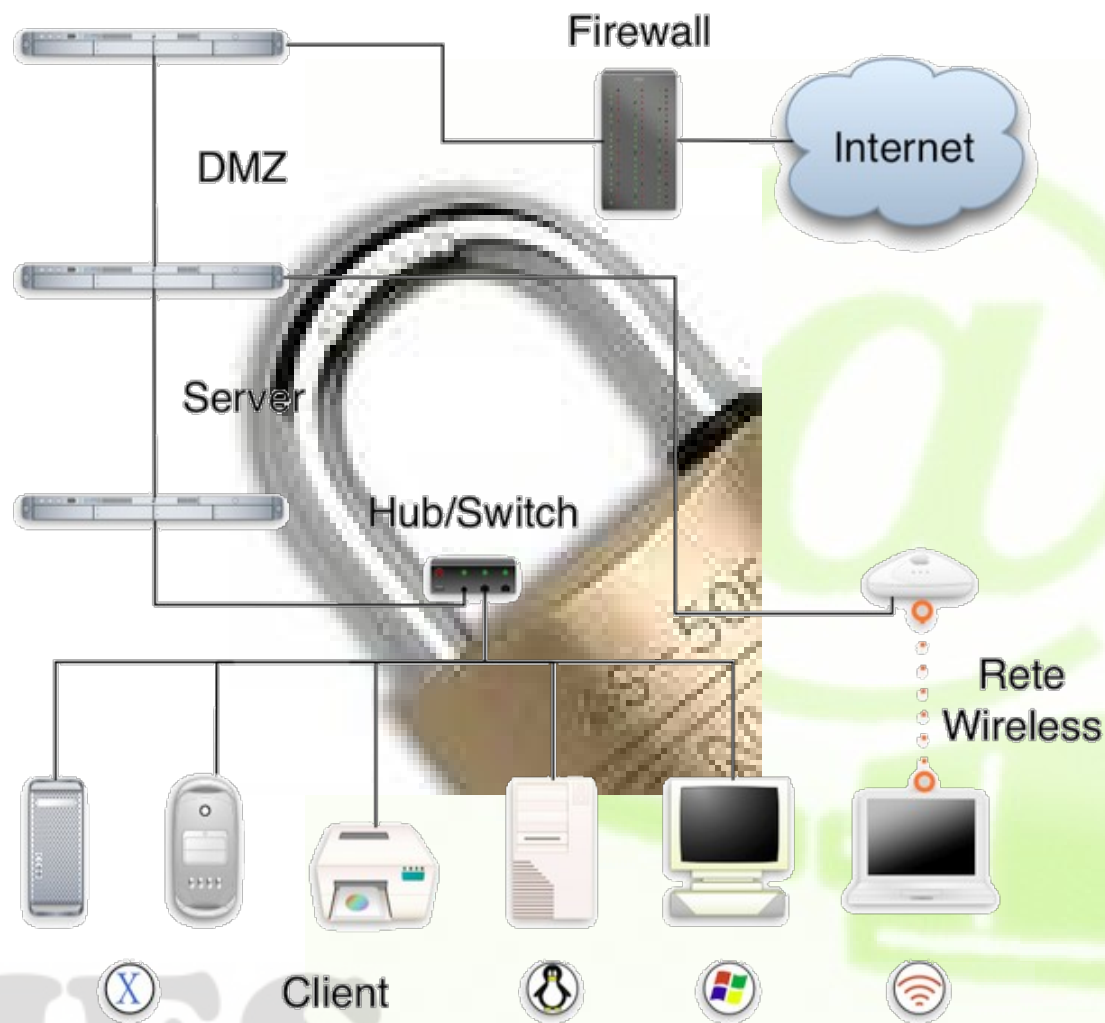




Taller de seguretat en xarxes





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



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 de forma similar a que l'inventor de l'energia nuclear no és el responsable de les Bombes d'Hiroshima ni totes les persones que fabriquen bombes són terroristes.



Legalitat i moralitat

♦ 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



Legalitat i moralitat

♦ Estem legalment prou protegits en aquests aspecte?

♦ LOPD: Llei Orgànica de Protecció de Dades

- Quantes actuacions s'han dut a terme per accions poc ètiques com per exemple:
 - Aconseguir l'usuari i la contrasenya d'un compte de correu i posteriorment bloquejar-ne l'accés modificant la contrasenya?
 - Explotar comercialment les dades estadístiques de visites de pàgines web a través d'un proxy "gratuït"?
 - És legal el que fa Google a l'utilitzar estadísticament les nostres dades d'us del correu Gmail?

