of attack is this?**
   a) Phishing
   b) Clipping
   c) Whaling
   d) Hooking

9. **When is an SQL injection attack possible?**
   a) When several SQL queries are joined together in a single line.
   b) When comment strings are used in SQL queries to ignore certain commands.
   c) When no antivirus software is running on the SQL server.
   d) When user input to the SQL database is unfiltered.

10. **What is the type of attack when a malicious script is embedded onto the comment page of a website?**

a) Script injection
b) Cross-site scripting
c) Denial-of-service
d) Website defacing

11. **The steps needed, in the order written below, to establish a "secure tunnel" between a client-server are:**
a) Clock synchronization, establishment of symmetric key pairs, encryption using an asymmetric cipher.
b) Verification of credentials, authentication through asymmetric key exchange, encryption using a symmetric cipher.
c) Authentication through asymmetric key exchange, establishment of symmetric key pairs, encryption using a symmetric cipher.
d) Establishment of symmetric key pairs, authentication through asymmetric key exchange, encryption using an asymmetric cipher.

12. **What is DNS cache poisoning?**
a) When IP addresses are changed at a DNS server.
b) When a DNS server's memory is corrupted.
c) When an intruder can obtain root level access at a DNS server.
d) When malware is injected onto a DNS server.

13. **In IPsec tunnel mode:**
a) It cannot be run within nested tunnels.
b) Only the payload of the original IP address is encrypted.
c) The packets do not need to arrive in order.
d) The entire original IP address is encrypted (including the original header).

14. **When you browse a new website you need to agree that your data will be collected in order to be able to continue. This was implemented recently in the EU, and it is due to:**
a) Stop Online Piracy Act
b) General Data Protection Regulation
c) The Information Security Act
d) Data Confidentiality Directive

15. **As the IT security manager of a company, it is good practice to...**
a) Develop your own custom encryption scheme
b) Only implement software patches every 6 months, irrespectively of patch release schedule, since that allows for better workflow within the company.
c) Do not allow users to choose their own passwords, and change them every week.
d) Write a security policy together with other departments and make it known to every employee.

16. **Your company loses on average 30.000 kr per year of losses due to employee machines being taken over by malware, coming from spam emails. The implementation of spam filters on the email server will cost 40.000 kr to install. On average, 0.1% of the spam emails will still get through the filter. Assume the losses per spam email are evenly distributed. Mark the most reasonable option:**

a) Implement the server, and do nothing else.
b) Do nothing, since the problem is unlikely to go away as some spam always passes through the filter.
c) Do nothing, since the up-front cost is expensive.
d) Implement the server, and implement a simple awareness program (yearly cost 1.000 kr) for the employees to stop them clicking on suspicious links on emails that pass through the filter.

17. **A Message Authentication Code is designed to ensure the following property of an information block:**
a) Assurance
b) Confidentiality
c) Integrity
d) Availability

18. **The RSA encryption scheme employs:**
a) Two identical keys.
b) One key as long as the plaintext.
c) One private key and one public key.
d) Three keys, of which two are public and one private.

19. **By exploiting a buffer overrun, a hacker is able to get access to the customer database of a online bookstore. This attack's main damage type is:**
a) Confidentiality
b) Integrity
c) Availability
d) Assurance

20. **A server in a network is targeted by multiple SYN flood attacks and is unable to respond to legitimate request from other users. This attack's main damage type is:**
a) Confidentiality
b) Integrity
c) Availability
d) Assurance

21. **What is the main problem when a user "A" can delegate access permissions to other users?**
a) It is not a problem since user "A" can only delegate new access rights in mandatory access control.
b) It is not a problem, since it is assumed that the users that gained new access rights are trustworthy.
c) If user "A" gains new access rights, this is not automatically passed along to the other users.
d) If user "A" loses his access rights, the previously delegated permissions are not automatically revoked.

22. **Which of the examples below best matches the Biba security model:**
a) System configuration files cannot be read by guest users.

b) Cookies should be stored safely.
c) The browser can run Javascript.
d) Downloaded executable files cannot be run without an administrator's permission.

23. **In a database the following alternative is true:**
a) Confidential information may be derived from non-confidential data.
b) One cannot make inferences from the data.
c) It is more efficient to have a single table with all the data.
d) Database security has the same challenges as standard file security.

