



# HardBox

CIBERSEGURIDAD Y HARDENING

MANEL MAYORAL, AHNUAR RAMIREZ, MAYA REYES Y  
JOSEP MARTÍNEZ

## INDICE:

IDEA PRINCIPAL .....	3
HARDWARE .....	4
ESQUEMA DE RED .....	4
ESQUEMA DE PERMISOS .....	4
HARDWARE FÍSICO .....	5
FIREWALL: .....	5
NAS1: .....	6
NAS2: .....	6
WINDOWS SERVER: .....	6
SWITCH: .....	7
SERVICIOS CLOUD .....	8
SERVIDOR SMTP: .....	8
SERVIDOR WEB: .....	8
SOFTWARE .....	9
RESUMEN DE NUESTRO SOFTWARE .....	9
HYPER-V .....	10
APACHE .....	11
POSTFIX .....	12
PFSENSE .....	13
REDIRECCIONES .....	13
DHCP .....	14
VPN .....	14
SISTEMAS DE BACKUP .....	15
VEEAM .....	15
COPIAS REMOTAS POR FTP .....	17
MYSQL DUMP .....	19
APLICACIÓN WEB .....	20
DISEÑO .....	20
BASE DE DATOS .....	23
DIAGRAMA RELACIONAL .....	23
TABLAS .....	23
DOMINIO .....	24
CLOUDFLARE .....	24
DNS .....	24

WAF .....	25
MAILING .....	25
SPF .....	26
DMARC .....	26
MAIL FORWARDING .....	27
CONTENIDO .....	28
TEMARIO .....	28
MAQUINAS .....	28
RETOS .....	28
GATEWAY CLIENTES .....	29
DHCP.....	29
SCRIPTS.....	30
ACTUALIZAR LAS MAQUINAS DE LA WEB .....	30
BACKUPS DE LA BASE DE DATOS .....	31
SOCKETS .....	32
ENVIO DE DATOS .....	32
RECIBO DE DATOS .....	32
IPTABLES:.....	33
REDIRECCIONAR PAQUETES A LA RED INTERNA .....	33
BLOQUEAR CONEXIONES VPN A SERVIDORES .....	33
ADMITIR EL ACCESO WEB SOLO POR CLOUDFLARE .....	34
INFORMACION DE DISPOSITIVOS Y USUARIOS .....	35
MEMORIA .....	37
NUESTROS INICIOS: .....	37
MONTANDO EL FIREWALL:.....	37
MONTANDO EL SERVIDOR: .....	37
CONFIGURANDO EL SERVIDOR WEB: .....	37
CONFIGURANDO EL SERVIDOR DE MÁQUINAS VIRTUALES: .....	38
CREACIÓN DE MÁQUINAS VIRTUALES: .....	38
APARTADO WEB: .....	38
COMUNICACIÓN ENTRE MAQUINAS.....	38
CONCLUSIONES .....	39
BIBLIOGRAFIA .....	40
CODIGO FUENTE DE LA WEB.....	41
WEB .....	41

## IDEA PRINCIPAL

Nuestra idea es enseñar a nuestros usuarios como tener sus sistemas protegidos y los diferentes ciberataques que pueden sufrir, con fines educativos, creando una plataforma web con retos de ciberseguridad y hardening.

Lo que queremos hacer es una plataforma web donde cada persona pueda crearse una cuenta y tenga una serie de retos asignados, cuando un usuario decida iniciar un reto o mejor dicho una máquina, la web tendrá una serie de máquinas abiertas donde cada día serán diferentes y luego desde la interfaz web saldrá la IP y las credenciales de la máquina para que el usuario se conecte e intente realizar las tareas de hardening o ciberseguridad. Cuando un usuario haya terminado una máquina se harán unas comprobaciones o el usuario introducirá la flag dependiendo el tipo de máquina y finalmente se dará una puntuación de la máquina.

Nuestra web también tendrá algunos retos CTF, donde cada usuario podrá crear y realizar retos para obtener una puntuación.