♦ Tenim la oportunitat de preguntar-li a un expert durant el seminari de **Delicte Informàtic**

Més val prevenir que curar (sobretot en temes jurídics ;-))



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



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**



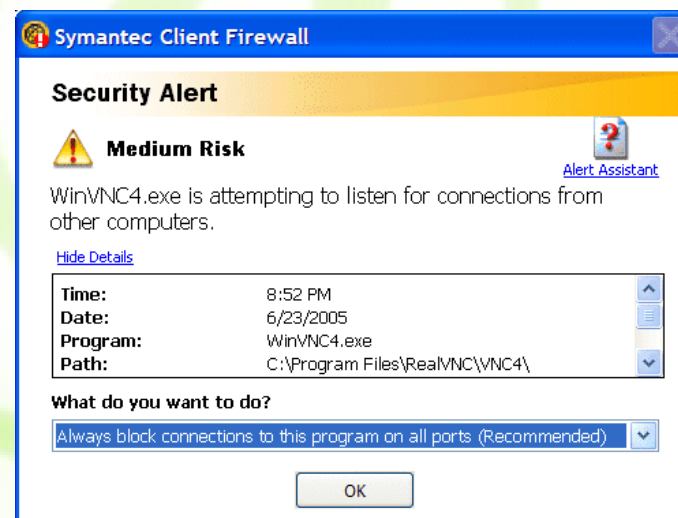
Alarmisme

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**.





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 desinformatats.
 - ♦ Per exemple és força senzill fer una transparència divertida que porti un “regalet” al darrere.



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 dígit!
- ♦ Que creieu què és més probable actualment: que ens ataquï 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



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

IES
Nicolau Copèrnic



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



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 Obscurity
VS
Security by Design



Security Through 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.



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.



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.



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



Criptografia

♦ Mite

- ♦ Els protocols que utilitzen xifratge de dades són 100% segurs (SSH, HTTPS, SSL, etc.)

♦ És la criptografia actual segura?

- ♦ És difícil de saber ja que la resposta depèn de molts factors
- ♦ No existeix el sistema criptogràfic perfecte
- ♦ Sistemes criptogràfics considerats segurs fa pocs anys, actualment ja han estat trencats
- ♦ Però sí que existeixen sistemes que **FINS ARA NO S'HA DEMOSTRAT PÚBLICAMENT** que es puguin trencar



Criptografia

- ♦ **La transparència ajuda a fer la informàtica més segura**
 - ♦ Hi ha múltiples concursos patrocinats per les pròpies companyies de seguretat amb premis importants per aquelles persones que demostrin la vulnerabilitat d'un sistema criptogràfic
 - [RSA_Factoring_Challenge](#)
 - Actualment ja s'han trencat codis RSA-640 utilitzant 5 mesos de processament amb 80 CPUs AMD a 2.2 Ghz
 - Hi ha un premi de \$200,000 USD per qui trenqui **RSA-2048**
- ♦ **Atenció!**
 - ♦ Sistemes criptogràfics com SSL o SSH són susceptibles a atacs Man-In-The-Middle



Criptografia

- ♦ **Qui ens pot assegurar que ningú coneix sistemes per trencar sistemes criptogràfics que actualment es consideren segurs?**
 - ♦ Per què Estats Units impedeix la exportació de certs Sistemes Criptogràfics a certs països?
 - ♦ Agències com la NSA o el FBI tenen sistemes per desxifrar aquests sistemes? El que és segur és que ho intenten:
 - **Carnivore:** Packet Sniffer del FBI
 - **Echelon:** Programa d'intercepció de comunicacions global de la NSA
 - **SELinux:** una “característica” de seguretat que porten algunes distribucions Linux on la NSA està involucrada



Windows. Trucs de seguretat?

♦ Exemples extrets d'una “revista d'informàtica”:

- ♦ **Verificar que totes les particions de disc estan formatades en NTFS**
 - Com? Els “avantatges” de NTFS no seran uns altres que no tenen res a veure amb la seguretat?
- ♦ **Protegir adequadament les carpetes compartides**
 - Com ho fem si resulta que les contrasenyes de SMB/CIFS es poden *sniffar* i trencar utilitzant eines com Ettercap i Ophcrack (amb taules específiques)
- ♦ **Habilitar el tallafocs i l'antivirus**
 - Ja hem parlat d'aquesta solució
- ♦ **Mantenir-se al dia amb actualitzacions de seguretat**
 - I d'aquesta manera serà Microsoft i no tu qui controlarà el teu PC i decidirà el que és bo per a tu com a usuari.



Windows. Trucs de seguretat?

- ♦ **Utilitzar paraules de pas per als comptes d'usuari**
- ♦ **Implantar polítiques de paraules de pas estrictes**
 - Només serveixen per protegir d'accessos puntuals.
 - Eines com *Ophcrack* demostren clarament que això no és cert.
 - De fet, si ens estimem la nostra contrasenya més val no posar-la a Windows.
- ♦ **Implantar polítiques de bloqueig de comptes**
 - I així afegim una vulnerabilitat més al sistema: un atacant intenta entrar tres cops i ens bloqueja l'accés!!! Genial!
- ♦ **Inhabilitar els serveis innecessaris**
- ♦ **Inhabilitar o eliminar els comptes d'usuari innecessaris**
 - Certes! Tornem, però, al compromís Servei vs Seguretat.



