1. Pojęcia

Trusted Computer System Evaluation Criteria (TCSEC) - "**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 Trusted Networking Interpretation - 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 żadany 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 stwierdzajacy
  zgodność produktu z określonym profilem ochrony lub, spełnienie określonych wymagań bezpieczeństwa lub, przypisanie do konkretnego poziomu bezpieczeństwa (Evaluation Assurance Level - EAL).

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. Polityka bezpieczeństwa

Zespól i pełnomocnik ds. zarządzania bezpieczeństwem
Audyt bezpieczeństwa, Analiza ryzyka, drzewa zdarzeń i błędów
TISM – rodzaj polityki

4. Zagrożenia internetowe

???

5. Sniffing

Packet-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

Więcej: http://hacking.pl/sniffing/sniff_faq.htm (Jezu kto to pisał?), albo http://www.robertgraham.com/pubs/sniffing-faq.html (polecam)

6. Spoofing

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 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 spoofing 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.

ARP spoofing. ARP (Address Resolution Protocol). Jest to protokół odopowiedzialny za tłumaczenie adresu IP na adresy sprzętowe.
Adresy IP maszyn oraz skojarzone z nimi adresy sprzętowe są przechowywane w buforze (cache) ARP kazdego 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 nie odbierane. 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.
Aby bronić się przed spoofingiem ARP, stosuje się wpisy permanentne w przypadku hostów o szczególnym znaczeniu.

Web spoofing is a man-in-the-middle attack that makes the user think they have a secured session with one specific web server, when in fact they have a secured session with an attacker's server. At that point, the attacker could persuade the user to supply credit card or other personal info, passwords

Ochrona **pasywna, aktywna** ???? co to k...

http://gazeta.linux.krakow.pl/issue63/sharma.html
http://linux.sote.pl/node14.html
http://www.nmrc.org/faqs/hackfaq/hackfaq-9.html (ang)
http://www.linuxgazette.com/issue63/sharma.html

7. Algorytmy krypotograficzne

Szyfrowanie symetryczne:
-Algorytmy z kluczem prywatnym
(Szyfr Cezara, skipjack, IDEA, RC2,4,5, DES, 3DES)
Szyfrowanie asymetryczne:
-Algorytmy z kluczem publicznym (DSA, RSA, ElGamal)
-Algorytmy haszujące (MD2,4,5, SHA, Snefru, Haval)

8. Podpis cyfrowy

Wiadomość – szyfrowana **kluczem symetrycznym**
Klucz symetryczny – szyfrowany kluczem **publicznym odbiorcy**
Podpis cyfrowy – uzyskany po użyciu **f-cji mieszającej** wiadomości ; powstaje skrót który zostaje następnie zaszyfrowany kluczem prywatnym nadawcy

Sprawdzenie autentyczności – porównanie **skrótów** (odszyfrowany podpis cyfrowy i odszyfrowana wiadomość skrócona f-cją mieszającą)

9. 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 $X(Y)= g^{x(y)} \bmod n$.
Wymiana X i Y. Następnie obliczają klucz sesyjny: $k=Y(X)^{x(y)} \bmod n$. Klucz tajny, sesyjny ($k = g^{xy} \bmod n$) obliczony jest przez abonentów niezależnie.

10. Uwierzytelnianie użytkowników

Metody:
- hasło
- protokół sKey = hasła jednorazowe, wykorzystuje f-cje skrótu
- metody znacznikowe

Ochrona haseł: nadzorowanie, zabezpieczenie przed odgadnięciem, bezpieczne przechowywanie

Weryfikacja metodą hasło – odzew

Weryfikacja hasłami jednorazowymi
- zdefiniowany w RFC 1760
- wykorzystuje funkcje skrótu
- zabezpiecza przed ponownym wykorzystaniem
- wstępne elementy: wspólny klucz tajny, licznik powtórzeń (repetycji)
- zachowywane jest ostatnie hasło, dla weryfikacji bieżącego

Uwierzytelnianie dwustronne (?)

Metoda znacznikowa
- Użytkownik łączy się z serwerem
- Hasło (klucz) generowane po stronie serwera
- Serwer sprawdza na poziomie skrótów czy odzew klienta prawidłowy

Metoda tokenowa – hasło generowane co minutę (LucasBank)

11. Standard X 509

Struktura: nr wersji, nr seryjny, id. Algorytmu, id. Wystawcy, okres ważności, użytkownik certyfikatu, informacja o kluczu publicznym, podpis cyfrowy

11. 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.

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.

