Monitoratge de Xarxes

Xavier Tartera

Monitoratge de xarxes

- Per controlar i garantir un bon nivell de qualitat de servei en les xarxes,cal disposar dels mecanismes de monitoratge i control adequats.
- Cal tenir mecanismes perquè només els usuaris legítims puguin fer ús de les xarxes i que ho facin en els termes que estableixin els administradors de sistemes o els encarregats de gestionar l'ús de la xarxa.

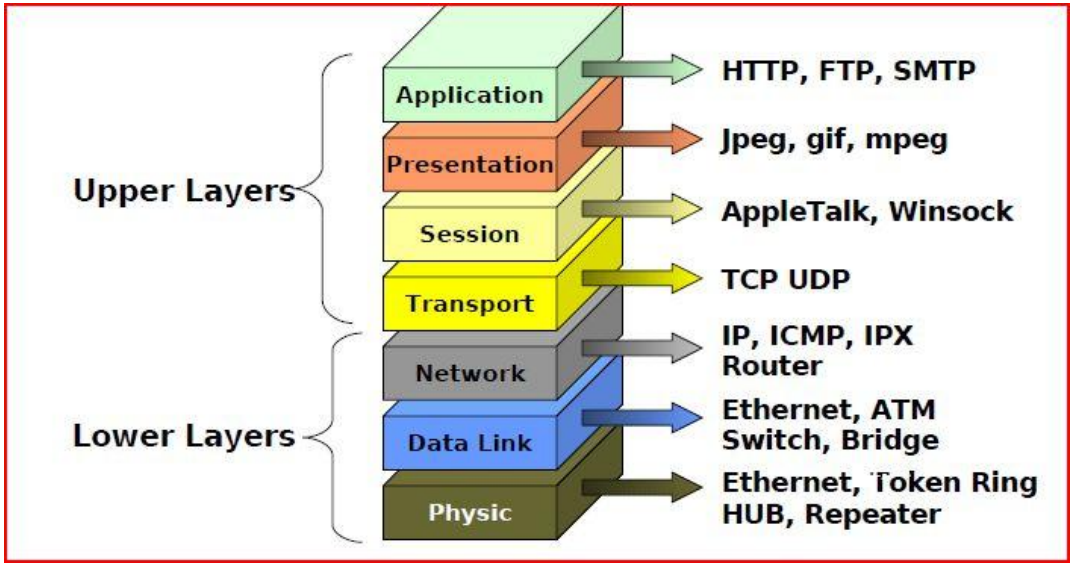
Monitoratge de xarxes

- Les xarxes s'estructuren lògicament en una sèrie de capes. El maquinari i el programari involucrat en el funcionament de la xarxa fa operacions específiques d'alguna capa o de diverses. Les capes que hi ha són les següents:
- Capa d'aplicació
- Capa de presentació
- Capa de sessió
- Capa de transport
- Capa de xarxa
- Capa d'enllaç de dades
- Capa física

El model de capes es coneix amb el nom de model **OSI (open system interconnection)**, és a dir, model d'interconnexió de sistemes oberts. El va definir l'organització OSI i defineix com interconnectar sistemes de comunicació.

