1. Podstawowe pojęcia z zakresu bezpieczeństwa.
   Kategorie bezpieczeństwa:
   Poufność – ochrona danych przed odczytem i kopiowaniem przez osobę nieupoważnioną. Jest to ochrona nie tylko całości danych, ale również ich fragmentów.
   Spójność danych – ochrona informacji przed usunięciem lub jakimkolwiek nieuprawnionymi zmianami np. zapisy systemu rozliczania, kopie zapasowe, atrybuty plików.
   Dostępność – ochrona świadczonych usług przed zniekształceniem i uszkodzeniem.

   Orange Book:
   D -Ochrona minimalna (Minimal Protection)
   C - Ochrona uznaniowa (Discretionary Protection)
   C2 - Ochrona z kontrolą dostępu (Controlled Access Protection)
   B - Ochrona z etykietowaniem (Labeled Security Protection)
   B2 - Ochrona strukturalna (Structured Protection)
   B3 - Ochrona przez podział (Security Domains)
   A - Konstrukcja zweryfikowana (Verified Design)

   Czerwona Księga:
   Zawiera kryteria oceny bezpieczeństwa sieci komputerowych.

   Zielona Księga:
   Zawiera wytyczne dotyczące stosowania i wykorzystania haseł.

   Common Criteria:
   CC mają na celu wprowadzenie ujednoliconego sposobu oceny systemów informatycznych pod względem bezpieczeństwa.
   Określają, co należy zrobić, aby osiągnąć żądany cel ale nie jak to zrobić
   CC są katalogiem schematów konstrukcji wymaga związanych z ochroną informacji.
   CC odnoszą się do produktów programowych i sprzętowych.
   CC nie zalecają ani nie wspierają żadnej znanej metodyki projektowania i wytwarzania systemów.
   Wynikiem oceny jest dokument stwierdzający zgodność produktu z określonym profilem ochrony lub, spełnienie określonych wymagań bezpieczeństwa lub, przypisanie do konkretnego poziomu bezpieczeństwa

2. Dokumenty normatywne:
   1.Ustawa z dn. 22.0 .999 O ochronie informacji niejawnych (1999)
   2.Ustawa z dn. 29.08.997 O ochronie danych osobowych. (1997)
   3.Rozporządzenie Prezesa Rady Ministrów W sprawie podstawowych wymaga bezpieczeństwa systemów i sieci teleinformatycznych (1999)
   4.Rozporządzenie MSWiA W sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiada urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (1998)
   5.Kodeks karny i przestępczość komputerowa (art.267-292)

3. Konstruowanie polityki bezpieczeństwa:
4. Wybrane zagrożenia sieciowe i ich charakterystyka:
   Sniffing: sniffer - jest to program, który jest uruchomiony na jakieś maszynie w sieci i "podsłuchuje" (przechwytuje) pakiety, które są przesyłane. Jest to coś podobnego do podsłuchu na linii telefonicznej tyle, że sniffer jest umieszczany na jednej z maszyn w sieci.
   Jak działa sniffer?
   -sniffer (przeważnie) przestawia kartę sieciową w tryb PROMISCIUOUS (mieszany) aby karta odbierała wszystkie pakiety wędrujące w sieci (segmencie sieci) nie tylko te, które są przeznaczone dla niej.
   - przechwytuje pakiety przesyłane w sieci (przeważnie określone np.: z danego hosta)
   Sniffera możemy użyć do:
   - przechwycenia przesyłanego niezaszyfrowanego tekstu (np.: haseł i loginów użytkownika używającego telneta itp.)
   - konwersja danych (pakietów) na zrozumiałe dla człowieka informacje

- podsłuchiwanie ruchu w sieci (z jakimi serwerami łączy się dana maszyna w sieci)
- analizowanie problemów w sieci np.: dlaczego maszyna A nie może nawiązać połączenia z maszyną B?
- logowanie ruchu w sieci (wykrywanie włamań), aby stworzyć logi, do których haker nie może się włamać ani usunąć