Paraules de pas

♦ Mite

- ♦ 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.

♦ Aquestes frases són parcialment certes

- ♦ Les paraules de pas milloren la seguretat però no són la solució definitiva.
- ♦ Les contrasenyes s'han de guardar físicament en algun lloc. Normalment és guarden xifrades.
- ♦ Tot sistema de xifratge és susceptible de ser atacat per força bruta.



Paraules de pas

- ♦ **El xifratge utilitzat és important**
 - ♦ Hi ha sistemes que tenen errors de disseny o vulnerabilitats comprovades
- ♦ **En Windows les paraules de pas no són segures**
 - ♦ Tenen un altra filosofia:

2005, un expert de Microsoft declara: "crec que la política sobre paraules de pas hauria de ser escriure les contrasenyes en algun lloc per poder recordar-les. Jo tinc 68 contrasenyes diferents. Si no em permeten escriure-les endevina què faré; doncs utilitzar sempre la mateixa!"

- ♦ Però aquestes polítiques són només per comoditat de treball o hi ha alguna raó més oculta?

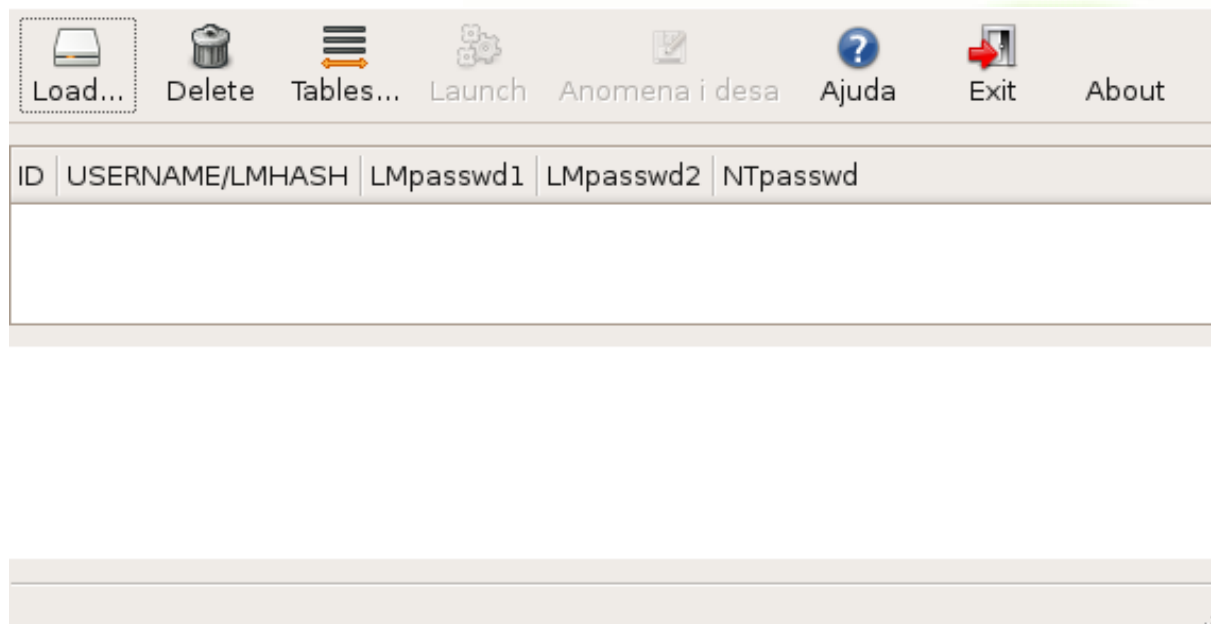


- ♦ **Ophcrack és un cracker de contrasenyes de Windows**
 - ♦ Utilitza **rainbow table** per trencar les paraules de pas
 - Taules gratuïtes:
 - SSTIC04-5k (720MB) màquines amb mínim de 500Mb de RAM
 - SSTIC04-10k (388MB) màquines menys potents
 - **Tant per cent èxit: 99.9%**
 - Taules de pagament: per trencar contrasenyes SMB/CFIS
 - ♦ Multiplataforma (Windows, Mac OS X, Linux)
 - ♦ Hi ha una versió en Live-CD a la web
 - ♦ Hi ha una solució simple per ser immune a les taules d'arcs de sant martí (utilitzada a totes les distribucions Linux)
- ♦ **<http://ophcrack.sourceforge.net/index.php>**



