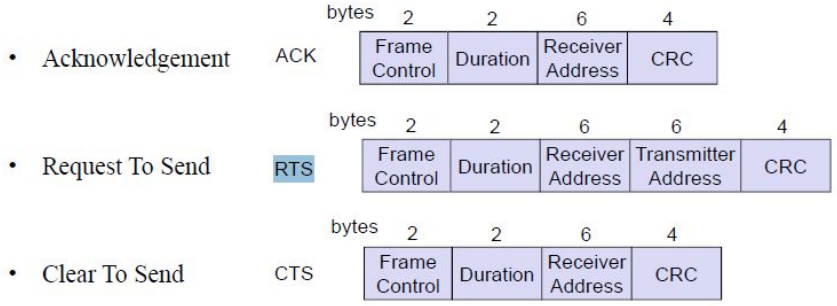
1. **Ramki RTS/CTS:**
   a. **wspieraja dzialanie mechanizmu Wektora Alokacji Sieci NAV (Network Alocation Vector)**
   b. **zawieraja FCS**
   c. dla przyspieszenia procesu rezerwacji kanału są nadawane z maksymalną dostępną szybkością transmisji - chyba są nadawane z najmniejszą prędkością dla kompatybilności - ktoś potwierdzi? // potwierdzam mam zapisane z wykładu, że RTS i CTS są transmitowane z 1 Mbit/s, są na bank nadawane z najniższą szybkością
   d. są równej długości RTS dłuższy



2. Jaki profil standardu Bluetooth jest używany do zapewnienia komunikacji między komputerem PC i klawiaturą lub myszką
   a. DUN - profil dostępu do sieci stosowany jest przez komputer do uzyskania komputerowego dostępu do Internetu poprzez telefon komórkowy lub modem
   b. **HID**
   c. OPP - profil przesyłania obiektów, np. wizytówek biznesowych
   d. HFP - opisuje, jak urządzenie bramy wejściowej może być użyte do wykonywania i odbierania rozmów poprzez urządzenie niewymagające używania rąk.

3. Metoda wstrzykiwania pakietów do AP w celu złamania hasła zaszyfrowanego algorytmem WEP
   a. **jest możliwa w przypadku uwierzytelniania z użyciem współdzielonego klucza (Shared Key Authentication)**
   b. **wymaga przejścia stacji w tryb Monitor** //Packet injection means sending data while in Monitor mode because it's a passive-only mode
   c. wymaga wcześniejszego przyłączenia się do punktu dostępu
   d. zawsze wymaga zmiany adresu MAC w celu podszycia się pod inną stację

4. Algorytm Wired Equivalent Privacy (WEP)
   a. **umożliwia użycie kluczy użytkownika o stałej długości równej 40 i 104 bity**
   b. podczas szyfrowania 128-bitowego stosuje zmienną długość klucza RC4
   c. **szyfruje tekst jawny przy pomocy operacji XOR ze strumieniem klucza**
   d. długość klucza użytkownika zawsze wynosi 48 bitów dla klucza RC4 o rozmiarze 64 bity //wynosi 40 bitów dla klucza RC4 o rozmiarze 64 bity

5. Parametr RTS Threshold pozwalając uruchomić mechanizm RTS/CTS w sieciach ad-hoc w przypadku dużej liczby stacji działających w stanie nasycenia

a. po ustawieniu na dużą wartość zmniejsza wydajność pracy sieci gdy przesyłane są (Głównie) bardzo krótkie ramki danych - to chyba też fałsz nie? choć bym się z tym wstrzymał, zależy od warunków
b. powoduje podział ramek większych niż wartość parametru na mniejsze fragmenty transmitowane osobno - to by był frag treshold w, RTS threshold nie dzieli żadnych ramek
c. poprzez ustawienie na wartość niższą niż rozmiar transmitowanych ramek danych pozwala zmniejszyć czas zajętości kanału przez transmisję ramek kontrolnych
d. powoduje stosowanie wstępnej rezerwacji kanału radiowego dla wszystkich ramek większych niż wartość parametru wszystkie ramki większe niż RTS_Threshold podlegają wysyłaniu RTS/CTS

6. Uruchomienie maskarady IP/NATa na kliencie sieci WLAN umożliwia:
a. planowanie, śledzenie i zarządzanie przestrzenią adresów IP używanych w sieci komputerowej - chyba fałsz co sądzicie // ja bym powiedział, że fałsz bo mi to śledzenie i planowanie nie pasuje // jak na brzegu sieci zmieniamy IP no to po śledzeniu chyba // fałsz 100 pro
b. zmianę źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu przez to urządzenie
c. uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci - to jest DHCP
d. zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową

7. Narzędzie do badania wydajności pracy sieci iperf:
a. straty pakietów tcp - fałsz, w TCP nie ma strat, będą retransmisje
b. straty pakietów udp
c. pomiar opóźnień pomiędzy stacją nadawczą a odbiorczą (a nie false, bo mierzy jitter dla UDP tylko, a to jest wahanie się opóźnień a nie same opóźnienia?) to w takim razie dopyta sie już o to na kolosie o co im chodziło
d. pracuje w konfiguracji o p2p
e. pracuje w trybie klient serwer
f. pozwala na analizę wydajności pracy sieci WLAN z użyciem protokołów TCP/UDP
g. klient może zestawić kilka sesji połączeń
h. pozwala na pomiar strat pakietów między stacją nadawczą i odbiorczą z użyciem protokołu…
i. pozwala na pomiar jittera między stacją nadawczą i odbiorczą

8. Oprogramowanie Kismet
a. PASYWNIE wykrywa sieci WLAN
b. pozwala wysyłać deauthentication
c. aktywnie wykrywa sieci, wysyłając do AP i wymuszając odesłanie info o SSID
d. potrafi wykryć sieci WLAN z ukrytym SSID

9. Wymień warstwy standardu Bluetooth

a. **L2CAP** *na wykładzie z bluetooth na slajdzie 16 jest L2CA*
b. mac
c. **RFCOMM**
d. LLC

10. Pole adresowe SOURCE w nagłówku ramki WLAN

a. Nie może zawierać adresu przewodowego interfejsu sieciowego (ethernet) (może jak komputer jest podpięty kablem do AP, to wtedy source jest adresem karty Ethernetowej kompa a transmitter address MAC'iem AP)
b. informuje o adresie IP nadawcy ramki **informuje o adresie MAC nadawcy ramki**
c. zawsze zawiera informacje o adresie interfejsu bezprzewodowego transmitującego ramkę (to byłby transmiter address)
d. ma zawsze rozmiar 6B
e. może być to adres rozgłoszeniowy
f. może zostać podmieniony *ale tylko w przypadku ataku, w normalnej pracy sieci nie*

11. Ktora odmiana protokołu EAP zapewnia najwyższy poziom bezpieczeństwa?

a. EAP-MD5
b. EAP-TLS
c. PEAP
d. LEAP

12. Symulator Riverbed należy do grupy symulatorów

a. zdarzeń dyskretnych
b. z czasem dyskretnym
https://www.riverbed.com/pl/products/steelcentral/steelcentral-riverbed-modeler.html
c. **z czasem ciągłym** - ja bym powiedział, że czas ciągły, bo daje lepsze wyniki w google niż dyskretny :D ktoś pamięta jak Prasnal/Natkaniec mówił, że symulacje w tym symulatorze trwają krócej, bo pomijamy okresy, kiedy nic się nie dzieje w sieci? to chyba będzie czas dyskretny
d. https://www.google.pl/search?q=continuous+time+site:riverbed.com
e. zdarzeń synchronicznych