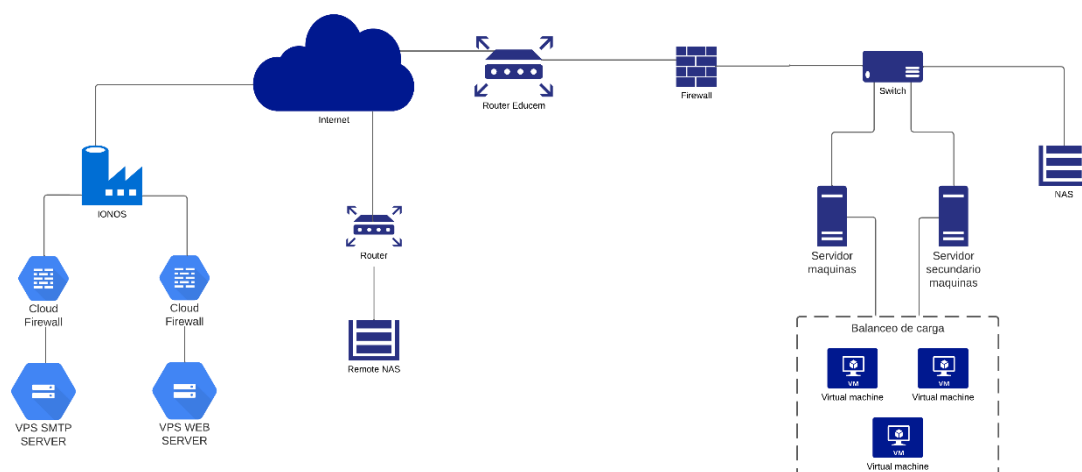
Cada usuario tendrá su cuenta de la plataforma web, pero deberá conectarse por VPN para tener conexión directa a las máquinas.

En conclusión queremos transmitir a los usuarios buenas prácticas en el ámbito de ciberseguridad y técnicas de hardening para diferentes sistemas aparte de informar de diferentes ataques muy comunes pero fáciles de defender.

