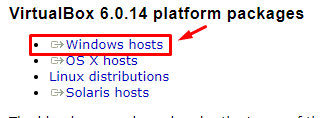
**1) Instal·la *VirtualBox* al teu equip.**

Per poder duu a terme la instal·lació del programa VirtualBox, hem de seguir els següents passos:

- Anar a la pàgina [*www.virtualbox.org*](http://www.virtualbox.org), i fer clic sobre la secció *Downloads*.



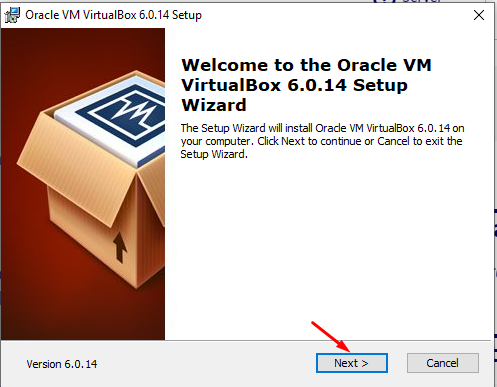
- A continuació, fem clic sobre l’opció del sistema operatiu que tinguem instal·lat en el nostre ordinador, que en el meu cas es *Windows 10*, llavors escullo l’opció *Windows hosts*.

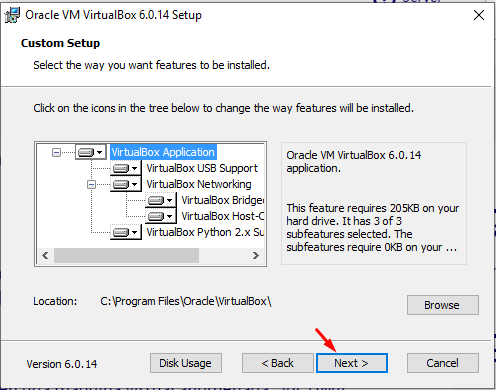


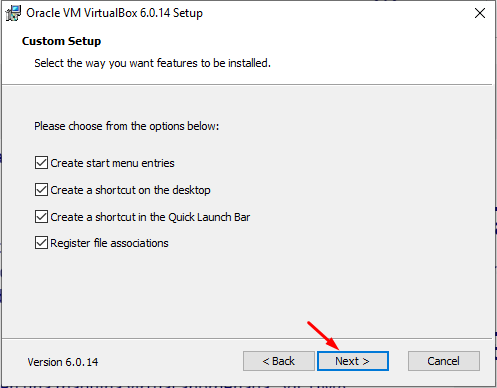
- Una vegada fet el pas anterior, comença la descàrrega.

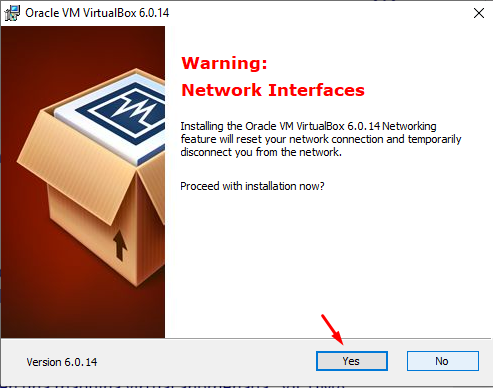
C:\Users\marcv\OneDrive\Escritorio\Screenshot_3.png

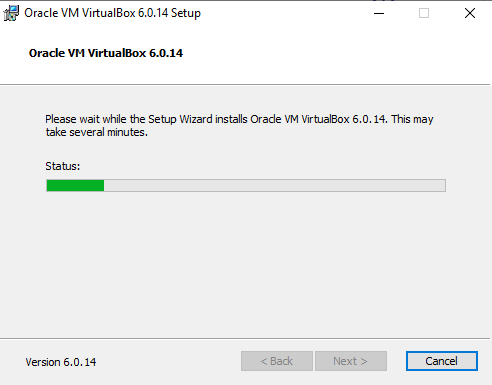
- Una vegada ha acabat la descàrrega, procedirem a la instal·lació escollint les opcions marcades amb les fletxes vermelles.