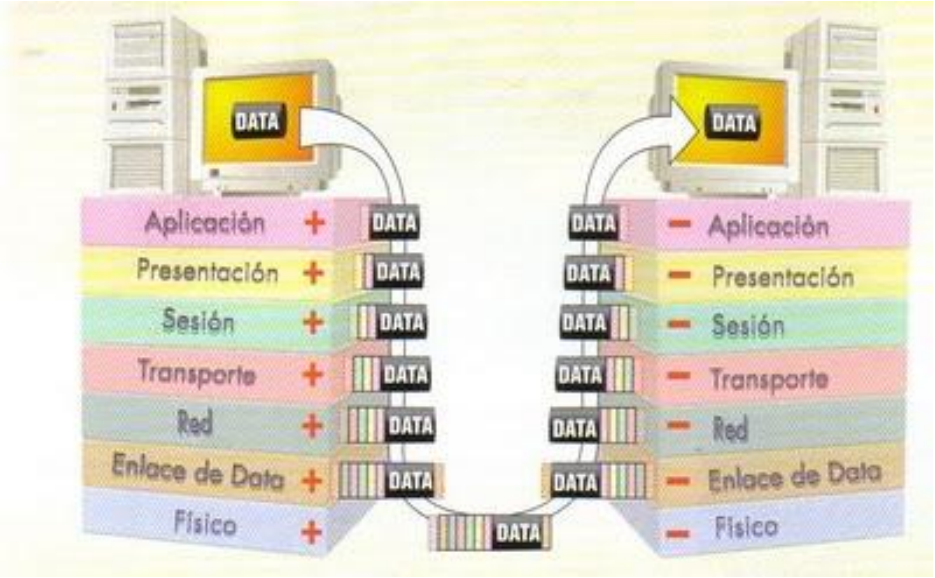
Monitoratge de xarxes

- Cada capa del model OSI té un protocol propi, és a dir, que envía la informació seguint unes normes determinades. La informació es va afegint en els paquets de dades per tal que els diversos dispositius de la xarxa la puguin tractar.



Monitoratge de xarxes

- En un paquet de dades que circuli per la xarxa hi haurà l'adreça d'origen i de destinació, que tractaran els dispositius d'encaminament; bits d'integritat, que comprovaran si part de la informació que es transporta s'ha alterat,etc…



Monitoratge de xarxes

- S'han de distingir dos tipus d'anàlisi de la informació d'una xarxa: la que està destinada al monitoratge d'aquesta xarxa i la captació d'informació per part de hackers.

Monitoratge de xarxes

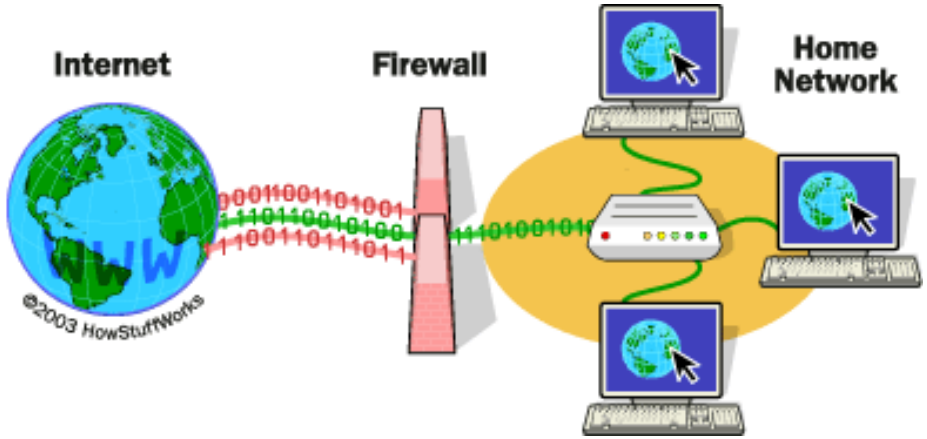
- Hi ha molts dispositius en una xarxa que prenen decisions a partir de la informació que hi circula. Aquests dispositius són necessaris perquè la xarxa funcioni correctament. Els més rellevants són:
  - Encaminadors
  - Tallafocs
  - Sistemes de detecció de intrusos IDS
  - Sistemes de monitoratge

Monitoratge de xarxes

- **Encaminadors**. Els encaminadors són els encarregats de fer circular la informació per tota la xarxa. Segons l'adreça de destinació i les regles d'encaminament, prenen decisions que determinen on han d'anar distribuint la informació.

Monitoratge de xarxes

- **Tallafocs**. Els tallafocs són sistemes que permeten o impedeixen el pas dels paquets d'informació a partir de certes regles. Per exemple, es pot filtrar que no es permeti el pas als paquets que tinguin com a destinació una adreça determinada.