## HARDWARE

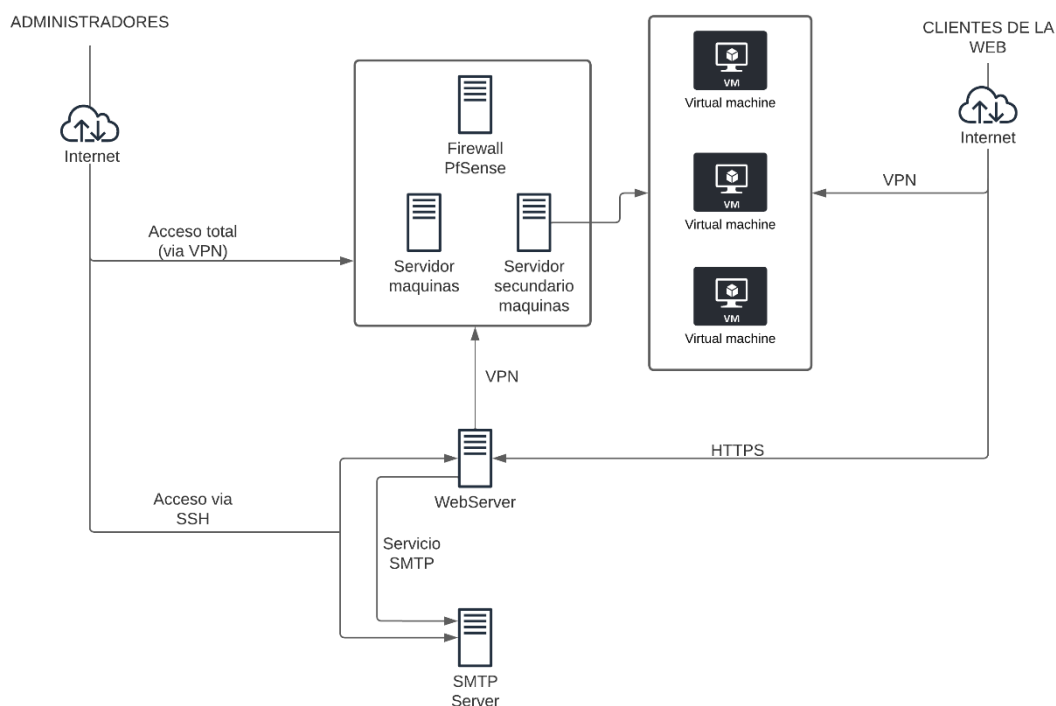
### ESQUEMA DE RED

Éste es el esquema de nuestra red, como podemos observar, tenemos varios servicios distribuidos en varios servidores y en varias localizaciones. Más adelante lo veremos más detallado, pero en la propia red del educem, tenemos un servidor que nos ofrece máquinas virtuales, pero además tenemos servicios externos en el cloud de IONOS, que es una empresa de hosting, como el servicio web, base de datos y servicio de correo.



### ESQUEMA DE PERMISOS

En este esquema vemos hasta dónde pueden acceder los usuarios administradores y clientes.



## HARDWARE FÍSICO

### FIREWALL:

- Ordenador HP Optiplex:
  - 160 GB de disco duro
  - 2GB de RAM
  - 2 Interfaces de red (LAN y WAN)

Con el firewall, principalmente, gestionaremos la VPN y el servidor DHCP, a parte, nos ofrecerá la seguridad de nuestra red local y el acceso a las redes publicas (internet) ya que cuenta con 2 interfaces de red, una para nuestra red de HardBox y la otra para el acceso a internet desde la red del educem.



# LAN

192.168.1.0/24

# WAN

10.0.0.0/16 (Educem)

#### NAS1:

- Modelo: Netgear ReadyNas NVX RNDX400E
  - Bahías: 4
  - Capacidad de almacenamiento: 16TB
  - RAM: 1 GB DDR2

En este NAS, guardaremos copias de seguridad e imágenes de máquinas virtuales, éste nas está físicamente en nuestra red del centro.



#### NAS2:

- D-Link 320L
  - 2 Bahías para almacenamiento
  - RAM: 256 MB
  - Capacidad de almacenamiento 2TB

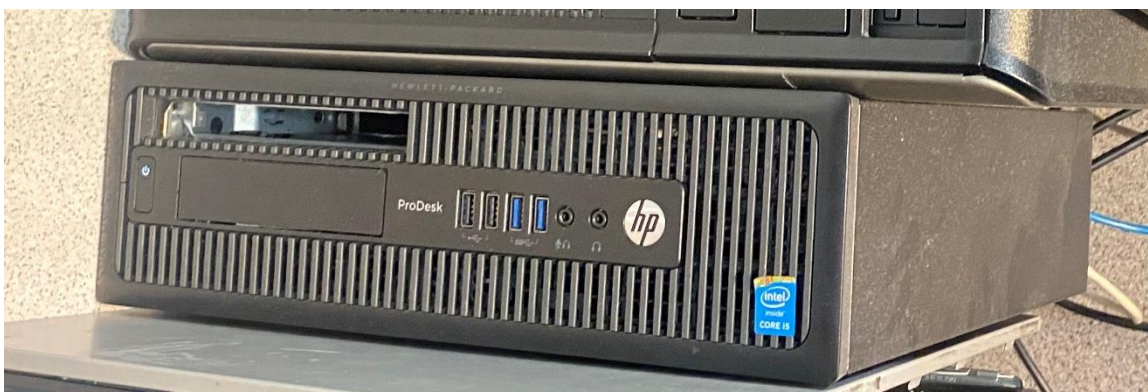
Éste NAS, estará ubicado remotamente, y será donde se suban las copias de seguridad a través de internet.



