Instituto Superior de Engenharia de Lisboa

Departmental Area of Electronics and Telecommunications and Computer Engineering

MEIC/MEET/MRCM/LERCM - Security in Computer Networks - 6/15/2016 - 2nd test

Name:_____; Number _ _ _ _ _ _

Professor: João Ferreira ☐ Vitor Almeida ☐ **Course**: LERCM ☐ MEIC ☐ MEET ☐ ☐ MERCM

In multiple response check with a V or a T (true) or a F (false) or do not put anything (it doesn't count ou discount).

1) [PPTP] Consider the PPTP Protocol:

☐☐1.1) The PPP data channel corresponds to a GRE over IP channel #

☐☐1.2) The PPP control channel uses the UDP transport protocol

☐☐1.3) To ensure confidentiality using encryption of PPP protocols

☐☐1.4) PPTP encapsulates PPP frames replacing the PPP headers by a PPTP header

☐☐1.5) For each PPTP message there is only one IP header, the one from the IP packet that carries it

2) [PPTP] PPTP:

☐☐1.6) PPTP provides a 2-level (OSI model) service #

☐☐1.7) A DoS attack can be accomplished by attacking TCP that transports the signaling

☐☐1.8) The reason for the creation of the PPTP was the need to extend the PPP between two points belonging to different IP networks #

☐☐1.9) PPTP is dependent on the use over IP, only #

3) [PPTP/L2TP] The main difference between PPTP and L2TP is:

☐☐1.10) PPTP uses PPP and L2TP does not

☐☐1.11) The security provided by L2TP is superior to the one provided by PPTP

☐☐1.12) L2TP provides a level 2 service (OSI model) and PPTP a level 3

☐☐1.13) L2TP can run over several network protocols (Frame Relay, UDP/IP, ...) and PPTP doesn't V

4) [IPSec] You intend to create a VPN that allows avoiding traffic analysis using IPSec you would choose:

☐☐1.14) ESP with encryption

☐☐1.15) Tunnel Mode #

☐☐1.16) Transport Mode

☐☐1.17) Random sequence numbers

☐☐1.18) Security Parameters Index encrypted

☐☐1.19) ESP with authentication instead of AH

5) [IPSec] In which of the following IPSec modes the original IP packet header (at the entrance of IPSec) is encrypted:

☐☐1.20) AH tunnel mode

☐☐1.21) ESP in tunnel mode #

☐☐1.22) AH in transport mode

☐☐1.23) ESP in transport mode

6) [IPSec] IPSec resists attacks by repetition using:

☐☐1.24) Sequence number in the *header* AH #

☐☐1.25) Sequence number in the *header* ESP #

☐☐1.26) Use the command "no direct broadcast" in the routers of the networks that use IPSec

☐☐1.27) Encrypting the Identifier field in the header of the IP datagram

7) [IPSec] In IPSec the protection against replay attacks is optional and is based on:

☐☐1.28) Use of the 64-bit sequence number instead of 32 bits

☐☐1.29) Renegotiation of a new SA when the counter "gives back" #

☐☐1.30) Use of confidentiality in ESP mode

☐☐1.31) Joint use of protocols AH and ESP

☐☐1.32) Using a sliding window #

8) [IPSec] The "authentication data" field exists in the ESP messages when it is used:

☐☐1.33) AH

☐☐1.34) ESP with authentication #

☐☐1.35) ESP with confidentiality

☐☐1.36) ESP with confidentiality and authentication #

☐☐1.37) Never

9) [IPSec] Assume that a reception window in IPSec (AH or ESP) has a dimension of 32 and is in the beginning [0 .. 31]. If a correctly authenticated message arrives with an id = 32 to what values moves the window?

☐☐1.38) [1 .. 32] #

☐☐1.39) [0 .. 31]

☐☐1.40) [0 .. 63]

☐☐1.41) [32 .. 63]

10) [IKEv2] Consider the IKEv2:

☐☐1.42) Requires certificates on the part of both participants in the session

☐☐1.43) The cryptographic algorithms used in SA can be negotiated #

☐☐1.44) The *nonces* exchanged between entities are used in the calculation of the master key #

☐☐1.45) Only IKE SA is required for each IPSec connection between two entities

☐☐1.46) Mutual authentication is performed first and then define the master key

11) 10) [IKEv2] When referring to the "granularity" of the security service we are talking about:

☐☐1.47) Size of IKE messages

☐☐1.48) Size of the IPSec datagrams

☐☐1.49) Definition of what are the characteristics of the IP flows associated with distinct VPNs #

☐☐1.50) Size of the keys used in encryption and authentication algorithms

☐☐1.51) Amount of SAs generated for each VPN support

12) 11) [IKEv2] In IKEv2:

☐☐1.52) All IKEv2 messages exchanged encrypted passwoords

☐☐1.53) The IKEv2 *suites* are in common use with the ones of IPSec

☐☐1.54) IKEv2 does not generate SAs for IPSec

☐☐1.55) All IKEv2 messages exchanged include fields that allow authentication and integrity

☐☐1.56) Mutual authentication in IKEv2 can be performed using digital certificates or pre-shared keys V

13) [IKEv2] Why does the identity of the initiator can be discovered and the answer from the responder is protected from an active attacker?

