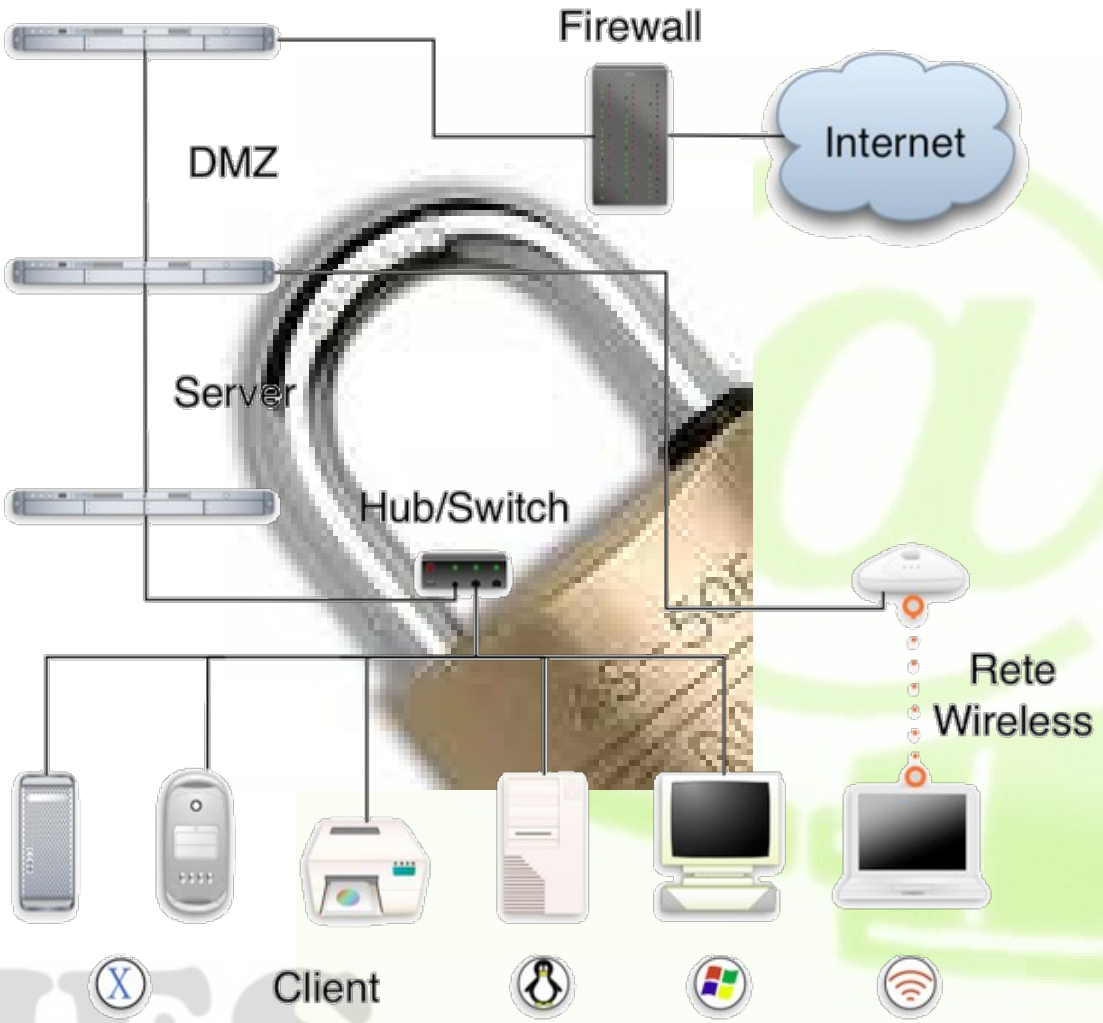
Taller de seguretat en xarxes



Autor: Sergi Tur Badenas

Hackers vs Crackers

- **Són els Hackers els que provoquen la inseguretat de les xarxes?**
  - Rotundament i per definició NO!

Hacker: entusiasta dels ordinadors. Comunament utilitzat en to pejoratiu.
Hacking: art informàtica de construir i solucionar problemes que atempten contra la vulnerabilitat dels sistemes informàtics.
Ethical hacking: ús ètic del hacking.
Cracker: persona que viola la seguretat d'un sistema informàtic de forma similar a com ho faria un hacker però, a diferència d'aquest últim, el cracker realitza la intrusió com a benefici personal o per fer mal.
Lamer: persona o producte que per falta de maduresa, sociabilitat o habilitats tècniques és considerat un incompetent en una matèria o activitat específica.
Script kiddie: "niñato" que fa scripts

  - Cal saber diferenciar entre el saber fer i el fer amb males intencions

Autor: Sergi Tur Badenas

Objectius del seminari

Fer pedagogia sobre la seguretat

- Informar per a lluitar contra la ignorància i el desconeixement.
- Reflexionar per tal de poder decidir per nosaltres mateixos i ser més lliures.
- Conèixer per combatre la mitologia i la desinformació. Combatre la idea cada vegada més estesa que l'ignorant és la persona més feliç.
- Educar per ser constructivament crítics sobre les noves tecnologies.

MOLT IMPORTANT:
El ponent no es fa responsable dels usos que es facin de lo explicat en aquest seminari.

Autor: Sergi Tur Badenas

Legalitat i moralitat. Protecció legal

- **Preguntes per a la reflexió**
  - És il·legal deixar la meva **xarxa sense fils oberta** i capturar les dades de qui la utilitzi?
  - És il·legal oferir un servei de **Proxy gratuït** i capturar les dades de qui l'utilitzi?
  - És il·legal instal·lar-me un **keylogger** al meu ordinador i capturar les contrasenyes de qui l'utilitzi?
  - És il·legal utilitzar un **sniffer de xarxa** a la xarxa de casa meva?
  - És il·legal aconseguir la **clau d'accés WEP** d'una connexió sense fils i connectar-me a aquesta xarxa?
  - Si trobo una **xarxa sense fils oberta** sóc lliure d'utilitzar-la?
- **Segurament el que no hauria de ser legal és el mal ús de les dades obtingudes**

