Eines de hacking. Sniffers. Tcpdump i Ethereal. Rootkits. Contrasenyes. Tècniques de força bruta

Autor: Sergi Tur Badenas

Eines de hacking

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 que a diferència d'aquest últim, el cracker realitza la intrusió com a benefici personal o per a fer mal.
Lamer: persona o producte que fer falta de maduresa, sociabilitat o habilitats tècniques és considerat un incompetent en una matèria o activitat específica.

- **Cultura Hacker**
  - Hacker Slang (argot hacker): Jargon File
- **Veurem algunes de les eines més famoses o importants.**
- **Hacking Tools a la wiki del curs**

Autor: Sergi Tur Badenas

Packet Sniffers

És un programari o sistema de maquinari que pot interceptar i enregistrar el tràfic 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:**
  - 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

Packet Sniffers

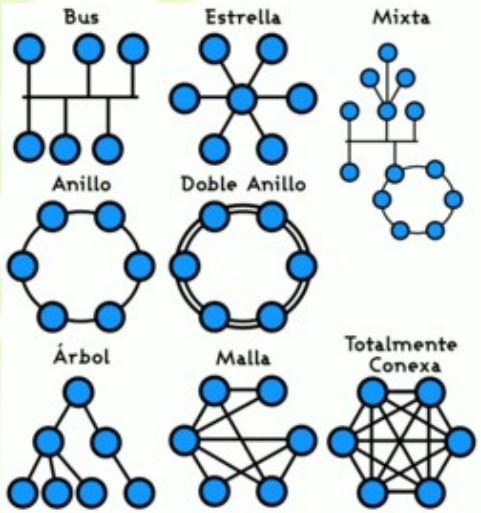
- tcpdump
- Ethereal / WireShark
- DSniff
- Ettercap
- Kismet (xarxes wireless)
- Ksniffer
- Open Source Packet Sniffer (Windows/Wincap)
- NetworkMinner
- Hi ha moltes solucions comercials que podeu consultar a la la wikipedia

Autor: Sergi Tur Badenas

Mode promiscu

És el mode en que un node (ordinador, dispositiu de comunicacions, etc.) connectat a una xarxa compartida captura tot el tràfic que circula pel node amb independència de si el tràfic és per al node o no.

- El funcionament del mode promiscu depèn molt de la tipologia (anell, bus...) i del tipus de xarxa (cablejada, sense fils...), del tipus de transmissió (unicast, broadcast) i dels dispositius de xarxa utilitzats (HUB, Switch...)
- No tots els dispositius de xarxa (targetes) ens permeten utilitzar el mode prosmiscu



Autor: Sergi Tur Badenas

Mode promiscu. Ifconfig

- **Com podem saber si som promiscus ;-)?**
  - Consultant les característiques de la nostra targeta de xarxa amb **ifconfig**

```
$ ifconfig eth0 promisc
$ ifconfig eth0
eth0  Link encap:Ethernet  HWaddr 00:80:C8:F8:4A:51
      inet addr:192.168.99.35  Bcast:192.168.99.255  Mask:255.255.255.0
      UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1412  Metric:1
      RX packets:190312 errors:0 dropped:0 overruns:0 frame:0
      TX packets:86955 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:30701229 (29.2 Mb)  TX bytes:7878951 (7.5 Mb)
      Interrupt:9 Base address:0x5000
```

```
$ ip link show | grep eth0
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
```

  - **Ifconfig a la wiki del curs**

Autor: Sergi Tur Badenas

Ethernet

- **Nivell 1 TCP/IP (Nivell físic 1 i d'enllaç 2 a OSI).**
- **Família d'estàndards IEEE 802:**
  - 802.2: **Capa LLC** (Logical Link Control). Interfície comuna entre el nivell de xarxa i la família de protocols.
  - La resta de protocols defineixen el nivell físic i el subnivell **MAC**.
    - **802.3 Ethernet**
    - 802.4 Token Ring
    - 802.11 Wi-FI
    - 802.15 Bluetooth

Autor: Sergi Tur Badenas

Ethernet

- **Nivell LLC (Logical Link control). Compartit per tots els protocols de la família.**
  - Lògica de reenviaments
  - Control de flux
  - Comprovació d'errors
- **Nivell MAC (Medium Acces Control).**
  - Control d'accés a medi compartits (cables en bus, ràdio, etc.)
  - No utilitzat en protocols punt a punt (no hi ha medi compartit)
  - **Adreça MAC**: sistema adreçament de nivell 2 equivalent a les adreces IP al nivell 3

Autor: Sergi Tur Badenas

Ethernet. Nivell MAC. Conceptes

- **Segments de xarxa**
  - És una porció de xarxa separada de la resta per un dispositiu de xarxa com:
    - Repetidor
    - Bridge o Switch
    - Router
- **Domini de col·lisió**
  - És un segment lògic de xarxa on els paquets poden col·lisionar al ser enviats a un medi compartit.

Autor: Sergi Tur Badenas

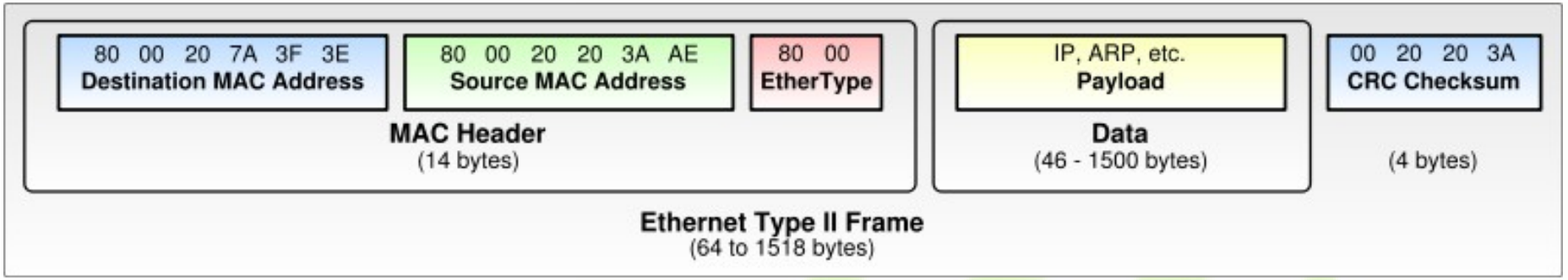
Ethernet. Nivell MAC

Algorismes MAC

- **Aloha i Aloha Ranurat** (desenvolupats per la Universitat de Hawai). S'envia un paquet i si hi ha col·lisió es torna a enviar.
- **CSMA/CD (*Carrier sense multiple access with collision detection*)**. Detecta si hi ha senyals utilitzant el medi i té un procediment en cas de col·lisió.
- Antics sistemes Ethernet funcionaven amb coaxials en bus físic i lògic.
- Actualment el problema de les col·lisions està més limitat gràcies als switches.
- Torna a ser un tema candent en xarxes wireless (l'aire és un medi compartit).

Autor: Sergi Tur Badenas

Trama Ethernet



- **Origen:** Adreça MAC origen de la trama
- **Destí:** Adreça MAC destinació de la trama
- **Tipus:** EtherType. Tipus d'ethernet.
- **Dades**
- **CRC Checksum:** Control d'errors

Autor: Sergi Tur Badenas

Switched LAN. Hubs i Switchs

- **Les LANs 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 “tonto” (dumb)
  - **Switch:** s'utilitza una base de dades per recordar les MACs (IPs) 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 switches són més segurs.

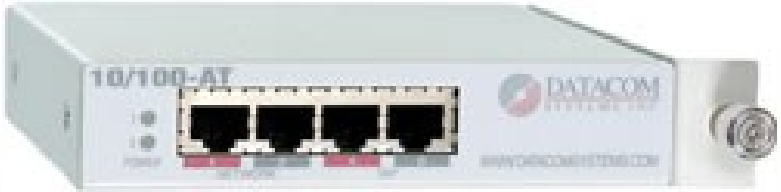
Autor: Sergi Tur Badenas

Switches

- **Tipus:**
  - **Home Switches** (no gestionats). Típics en entorns SoHo (Small Office/ Home Office).
  - **Switches gestionats** (Managed Switches).
    - Controlar el port de forma individual (on/off)
    - Control de la velocitat del link
    - Prioritats de ports
    - Filtratge MAC
    - Port Mirroring per tal de monitoritzar ports
    - Altres: Suport per SNMP, VLAN, Link Aggregation
  - **Switches intel·ligents**. Realitzen tasques de forma automàtica: establir velocitats d'enllaç, permetre connexions directes i creuades, etc.