Inne cechy:
-może "podsłuchiwać" tylko w segmencie sieci, w którym się znajduje, czyli "nie przejdzie": węzłów komputerowych(switch-ów), routerów ani mostów sieciowych(brige-y)
-działający w sieci gdzie panuje "duży ruch" może skutecznie go zwolnić, a w przypadku zapisywania przez sniffer przechwyconych danych na dysk może go w nawet szybkim czasie zapełnić (zależy od pojemności)
-aby uruchomić sniffera jest potrzebny dostęp do konta root

Spoofing: oznacza podszywanie się pod inną maszynę w sieci. Narażone na to zjawisko są warstwy: sprzętowa, interfejsu danych, transportowa aplikacji. Wszystkie protokoły warstwy aplikacji są narażone na spoofing, jeżeli nie są spełnione odpowiednie wymogi bezpieczeństwa warstw niższych.

IP spoofing: w wysyłanych datagramach zawarty jest wpis o adresie źródłowym IP. Jeżeli użytkownik potrafi zmodyfikować pakiet tak, aby zawierał on inny niż rzeczywisty adres IP, działanie takie zostanie zakwalifikowane jako spoofing IP.
Spoofing IP i TCP - zapobieganie:

- Ściany ogniowe
- Kerberos
- Szyfrowanie sesji IP
- Opuszczanie wszystkich sesji terminalowych wtedy, kiedy stają się one nieaktywne i uruchamianie wtedy gdy są potrzebne
- Konfiguracja sieci, na poziomie routera, w taki sposób, aby nie przyjmował pakietów z Internetu podających się za pakiety z sieci lokalnej
- Szyfrowanie sesji na poziomie routera
- Blokowanie przyjmowania TCP na poziomie zapory sieciowej i korzystanie z protokołu IPX wewnątrz sieci

Spoofing systemu routingu IP: polega na kierowaniu pakietów do innej maszyny, czy podsieci. Generalnie zmiana routingu powoduje zmianę dróg, jakimi są przesyłane pakiety w sieci. Spoofing routingu jest przez to podobny do spoofingu ARP, który zakłada niepoprawne dostarczanie datagramów dostarczanych lokalnie. Jeżeli w sieci mamy ustawiony domyślny routing, atakujący może zmienić wpis w tablicy routingu i cały ruch przesyłać inną drogą, gdzie dane mogą być podsłuchiwane przez snifery. Jeżeli pakiety dalej będą dostarczane zgodnie z przeznaczeniem, dla użytkownika będzie to niezauważalne. Spoofing routingu wykorzystuje protokół ICMP. Spoofing routingu opartego na RIP wykorzystuje port 520 UDP.

ARP spoofing: ARP (Address Resolution Protocol). Jest to protokół odpowiedzialny za tłumaczenie adresu IP na adresy sprzętowe. Adresy IP maszyn oraz skojarzone z nimi adresy sprzętowe są przechowywane w buforze (cache) ARP każdego hosta. Kiedy datagram jest przesyłany przez sieć, sprawdzana jest zawartość bufora ARP i, jeżeli istnieje tam wpis odpowiadający adresowi docelowego miejsca, gdzie ma dotrzeć datagram, nie ma potrzeby wysyłania zapytania ARP.
Zapisy w buforze ulegają przeterminowaniu po kilku minutach od ich stworzenia. Kiedy wpis ARP o danym hoście wygaśnie, wysyłane jest zapytanie ARP. Jeżeli komputer będzie wyłączony, zapytanie zostanie bez odpowiedzi. Zanim jednak wpis zostanie przeterminowany, datagramy są wysyłane, lecz nieodbierane. Klasycznym przykładem spoofingu ARP jest zmiana adresu IP na adres maszyny wyłączonej. Włamywacz może zorientować się, jaka maszyna w sieci jest wyłączona, lub samemu ją wyłączyć. Wtedy zmieniając konfigurację swojej maszyny może on skonfigurować ją tak, aby wskazywała IP odłączonej maszyny. Kiedy ponownie zostanie wysłane zapytanie ARP, jego system odpowie na nie, przesyłając nowy adres sprzętowy, który zostanie skojarzony z adresem IP wyłączonej maszyny. Jeżeli jakieś usługi w sieci były udostępniane na podstawie zaufania według danych wskazywanych przez ARP, będą one dostępne dla osoby niepowołanej.
Atak za pomocą spoofingu ARP jest również możliwy w przypadku, kiedy istnieją w sieci maszyny o dwóch takich samych adresach IP. Tak sytuacje powinna być niedopuszczalna, jednak często wystepuje takie