13. W symulatorze Riverbed można tworzyć sieci

a. o topologii gwiazdy (czy tam innej rozgwiazdy - nie pamiętam dokładnie)
b. kratowe(mesh)
c. w standardzie 802.11ac
d. w standardzie 802.11a
e. ad-hoc

z instrukcji : a/n/c/e g? a nie tylko 802.11 a, e, n? tyle jest w instrukcji, TO WAŻNE

14. Oprogramowanie crunch stosowane przy łamaniu WPA2 umożliwia

a. łamanie klucza wpa2 poprzez bruteforce
b. przestawienie interfejsu WLAN w tryb monitor
c. łamanie WPA2 poprzez zastosowanie algorytmu wyznaczającego klucz na podstawie statystyk zebranych z zrzutu atakowanej sieci

d. **utworzenie dowolnego słownika z określonego zestawu znaków**
e. **łamanie klucza WPA2 poprzez podstawianie kolejnych haseł słownikowych**

15. Czym roznia sie protokoly EAP-MD5 I PEAP

a. nie ma roznic odnosnie formatu przesylanych pakietow
b. PEAP ma wyższy poziom bezpieczeństwa dzięki szyfrowaniu WPA2, podczas gdy EAP-MD5 korzysta z WPA
c. **PEAP nie jest podatny na ataki MITM, EAP-MD5 jest podatny**
d. PEAP ma wyższy poziom bezpieczeństwa dzięki szyfrowaniu WPA, EAP-MD5 korzysta z WPA2
e. **W EAP-MD5 hasło i login przesyłane są z wykorzystaniem funkcji skrótu, a w PEAP za pomocą szyfrowanej transmisji SSL**
f. PEAP ma wyższy poziom bezpieczeństwa dzięki szyfrowaniu WPA, podczas gdy EAP-MD5 korzysta z WEP

//PEAP może korzystać z WPA LUB WPA2 a EAP-MD5 tylko hashuje to i tyle.

16. Tryb ad-hoc w 802.11

a. **pozwala rozgłaszać SSID sieci** - co więcej w sieciach ad-hoc zawsze się rozgłasza SSID
b. pozwala na stosowanie wylacznie kanałów o szerokosci 20MHz - potwierdzone info, w 5Ghz masz kanały 20/40/80/160 Mhz. // nie doczytałem, ze chodzi o adhoc // wg en wiki 802.11 ax ad-hoc może mieć 80 Mhz kanał.
c. **nie wymaga obecnosci punktu dostepowego**
d. **jest inaczej nazywany IBSS**
e. **w standardzie 802.11ac pozwala rozgłaszać kanały 80MHz**

17. Basic rate służy do

a. transmisji broadcast i multicast
b. **transmisji ramek sterowania**
c. **kompatybilności wstecznej**
d. jedna z wartości przesyłania danych w 802.11c ??
e. **nadawania ramek zarządzających**
f. nadawania ramek danych zgodnych ze standardem IEEE 802.11g
g. **uzyskania kompatybilności współpracy ze wszystkimi "starszymi" urządzeniami standardu IEEE 802...**

19. Dla topologii gdzie jest 1000 stacji które coś tam robią i jest CWmax jakieś tam (czyli to co mieliśmy w Riverbedzie na jednym z labów) optymalna wartość CWmin to:

a. jakaś liczba
b. 64
c. jakaś liczba
d. **1023** - z doców z zeszłych lat wiadomo xD, to jest na 100% pewne, symulowaliśmy to i odgrzebałem doca z wynikami symulacji - 1023 dla nasyconej, ~64 dla nienasyconej

20. Z RADIUS korzystają

a. iperf
b. tacacs
c. **RADIUS**
d. diameter
e. tacacs+

Mają tylko tę wspólną cechę, że są serwerami AAA

21. Aby złamać WEP należy

a. zebrać odpowiednia liczbę pakietów z tym samym IV
b. **zebrać dużo pakietów różniących się wektorem inicjalizacyjnym IV**

~WIKI~Wstrzykiwanie pakietów - Odzyskanie hasła WEP wymaga przechwycenia odpowiednio dużej liczby pakietów z unikatowymi IV. ←- z sekuraka

22. Port logiczny 802.1X dla sieci 802.11:

a) port wydzielony w AP do komunikacji klienta z serwerem RADIUS
b) port do przesyłania komunikatów e-poll request i e-poll response
c) asocjacja klienta z serwerem RADIUS do uwierzytelnienia
d) …

23. Iptables to:

a) framework jądra Linux do zmiany ustawień czegoś
b) aplikacja w systemie Linux do monitorowania sieci (czy coś)
c) program w systemie Linux do ustawiania reguł sieciowych, NAT
d) moduł jądra Linux do …

24. WDS Repeater:

a) **sprawdza pole FCS**//zmieniając adres pasowałoby policzyć nowe FCS- ok, ale czy sprawdza najpierw czy jest ok? No inaczej tym bardziej nie byłoby sensu. przesyłać coś na pałę? o WDS repeater....still…
b) tworzy nowy nagłówek warstwy fizycznej // chyba tylko podmienia adres, po co tworzyć nowy nagłówek?
c) odtwarza nagłówek warstwy fizycznej to by było przy regeneratorze
d) **modyfikuje pola adresu w nagłówku MAC** tak wychodzi ze strony dd-wrt, potwierdzone jakimś pieprzonym konfigiem sieci.
e) Wymaga szyfrowanego połączenia

25. Polecenie: "*iptables -I INPUT -i br1 -p udp --dport 53 -j ACCEPT*"

***a.* Włączenie możliwości br1 połączenia się z portem 53 na ruterze (DNS) przez UDP**

a. zapewnienie dostępu br1 z uzyciem pakietów UDP do DNS na routerze
b. blokadę komunikacji dwukierunkowej br1 z br0
c. limit prędkości pobierania dla mostu br1
d. zapewnienie możliwości konfiguracji routera z użyciem pakietów TCP dla interfejsów przypisanych

26. EAP MD5 i PEAP

a) różnią się warstwami w komunikacji pomiędzy przełącznikiem a RADIUSem -NIEPOTWIERDZONE
b) EAP MD5 jest haszowany tylko username i password a w PEAPie wszystko certyfikatem
c) pole Vendor specific znajduje się w PEAPie - TEŻ NIEPOTWIERDZONE

27.Maksymalna moc w Bluetooth:

a) 100 mW
b) 10 mW
c) ? dBm
d) 20 dBm

28. Co zwiększa zasięg wifi?

a) Dodanie anten. // zmiana na lepsze, owszem // tu chyba True?//samo dodanie nic nie da chyba ze dodasz anteny mocniejsze // nie umiesz czytac ty “tu chyba True” ? // tu chyba true
b) WDS
c) Regeneracja
d) AP na kablu

29. Które są wspierane z 802.11:

a) EAP FAST
b) EAP TLS
c) EAP TTLS
d) EAP MD5*

30. Jaka jest modulacja w Bluetooth?

a) 16QAM
b) BPSK
c) GFSK
d) 8DPSK
e) pi/4DQPSK

What kind of modulations use 802.11 and Bluetooth devices?
-System wykorzystuje modulacje FSK (Frequency Shift Keying), dając prędkości transmisji 1 Mbit/s, jednak duża cześć tego widma jest zajęta przez nagłówek. Aby przydzielić kanały sprawiedliwie, wykorzystuje się skakanie częstotliwości (1600 skoków na sekundę).

dodatkowo:
Since the introduction of Bluetooth 2.0+EDR, **π/4-DQPSK**(Differential Quadrature Phase Shift Keying) and **8DPSK** modulation may also be used between compatible devices.

31. Jakiej szerokości są kanały w bluetooth?45110T

a) 83.4 kHz
b) 834 kHz
c) 1000 kHz
d) jest ich 79

32: Kismet skanując sieci:
T: wykorzystuje tylko pasywną analizę sieci.
F: działa jako aktywny sniffer.
T: wykorzystuje sekwencję przeskoków pomiędzy odległymi kanałami zwiększającą efektywność analizy.