Autor: Sergi Tur Badenas

Network Taps



- **Són dispositius de maquinari que permeten accedir a les dades que circulen per un cable de xarxa**
  - També anomenat Test Acess Port o Test Access Point
  - Útils per depurar errors
  - Hi ha sistemes més escalables per controlar la xarxa
  - Com construir el teu propi Network Tap
  - Network Tap a la wikipedia

Autor: Sergi Tur Badenas

tcpdump

Desenvolupador: The Tcpdump team
OS: gairebé tots
Llicència: lliure (BSD)

- Eina de línia de comandes que permet visualitzar el tràfic de xarxa (Packet Sniffer)
- Hi ha un “port” per a Windows (WinDump) basat en Wincap (port de libcap)
- Cal ser superusuari (root) per utilitzar tcpdump (sudo). Activa automàticament el mode promiscu
- Com gairebé el 100% d'analitzadors de xarxa utilitza la llibreria libcap
  - Tcpdump a la wiki del curs
  - Pàgina oficial
  - **man tcpdump**

Autor: Sergi Tur Badenas

tcpdump

- **Instal·lació**

```
$ sudo apt-get install tcpdump
```

- **Filtres**
  - Podem aplicar filtres segons l'origen o destinació del paquet, segons els protocol, per màquines, per xarxes, per ports...

```
$ sudo tcpdump tcp and \(port 22 or port 23\)
```

```
$ sudo tcpdump -i lo
```