Więcej: http://linux.sote.pl/node53.html

12. Mechanizmy kontroli dostępu

Weryfikacja względem praw dostępu:
-Listy kontroli dostępu (ACL) – dla pliku
-Listy możliwości – dla użytkownika, aplikacji
-Etykiety poziomów zaufania

Ukryte kanały: czasowy, pamięciowy

14. Archiwizacja w Unix i NT (???)

15. Inspekcja i jej implementacja

Linux – program ***sa***

WINNT: polityki audytu (zdarzeń, zasobów, drukarek)
-użycie plików/ katalogów
-logowanie, uruchomienie, zatrzymanie systemu
-zmiany w definicji grup/ użytkowników
-zmiany w polityce bezpieczeństwa
-dozwolone /niedozwolone dostępy do zasobów

16. Firewalls

Zapory:
- host z dwoma portami
- dławik – router bez firewalla, nie chroni przed pakietami z www, ftp, dostępne jest filtrowanie
- dławik i brama – cały ruch przez bramę, zabezpiecza przed wysyłaniem niewłaściwej informacji z warstw wyższych
- 2 dławiki i brama

Filtrowanie pakietów
a) bezstanowe filtrowanie – kłopot z filtrowaniem usług wymagających kanału zwrotnego
- adresów IP
- portów (Telnet, NetBIOS, POP, NFS, X Windows)
- routing źródłowy
- fragmentacja

b) z badaniem stanu

Proxy – sprawdzanie URL, filtrowanie pakietów przed wysłaniem, zastępuje przepływ pakietów między siecią wew. a zew.
Zalety:
- klient niewidoczny
- blokada niebezpiecznych URL, filtrowanie zawartości (wirusy, konie)
- badanie spójności przesyłanej informacji
- zapewnienie pojedynczego punktu dostępu (nadzór, audyt)

Wady:
- wrażliwość na awarie, zatory
- każda usługa, oprogramowanie musi mieć proxy
- nie chroni SO
- małe bezpieczeństwo konfiguracji domyślnych

Translacja adresów (NAT):
Statyczna (jaki serwer ma być widoczny z zew.), dynamiczna, ze zrównoważonym obciążeniem (rozrzucanie zgłoszeń z zew. na poszczególne serwery), ze zwielokrotnionymi połączeniami

Zakres f-cji firewall (slajd 16)

17. SSL, S-HTTK, SSH, IPSec, Secure RPC

IPSec
– tryb transportowy, tunelowy,
– nie ma dystrybucji kluczy

Dwa tryby pracy IPSec:
Tryb transportowy – 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 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.

Protokół AH (*Authentication Header*), jak sama nazwa wskazuje zapewnia usługi związane z uwierzytelnieniem pakietu. Robi to za pomocą algorytmów typu MAC (*Message Authentication Code*). Dodatkowo zapewnia to również integralność przesyłanych danych.
Protokół ESP (*Encapsulation Security Payload*) zapewnia poufność danych plus funkcjonalność protokołu AH. Oprócz mechanizmów MAC stosuje on algorytmy szyfrujące dane.

Więcej: http://ipsec.pl/prezentacje/ipsec-ntsec/ipsec-ntsec-materialy.html

SSL (Secure Socket Layer) - 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

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 - nie chronione

-**nagłówki HTTP** - chronione przez enkapsulację

S-RPC

- mechanizm znaczników czasowych
- ograniczenie: opiera się na NIS lub NIS+

SSH

- jak w HTTP +
- wykrywane protokoły:

1. SSH-TRANS – uwierzytelnianie serwera
2. SSH-USERAUTH – autoryzacja użytkownika (opcjonalnie)
   Metody autentykacji:
   -public key,
   -hostbased – rozbudowano o uwierzytelnianie hosta klienta
   -password – idzie otwartym tekstem
3. SSH-CONN - połączenie

18. Testy penetracyjne

Test penetracyjny

Rekonesans
Skanowanie: przestrzeni adresowej, sieci tel., portów serwerów i urządzeń
Identyfikacja systemu
Symulacja włamania

Skanowanie: połączeniowe, pół-otwarte, skryte

Enumeracja – proces wyszukiwania poprawnych kont użytkowników lub źle zabezpieczonych zasobów współdzielonych
WinNT – net view, nbtstat
UNIX – NFS i showmount, NIS I pscan…

19-20. Systemy wykrywania włamań, Pułapki internetowe

Pułapka internetowa – uprawnione oszustwo – żeby skierować uwagę intruza na fikcyjne zasoby, gromadzenie informacji, reagowanie

Rodzaje – tarcze (emulowanie niewykorzystanych serwisów**), pola minowe (**komputer pułapka**), ZOO (**cała sieć**)**

Przykłady:

- Specter Intrusion Detection System
- Verizon NetFacade