Autor: Sergi Tur Badenas

Protecció tècnica

- **Estem protegits tècnicament?**
  - Possiblement NO. A més, segurament moltes de les tècniques/eines que utilitzem no ens són de gaire ajuda.
- **Hi ha motius per alarmar-se?**
  - Depèn de cada situació
  - Depèn del que poguéssim perdre
  - No si s'han pres les mesures adequades
  - Mai s'està 100% segur
  - Estem sols a la nostra xarxa LAN de casa i accedim a Internet amb un encaminador mitjançant NAT
  - No és l'objectiu d'aquest seminari provocar alarmisme
  - De fet l'alarmisme pot arribar a ser de per si una font d'inseguretats

Autor: Sergi Tur Badenas

Factors que promouen la inseguretat

- **EL DESCONEIXEMENT**
- **LA DESINFORMACIÓ**
- **LA POR, LA INCERTESA I EL DUBTE**
  - FUD (Fear, Uncertainty and Doubt)
- **EL SECRETISME**
  - SECURITY THROUGH OBSCURITY
- **LA COMODITAT**
- **LA SIMPLICITAT**
- **EL COMPROMÍS ENTRE NIVELL DE SERVEI I SEGURETAT**

Autor: Sergi Tur Badenas

Security Throught Obscurity

És un controvertit principi de seguretat la idea bàsica del qual és utilitzar el secretisme per a proveir seguretat.

- Aquests tipus de sistemes solen tenir vulnerabilitats de seguretat (tot sistema té vulnerabilitats) però els seus propietaris o dissenyadors no els modifiquen perquè creuen que aquests problemes són desconeguts.

- **Windows és model clar d'aquest funcionament**
  - Per exemple, les claus de Windows són insegures per disseny des de fa molt de temps. És una vulnerabilitat coneguda però mai solucionada (Windows Vista la manté).
  - A Internet podeu trobar diversos articles sobre la particular lentitud de Microsoft per resoldre bugs i vulnerabilitats.

Autor: Sergi Tur Badenas

Seguretat per disseny

- **Aquest model té en compte la seguretat des del disseny de l'aplicació**
  - Parteixen de la màxima que cap sistema és 100% segur i encara més important és conèixer i solucionar quan abans millor les teves vulnerabilitats.
  - També és igual d'important informar als usuaris d'una aplicació dels possibles problemes de seguretat.
- **Hi ha nombroses llistes d'avisos de seguretat**
  - http://www.us-cert.gov
  - http://www.cert.org
  - http://escert.upc.edu
- **Disposar del codi font d'una aplicació permet auditar-ne la seva seguretat**

Moltes institucions o empreses on la seguretat sigui quelcom altament crític utilitzen programari tancat de tercer en els seus sistemes.

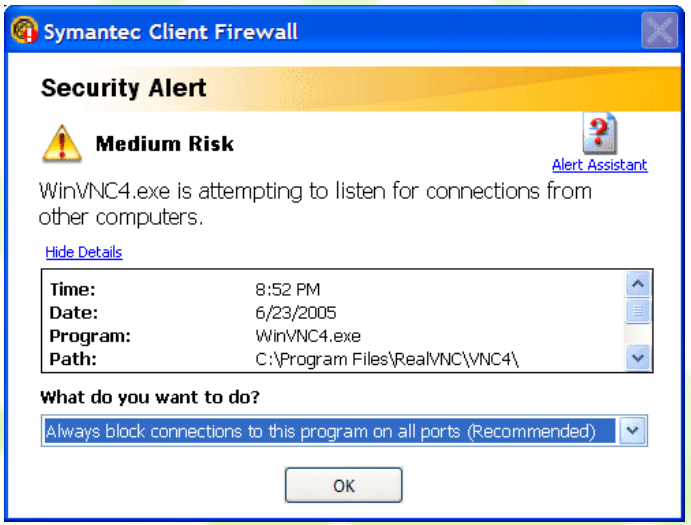
Autor: Sergi Tur Badenas

Alarmisme

Exemple:
Curs d'iniciació a la informàtica per a gent gran

Continguts del curs

- Tallafocs i antivirus
- Quin significat creieu que té per a un usuari novell un missatge com:
  - És com si li parlessin en xinès
- Què tal estaria educar en el sentit comú i no pas en productes concrets?



- Els alumnes novells no saben d'informàtica però estan molt ben instruïts en el **FUD**.

Autor: Sergi Tur Badenas

Alarmisme

- **És segur navegar per Internet? Em costa diners?**
  - Amb una connexió ADSL no costa res més que la tarifa plana.
  - És segur si apliquem el nostre sentit comú. Per exemple:
    - No hem de donar mai les nostres dades personals a no ser que estiguem segurs del lloc web que estem visitant.
    - Si donem les nostres dades bancàries o de targetes de crèdit aleshores segur que ens costa diners.
    - Moltes pàgines d'activitats no legals (programes pirates) o de valors morals controvertits (pornografia, pròxies) són sovint fonts de malware.
- **Estem segurs amb un tallafocs i un firewall instal·lats?**
  - NO. Sobretot si estem desinformats.
  - Per exemple és força senzill fer una transparència divertida que porti un “regalet” al darrere.

Autor: Sergi Tur Badenas

Seguretat informàtica

- **És la informàtica intrínsecament insegura?**
  - És segur entregar la nostra targeta de crèdit a un cambrer en un restaurant?
  - Són segures les targetes de crèdit?
  - Les contrasenyes d'un ordinador quan més complicades millor però els PINS de les nostres targetes de crèdit són només de 4 dígits!
  - Que creieu què és més probable actualment: que ens ataqui un hacker o que ens robin pel carrer?
  - Estem sent coherents amb la informàtica?
  - El criteri està sempre en trobar un punt mig entre:

Seguretat vs Servei

Autor: Sergi Tur Badenas

Podem, doncs, estar segurs?