#### WINDOWS SERVER:

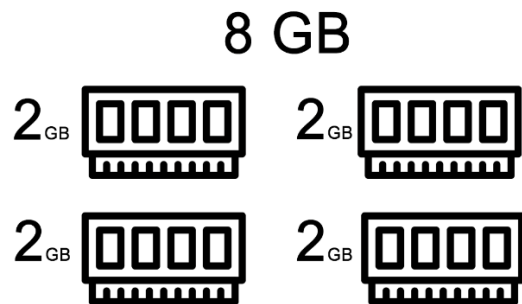
- HP Pro desk 600
  - Intel Core i5-4590
  - 8GB Ram
  - Disco duro C: 120GB SSD
  - Disco duro D: 600GB HDD

Este servidor tendrá un windows server dónde tendremos el servicio de virtualización para las máquinas de los clientes.



En nuestro windows server, hemos ampliado la memoria RAM, ya que tenia 4GB y le hemos puesto 8GB, esto nos permitirá abrir más máquinas virtuales simultaneamente.

Antes tenía 2 módulos de 2 GB y ahora tiene 4 módulos de 2 GB:



#### SWITCH:

- TP-LINK Desktop switch
  - 8 Puertos RJ-45
  - 10/100/1000 Mb

Éste es el switch que nos permitirá interconectar todos los servidores a nuestra red a una velocidad de 1000Mb, si el cable lo permite.





## SERVICIOS CLOUD

Para este proyecto, hemos utilizado dos servidores virtuales (VPS), que dos miembros del equipo teníamos ya contratados, éstos servidores nos ofrecerán un servicio 24/7 sin ningún tipo de caída ya que están en la nube y serán perfectos para alojar nuestra web y el servicio de mailing que veremos más adelante.

El precio de éstos servidores es de tan solo 1€ al mes, aunque sus recursos son muy limitados, a nosotros ya nos son suficientes para llevar a cabo estos servicios.

	CPU	RAM	SSD	Precio
VPS S	1 vCore	512 MB	10 GB	Solo <b>1</b> €/mes IVA excl.
				<a href="#">Configurar</a>

### SERVIDOR SMTP:

- VPS S
  - 1 virtual core.
  - 512 MB RAM.
  - 10 GB SSD.
  - 400Mb Velocidad internet.

Éste servidor, está ubicado remotamente en el datacenter de IONOS de estados unidos y nos ofrecerá el servicio de mailing para nuestra aplicación web.

### SERVIDOR WEB:

- VPS S
  - 1 virtual core.
  - 512 MB RAM.
  - 10 GB SSD.
  - 400Mb Velocidad internet.

Éste servidor, está ubicado remotamente en el cloud de IONOS, exactamente en el datacenter de Madrid y será donde esté el servicio web y de base de datos.

## SOFTWARE

### RESUMEN DE NUESTRO SOFTWARE

Hemos utilizado una gran variedad de programario para poder hacer que funcione todo correctamente, con seguridad y redundancia de datos.

	Windows Server	Sistema Operativo del servidor de máquinas
	Ubuntu Server	Sistema Operativo del servidor Web y SMTP
	Apache	Servicio WEB
	MySQL	Servicio de base de datos
	PHP	Lenguaje de programación para la aplicación WEB
	Hyper-v	Servicio de virtualizacion de máquinas.
	PowerShell	Lenguaje de programación para los scripts de windows
	Bash	Lenguaje de programación de scripts de ubuntu
	OpenVPN	Servicio de VPN
	Postfix	Servicio de envío de correo
	Veeam	Servicio de copias de seguridad
	PfSense	Sistema operativo del firewall
	Cloudflare	Web Application Firewall, protege nuestra web de conexiones no deseadas y también hace de relay de correos electrónicos

## HYPER-V

Éste es el servicio de virtualización que hemos utilizado y va sobre windows server, en el panel de control podemos ver las máquinas que tenemos, encenderlas, apagarlas, etc.

