



JESUÏTES El Clot  
Escola del Clot

# **M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT**

***UF3- Instal·lació i Configuració d'un servidor intermediari***

## **ACTIVITAT 3 : IP tables a Linux, intepretació de scripts**

**Curs:** 2018-19

**CFGs:** ASIX2

**Alumne :** Arnau Subirós Puigarnau

**Data :** 02/03/2019

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## ACTIVITAT 3 : IP tables a Linux, intepretació de scripts

### Introducció i eines útils

L'objectiu d'aquesta activitat és familiaritzar-se amb la sintaxis i l'entorn de la configuració de Iptables en un sistema Linux i conèixer una mica millor quin és el seu funcionament a partir del que s'ha explicat a classe. Una eina útil en molts casos és el man de Linux per examinar en detall que ens ofereix un comandament de Linux i quins paràmetres té. En aquesta línia hi ha un recurs molt interessant per explicar les parts d'un comandament del Shell de Linux. Aquest recurs es tracta d'una pàgina web ( <https://explainshell.com/explain?cmd=iptables>) on desglossa les part d'un comandament Linux, en el nostre cas, les iptables i n'extreu les parts a partir del man de Linux. A continuació en teniu un exemple per averiguar les parts de la creació d'una regla com és el cas del següent comandament:

```
iptables -A INPUT -p tcp -s 192.168.30.0/24 --dport 80 -j ACCEPT
```



A més a més de la teoria de classe, el següent link et pot servir per obtenir més informació  
<https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/>

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

### **Activitat: Anàlisi d'un script de configuració de firewall**

A continuació hi ha un script per a fer una configuració senzilla d'un Firewall a Linux d'una xarxa fictícia (10.0.0.0). Suposa que aquest script s'executa en un Firewall a nivell de xarxa, en una màquina servidora que fa d'intermediari (Proxy) entre la xarxa exterior i els equips de la LAN (10.0.0.0). A partir del que s'ha explicat a classe i l'eina proposada investiga que fa cada una de les regles que s'hi utilitzen. Comenta en negreta que fa cada regla i analitza'n els diferents blocs que componen el script:

```
#!/bin/sh
# Script cortafuegos.sh para la configuración de iptables
#
# BLOC 1 (setup)
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# BLOC 2: (política de seguretat)
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

iptables -A INPUT -i lo -j ACCEPT

# BLOC 3:
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 21 -j ACCEPT

# BLOC 4:
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 443 -j ACCEPT

# BLOC 5:
#iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 53 -j ACCEPT
#iptables -A FORWARD -s 10.0.0.0/8 -p udp --dport 53 -j ACCEPT

# BLOC 6 (final de Firewall):
iptables -A FORWARD -s 10.0.0.7 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -j DROP
iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE

# Activemem enrutament
echo 1 > /proc/sys/net/ipv4/ip_forward

# Comprobamos les regles
iptables -L -n
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

Primer de tot estudiarem bloc , per bloc lo que fa cada comanda del script.

## A.BLOC 1 (SETUP)

### # BLOC 1 (setup)

```
iptables -F  
iptables -X  
iptables -Z  
iptables -t nat -F
```

Primer de tot utilitzaré el comando man iptables per saber el significat . Per utilitzar les regles, utilitzaré l'usuari **"root"** o que tingui el privilegi de **"sudo"**

```
uruloki@kali-anonymous:~$ man iptables | more  
IPTABLES(8)                                iptables 1.6.2  
  
NAME  
    iptables/ip6tables - administration tool for IPv4/IPv6 packet filtering and NAT  
  
SYNOPSIS
```

- ❖ **iptables -F** → Neteja la cadena seleccionada (totes les cadenes de la taula, si no hi ha cap). Això és equivalent a esborrant totes les regles una per una

```
-F, --flush [chain]  
    Flush the selected chain (all the chains in the table if none is given). This is equivalent to deleting all the rules one by one.
```

```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -F  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

- ❖ **iptables -X** → Eliminar la cadena especificada per l'usuari opcional especificada. No ha d'haver-hi referències a la cadena. Si existeixen, ha d'eliminar o reemplaçar les regles de referència abans de poder eliminar la cadena. La cadena ha d'estar buida, és a dir, no contenir cap regla. Si no es dona cap argument, intentarà eliminar totes les cadenes no incorporades en la taula.

```
-X, --delete-chain [chain]
Delete the optional user-defined chain specified. There must be no references to the chain. If there are, you must delete or replace the referring rules before the chain can be deleted. The chain must be empty, i.e. not contain any rules. If no argument is given, it will attempt to delete every non-builtin chain in the table.
```

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$
uruloki@kali-anonymous:~$ sudo iptables -X
[sudo] contrasenya per a uruloki:
uruloki@kali-anonymous:~$
```

- ❖ **iptables -Z** → Posa a zero els comptadors de paquets i bytes en totes les cadenes, o només la cadena donada, o només la regla donada en una cadena. És legal també especificar l'opció -L, --list (llista), per a veure els comptadors (Immediatament abans que s'esborrin)

```
-Z, --zero [chain [rulenum]]
Zero the packet and byte counters in all chains, or only the given chain, or only the given rule in a chain. It is legal to specify the -L, --list (list) option as well, to see the counters immediately before they are cleared. (See above.)
```

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -Z
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## ❖ iptables -t nat -F

1. **-t** → Aquesta opció **especifica la taula de coincidència de paquets en la qual ha d'operar el comando**. Si l'el kernel està configurat amb la càrrega automàtica de mòduls, s'intentarà carregar el Mòdul apropiat per a aquesta taula si no està ja allí.
  - 1.1. **nat** →: Aquesta taula es consulta quan es troba un paquet que crea una nova connexió. Això consta de tres funcions integrades :
    - PREROUTING(per a alterar paquets quan entren)
    - OUTPUT (per a alterar paquets generats localment abans del enrutament)
    - POSTROUTING (per a alterar paquets) ja que estan a punt de sortir).
2. **-F** → Neteja la cadena seleccionada (totes les cadenes de la taula, si no hi ha cap). Això és equivalent a esborrant totes les regles una per una

### TABLES

There are currently five independent tables (which tables are present at any time depends on the kernel configuration options and which modules are present).

#### **-t, --table table**

This option specifies the packet matching table which the command should operate on. If the kernel is configured with automatic module loading, an attempt will be made to load the appropriate module for that table if it is not already there.

#### **nat:**

This table is consulted when a packet that creates a new connection is encountered. It consists of four built-ins: **PREROUTING** (for altering packets as soon as they come in), **INPUT** (for altering packets destined for local sockets), **OUTPUT** (for altering locally-generated packets before routing), and **POSTROUTING** (for altering packets as they are about to go out). IPv6 NAT support is available since kernel 3.7.

Every other iptables command, if applied to the specified table (filter is the default).

#### **-F, --flush [chain]**

Flush the selected chain (all the chains in the table if none is given). This is equivalent to deleting all the rules one by one.

uruloki@kali-anonymous: ~

Fitxer Editar Visualitza Cerca Terminal Ajuda

