

## 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 IP w wersji 4.
2. [2 pkt.] Zdefiniuj w jednym zdaniu filozofię, która powinna przyświecać tworzeniu reguł ściany ogniowej lub przydziałowi uprawnień użytkownikom.
3. [2 pkt.] Co to jest boczne wejście do programu?
4. [2 pkt.] Czy, znając klucz publiczny RSA, można obliczyć odpowiadający mu klucz prywatny?
5. [2 pkt.] Jak w praktyce chroni się integralność danych?
6. [2 pkt.] Wymień zalety i wady trybów ECB, CBC i licznikowego przy szyfrowaniu plików dyskowych za pomocą szyfru blokowego.

7. [2 pkt.] Jak można wykorzystać błąd przepełnienia bufora w implementacji serwera jakiejś usługi do uzyskania uprawnień administratora systemu, na którym uruchomiony jest ten serwer?

8. [2 pkt.] Co chroni uwierzytelnianie metodą zawołanie-odzew (ang. challenge-response) przed atakiem powtórzeniowym?

9. [2 pkt.] Dlaczego nie powinno się wydawać certyfikatów poświadczających prawdziwość klucza publicznego z nieskończonym okresem ważności?

10. [2 pkt.] Dlaczego zamiast opracować bezpieczne (umożliwiające uwierzytelnianie i szyfrowanie komunikacji) wersje protokołów takich jak SMTP czy HTTP, stosuje się ich tunelowanie w SSL/TLS?

11. [2 pkt.] W jaki sposób w protokole Kerberos serwer uwierzytelniający broni się przed fałszywym klientem, próbującym podszyć się pod uprawnionego klienta, proszącym o wydanie biletu do usługi przyznawania biletów?

12. [2 pkt.] W jaki sposób błąd w implementacji klienta DNS, polegający na ignorowaniu czasu ważności uzyskanych rekordów, umożliwia darmowe korzystanie z płatnych punktów dostępowych (ang. hot spot) Wi-Fi?