1. In cazul retelelor de calculatoare fara fir putem avea:
2. Atacuri pasive
3. Atacuri active
4. Atacuri pasive si active
5. Atacuri topologice
6. Atacul de tip deturnarea sesiunii presupune:
7. Alterarea pachetelor de la punctual de acces la client
8. Copierea adresei MAC a punctului de acces, dezasocierea clientului si transfer de date intre atacator si punctual de acces
9. Oprirea lucrului punctului de acces
10. Stabilirea legaturii intre atacator si client
11. Atacul de tip negarea serviciului (DoS) presupune:
12. Numai oprirea functionarii retelei la nivel fizic
13. Numai impiedicarea accesului statiilor la conexiune la nivelul legatura de date
14. Numai supraincarcarea tabelului de rutare, eliminarea selective de pachete, modificarea pachetelor de …
15. Toate acestea impreuna
16. Atacul de tip om la mijloc presupune:
17. Ca atacatorul devine punct de acces pentru client si client pentru punctual de acces propriuzis
18. Ca atacatorul schimba SSID-ul punctului de acces
19. Ca se creaza o noua celula
20. Ca se extinde celula existenta
21. Protocolul WEP:
22. Foloseste un algoritm diferit pentru mesajul transmis si cel receptionat
23. Nu are camp pentru protejarea impotriva modificarilor neautorizate
24. Cripteaza toate campurile cadrului
25. Nu cripteaza campul IV
26. Identificatorul SSID
27. Este un identificator numai pentru punctul de acces
28. Este un identificator numai pentru client
29. Este un mesaj criptat in cadrele de informare (Beacon)
30. Este un identificator ce ofera posibilitatea de separare logica a retelelor fara fir
31. Autentificarea cu cheie partajata ???????
32. Presupune autentificarea clientului
33. Presupune autentificarea punctului de acces
34. Presupune atat autentificarea punctului de acces cat si a clientului
35. Presupune ca punctual de acces are o baza de date pentru autentificare
36. Vectorul de initializare in cazul protocolului WEP
37. Acest camp se foloseste la calcularea campului ICV
38. Este un camp care nu se adauga la cheia statica, fiind folosit autonom
39. Este un camp folosit optional
40. Este un camp care se adauga la cheia statica
41. Standardul de autentificare 802.1x
42. Este un standard bazat pe porturi si server de autentificare
43. Este un standard bazat numai pe porturi
44. Este un standard bazat numai pe serverul de autentificare
45. Este un standard bazat pe autentificarea dispozitivelor
46. Protocolul EAP foloseste
47. Foloseste numai pachete la nivel inferior EAPOL
48. Foloseste numai pachete la nivel aplicatie RADIUS
49. Foloseste ambele tipuri de pachete
50. Acest protocol se foloseste numai de catre retelele fara fir
51. Protocolul de autentificare EAP-MD5
52. Este un protocol bazat pe o autoritate de certificare
53. Protejaza schimbul de mesaje prin crearea unei amprente unice cu care semneaza digital
54. Foloseste certificate PKI
55. Permite eliminarea atacurilor de tip om interpus
56. Protocolul extins de autentificare cu securitate la nivel transport (EAP-TLS)
57. Este un protocol care se bazeaza pe certificate PKI solicitand ca atat serverul cat si clientul… CORECTAT
58. Nu realizeaza autentificare mutuala
59. Nu se bazeaza pe certificate X.509
60. Se bazeaza pe autentificarea prin nume utilizator si parola
61. Protocolul extins si protejat de autentificare (PEAP)
62. Asigura autentificarea pe baza de nume\_utilizator si parola
63. Nu ofera suport pentru autentificarea mutuala
64. Clientul PEAP se autentifica direct la serverul de autentificare
65. Nu are suport pentru fragmentare
66. Protocolul WPA
67. Foloseste criptarea bazata pe WEP
68. Realizeaza confidentialitatea folosind protocolul TKIP
69. Asigura integritatea mesajelor folosind ICV
70. Are un vector de initializare ca si WEP
71. Protocolul de intergritate cu cheie temporara TKIP
72. Foloseste mixarea cheilor intr-o singura faza
73. Nu foloseste un numarator de secventa
74. Foloseste ca si cod de integritate a mesajelor codul MIC
75. Cripteaza intreg cadrul MPDU, inclusiv antetul
76. Codul de integritate al mesajului MIC
77. Foloseste acelasi cadru ca si protocolul WEP
78. Foloseste un cadru cu numere de secventa