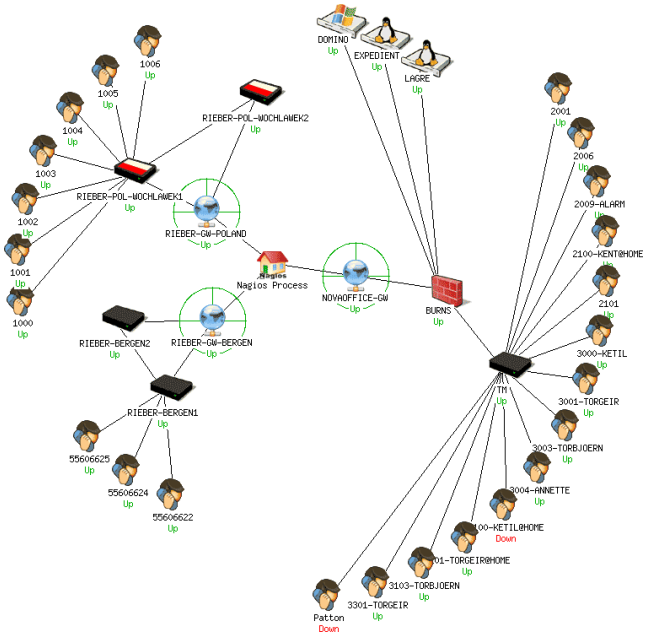


Monitoratge de xarxes

- **Sistemes de detecció d'intrusos (IDS)**. Aquests sistemes avaluen la informació que circula per la xarxa per intentar trobar-hi paquets que indiquin activitat de possibles atacants. Els IDS són sistemes intel·ligents que, a partir de regles complexes, poden discriminar si hi ha activitat perillosa.

Monitoratge de xarxes

- **Sistemes de monitoratge**. Els sistemes de monitoratge avaluen el rendiment d'una xarxa. Per fer-ho, si s'hi detecta alguna anomalia, envien alertes als administradors. Per exemple, de tant en tant fan ping als servidors per comprovar que responen.



Nagios

Zenoss®
Open Source IT Management

Monitoratge de xarxes

- Un detector (sniffer) és qualsevol programa que permet el monitoratge i l'anàlisi dels paquets d'informació que circulen per una xarxa.
- L'ús d'aquest tipus de programari per part d'un atacant permet que pugui accedir a informació confidencial dels usuaris de la xarxa. L'atacant pot aconseguir contrasenyes, números de targetes de crèdit i altre informació privada.

Monitoratge de xarxes

- les eines de sniffing permeten modificar els paquets d'informació, cosa que comporta un risc encara més gran de patir atacs de suplantació d'identitat, captures de sessions, etc.
- La clau per evitar que possibles atacants puguin "esnifar" la informació és que estigui xifrada. La informació no es pot llegir si no es té la clau de xifratge corresponent. Hi ha diferents mecanismes per aconseguir-ho com (PGP,truecrypt, steghide...).

Monitoratge de xarxes

- Les xarxes transporten paquets d'informació que contenen tant dades finals per ser intercanviades pels usuaris i aplicacions com dades necessàries per al bon funcionament de la xarxa (per exemple, dades d'encaminament, dades de control de la integritat de la informació...).
- El monitoratge de les xarxes és el conjunt d'eines i mecanismes que es fan servir per analitzar la informació que és transportada a través de la xarxa i, a partir d'aquestes anàlisis, poder extreure informació sobre el seu funcionament.

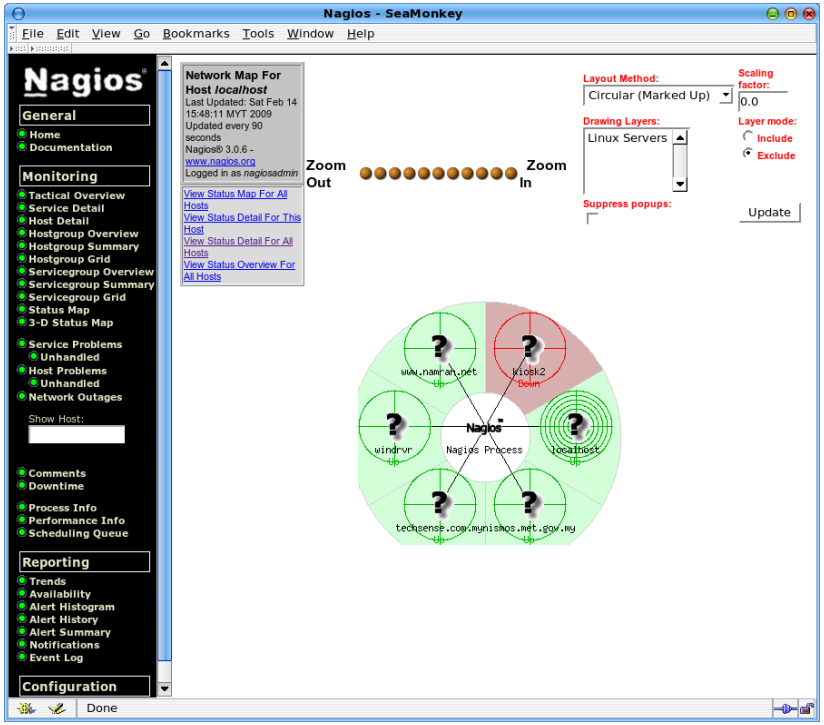
MONITORATGE DE XARXES:

- Els responsables de gestionar la xarxa també han de controlar quins serveis estan permesos en cada cas.