F: wykorzystuje sekwencję skanującą kanał po kanale, zwiększającą w ten sposób efektywność analizy.
F: jest w stanie wykryć tylko te rozsyłające ramki BEACON.
T: potrafi w locie dekodować pakiety WEP.
F: pracuje z każdą kartą bezprzewodową obsługującą standardy 802.11.
T: może rozpoznać dostawców wykrytych kart bezprzewodowych.

33: Program Kismet:
F: za pomocą wbudowanego IDS potrafi rozpoznać zagrożenia tylko na podstawie sygnatur.
T: może rozpoznać zagrożenia w sieci na podstawie analizy ruchu w warstwie 2.
T: jest zbudowany w oparciu o architekturę client-server
F: zapisuje pobrane pakiety w formatach popularnych baz danych(MySQL, PostgreSQL,Oracle, MS SQL)
T: Mając do dyspozycji moduł GPS generuje mapy rozmieszczenia wykrytych sieci.
F: Mierzy moc odbieranych sygnałów sieci w mW
F: Dostępny jest do nieodpłatnego użytku tylko do celów niekomercyjnych.

34. Siec WLAN działająca na 5GHz:

a. **moze wykorzystywac MIMO //może, chociażby 802.11n ma MIMO**
b. **802.11n //zarówno 2,4 jak i 5Ghz**
c. 802.11b //nie, 2,4 giga
d. **802.11a**
e. moze wykorzystywac kanał 11 // kanał 11 jest na 2,4 Ghz, 5 Ghz zaczyna się od 36
f. może wykorzystywać technologię DSSS (direct sequence spread spectrum)

34a. Sieć WLAN działająca w paśmie 2.4GHz może:

a. **pracować w oparciu o standard 802.11b**
b. pracować w oparciu o standard 802.11ac
c. wykorzystywać kanał o szerokości 80 MMHz
d. **pracować w oparciu o standard 802.11g**

35.W jaki sposób można zautomatyzować wykonywanie symulacji w COMNET:

a. **wykorzystując opcję Experiment on Factor**
b. wykorzystując opcję Export Stats after each run
c. wykorzystując opcję Number of replications
d. wykorzystując opcję Repeat until defined treshold

36.Tworzenie interfesjów wirtualnych:

a. wymaga przełączenia interfejsu sieciowego WLAN w tryb pracy monitor
b. **pozwala na rozgłaszanie sieci o różnych SSID przez jeden interfejs sieci WLAN**
c. jest możliwe w systemie operacyjnych Linux z użyciem większości kart sieci WLAN - chyba nie,niech ktoś potwierdzi.
d. **może być używane w celu wydzielenia otwartej sieci dostępowej dla gości**
e. jest wspierane tylko przez urządzenia standardu 802.11ac
f. to inaczej funkcja AP isolation
g. **jest możliwe przy użyciu mostu sieci WLAN**

37. Wirtualne sieci bezprzedowowe:

a. muszą być zabezpieczone tym samym kluczem WEP lub WPA jeśli zostały utworzone przy pomocy jednego i(coś dalej)
b. mogą się różnić pasmem uplink i downlink udostępnianym dla użytkowników
c. mogą się różnić politykami dostępu do sieci WAN
d. mogą być tworzone tylko na urządzeniach wspierających technologię MIMO(multiple input multiple output)
e. mogą posiadać różne SSID mimo utworzenia przy pomocy jednego interfejsu radiowego WLAN
f. mogą być utworzone tylko w oparciu o standard 802.11n

38. Nagłówek PLCP:

a. jest zabezpieczony sumą kontrolną CRC
b. jest poprzedzony preambułą
c. poprzedza nagłówek MAC standardu IEEE 802.11
d. zawiera informację o prędkości transmisji danej ramki
e. zawiera pola adresowe
f. zawiera numer sekwencyjny
g. zawiera BSSID
h. zawiera SSID
i. w celu zapewnienia niezawodności transmisji, nadawany jest zawsze z najniższą możliwą prędkością

39. Wymień profile standardu Bluetooth:

a. LAN Access Profile (LAP)
b. Standard discovery Application Profile(SDAP) **(Service Discovery Application Profile)**
c. Object Exchange (OBEX) (protokół a nie profil)
d. Hybrid Serial Profile (HSP)
e. Secure Port Profile (SPP) **(Serial Port Profile)**
f. File Transfer Profile(FTP)

40. Wymień serwery/protokoły AAA

a. TACACS
b. SVN
c. Diameter
d. iperf
e. TACACS+
f. DHCP
g. Radius

41. Problem węzła eksponowanego

a. można próbować neutralizować poprzez regulację czułości odbiorników stacji nadających

b. **można próbować neutralizować poprzez regulację mocy nadawanej przez stację**
c. **występuje gdy 2 stacje nadające znajdują się tak blisko siebie, że niemożliwa jest ich równoczesna transmisja pomimo…**
d. występuje gdy stacje nadające znajdują się tak blisko siebie, że skierowane do nich transmisje wzajemnie się zakłócają
e. występuje gdy stacje odbiorcze znajdują się na tyle blisko siebie, tak że skierowane do nich transmisje wzajemnie się za…?(zagłuszają??)
f. **można rozwiązać przy użyciu rezerwacji kanału za pomocą ramek RTS/CTS**

42. Jakie narzędzie programowe umożliwia rozłączenie stacji od AP przy łamaniu zabezpieczeń WPA2

a. airodump -ng
b. **aireplay -ng**
c. airocon -ng
d. aircrack -ng
e. airrecon-ng

43. Ramka Beacon:

a. **może zawierać pole SSID o zerowej długości**
b. **zawsze zawiera BSSID**
c. **jest transmitowana cyklicznie przez każdy punkt dostępowy**
d. nie jest transmitowana cyklicznie gdy dana sieć jest ukrytą
e. **w polu adresu docelowego ma andres rozgłoszeniowy (broadcast)**
f. nie jest przeznaczona do informowania stacji o konfiguracji sieci
g. dzięki szyfrowaniu pozwala ukryć SSID sieci

44. Jaka powinna być optymalna wielkość parametry CWMIN dla sieci WLAN badanej w symulatorze COMNET ,złoż… nasycenia

a. **CWMIN=1023**
b. CWMIN=31
c. CWMIN=15
d. CWMIN=127
e. CWMIN=63

45. Ile interfejsów wirtualnych VAP może być zdefiniowanych dla jednego interfejsu sprzętowego sieci WLAN

a. co najwyżej 1
b. **dla kart WLAN wykonanych na starszych chipsetach tworzenie interfejsów wirtualnych może być całkowicie niemożliwe**
c. co najmniej 1
d. dla kart WLAN wykonanych na starszych chipsetach może to być więcej niż 1 VAP, ale wszystkie interfejsy będą miały identyczny MAC
e. trudno jest to jest to jednoznacznie ustalić, ale dla kart WLAN opartych na chipsecie Broadcom możliwość tworzenia VAP można sprawdzić poleceniem nvram g…

f. **maksymalna liczba interfejsów zależy od chipsetu karty WLAN oraz użytego sterownika**

46. Parametr okna współzawodnictwa ma największy wpływ na uzyskanie największej możliwej sieci WLAN badanej w symulatorze COMNET złożonej ze 100 stacji pracującej w … okna zdefiniowanych w IEEE 802.11

a. **zarówno CWMIN jak CWMAX powinno być duże**
b. wyłącznie CWMIN które powinno być małe
c. zarówno CWMIN jak i CWMAC przy czym CWMIpowN inno być małe, a CWMAX duże
d. wyłącznie CWMAX które powinno być duże