☐☐1.57) The use of *cookies* safeguards the identity of the responder

☐☐1.58) The identity of the *initiator* passes in an initial message without being encrypted

☐☐1.59) A mutual authentication failure causes that there is no longer the IKE_AUTH message reply from the responder #

☐☐1.60) A MITM attacker can generate sets of keys equal to the *initiator* and the responder and thus gaining access to the contents of all IKE messages

14) [IKEv2] In IKE creating additional child SA implies the exchange of more CREATE_CHILD_SA messages. What is used to create the new keys for these connections if it is not necessary Perfect Forward Secrecy?

☐☐1.61) Digital certificates

☐☐1.62) Traffic selectors

☐☐1.63) Nonces #

☐☐1.64) Diffie-Hellman values

15) [WEP] In WEP using the initialization vector (IV) serves:

☐☐1.65) As different session key for each of the one of the frames

☐☐1.66) To increase and vary the cipher key of each frame #

☐☐1.67) As a sequence number to avoid replay attacks

☐☐1.68) As an index to the session key that is being used

16) [WEP] To provide integrity the WEP uses:

☐☐1.69) HMAC-MD5 of concatenation of the frame with the shared key

☐☐1.70) WEP gives no guarantee of integrity

☐☐1.71) RC4 on the data field of the frame

☐☐1.72) A CRC protected by RC4 #

17) [WEP] The WEP protection of the integrity of the messages is carried out via:

☐☐1.73) CCMP

☐☐1.74) HMAC

☐☐1.75) Encrypted CRC #

☐☐1.76) Hash protected

☐☐1.77) CRC not encrypted

18) [WPA2] WPA2:

☐☐1.78) Uses a CRC to ensure the integrity

☐☐1.79) Does not provide protection against replay attacks

☐☐1.80) Uses the AES as encryption support algorithm #

☐☐1.81) The algorithms for integrity support are based on the RC4

☐☐1.82) Uses the MIC algorithm to ensure authentication and integrity

19) [SSL] The pre master secret may be generated:

☐☐1.83) By the client #

☐☐1.84) By the server

☐☐1.85) For both through DH exchange #

☐☐1.86) Specified through shared secrets manually

20) [SSL] In SSL/TLS the Master Secret:

☐☐1.87) The *Master Secret* never passes on the network V

☐☐1.88) Is generated from the *pre Master Secret* V

☐☐1.89) Is exchanged between client and server through Diffie-Hellman

☐☐1.90) It is exchanged between client and server ciphered with an asymmetric algorithm and asymmetric public key from the server

21) [SMTP] In SMTP CRAM-MD5 AUTH mode means that the login user and password in the connection:

☐☐1.91) Are never sent

☐☐1.92) Both are sent encrypted

☐☐1.93) Only the password is encrypted using the hash, MD5 algorithm, with the challenge received from the server as key

☐☐1.94) The user goes in clear and the *password* goes on a *string* resulting from a *hash* of the *password* with a challenge received from the server V

22) [SMIME] To send an email with guarantee of origin it is necessary that:

☐☐1.95) The receiver has a certificate

☐☐1.96) The issuer is in possession of a certificate #

☐☐1.97) No certificate is necessary because SMTP already ensure source guarantee

☐☐1.98) The transmitter has a copy of the certificate of the receiver

23) [SPF] If you use a Sender Policy Framework (SPF) in the email Server it will:

☐☐1.99) Check in DNS which the is the public key of the sender and server checks the signature of messages received

☐☐1.100) Query DNS to verify that the server that is sending the email message is authorized to do so on behalf of the sender's domain#

☐☐1.101) Requires customers to use SMIME to ensure message authentication

☐☐1.102) Guarantees the confidentiality of messages between email servers

24) [SPF] In a DNS server exists in the following registry: alunos.isel.ipl.pt. 3600 IN TXT "v = spf1 ip4:193.137.220.0/25 ip4:62.48.232.168 -all"

☐☐1.103) Indicates that for the alunos.isel.ipl.pt domain can only be sent email messages from servers at ip4: ip4:193.137.220.0/25 and 62.48.232.168

☐☐1.104) Indicates that the *e-mail* servers that can send mail on behalf of the alunos.isel.ipl.pt domain are the ones with addresses ip4: ip4:193.137.220.0/25 and 62.48.232.168#

☐☐1.105) Indicates who can send *email* from the alunos.isel.ipl.pt domain are only residents in the networks machines with IP addresses 193.137.220.0/25 and 62.48.232.168

☐☐1.106) Indicates to the servers residing on the addresses Ipv4: 193.137.220.0/25 and 62.48.232.168 can only be sent messages whose content is text only

25) [Domain Keys] In Domain Keys how it is retrieved the certificate contains the public key of the issuer?

☐☐1.107) Certification authority (CA) indicated in the DNS server referenced by the source server

☐☐1.108) Domain Keys server resident near the source email server

☐☐1.109) DHCP Server (BOOTP protocol extension)

☐☐1.110) From a DNS server #

☐☐1.111) The public key is always exchanged between the source and destination email servers using x.509v3 certificates, it does not require any specific server for this purpose