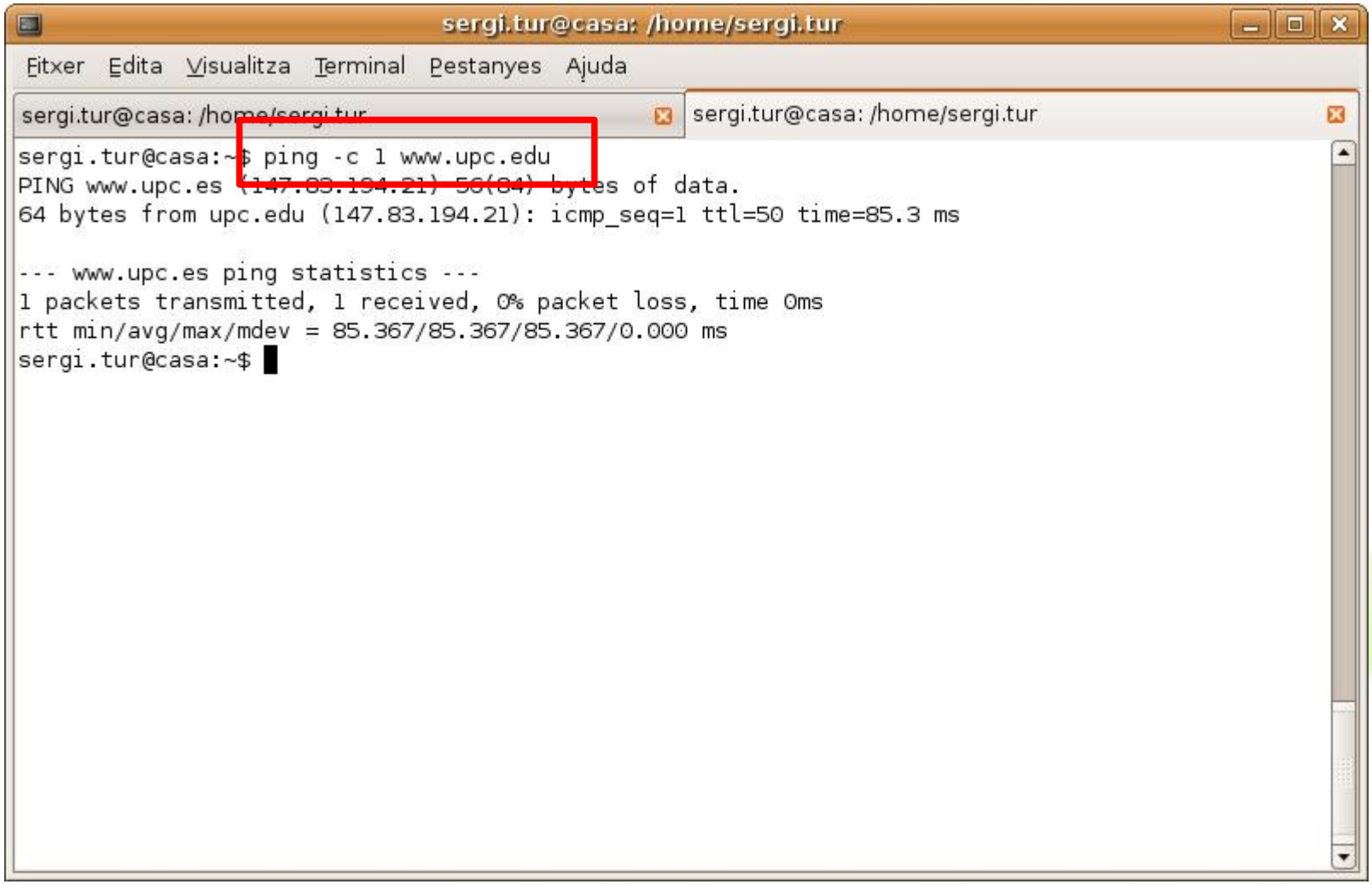
```
$ sudo tcpdump icmp
```

  - Activitat per parelles: Provem de **capturar pings**

Autor: Sergi Tur Badenas

TCPDUMP

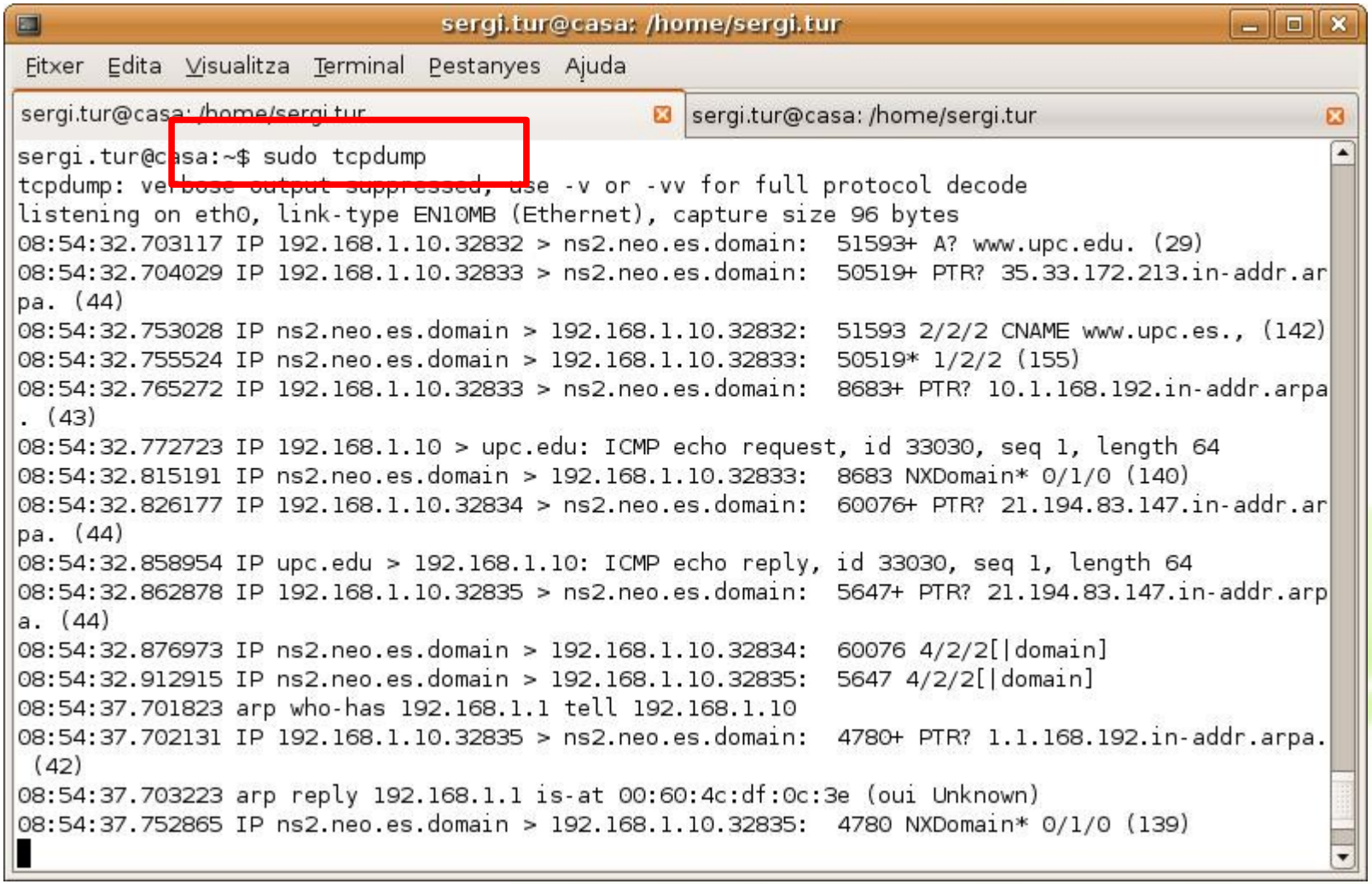
- **Exemple. Captura d'un ping**



Autor: Sergi Tur Badenas

TCPDUMP

- **Exemple. Captura d'un ping**



Autor: Sergi Tur Badenas

Protocols no segurs (no xifrats)

- **Amb tcpdump podem comprovar la inseguretat d'alguns protocols com p. ex. telnet**
  - Instal·leu **telnetd** i feu una connexió a un company

```
$ sudo apt-get install telnetd
```

```
$ telnet ip_maquina_company
```

  - Executeu tcpdump i comproveu com el text viatja en clar!

```
$ sudo tcpdump -X port 23
```

```
$ hola
-bash: hola: command not found
```

```
.....................
        0x0000:  4510 0054 d3d8 4000 4006 e365 c0a8 0103  E..T..@.@..e....
        0x0010:  c0a8 0102 0017 cca6 2241 5d60 2dca e78f  ........"A]`-...
        0x0020:  8018 05a8 0437 0000 0101 080a 1a7c 399f  .....7.......|9.
        0x0030:  0035 4475 2d62 6173 683a 2068 6f6c 613a  .5Du-bash:.hola:
        0x0040:  2063 6f6d 6d61 6e64 206e 6f74 2066 6f75  .command.not.fou
        0x0050:  6e64                                     nd
```


Autor: Sergi Tur Badenas

TCPDUMP

- **Utilitats:**
  - Per depurar aplicacions que utilitzen la xarxa per comunicar-se. Per exemple es pot utilitzar per comprovar el funcionament d'un tallafocs.
  - Per depurar la xarxa mateixa.
  - Per comprovar quan la NIC està transmetent o reben dades.
  - Per capturar i llegir dades enviades per altres usuaris o ordinadors. Un usuari que té el control d'un encaminador pel qual circula tràfic pot obtenir la informació que no viatgi xifrada.

