Zebrane pytania z Egzaminu BSI z dnia 9 lutego 2011	
_Pytania:	**Odpowiedzi:**
Algorytm IDEA	IDEA jest algorytmem szyfrowania konwencjonalnego ze 128 bitowym kluczem działający na blokach 64bit
Algorytmy z klucze tajnym:	DES, Blowfish, IDEA (International Data Encryption Algorithm), RC4, SAFER, Algorytmy bazujące na funkcji hashującej
Co to jest Kerberowanie systemu?	Integrowanie z innymi czesciami systemu.
Co to jest Kryptoanaliza?	Nauka o łamaniu szyfrów.
Co to jest Kryptologia?	Nauka o szyfrowaniu.
Co to jest protokół X.509?	Jest to standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu
Co trzeba zrobić aby mieć C2 (Kontrola Dostępu)	C2 - kontrola dostępu, trzeba mieć D(ochrona minimalna) i C1(ochrona uznaniowa) || D,C1,C2,B1,B2,B3,A1 ROSNĄCO
Co zapewnia nagłówek ESP?	Uwierzytelnianie, Integralnosc, Poufnosc
Co zapewnia PPTP?	Uwierzytelnianie, Kompresję, Kapsułkowanie
Czym jest Kerberos?	Weryfikacja i sprawdzanie tożsamości.
Czym zajmuje się authentication serwer w systemie Kerberos?	Wydawaniem biletów i sprawdzanem tożsamości.
DNS poisoning:	Technika phishingu polegająca na wysłaniu do serwera DNS fałszywego rekordu kojarzącego nazwę domeny z adresem IP
Do czego służy skrót wiadomości	Do stwierdzenia autentycznosci (integralnosci) wiadomości.
Filtrowanie bezstanowe	Zapory sieciowe; Odrzuca na podstawie analizy pojedynczych pakietów.
Filtrowanie stanowe	Zapory sieciowe; Analizuje nie tylko pakiety, ale również ogólny ruch w sieci.
HASP NASP	Przeglądanie, logów w systemie aby wykryć anomalie/włamanie zajmuje się
ISO	PN ISO/IEC 27001:2007 oraz PN ISO/IEC 17799:2007.
Kolejność pakietów w IPSec:	Tunelowanie PRZED, Transportowanie PO
Księga czerwona	Kryteria oceny bezpieczeństwa sieciowego.
Księga pomarańczowa	Bezpieczeństwo systemu.
Księga zielona	Hasła
Który z algorytmów szyfrowania używa klucza publicznego?	(EIN),DSA,RSA.ELGAMAL
Metoda nadużyć	???
Metoda udostępniania kluczy	???
Nagłówek AH:	Uwierzytelnianie, Integralność.
Nagłówki IPSec	Nagłówek ESP
Orange Book	Porzadkowanie
Protokół cerbera:	KDC szyfruje klucz sesyjny, przesyła Abonentowi 1 inf. zaszyfrowaną kluczem 2. Ab.1 wysyła Ab.2 inf., Obaj abonenci posiadają klucz .
Rozwiń skrót IDS.	Intrusion Detection System
Serwer FTP działa domyślnie na porcie:	21
SHAMIRA	2 osoby ,asymetryczny, inaczej RSA, deszyfrowanie - klucz prywatny,
Skanowanie pół otwarte:	Polega na wyslaniu przez klienta zapytania w postaci pojedynczego pakietu SYN na odpowieni port
Skanowanie TCP FIN	Metoda polegająca na przesłaniu do zdalnego portu pakietu z flagą FIN , wymusza odpowiedz RST
Spoofing ARP	Fałszowanie relacji, weryfikacja pytania ARP przezRARP
Spoofing DNS	Podszywanie sie pod serwer DNS
Szyfrujemy waidomość czy skrót wiadomości?	Wiadomość
Ticket Granting	Wydawanie zezwoleń na korzystanie z usług serwera aplikacji
W Której warstwie znajduje się IPSec?	Warstwa: 3 (sieciowa)
W Której warstwie znajduje się SSL?	Warstwa: 4 (transportu)