Bezpieczeństwo sieci komputerowych, MSUI
Egzamin końcowy, 10 czerwca 2008

Imię i nazwisko: .....
.....

W każdej kratce należy wpisać literę T lub N w zależności od tego, czy odpowiedź się zgadza, czy nie, np:

1. Pan Samochodzik to

   [N] **A** model Opla;

   [N] **B** bohater powieści Ernesta Hemingwaya;

   [T] **C** bohater powieści młodzieżowej.

W poniższym teście możliwa jest każda konfiguracja odpowiedzi T, N. Skala ocen: 10 na 3, 12 na 3+, 14 na 4, 16 na 4+, 18 na 5.

1. W nieadaptywnym ataku z wybranym tekstem jawnym:

   [ ] **A** atakujący może poznać szyfrogram dla wybranego tekstu jawnego

   [ ] **B** atakujący może wybrać tekst jawny w trakcie ataku

   [ ] **C** atakujący może wybrać wiele tekstów jawnych przed rozpoczęciem ataku

2. Najmniej bezpiecznym trybem szyfrowania blokowego jest:

   [ ] **A** CBC (*Cipher Block Chaining*)

   [ ] **B** OFB (*Output Feedback*)

   [ ] **C** ECB (*Electronic Code Book*)

3. Protokół SSL:

   [ ] **A** służy wyłącznie do zabezpieczania połączeń HTTP

   [ ] **B** umożliwia ustalenie klucza sesji gdy żadna ze stron nie posiada certyfikatu

   [ ] **C** umożliwia ustalenie klucza sesji w oparciu o certyfikat serwera i kryptografię klucza publicznego

4. W protokole SSL sposób szyfrowania dla danej sesji:

   [ ] **A** jest ustalony w certyfikacie serwera

   [ ] **B** wybiera klient z listy zaoferowanych przez serwer

   [ ] **C** klient serwer z listy zaoferowanych przez klienta

5. Protokół SSH:

   - [ ] **A** służy wyłącznie do nawiązywania interaktywnych sesji terminalowych
   - [ ] **B** może służyć do tunelowania dowolnego połączenia TCP na zasadach podobnych do SSL
   - [ ] **C** ma wbudowane tunelowanie protokołu X Window

6. W protokole SSH:

   - [ ] **A** algorytmy szyfrowania, hasha kryptograficznego i kompresji są ustalane niezależnie dla każdego kierunku transmisji
   - [ ] **B** protokół transportu odpowiada za uwierzytelnienie stron
   - [ ] **C** protokół połączenia pozwala na tunelowanie połączeń TCP

7. Zakładając, że usługi o których mowa działają na standardowych portach, administrator sieci może konfigurując firewall zablokować użytkownikom sieci:

   - [ ] **A** dostęp do zewnętrznych serwerów HTTP używając filtrowania statycznego
   - [ ] **B** dostęp do określonej strony na określonym serwerze używając filtrowania dynamicznego
   - [ ] **C** dostęp do wskazanego zewnętrznego serwera SSH z użyciem określonej nazwy użytkownika, używając filtrowania opartego o proxy

8. Stwierdzenia prawdziwe dla maskarady:

   - [ ] **A** adres źródłowy w pakietach wychodzących z sieci lokalnej ulega zmianie
   - [ ] **B** adres źródłowy w pakietach przychodzących do sieci lokalnej ulega zmianie
   - [ ] **C** różnym adresom lokalnym przypisywane są różne adresy zewnętrzne

9. Pakiety między nadawcą a odbiorcą przechodzą przez NAT i podlegają translacji adresów. W takiej sytuacji w IPsec można skutecznie stosować:

   - [ ] **A** tryb tunelowy ESP
   - [ ] **B** uwierzytelnianie wraz z trybem transportowym ESP
   - [ ] **C** uwierzytelnianie przed szyfrowaniem