47. Dwie sieci WLAN (A i B) pracujące na tym samym obszarze:

a. nie mogą być skonfigurowane do pracy w standardzie 802.11n w dwóch różnych pasmach 2,4 i 5 GHz
b. mogą wpływać na siebie jeśli sieć A pracuje w standardzie 802.11b/g, a sieć B w standardzie 802.11a
c. nie mogą wpływać na siebie jeśli sieć A pracuje w standardzie 802.11a, a sieć B w standardzie 802.11ac
d. **nie mogą wpływać na siebie jeśli sieć A pracuje w standardzie 802.11b/g, a sieć B w standardzie 802.11ac**

48. Sieć WLAN działająca w paśmie 5GHz może:

a. **pracować w standardzie wykorzystującym technologię MIMO**
b. **pracować w oparciu o standard 802.11n**
c. pracować w oparciu o standard 802.11b
d. wykorzystywać technologię DSSS // zamiast dsss jest mimo
e. **pracować w oparciu o standard 802.11a**

49. Odzyskanie hasła zaszyfrowanego za pomocą WEP

a. przy użyciu metody pasywnej jest niezależne od generowanego w sieci ruchu
b. polega na przechwycaniu i porównaniu pakietów z identycznymi IV
c. **wymaga przechwycenia odpowiednio dużej ilości pakietów z unikalnymi IV**
d. **jest możliwe przy użyciu metody wstrzykiwania pakietów Address Resolution Protocol do AP**

50. WPA-Enterprise:

a. może korzystać z protokołu EAP-MD5
b. jest podatne na ataki słownikowe, ponieważ wykorzystuje prekonfigurowany klucz zabezpieczeń
c. **wykorzystuje serwer RADIUS w celu uwierzytelnienia stacji dołączającej do sieci WLAN**
d. może korzystać z szyfrowania WEP
e. autoryzuje użytkownika w oparciu o adres MAC

51. Nagłówek MAC ramki danych standardu IEEE 802.11

a. jest bezpośrednio poprzedzony preambułą // chyba natkaniec mowil ze to jest zle na wykł//jest poprzedzony naglowkiem plcp a on dopiero jest poprzedzony preambula
b. **może zawierać 4 pola adresowe**
c. **zawiera informacje, czy ramka jest retransmitowana**
d. **zawiera numer sekwencyjny ramki**

52. Jaka powinna być optymalna wielkość parametru CWmin (dająca największą przepustowość) dla sieci WLAN badanej w symulatorze comnet złożonej ze 100 stacji przesyłających ramki o długości 2000B przy CWmax=8191 szczelin, pracującej w warunkach nasycenia?

a. CWmin=52
b. CWmin=127
c. CWmin=63 **(gdy jest 5 stacji)**
d. CWmin=31
e. **CWmin=1023**

53. Jakie parametry można zdefiniować w symulatorze Riverbed przy tworzeniu źródła ruchu?

a. **start time**
b. **stop time**
c. **OFF time**
d. **ON time**

54. Klasa dostępu (access class) Video (AC_VI) w sieciach WLAN:

a. nie wspiera blokowego potwierdzenia Block_ACK
b. nie może służyć do transmisji ruchu HTTP
c. **pozwala na korzystanie z mechanizmu RTS/CTS**
d. **może wykorzystywać działanie mechanizmu TXOP**

55. Jak uzyskać bezwarunkowe (niezależnie od timeoutu) wymuszenie ponownego uwierzytelniania klienta na przełączniku?

a. # dot1x reauthentication unlimited timeout
b. config-if# dot1x reauthentication
c. config-if# dot1x force-unauthorized host (host name)
d. **# dot1x re-authenticate interface (interface number)**

56. Wymień wady algorytmu Wired Equivalent Privacy (WEP)

a. **ten sam klucz (secret key) jest używany w wielu różnych wektorach IV**
b. wektor IV jest zaszyfrowany lecz jego długość wynosi zaledwie 24 bity // nie jest zaszyfrowany
c. **w niektórych kartach WLAN przy inicjalizacji wartość wektora IV jest ustawiony na** // "część producentów resetuje IV do 0 zawsze gdy jest inicjalizowana i inkrementowana"
d. cztery pierwsze bajty pola Data Field są znane i zawsze posiadają stałą wartość **(dwa pierwsze bajty są znane i równe 0xAAAA)**

57. Ustawienie parametru RTS threshold w punkcie dostępowym na wartość 100B oznacza

a. rozwiązania problemu stacji ukrytych dla trzech stacji, z których dwie skrajne się nie słyszą podczas wymiany ramek o długości 200(ucięte, więc nie wiem czy cos dalej jest) //chyba dobrze
b. włączenie mechanizmu wirtualnego śledzenia nośnej dla ramek o długości 1500 bajtów
c. stosowania wstępnej rezerwacji kanału radiowego dla wszystkich ramek mniejszych niż 100B
d. zmniejszenie wydajności pracy sieci dla obszaru, na którym aktywnie pracuje wyłącznie jedna stacja kliencka nadająca ramki do AP

58. W jaki sposób można zwiększyć bezpieczeństwo transmisji z użyciem punktu dostępowego Bluetooth

a. stosując algorytm RC4 dla zaszyfrowania przesyłanych danych
b. tworząc tzw. klucz połączenia z użyciem protokołu RC5
c. uruchamiając w punkcie dostępowym serwer RADIUS
d. stosując Bluetooth Passkey dla zapewnienia kontroli dostępu //jeśli passkey to PIN to tak

59. Aby zastosować metodę Packet Injection do łamania klucza WEP

a. na punkcie dostępowym nie może być ustawiona opcja MAC Filter List //jeśli potrzebujemy fake authentication to nie może być
b. MOŻNA wykorzystać adres MAC klienta zasocjowanego z punktem dostępowym
c. należy wydać na komputerze na którym przeprowadzana jest operacja łamania klucza polecenie aireplay-ng
d. trzeba wykorzystać MAC klienta zasocjowanego z punktem dostępowym //a nie jest tak ze MUSIMY wykorzystac mac zasocjowanego? przeciez jesli nie jest to AP odrzuci wszystkie zapytania. czy moze chodzi o to ze jak nie jest zasocjowany to robimy fake authentication? ale wtedy i tak korztstamy z tego MAC'a…

60. Parametr "Fragmentation Threshold" z wyłączonym mechanizmem RTS/CTS w przypadku niewielkiej sieci ad-hoc standardu IEEE 802.11 działającej w stanie nasycenia

a. powoduje podział ramek większych niż wartość parametru na mniejsze fragmenty transmitowane osobno
b. po ustawieniu na małą wartość może poprawić wydajność transmisji gdy przesyłane są bardzo krótkie ramki i występują zakłócenia powodujące retransmisje
c. ma nieznaczny wpływ na wydajność transmisji jeśli transmitowane są bardzo krótkie ramki
d. po ustawieniu na małą wartość może poprawić wydajność transmisji gdy przesyłane są długie ramki i występują zakłócenia powodujące retransmisje

61. Co potrafi wireshark

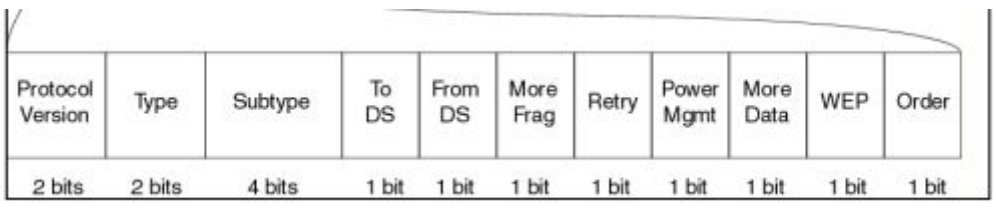
filtrowanie

kolorowanie list pakietów
zapisywanie do pliku
wczytywanie z pliku
robienie statystyk
szukanie pakietów które spełniają określone kryteria

62. Kismet skanując sieci:
T: Wykorzystuje tylko pasywną analizę sieci.
F: działa jako aktywny sniffer.
T: Wykorzystuje sekwencję przeskoków pomiędzy odległymi kanałami zwiększającą efektywność analizy.
F: wykorzystuje sekwencję skanującą kanał po kanale, zwiększającą w ten sposób efektywność analizy.
F: jest w stanie wykryć tylko te rozsyłające ramki BEACON.
T: potrafi w locie dekodować pakiety WEP.
F: pracuje z każdą kartą bezprzewodową obsługującą standardy 802.11.
T: może rozpoznać dostawców wykrytych kart bezprzewodowych.