```
uruloki@kali-anonymous:~$ sudo iptables -t nat -F
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## B.BLOC 2 (polítiques de seguretat)

```
# BLOC 2: (política de seguretat)
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

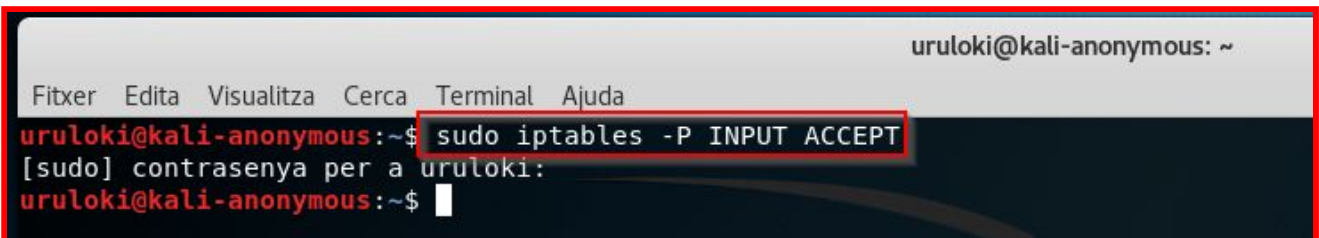
iptables -A INPUT -i lo -j ACCEPT
```

### ❖ iptables -P INPUT ACCEPT

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-P** → Estableix la política de la cadena per a la meta donada. Només les cadenes integrades (no definides per l'usuari) poden tenir polítiques, i no incorporades ni definides per l'usuari. Les cadenes poden ser objectius polítics.
2. **INPUT** → s'aplica als paquets que tenen com a destí(entrada) la nostra màquina
3. **ACCEPT** → (target) es deixa passar el paquet

```
-P, --policy chain target
Set the policy for the built-in (non-user-defined) chain to the given target. The policy target must be either
ACCEPT or DROP.
```



```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -P INPUT ACCEPT
[sudo] contrasenya per a uruloki:
uruloki@kali-anonymous:~$
```



**Nom i Cognoms**

Arnau Subirós Puigarnau

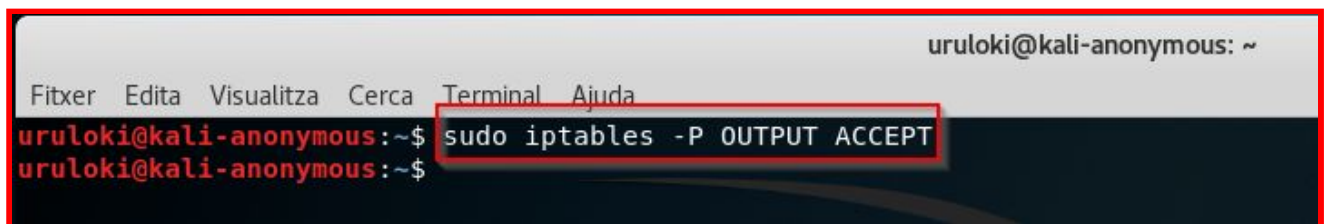
**Data**

02/03/2019

### ❖ iptables -P OUTPUT ACCEPT

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-P** → Estableix la política de la cadena per a la meta donada. Només les cadenes integrades (no definides per l'usuari) poden tenir polítiques, i no incorporades ni definides per l'usuari Les cadenes poden ser objectius polítics.
2. **OUTPUT** → s'aplica als paquets generats en el nostre sistema i són enviats enviats a l'exterior (sortida)
3. **ACCEPT** → (target) es deixa passar el paquet

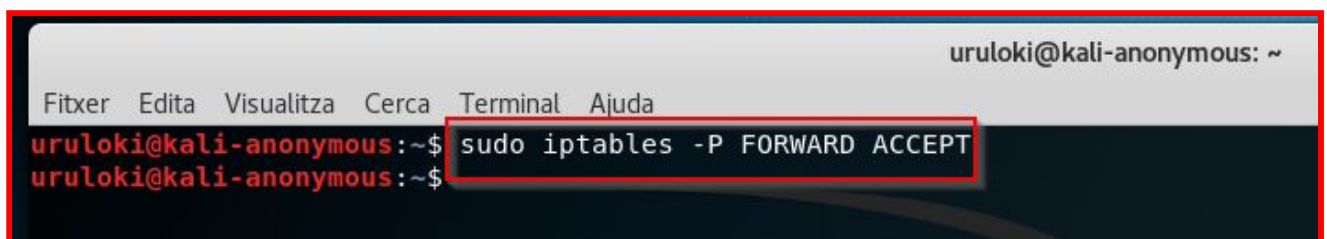


```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -P OUTPUT ACCEPT  
uruloki@kali-anonymous:~$
```

### ❖ iptables -P FORWARD ACCEPT

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-P** → Estableix la política de la cadena per a la meta donada. Només les cadenes integrades (no definides per l'usuari) poden tenir polítiques, i no incorporades ni definides per l'usuari Les cadenes poden ser objectius polítics.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -P FORWARD ACCEPT  
uruloki@kali-anonymous:~$
```



**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## ❖ iptables -t nat -P PREROUTING ACCEPT

1. **-t** → Aquesta opció **especifica la taula de coincidència de paquets en la qual ha d'operar el comando**. Si l'el kernel està configurat amb la càrrega automàtica de mòduls, s'intentarà carregar el Mòdul apropiat per a aquesta taula si no està ja allí.
  - 1.1. **nat** →: Aquesta taula es consulta quan es troba un paquet que crea una nova connexió.
2. **-P** → Estableix la política de la cadena per a la meta donada. Només les cadenes integrades (no definides per l'usuari) poden tenir polítiques, i no incorporades ni definides per l'usuari Les cadenes poden ser objectius polítics.
3. **PREROUTING** → s'aplica als paquets tan punt arriben al tallacos.
4. **ACCEPT** → (target) es deixa passar el paquet

