TTM4135 Informasjonssikkerhet eksamen --- løsningsforslag

Answers to multiple choice questions

**Evaluation rules**

Category *"Check the one statement that applies":* 1 weight point is assigned if and only if the correct statement is selected and the two incorrect choices are left blank, else 0 point is assigned.

Category *"Check all statements that apply".* 1 weight point is assigned if and only if all the correct statements are selected and all of the incorrect choices are left blank, else 0 point is assigned.

Category *"True or False".* 1 weight point is assigned if and only if the correct truth value is selected and the negation is left blank, else 0 point is assigned.

| *Question* | *Choice* | | |
|---|---|---|---|
| | A | B | C |
| 1 | | ✘ | |
| 2 | ✘ | | |
| 3 | ✘ | | |
| 4 | | ✘ | |
| 5 | ✘ | | ✘ |
| 6 | ✘ | ✘ | |
| 7 | ✘ | | ✘ |
| 8 | ✘ | ✘ | ✘ |
| 9 | ✘ | ✘ | |

| | True | False |
|---|---|---|
| 10 | | ✘ |
| 11 | | ✘ |
| 12 | ✘ | |

| | A | B | C |
|---|---|---|---|
| 13 | ✘ | | |
| 14 | ✘ | ✘ | ✘ |
| 15 | | | ✘ |
| 16 | ✘ | | |

Some remarks to multiple choice questions:
2. B: digital certificate is false. C: URL address is false.
3. B: encryption will not produce executable code. C: Any code is visible in the executable object file.
5. B: Replay attack is not DOS attack, because its goal is acceptance by receiver, not traffic increase.
6. B: Read the Greek mythology about KERBEROS the fierce watchdog of Hades. It was depicted as a three-headed dog with a serpent's tail, a mane of snakes, and a lion's claws.C: Kerberos system does not use public-key(, nor the hound of Hades).
7. B: Compression is an important part of PGP.
9. All text is copy from http://www.datatilsynet.no English page, but C replaces "public" with "private".
10. Many viruses hide themselves in scripts that are part of the message.
11. Of course you do, in general, a modem line is just another link connection for TCP/IP.
12. They try to do it daily. Get Ad-Aware to root out spyware: www.lavasoftusa.com.
15. You knew this already, of course, it is always the others that are ignorant ;-)
16. B: Too farfetched and idealistic. C: "Attraction", active provocation of criminal acts is itself illegal and probably not acceptable as legal evidence.

17. Two important SSL concepts are the SSL session and the SSL connection.
An SSL connection is a transport layer peer-to-peer service. Every connection is associated with one communication session.
An SSL session is a client-server association established by the Handshake Protocol. The session defines security parameters that can be used in several SSL connections.

18. SSL threats and countermeasures:

1) Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
   SSL protection by using secure symmetric ciphers with key lengths of at least 128 bits and up.
2) Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against the full ciphertext to determine the right one. This attack is especially effective

against small key sizes (E.g. 40-bit keys).
SSL protection by using secure symmetric ciphers with key lengths of at least 128 bits and up.

3) Replay Attack: Intercepted SSL messages are replayed.
SSL protection by use of randomized parameters ("nonces").
4) Man-in-the-Middle Attack: An attacker acting both as client to the server and as server to the client.
SSL protection by authentication based on digital certificates and shared secret keys.
5) Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.
SSL protection by encryption.
6) IP spoofing: Using forged IP addresses to get the receiver into accepting bogus data.
SSL protection is by providing a secure (authentic and encrypted) channel between client and server.
7) IP Hijacking: An active, authenticated connection between client and server is disrupted and the attacker takes the place of one of them.
SSL protection is the same as previous (item 6).
8) SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the "half-open connection" around for a few minutes. Repeated SYN messages can clog the TCP module.
SSL protocol design does not protect against this denial-of-service attack.

19. A firewall should realize the requirements of the reference monitor concept, both for incoming and outgoing traffic.

1. Complete mediation of access, that is, all communication between "inside" and "outside" must pass through the firewall.

2. Correct and complete operation, that is, only communication authorized by the security policy is allowed.

3. Integrity, that is, the firewall itself must be protected against unauthorized modification.

20. The system comprises Registration Authority (RA), Certificate Authority (CA), Validation Authority (VA), and Signature Authority (SA), and the user clients and servers of the system.
A digital certificate on a user's public keys is requested to the RA, signed by the SA, stored and provided on request by the CA, and state of certificate validity can be verified by querying the VA. Only SA (the most critical entity storing the private key of the certificate authority) can modify a certificate, that is, carry out a signature using the stored private key.

21.

1) See figure 3.11 page 77

2) Y_A = 2^8 mod 13 = 9, hence X_A = 8
3) Y_B = 2^4 mod 13 = 3, hence K= 9^4 mod 13 = 3^8 mod 13 = 9

22.

1) Let the block be divided in a left half L and right half R, and the round key is K. $R_2 = L_1$ xor $F(R_1,K) = L_1$ xor $F(L_2,K)$ implies $L_1 = R_2$ xor $F(L_2,K)$. Hence a Feistel function is its own inverse (involution).

2) The result in item 1) suggests that we can replace the one-way "round" function $F(R,K)$ with a one-way hash function $H(R,K)$ adapted to appropriate length of input and output. For DES, $F(R,K)$) maps a 32-bit R and a 48-bit K into a 32-bit output.