63. Program Kismet
F: za pomocą wbudowanego IDS potrafi rozpoznać zagrożenia tylko na podstawie sygnatur.
T: Może rozpoznać zagrożenia w sieci na podstawie analizy ruchu w warstwie 2.
T: Jest zbudowany w oparciu o architekturę client-server
F: zapisuje pobrane pakiety w formatach popularnych baz danych(MySQL, PostgreSQL,Oracle, MS SQL)
T: Mając do dyspozycji moduł GPS generuje mapy rozmieszczenia wykrytych sieci.
F: Mierzy moc odbieranych sygnałów sieci w mW
F: Dostępny jest do nieodpłatnego użytku tylko do celów niekomercyjnych.

64. Prawdziwymi stwierdzeniami o 802.11 i jego strukturze pakietu są:
F: nagłówek MAC może zawierać w sobie do pięciu adresów
T: Do nagłówka MAC należy sekwencja kontrolna
T: Do nagłówka MAC należy FCS zawierające 32-bitowe CRC // a FCS nie jest na końcu ramki, po payload? no wlasnie tak jest.... // jest i tu i tu
T: Struktura pakietu zawiera preambułę i nagłówek PLCP w warstwie fizycznej.
F: Nagłówek MAC znajduje się w warstwie fizycznej struktury pakietu.
T: część transmisji PLCP jest zawsze wysyłana najniższą powszechnie używaną wartością data rate.
F: Typ w polu frame control może być jedną z czterech wartości. // 2 bity- dlaczego fałsz?//bo masz tylko 3 wartosci do wyboru:ramki kontrolne, zarzadzajace i ramki danych



F: Frame Control to pole o wielkości czterech bajtów w nagłówku MAC

65. Plik ap_manuf pozwala na modyfikację następujących parametrów Access Pointa:
T: Adresu IPv4
T: Kanału transmisyjnego
F: Szerokości kanału transmisyjnego AP
T: Pola SSID
F: Producenta access pointa
F: Szerokości pasma transmisyjnego
F: Maksymalnej przepustowości transmisji
F: Długości bufora AP

66. Wireshark zezwala na:
T: przechwytywanie pakietów z interfejsu sieciowego w czasie rzeczywistym
T: zapisywanie przechwyconego ruchu do pliku .pcap
T: filtrowanie przechwytywanego ruchu z wykorzystaniem odpowiednich reguł filtrujących
T: kolorowanie pakietów ze względu na typ przechwytywanych pakietów
F: przechwytywanie tylko niektórych rodzajów pakietów
F: wykorzystywanie tylko wbudowanych reguł filtrujących
F: nie zezwala na filtrowanie pakietów danych przechwytywanych
F: nie zezwala na podglądanie nagłówków protokołów przechwyconych pakietów danych

67. Nagłówek MAC 802.11 zawiera:
T: kontrola ramki (Frame Control)
T: Adres źródłowy (Source address)
T: Adres docelowy (Destination address)
T: Kontrola sekwencji (Sequence Control)
F: Cykliczna kontrola nadmiarowa ramki (Cyclic Redundancy Check) /a to nie jest prawda? w FCS jest przecież CRC // tak ale FCS jest na koncu ramki 802.11 a nie nagłówka MAC w tej ramce
T: Typ ramki (Type of frame)
F: Znacznik początkowy ramki (Start frame delimiter filed)
F: Preambuła (preamble filed)

68. To perform password sniffing You need:
T: Prepare two terminals: sniffer and client
T: Connect client to the service server (FTP,SMTP)
T: Disconnect client from the service server
T: Filter Wireshark data in order to find passwords
F: Connect Wireshark to service server
F: Prepare three terminals: client, server and sniffer.
F: You don't need to analyze data, Wireshark will do it itself.
F: Wireshark can only sniff traffic without capturing

69. Parameters used in wireless frame are:
T: To DS and From DS, both are 1 bit parameters.

T: To DS, From DS, More Fragment, Power Management, More Data, WEP, Order
T: More Data which indicates that there are more frames in AP buffer
T: The are parameters in Frame Control field such as Retry, WEP and Order.
F: The are parameters in Frame Control field such as Address, Duration and CRC.
F: Order, To DS and From DS parameters are 10 bytes long.
F: WEP parameter indicate that frame body is not encrypted according WEP
F: Frame control is 10 bytes field filled with parameters.

70. Informacje potrzebne do przeprowadzenia ataku typu "full-knowledge" to:
T: identyfikator BSSID
F: adres IP AP
T: numer kanału
T: adres MAC punktu dostępowego
T: adres MAC klienta sieci
F: nazwa producenta AP
T: SSID (Service Set Identifier)
F: adres IP klienta

71. Które informacje dotyczące WEP są prawdziwe:
F: Wykorzystuje algorytm RC5
T: Można ustawić maksymalnie 4 klucze na punkcie dostępowym
F: Jest skrótem Wireless Encryption Protocol **//Wireless Equivalent Privacy**
T: Niektóre karty sieciowe umożliwiają ustawienie tylko 1 klucza
T: Wykorzystuje CRC-32
T: Klucze ustawione na AP i urządzeniu klienckim muszą się zgadzać
F: Trzeba ustawić minimalnie 4 klucze na AP
T: Wykorzystuje RC4

72. Aby zastosować packet-injection do łamania klucza WEP:
F: Trzeba wykorzystać adres MAC klienta zasocjowanego z punktem dostępowym
F: Wystarczy polecenie aircrack-ng
T: Można wykorzystać fake-authentication
T: Najczęściej wykorzystuje się przechwycone pakiety ARP
T: Można wykorzystać adres MAC klienta zasocjowanego z AP
F: Na AP nie może być ustawiona MAC Filter List
T: Należy wpisać polecenie aireplay-ng
T: Należy przestawić interfejs sieciowy w tryb pracy RFMON

73. Podczas łamania klucza WEP wykorzystywane są narzędzia:
T: airodump-ng: przechwytuje pakiety i zapisuje je do pliku
T: aireplay-ng: zalewa AP pakietami ARP request
T: aircrack-ng: generuje klucz WEP na podstawie pakietów zgromadzonych w pliku
F: airodump-ng: zapisuje informacje **o sieci** do pliku
F: airogain-ng: przechwytuje i zapisuje pakiety do pliku
F: aircrack-ng: generuje klucz WEP na podstawie podsłuchanych informacji o sieci (między innymi adresu MAC AP)

F: aireplay-ng: odpowiada na zapytania AP podszywając się za klienta
F: airhack-ng: wywołuje procedurę łamania klucza na podstawie pakietów zapisanych w pliku

74. Access point Cisco Aironet 1100 Series z zainstalowanym systemem operacyjnym IOS Cisco może funkcjonować w trybie:
T: with limited authorizations (USER EXEC) będącym trybem domyślnym
T: privileged (PRIVILEGED EXEC) uruchamianym komendą enable
T: configuration (GLOBAL CONFIGURATION) uruchamianym komendą configure
T: interface configuration (INTERFACE CONFIGURATION)
F: interface configuration (INTERFACE CONFIGURATION) uruchamianym komendą configure
F: privileged (PRIVILEGED EXEC) służącym do tworzenia VLANów
F: privileged (PRIVILEGED EXEC) wymagającym skonfigurowania dostępu hasłem
F: configuration (GLOBAL CONFIGURATION) służącym do adresowania interfejsu