Opchcrack

♦ Menú Aplicacions/Accessoris/Opchcrack



♦ Afegiu les taules. Icona Tables

IES Nicolau Copèrnic



Ophcrack

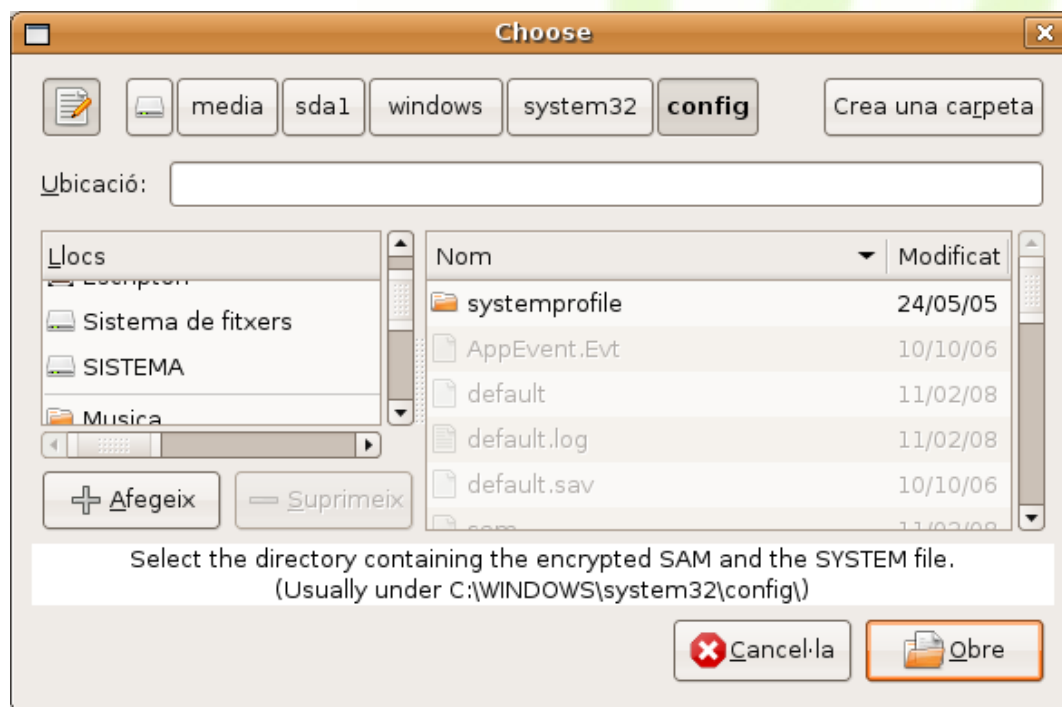
- ♦ **Seleccionem la taula SSTIC04-5k**
 - ♦ La trobareu al vostre escriptori dins la carpeta SSTIC04-5k