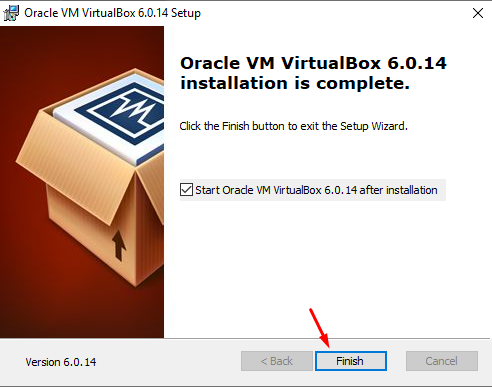




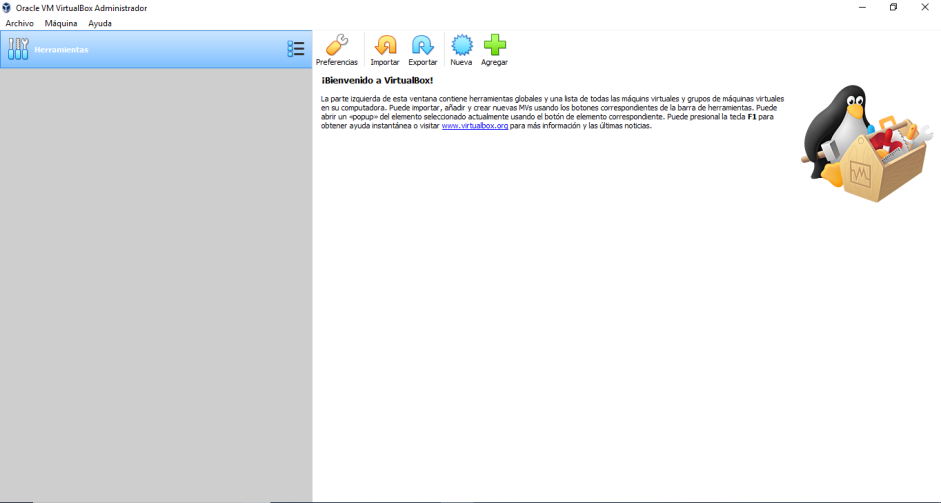






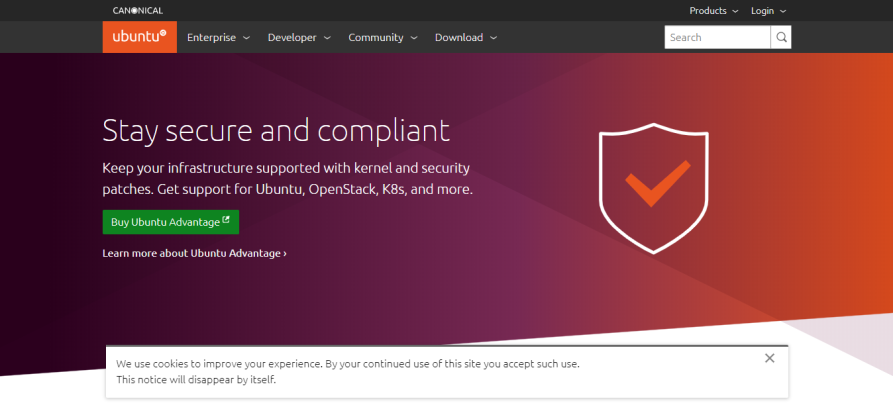


- Una vegada acabada la instal·lació, ja podem obrir el programa, sense cap error.

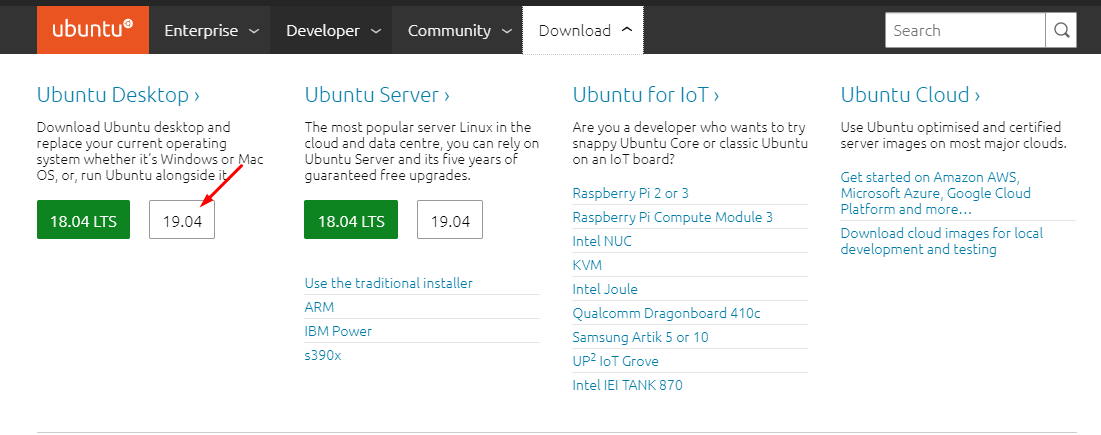


**2) Descarrega't una imatge *Ubuntu* i instal·la-la en una màquina virtual anomenada "VICTIMA". Configura la xarxa en mode "pont".**

