ZAKRES TEMATYCZNY Z WYKŁADU

Zarządzanie kluczami i ich dystrybucja.

Wymień sposoby dostarczania klucza sesji komunikującym się partnerom. Jaka jest różnica między kluczem sesji a kluczem nadrzędnym? Co to jest centrum dystrybucji kluczy? Wymień dwa sposoby wykorzystywania kryptografii z kluczami publicznymi na potrzeby dystrybucji kluczy. Wymień cztery główne kategorie schematów dystrybucji kluczy publicznych. Jakie są zasadnicze elementy infrastruktury kluczy publicznych? Co to jest certyfikat klucza publicznego? Z czym związany jest standard X.509? Co to jest ścieżka certyfikacyjna? W jaki sposób w świetle uregulowań standardu X.509 unieważnia się certyfikat klucza?

Uwierzytelnianie użytkowników.

Z intencją rozwiązania jakich problemów zaprojektowano Kerberos? Jakie są trzy główne zagrożenia związane z uwierzytelnianiem użytkowników w sieciach komputerowych i w Internecie? Wymień trzy podejścia do bezpieczeństwa uwierzytelniania użytkowników w środowisku rozproszonym. Jakie cztery główne wymagania postawione zostały przed projektowanym systemem Kerberos? Jakie encje składają się na środowisko Kerberosa? Co oznacza pojęcie tożsamość federacyjna?

Bezpieczeństwo transportu danych.

Jakie podprotokoły składają się na protokół SSL? Wymień parametry składające się na stan połączenia SSL i krótko wyjaśnij ich znaczenie. Wymień parametry składające się na stan sesji SSL i krótko wyjaśnij ich znaczenie. Jakich usług dostarcza podprotokół rekordu SSL? Jakie kroki składają się na akcję podprotokołu rekordu SSL? Jakie jest zadanie protokołu HTTPS? Dla jakich aplikacji użyteczny jest mechanizm SSH? Wymień protokoły składające się na mechanizm SSH i krótko wyjaśnij ich rolę.

Bezpieczeństwo sieci bezprzewodowych.

Jakie są podstawowe komponenty sieci bezprzewodowej standardu IEEE 802.11? Wymień i krótko zdefiniuj usługi standardu IEEE 802.11. Jakie aspekty bezpieczeństwa uwzględnione zostały w standardzie IEEE 802.11i? Opisz krótko cztery fazy operacji IEEE 802.11i. Jaka jest różnica między filtrem HTML a proxy WAP? Jakie usługi udostępniane są przez WSP? Wymień i krótko zdefiniuj usługi bezpieczeństwa oferowanie przez WTLS. Opisz krótko cztery podprotokoły protokołu WTLS. Wymień i krótko zdefiniuj klucze używane przez protokół WTLS.

Bezpieczeństwo poczty elektronicznej.

Wymień pięć podstawowych usług oferowanych przez PGP. Na czym polega konwersja R64? Jaką rolę spełnia konwersja R64 w aplikacjach e-mail? W jaki sposób PGP realizuje koncepcję zaufania? Co to jest MIME? Co to jest S/MIME? Co to jest DKIM?

Bezpieczeństwo protokołu IP.

Podaj przykłady zastosowań IPsec. Jakie usługi oferuje IPsec? Jakie są różnice między trybem transportowym a trybem tunelowym? Na czym polega atak powtarzania? Jaka jest rola pola dopełnienia w pakiecie ESP?

Szkodliwe oprogramowanie.

Wymień i krótko scharakteryzuj trzy kategorie intruzów. Jakie są podstawowe techniki ochrony plików z hasłami? Jakie trzy główne korzyści wynikają ze stosowania systemu detekcji włamań? Co to jest honeypot? Czemu służy kompresja wykonywana przez wirusy? W jakim celu wirusy wykorzystują szyfrowanie? Jakie są fazy cyklu życiowego typowego wirusa i robaka? Co to jest system odporności cyfrowej? Jak działa blokowanie podejrzanych zachowań? Jakie są metody rozprzestrzeniania się robaków? Jakie są metody walki z robakami? Co oznacza skrót DDoS? Scharakteryzuj przykładowe ataki DDoS?

Firewalle.

Wymień trzy cele projektowania firewalli. Wymień cztery techniki wykorzystywane przez firewalle w celu kontrolowania dostępu i wymuszania reguł polityki bezpieczeństwa. Jakie informacje wykorzystywane są w ramach typowego filtrowania pakietów. Jakie są niedostatki firewalli wykonujących wyłącznie proste filtrowanie pakietu. Co to jest brama aplikacyjna? Co to jest brama transmisyjna? Co to jest strefa DMZ i jakiego typu systemy powinny się w niej znajdować? Jaka jest różnica między firewallem zewnętrznym a firewallem wewnętrznymi. Omówić przykłady zastosowań stref zmilitaryzowanych i bastionów. Korzystając z dowolnych źródeł, omówić implementację ściany ogniowej. Architektury ścian ogniowych.

ZAKRES TEMATYCZNY Z LABORATORIUM

Dokonać analizy trzech przykładowych ataków na warstwę II modelu ISO/OSI. W jaki sposób realizowane są ataki typu DDoS? Przeanalizować ich efektywność oraz skuteczność metody ochrony przed nimi. Sklasyfikować testy penetracyjne - jaki jest cel ich wykorzystania oraz skuteczność? Opisać budowę i funkcje skanerów luk zabezpieczeń - wymienić ich wady oraz zalety. Przedstawić kompleks działań mających na celu uchronienie osoby przed oszustwami wykorzystującymi podejście socjotechniczne. Wybrać i opisać atak socjotechniczny, którego celem jest wyłudzenie informacji. Scharakteryzować podatność systemu informacyjnego przedsiębiorstwa na poszczególne typy zagrożeń. Na jakie zagrożenia należy zwracać szczególną uwagę dla wybranego przedsiębiorstwa.