75. Klucz SSID:
T: identyfikuje bezprzewodowe sieci lokalne
T: jest wysyłany tekstem jawnym
F: chroni sieć lokalną przed próbą nieautoryzowanego dostępu
F: wykorzystywany jest do autoryzacji użytkowników
T: ma długość 32 bitów
T: dzięki wbudowanym opcjom pozwala ograniczyć liczbę użytkowników sieci
F: musi być rozgłaszany przez każdą sieć lokalną
T: dodawany jest do nagłówków pakietów IP

76. Protokół EAP:
T: to skrót oznaczający Extensible Authentication Protocol
T: jego odpowiednikiem dla urządzeń sieciowych Cisco jest LEAP
T: podobnie jak Open System i Shared Key służy do uwierzytelniania
T: posiada wbudowane mechanizmy pozwalające na eliminację pojawiających się duplikatów pakietów
F: nie posiada możliwości negocjacji używanej metody uwierzytelniania
F: nie posiada mechanizmu pozwalającego na ponowną retransmisję zagubionych pakietów
F: gwarantuje obsługę mechanizmu fragmentacji ramek
F: nie jest używany w sieciach korzystających z protokołu IEEE802

77. Protokół RADIUS:
T: dostarcza możliwość autoryzacji użytkowników sieci lokalnych
T: jest protokołem typu klient/serwer
T: do szyfrowania wykorzystuje funkcję skrótu MD5
T: okresowo autoryzuje użytkowników dołączonych do sieci
T: nie pozwala na korzystanie z funkcjonalności proxy
F: wykorzystywany jest jedynie w bezprzewodowych sieciach lokalnych
F: wykorzystuje protokół TCP
F: szyfruje nadawane komunikaty

78. Protokół SNMP:
T: domyślnie wysyła komunikaty Trap na port 162 UDP
T: używa do przesyłania pakietów protokołu UDP, zlokalizowanego w warstwie transportowej
T: domyślnie działa na porcie 161 UDP
T: to skrót Simple Network Management Protocol
T: jest protokołem warstwy aplikacji
F: Jest odporny na ataki słownikowe.
F: używa do przesyłania pakietów protokołu zlokalizowanego w warstwie sieciowej
F: jest protokołem warstwy piątej modelu ISO/ OSI

79. Stwierdzeniami prawdziwymi o protokole SNMP są:
T: Każda wartość w nim jest jednoznacznie identyfikowana przy pomocy identyfikatora liczbowego OID.
F: W sieci zarządzanej przy jego pomocy można wyróżnić cztery kluczowe komponenty.
F: Agent otrzymuje żądania na port 162 UDP.
T: Wszystkie jego wersje są podatne na ataki typu brute force
T: Do tej pory można wyróżnić trzy jego wersje.
T: W wersji pierwszej posiada pięć komend.
T: Obiekty, które charakteryzują dany parametr przechowywane są jako liście w drzewiastej strukturze
F: Manager domyślnie działa na porcie 180 UDP.
F: Sposobem kodowania struktur danych jego komunikatów jest uproszczony ASN.1.

80. MIB to:
T: Skrót, który oznacza Management Information Base
T: To baza znajdująca się w Managerze
T: To baza zawierająca informacje między innymi o nazwie, wartości, typie danego parametru
F: To skrót, który oznacza mobility information base
F: Organizacja zrzeszająca producentów sprzętu sieciowego
F: Chipset firmy Broadcom
F: Oprogramowanie firmy Broadcom
F: To skrót, który oznacza main integration base

81. Rodzaje komunikatów w SNMP
T: Get, GetNext
F: Get, Request, Set
F: Trap, Ack, Set
T:Trap, Response
T: GetBulk, Inform
F: Ack, Idle, Request
F: Set, Idle, Response
F: Done, Request, Idle

82. Sieć typu ad-hoc:
F: jest dużo bardziej odporna na wystąpienie kolizji pakietów w porównaniu z siecią wykorzystującą punkt dostępowy.
F: wymaga rozbudowanej infrastruktury.
F: może zostać zestawiona pomiędzy urządzeniami należącymi do różnych podsieci.
T: może wykorzystywać wiele kanałów.
T: do poprawnego działania nie potrzebuje użycia punktu dostępowego.
T: umożliwia transmisję szybszą niż sieć DLAN.
F: zawsze zapewnia bezpośrednie połączenie pomiędzy dowolnymi urządzeniami w sieci.
F: wymaga, żeby przynajmniej jedno z podłączonych urządzeń działało jako serwer DHCP.

83. Do oceny parametrów sieci ad-hoc może zostać wykorzystane oprogramowanie:
F: iperf - używane do przechwytywania pakietów.
F: AdapterWatch - pozwalające określić taktowanie zegara karty sieciowej.
T: PCATTCP - narzędzie badające wydajność pomiędzy dwoma urządzeniami z systemem Windows.
F: PCATTCP - tylko jeżeli korzystamy z protokołu TCP.
T: IPERF - do wygenerowania potrzebnego ruchu sieciowego.
F: PCATTCP - prezentujące wyniki pomiarów w formie wykresów.
F: Wireshark - umożliwiające przechwycenie pakietów sterujących warstwy trzeciej.
T: strumieniujące filmy (metoda organoleptyczna).

84. Oprogramowanie iperf:
F: daje możliwość korzystania tylko z protokołu TCP.
F: daje możliwość korzystania tylko z protokołu UDP.
T: umożliwia korzystanie zarówno z protokołu TCP oraz UDP.
T: wymaga uruchomienia serwera jak i klienta.
F: nie umożliwia sprawdzenia strat pakietów.
T: umożliwia sprawdzenie opóźnienia pakietów.
T: mierzy pasmo przesyłanych danych.
T: nie umożliwia przesyłu danych w formie broadcast. wg StackOverflow nie moze dzialac w broadcascie

85. Oprogramowanie BWMeter:
T: mierzy pasmo.
T: monitoruje i kontroluje ruch wchodzący i wychodzący z komputera użytkownika,
F: nie posiada graficznego interfejsu użytkownika,
T: jedną z głównych cech jest obserwacja wpływu interferencji.
T: monitoruje wszystkie typy ruchu w sieci.
F: monitoruje tylko wybrane interfejsy sieciowe.
F: nie może pracować w trybie real-time.
T: używa filtrów definiowanych przez użytkownika celem pomiaru pasma.

86. Na których z poniższych częstotliwości może pracować Bluetooth:
F: Wszystkie odpowiedzi są prawidłowe
F: Żadna z odpowiedzi nie jest prawidłowa

T: 2,4 GHz
F: 5 GHz
F: 900 MHz
F: 3,6 GHz
F: 10 GHz
F: 13 GHz

87. W systemie LINUX aby upewnić się czy urządzenie bluetooth zostało wykryte należy wykonać komendę:
F: Wszystkie odpowiedzi są prawidłowe
F: Żadna z odpowiedzi nie jest prawidłowa
T: hcitool dev
T: hciconfig -a
T: lspci
F: ifconfig
F: mesg
T: lsusb

88. W technologii Bluetooth:
T: urządzenia są zorganizowane w grupy liczące od dwóch do ośmiu składników zwanych pikonetami (piconets)
F: określono rozszerzenie widma przez pseudolosowe skakanie po 109 częstotliwościach w paśmie 1,4 - 4,4 GHz
T: definiujemy trzy klasy mocy nadawanej o zasięgu 100, 10 oraz 1 metr
F: są zdefiniowane między innymi profile STP (Service Transfer Protocol) oraz HPP (Headset Port Profile)
T: Sterownik HCI jest używany w komputerze do sprzęgania aplikacji Bluetooth z protokołem transportowym
F: Komunikacja funkcjonuje w licencjonowanym paśmie IMS
T: L2CAP zapewnia sprzęganie z kontrolerem łącza i kompatybilność między urządzeniami
F: Sieci pikonet mogą być formowane tylko statycznie