Primer de tot, per poder descarregar-nos una imatge *Ubuntu*, el que tenim que fer és anar a la pàgina <https://ubuntu.com/>.



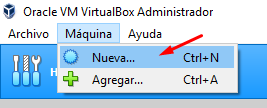
- A continuació, hem d’anar a l’apartat *Download,* i seleccionar la següent opció.



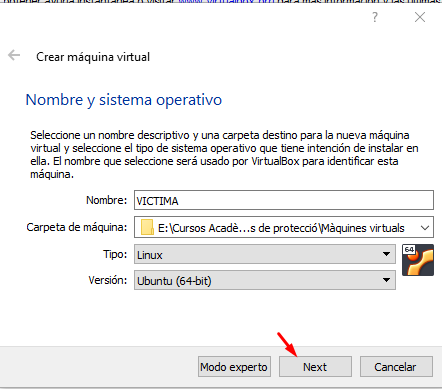
- Una vegada fet el pas anterior, comença la descàrrega de la nostra *ISO*.

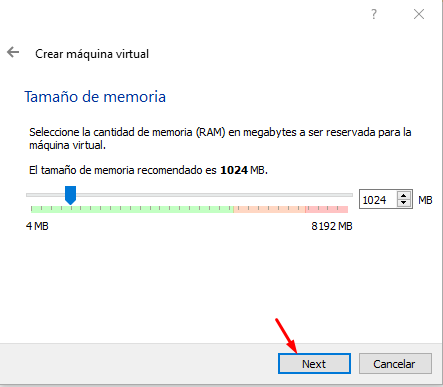
E:\Cursos Acadèmics\UOC-Ciberseguridad\Pràctiques\Tallers\Taller 3. Sistemes de protecció\Captures\Apartat 2\Screenshot_3.png

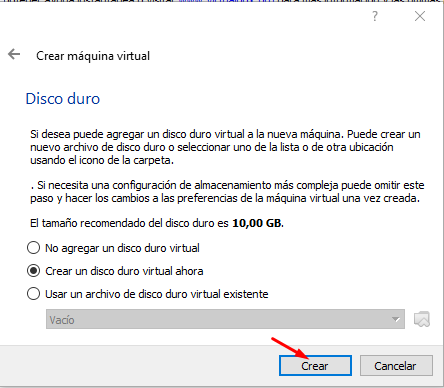
- A continuació, una vegada acabada la descàrrega, procedirem a la creació i/o instal·lació de la màquina virtual.

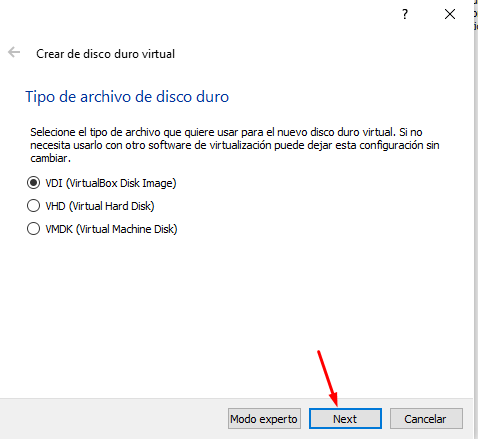


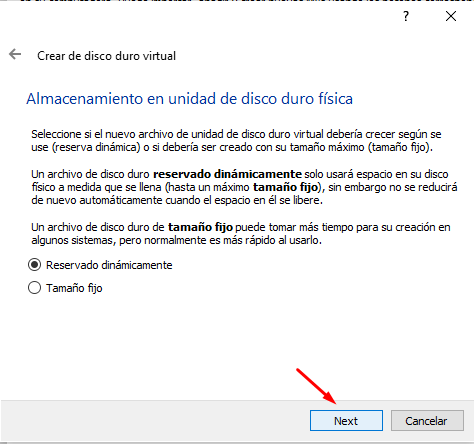
- Determinem les característiques de la màquina virtual.