Ophcrack

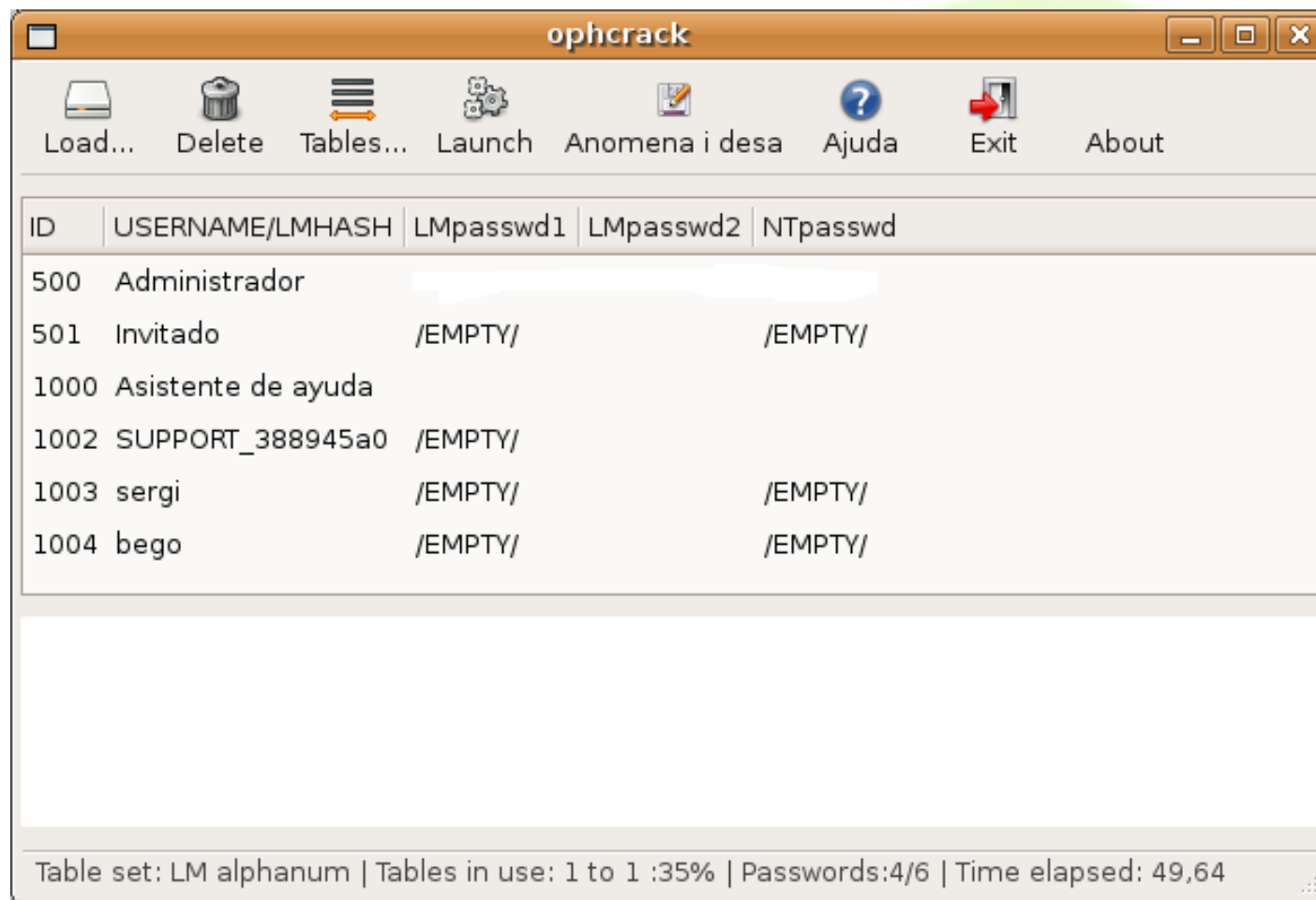
- ♦ **Ara carreguem les contrasenyes de Windows**
 - ♦ Feu clic al botó Load i escolliu l'opció From Encrypted SAM
 - ♦ **SAM (Security Accounts Manager)** és la base de dades de contrasenyes de Windows
 - ♦ Aneu a Sistema /media/sda1/Windows/System32/config





Ophcrack

- ♦ **Voilà! Ja teniu les contrasenyes**





Ophcrack

♦ Solució

- ♦ No utilitzar Windows ;-)
- ♦ Utilitzar sistemes operatius lliures o al menys donar-los suport ;-)
- ♦ Pressionar a Windows perquè faci més segurs els seus sistemes?
- ♦ Hi ha algunes solucions molt simples a aquest problema i que podrien estar implementades per defecte a Windows.
- ♦ Les solucions es deixen com exercici per al lector (entre d'altres coses perquè el ponent fa temps que no treballa per Microsoft)



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

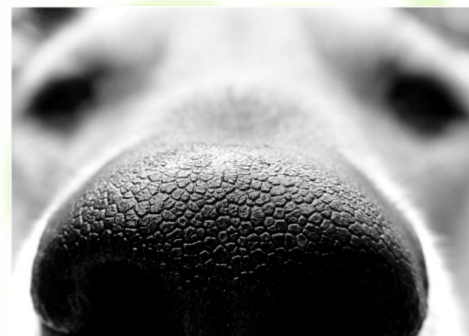
- ♦ Al principi ningú es preocupava per la seguretat. Tots les protocols eren sense xifrar (Telnet, FTP, HTTP, etc.)
- ♦ Actualment encara s'arrossega aquesta tendència
- ♦ Encara que un protocol estigui xifrat és susceptible a un robatori d'identitat



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](#)



IES
Nicolau Copèrnic



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



IES Nicolau Copèrnic



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).

IES Nicolau Copèrnic



Ethereal

♦ Utilitats:

