**Bezpieczeństwo systemów informatycznych**

Test 1

1. Podstawowe pojęcie o bezpieczeństwie systemów informatycznych
2. Różnice w implementacji ICMP
3. Ataki poprzez zalew pakietów
4. Wymienić wybrany modele ochrony
5. Rozwiązania typu NIDS

Test 2

1. Wybrane pojęcia bezpieczeństwa informatycznego
2. Zjawisko sniffingu
3. Zalew SYN (SYN Flooding)
4. Funkcjonowanie kontroli dostępu
5. System typu NNIDS

Test 3

1. Dokumenty standaryzujące stosujący się bezpieczeństwa
2. Techniki wykrywania sniferów
3. Atak land, Smurf, Fraggle
4. Kanały ukryte
5. Klasyfikacja IDS według metod analizy

Test 4

1. Metody przeciwdziałania zagrożeniom i klasyfikacja metod ochrony
2. Spoofing,
3. Rozproszone ataki DoS
4. Bezpieczne protokoły sieciowe, [IPSec](http://edu.pjwstk.edu.pl/wyklady/bsi/scb/index70.html)
5. Klasyfikacja IDS według typów odpowiedzi

Test 5

1. Enumeracja Windows
2. Spoofing ARP
3. Kryptograficzne metody ochrony informacji
4. Baza SPD
5. Podjęcie akcji przeciwko intruzowi.

Test 6

1. SNMP (Simple Network Management Protocol)
2. Spoofing usługi routingu
3. Algorytmy szyfrowania z kluczem tajnym
4. Tryb transportowy
5. Pułapki SNMP.

Test 7

1. DNS i SID
2. Spoofing DNS
3. ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher FeedBack), OFB (Output FeedBack)
4. Tryb tunelowy
5. Typowe symptomy działania intruzów

Test 8

1. Przechwytywanie etykiet
2. Scenariusz ataku na serwer dns1.firma.com
3. Algorytmy szyfrowania z kluczem publicznym
4. Podstawowe protokoły negocjacji i dystrybucji:
5. Pułapki internetowe

Test 9

1. Enumeracja systemu Linux
2. Scenariusz ataku na serwer dns1.firma.com
3. Algorytmy skrótu
4. L2TP i PPTP
5. Bezpieczeństwo poczty elektronicznej

Test 10

1. NFS (Network File System).
2. Obrona przed atakiem
3. Podpis cyfrowy
4. Protokół PPTP
5. Atrybuty bezpiecznego systemu pocztowego

Test 11

1. Idea testów penetracyjnych
2. Porywanie sesji (hijacking)
3. Dystrybucja kluczy kryptograficznych
4. Protokół L2TP
5. Zagrożenia dla bezpieczeństwa systemu przekazywania poczty

Test 12

1. Metody i techniki rekonesansu
2. Wczesna desynchronizacja
3. Infrastruktura klucza publicznego, PKI (Public Key Infrastructure)
4. Protokół SSL i TLS
5. Zagrożenia umożliwiające manipulację autorstwem przesyłki:

Test 13

1. Techniki skanowania
2. Desynchronizacja za pomocą pustych danych
3. Podstawowe elementy występujące w certyfikacie
4. Zapory sieciowe firewall
5. Zagrożenia dla dostępności przesyłki lub systemu pocztowego

Test 14

1. Skanowanie ICMP
2. Obrona przed atakiem
3. Systemy uwierzytelniania
4. Filtrowanie pakietów
5. Zagrożenia bezpieczeństwa na zewnątrz

Test 15

1. Skanowanie TCP
2. Porywanie sesji (hijacking)
3. Słowniki haseł, ochrona haseł
4. Filtrowanie portów lub filtrowaniem protokołów wyższych warstw
5. Konie trojańskie

Test 16

1. Techniki specjalne TCP
2. Wczesna desynchronizacja
3. Bezpieczne przechowywanie haseł
4. Filtry z badaniem stanu
5. Protokoły pocztowe a bezpieczeństwo

Test 17

1. Skanowanie UDP
2. Desynchronizacja za pomocą pustych danych
3. Systemy haseł jednorazowych
4. Translacja adresów
5. Zagrożenia związane z protokołem POP3 i IMAP4

Test 18

1. Różne techniki skanowania
2. Obrona przed 2 wybranymi atakami
3. System Kerberos
4. Usługi proxy
5. Rozwiązania zwiększające bezpieczeństwo systemu pocztowego

Test 19

1. Ukrywanie skanowania
2. Ataki odmowy usługi (Denial of Service):
3. Wymiana informacji między klientem (C1) i serwerem przepustek (TGS)
4. Etapy budowy zapory, planowanie konfiguracji zapory sieciowej
5. Polityka bezpieczeństwa

Test 20

1. Zdalna identyfikacja systemu operacyjnego
2. Wykorzystanie fragmentacji pakietów
3. Wymiana informacji między klientem (C1) i serwerem aplikacji (S1)
4. Wykrywanie intruzów,[koncepcja systemów wykrywania intruzów](http://edu.pjwstk.edu.pl/wyklady/bsi/scb/index84.html)
5. Zadania zespołu d/s bezpieczeństwa

Test 21

1. Analiza stosu TCP/IP
2. Ataki Ping of Death i Teardrop
3. Kontrola dostępu, macierz dostępów
4. Klasyfikacja IDS według źródeł informacji
5. Procedura tworzenia polityki bezpieczeństwa

Test 22

1. Obsługa fragmentacji
2. Nakładanie fragmentów (Fragment Overlapping)
3. Etykiety poziomów zaufania
4. Rozwiązania typu NIDS
5. Drzewa zdarzeń i drzewa błędów