Zagadnienia do egzaminu: Ochrona danych i bezpieczeństwo systemów informatycznych

1. Definicja danych, ich typy i zastosowania
2. Rodzaje zagrożeń dla danych
3. Idea i składniki polityki bezpieczeństwa
4. Przyczyny tracenia danych i metody zapobiegawcze
5. Systemy ciągłej ochrony danych
6. Istota regulacji prawnych ACTA
7. Podstawowe zagrożenia w bezpieczeństwie teleinformatycznym
8. Metody szyfrowania informacji analogowych i cyfrowych
9. Pojęcie scramblingu i jego typy
10. Podstawowe elementy bezpieczeństwa telefonii GSM
11. Ataki radioelektroniczne i zasady zapobiegania im
12. Podstawowe ataki na zasoby firmy i ich konsekwencje
13. Zadania administratora bezpieczeństwa w firmie lub instytytucji
14. Istota cyklu Deminga
15. Składniki reguł polityki bezpieczeństwa
16. Zadania modelu CIA
17. Najważniejsze technologie bezpieczeństwa w firmach
18. Dedykowane, a zintegrowane technologie bezpieczeństwa
19. Technologie składowe UTM
20. Zalet i wady technologii UTM
21. Istota wykrywania komputerów i usług w sieci
22. Narzędzia śledzenia ścieżek danych
23. Widoczność wejściowa, a widoczność wyjściowa hostów
24. Sposoby ukrywania skanowania
25. Metody destabilizacji systemu
26. Zasady podszywania się – spoofing
27. Zasady oszukiwania IDS
28. Składniki listy kontrolnej bezpieczeństwa
29. Funkcje bezpieczeństwa Windows XP Pro i nowszych
30. Składniki profilu atakowanego komputera
31. Elementy ochrony systemów Windows
32. Funkcje Active Directory w aspekcie bezpieczeństwa
33. Zadania protokołu Kerberos
34. Zastosowania dynamicznego DNS (DDNS)
35. Etapy ataku na Active Directory
36. Składniki listy kontrolnej zabezpieczeń Active Directory
37. Wykorzystanie serwerów DNS w atakach i stosowane zabezpieczenia
38. Procedury ataku na hosty Unix
39. Zasady przygotowania bezpiecznego systemu Unix