

Egzamin z BSK, 27 stycznia 2010 r.

Imię i nazwisko: ..... Nr indeksu: .....

Odpowiedzi *tylko na temat* proszę pisać *wyraźnie* na otrzymanym formularzu.

1. [2 pkt.] Wymień słabości, z punktu widzenia bezpieczeństwa, protokołu TCP.
2. [2 pkt.] Co to jest aplikacja pośrednicząca (ang. proxy service)?
3. [2 pkt.] Co to jest bomba logiczna?
4. [2 pkt.] Wymień pożądane cechy kryptograficznej funkcji skrótu.
5. [2 pkt.] Jak w praktyce chroni się poufność poczty elektronicznej?
6. [2 pkt.] Wymień zalety i wady trybów ECB, CBC i licznikowego w zastosowaniu do szyfrowania urządzeń dyskowych za pomocą szyfru blokowego.

7. [2 pkt.] IPsec używa bezpołączeniowego protokołu IP – każdy pakiet jest przetwarzany indywidualnie. Skąd zatem odbiorca pakietu wie, jakiego klucza użyć do jego odszyfrowania?

8. [2 pkt.] Czy uwierzytelnianie jednokierunkowe chroni podmiot uwierzytelniający się przed atakiem typu człowiek w środku (ang. man in the middle)? Odpowiedź krótko uzasadnij.

9. [2 pkt.] Na czym polega wstrzykiwanie kodu SQL?

10. [2 pkt.] Wymień obszary zastosowań systemów RFID.

11. [2 pkt.] Wymień słabości protokołu Kerberos.

12. [2 pkt.] W jaki sposób w protokole SSH serwer uwierzytelnia się wobec klienta?