- Per exemple, hi ha xarxes en què serveis de missatgeria instantània no estan permesos per tal d'evitar possibles distraccions o intrusions dels usuaris o altres no benvinguts.

MONITORATGE DE XARXES:

- La configuració, el manteniment i la gestió d'una xarxa pot ser una tasca complicada. S'han de monitorar els equips i els serveis crítics, els usuaris dels recursos de la xarxa, el rendiment d'aquesta mateixa xarxa, l'aparició de possibles atacants, etc..



Factors a tenir en compte en el monitoratge de xarxes

- A l'hora d'inventariar i controlar els serveis d'una xarxa s'han de tenir en compte el factors següents:
  - Rang d'adreces IP
  - Inventari d'adreces MAC
  - Ports
  - Serveis de xarxa actius
  - SNMP

Rang adreces IP

- Els serveis de la xarxa utilitzen les adreces IP per poder encaminar la informació entre diferents equips.
- Dins una mateixa xarxa, no hi pot haver dos equips amb la mateixa adreça, ja que això provocaria un conflicte d'adreces.

Rang adreces IP

- Hi ha uns rangs d'adreces IP que són reservats, és a dir, que no es fan servir en l'àmbit d'Internet. Això permet que es puguin fer servir de manera interna dins una xarxa corporativa o domèstica.
- Els rangs de les adreces IP que hi ha són els següents:
  - 10.0.0.0 <–> 10.255.255.255
  - 172.16.0.0 <–> 172.31.255.255
  - 192.168.0.0 <–> 192.168.255.255.

Inventari adreces MAC

- El codi MAC és un conjunt de números que identifica de manera unívoca un dispositiu.
- No hi pot haver dos dispositius amb el mateix MAC.
- Un mètode que es fa servir per assignar adreces IP de manera estàtica és fer-ho a partir del MAC dels equips de la xarxa. Segons el MAC de l'equip que es connecta se li assigna una IP, de manera que es controla quins equips tenen dret a tenir una IP.

Ports

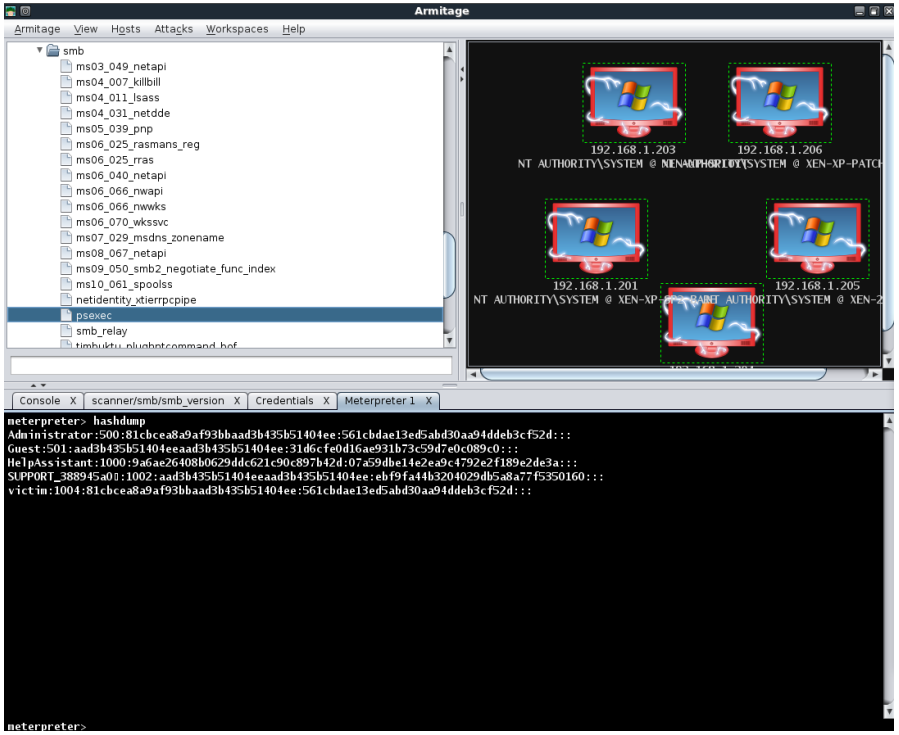
- Les xarxes fan servir els protocols TCP o UDP per a les comunicacions.
- Aquests protocols permeten la definició de ports perquè les aplicacions i els serveis es puguin comunicar de manera directa.
- El port més conegut és el port 80, que identifica el servei HTTP. Quan un navegador accedeix a un URL, està accedint a un equip remot i, en concret, a l'aplicació que és en el port 80. Aquesta aplicació serà típicament un servidor web que escoltarà peticions HTTP i les respondrà.