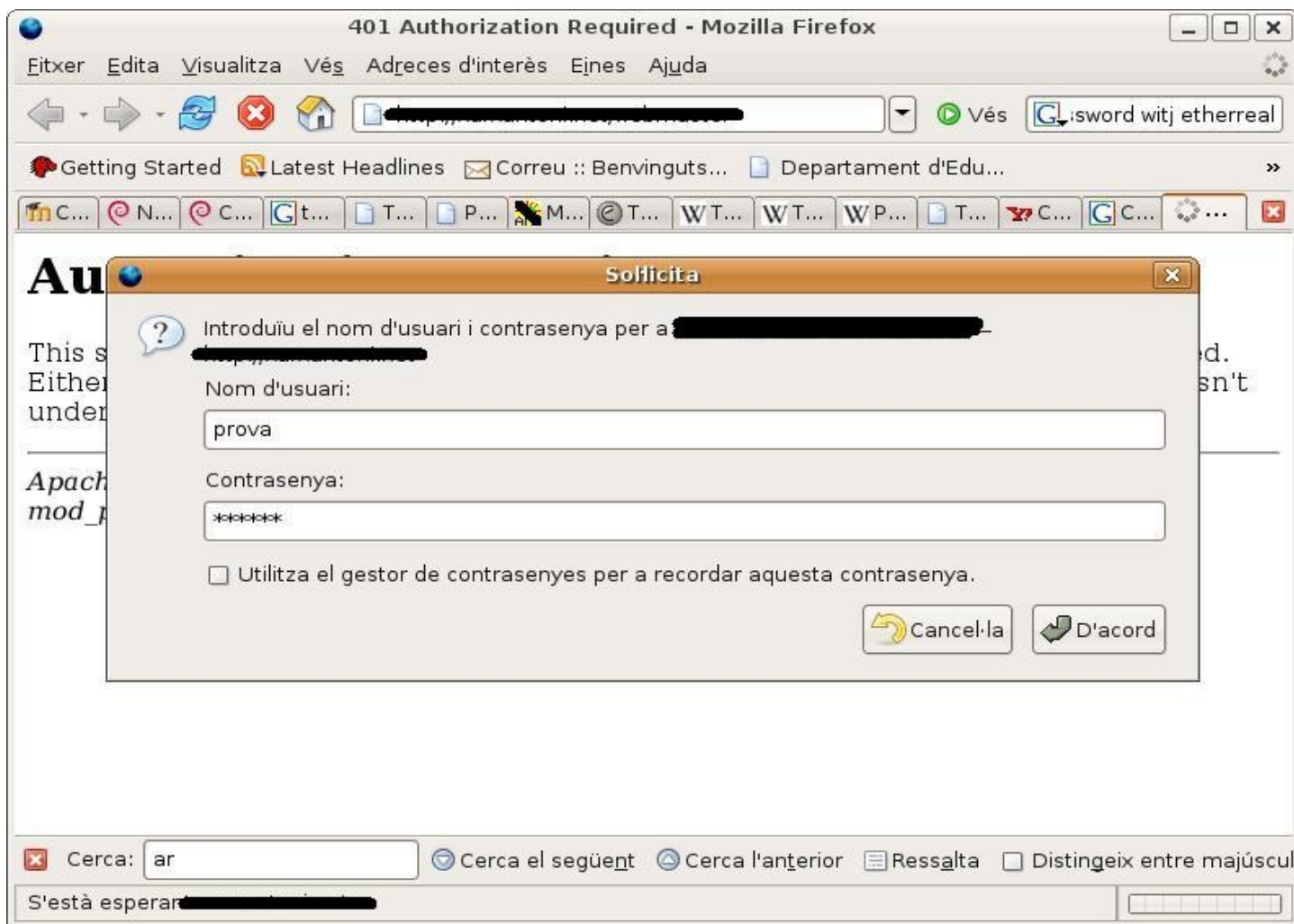
- ♦ Anàlisi i solució de problemes en xarxes de comunicacions.
- ♦ Desenvolupament de software i protocols.
- ♦ Eina didàctica per a l'educació que permet visualitzar el comportament de diferents protocols i veure els paquets i trames concrets que s'utilitzen.
- ♦ Altres usos menys didàctics (Sniffer,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

IES Nicolau Copèrnic



Ethereal. Captura contrasenyes HTTP

♦ Exemple. Captura paraula de pas web.





Ethereal. Captura contrasenyes HTTP

Wireshark (Untitled) - Wireshark

Filter: http

No.	Time	Source	Destination	Protocol	Info
6	4.483296	62.57.214.111	87.219.198.158	HTTP	GET /wiki_privada HTTP/1
8	4.554327	87.219.198.158	62.57.214.111	HTTP	HTTP/1.1 401 Authorizati
17	16.099901	62.57.214.111	87.219.198.158	HTTP	GET /wiki_privada HTTP/1
18	16.170132	87.219.198.158	62.57.214.111	HTTP	HTTP/1.1 401 Authorizati

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

Referer: http://www.iescopernic.com/mediawiki/index.php/Usuari:Xmarruecos/apuntes_primer_tri

Cache-Control: max-age=0, max-age=0\r\n

Authorization: Basic cHJlZWJhd2lraToxMjMONQ==\r\n

Credentials: pruebawiki:12345

0270 61 78 2d 61 67 65 3d 30 0d 0a 41 75 74 68 6f 72 ax-age=0 ..Author

0280 59 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 63 ization: Basic c

0290 48 4a 31 5a 57 4a 68 64 32 6c 72 61 54 6f 78 4d HJlZWJhd 2lraToxM

02a0 6a 4d 30 4e 51 3d 3d 0d 0a 0d 0a jMONQ==. ...