89. Wykrywanie urządzeń Bluetooth,
T: Może zostać przeprowadzone za pomocą programu BTScanner
F: Polega na ustaleniu identyfikatora HCI (Hide Connection Identifier) stacji szukanej
T: W systemie Linux może zostać przeprowadzone z poziomu linii komend, przykładowo poleceniem hcitool scan
F: Jest możliwe w trybie Dial-up
F: Jest możliwe za pomocą komendy hcidump
F: Jest możliwe tylko w profilach PAN, SPP oraz HSP
T: Jest możliwe za pomocą komendy hcitool dev
F: opiera się o mechanizmy detekcji z warstwy L2CAP

90. Interferencje pomiędzy sygnałami WiFi i Bluetooth:
F: Nie mogą wystąpić, ponieważ obie sieci pracują na innych pasmach częstotliwościowych

T: Mogą wystąpić, ponieważ obie sieci mogą pracować w paśmie 2.4GHz
F: Nie mają wpływu na pracę obu sieci
T: Mogą mieć wpływ na prędkość transmisji danych w obu sieciach
T: Mogą zostać wyeliminowane, poprzez migrację sieci WiFi do pasma 5GHz
F: Mogą zostać zmniejszone, przy uzyciu adaptacyjnego skakania po częstotliwościach (ADH - Addaptive Frequency Hopping), techniki używanej w standardzie WiFi
T: Mogą zostać zmniejszone, przy uzyciu adaptacyjnego skakania po częstotliwościach (ADH - Addaptive Frequency Hopping), techniki używanej w standardzie Bluetooth
F: Mogą zostać wyeliminowane dzięki użyciu standardu Bluetooth 4.0 i nowszych

91. Aplikacja PCATTCP
T: Służy do badania wydajności protokołów warstwy transportowej pomiędzy dwoma systemami
F: Służy do badania wydajności protokołu IP pomiędzy dwoma systemami
T: Pozwala na zmierzenie prędkości przesyłania danych w sieci
T: Może zostać uruchomiona w trybie odbiornika
T: Może zostać uruchomiona w trybie nadajnika
F: Może zostać uruchomiona jako serwer
T: W jednym z trybów pozwala na wybór ilości oraz rozmiaru pakietów, które mają zostać wysłane
F: Do jej poprawnego działania wystarczy uruchomienie na jednym systemie

92. Aplikacja iperf:
T: Może zostać uruchomiona w trybie klienta
F: Może zostać uruchomiona jedynie w trybie serwera
T: Może zostać uruchomiona w trybie klient-serwer
T: Może zostać użyta do pomiarów przepustowości
T: Może generować strumień danych zarówno protokołu TCP jak i UDP
F: Może generować jedynie strumień danych protokołu TCP
F: Może generować jedynie strumień danych protokołu UDP
T: Przy testowaniu protokołu UDP pozwala sprecyzować rozmiar datagramu

93. Które z poniższych czynności w konfiguracji Access Point'a są niezbędne do poprawnego jego działania w trybie Repeater?
T: Ustawienie AP w tryb pracy "Repeater" .
F: Ustawienie pola "Remote AP MAC" na adres fizyczny interfejsu WLAN Access Pointa z którym skojarzony jest Repeater.
T: Ustawienie pola "Remote AP MAC" na adres fizyczny interfejsu Ethernet Access Pointa z którym skojarzony jest nasz Repeater.
F: Ustawienie Access Pointa do pracy na kanale nr 12.
T: Ustawienie poprawnego adresu IP, maski podsieci oraz SSID. // ?
F: Ustawienie trybu szyfrowania na WEP.
F: Ustawienie mocy nadawanego sygnału na najniższą możliwą.
T: Ustawienie Access Pointa do pracy na dowolnym kanale.

94. Access Point działający w trybie pracy "Repeater" :
F: Zmienia logiczną strukturę ramki którą otrzymuje a następnie przesyła.
T: Pracuje w warstwie pierwszej modelu OSI/ISO.
F: Pracuje w warstwie drugiej modelu OSI/ ISO.
T: Zwiększa zasięg sieci WIFI z którą jest połączony.
F: Może pracować tylko i wyłącznie w paśmie częstotliwości 2,4GHz
T: Umożliwia ustawienie mocy transmisji nadawanego sygnału.
T: Może powodować dodatkowe opóźnienia w transmisji.
F: W sieciach WLAN może być używany na długich dystansach.

95. Jakie są wady używania trybu Repeater?
T: Tryb Repeater redukuje przepustowość sieci o minimum 50%
F: Użycie trybu Repeater powoduje duże zużycie mocy Access Point'a
T: Zwiększona jest podatność na interferencje w sieci lokalnej //np. przez mikrofalówki
F: Do poprawnej pracy trzeba użyć urządzeń tego samego producenta
T: Repeater musi mieć stałe źródło zasilania
F: Repeater wymaga użycia szyfrowania WEP
T: Repeater posiada ograniczony zasięg
F: Tryb repeater wymaga zastosowania uwierzytelnienia

96. Jakie są cechy wspólne trybów pracy Repeater i Bridge w urządzeniu Access Point?
T: Zarówno w trybie Repeater jak i w trybie Bridge należy podać adres MAC urządzenia dostarczającego sygnał
F: Zarówno w trybie Repeater jak i w trybie Bridge można tworzyć połączenia pomiędzy dwoma sieciami
T: Zarówno Repeater jak i Bridge można wykorzystać do zwiększenia zasięgu sieci
F: Tryb Repeater i tryb Bridge nie modyfikuje przesyłanych ramek
T: Tryb Repeater oraz tryb Bridge pozwalają na wykorzystanie szyfrowania WEP
F: Tryb Repeater oraz tryb Bridge pracują w trzeciej warstwie modelu OSI/ISO
T: Zarówno w trybie Repeater jak i w trybie Bridge jest możliwość wybrania kanału, na którym prowadzi się transmisję
F: Zarówno w trybie Repeater jak i w trybie Bridge nie można wybrać kanału, na którym ma być prowadzona transmisja

97. Parametr RTS threshold dla access pointa oznacza://To pewne odp?
T: Opóźnienie wysłania wiadomości Request to Send przez AP
F: Czas, który musi odczekać komputer klienta przed wysłaniem danych do AP
T: Czas, który musi odczekać AP przed wysłaniem wiadomości RTS do komputera klienckiego
F: Czas, który musi odczekać AP przed wysłaniem danych do komputera klienckiego
F: Opóźnienie wysłania wiadomości Request to Send przez komputer klienta
F: Czas, który musi odczekać komputer klienta przed wysłaniem wiadomości RTS do access pointa
F: Opóźnienie wysłania wiadomości Response to Server przez komputer klienta
F: Opóźnienie wysłania wiadomości Response to Server przez access point

98. Statystyki/dane zbierane podczas symulacji w programie OPNET:
T: Mogą być zbierane dla pojedynczych węzłów
F: Mogą być zbierane wyłącznie dla całej sieci
T: Są obliczane w oparciu o dyskretne dane symulatora
F: Są obliczane w oparciu o ciągłe dane wyjściowe symulatora
T: Mogą być wartościami uśrednionymi w czasie parametru sieci
T: Mogą być zbiorem wartości chwilowych danego parametru sieci
F: Nie mogą przedstawiać opóźnienia, bo nie jest ono modelowane podczas symulacji
F: Nie zależą od czasu symulacji