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

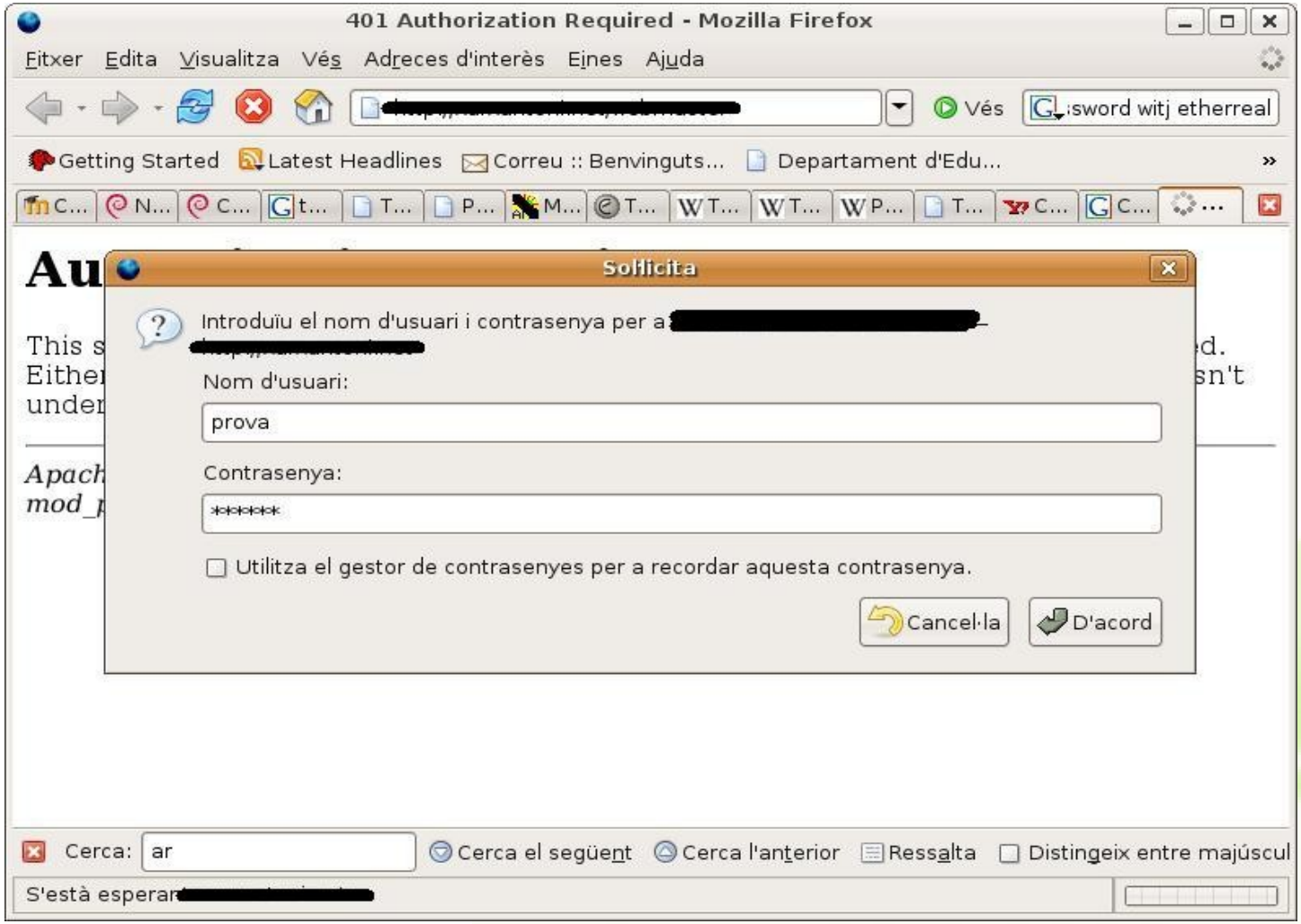
Ethereal

- **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

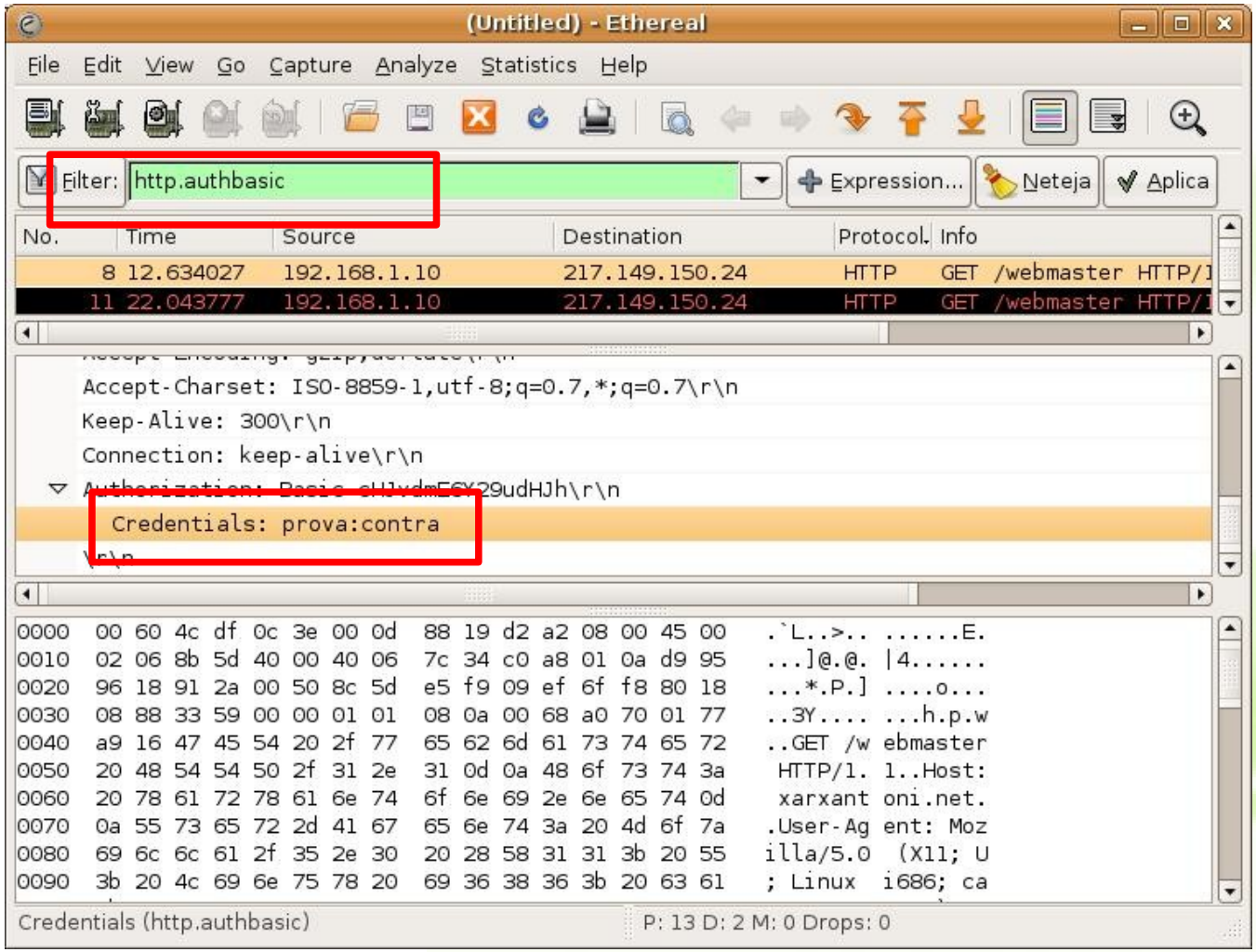
- **Exemple. Captura paraula de pas web.**



Autor: Sergi Tur Badenas

Ethereal

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



Autor: Sergi Tur Badenas

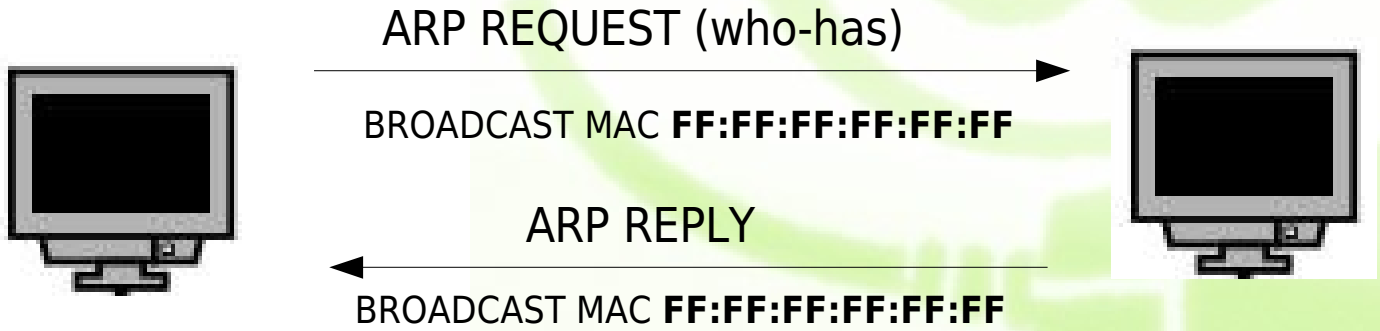
Ethereal

- **Paquets necessaris**
  - ethereal
- **Referències**
  - man tcpdump
  - **Article de la wikipedia**
  - **Pàgina oficial de tcpdump**
- **Altres enllaços**
  - **WinDump**
  - **Article de la wikipedia sobre Paquet Sniffers**

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 IPs de tots els PCs de la xarxa

Autor: Sergi Tur Badenas

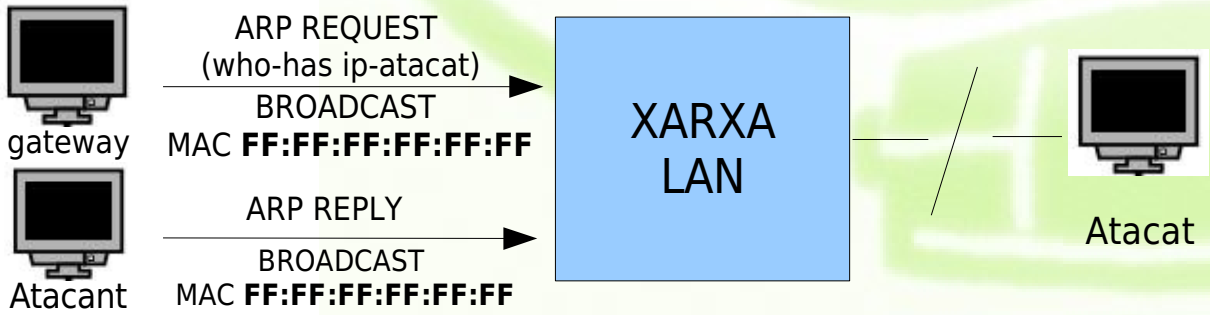
ARP Spoofing (Enverinament ARP)

- **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

- **Es poden “sniffar” switched LANS?**
  - Sí. Ettercap és un packet sniffer per a switched LANs
  - Utilitza dos modes de treball:
    - **Unified sniff** (per defecte): Captura tots els paquets que passen per una targeta de xarxa. Reenvia els paquets a l'atacat amb ip_forwarding de nivell 3 (router)
    - **Bridged sniff**: Dues targetes de xarxa. Converteix la màquina en un bridge (nivell 1). Més difícil de detectar
  - Atacs Man In The Middle
  - Un cop actiu ens mostra una llista de màquines i connexions establertes i el seu estat
  - Té plugins que faciliten la tasca de “recol·lectar” contrasenyes

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 (inclòs 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 tràfic

- **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 correcta

```
$ 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
```

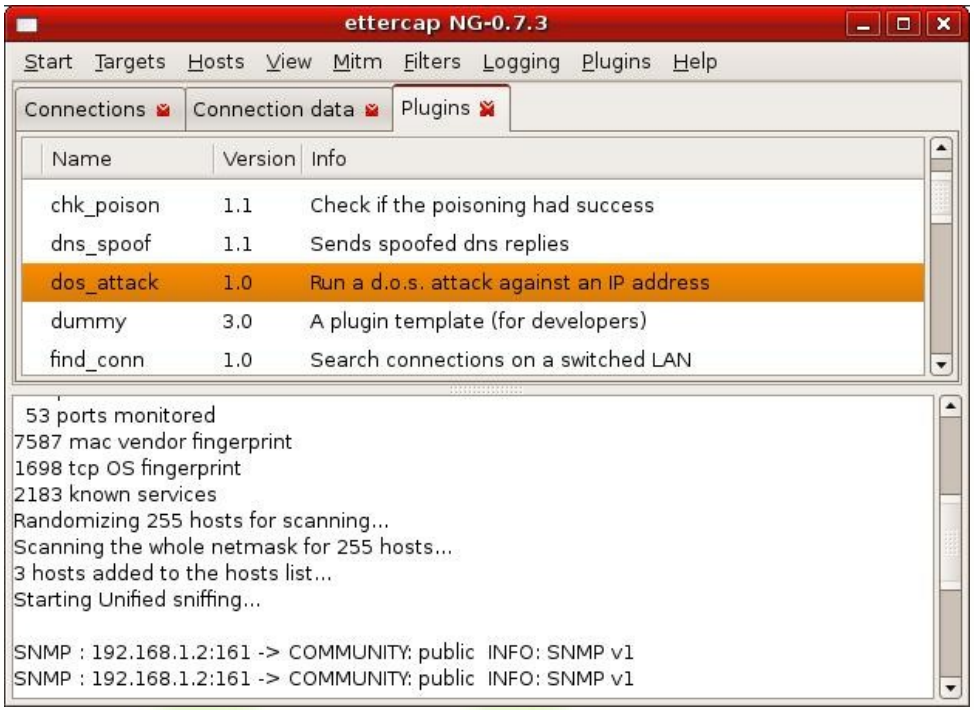
- Tothom utilitza la MAC de l'atacant!