```
uruloki@kali-anonymous: ~  
Fitxer  Editar  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -t nat -P PREROUTING ACCEPT  
uruloki@kali-anonymous:~$
```

## ❖ iptables -t nat -P POSTROUTING ACCEPT

1. **-t** → Aquesta opció **especifica la taula de coincidència de paquets en la qual ha d'operar el comando**. Si l'el kernel està configurat amb la càrrega automàtica de mòduls, s'intentarà carregar el Mòdul apropiat per a aquesta taula si no està ja allí.
  - 1.1. **nat** →: Aquesta taula es consulta quan es troba un paquet que crea una nova connexió.
2. **-P** → Estableix la política de la cadena per a la meta donada. Només les cadenes integrades (no definides per l'usuari) poden tenir polítiques, i no incorporades ni definides per l'usuari Les cadenes poden ser objectius polítics
3. **POSTROUTING** → s'aplica als paquets quan estan a punt de sortir del tallafocs
4. **ACCEPT** → (target) es deixa passar el paquet

```
uruloki@kali-anonymous: ~  
Fitxer  Editar  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -t nat -P POSTROUTING ACCEPT  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## ❖ iptables -A INPUT -i lo -j ACCEPT

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **INPUT** → s'aplica als paquets que tenen como a destí(entrada) la nostra màquina
3. **-i** → Nom d'una interfície mitjançant la qual es va rebre un paquet (només per a paquets d'entrar en l'ENTRADA , FORWARD i PREROUTING cadenes). Quan el "!" argument s'utilitza abans del nom de la interfície, el sentit és invertida Si el nom de la interfície acaba en un "+", llavors qualsevol interfície que comenci amb aquest nom coincidirà. Si s'omet aquesta opció, qualsevol nom d'interfície coincidirà.
4. **lo** → interfície loopback ( on la transmissió de dades es el propi host -->localhost 127.0.0.1)
5. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
6. **ACCEPT** → (target) es deixa passar el paquet

**-A, --append chain rule-specification**  
Append one or more rules to the end of the selected chain. When the source and/or destination names resolve to more than one address, a rule will be added for each possible address combination.

**[!] -i, --in-interface name**  
Name of an interface via which a packet was received (only for packets entering the INPUT, FORWARD and PREROUTING chains). When the "!" argument is used before the interface name, the sense is inverted. If the interface name ends in a "+", then any interface which begins with this name will match. If this option is omitted, any interface name will match.

**-j, --jump target**  
This specifies the target of the rule; i.e., what to do if the packet matches it. The target can be a user-defined chain (other than the one this rule is in), one of the special builtin targets which decide the fate of the packet immediately, or an extension (see EXTENSIONS below). If this option is omitted in a rule (and -g is not used), then matching the rule will have no effect on the packet's fate, but the counters on the rule will be incremented.

```
uruloki@kali-anonymous: ~  
Fitxer  Editar  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ ip a | grep lo  
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  
        inet 192.168.1.130/24 brd 192.168.1.255 scope global noprefixroute eth0  
uruloki@kali-anonymous:~$ ping 127.0.0.1  
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms  
^C  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.020/0.020/0.020/0.000 ms  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## C.BLOC 3

### # BLOC 3:

```
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 21 -j ACCEPT
```

### ❖ iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 25 -j ACCEPT (per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa : **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → port de destí
  - 5.1. Port de destí: **25** ( protocol :**smtp**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet

**-S, --list-rules [chain]**

Print all rules in the selected chain. If no chain is selected, all chains are printed like iptables-save. Like every other iptables command, it applies to the specified table (filter is the default).

**[!] -p, --protocol protocol**

The protocol of the rule or of the packet to check. The specified protocol can be one of **tcp**, **udp**, **udplite**, **icmp**, **icmpv6**, **esp**, **ah**, **sctp**, **mh** or the special keyword **"all"**, or it can be a numeric value, representing one of these protocols or a different one. A protocol name from /etc/protocols is also allowed. A **"!"** argument before the protocol inverts the test. The number zero is equivalent to **all**. **"all"** will match with all protocols and is taken as default when this option is omitted. Note that, in ip6tables, IPv6 extension headers except **esp** are not allowed. **esp** and **ipv6-nonext** can be used with Kernel version 2.6.11 or later. The number zero is equivalent to **all**, which means that you cannot test the protocol field for the value 0 directly. To match on a HBH header, even if it were the last, you cannot use **-p 0**, but always need **-m hbh**.

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 25 -j ACCEPT  
[sudo] contrasenya per a uruloki:  
uruloki@kali-anonymous:~$
```

### ❖ iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 110 -j ACCEPT (per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa : **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → port de destí
  - 5.1. Port de destí: **110** ( protocol :**pop3**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 110 -j ACCEPT  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

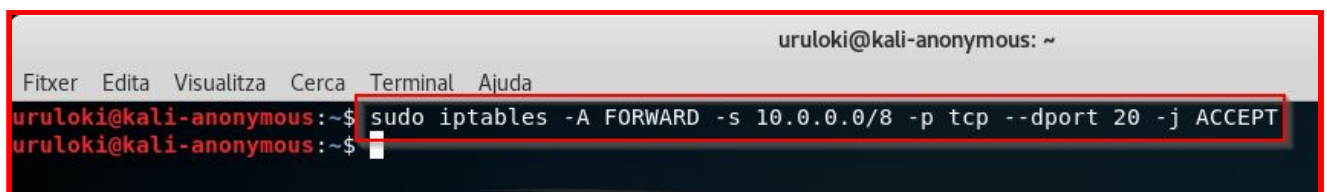
**Data**

02/03/2019

## ❖ iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 20 -j ACCEPT

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resol en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa : **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → Port de destí
  - 5.1. port de destí: **20** ( protocol: **ftp-data**)
  - 5.2. a
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 20 -j ACCEPT  
uruloki@kali-anonymous:~$
```



**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

### ❖ iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 21 -j ACCEPT (per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa : **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → Port de destí
  - 5.1. port de destí: **21** ( protocol: **ftp**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 21 -j ACCEPT  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

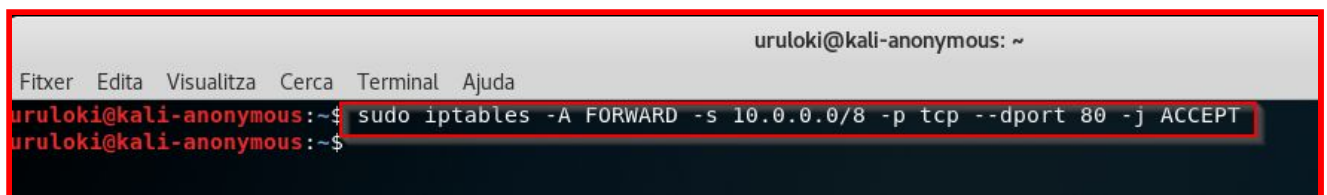
## D.BLOC 4

**# BLOC 4:**