- **Segurament la resposta és que MAI podrem estar completament segurs**
  - El SENTIT COMÚ, la informació i la constància són segurament les úniques opcions que tenim per apropar-nos a l'ideal de seguretat

> El sentit comú és el menys comú dels sentits

  - Cal conèixer per tal de poder tenir un criteri propi i que cadascú pugui decidir quines mesures de seguretat li convenen més

Autor: Sergi Tur Badenas

Desconeixement i desinformació

- **Hi ha molts mites entorn la seguretat**
  - La utilització de commutadors (switchs) ha fet que les xarxes LAN siguin segures
  - El meu ordinador és segur perquè té una contrasenya d'accés al Sistema Operatiu
  - La seguretat de les contrasenyes només depèn de la qualitat de la mateixa
  - Els protocols que utilitzen el xifratge de dades són segurs (SSH, HTTPS, SSL ,etc.)
  - La majoria d'atacs que rep una xarxa són a través d'Internet
  - Els sistemes tancats són més segurs que els sistemes oberts
  - Un ordinador sense connexió a l'exterior és una màquina segura

Autor: Sergi Tur Badenas

Desconeixement i desinformació

- Estem més segurs si utilitzem un tallafocs i un antivirus
- Windows és un sistema operatiu segur
- Els sistemes operatius Linux són segurs

- **Sistemes operatius**
  - No hi ha sistemes operatius que intrínsecament siguin més segurs que altres

És més segur un Windows ben administrat que un servidor Linux mal administrat

  - Però sí que algunes formes de fer i certes filosofies estan més orientades a la seguretat

Security Throught Oscurity
vs
Security by Design

Autor: Sergi Tur Badenas

Seguretat física

- **Mites**
  - Un ordinador sense connexió a l'exterior és una màquina segura.
  - El meu ordinador és segur perquè té una contrasenya d'accés al Sistema Operatiu. És més, tinc una contrasenya d'accés al sistema.
- **Inseguretats**
  - Em puc endur l'ordinador, tirar-lo per la finestra, obrir-lo i endur-me el disc dur...
  - Puc accedir al sistema amb un CD-LIVE, muntar el disc dur i modificar les dades que calgui (usuaris, paraules de pas...)
- **Solucions**
  - Controlar l'accés físic al sistema.
  - Xifrar totes les dades del disc.

Autor: Sergi Tur Badenas

Seguretat física

Els sistemes operatius apagats són com el Falcó Mil·lenari sense escuts de protecció.

- **A l'escriptori teniu un accés directe a les dades de la partició de Windows d'aquest disc**
  - NOTA: El mateix passa amb qualsevol sistema operatiu. Per exemple amb les eines adequades es pot accedir a un sistema Linux des de Windows en una màquina amb arrancada Dual.
- **Bon ús**
  - Recuperació de dades en caos d'emergència, reparacions, etc.

Round 1: Simplicitat i comoditat WINS! Xifrar el disc dur és complicat i gestionar contrasenyes d'accés requereix temps

Autor: Sergi Tur Badenas

Seguretat en xarxes

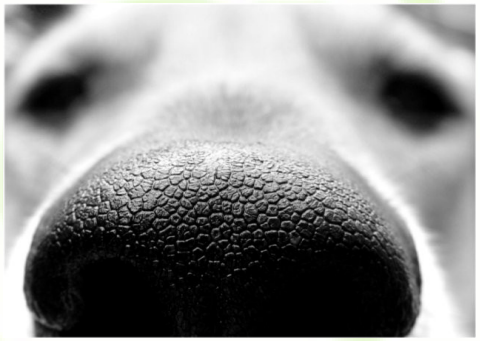
- **Mites**
  - La utilització de commutadors (switchs) ha fet que les xarxes LAN siguin segures
  - Els protocols que utilitzen xifratge de dades són segurs (SSH, HTTPS, SSL, etc.)
  - La majoria d'atacs que rep una xarxa són a través d'Internet
- **Les xarxes són insegures per definició i història**
  - Al principi ningú es preocupava per la seguretat. Tots les protocols eren sense xifrar (Telnet, FTP, HTTP, etc.)
  - Actualment encara s'arrossega aquesta tendència
  - Encara que un protocol estigui xifrat és susceptible a un robatori d'identitat

Autor: Sergi Tur Badenas

Packet Sniffers

És un programari o sistema de maquinari que pot interceptar i enregistrar el trànsit que circula per un segment de xarxa

- També coneguts com a Analitzadors de Xarxa o Analitzadors de protocols.
- Tipus de xarxes:
  - **Ethernet sniffers**
  - **Wireless sniffers**



- Durant la captura de paquets ofereixen eines per descodificar i analitzar els protocols i especificacions més comuns.
- Packet Sniffer a la wikipedia

Autor: Sergi Tur Badenas

Packet Sniffers

- **Utilitats "legals":**
  - Monitoritzar l'ús de la xarxa i/o realitzar estadístiques
  - Analitzar problemes de xarxa
  - Detectar intrusions a la xarxa
  - Espiar la xarxa i obtenir informació sensible (contrasenyes, documents secrets, etc.)
  - Enginyeria inversa de protocols
  - Depurar aplicacions client/servidor o implementacions de protocols
  - Depurar problemes de connectivitat

Autor: Sergi Tur Badenas

Ethereal (WireShark)

- **Característiques:**
  - Ethereal és un analitzador de protocols utilitzat per analitzar i solucionar problemes de xarxes de comunicacions.
  - És similar a Tcpdump però amb una interfície gràfica i moltes opcions extres d'organització i filtratge de la informació.
  - Com Tcpdump és un codi obert està disponible per gairebé totes les plataformes (UNIX/LINUX, MAC OS i Windows).