- **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
.........................
```

- DOS ettercap a la wiki del curs

Autor: Sergi Tur Badenas

ARP SPOOFING

- **Defenses**
  - 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 MC 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

Man in the middle attacks (Mitm)

És un atac que permet a un atacant llegir, modificar o inserir missatges a la comunicació entre dues entitats sense que aquestes en siguin conscients.

- **Hi ha múltiples formes d'aconseguir un Mitm**
  - L'atacant pot observar i/o modificar les dades de la comunicació.
    - **eavesdropping**: observar el tràfic (captura de contrasenyes)
    - **substitution attack**:l'atacant pot sostreure la identitat
    - **denial-of-service (DOS) attack**:impedir les comunicacions
    - **phishing attacks:** obligar a l'atacant a aportar dades personals (comptes bancaris, números secrets)
  - Especialment útil en sistemes de clau pública.
- **Man In The Middle Atacks a la wiki del curs**

Autor: Sergi Tur Badenas

SSH i Man in The Middle

Primera connexió a un servidor

```
$ ssh sergi.tur@10.0.2.2
The authenticity of host 'tjener (10.0.2.2)' can't be established.
RSA key fingerprint is ab:37:e2:3f:6f:16:27:5e:9a:02:a1:e1:9a:34:7f:69.
Are you sure you want to continue connecting (yes/no)?yes
password:
```

Man-in-the-middle warning

```
$ ssh sergi.tur@10.0.2.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
f2:92:1d:da:81:2a:d7:16:0a:48:f0:43:20:1c:f4:b5.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending key in ~/.ssh/known_hosts:5
Password authentication is disabled to avoid man-in-the-middle attacks.
X11 forwarding is disabled to avoid man-in-the-middle attacks.
Permission denied (publickey,password,keyboard-interactive).
```

Solució:

```
sed -i '5d' ~/.ssh/known_hosts
```


Autor: Sergi Tur Badenas

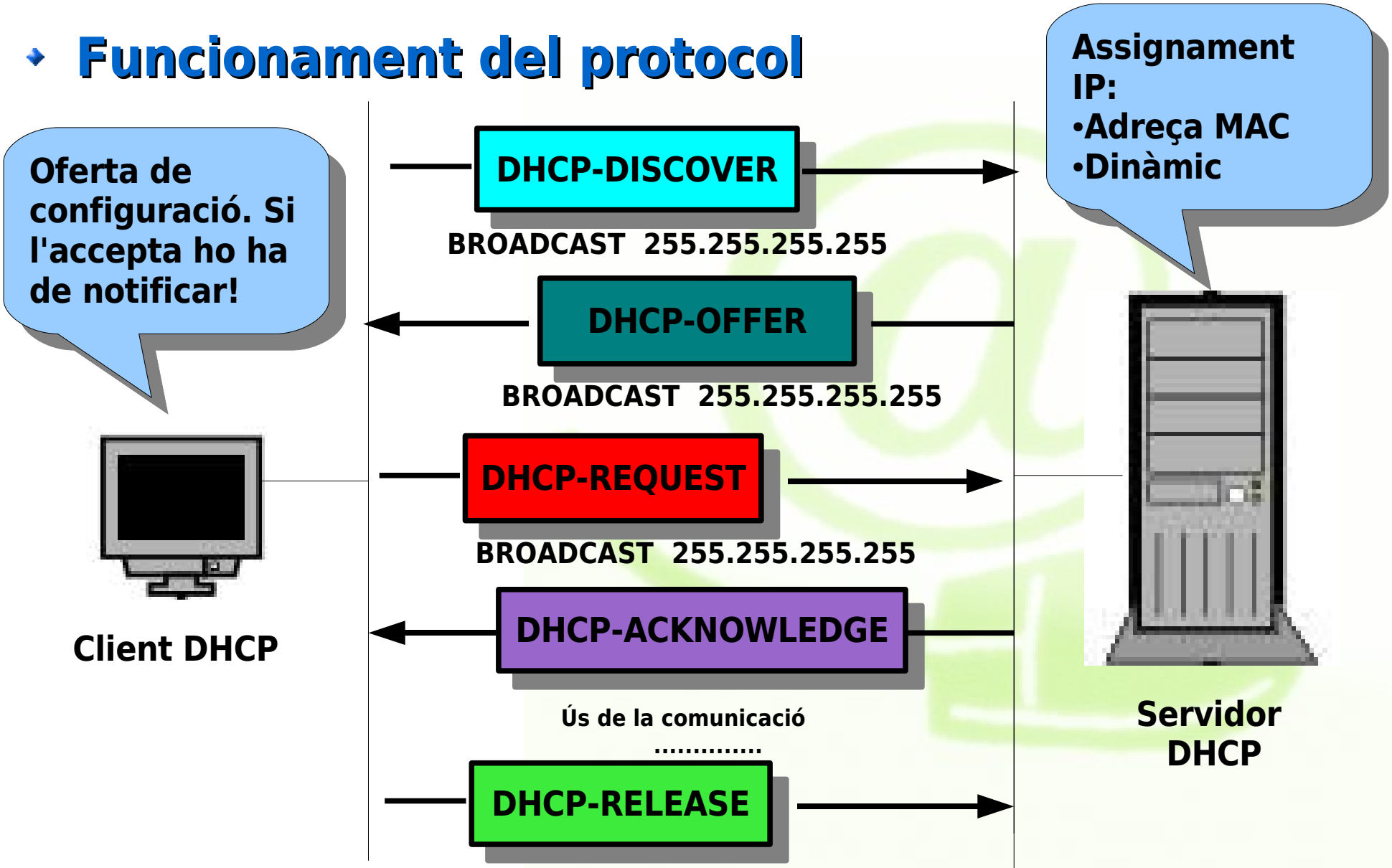
Port Stealing (robo de puerto)

- **Es basa en enviar molts frames (unitats de dades del nivell 2 d'enllaç) amb l'adreça MAC de la víctima.**
  - El resultat és que el commutador (switch) creu que la víctima està connectada al port de l'atacant.
  - Quan l'atacant rep un paquet, la destinació del qual era la víctima, l'atacant genera un AR-request preguntant per la IP de la víctima. Quan la víctima respon el commutador torna a conèixer la MAC de la víctima i aleshores reenviar el paquet capturat a la víctima (modificat o sense modificar).
  - El procés es repeteix periòdicament. La connexió de la víctima es degrada notablement i és un atac fàcil de detectar per un IDS.
  - L'ús de taules estàtiques en els clients no resol el problema. El mapeig estàtic s'ha de fer al commutador (port security, 802.1x, Nap o NAC).
  - Ettercap suporta Port Stealing.

Autor: Sergi Tur Badenas

DHCP

- **Funcionament del protocol**



Autor: Sergi Tur Badenas

DHCP Spoofing

- **Els paquets DHCP-REQUEST són enviats a tota la xarxa en mode broadcast i per tant poden ser escoltats per tots els dispositius de la xarxa.**
  - Un atacant pot aprofitar per respondre abans que el servidor de DHCP vàlid.
  - L'atacant pot aprofitar per enviar informació incorrecta al client. Per exemple pot indicar-li a la màquina que el gateway és ell i capturar tot el tràfic cap a Internet de la màquina.
  - És fàcil respondre abans que els servidors de DHCP, ja que aquests fan algunes verificacions abans de respondre al client.
  - Aquests atacs són fàcils de detectar per un IDS quan es troben múltiples respostes DHCP en una mateixa xarxa.
  - Ettercap permet fer atacs DHCP.

Autor: Sergi Tur Badenas

DNS spoofing

- **L'atac consisteix en llançar respostes falses de resolució de DNS a les peticions de resolució DNS de les víctimes.**
  - Dos mètodes:
    - DNS "ID Spoofing": es basa en obtenir els identificadors de petició de resolució de DNS a través d'algun atac d'sniffing. Si l'atacant pot escoltar les peticions de DNS pot intentar contestar abans que el servidor real, enganyar a la víctima i enviar la seva petició on l'atacant desitgi.
    - **"Cache poisoning" (envenenamiento de la cache)**: similar a l'anterior però dirigit als servidors de cache de DNS.
  - Per aquesta raó els servidors de cache de DNS utilitzen identificadors aleatoris.
  - Els IDS són capaços de detectar aquests atacs . DNSSec també és una solució.

Autor: Sergi Tur Badenas

ICMP Redirect

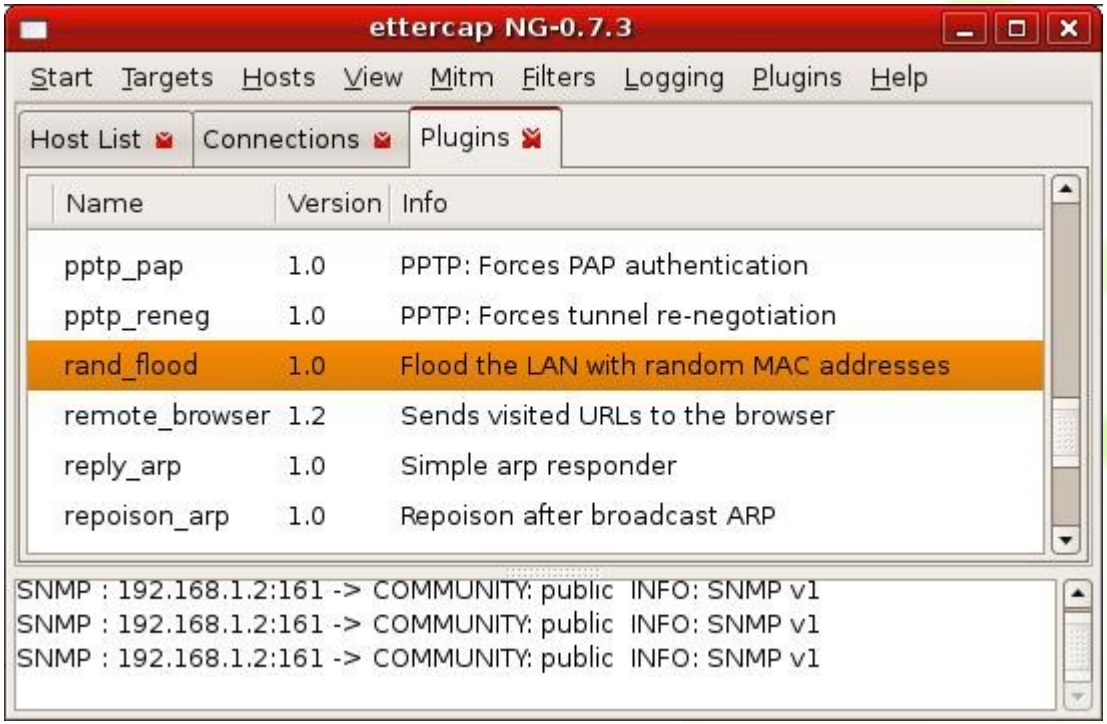
- **Utilitza el paquet ICMP Redirect per fer-nos passar pel gateway de la xarxa LAN**