```
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT  
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 443 -j ACCEPT
```

### ❖ **iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT** (per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa : **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → Port de destí
  - 5.1. port de destí: **80**( protocol: **http**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT  
uruloki@kali-anonymous:~$
```



**Nom i Cognoms**

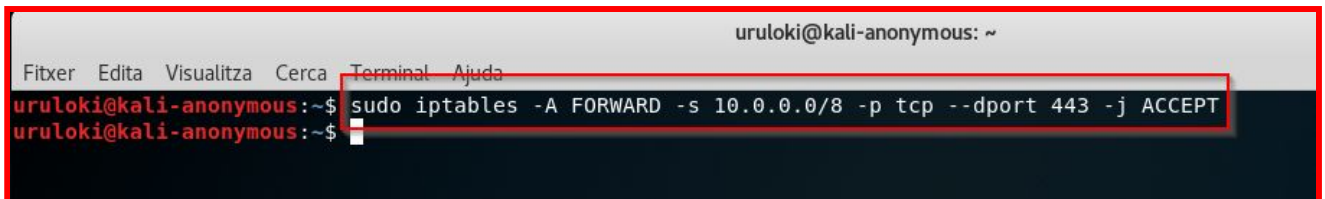
Arnau Subirós Puigarnau

**Data**

02/03/2019

## ❖ iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 443 -j ACCEPT (per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → Port de destí
  - 5.1. port de destí: **443**( protocol: **https**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 443 -j ACCEPT  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

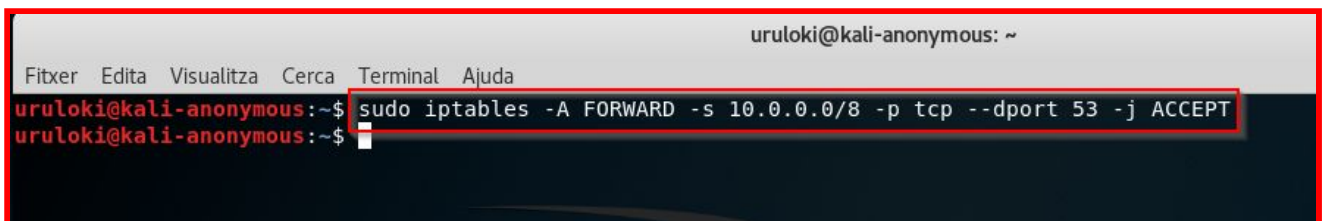
## E.BLOC 5

**# BLOC 5:**

```
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 53 -j ACCEPT  
iptables -A FORWARD -s 10.0.0.0/8 -p udp --dport 53 -j ACCEPT
```

### ❖ **iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 53 -j ACCEPT** (per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **TCP**
5. **--dport** → Port de destí
  - 5.1. port de destí: **53** (protocol: **dns**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 53 -j ACCEPT  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

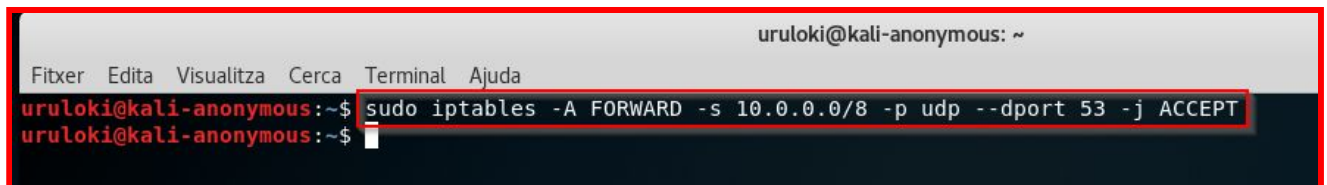
**Data**

02/03/2019

## ❖ iptables -A FORWARD -s 10.0.0.0/8 -p udp --dport 53 -j ACCEPT

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 3.1. IP de la xarxa **10.0.0.0/8**
4. **-p** → El protocol de la regla o del paquet a verificar.
  - 4.1. El protocol especificat: **UDP**
5. **--dport** → Port de destí
  - 5.1. port de destí: **53** (protocol: **dns**)
6. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -p udp --dport 53 -j ACCEPT  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## F. BLOC 6(final de Firewall)

**#Bloc 6:**

```
iptables -A FORWARD -s 10.0.0.7 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -j DROP
iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE
```

**# Activemem enrutament**

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

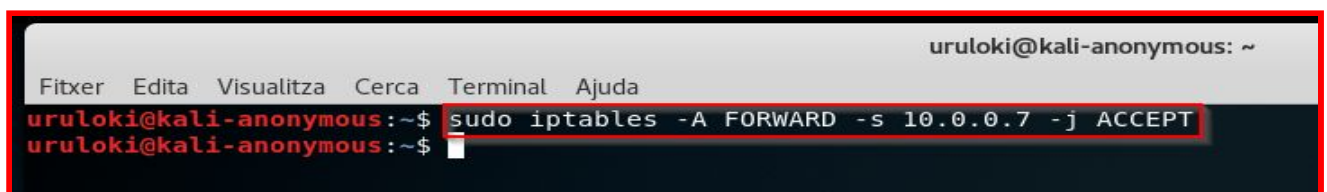
**# Comprobamos les regles**

```
iptables -L -n
```