10. Protokół IPSec:

    - ☐ **A** służy do zapewnienia bezpiecznej komunikacji na poziomie warstwy sieci
    - ☐ **B** pozwala korzystać z uwierzytelniania bez szyfrowania
    - ☐ **C** pozwala korzystać z uwierzytelniania wraz z szyfrowaniem

11. W SNMPv2 środki zapewniania bezpieczeństwa mogą zapewnić:

    - ☐ **A** ochronę przed analizą ruchu
    - ☐ **B** poufność
    - ☐ **C** uwierzytelnienie

12. Baza danych stron w SNMPv2 zawiera dla zdalnej strony:

    - ☐ **A** informację o używanym algorytmie szyfrowania
    - ☐ **B** jej aktualny czas (zegar)
    - ☐ **C** listę pól MIB, do których strona ma dostęp

13. Zmodyfikowany schemat Needhama-Schrödera:

    - ☐ **A** wymaga od serwera uwierzytelnienia (*authentication server*) znajomości hasła-klucza zleceniodawcy
    - ☐ **B** wymaga od serwera przepustek (*tickets server*) znajomości hasła-klucza zleceniodawcy
    - ☐ **C** wymaga od zleceniodawcy znajomości hasła-klucza serwera usługi

14. Kerberos 4:

    - ☐ **A** korzysta z szyfrowania symetrycznego DES
    - ☐ **B** korzysta z szyfrowania z kluczem publicznym RSA
    - ☐ **C** korzysta z dwóch rodzajów serwerów Kerberosa, które mogą być umieszczone na różnych maszynach

15. W PGP w przypadku wiadomości podpisanej, nie zaszyfrowanej:

    - ☐ **A** nadawca musi posiadać certyfikat podpisany przez jednostkę certyfikującą
    - ☐ **B** odbiorca musi posiadać certyfikat podpisany przez jednostkę certyfikującą
    - ☐ **C** skrót (*hash*) wiadomości szyfruje się kluczem prywatnym nadawcy

16. PGP zapewnia

- ☐ **A** możliwość uzyskania przez odbiorcę pewności, że osoba wysyłająca nie wyprze się, iż go wysłała
- ☐ **B** możliwość uzyskania poprzez wysłanie listu pewności, że osoba odbierająca nie wyprze się, iż go otrzymała
- ☐ **C** możliwość uzyskania pewności, że wiadomość zostanie odczytana tylko przez uprawnionego odbiorcę

17. Zabezpieczenie „przez znacznik" w DHCP:

- ☐ **A** chroni przed wyczerpaniem całej puli adresów IP przez złośliwego klienta
- ☐ **B** używa technik kryptograficznych do ochrony przed podsłuchaniem hasła-znacznika
- ☐ **C** w pewnym stopniu chroni przed atakami intruzów nie mających wcześniejszego dostępu do danej sieci

18. W DHCP (bez pośrednika) zabezpieczonym przez „uwierzytelnienie z opóźnieniem":

- ☐ **A** stosowane są bezpieczne funkcje haszujące
- ☐ **B** intruz może obciążyć obliczeniowo serwer
- ☐ **C** intruz może wyczerpać pulę adresów IP

19. Dlaczego algorytmu RSA zazwyczaj nie używa się bezpośrednio do szyfrowania dużych porcji danych?

- ☐ **A** ponieważ algorytm pozwala szyfrować jedynie porcje danych o długości 384 (wersja zwykła), 512 (wersja komercyjna) lub 1024 (wersja wojskowa) bitów
- ☐ **B** jest on istotnie wolniejszy od algorytmów symetrycznych
- ☐ **C** przy dużych blokach danych jest on istotnie bardziej narażony na odszyfrowanie niż algorytmy symetryczne

20. MAC (*Message Authentication Code*):

- ☐ **A** jego wygenerowanie wymaga znajomości hasła/klucza
- ☐ **B** jego weryfikacja wymaga znajomości hasła/klucza
- ☐ **C** algorytm służący generowaniu i weryfikacji MAC można uzyskać za pomocą schematu CMAC z algorytmu szyfru blokowego spełniającego pewne wymagania