Autor: Sergi Tur Badenas

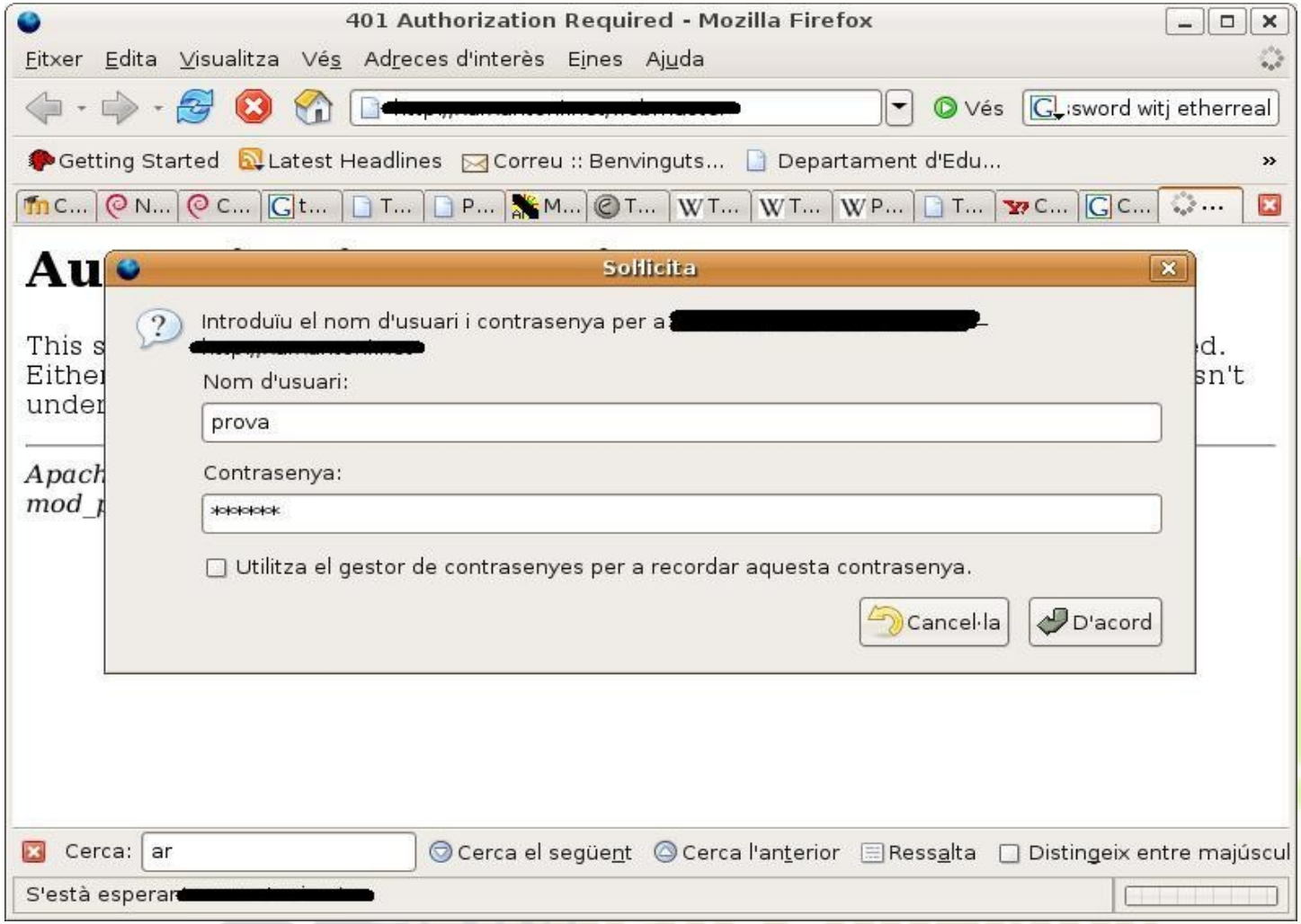
Ethereal

- **Utilitats:**
  - Anàlisi i solució de problemes en xarxes de comunicacions.
  - Desenvolupament de software i protocols.
  - Eina didàctica per a l'educació que permet visualitzar el comportament de diferents protocols i veure els paquets i trames concrets que s'utilitzen.
  - Altres usos menys didàctics (Sniffer, capturar contrasenyes...)