```
$ sudo tcpdump icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
11:18:27.316196 IP 192.168.1.1 > 192.168.1.2: ICMP redirect 217.149.150.24 to host 192.168.1.2, length 36
11:18:27.316250 IP 192.168.1.1 > 192.168.1.2: ICMP redirect 63.245.213.21 to host 192.168.1.2, length 36
11:18:27.388111 IP 192.168.1.1 > 192.168.1.2: ICMP redirect 63.245.213.21 to host 192.168.1.2, length 36
```


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

Altres atacs Mitm

- **Existeixen múltiples atacs Mitm**
  - STP Mangling
  - ICMP redirection
  - IRDP spoofing
  - Route mangling

Autor: Sergi Tur Badenas

Autenticació Linux. Contrasenyes

- **Usuari i contrasenya emmagatzemats en fitxers locals:**
  - **/etc/passwd**: Conté la informació de les comptes d'usuari (llegible per tots els usuaris).
  - **/etc/shadow**: Conté les contrasenyes. Només llegible per root i el grup shadow.
  - **/etc/group**: Conté els grups i els usuaris que hi pertanyen.

```
pete:x:1000:1000:Peter Hernberg,,,1-800-FOOBAR:/home/pete:/bin/bash
```

```
pete:/3GJllg1o4152:11009:0:99999:7:::
```

```
pasta:x:103:spagetti,fettucini,linguine,vermicelli
```

- **Autenticació Linux a la wiki**

Autor: Sergi Tur Badenas

Contrasenyes

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!"

- **Generador de contrasenyes**

```
$ sudo apt-get install makepasswd
$ makepasswd
DnqTBW96
```

- **Contrasenyes fluixes**
  - Número de pin, dates (naixement, celebracions o altres), només dígits, no combinar números amb dígits o caràcters estranys i contrasenyes curtes, etc.
- **Actualment es parla de passphrase com a sistema més segur**
  - Contrasenyes a la wiki del curs

Autor: Sergi Tur Badenas

Contrasenyes

- **Recomanacions**
  - Mínim 7 caràcters de longitud
  - No utilitzeu paraules de diccionari o seqüències lògiques (aaa555ccc, 1234567890 etc.)
  - Evitar utilitzar la mateixa contrasenya a tot arreu (evitar el PIN del mòbil)
- **Idees**
  - Escull una paraula coneguda i introdueix canvis (ordena-la al revés, reemplaça algun caràcter per dígits, treu vocals i afegeix algun caràcter estrany, usa majúscules, etc...)
  - Considera almenys utilitzar un caràcter estrany
  - Aplica tot l'anterior a frases fàcils de recordar (llc1hlqnsdcuM)

Autor: Sergi Tur Badenas

Força Bruta

- **Límits teòrics**
  - Creixement exponencial amb la longitud de la clau.
  - Límit de temps: edat de l'univers $1.3x10^{10.}$
  - Llei de Moore: la potència de processament de les màquines és doble, aproximadament cada dos anys.
  - Una clau de 128 bits amb un sistema capaç de provar 10^{18} contrasenyes per segon requereix d'uns 10^{13} anys.
  - Una clau de 256 bits amb un sistema capaç de provar 1018 contrasenyes per segon requereix requereix de 3x1051 anys

Mida de la contrasenya	Combinacions (36 caràcters)	Temps
1	36	0.0004s
2	1296	0,01s
3	46656	0.5s
4	1679616	17s
5	60466176	10 minuts
6	2176782336	7 hores
7	78364164096	9 dies
8	$2.8211099x10^{12}$	10 mesos
9	$1.0155995x10^{14}$	32 anys
10	$3.6561584x10^{15}$	1161 anys
11	$.3162170x10^{17}$	41822 anys
12	$4.7383813x10^{18}$	1,505,614 anys

Autor: Sergi Tur Badenas

John the Ripper

- **Como va dir Jack l'esbudellador anem per parts:**

És una aplicació de criptografia que aplica tècniques de **cerca fer força bruta** per desxifrar contrasenyes.

Té capacitat per a trencar diferents algorismes de xifrat com DES, SHA-1 i altres.

Eina de Password Cracking però també eina d'administrador (permet comprovar que les contrasenyes dels usuaris són suficientment bones).

És capaç de detectar automàticament el tipus de xifrat i a més es pot personalitzar.

L'eina està relacionada amb el projecte OpenWall.

John The Ripper a la wiki del curs

Autor: Sergi Tur Badenas

John The Ripper

- Són bones les nostres contrasenyes d'usuari de sistema?
- Instal·lar john the ripper i comprovar...