HTTP Authorization header (http.authorization), 47 bytes P: 21 D: 4 M: 0 Drops: 0

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



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

IES
Nicolau Copèrnic



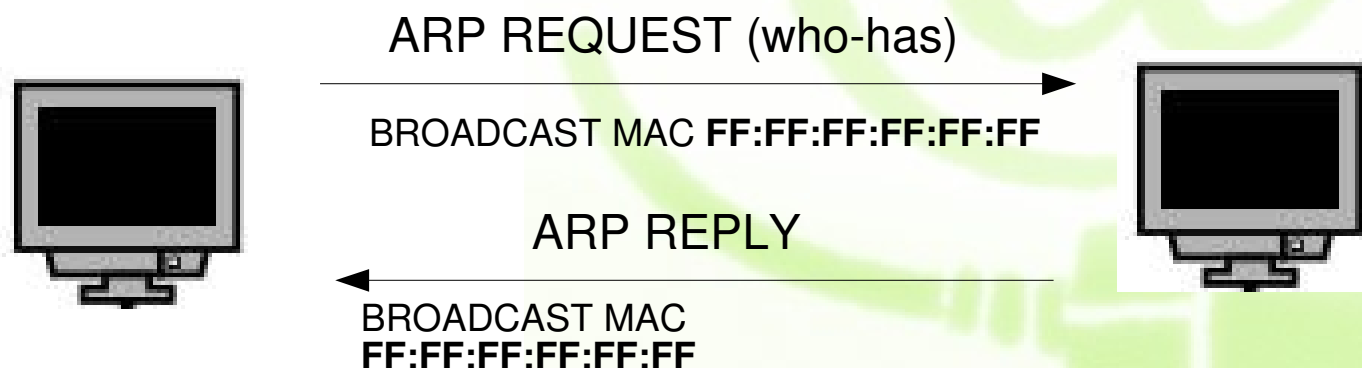
Switched LAN. Hubs i Switchs

- ♦ **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



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)
```



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



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](#)

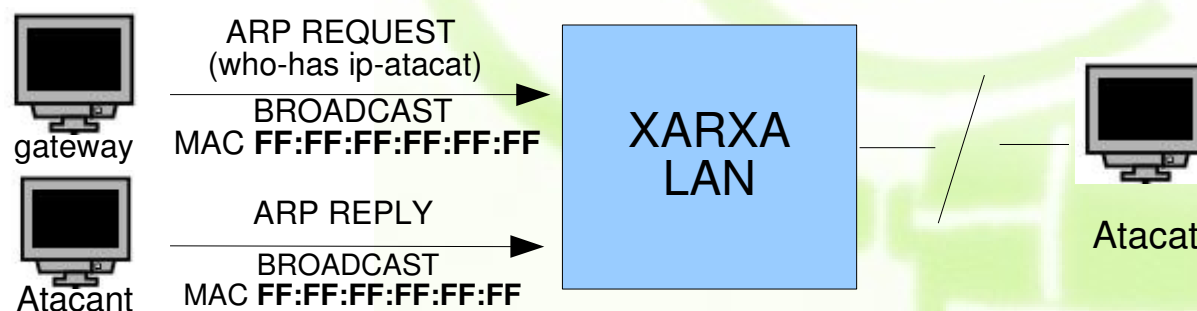




ARP Spoofing

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



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.**"





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.
- ◆ Escàner de LAN: hosts, ports oberts, serveis...
- ◆ Detecció d'altres enverinaments ARP a la xarxa.
- ◆ **Port Stealing:** nou mètode sense ARP-Spoofing.



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 Poisoning (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



Ettercap

▶ Capturar les trames ARP falses amb Tcpcap

◆ 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

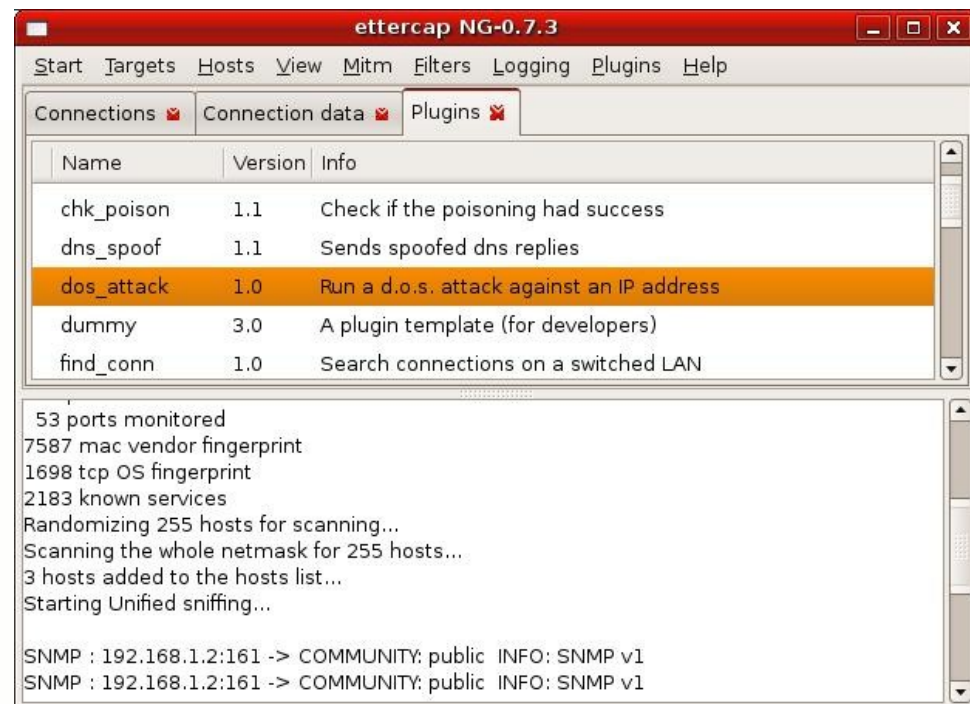


Ettercap

◆ 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
.....
```

