Svar till TestProv

Tillåtna hjälpmedel; penna, suddgummi, linjal.

Frågorna skall besvaras på ett sådant sätt att en insatt kollega skall känna sig informerad.

1. När man pratar om datasäkerhet brukar man indela området i två huvudområden, vilka är dessa och vad skiljer dem åt? 4p

Logisk säkerhet och Fysisk säkerhet.
Logisk är den säkerhet som rör någon form av program som kan vara applikationer och skyddsprogramvara i form av brandväggar och larm samt säkerställandet av informationens bevarande såväl som oönskad modifiering eller åtkomst samt hinder.
Däri innefattas datorutrustning och nätverk

Fysisk säkerhet rör sig om rent maskinell åtkomst, skydd mot stöld av dito och mekanisk åverkan på maskinell utrustning samt den apparatur däri information är lagrad Avlyssning med spektakulära metoder som till exempel utstrålning från nätverk och bildskärmar tillhör också fysisk säkerhet.

Det som skiljer dem åt är just det faktum att den fysiska säkerheten rör sig om apparater och kablar samt hur man på olika sätt påverkar dem Den logiska säkerheten är mycket mera dimmig till sitt begrepp, ofta rör det sig om just programvara och inga mekaniska verktyg.

2. Olika typer av brandväggar förekommer, vilka är huvudtyperna och vad skijer dem åt ? 3p

Paketfiltrerande
TCP-Koppel
Applikations

Paketfiltrerande opererar på IP huvudet och de parametrar som finns där, enklast är IP adresser och applikationsportar samt throttle funktioner mot DOS/DDOS attacker och felaktiga IP paket.
TCP-Koppel jobbar på sessionsnivå, klienten upprättar en session mot brandväggen och denna kopplar vidare sessionen till destinationen efter en kontroll rörande applikationsportar och sessionens destination respektive källa.
Applikationsbrandväggar arbetar med hela TCP/IP stacken, denna typ av brandvägg kan öppna upp IP paketens data och söka efter mönster passande olika former av virus eller liknande. Likt de två övriga modellerna kontrolleras källa och destination.
Man brukar också skilja mellan transparenta och icke transparenta brandväggar.
De transparenta kräver oftast ingen klientprogramvara medan de icke transparenta kräver detta. Båda kan dock kräva någon form av autenticering.

3. Det finns nio hotbilder man brukar diskutera, nämn fem hotbilder och förklara kort vari hotet ligger. 5p

Trafikanalys, Förnekande, Återuppspelning, Falsk identitet, Manipulering

4. Vad menas med Spoofing ? 2p

Utge sig för att vara någon annan än man är, tex stulen IP adress, förfalska DNS data. Ofta föregås en ”Man in the middle” -avlyssning av en spoofad adress eller identitet.

5. Förklara skillnaden i DOS och DDOS attacker, vad är medicinen ? 4p

Denial of Service, Distributed denial of Service. Överbelastning av applikation/host/router till den grad att annan verksamhet hindras. Dos utgår från en källa likt en kulspruta, Ddos utgår från flera oberoende källor likt flera kulsprutor vilka alla inriktar sig på en eller ett fåtal destinationer, ofta räknas källorna i hundratusentals och varje källa levererar en serie om kanske 10 paket. Medicin är throttle, men i värsta fall måste man byta ip adresser om DDOS attacken inte går att stoppa.

6. Hur fungerar en TCP SYN flood attack ? 2p

Denna attack är väldigt lik DOS/DDOS attacken och kan vara en sådan också. Handskakningsförsök görs genom att leverera en serie SYN paket, vilket är TCP handskakningens uppkopplingsmeddelande. Olika former av kvalificerade SYN paket kan sammanställas med syfte att ta över en pågående TCP session Medecinen är att noga hålla reda på sessionsnummer vilket föreslås i RFC:er rörande TCP trafik.

7. Alla moderna www-browsers har en virtuell maskin, vad bör man ha i åtanke när man tillåter java och active-x ? Vad är en cookie ? 4p

Att ett program tillåts att exekveras i min dator, som kommer från en främmande källa. Det finns buggar och mängder av kryphål i www-browsers, dessa kan utgöra en fara för min lokala dator rakt genom brandväggar och filter. En cookie är ett litet id-nummer (en ticket) som innehåller information om att sidan besökts och information om när samt bäst före dag. Detta reducerar bandbreddsbehoven en del. Det är alltså inget program som många tror.

8. Vilka två huvudtyper av kryptering brukar man prata om, vad skiljer dem åt ? 4p

Symmetriska
Assymetriska
Dessa skiljer sig åt i huvudsak på hur nycklarna hanteras, Symmetriska har en lokal nycker och denna måste levereras till de som skall läsa meddelandet. Nyckeln är också känd som den elektroniska kodboken. Assymetriska innebär att varje part i ”dialogen” har en privat nyckel samt en publik nyckel vilken måste delas ut till de som vill deltaga för att de skall kunna dekryptera meddelanden. I värsta fall kan en symmetrisk kodning innebära att man kan se mönster i det kodade meddelanet mycket enkelt. De assymetriska nyttjar en mer avancerad logisk funktion för att generera det kodade meddelandet än de symmetriska.