zjawisko i nie zawsze jest one zamierzone. Dzieje się tak np. przez instalowanie jednej kopii oprogramowania na wielu maszynach z jedną konfiguracją. Kiedy jest wysyłane zapytanie ARP każdy z hostów o danym IP odpowie na nie. W zależności od systemu albo pierwsza albo ostatnia odpowiedź zostanie umieszczona w buforze. Niektóre systemy wykrywają taką sytuację i jest to oznaka możliwości wystąpienia spoofingu.
Spoofingiem ARP - zapobieganie:

- Zaprzestanie używania ARP
- Bariery sprzętowe (routery)
- Pasywna detekcja na poziomie hosta
- Aktywna detekcja na poziomie hosta
- Detekcja na poziomie serwera
- Detekcja na poziomie sieci przez okresowe kontrole
- Detekcja na poziomie sieci przez ciągle monitorowanie
- Wpisy permanentne

Spoofing DNS: należy porównywać odpowiedzi z równych serwerów. Należy stosować pytania iteracyjne zamiast rekursywnych.

Hijacking: odgadując numer sekwencyjny IP, haker przejmuje istniejące połączenie pomiędzy dwoma komputerami i gra rolę jednej ze strony takiego połączenia. Leglny użytkownik lub host zostaję rozłączony a haker dziedziczy możliwość do aktualnej sesji. Możliwosc taką stwarza niewłaściwa implementacja randomizacji numerów sekwencyjnych w stosie TCP/IP – ISN.
Wczesna desynchronizacja:

1. Atakujący nasłuchuje pakietów SYN/ACK zaadresowanych od serwera do klienta
2. Po wykryciu takiego pakietu wysyła do serwera pakiet RST zamykając połaczenie. Generuje pakiet SYN ze sfałszowanym adresem źródła.
3. Serwer zamknie połączenie od klienta, po czym po otrzymaniu pakietu SYN otworzy drugie połączenie wysyłając do klienta pakiet SYN/ACK
4. Atakujący wykryje pakiet SYN/ACK od serwera i potwierdzi go wysyłając pakiet ACK. Serwer przejdzie do stanu stabilnego.

Desynchronizacja za pomocą pustych danych:

1. Atakujący przygląda się sesji bez ingerowania w nią
2. W wybranym momencie atakujący wysyła dużą ilości pustych danych do serwera. Bajty sekwencji poleceń zostaną zinterpretowanie i usunięte ze strumienia bez widocznych dla użytkownika efektów. Po przetworzeniu danych atakującego dany serwer posiadać będzie numer potwierdzenia różny od tego, którego spodziewa się klient.
3. Atakujący postępuje w ten sam sposób z klientem.

Hijacking - zapobieganie:

- Porównywanie numerów sekwencyjnych po obu stronach połączenia
- Wykrywanie burzy pakietów ACK

Denial Of Service: łączy w sobie użycie standardowych protokołów lub procesów połączeń z intencja przeciążenia lub zablokowania całego systemu. Jest to sposób blokowania działania systemu metodą wysyłania pakietów IP – w dużej liczbie lub nieprawidłowych, co powoduje zapchanie „jałowa robotą" zaatakowanego systemu.
TCP SYN Floods: atak polegający na zasypaniu komputera zleceniem połączenia (pakiet SYN) bez konsekwentnego kończenia tej procedury, co powoduje przyrastanie po stronie odbierającej niezakończonych procesów nawiązywania połączenia TCP, powiązanych z przydziałem odpowiednich bloków sterujących TCP do każdego z nich, co szybko prowadzi do wyczerpania zasobów. Istnieje także UDP Flooding.
Smurt: atak polegający na wysyłaniu dużej liczby pakietów PING pod adresami okólnikowymi IP, z podaniem w polu adresu źródła adresu atakowanego komputera. Urządzenie trasujące przekazuje pakiet pod

wszystkie adresy objęte okólnikiem, wykonując funkcje rozgłaszania IP, po czy hosty w sieci odbierające pakiet echa wysyłają odpowiedź na to echo – oczywiście pod adresem źródła.
Fraggle: używa echa UDP
Ping of Death: wysyłanie sfragmentowanego datagramu ICMP Echo request o łącznym rozmiarze przekraczającym 65535 bajtów.
DoS – zapobieganie:

- Skonfigurowanie list dostępu na routerach i zaporach ogniowych
- Używanie i udostępnianie tylko niezbędnych usług
- Ustalenie systemu ograniczeń na zasoby
- Wprowadzenie systemu monitorowania dostępności i wykorzystania zasobów
- Skonstruowanie odpowiedniej topologii sieci

Złośliwe programy:
Bomba logiczna: program, który powoduje uszkodzenie w momencie zaistnienia odpowiedniego stanu systemu.
Hak pielęgnacyjny: zbiór specjalnych instrukcji w oprogramowaniu umożliwiający łatwa obsługę i dalszy rozwój. Mogą pozwalać na wejście do programu w nietypowy sposób.
Koń trojański: program zawierający obiekty złośliwe umożliwiające nieuprawnione gromadzenie, fałszowanie lub niszczenie danych
Robak: program, który może samodzielnie rozprzestrzeniać się w systemach i sieciach poprzez samopowielanie.

5. Testy penetracyjne:

Testy penetracyjne:
Cele testów penetracyjnych:

- Empiryczne określenie odporności systemu na ataki
- Mogą być prowadzone z wnętrza badanej sieci oraz z zewnątrz
- Należy liczyć się z możliwością załamania się systemu
- Należy utworzyć pełne kopie zapasowe

Fazy testów penetracyjnych:

- Zbieranie informacji o systemie poza nim samym
- Próby uzyskania dostępu do zasobów badanego systemu
- Wstępna ocena możliwości systemu w zakresie wykrywania i blokowania włamań
- Próby włamań

Skanowanie:
Cele skanowania:

- Detekcja urządzeń
- Detekcja usług
- Rozpoznanie systemu operacyjnego
- Rozpoznanie topologii sieci
- Rozpoznanie konfiguracji urządzeń dostępowych

Techniki:

- Skanowanie z wykorzystaniem protokołu UDP: odpowiedź ICMP Port Unreachable, odpowiedź ICMP Host Unreachable
- Skanowanie z wykorzystaniem protokołu ICMP: ICMP Echo Request, Timestamp Request, Address Mask Request
- Specjalne techniki TCP: SYN/ACK, FIN, XMAS, NULL, RST
- Skanowanie protokół FTP
- Wykorzystanie protokołu ident – zwraca dane właściciela procesu, z którym zostało nawiązane połączenie TCP

Enumeracja: proces wyszukiwania poprawnych kont użytkowników lub źle zabezpieczonych zasobów współdzielonych.
Zbierane informacje:

- Zasoby sieciowe i sposób ich udostępniania
- Użytkownicy i grupy
- Aplikacje

Techniki:

- Enumeracja NetBIOS: porty 135 – 139, puste sesje net use
- Enumeracja poprzez SNMP: uruchomione usługi, nazwy zasobów sieciowych, nazwy uzytkowników, nazwy domen, nazwy komputerów
- Enumeracja systemu Windows DNS: rekordy srv, transfer strefy – program nslookup
- Enumeracja Active Directory
- Enumeracja systemu UNIX/Linux: rwho, rusers, w, wykrywanie kont za pomocą SMTP, SNMP, wykrywanie zasobów NIS, NFS,RPC, pozyskiwanie banerów

NetBIOS – zapobieganie:

- Blokowanie portów
- Poprawka RestrictAnonymuous w kluczu HKLM\SYSTEM…

SNMP – zapobieganie:

- Usunięcie agenta, wyłączenie usługi
- Skonfigurowanie prywatnej nazwy wspólnoty
- Określenie adresów zaufanych serwerów
- Modyfikacja rejestru HKLM\SYSTEM…\ValidCommunities
- Modyfikacja rejestru HKLM\SYSTEM…\ExtensionAgents
- Blokada portu 161 TCP i UDP w granicznych urządzeniach kontroli dostępu (odciecie od sieci publicznej)

Zdalna identyfikacja systemu:

Techniki pasywne:

- Fingerprinting w warstwie aplikacji
- Analiza ruchu sieciowego

Techniki aktywne:

- Zbieranie banerów, plików binarnych
- Analiza odpowiedzi na segmenty TCP
- Skanowanie ICMP
- Badanie wartości ISN, RTO

6. Podstawy kryptografii:

Algorytmy kryptograficzne:

Algorytmy z kluczem prywatnym:

- Szyfr Cezara, skipjack, IDEA, RC2, RC4, RC5, DES, 3DES

Algorytmy z kluczem publicznym:

- DSA, ElGamal, RSA

Algorytmy haszujace:

- MD2, MD4, MD5, SHA, Snefru, Haval

Podpis cyfrowy:

Nadawca podpisanej informacji używa tzw. Funkcji haszującej, do wytworzenia unikatowej, skróconej wersji oryginalnego tekstu, określanej mianem „abstraktu wiadomości" lub skrótem. Praktycznie prawdopodobieństwo wystąpienia takiego samego abstraktu wiadomości w dwóch różnych dokumentach jest bliskie zeru i dlatego też nawet najmniejsza zmiana w treści dokumentu spowoduje zmiany w abstrakcie. Taki abstrakt jest następnie szyfrowany kluczem prywatnym stając się podpisem cyfrowym. Sama wiadomość może też być zaszyfrowana. Strona odbierająca wiadomość z załączonym podpisem deszyfruje podpis kluczem publicznym w celu odtworzenia źródłowego abstraktu wiadomości „szatkuje" wiadomość taką samą funkcją haszujacą i porównuje obie wartości, – jeśli są równe to podpis jest autentyczny.

Dystrybucja kluczy kryptograficznych:

- Protokół CERBERA

  KDC szyfruje klucz sesyjny, przesyła Abonentowi 1 inf. zaszyfrowaną kluczem 2.

Ab.1 wysyła Ab.2 inf., Obaj abonenci posiadają klucz .

- Protokół SHAMIRA
  Ab.1 generuje klucz sesyjny, przesyła zaszyfrowany (C1) do Ab.2. Ab.2 szyfruje wiadomość (C2) i wysyła do Ab.1. Ab.1 deszyfruje C2 i przesyła C3. Ab.2 deszyfruje klucz sesyjny.
- Protokół WYMIANY KLUCZA ZASZYFROWANEGO
  Ab.1 przesyła klucz jawny K' zaszyfrowany symetrycznie do Ab.2.
  Ab.2 wytwarza klucz sesyjny szyfruje do tajnym i śle do Ab.1.
  Ab.1 deszyfruje a następnie przesyła ciąg losowy Ra1 zaszyfrowany kluczem sesyjnym. Ab.2 przesyła swój Ra2 i Ra1 do Ab.1, który porównuje klucz Ra1. Potem wysyła Ra2 do Ab.2, który porównuje go. Jeśli ok., to ok. ;)
- Protokół PODSTAWOWY
  Ab.1 szyfruje Kses jawnym Ab.2. Ab.2 deszyfruje do swoim tajnym.
- Protokół BLOKUJĄCY
  Wymiana jawnych. Ab.1 generuje klucz sesyjny. Potem po ½ wiadomości zaszyfrowanej jawnym. Łączenie, deszyfracja no i jazda.
- Algorytm DIFFIE-HELLMANA
  Ab.1 i Ab.2 losują duże liczby x i y. Obliczają X(Y)= gx(y) mod n.
  Wymiana X i Y. Następnie obliczają klucz sesyjny: k=Y(X)x(y) mod n. Klucz tajny, sesyjny (k = gxy mod n) obliczony jest przez abonentów niezależnie.

Infrastruktura klucza publicznego PKI:
Umożliwia centralne tworzenie, dystrybucję, śledzenie i odwoływanie kluczy. Zapewnia zarządzanie kluczami oraz certyfikatami stosowanymi w kryptografii klucza publicznego.
PKI składa się z 5 podstawowych komponentów:

- CA *Certification Authorieties* – wydawcy certyfikatów, przydzielającego i odbierającego certyfikaty
- ORA Organizational Registration *Authorieties* – ciała poręczającego za powiązania pomiędzy kluczami publicznymi, tożsamość posiadaczy certyfikatów
- Posiadaczy certyfikatów, którym są wydawane certyfikaty i którzy mogą podpisywać dokumenty cyfrowe
- Klientów, którzy zatwierdzają cyfrowe podpisy
- Katalogów przechowujących i udostępniających certyfikaty oraz listy certyfikatów unieważnionych

7. Systemy uwierzytelniania użytkowników:
   Uwierzytelnianie – proces stwierdzania autentyczności, czyli wiarygodności, weryfikacji tożsamości użytkownika.