```
$ sudo apt-get install john
```

- Podem fer proves amb

```
#Afegir usuaris amb contrasenyes fàcils
$ sudo adduser pep
$ mkdir john
$ cd john
$ sudo unshadow /etc/passwd /etc/shadow > contrasenyes
$ john --single contrasenyes
$ john -wordfile:catala-wordlist.txt contrasenyes
```

- Segons la teoria, quines combinacions podríem provar amb el temps que disposem?
- Consulteu la wiki del curs per veure més exemples.
- Hi ha altres crackers com Cain i Abel per a Windows.

Autor: Sergi Tur Badenas

Vulnerabilitats relacionades amb contrasenyes

- **No només hi ha contrasenyes a /etc/shadow**
  - També hi ha contrasenyes d'altres aplicacions (bases de dades, aplicacions web, fitxers de configuració...)
  - Hi ha moltes formes d'explotar aquestes vulnerabilitats
    - Utilitzar Google per detectar màquines

```
"phpMyAdmin" "running on" inurl:"main.php"
```

    - Usuaris de sistema sense permisos de root però amb accés a fitxers.
    - Màquines amb administradors compartits
    - Contrasenyes escrites en fitxers
    - Conèixer les aplicacions a atacar
  - Contrasenyes a la wikipedia

```
$ locate htaccess
$ locate passwd
$ locate htpasswd
$ locate secret
$ locate password
$ locate contrasenya
$ locate contraseña
```


Autor: Sergi Tur Badenas

Rootkit

Un rootkit és una aplicació o conjunt d'aplicacions que tenen com a finalitat obtenir el control d'un sistema remot de forma secreta.

- L'origen del nom està en un conjunt d'eines de Unix precompilades (ps, netstat, passwd, cd...) que fan les mateixes tasques que les comandes originals però que a més permeten a un intrús mantenir un accés de root sense que l'administrador real del sistema sàpiga de la seva existència.
- Actualment hi ha rootkits per a tots els sistemes operatius.
- Els rootkits són considerats troians.
  - **Rootkits de kernel:** s'integren al kernel modificant el kernel amb un driver o mòdul fals. La seva detecció és més complexa.
  - **Rootkits a nivell d'aplicació:** reemplacen aplicacions executables originals per versions modificades.

Autor: Sergi Tur Badenas

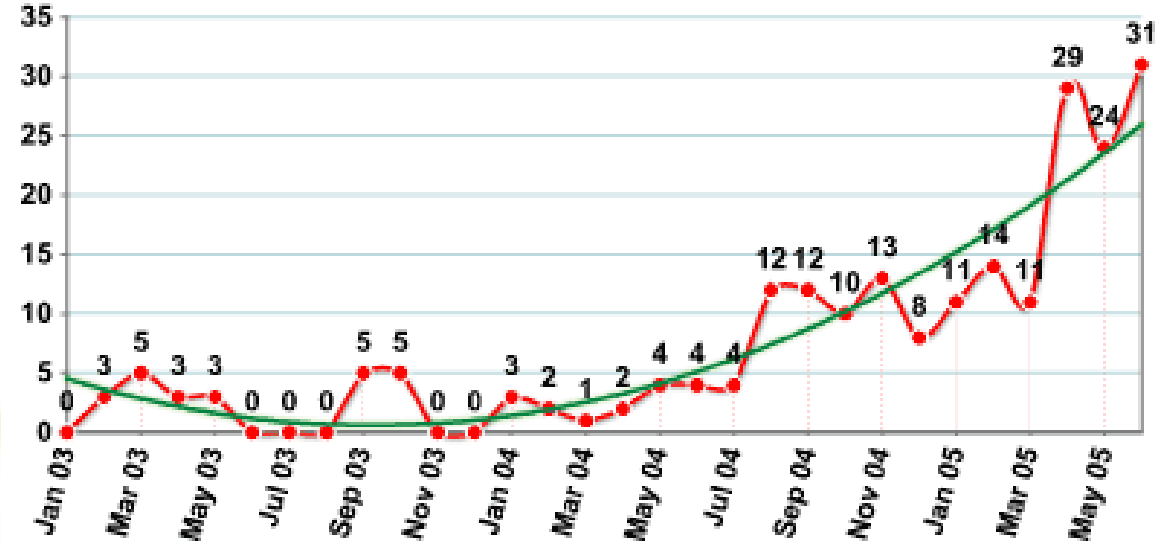
Rootkit

- Els rootkits eviten deixar cap rastre esborrant inicis de sessió (logins), processos, arxius i/o registres (logs).
- Alguns inclouen eines per interceptar dades de terminals, connexions de xarxa (sniffers) o fins i tot interceptar el teclat (keylogger).
- Solen incloure una porta del darrera (backdoor) que ajuden als intrusos a accedir al sistema.
- Sovint els rootkits s'utilitzen per utilitzar la màquina víctima com a base d'operacions per llançar atacs (com DoS o SPAM) a altres màquines.
- Rootkits a la wiki del curs

Autor: Sergi Tur Badenas

Rootkit

- **Rootkits coneguts**
  - FU Rootkit
  - SuckIT
  - Adore
  - T0rn
  - Hacker Defender
  - Ambient's Rootkit (ARK)
  - First 4 Internet XCP (Extended Copy Protection) DRM



Autor: Sergi Tur Badenas

Detecció de rootkits

- Són complicats de detectar. Executar un detector des del sistema infectat no és una tasca fiable.
- Sovint l'únic sistema fiable és accedir al sistema operatiu infectat des d'un LIVE-CD. Un rootkit inactiu no pot ocultar la seva presència.
- La detecció i eliminació de rootkits és una batalla permanent entre els creadors de rootkits i els programes de seguretat.
- **Detectors de rootkits**
  - **chkrootkit** (UNIX/Linux) i **rkhunter** (UNIX/Linux)
  - Windows Blacklight (gratuito para uso personal)
  - www.antirootkit.com (Windows/UNIX/Linux)
  - RootkitRevealer (Windows)
  - Altres aplicacions shareware...

Autor: Sergi Tur Badenas

Chkrootkit i Rkhunter

- **Instal·lació:**

```
$ sudo apt-get install rkhunter
$ sudo apt-get install chkrootkik
```

- **Execució:**

```
$ sudo rkhunter -c
```

```
$ sudo chkrootkit
```

  - El fet de passar un detector amb èxit no implica que no tinguem cap rootkit.
  - La forma ideal de passar el rootkit és sobre un sistema no actiu (P. ex. accedint des d'un live CD).

Autor: Sergi Tur Badenas

Sony CD Rootkits

- **Només ens ataquen els hackers?**
- **Sony CDs rootkit?**
  - Durant el 2005 Sony BMG va vendre un sèrie de Cds amb un “rootkit” incorporat.
  - Els CDs instal·laven automàticament un sistema anticòpia en les màquines Windows.
  - Van ser obligats a retirar-ho i a publicar un pegat a la seva pàgina web.
  - Llista de CDs amb el rootkid cd Sony
  - Més informació

Autor: Sergi Tur Badenas

IDS

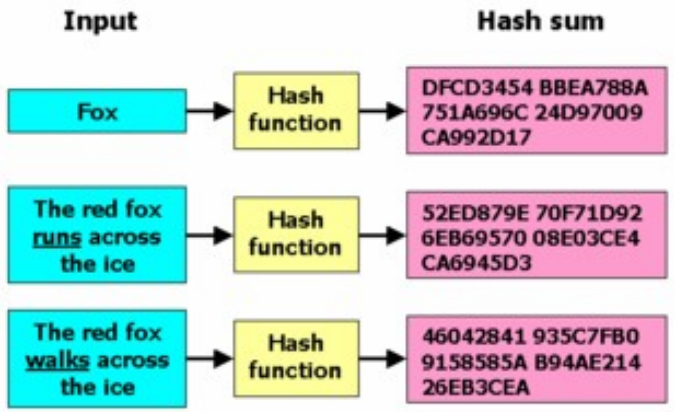
- **Intrusion Detection Systems**
  - La idea general de tots els IDS és la mateixa:
    - Crear una base de dades de tots els fitxers del sistema, guardar-la en un lloc segur i periòdicament comprovar que no s'ha canviat cap fitxer sense el nostre coneixement.
  - El problema és mantenir aquests sistemes (quina fitxer controlar i quins no, actualitzacions, etc.)
  - Hi ha altres sistemes basats en l'anàlisi del tràfic de xarxa (SNORT)
  - Utilitzen les funcions criptogràfiques de HASH
    - Funció criptogràfica de HASH

Autor: Sergi Tur Badenas

Funció criptogràfica HASH

A criptografia, una funció de hash és una transformació que converteix una entrada qualsevol en un conjunt de caràcters (String) de longitud fixa anomenat valor de hash.

- **Propietats**
  - El valor de hash és un representació única de l'entrada original. Petjada Digital (Digital Fingerprint)
  - També anomenades funcions **digest**
  - Les més conegudes són MD5 i SHA-1 (al 2005 es van identificar debilitats a totes dues)
- **Utilitats**
  - Comprovació de la integritat
  - Identificació digital



Autor: Sergi Tur Badenas

Funció criptogràfica HASH

- **md5sum**
  - Permet calcular el hash d'un fitxer