79. In calculul MIC nu intra adresele MAC sursa si destinatie
80. Foloseste pentru calcul numai datele cadrului
81. Protocolul 802.11i
82. Nu realizeaza un serviciu robust de securitate
83. Foloseste pentru criptare numai protocolul AES
84. Nu are posibilitatea de a realiza o autentificare mutuala
85. Se folosesc aceleasi chei indiferent de timpul transmisiei
86. Managementul cheilor in cadrul standardului 802.11i este realizat
87. Numai printr-o cheie pereche
88. In cadrul dialogului in patru faze
89. Numai printr-o cheie prepartajata
90. Numai printr-o cheie de grup
91. Protocolul CCM(CCMP)
92. Foloseste algoritmul RC4
93. Foloseste AES
94. Cripteaza intregul cadru CCMP
95. Foloseste un antet format numai din numarul pachetului curent
96. Autentificarea SIM ?????
97. Foloseste carduri SIM pentru serviciul RADIUS
98. Nu foloseste o cheie partajata cunoscuta de SIM si centrul de autentificare GSM
99. Algoritmii de autentificare si criptare sunt stocati in serverul RADIUS
100. Asigura o autentificare mutuala intre client si un server AAA
101. Protocolul de autentificare LEAP
102. Realizeaza o autentificare mutuala
103. Folloseste certificate PKI
104. Este un protocol neproprietar
105. Foloseste pentru autentificare module SIM
106. Autentificarea MAC
107. Presupune verificarea de catre client a adresei MAC a punctului de acces
108. Presupune verificarea de catre punctual de acces a adresei MAC a clientului
109. Presupune ambele verificari, adica a adresei MAC a punctului de acces si a clientului
110. Presupune folosirea unui protocol EAP pentru verificarea adreselor MAC
111. In autentificarea folosind protocolul EAP portul necontrolat este
112. Un port care permite numai transmiterea mesajelor de autentificare
113. Un port care permite transmiterea si a celorlalte date
114. Un port deschis numai la terminarea sesiunii de lucru
115. Un port care este folosit numai de catre datele ce reprezinta adrese MAC
116. Protejarea impotriva atacului de negarea serviciului se face
117. Necesita autentificarea reciproca de la un capat la altul
118. Se indreapta antenele directionale spre exteriorul cladirii
119. Se realizeaza ocuparea canalelor de transmisie
120. Utilizarea nodului victimei ca nod intermediar pentru retransmiterea continua de pachete de date inutile
121. Punctele de acces stand-alone
122. Au un management centralizat pentru puterea si frecventele de emisie
123. Au costuri mari de achizitie, instalare si exploatare
124. Pot functiona de sine statatoare, aigurand autentificarea, securitatea si managementul intr-o singura unitate
125. Nu sunt indicate pentru firmele mici si medii
126. Regenerarea cheilor de criptare la interval specificate
127. Asigura o transmisiune fara erori
128. Este o metodologie ce nu necesita servere RADIUS
129. Asigura un management mai simplu al securitatii retelei
130. Asigura o confidentialitate sporita a datelor
131. Gruparea in domenii de lucru a retelelor fara fir ?????
132. Presupune crearea de celule numai la nivel de departament
133. Presupune un serviciu fara fir cu acelasi SSID ??
134. Presupune crearea de celule numai dupa acelasi tip de punct de acces
135. Presupune crearea de celule numai dupa acelasi tip de client
136. Sistemul de autentificare RADIUS
137. Foloseste numai servere cu baze de date centralizate
138. Foloseste numai servere cu baze de date distribuite
139. Foloseste numai servere cu baze de date legate intre ele
140. Foloseste servere cu baze de date distribuite sau centralizate
141. Dispozitivele de monitorizare a traficului la nivelul legaturii de date
142. Pot fi contracarate prin criptarea datelor transmise
143. Pot fi contracarate prin analizarea desfasurarii traficului
144. Pot fi contracarate prin folosirea de servere puternice
145. Pot fi contracarate prin folosirea de canale nesuprapuse
146. Protejarea impotriva atacurilor de tip punct de acces fals
147. Se realizeaza prin folosirea de viteze de lucru mari
148. Se realizeaza prin folosirea de autentificari mutuale
149. Se realizeaza prin folosirea de puncte de acces multisystem
150. Se realizeaza prin folosirea de celule pe domenii