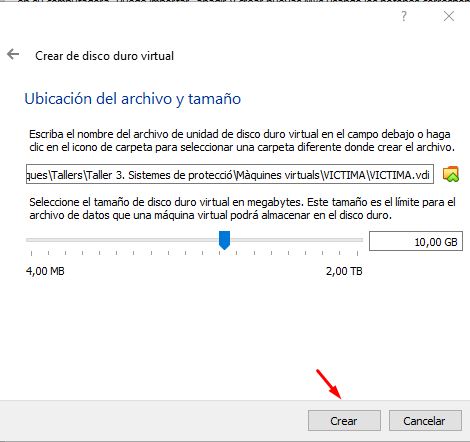




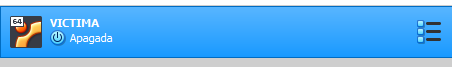








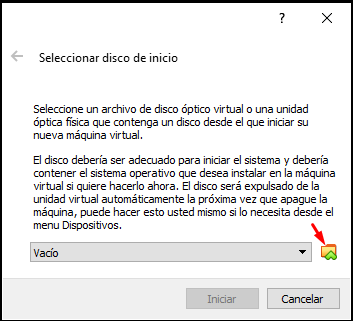
- Una vegada fets els passos anteriors, ja tenim la màquina virtual amb *Ubuntu* creada.

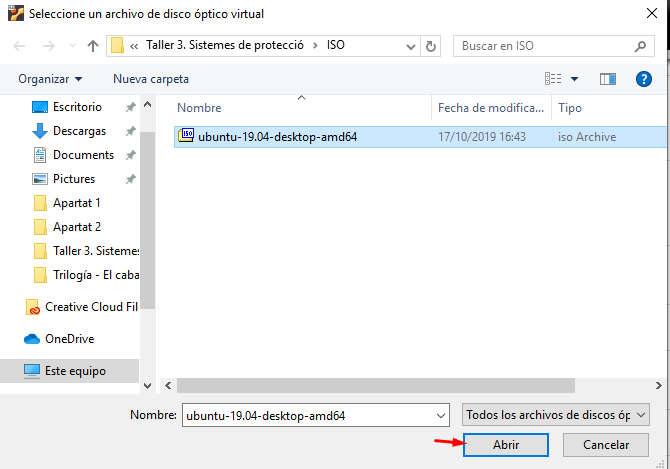


- Tot seguit, procedirem a iniciar la màquina virtual.

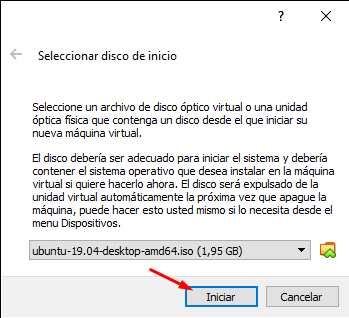


- Seleccionem la *ISO*.





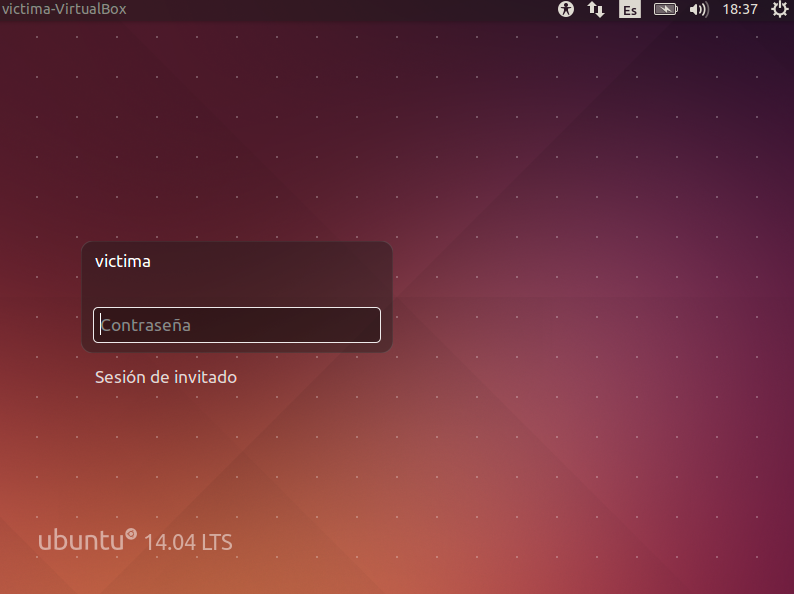
- Una vegada seleccionada, l’iniciem.