   Podstawowe metody uwierzytelniania:
   - Hasło
   - System S/Key = hasła jednorazowe, wykorzystuje funkcje skrótu: klient przesyła jednorazowe hasło do serwera, w serwerze znajduje się plik zawierający dla każdego użytkownika jednorazowe hasło z poprzedniego pomyślnego logowania, serwer przepuszcza odebrane hasło przez funkcje mieszającą, wynik powinien odpowiadać hasłu z poprzedniego logowania.
   - Procedury uwierzytelniania X.509
   - Tokeny

   Standard X.509
   Uwierzytelnianie jednokierunkowe.
   Struktura:
   - Nazwa nadawcy
   - Nazwa odbiorcy
   - Znaczniki czasu określające czas utworzenia i ważności wiadomości
   - Liczba losowa wygenerowana przez nadawcę
   - Podpis cyfrowy nadawcy

   System Kerberos:

Kerberos to system weryfikacji autentyczności wykorzystujący algorytm DES, bazuje na tzw. ``biletach'', które służą jako przepustki do korzystania z usług sieciowych. Przepustka jest zaszyfrowana hasłem użytkownika, dzięki czemu tylko ten, kto zna jego hasło, może z niej skorzystać. Ponieważ dane przesyłane przez sieć w systemie Kerberos są przesyłane w postaci zaszyfrowanej, system ten jest odporny na podsłuch. Standardowe hasła użytkownika są zaszyfrowane za pomocą jednokierunkowej funkcji haszującej, która jest nieodwracalna; w systemie Kerberos wszystkie hasła są zaszyfrowane za pomocą algorytmu DES i można uzyskać ich postać jawną, jeżeli posiada się odpowiedni klucz. Kerberos nie używa kryptografii z kluczem publicznym.
Kiedy użytkownik otrzyma przepustkę udzielającą przepustki, może rozpocząć pracę z systemami wymagającymi autoryzacji. Za każdym razem, zamiast przesyłać hasło, przedstawia on odpowiednią przepustkę, na podstawie, której system, albo zezwala na korzystanie z danej usługi, albo zabrania dostępu. Aby uzyskać przepustkę, stacja robocza musi się skontaktować z serwerem udzielającym przepustki (TGS) i przedstawić mu odpowiednią przepustkę do tego serwera. Przepustka taka składa się z dwóch ważnych informacji:

- klucz sesyjny Kses
- przepustka do serwera przepustek, zaszyfrowana kluczem sesyjnym oraz kluczem serwera przepustek

Po uzyskaniu odpowiedniej przepustki, klient może się kontaktować z jednostką w strefie (realm) Kerberos. Strefa Kerberos to zbiór serwerów i użytkowników znanych serwerowi Kerberos.

Idea:

- Rejestracja użytkownika
- Bilet do usługi pryznawania biletów
- Bilet do usługi
- Usługa dla klienta

Kerberos – 2 serwery:

- Uwierzytelniający (przyznaje bilet do usługi przyznawania biletów) i przyznający bilety (przyznaje bilet do usługi)
- Serwer aplikacji – sprawdza bilet do usługi

Atrybuty biletów: początkowe, nieważne, odnawialne, postdatowe, upełnomocniające i upełnomocnione, przekazywalne.

8. Bezpieczne protokoły:

IPSec:

Może przeprowadzać autoryzację nadawcy, sprawdzać integralność danych, zapewniać poufność transmisji i sterować dostępem w sieciach. Posiada dwa tryby:

Tryb transportowy:

- ESP chroni tylko oryginalny ładunek IP, nie ochrania oryginalnego nagłówka IP
- W tym trybie nagłówki związane z IPSec (AH/ESP) są dodawane po nagłówku IP, a więc nagłówek IP nie jest ukrywany. Z tego powodu można go stosować tylko do transmisji w sieciach LAN (w WAN – problemy z fragmentacją i routingiem). Tryb transportowy stosuje się do komunikacji między komputerami, oraz komunikacji komputerów z gatewayami IPSec.