99. Przy włączonej funkcji PCF - Point Coordination Function:
T: Symulator sieci OPNET wykonuje więcej obliczeń i wydłuża się czas uruchomienia symulacji
F: Czas dostępu do medium zostaje równo podzielony pomiędzy klientów
T: Access point steruje przesyłaniem ramek gdyż nie panują zasady konkurencji w dostępie do medium
F: Panują określone zasady konkurencji przy wysyłaniu ramek
T: Średnia przepustowość rośnie w stosunku do wyłączonego PCF
F: Access point przestaje sterować przesyłaniem ramek, obowiązują zasady konkurencji
F: Access point steruje zasadami przesyłania pakietów przez stacje robocze
F: Średnia przepustowość maleje

100. W sieciach Wireless LAN:
T: Liczba stacji roboczych nie ma znaczącego wpływu na przepustowość sieci //na pewno?
F: Przepustowość sieci jest większa dla wiadomości długości 128B niż dla 1024B
T: Przepustowość jest mniejsza dla wiadomości długości 128B niż dla 1024B
F: Parametr Beacon Interval zwiększa średnie opóźnienie transmisji
F: Parametr Fragmentation threshold nie wpływa na przepustowość
F: Parametr Beacon Interval zmniejsza średnie opóźnienie transmisji
T: Parametr Fragmentation threshold określa minimalny rozmiar wiadomości, która zostanie podzielona
F: Parametr Beacon Interval nie może być ustawiony na więcej niż 1ms

101. Źródło Sesji w symulatorze COMNET III:
T: może być używane w przypadku analizy ruchu zorientowanej na połączenie
T: jest jednym z 3 możliwych do zdefiniowania źródeł ruchu symulatorze COMNET III
T: jest źródłem ruchu które najpierw zestawia sesje pomiędzy węzłami sieci a później przesyła wiadomości pomiędzy nimi
F: umożliwia jedynie zestawienie sesji pomiędzy węzłami sieci
F: nie jest możliwe do zdefiniowania
F: nie jest używane w analizie ruchu zorientowanej na połączenie
T: nie jest używane w symulacji ruchu pakietowego
F: jest używane w symulacji ruchu pakietowego

102. Źródło Odpowiedzi w symulatorze COMNET III:
T: jest generatorem odpowiedzi zwrotnych
T: może generować np. odpowiedzi na zapytania bazy danych, odpowiedzi e-mail
T: wymaga wiadomości przychodzącej do danego węzła aby generować wiadomości zwrotne
T: wymaga unikalnego (w ramach projektu) parametru Message Name
F: nie jest możlwe do zdefiniowania
F: generuje wiadomości niezależnie od ruchu przychodzącego do danego węzła
F: jest jednym z 2 dostępnych źródeł ruchu
F: musi mieć taki sam parametr Message Name jak Źródło Wiadomości aby generowało wiadomości

103. Symulator COMNET III:
F: umożliwia symulację tylko standardu 802.11
T: umożliwia symulację zarówno sieci LAN jak i WAN
F: umożliwia przegląd danych tylko po zakończeniu symulacji
T: umożliwia przegląd danych podczas trwania symulacji
T: pozwala na zbierania danych statystycznych symulacji
T: pozwala na zdefiniowanie 3 źródeł ruchu
F: nie pozwala na zdefiniowanie protokołu warstwy transportowej
F: umożliwia symulację jedynie ruchu FTP i HTTP

104. Parametr źródeł ruchu Message Priority w symulatorze COMNET III:
T: musi mieć wartość od 1 do 99
T: określa priorytet dla pakietów w buforze
F: może mieć dowolną wartość całkowitą
F: musi mieć wartość od 1 do 20
T: jest wprost proporcjonalny do priorytetu pakietu
F: jest odwrotnie proporcjonalny do priorytetu pakietu
F: jest zależny od parametru Interarrival
T: jeśli jest równy dla danych pakietów są one umieszczane w buforze FIFO

105. Jakie informacje musimy uzyskać z programu Kismet przy łamaniu zabezpieczeń WPA?:
T: Nazwa atakowanej sieci (SSID)
T: Adres MAC punktu dostępowego
T: Adres BSSID
F: Adres IP routea
F: Adresy IP wszystkich klientów sieci
T: Adresy MAC klientów sieci
T: Numer kanału
F: Metodę zabezpieczenia sieci

106. W celu złamania zabezpieczeń WPA?
T: Należy przechwycić pakiety 4-way handshake wykorzystując polecenie airodump
F: Należy przechwycić pakiety 4-way handshake przy pomocy polecenia aircrack

T: Można wykorzystać wcześniej zdefiniowany słownik wyrazów
T: Można wykorzystać generator słów do przeprowadzenia ataku typu Brute Force
F: Należy przechwycić pakiety 3-way handshake przy pomocy polecenia airodump
F: Nie można wykorzystywać własnoręcznie napisanych słowników wyrazów
T: Należy wymusić ponowne uwierzytelnianie klienta sieci, aby uzyskać 4-way handshake
F: Należy wymusić ponowne uwierzytelnianie klienta sieci w celu uzyskania 3-way handshake

107. Co oznacza skrót WPA?
T: Skrót z ang.: Wi-Fi Protected Access
F: Skrót z ang.:Wireless Protected of Access
F: Skrót z polskich wyrazów: Wysoka Protekcja Algorytmowa
F: Nic nie onacza
F: Brak rozwinięcia skrótu
F: Wszystkie wymienione odpowiedzi są poprawne
F: Z francuskiego Wifi Protection d'Accès XDDDD
F: Skrót z ang.:Wireless Protected of Anonymous
F: Skrót z ros. Cyka Blyat Protected Access //potwierdzone info

108. Z czego korzysta WPA?
T: TKIP, EAP oraz MIC
F: MIC, TKIP, EAP oraz AES //AES tylko w WPA2
F: Wszystkie wymienione odpowiedzi są poprawne
T: 802.1x + TKIP
F: AES oraz MIC
F: AES oraz TKIP
F: EAP i AES
F: MIC, EAP, TKIP i 801.2x

109. Pole “Association id” w ramkach standardu…
a) ma 2 bajty
b) stanowi identyfikator stacji przydzielony jej przez punkt dostępu
c) stanowi część ramki “Association request”
d) wartość pola AID stanowi liczbę z zakresu 1-2007

110. Moduł TC (Traffic Control) stosowany przy konfiguracji interfejsów wirtualnych
a) umożliwia realizację funkcji AP isolation
b) umożliwia definicję sposobu kolejkowania pakietów na poziomie warstwy transportowej
c) uruchamia tłumaczenie adresów sieciowych (NAT) na porcie WAN
d) umożliwia przetwarzanie ruchu przy użyciu trzech obiektów: QDISC, CLASSES, FIL…..

111. Łamanie algorytmu WPA2 sieci standardu IEEE 802.11

a) polega na rozłączeniu stacji od AP, a następnie przechwyceniu tzw. 4-Way Handshake…
b) jest możliwe także w sieci z ukrytym SSID
c) polega na wykorzystaniu spreparowanej ramki Deauthentication w celu wymuszenia p.. narzędzia do łamania klucza WPA2 z atakiem brute force
d) polega na pasywnym nasłuchiwaniu ramek atakowanej sieci WLAN, gromadzeniu odp…

112. Jaki profil standardu Bluetooth jest używany do zastąpienia łączności z wykorzystaniem łącza szeregowego RSZ….

a. PAN
b. SSP
c. AZDP
d. DUN

113. Element Traffic Indication Map (TIM)

a. ma zmienną długość, zależną od liczby stacji uczestniczących w transmisji
b. jest wysyłany w nagłówku MAC przez stacje do punktu dostępowego podczas procesu asocjacji
c. musi poprzedzać wysłanie przez stację ramki PS-Poll
d. posiada ścisły związek z polem AiD