- Un vegada iniciada, comença el procés d’instal·lació.



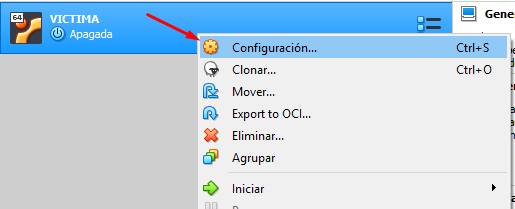
- Una vegada s’ha acabat d’instal·lar, reiniciem la màquina, i tenim el següent:

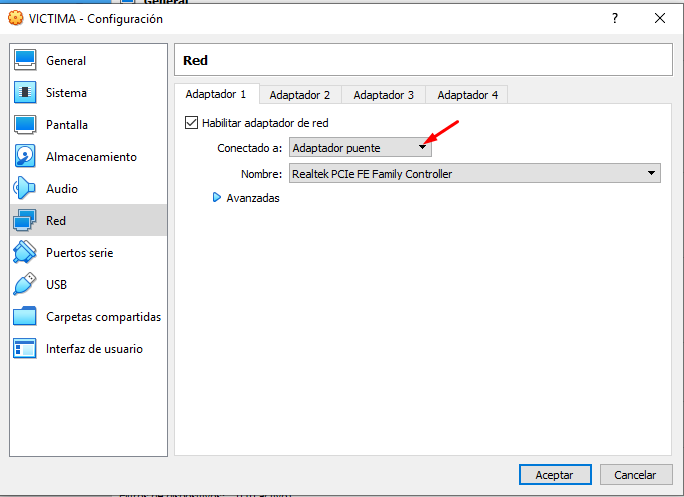


- Iniciem sessió.



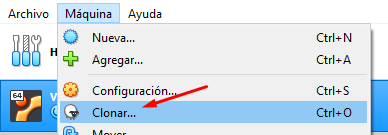
- Per últim, canviem la targeta de xarxa en mode pont.



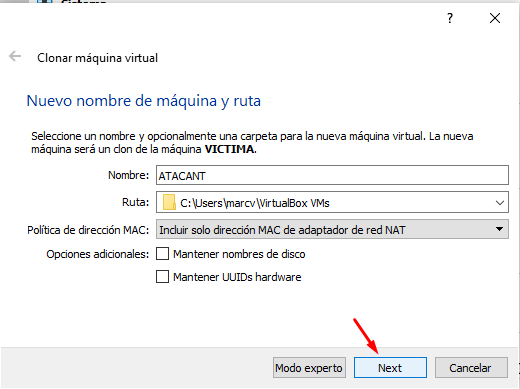


**3) Fes un clon de la imatge, anomena-la "El teu nom ATACANT".**

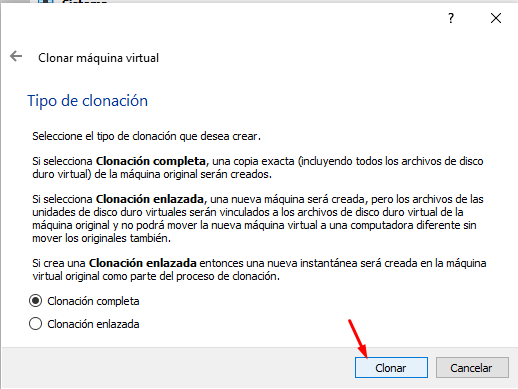
Per poder crear un clon de la màquina creada anteriorment, hem d’anar a l’apartat *Máquina 🡪 Clonar*.



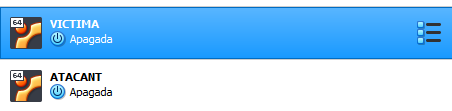
Posem el nom de la nova màquina clonada.



Procedim a la clonació.



Una vegada fets els passos anterior, ja tenim les dues màquines virtuals, amb les que treballarem, creades.



**4) En la màquina "VICTIMA" instal·la *Apache2* (*sudo apt-get update, sudo apt-get install apache2*) i *iptables* (*sudo apt-get install iptables*).**

Primer de tot, actualitzem el sistema operatiu.