### ❖ **iptables -A FORWARD -s 10.0.0.7 -j ACCEPT**

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen  
3.1. IP del host(segurament l'Administrador de la Xarxa): **10.0.0.7/8**
4. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
5. **ACCEPT** → (target) es deixa passar el paquet



```
uruloki@kali-anonymous: ~
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.7 -j ACCEPT
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

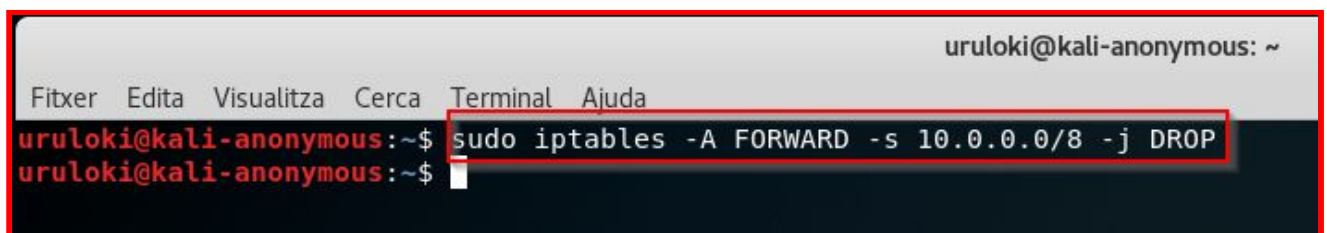
**Data**

02/03/2019

## ❖ iptables -A FORWARD -s 10.0.0.0/8 -j DROP

(per defecte al no especificar ,aquesta regla actúa en la taula filter)

1. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els noms es resolen en més d'una adreça, s'agregarà una regla per a cada adreça possible combinació.
2. **FORWARD** → s'aplica als paquets destinataris a altres maquines que han de travessar la nostre.
3. **-s, --source**: Amb aquest parametre especifica la IP d'origen  
3.1. IP de la xarxa **10.0.0.0/8**
4. **-j** → Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
5. **DROP** → (target) s'ignora el paquet com si l'ordinador estigués apagat.



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A FORWARD -s 10.0.0.0/8 -j DROP  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## ❖ iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE

1. **-t** → Aquesta opció **especifica la taula de coincidència de paquets en la qual ha d'operar el comando**. Si l'el kernel està configurat amb la càrrega automàtica de mòduls, s'intentarà carregar el Mòdul apropiat per a aquesta taula si no està ja allí.
  - 1.1. **nat**→: Aquesta taula es consulta quan es troba un paquet que crea una nova connexió.
2. **-A** → Agrega una o més regles al final de la cadena seleccionada. Quan la font i / o destinació els
3. **POSTROUTING**→ s'aplica als paquets quan estan a punt de sortir del tallafocs
4. **-s, --source**: Amb aquest parametre especifica la IP d'origen
  - 4.1. IP de la xarxa **10.0.0.0/8**
5. **-o**→ s'aplica nom d'una interfície a través del qual serà enviat (per als paquets que entren en un paquet FORWARD OUTPUT i POSTROUTING cadenes). Quan el "!" argument s'utilitza abans del nom de la interfície, l'el sentit està invertit Si el nom de la interfície acaba en un "+", llavors qualsevol interfície que comenci amb això el nom coincidirà. Si s'omet aquesta opció, qualsevol nom d'interfície coincidirà.
  - 5.1. interfície de sortida : **eth0**
6. **-j**→ Això especifica l'objectiu de la regla; és a dir, què fer si el paquet el coincideix. L'objectiu pot ser una cadena definida per l'usuari (a part de la qual es troba en aquesta regla), un dels objectius incorporats especials que decideixen la destinació del paquet immediatament, o una extensió . Si l'opció s'omet en una regla (i -g no s'usa), llavors el fet que coincideixi amb la regla no tindrà efecte en la destinació del paquet, però els comptadors en la regla s'incrementaran.
7. **MASQUERADE** →S'especifica l'objectiu de -j MASQUERADE per a emmascarar l'adreça IP privada d'un node amb l'adreça IP del tallafocs/porta d'enllaç.

```
[!] -o, --out-interface name  
Name of an interface via which a packet is going to be sent (for packets entering the FORWARD, OUTPUT and POSTROUTING chains). When the "!" argument is used before the interface name, the sense is inverted. If the interface name ends in a "+", then any interface which begins with this name will match. If this option is omitted, any interface name will match.
```

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE  
[sudo] contrasenya per a uruloki:  
uruloki@kali-anonymous:~$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## ❖ #Activarem enrutament

- **echo 1 > /proc/sys/net/ipv4/ip\_forward**

S'utilitza per fer que la nostre màquina linux actuï com un ruteador, o com a porta d'accés a internet compartida. Haurem d'activar "IP forwarding" en la nostre màquina virtual que actuarà com ruteador. Però aquesta comanda, el canvi és temporal i s'hauria de fer cada vegada que es reinici la màquina

```
root@kali-anonymous: /home/uruloki
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ echo "Activarem enrutament"
Activarem enrutament
uruloki@kali-anonymous:~$ sudo echo 1>/proc/sys/net/ipv4/ip_forward
bash: /proc/sys/net/ipv4/ip_forward: S'ha denegat el permís
uruloki@kali-anonymous:~$ sudo su
root@kali-anonymous:/home/uruloki# echo 1>/proc/sys/net/ipv4/ip_forward
bash: echo: error d'escriptura: L'argument passat no és vàlid
root@kali-anonymous:/home/uruloki# echo 1 >/proc/sys/net/ipv4/ip_forward
root@kali-anonymous:/home/uruloki#
```

Per verificar si està correctament habilitat utilitzarem la comanda "**cat /proc/sys/net/ipv4/ip\_forward**" que ens dona el valor 1(que significa SI)

```
root@kali-anonymous: /home/uruloki
Fitxer Edita Visualitza Cerca Terminal Ajuda
root@kali-anonymous:/home/uruloki# cat /proc/sys/net/ipv4/ip_forward
1
root@kali-anonymous:/home/uruloki#
```



**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

Si en lloc de reiniciar la màquina, si volem desactivar l'enrutament hauriem d'escriure:

**echo "0" > /proc/sys/net/ipv4/ip\_forward**

posteriorment per confirmar que s'ha desactivat escriure la següent comanda que el seu valor serà **0** *que significa NO*)

**cat /proc/sys/net/ipv4/ip\_forward**

```

root@kali-anonymous: /home/uruloki
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
root@kali-anonymous:/home/uruloki# cat /proc/sys/net/ipv4/ip_forward
1
root@kali-anonymous:/home/uruloki# echo "0">/proc/sys/net/ipv4/ip_forward
root@kali-anonymous:/home/uruloki# cat /proc/sys/net/ipv4/ip_forward
0
root@kali-anonymous:/home/uruloki#

```

## ❖ Comprovarem les regles

- **iptables -L -n**

```

uruloki@kali-anonymous: ~
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
root@kali-anonymous:/home/uruloki# exit
exit
uruloki@kali-anonymous:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target    prot opt source                destination

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:25
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:110
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:20
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:21
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:80
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:443
ACCEPT    tcp  --  10.0.0.0/8             0.0.0.0/0             tcp dpt:53
ACCEPT    udp  --  10.0.0.0/8             0.0.0.0/0             udp dpt:53
ACCEPT    all  --  10.0.0.7               0.0.0.0/0
DROP      all  --  10.0.0.0/8             0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
uruloki@kali-anonymous:~$

```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

Fes una explicació a grans trets de que n'opines del Firewall ara que n'has inspeccionat en detall les seves normes, quina és la seva política de seguretat (definida al BLOC 2) i quines possibles fugues de seguretat no és contemplen. Afegiries alguna regla més?