Autor: Sergi Tur Badenas

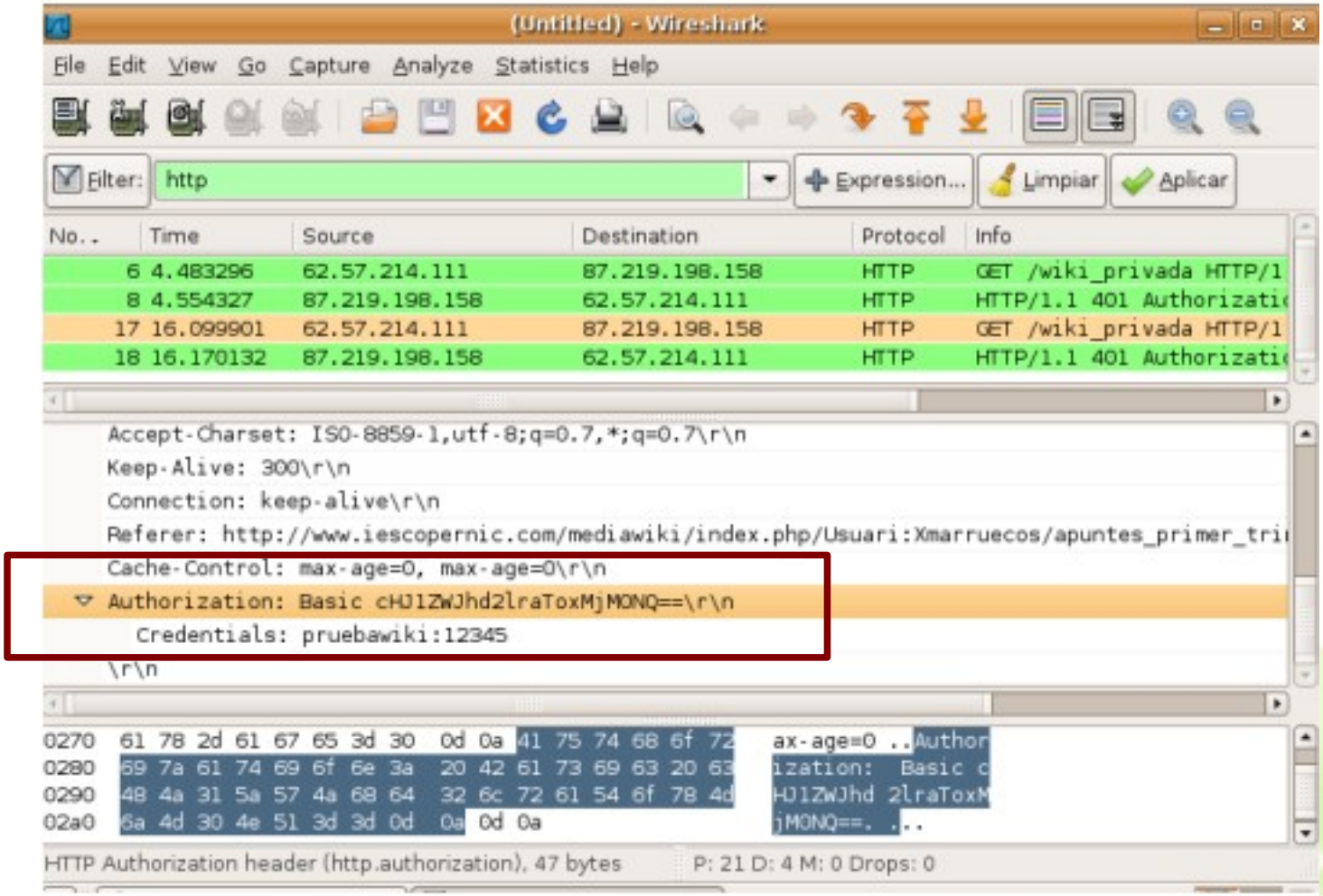
Ethereal. Captura contrasenyes HTTP

- **Exemple. Captura paraula de pas web.**



Autor: Sergi Tur Badenas

Ethereal. Captura contrasenyes HTTP



Round x: Torna a guanyar per el servei (facilitat d'ús, simplicitat) a la seguretat

Autor: Sergi Tur Badenas

Seguretat xarxes LAN

- **Mites**
  - Les xarxes LAN commutades són immunes a l'sniffing
- **Xarxes LAN Commutades**
  - L'exemple que hem vist anteriorment no serveix per veure el trànsit d'un màquina de la xarxa si la xarxa és commutada (utilitza un Switch)
  - Però això no implica que no hi hagin altres tècniques

Autor: Sergi Tur Badenas

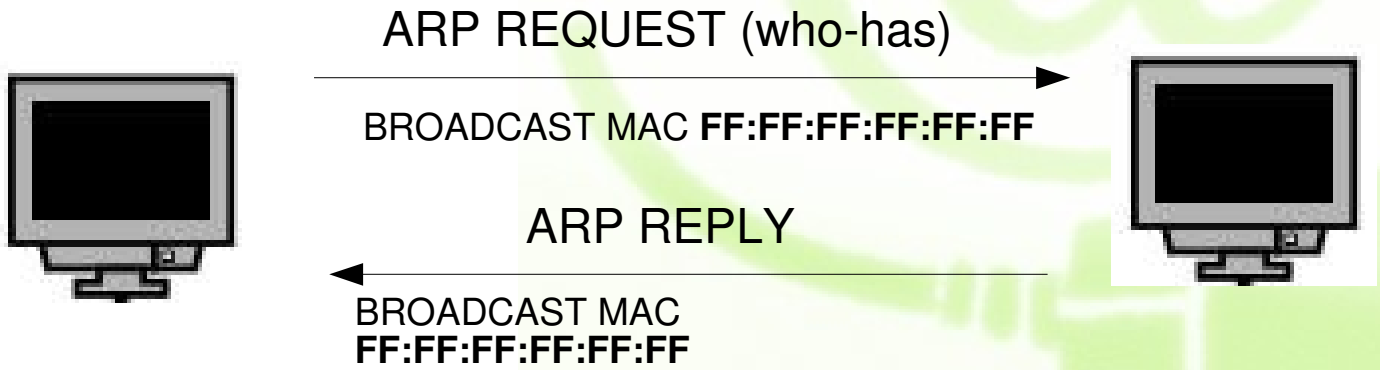
Switched LAN. Hubs i Switchs

- **Les LAN connectades a *switchs* o *hubs* tenen una topologia física d'estrella.**
- **Topologia lògica:**
  - **HUB:** mateix segment de xarxa (bus compartit). Treballa a nivell físic (mecànic). Dispositiu “ximple” (dumb)
  - **Switch:** s'utilitza una base de dades per recordar les MAC de cada port i es connecta de forma directa als ports d'origen i destinació d'una comunicació. Treballa a nivell d'enllaç (taula de MACS). Dispositiu intel·ligent.
    - LAN Commutada. Cada PC té el seu propi segment de xarxa no compartit.
    - Els commutadors són més segurs.
  - Però les xarxes *Ethernet* són insegures per disseny

Autor: Sergi Tur Badenas

Protocol ARP

- **ARP és un protocol a cavall entre el nivell de xarxa i el nivell d'enllaç (MAC)**
  - Permet resoldre adreces MAC a partir d'adreces IP.
  - S'utilitza en xarxes LAN (nivell 2) per poder treballar amb adreces IP (nivell 3)




```
$ sudo tcpdump
17:51:38.740533 arp who-has 192.168.1.2 tell mygateway1.ar7
17:51:38.740550 arp reply 192.168.1.2 is-at 00:30:1b:b7:cd:b6 (oui Unknown)
```


Autor: Sergi Tur Badenas

Protocol ARP

- **Exercici:**
  - Consultem la taula ARP

```
$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
mygateway1.ar7           ether   00:15:E9:CA:34:A5   C                     eth0
```

  - Executem alguna comanda que obligui a fer un broadcast de la xarxa (utilitzar totes les IPs)

```
$ ping 192.168.1.255 -b

$ sudo nmap 192.168.1.1-255
```

  - Tornem a consultar la taula ARP i podrem comprovar com ja tenim assignades les adreces MAC a adreces IP de tots els PC de la xarxa