```
$ dpkg -S md5sum | grep bin
....
coreutils: /usr/bin/md5sum
$ sudo apt-get install coreutils
$ touch prova.iso
$ md5sum prova.iso
d41d8cd98f00b204e9800998ecf8427e  prova.iso
```

- **Utilitzat per comprovar la integritat i la validesa d'un fitxer descarregat d'Internet.**

Autor: Sergi Tur Badenas

debsums

- **Permet comprovar quins paquets debian han sofert canvis des de la seva instal·lació**
  - Instal·lació:

```
$ sudo apt-get install debsums
```

  - Comprovació:

```
$ sudo debsums -ce bind9
/etc/bind/named.conf.options
/etc/bind/named.conf.local
```

  - Podem saber quins paquets no tenen debsums amb:

```
$ sudo debsums -l

$ sudo -i
# cd /var/cache/apt/archives
# apt-get --download-only --reinstall install `debsums -l`
# debsums --generate=keep,nocheck *.deb
```

  - Altres utilitats (saber quins fitxers de configuració hem modificat, recuperació d'un sistema de dades corrupte, etc...)

Autor: Sergi Tur Badenas

Tripwire

- **Intrusion Detection System**
  - Crea una base de dades dels fitxers del nostre sistema
  - Crear la base de dades:

```
$ sudo tripwire -m i
```

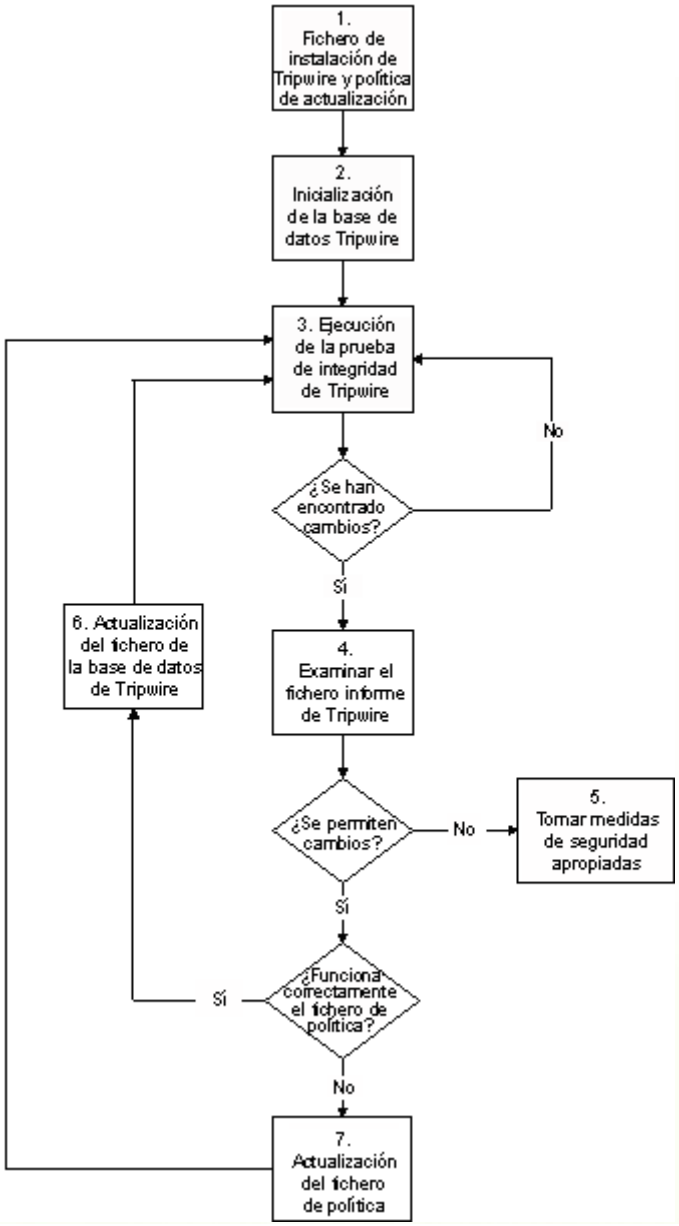
  - Comprovar sistema

```
$ sudo tripwire -m c
```

  - Fitxer de configuració

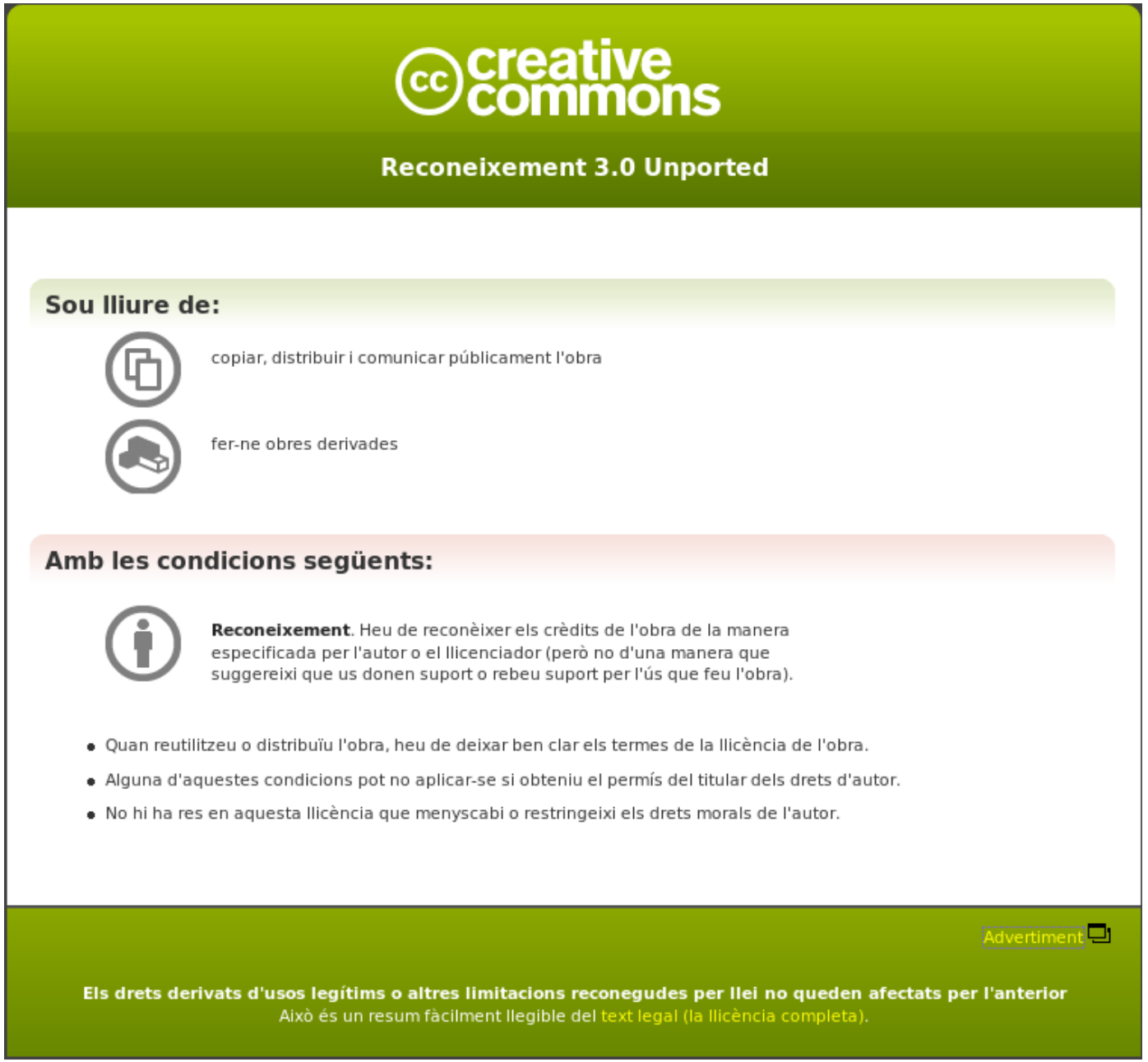
```
/etc/tripwire/twpol.txt
```

- **Hi ha altres IDS com AIDE o Integrit o samhain**



Autor: Sergi Tur Badenas

Llicència Creative Commons



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

Autor: Sergi Tur Badenas