```
# BLOC 2: (política de seguretat)
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING
ACCEPT
iptables -A INPUT -i lo -j ACCEPT
```

Primer analitzem varies coses:

- ☐ La majoria de polítiques estan destinades a la “Taula Filter” ( per defecte)
- ☐ En el BLOC 1 , 2 i 6 s'especifica en alguna regla l'utilització de la “Taula Nat” fent servir el comando : **-t nat**

**#BLOC 1** : serveix per netejar totes les polítiques anteriors, començar de 0.

- **iptables -F** : esborrar regles (taula filter)
- **iptables -X** : esborrar cadenes (taula filter)
- **iptables -Z** : estadístiques a zero (taula filter)
- **iptables -t nat -F** : esborrar regles (taula nat)

**#BLOC 2** : base d'un tallafocs permissiu ja que deixa a tots els paquets circular lliurement. ( polítiques per defecte :ACCEPTAR )

- ❖ **iptables -P INPUT ACCEPT** :Acceptar com a política per defecte dels paquets d'entrada (taula filter)
- ❖ **iptables -P OUTPUT ACCEPT**:Acceptar com a política per defecte dels paquets de sortida(taula filter)
- ❖ **iptables -P FORWARD ACCEPT**Acceptar com a política per defecte la redirecció de paquets (taula filter)
- ❖ **iptables -t nat -P PREROUTING ACCEPT**:Acceptar com a política per defecte sobre el paquet abans de ser enrutat (taula nat)
- ❖ **iptables -t nat -P POSTROUTING ACCEPT**:Acceptar com a política per defecte sobre el paquet abans de sortir al tallafocs- (taula nat)

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

- ❖ **iptables -A INPUT -i lo -j ACCEPT:** Afegir acceptar com a política per defecte l'interfície loopback(127.0.0.1).

➤ **Per evitar errors del sistema hem d'acceptar totes les comunicacions per l'interfície lo (localhost)**

En la pràctica és gairebé com no tenir tallafocs ja que deixa permetre qualsevol paquet que no consti en les posteriors regles, una política de denegació és més costosa però em de ser conscients que amb aquesta política augmenta el risc de permetre atacs. O sigui que aquesta política per defecte és més fàcil d'utilitzar que una política restrictiva, però hem de tenir una especial cura a l'hora de posar regles.

### **#BLOC 3:** Afegeix polítiques a la taula filter (les comunicacions que ens interessin)

```
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 21 -j ACCEPT
```

S'està afegint 4 regles permissives en la taula filter en que els paquets passen per la nostra màquina, i l'origen de la seva IP és la xarxa LAN : 10.0.0.0/8 on accepta els paquets que utilitzen els ports de les següents aplicacions : ftp-data,ftp,pop3 i smtp

### **#BLOC 4**

```
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 443 -j ACCEPT
```

S'està afegint 2 regles permissives en la taula filter en que els paquets passen per la nostra màquina, i l'origen de la seva IP (la IP de la xarxa 10.0.0.0/8) on accepta els paquets que utilitzen els ports de les següents aplicacions : http i https.

### **# BLOC 5:**

```
#iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 53 -j ACCEPT
#iptables -A FORWARD -s 10.0.0.0/8 -p udp --dport 53 -j ACCEPT
```

S'està afegint 2 regles permissives en la taula filter en que els paquets passen per la nostra màquina, i l'origen de la seva IP (la IP de la xarxa 10.0.0.0/8) on accepta els paquets que utilitzen els ports de les següents aplicacions : dns que utilitza el protocol TCP i UDP.

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

## # BLOC 6 (final de Firewall):

**iptables -A FORWARD -s 10.0.0.7 -j ACCEPT** → S'esta afegint 1 regles permisiva en la taula filter en que els paquets passen per la nostre màquina, i l'origen de la seva IP (10.0.0.7/8 on s'accepta tots els paquets..

**iptables -A FORWARD -s 10.0.0.0/8 -j DROP** → S'esta afegint 1 regles restrictiva en la taula filter en que els paquets passen per la nostre màquina, i l'origen de la seva IP (la IP de la xarxa 10.0.0.0/8) on s'ignoren els paquets.

**iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE**

- Utilitzar nat per que els paquets puguin arribar a internet (el nostre linux rep directament una IP publica)
- És fa un emascarament de la xarxa local( 10.0.0.0/8) on la seva interfície es eth0 ja que la IP és pública i pot variar amb el temps

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

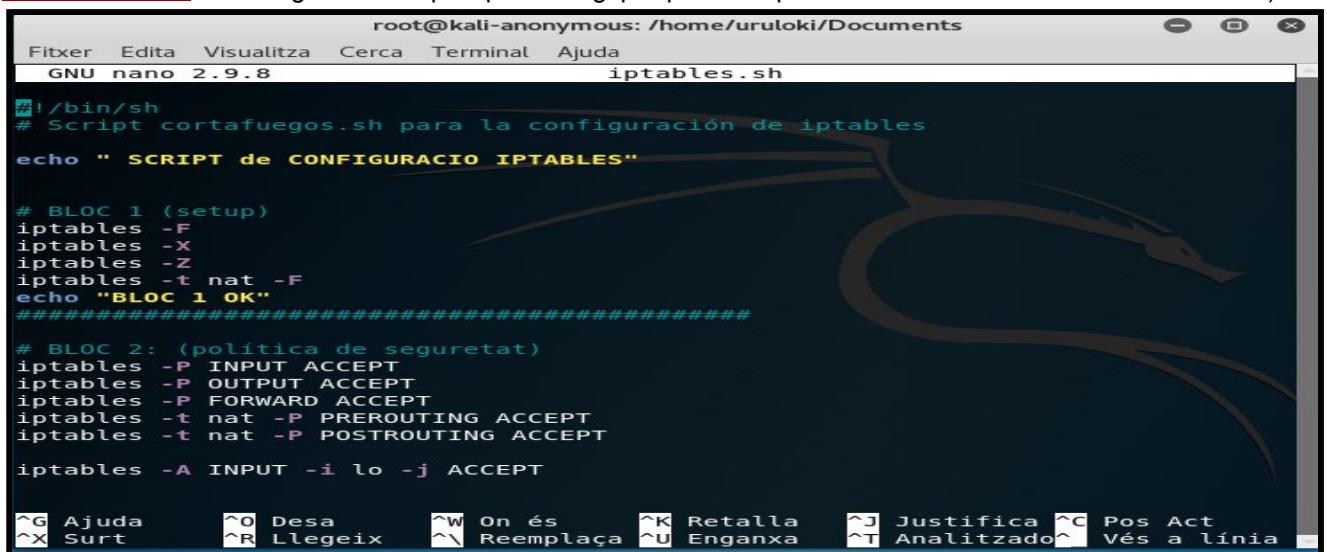
## RESUMINT:

- He vist que s'ha utilitzat la política **FORWARD** que permet a l'Administrador controlar on s'enviaran els paquets dins d'aquesta LAN ( IP de la Xarxa : 10.0.0.0/8).
- La màquina Linux amb una interfície **eth0** a la LAN : 10.0.00/8 actúa com a proxy que permet els paquets a internet desde aquesta xarxa utilitzant:
  - **ftp-data**
  - **ftp**
  - **pop3**
  - **smtp**
  - **dns**
  - **http**
  - **https**
- A més a més permet dona permís sense restriccions a la IP : **10.0.0.7** ( segurament la IP de l'Administrador de la Xarxa )

## VISUALITZACIÓ del SCRIPT: “ iptables.sh ”

Obrirem l'editor nano i escriurem el script amb el nom **iptables.sh**

**ANOTACIONS:** He afegit “echos “ per que es vegi per pantalla que cada block s'ha realitzat correctament)