Máquinas virtuales							
Nombre	Acción en c...	Uso de CPU	Memoria asignada	Tiempo activo	Estado	Versión de c...	Mantenimient...
ASIX	ejecutando	0 %	512 MB	19:17:07		9.0	No aplicable
MRROBOT	ejecutando	0 %	512 MB	00:00:24		9.0	No aplicable
Ubuntu	ejecutando	0 %	1024 MB	11.09:26:49		9.0	No aplicable

También podemos conectarnos a las VM:



```
josep@dhcp:~$ ls
josep.ovpn  prueba.sh  reciveRew.sh  requests_log.txt
josep@dhcp:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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
```

Lo bueno de este servicio, es que las máquinas se quedan abiertas en segundo plano y con scripts de power shell podemos automatizar tareas en función de la necesidad de los usuarios.

## APACHE

Para el servidor web, hemos configurado un virtual host en el apache, el cual hemos hecho alguna pequeñas configuraciones, aunque las opciones de seguridad las administraremos mediante Cloudflare.

Para comenzar hemos generado los certificados SSL con Let's encrypt, ya que es una autoridad certificadora válida:

```
josep@localhost:~$ sudo ls -l /etc/ssl/private/ssl-cert-snakeoil.key
-rw-r----- 1 root ssl-cert 1708 Apr 20 16:59 /etc/ssl/private/ssl-cert-snakeoil.key
josep@localhost:~$ ls -l /etc/ssl/certs/ssl-cert-snakeoil.pem
-rw-r--r-- 1 root root 1099 Apr 20 16:59 /etc/ssl/certs/ssl-cert-snakeoil.pem
josep@localhost:~$
```

Luego hemos puesto la ruta de los certificados en el virtual host del apache:

```
SSLEngine on
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

Luego hemos reiniciado el servicio y ya podíamos acceder por HTTPS sin ningún problema.

Entre otras configuraciones del apache, también hemos deshabilitado el directory listing de nuestra web, esto es importante para la seguridad, así ningún usuario puede ver los archivos ocultos que podemos tener en la carpeta pública del apache.

Ésto lo hemos hecho con un pequeño fichero en la carpeta pública, que contiene la siguiente información:

```
root@localhost:/var/www/html# cat .htaccess
Options +Indexes
```

## POSTFIX

Este servicio va a ser el que realmente envíe los correos electrónicos, lo hemos instalado en un servidor VPS y es el servicio “Postfix”.

A continuación, veremos un poco la configuración que hemos llevado a cabo para que funcione el servicio.

Aquí tenemos la configuración básica, donde hemos indicado nuestro dominio, las ip que tenemos permitidas enviar correos y otras configuraciones.

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = smtp.hardbox.ga
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, smtp.hardbox.ga, hardbox, localhost.localdomain, localhost.localdomain, localhost
relayhost =
mynetworks = 85.48.53.144 127.0.0.1/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

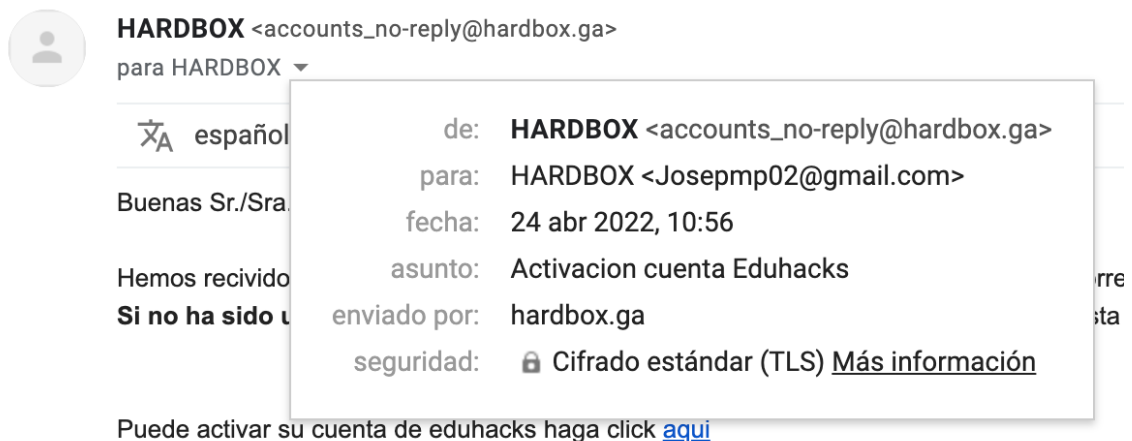
También hemos configurado el TLS, que sirve para que los correos se envíen encriptados y no se puedan interceptar, para ello hemos generado un certificado con let's encrypt.