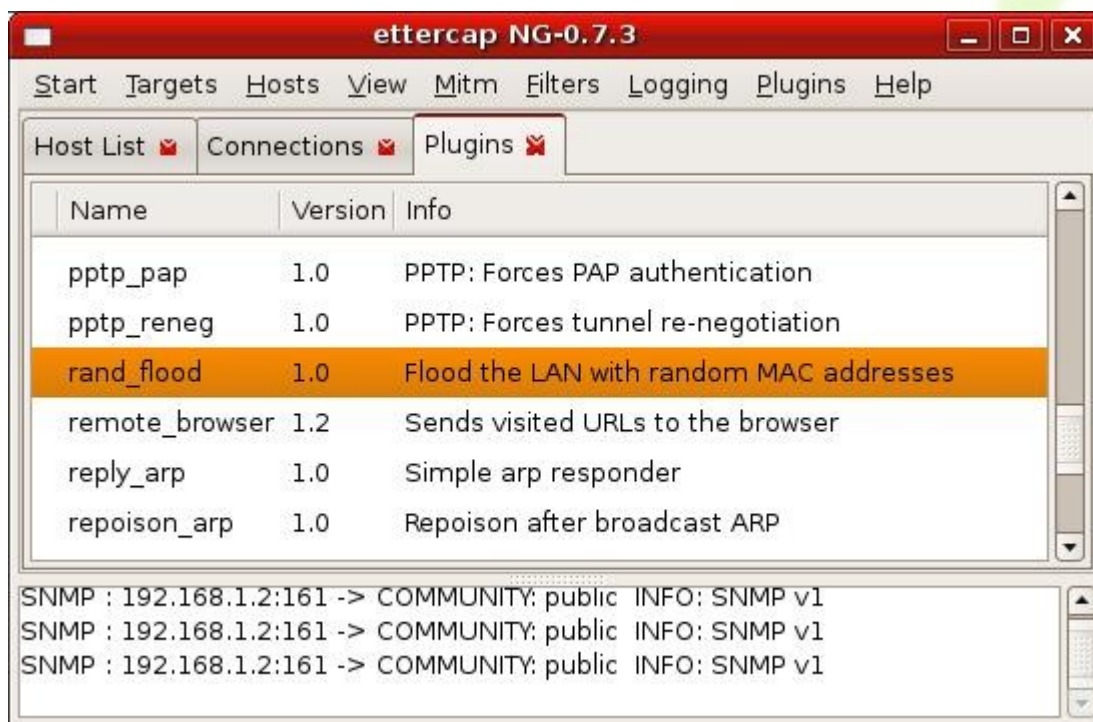




MAC Flooding

♦ 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
```



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.

IES
Nicolau Copèrnic



BACKTRACK i altres eines

- ♦ **Hi ha varies Distribucions Linux orientades a l'auditoria de xarxes**

- ♦ BackTrack
- ♦ nUbuntu
- ♦ Knoppix STD



for the security aware

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

IES Nicolau Copèrnic



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 Attacks



Reconeixement 3.0 Unported

Sou lliure de:



copiar, distribuir i comunicar públicament l'obra



fer-ne obres derivades

Amb les condicions següents:



Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador (però no d'una manera que suggereixi que us donen suport o rebeu suport per l'ús que feu l'obra).

- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.
- No hi ha res en aquesta llicència que menyscabi o restringeixi els drets morals de l'autor.

Advertiment

Els drets derivats d'usos legítims o altres limitacions reconegudes per llei no queden afectats per l'anterior
Això és un resum fàcilment llegible del text legal (la llicència completa).

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