Round x: torna a guanyar pel servei (facilitat d'ús, simplicitat) a la seguretat

Autor: Sergi Tur Badenas

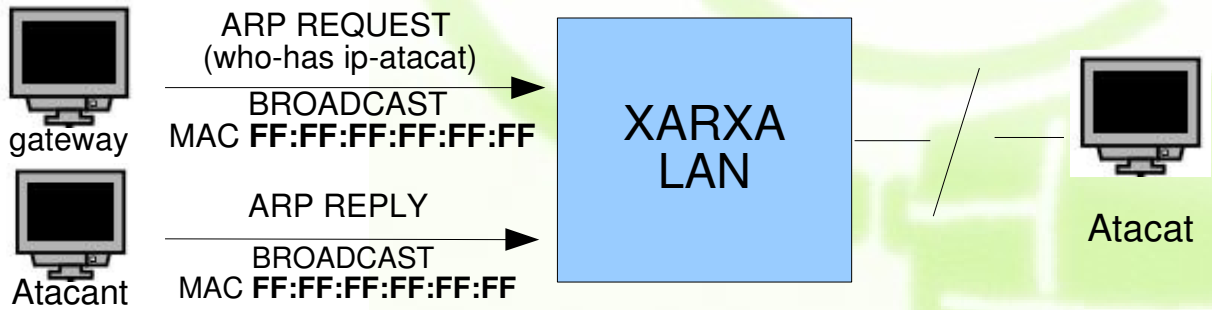
ARP Spoofing (Enverinament ARP)

- **ARP Spoofing (farsa arp)**
  - És un atac empleat en xarxes Ethernet que permet a un atacant interceptar trames d'una xarxa LAN.
  - L'atacant pot fer tres tipus d'atac:
    - **Atac passiu**: les trames interceptades no són modificades i s'envien als corresponents receptors.
    - **Atac actiu**: pot modificar les trames injectant dades.
    - **Aturar el tràfic**: atac de denegació de servei.
  - És necessari executar l'atac des d'una màquina de dins la xarxa Ethernet i les màquines que es poden atacar han de pertànyer al mateix segment de xarxa.
    - ARP Spoofing a la wikipedia
    - Spoofing a la wikipedia

Autor: Sergi Tur Badenas

ARP Spoofing

- **Com funciona?**
  - Enviant missatges AR falsos (fake frames).
  - S'envia un arp-reply fals associant la MAC de l'atacat a la IP de l'atacant. Els paquets s'envien a l'atacant en comptes de a l'atacat.
    - L'atacant pot escollir entre ser ***passiu*** (un cop llegides les trames les **reenvia** a l'atacat) o ***actiu*** (**injectar** o **modificar** dades **abans de reenviar** – **Man in the Middle**)



    - **DoS atack (Deny of Service):** s'assigna una IP no existent a la MAC de l'atacat o al seu gateway per defecte.

Autor: Sergi Tur Badenas

Ettercap

"Even if blessed with a feeble intelligence, they are cruel and smart..."

- És la descripció d'un Ettercap, un monstre del joc de rol Advanced Dungeons & Dragons.
- Es va escollir per la seva similitud amb la paraula **"ethercap"** (ethernet capture) i perquè el monstre té un **poderós verí** (ARP Poisoning).

The Lord Of The (Token)Ring
(the fellowship of the packet)

"One Ring to link them all, One Ring to ping them, one Ring to bring them all **and in the darkness sniff them**."

Autor: Sergi Tur Badenas

Ettercap

- **Funcions i característiques**
  - Suporta diferents protocols (inclosos els protocols xifrats com SSH1 o HTTPS/SSL) de forma activa i passiva.
  - Permet injectar dades (p. ex. una comanda) en una connexió establerta i filtrar en temps real en mode MiTM (Man in The Middle Attack).
- **Plug-ins**
  - Col·lectors de paraules de pas: Telnet, FTP, POP, Rlogin, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, Napster, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, Half-Life, Quake3, MSN.
  - **OS fingerprint**: detecció del sistema operatiu remot.
  - Matar connexions establertes i filtrat i substitució de paquets.
  - Escànner de LAN: hosts, ports oberts, serveis...
  - Detecció d'altres enverinaments ARP a la xarxa.
  - **Port Stealing:** nou mètode sense ARP-Spoofing.

Autor: Sergi Tur Badenas

Ettercap. Capturar trànsit

- **Per parelles. Dues màquines (atacat/atacant)**

```
$ sudo apt-get install telnetd
$ sudo -i
# ettercap -G
```

```
Sniff->unified Sniffing->eth0
Hosts->Scan for Hosts
Hosts->Hosts List->Eliminar màquines no volem atacar
Start->Start Sniffing
Mitm->ARP Poisnoning (Sniff remote connections)
View->Connections
```

  - Per evitar problemes només ataqueu una màquina per parella. Proveu de fer un telnet des de la màquina atacada:

```
$ telnet ip_maquina
```

- **Exemple pas a pas. Captura contrasenyes TELNET**

Autor: Sergi Tur Badenas

Ettercap

Capturar les trames ARP falses amb Tcpdump

- Funcionament correcte

```
$ sudo arp -d 192.168.1.1
$ sudo arp -d 192.168.1.3
$ sudo arp -d 192.168.1.6
$ ping 192.168.1.1
$ ping 192.168.1.3
$ ping 192.168.1.6
```

```
$ sudo tcpdump arp -n
09:54:40.061879 arp who-has 192.168.1.1 tell 192.168.1.2
09:54:40.062244 arp reply 192.168.1.1 is-at 00:15:e9:ca:34:a5
09:54:58.802487 arp who-has 192.168.1.3 tell 192.168.1.2
09:54:58.802576 arp reply 192.168.1.3 is-at 00:18:f3:fb:fc:4a
09:55:41.012054 arp who-has 192.168.1.6 tell 192.168.1.2
09:55:41.013671 arp reply 192.168.1.6 is-at 00:0e:35:29:2a:48
```

- Funcionament amb ettercap

```
10:03:11.168233 arp reply 192.168.1.3 is-at 00:30:1b:b7:cd:b6
10:03:11.168369 arp reply 192.168.1.6 is-at 00:30:1b:b7:cd:b6
10:03:11.200758 arp reply 192.168.1.2 is-at 00:30:1b:b7:cd:b6
10:03:11.200890 arp reply 192.168.1.6 is-at 00:30:1b:b7:cd:b6
10:03:11.220871 arp reply 192.168.1.6 is-at 00:30:1b:b7:cd:b6
10:03:11.221050 arp reply 192.168.1.3 is-at 00:30:1b:b7:cd:b6
10:03:11.248938 arp reply 192.168.1.2 is-at 00:30:1b:b7:cd:b6
10:03:11.249127 arp reply 192.168.1.3 is-at 00:30:1b:b7:cd:b6
10:03:11.264841 arp reply 192.168.1.6 is-at 00:30:1b:b7:cd:b6
10:03:11.264996 arp reply 192.168.1.2 is-at 00:30:1b:b7:cd:b6
```