```
root@kali-anonymous: /home/uruloki/Documents
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
GNU nano 2.9.8                                iptables.sh

#!/bin/sh
# Script cortafuegos.sh para la configuración de iptables

echo " SCRIPT de CONFIGURACIO IPTABLES"

# BLOC 1 (setup)
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
echo "BLOC 1 OK"
#####

# BLOC 2: (política de seguretat)
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

iptables -A INPUT -i lo -j ACCEPT

^G Ajuda      ^O Desa      ^W On és     ^K Retalla  ^J Justifica ^C Pos Act
^X Surt       ^R Llegeix   ^\ Reemplaça ^U Enganxa  ^T Analitzado ^_ Vés a línia
```



Nom i Cognoms

Data

Arnau Subirós Puigarnau

02/03/2019

```

root@kali-anonymous: /home/uruloki/Documents
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
GNU nano 2.9.8                                iptables.sh

#####

# BLOC 2: (política de seguretat)
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

iptables -A INPUT -i lo -j ACCEPT

echo "BLOC 2 OK"
#####

# BLOC 3:
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 21 -j ACCEPT
echo "BLOC 3 OK"
#####

# BLOC 4:

^G Ajuda      ^O Desa      ^W On és      ^K Retalla    ^J Justifica  ^C Pos Act
^X Surt       ^R Llegeix    ^\ Reemplaça  ^U Enganxa    ^T Analitzado ^_ Vés a línia

```

```

root@kali-anonymous: /home/uruloki/Documents
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
GNU nano 2.9.8                                iptables.sh

echo "BLOC 4 OK"
#####

# BLOC 5:
iptables -A FORWARD -s 10.0.0.0/8 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -p udp --dport 53 -j ACCEPT
echo "BLOC 5 OK"
#####

# BLOC 6 (final de Firewall):
iptables -A FORWARD -s 10.0.0.7 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/8 -j DROP
iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE
echo "BLOC 6 OK : final del firewall"
#####

# Activem enrutament
echo 1 > /proc/sys/net/ipv4/ip_forward
echo "Activem del enrutament activat OK"
#####

# Comprobamos les regles
iptables -L -n
echo "Revisem les regles:"

^G Ajuda      ^O Desa      ^W On és      ^K Retalla    ^J Justifica  ^C Pos Act
^X Surt       ^R Llegeix    ^\ Reemplaça  ^U Enganxa    ^T Analitzado ^_ Vés a línia

```

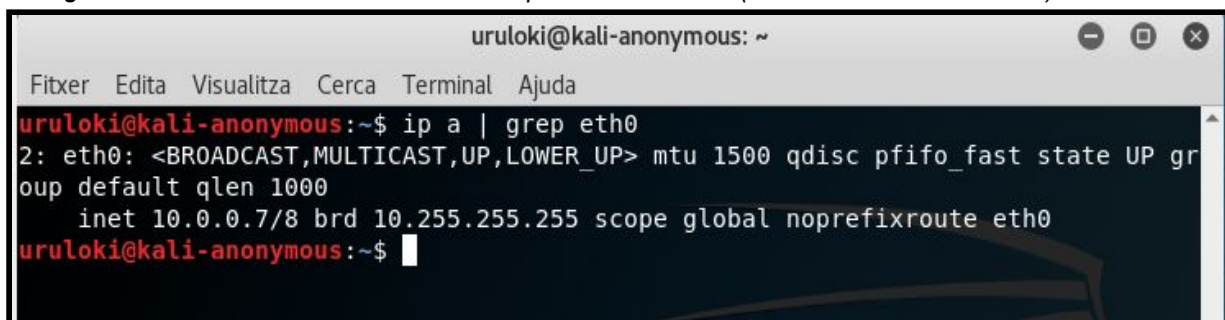
**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

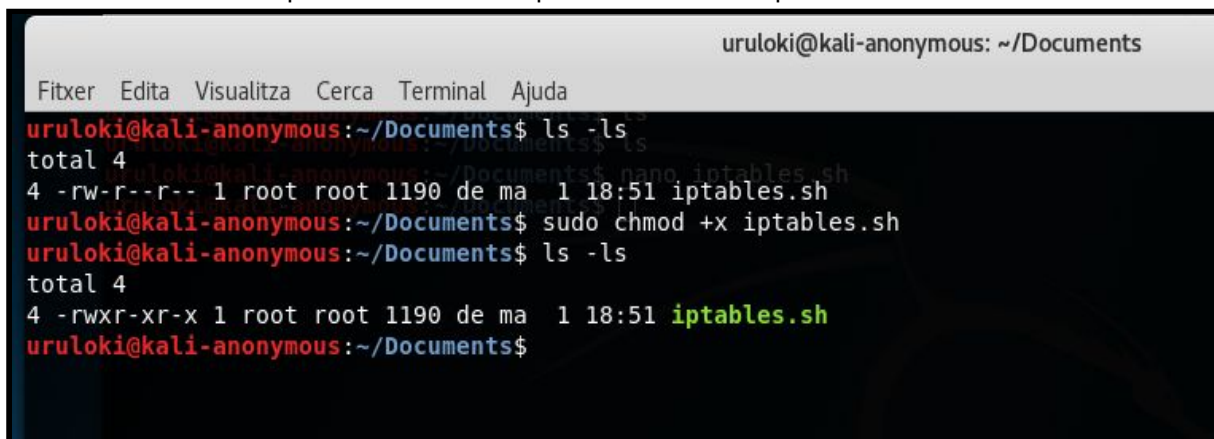
02/03/2019

Configurem la interfície eth0 amb la IP de la pràctica : 10.0.0.7(Administrado de la Xarxa)



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ ip a | grep eth0  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    inet 10.0.0.7/8 brd 10.255.255.255 scope global noprefixroute eth0  
uruloki@kali-anonymous:~$
```

