

Zagadnienia testu egzaminacyjnego z przedmiotu *Bezpieczeństwo systemów informacyjnych*

1. Podstawowe pojęcia z zakresu bezpieczeństwa.
2. Dokumenty normatywne związane z bezpieczeństwem systemów informatycznych. Charakterystyka i umiejscowienie w czasie.
3. Konstruowanie polityki bezpieczeństwa.
4. Wybrane zagrożenia sieciowe i ich charakterystyka
 - *Sniffing*.
 - *Spoofing*.
 - *Hijacking*.
 - *Denial of Service*.
 - Złośliwe programy.
5. Testy penetracyjne.
 - Cele i fazy testów penetracyjnych.
 - Cele i techniki skanowania.
 - Cele i techniki enumeracji.
 - Zdalne rozpoznawanie systemów operacyjnych.
6. Podstawy kryptografii.
 - Podstawowe algorytmy kryptograficzne.
 - Podpis cyfrowy.
 - Dystrybucja kluczy kryptograficznych.
 - Infrastruktura klucza publicznego.
7. Systemy uwierzytelniania użytkowników.
 - Podstawowe metody uwierzytelniania.
 - Standard X.509.
 - System Kerberos.
8. Mechanizmy kontroli dostępu.
9. Bezpieczne protokoły: IPSec, SSL, TLS, S-HTTP, SSH, , PPTP, L2TP.
10. Zapory sieciowe (*firewalls*).
 - Konfiguracje.
 - Filtrowanie pakietów.
 - Translacja adresów.
 - Serwery *proxy*.
 - Proces budowania zapory.
11. Systemy wykrywania włamań i pułapki internetowe.
 - Struktura systemów wykrywania włamań.
 - Metody wykrywania włamań.
 - Funkcje i zasady działania pułapek.
 - Metody „rozstawiania” pułapek.
12. Ochrona poczty elektronicznej.
 - Zagrożenia wewnętrzne i zewnętrzne systemu pocztowego.
 - Metody i narzędzia ochrony.

Przykładowe pytania testu końcowego z przedmiotu BSI

1. Który wariant określa uporządkowanie poziomów bezpieczeństwa systemów od najbardziej do najmniej bezpiecznych:
 - A. A1 B2 B1 C2 C1 D
 - B. A1 B1 B2 C1 C2 D
 - C. D C1 B1 A1
 - D. A1 B1 B2 C2 C1 D

2. Kategorie bezpieczeństwa: Ochronę świadczonych usług przed zniekształceniem i uszkodzeniem nazywamy:
 - A. zabezpieczeniem dostępności
 - B. zabezpieczeniem spójności danych
 - C. zabezpieczeniem poufności
 - D. audytem

3. Która z poniższych grup zawiera wyłącznie nazwy algorytmów szyfrowania z kluczem asymetrycznym:
 - A. RSA, DSA, ElGamal
 - B. DSA, DES, ElGamal
 - C. DSA, RC4, IDEA
 - D. IDEA, DES, RC2

4. Zadaniem serwera przyznawania biletów (*ticket-granting server*) w systemie Kerberos jest:
 - A. wydawanie zezwoleń na korzystanie z usług serwera aplikacji
 - B. sprawdzanie tożsamości użytkowników i wydawanie biletów uprawniających do korzystania z usługi przyznawania biletów
 - C. dostarczanie klientom żądanych przez nich usług w zakresie dostępu do plików
 - D. rejestrowanie realizowanych połączeń

5. *Spoofing* ARP powoduje fałszowanie:
 - A. skojarzeń <adres sprzętowy-adres IP>
 - B. skojarzeń <adres sprzętowy-nazwa hosta>
 - C. skojarzeń <adres IP-nazwa hosta>
 - D. haseł użytkownika