1. Bezczynne skanowanie (Idle Scanning) obejmuje:

A.Przechwytywanie wszystkich pakietów wysłanych przez docelowy komputer
B.Wysłanie pakietu TCP SYN ze zmienionym adresem źródłowym do docelowego komputera
C.Sprawdzeniu numeru sekwencyjnego pakietów komputera zombie
D.Wysłanie pakietu TCP RST ze zmienionym adresem źródłowym do docelowego komputera

2. Termin konfuzja oznacza:

A. Złożoność obliczeniową algorytmu
B. Rozsianie bitów tekstu jawnego i klucza po szyfrogramie
C. Ukrycie zależności pomiędzy tekstem jawnym, szyfrogramem i kluczem
D. Niemożliwość wyprowadzenia klucza deszyfrującego z klucza szyfrującego

3. Które bilety lub klucze Kerberos używane są do uwierzytelniania użytkowników?

A. Bilet TGT
B. Bilet ST
C. Klucz SA
D. Klucz KAB

4. Słabymi punktami technologii WEP są:

A. Dołączanie sumy kontrolnej pakietu za pomocą operacji XOR
B. Brak mechanizmu zarządzania kluczami
C. Zbyt krótki wektor inicjujący
D. Algorytm RC4

5. Zarządzanie ryzykiem polega na (wybierz najlepszą odpowiedź):

A. Wykryciu zagrożeń, klasyfikacji zagrożeń, ocenie ryzyka i jego akceptacji
B. Wykryciu zagrożeń, klasyfikacji zagrożeń, ocenie ryzyka i przeniesieniu go na kogoś innego
C. Wycenie zasobów, klasyfikacji zasobów, ocenie i minimalizacji ryzyka
D. Wykryciu zagrożeń, klasyfikacji zagrożeń, ocenie i minimalizacji ryzyka

6. Izolacja sesji 0 oznacza, że:

A. Usługi systemowe działają w sesji uruchomianej przez pierwszego zalogowanego użytkownika
B. Niemożliwa jest komunikacja pomiędzy usługami systemowymi a programami uruchomianymi przez użytkowników
C. Usługi systemowe działają z obniżonymi uprawnieniami
D. Usługi systemowe działają w osobnej sesji

7. Które rozwiązanie pozwala zwiększyć siłę uwierzytelniania użytkowników łączących się z naszym serwerem za pomocą modemu?

A. Zapora sieciowa
B. Szyfrowanie 3DES
C. SSH-1 (Secure Shell)
D. Oddzwanianie (callback)

8. DNSSpoofing to atak:

A. Polegający na zamianie nazwy DNS atakowanego komputera
B. Polegający na zastąpieniu adresu IP komputera o danej nazwie DNS adresem IP innego komputera
C. Mający na celu zablokowanie usługi DNS
D. Bazujący na „zaufaniu" pomiędzy protokołami różnych warstw modeli OSI

9. Dane przesyłane za pomocą protokołu https:

A. Są szyfrowane kluczem publicznym zapisanym w certyfikacie serwera WWW
B. Są szyfrowane kluczem prywatnym zapisanym w certyfikacie serwera WWW
C. Są szyfrowane uzgodnionym podczas nawiązywania połączenia kluczem symetrycznym
D. Są szyfrowane kluczem publicznym klienta

10. Który protokół pozwala zabezpieczyć sieć bezprzewodową?

A. ESP (Encapsulating Security Payload)
B. WEP (Wired Equivalent Privacy)
C. TLS (Transport Layer Security)
D. SSL (Secure Sockets Layer)

11. Ataki socjotechniczne bazują na:

A. Wrodzonym nam zaufaniu
B. Rutynie pracowników
C. Braku zaufania do komputerów
D. Wrodzonej nam gotowości do udzielania pomocy

12. Podczas szyfrowania klucz prywatny jest używany do:

A. Zaszyfrowania danych
B. Podpisania danych
C. Zaszyfrowania kluczy symetrycznych
D. Podpisania kluczy symetrycznych

13. Model kontroli dostępu w którym obiekty są klasyfikowane w hierarchii zabezpieczeń to:

A. DAC (Discretionary Access Control)
B. RBAC (Role Based Access Control)
C. LBACs (List Based Access Control)
D. MAC (Mandatory Access Control)

14. Wymianę wyzwania i odpowiedzi (np. w celu uwierzytelnienia) rozpoczyna:

A. Wysłanie przez klienta zaszyfrowanego hasła użytkownika
B. Wysłanie przez klienta pseudolosowego ciągu bajtów zaszyfrowanego współdzielonym z serwerem sekretem
C. Wysłanie przez serwer zaszyfrowanego hasła użytkownika
D. Wysłanie przez serwer pseudolosowego ciągu bajtów zaszyfrowanego współdzielonym z klientem sekretem