```
# TLS parameters
smtpd_tls_cert_file=/etc/letsencrypt/live/hardbox.ga/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/hardbox.ga/privkey.pem
smtpd_use_tls=yes
smtpd_tls_security_level=may

smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes

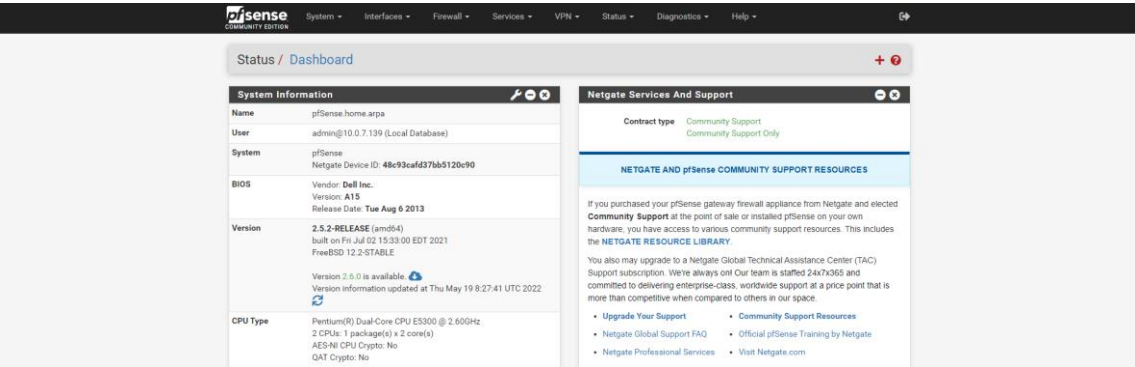
smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=encrypt
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtp_tls_note_starttls_offer = yes
```

A parte de esto hemos configurado el fichero de logs y algún parámetro más, finalmente el servicio funciona correctamente, para ello hemos probado con nuestra web:

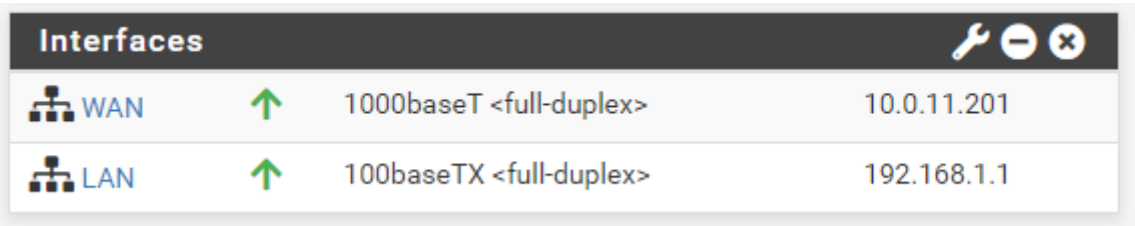


PFSENSE

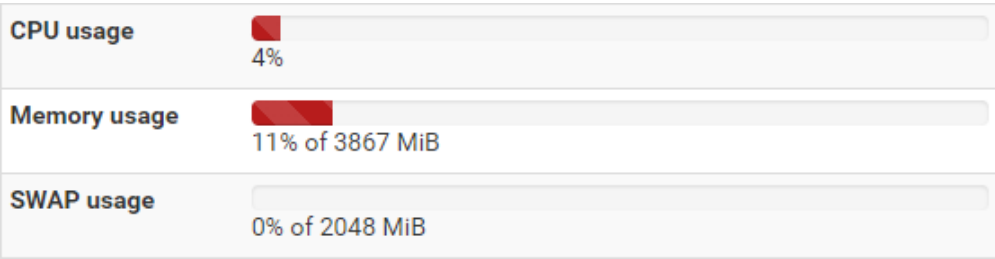
Este es el panel de nuestro firewall desde donde podemos realizar las configuraciones:



Vemos las IP que tenemos en las interfaces de red:



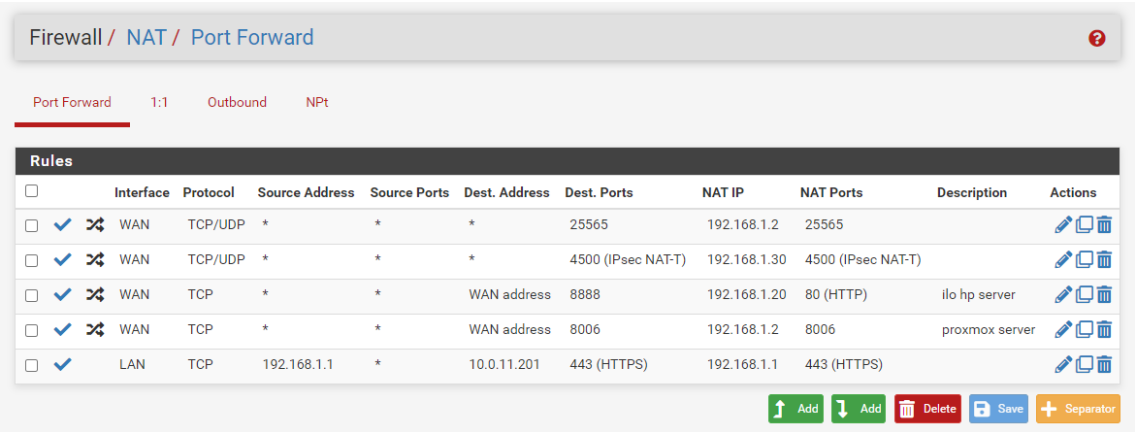
También vemos la carga del sistema:



REDIRECCIONES

En las redirecciones, tenemos los puertos que queramos que sean accesibles desde la red del educem y en caso de que el Tino, el administrador de la red de Educem, nos haya abierto los puertos a internet tendremos este servicio expuesto a internet.

En nuestro caso tenemos el puerto 4500 abierto a internet que es el puerto de la VPN para nuestros clientes.