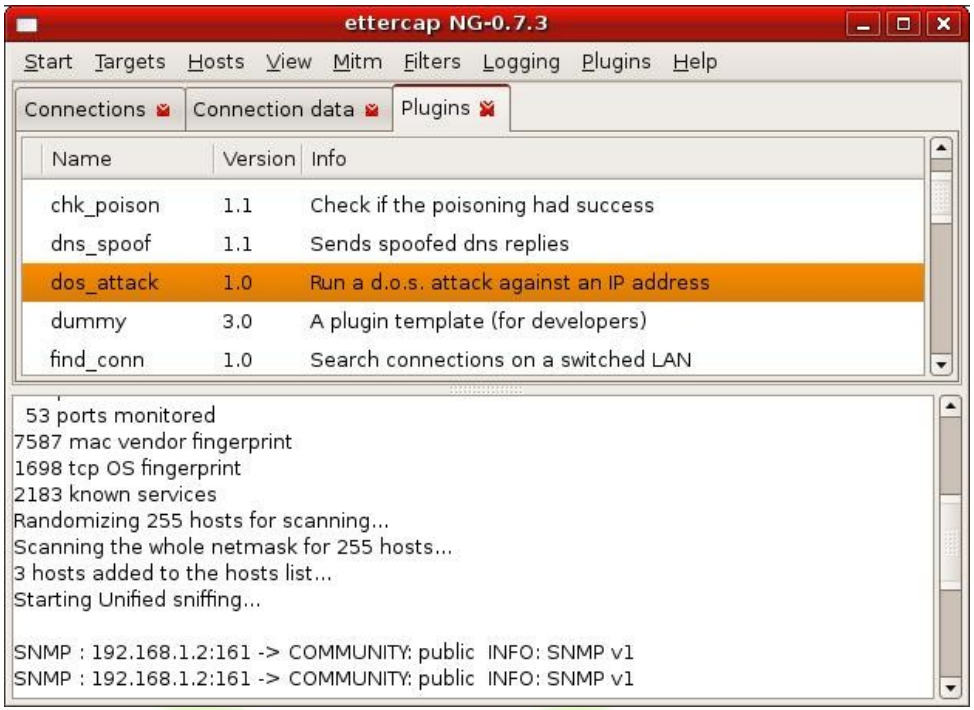
- Tothom utilitza la MAC de l'atacant!

Com funciona ettercap a la wiki del curs

Autor: Sergi Tur Badenas

Ettercap

- **Denegació de servei**
  - Plugin **dos_attack**
  - **ARP-REPLYS** que assignen una IP incorrecta a la màquina atacada.

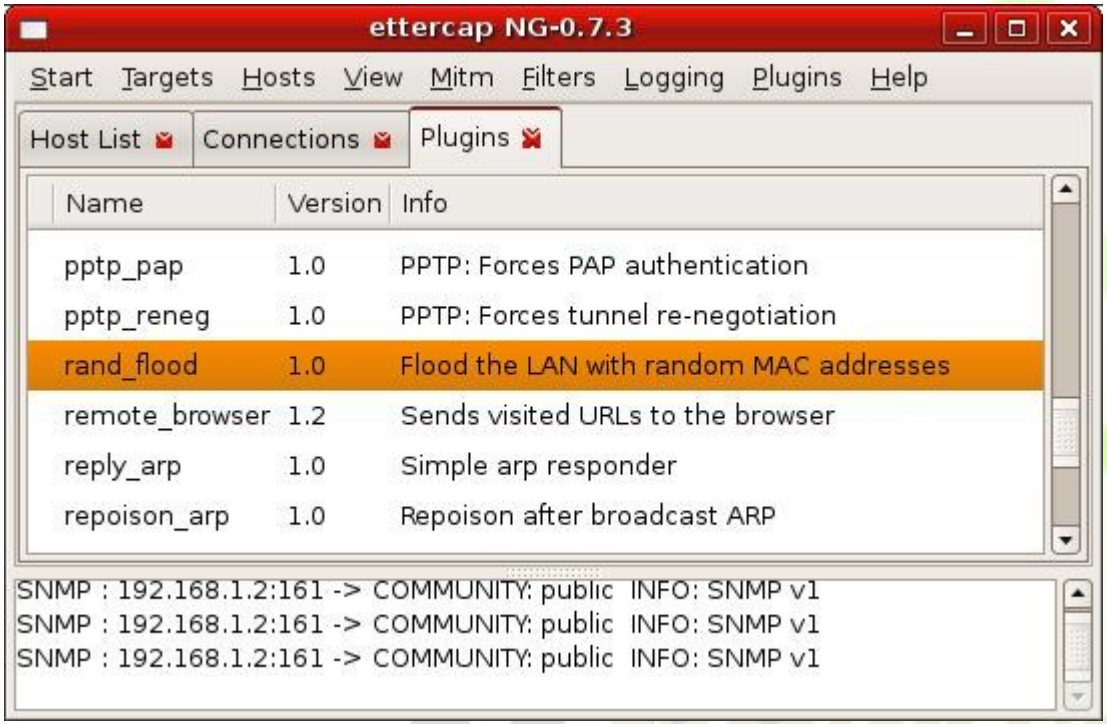



```
$ sudo tcpdump arp -n
10:13:18.926375 arp who-has 192.168.1.58 tell 192.168.1.6
10:13:19.036821 arp reply 192.168.1.58 is-at 00:30:1b:b7:cd:b6
10:13:19.039107 arp who-has 192.168.1.58 tell 192.168.1.2
10:13:19.039270 arp reply 192.168.1.58 is-at 00:30:1b:b7:cd:b6
10:13:20.039133 arp who-has 192.168.1.58 tell 192.168.1.2
10:13:20.039189 arp reply 192.168.1.58 is-at 00:30:1b:b7:cd:b6
10:13:20.956842 arp reply 192.168.1.3 is-at 00:30:1b:b7:cd:b6
10:13:20.956863 arp reply 192.168.1.6 is-at 00:30:1b:b7:cd:b6
.......................
```