9. Vilken av huvudtyperna tillhör krypteringen MD5 respektive Tripple DES. Hur fungerar MD5 kort. 4p

MD5 är en signeringsmetod, Message Digest, krypteringen av signaturen som ofta är enform av checksumma kan väljas både som Assymetrisk(vanligast) eller Symmetrisk.. Tripple des

Är en symmetrisk kodning med tre seriekopplade DES krypteringar för att erhålla längre nyckel.
MD5, ur ett meddelande framtages en checksumma, denna krypteras med en nyckel. Meddelandet överförs (krypterat eller okrypterat) tillsammans med den krypterade checksumman. När meddelandet mottages räknas checksumman fram igen och krypteras, eller så dekrypterar man den överförda checksumman. Dessa jämförs med varandra, är de identiska är meddelandet orört och stämmer.

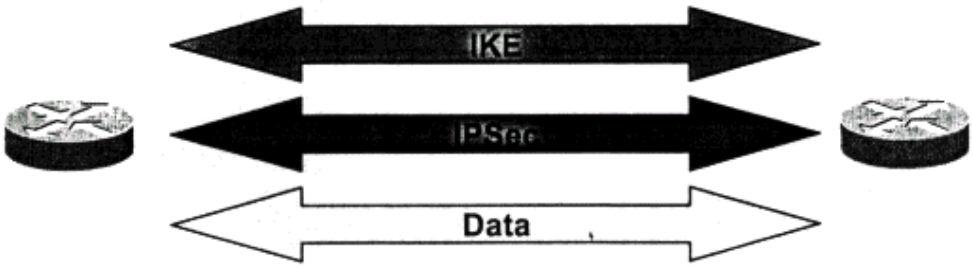
10. Hur kan man anordna så att ett meddelande kan påvisas vara omodifierat och äkta ?

Med MD5 enligt fråga 9, samt ett publikt certifikat utställt av avsändaren som kan verifieras med en CA vilken signerat avsändaren vid tidigare tillfälle..

11. Vad har CA för syfte, kan vem som helst bli CA ? 2p

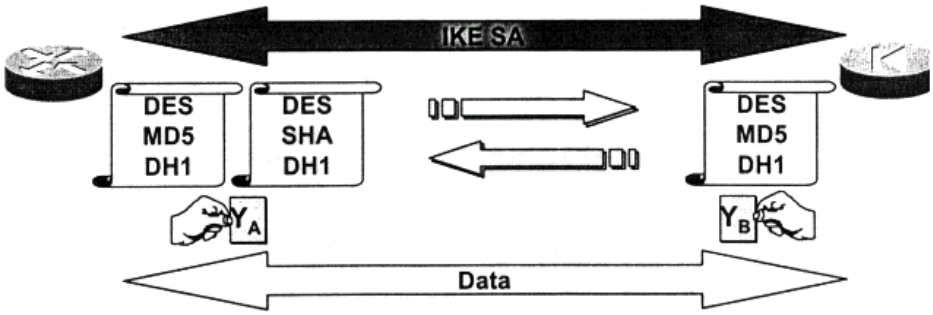
Certificat Authority, att signera andra system's/organisationers nycklar med sin egen och gå i god för att dessa som CA signerat finns till. Vem som helst kan bli CA, ofta signerar man sina egna certifikat. Det är i princip ingen skillnad på självsignerade certifikat och de som till exempel Verisign utfärdat. Det gäller bara att vinna kunders förtroende och sen kan man signera deras certifikat och gå o god för att de finns.

12. Säkerhet på TCP/IP paketnivå löses med IPSec, vilka två metoder jobbar man med med avseende på hur paketen hanteras.



Tunnelmode, IP paketen inpaketeras som datalast i IP paket som är signerade och krypterade.
Transport mode, IP huvudet i paketet är signerat för att bevisa dess härkomst

13. Förklara kort hur IKE fungerar.



Internet Key Exchange, ett särskilt protokoll för att utbyta publika nycklar innan själva kommunikationen mellan punkterna i nätet kan ta plats.

14. Vilka två webbservrar dominerar marknaden för närvarande ? 1p

IIS

Apache

15. Vad menas med WWW-hosting, vilka andra tjänster förutom webbservern måste konfigureras för att få detta att fungera, hur ? 2p

Man har en och samma www-server för att serva flera utifrån sett olika www-servrar. Man måste lägga upp en forward zone eller master zone, i sin dns, för varje domän man önskar serva. Dessutom måste man konfigurera www-servern att handha virtual hosts.

16. Vilket är den enklaste vägen att se om en brandvägg läcker ? 1p

Koppla in en net-sniffer tex. Etherreal eller SnifferPro och lyssna på trafiken, vad syns. ?