24. **One technique that Digital Rights Management employs to avoid unauthorized distribution of content is:**
a) Real-time dynamic compression
b) Forward error correcting codes
c) Encryption
d) Symmetric key distribution

25. **In cryptography Kerchkoff's principle states that:**
a) A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
b) A cryptosystem should be secure even if everything about the system, except the key, is private knowledge.
c) A cryptosystem is not secure when everything about the system, except the key, is public knowledge.
d) A cryptosystem is not secure when everything about the system, except the key, is private knowledge.

26. **The following is true about Salting:**
a) The password is inverted after hashing.
b) Salting appends extra random bits to the plaintext password before hashing.
c) Given the extra processing power required when salting a password, it is only recommended in very specific applications.
d) If salting adds an extra N bits to the password, the size of the dictionary table increases by N^2.

27. **A trusted key distribution center is most useful when:**
a) keys need to be transmitted over long distances
b) many keys need to be generated simultaneously
c) As a reliable way to authenticate remote parties
d) To minimize the chance of cross-site forgery attacks.

28. **A Kerberos realm has only one:**
a) Authorization server
b) Service.
c) Authentication server.
d) Administrator.

29. **Replay attacks are greatly mitigated when:**
a) Timestamps are added to the exchanged messages.

b) Messages are sent to random destinations.
c) The party initiating the session always uses the same handshake.
d) Each message has a different length.

30. **It is very important that X.509 certificates are:**
a) As short as possible to save bandwidth.
b) Privately stored, such that no one without proper credentials can see their contents.
c) Digitally signed to ensure authenticity.
d) Frequently updated, to randomly change their contents, minimizing the chance they are copied.

31. **An employee is able to exploit his internal knowledge at the company he works in order to gain admin access. He then uses that to change employee records in order to modify the number of worked hours in the month for some employees. This type of attack's main damage type is:**
a) Confidentiality
b) Integrity
c) Availability
d) Assurance

32. **Non-repudiation is the:**
a) Avoidance of packet collisions in a network.
b) Inability to deny issuing a statement.
c) Memory protection against corruption
d) Redundancy of communication links.

33. **A particular threat is realized on a system by two vulnerabilities in series. To cancel the threat it is enough to:**
a) Download the latest patch to the system.
b) Remove both vulnerabilities.
c) Remove only one of the vulnerabilities.
d) Implement a firewall on the inbound/outbound traffic.

34. **Out of the options below, the best strategy that a user can do to avoid having his password cracked is:**
a) Use a long word with two numbers added to the end.
b) Use a word from a foreign language.
c) Use short and easy to remember passwords and change them frequently.
d) Use a long and truly random password.

35. **The following measure *does not* mitigate social engineering attacks:**
a) Have a clear security policy known by all employees.
b) Make employees educated through awareness programs.
c) Keep software up-to-date.
d) Employ technological tools such as authentication.

36. **In modern commercial aircraft, the configuration files for critical systems (i.e. engines, avionics, etc...) must not be accessed by a passenger using the in-flight entertainment system. This is an example of the following**

model:
a) Biba
b) Bell-LaPadula
c) Kaminsky
d) Kerchkoff

37. **In modern encryption systems the component that is the most vulnerable, and thus needs special attention in practical implementations is:**
a) The encryption module.
b) The decryption module.
c) The key.
d) The certificate.

38. **One major weakness in a Kerberos system is:**
a) Time of check to time of use.
b) Replay attacks.
c) Its implementation as a ring network.
d) Multiple points of entry.

39. **A correct general statement about computer security is:**
a) You can always assume that if the software patch update schedule is up-to-date, no attacks will be successful.
b) At some point an attack will pass through your defenses and you need to have mitigation strategies in place.
c) You can always trust your employees completely if a proper user awareness program is in place.
d) You should always implement security measures irrespectively of cost.

40. **Non-repudiation can be ensured by:**
a) Digital signatures.
b) Adding parity bits to the data packets.
c) Sending the packets through multiple routes in the network.
d) Only accept the data packets that arrive in order.

Solutions

1. d)
2. d)
3. c)
4. a)
5. d)
6. d)
7. a)
8. a)
9. d)
10. b)
11. c)
12. a)
13. d)
14. b)
15. d)
16. a)
17. c)
18. c)
19. a)
20. c)
21. d)
22. d)
23. a)
24. c)
25. a)
26. b)
27. c)
28. c)

29. a)
30. c)
31. b)
32. b)
33. c)
34. d)
35. c)
36. a)
37. c)
38. a)
39. b)
40. a)