Tryb tunelowy:

- ESP chroni oryginalny nagłówek IP i ładunek IP, ale nie chroni nowego nagłówka IP
- Powoduje dodanie nowego nagłówka IP wraz z nagłówkami IPSec i w rezultacie ukrycie całego pakietu, łącznie z nagłówkami. Stosuje się go głównie do komunikacji gateway-gateway. Umożliwia on budowę sieci VPN (wirtualnych sieci LAN) przy użyciu Internetu.

SA określa:

- Informacje definiujące algorytm szyfrowania
- Informacje definiujące algorytm uwierzytelniania
- Informacje definiujące algorytm integralności
- Klucze szyfrujące i kodujące wykorzystywane w AH i ESP

- Okres ważności kluczy
- Okres ważności tunelu

AH zapewnia:

- Usługi związane z uwierzytelnieniem pakietu. Robi to za pomocą algorytmów typu MAC (Message Authentication Code). Dodatkowo zapewnia to również integralność przesyłanych danych.

ESP zapewnia:

- Poufność danych dzięki szyfrowaniu (nie ma tego w AH)
- Identyfikację i integralność

Protokoły negocjacji:

- ISAKMP
- Oakley
- IKE
- PHOTURIS
- SKIP

SSL:
Może używać różnych kluczy publicznych i systemów wymiany kluczy sesyjnych z kartami identyfikacyjnymi. Wymieniony klucz sesyjny może być używany w wielu różnych algorytmach z tajnym kluczem. System SSL jest publicznie dostępny przez anonimowe ftp

- SSL Record Protocol (skrót wiadomości, dane do przesłania, dane wypełniające)
- SLL Handshake Protocol - mechanizmy szyfrowania związane z SSL wykorzystywane

wykorzystują certyfikaty do uwierzytelniania serwera

TLS:
Jest metodą zabezpieczania wymiany danych miedzy serwerami webowymi i przeglądarkami. Wprowadza nową warstwę bezpieczeństwa do czterowarstwowego modelu odniesienia Internetu.

- Połączenie jest niejawne. Do szyfrowania stosuje się kryptografię symetryczną (DES, RC4)
- Połączenie jest rzetelne. Sprawdzenie integralności opiera się na MAC, wyliczonym przez funkcję haszującą.

S-HTTP:

- połączenie klient – serwer
- definicja protokołów bezpieczeństwa
- request (protokół i nagłówki) – response (np. protokół 200 OK)
- protokół dedykowany – nie wiem co to znaczy ale jak będzie pyt. Który dedykowany to ten ;)

S-HTTP jest rozszerzeniem protokołu HTTP, dlatego też klient łączy się na ten sam port TCP serwera, co w przypadku protokołu HTTP, czyli na port 80.
Główne elementy S-HTTP składające się na podwyższenie bezpieczeństwa przesyłanych danych to:

- Szyfrowanie,
- Integralność (MAC),
- Podpisy cyfrowe.

Wykorzystywane są tu dwa typy nagłówków:

- Nagłówki ogólne - definiują zastosowane mechanizmy ochrony informacji - niechronione
- Nagłówki HTTP - chronione przez enkapsulację

SSH:
Jak w HTTP +
Wykrywane protokoły:

- SSH-TRANS – uwierzytelnianie serwera
- SSH-USERAUTH – autoryzacja użytkownika (opcjonalnie)
- SSH-CONN - połączenie

Metody autentykacji:

- public key,
- hostbased – rozbudowano o uwierzytelnianie hosta klienta
- password – idzie otwartym tekstem

PPTP:
Umożliwia zwiększenie zasięgu VPN za pośrednictwem linii telekomunikacyjnych. Eliminuje potrzebę stosowania linii dzierżawionych i dedykowanych serwerów. Bazą jest protokół PPP (warstwa łącza danych).

- Uwierzytelnianie
- Kompresja
- Kapsułkowanie: TCP-> IP -> PPP

L2TP:
Rozszerza model PPP (patrz wyżej).