Ports

- HTTP és només un dels serveis que hi pot haver en una xarxa, però hi ha molts serveis possibles que hi poden funcionar. Cada servei utilitza un port concret.
- Els administradors de la xarxa s'han d'encarregar d'inventariar quins serveis han d'estar actius en quins equips de la xarxa.
- Els equips es poden configurar per establir quins ports poden estar actius.

Ports

- Els ports que no cal utilitzar han d'estar tancats o inactius.
- Tenir ports oberts sense cap finalitat és un risc molt important per a la seguretat, ja que una aplicació malintencionada ho podria utilitzar per accedir a la màquina.



Vigilar amb els ports que es pot entrar...

Serveis actius aconsellables

- HTTP és només un dels serveis que hi pot haver en una xarxa, però hi ha molts serveis possibles que hi poden funcionar. Cada servei utilitza un port concret.
- Els administradors de la xarxa s'han d'encarregar d'inventariar quins serveis han d'estar actius en quins equips de la xarxa.
- Els equips es poden configurar per establir quins ports poden estar actius.

Serveis actius aconsellables

- HTTP és la sigla dels termes anglesos *hypertext transfer protocol*, és a dir, protocol de transferència d'hipertext. L'hipertext és el terme originari amb el qual es feia referència a les pàgines web.
  - L'HTTP és el protocol web i fa servir el port 80.

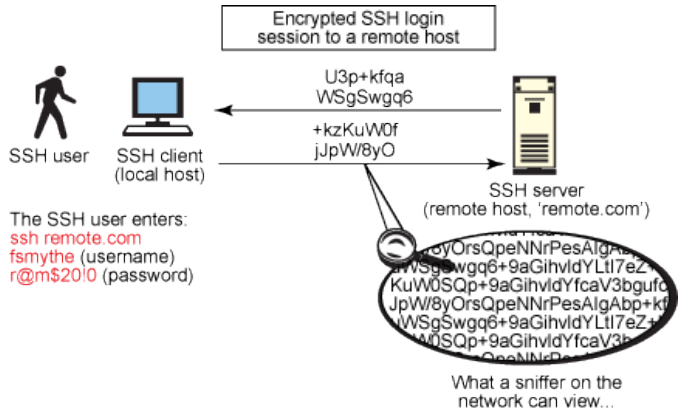
Serveis actius aconsellables

- HTTPS és la sigla d'HTTP segur. Amb el pas del temps es va veure que l'HTTP tenia mancances de seguretat molt importants, que són un risc per segons quins tipus de transaccions, com ara les compres en línia.
- Netscape va desenvolupar l'SSL (*secure socket layer*), que permet afegirseguretat a les transaccions HTTP.

Així va néixer l'HTTPS, que funciona pel port 443.

Serveis actius aconsellables

- SSH és la sigla dels termes anglesos *secure shell*. És el mecanisme més utilitzat per poder accedir a màquines remotes i poder operar-hi.
- Aquest protocol permet connexions autenticades i segures. Tot i així, les màquines que hagin de complir mesures de seguretat extremes han de deshabilitar-lo i permetre-hi només accés físic.
- L'SSH funciona pel port 22.