E:\Cursos Acadèmics\UOC-Ciberseguridad\Pràctiques\Tallers\Taller 3. Sistemes de protecció\Captures\Apartat 2\Screenshot_33.png

E:\Cursos Acadèmics\UOC-Ciberseguridad\Pràctiques\Tallers\Taller 3. Sistemes de protecció\Captures\Apartat 2\Screenshot_34.png

Tot seguit, executem la instal·lació del servidor web *Apache2*.

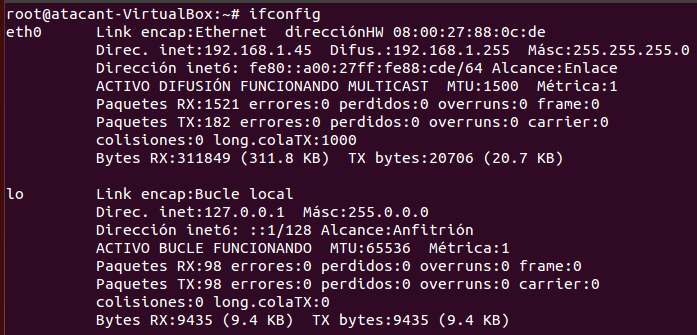
E:\Cursos Acadèmics\UOC-Ciberseguridad\Pràctiques\Tallers\Taller 3. Sistemes de protecció\Captures\Apartat 2\Screenshot_36.png

Per acabar, instal·lem el servei de les *iptables*.

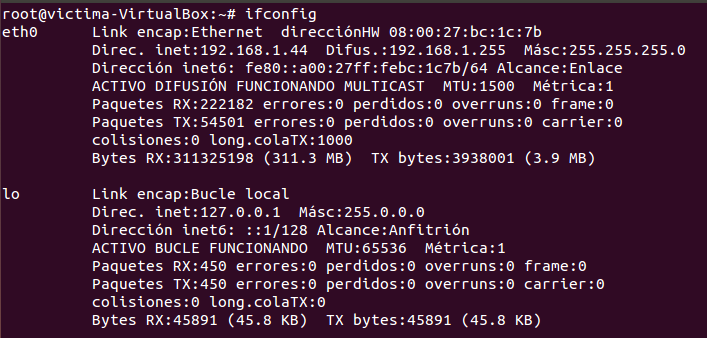
E:\Cursos Acadèmics\UOC-Ciberseguridad\Pràctiques\Tallers\Taller 3. Sistemes de protecció\Captures\Apartat 2\Screenshot_37.png

**5) Mostra que pots fer un *ping* de la màquina "El teu nom ATACANT" cap a "VICTIMA".**

Ens ubiquem a la màquina *ATACANT*, i fem un *ifconfig*, per poder saber quina és la seva adreça *IP*.

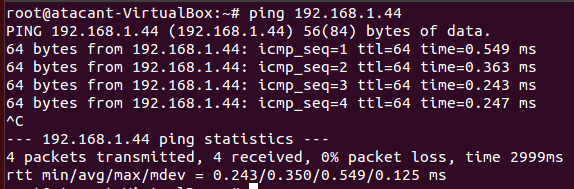


Ens ubiquem a la màquina *VICTIMA*, i fem un *ifconfig*, per poder saber quina és la seva adreça *IP*.

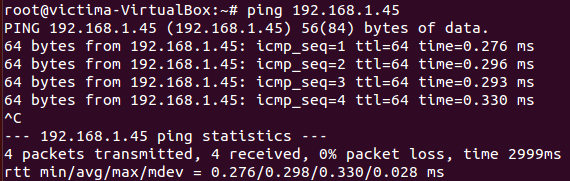


Llavors una vegada sabem les dues adreces *IP*, procedim a fer *ping* entre elles:

- Fem *ping* de la màquina *ATACANT* a la màquina *VICTIMA*.