A continuació es donen permisos d'execució per i executar el script.



```
uruloki@kali-anonymous: ~/Documents  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~/Documents$ ls -ls  
total 4  
4 -rw-r--r-- 1 root root 1190 de ma 1 18:51 iptables.sh  
uruloki@kali-anonymous:~/Documents$ sudo chmod +x iptables.sh  
uruloki@kali-anonymous:~/Documents$ ls -ls  
total 4  
4 -rwxr-xr-x 1 root root 1190 de ma 1 18:51 iptables.sh  
uruloki@kali-anonymous:~/Documents$
```



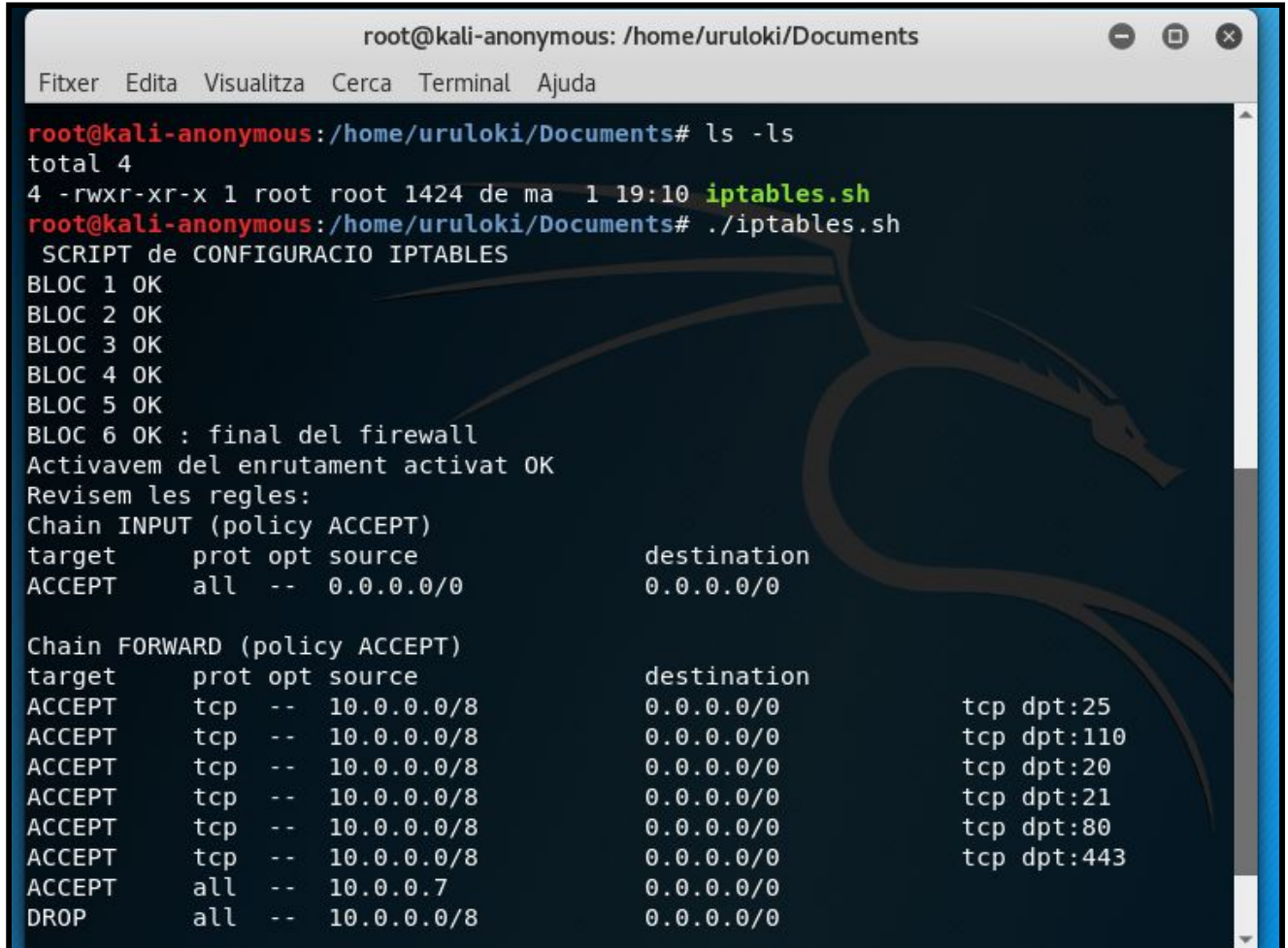
**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

02/03/2019

Executem el SCRIPT "iptables.sh"



```
root@kali-anonymous: /home/uruloki/Documents
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda

root@kali-anonymous:/home/uruloki/Documents# ls -ls
total 4
4 -rwxr-xr-x 1 root root 1424 de ma  1 19:10 iptables.sh
root@kali-anonymous:/home/uruloki/Documents# ./iptables.sh
SCRIPT de CONFIGURACIO IPTABLES
BLOC 1 OK
BLOC 2 OK
BLOC 3 OK
BLOC 4 OK
BLOC 5 OK
BLOC 6 OK : final del firewall
Activavem del enrutament activat OK
Revisem les regles:
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    all  --  0.0.0.0/0              0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination      tcp dpt:25
ACCEPT    tcp  --  10.0.0.0/8            0.0.0.0/0        tcp dpt:110
ACCEPT    tcp  --  10.0.0.0/8            0.0.0.0/0        tcp dpt:20
ACCEPT    tcp  --  10.0.0.0/8            0.0.0.0/0        tcp dpt:21
ACCEPT    tcp  --  10.0.0.0/8            0.0.0.0/0        tcp dpt:80
ACCEPT    tcp  --  10.0.0.0/8            0.0.0.0/0        tcp dpt:443
ACCEPT    all  --  10.0.0.7              0.0.0.0/0
DROP      all  --  10.0.0.0/8            0.0.0.0/0
```