15. Które technologie zapobiegają lub utrudniają atak polegający na przepełnieniu bufora:

A. DEP (Data Execution Prevention)
B. GC (Garbage Collector)
C. ASLR (Address Space Layout Randomization)
D. Flaga kompilatora /GS

16. Ochronę przed atakami przepełniania bufora dają:

A. Uruchamianie programów z uprawnieniami zwykłych użytkowników
B. Sprzętowe mechanizmy oznaczania pamięci zawierającej kod wykonywalny
C. Języki z silną kontrolą typów których kod jest sprawdzany przez środowisko uruchomieniowe przed wykonaniem
D. Opcje kompilatorów powodujące zapisywanie na stosie danych kontrolnych

17. Połączenie z serwerem WWW poprzez protokół https wymaga otwarcia na zaporze portu:

A. UDP (User Datagram Protocol) 80

B. TCP (Transmission Control Protocol) 80
C. UDP (User Datagram Protocol) 443
D. TCP (Transmission Control Protocol) 443

18. W którym trybie szyfrów blokowych każdy blok tekstu jawnego przed zaszyfrowaniem jest przekształcany funkcją XOR z szyfrogramem uzyskanym poprzez zaszyfrowanie poprzedniego bloku wiadomości?

A. Trybie elektronicznej książki kodowej ECB
B. Trybie łańcuchowego szyfru blokowego CBC
C. Trybie sprzężenia zwrotnego OFB
D. Trybie licznika CTR

19. Który protokół jest używany do zabezpieczenia komunikacji z serwerem WWW:

A. IPSec (Internet Protocol Security)
B. HTTP (Hypertext Transfer Protocol)
C. SSL (Secure Sockets Layer)
D. L2TP (Layer 2 Tunnelling Protocol)

20. Zasady ograniczeń oprogramowania pozwalają zidentyfikować programy na podstawie:

A. Sygnatur
B. Lokalizacji plików
C. Certyfikatów ich wydawców
D. Wykonywanych przez nie operacji

21. Przejęcie ciasteczka (cookies) to atak typu:

A. Footprinting
B. Spoofing
C. Denial of Service
D. Brute Force

22. Klucz systemu Windows (syskey) może:

A. Zostać zapisany na dyskietce
B. Zostać zapisany na dysku systemowym
C. Zostać zapisany na dysku USB
D. Być wyprowadzany z podawanego przez użytkownika hasła

23. Jakie programy wyszukują słabe punkty w bezpieczeństwie zdalnych komputerów?

A. Skanery luk np. Nessus
B. Systemy wykrywania włamań IDS np. 1SS
C. Skanery portów np. NetMap
D. Skanery antywirusowe np. AVG

24. Atak polegający na uzyskaniu takich samych sygnatur dla dwóch różnych wiadomości to:

A. Atak typu man in the middle
B. Atak pełnego przeglądu (Brute force)
C. Atak urodzinowy
D. Atak słownikowy

25. Główną wadą algorytmów symetrycznych jest:

A. Wydajność
B. Podatność na analizę częstości
C. Wymagania pamięciowe

D. Dystrybucja kluczy

26. Urządzenia biometryczne umożliwiają:

A. Uwierzytelnienie
B. Autoryzację
C. Rozliczenie
D. Certyfikacje

27. Które typy zagrożeń można wyeliminować za pomocą pasywnych zabezpieczeń?

A. S Spoofing identity (Fałszowanie tożsamości)
B. T Tampering with data (Modyfikowanie danych)
C. R Repudiability (Zaprzeczalność)
D. D Denial of Service (Odmowa obsługi)

28. Polityka bezpieczeństwa:

A. Powinna uwzględniać informacje od użytkowników
B. Powinna być dokładnym wdrożeniem gotowych szablonów zabezpieczeń
C. Nie musi być monitorowana
D. Nie musi być aktualizowana

29. Wyrażenie regularne A[A-Za-z9-0]{l,32} jest zgodne z:

A. Ciągiem znaków „Marcin"
B. Ciągiem znaków „TajneHasłol23"
C. Pustym ciągiem znaków
D. Ciągiem znaków „P@sswOrd"

30. Które rozwiązanie najskuteczniej chroni przed przejęciem tożsamości?

A. Tunel VPN
B. Wymuszenie stosowanie silnych haseł
C. Hasła jednorazowe
D. Protokół SSH