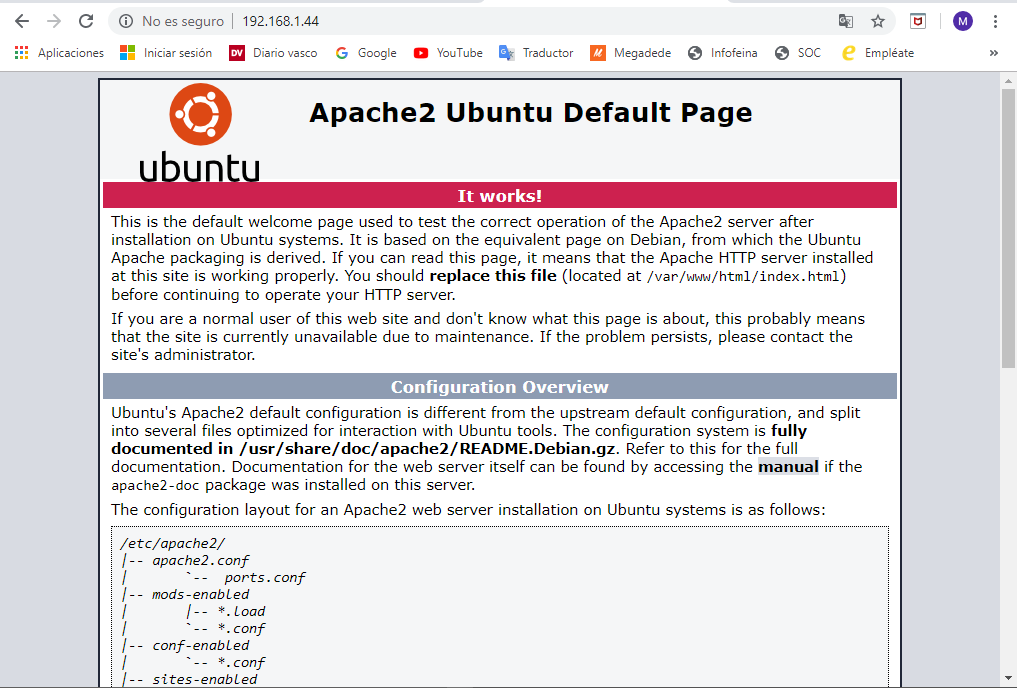


- Fem *ping* de la màquina *VICTIMA* a la màquina *ATACANT*.



**6) Mostra, també, que des de la màquina *hoste* i des de la màquina "El teu nom ATACANT" pots accedir, amb un navegador, al web de la màquina "VICTIMA", ja que s'hi està executant *Apache*.**

Accedim, a través de la nostra màquina hoste, a la web de l’*Apache* de la màquina *VICTIMA*.

****

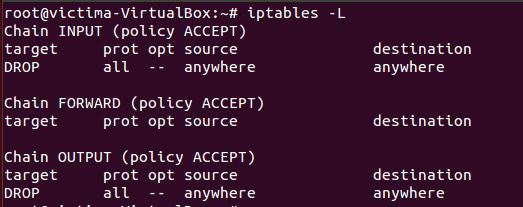
Accedim, a través de la màquina *ATACANT*, a la web de l’*Apache* de la màquina *VICTIMA*.

****

**7) Amb *iptables*, estableix una política per defecte de DROP a la màquina "VICTIMA".**

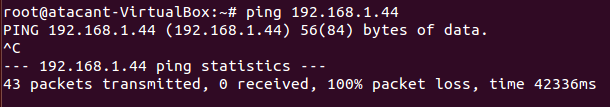
Ens situem en la màquina virtual *VICTIMA*, i executem les següents comandes de les *iptables*.

**E:\Cursos Acadèmics\UOC-Ciberseguridad\Pràctiques\Tallers\Taller 3. Sistemes de protecció\Captures\Apartat 2\Screenshot_47.png**

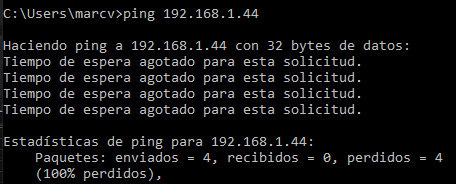
****

**8) Demostra que ara no hi pots fer *ping*.**

Des de la màquina *ATACANT*, intentem fer *ping* a l’adreça *IP* de la màquina víctima, i es perden tots els paquets, per tant, no ho permet fer.

****

També, des de la màquina *hoste*, intentem fer *ping* a l’adreça *IP* de la màquina víctima, i es perden tots els paquets, per tant, no ho permet fer.

****

**9) Afegeix regles per tal que es pugui accedir al servidor *Apache* i perquè es pugui fer *ping* només des de la màquina "El teu nom ATACANT". Demostra que funciona.**