Autor: Sergi Tur Badenas

MAC Flooding

- **Objectiu: desbordar la memòria del switch a base de MACs inventades**
  - Els switchs tenen una taula de MAC amb una memòria limitada. Si aquesta taula es desborda alguns switchs passen a mode "failopen" i es transformen en HUBS.




```
$ sudo tcpdump arp -n
11:07:01.746056 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.750043 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.754050 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.758355 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.762106 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.766055 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.770044 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.774052 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.778046 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.782045 arp who-has 0.0.0.0 tell 0.0.0.0
11:07:01.786079 arp who-has 0.0.0.0 tell 0.0.0.0
```


Autor: Sergi Tur Badenas

ARP SPOOFING

- **Defenses/Solucions**
  - Utilitzar un sistema de taules ARP estàtiques. Difícil de mantenir en xarxes grans.
  - **DHCP Snooping:** amb DHCP, el dispositiu de xarxa manté una llista de les adreces MAC connectades a cada port (switchs gestionats o d'alta gama).
  - **Arpwatch:** programa que permet detectar quan hi ha arp-reply falsos i envia una notificació per correu electrònic.
  - **RARP:** ARP invers.

Autor: Sergi Tur Badenas

BACKTRACK i altres eines

- **Hi ha vàries Distribucions Linux orientades a l'auditoria de xarxes**
  - BackTrack
  - nUbuntu
  - Knoppix STD

- **Són eines molt adequades per aprendre més coses sobre xarxes**

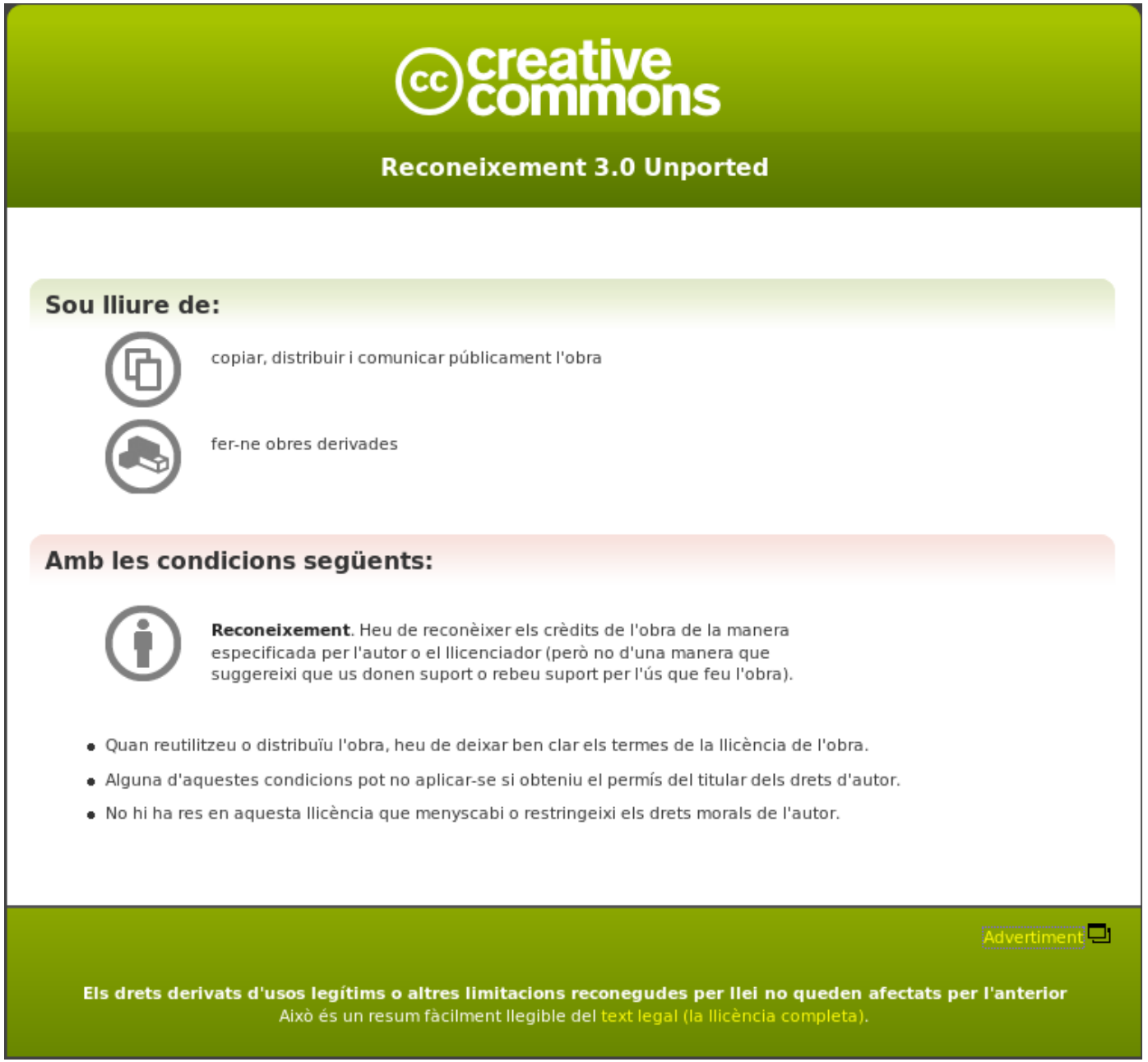
Autor: Sergi Tur Badenas

Més informació

- **Curs de Seguretat en xarxes en format Moodle**
  - El podeu trobar al Campus Virtual del centre (Moodle)
  - http://www.iescopernic.com/moodle
  - Seguretat en xarxes informàtiques
  - Altres cursos
    - Cursos Moodle Sergi Tur
- **Documentació a la wiki del ponent**
  - ARP SPOOFING
  - Ettercap
  - Man in The Middle Atacks

Autor: Sergi Tur Badenas

Llicència Creative Commons



http://creativecommons.org/licenses/by/3.0/deed.ca

Autor: Sergi Tur Badenas