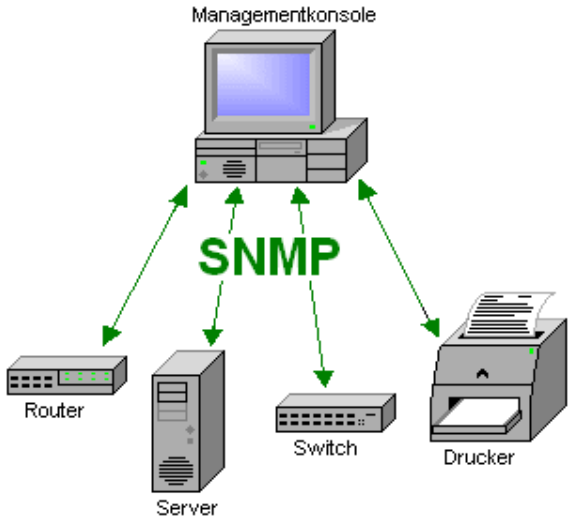


Serveis actius aconsellables

- FTP és la sigla dels termes anglesos *file transfer protocol*, és a dir, protocol de transferència de fitxers. És un dels mecanismes més utilitzats per intercanviar fitxers entre maquines remotes d'una mateixa xarxa.
- S'ha de controlar quins usuaris tenen dret a transferir fitxers a quines màquines.
- L'FTP funciona pel port 20.

SNMP

- SNMP és la sigla dels termes anglesos simple network management protocol, és a dir, protocol simple d'administració de xarxes.
- L'SNMP permet la gestió simple, remota i centralitzada dels recursos d'una xarxa, ja que pot detectar-hi punts de fallida, rendiments, etc.



SNMP

- Una xarxa administrada mitjançant SNMP utilitza tres tipus de components:
  - Dispositius administrats
  - Agents
  - Sistemes administradors de la xarxa

SNMP

- Un **dispositiu administrat** és un punt de la xarxa que té un agent SNMP. Els **agents** recullen i emmagatzemen informació per a l'administració de la xarxa i l'envien als sistemes administradors.

- Els **dispositius administrats** poden ser qualsevol element que formi part de la xarxa, des d'encaminadors (routers) fins a impressores, servidors d'aplicacions, tallafocs...

SNMP

- Els **agents** són petits mòduls de programari que resideixen en els dispositius administrats. Els **agents** tenen coneixement local de la informació del dispositiu en què resideixen (memòria lliure, rendiment del dispositiu, etc.). Els agents tradueixen aquesta informació a un format compatible amb l'SNMP i l'envien als sistemes administradors.

SNMP

- Els sistemes administradors executen aplicacions que supervisen i controlen els dispositius administrats de manera centralitzada.
- Hi ha tres versions d'SNMP: SNMPv1, SNMPv2 i SNMPv3. L'SNMPv2 ofereix certes millores i funcionalitats envers la primera versió. L'SNMPv3 ofereix seguretat respecte de les versions anteriors, ja que les comunicacions entre els elements poden anar xifrades.

Fraus informàtics: Enginyeria Social

- Una de les màximes més importants que cal tenir en compte quan es tracta de la seguretat és que la cadena sempre es trenca per la baula més dèbil.
- Actualment, els equips informàtics cada cop tenen més sistemes tecnològics que permeten que usuaris malintencionats puguin fer un ús fraudulent d'equips no legítims.

Fraus informàtics: Enginyeria Social

- Els sistemes operatius incorporen de sèrie tallafocs simples. Tanmateix, poden ser efectius contra cavalls de Troia (Trojans) i cucs (worms).

- La majoria de programes s'actualitzen automàticament per anar solucionant forats de seguretat i cada cop hi ha més antivirus d'ús gratuït per a usuaris finals.

Fraus informàtics: Enginyeria Social

- Atès que els hackers cada cop tenen més dificultats per poder cometre els delictes, sovint fan servir tècniques d'enginyeria social que es basen en la màxima següent: "Els usuaris són la baula més feble de la seguretat".

- Des del punt de vista de la seguretat informàtica, l'enginyeria social és la pràctica d'aconseguir informació confidencial per mitjà de la manipulació o l'engany d'usuaris legítims.

Fraus informàtics: Enginyeria Social

- Segons defineixen alguns hackers, l'enginyeria social es basa en quatre preceptes. Són els següents:
  - A tots ens agrada ajudar els altres.
  - No ens agrada crear problemes o dir que no.
  - La primera impressió envers l'altra persona sempre és de confiança.
  - A tothom li agrada que l'alabin.

Fraus informàtics: Enginyeria Social

- La mesura de seguretat principal contra els fraus que es basen en enginyeria social (phishing, pharming, Hoax, etc..), consisteix a conscienciar i educar els usuaris envers aquests tipus de riscos.