## DHCP

El PfSense, también nos hace de DHCP para nuestra red y tenemos configurada un rango de IP's: 192.168.1.20 - 192.168.1.100, aunque en teoría en nuestra red no habra clientes, ya que será la VPN quien asigne las IP, a parte hemos configurado clientes fijos por su dirección mac al windows server y al servidor NAS.

Status / DHCP Leases

Search

Search term

All

Search

Clear

Enter a search string or \*nix regular expression to filter entries.

Leases

	IP address	MAC address	Client Id	Hostname	Description	Start	End	Online	Lease Type	Actions
	192.168.1.10	00:22:3f:a9:a5:df	NAS	nas-A9-A5-DE	servidor nas	n/a	n/a	online	static	
	192.168.1.3	ec:b1:d7:49:01:dc	virtualserver	virtualserver	server de m	n/a	n/a	online	static	
	192.168.1.2	18:a9:05:2d:ae:68	WebServer	web	Web server	n/a	n/a	offline	static	
	192.168.1.30	00:15:5d:01:03:09		dhcp		2022/05/19 08:25:19	2022/05/19 10:25:19	online	active	

Leases in Use

Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.1.20	192.168.1.100	1

Host	MAC	IP
NAS	00:22:3f:a9:a5:df	192.168.1.10
Windows Server	ec:b1:d7:49:01:dc	192.168.1.3

## VPN

La VPN de administración se ejecuta directamente en el firewall y será donde nos conectaremos para administrar los servidores. Esta VPN funciona sobre el puerto 1196 que fue el que el administrador de red del educem nos asignó a nuestra IP

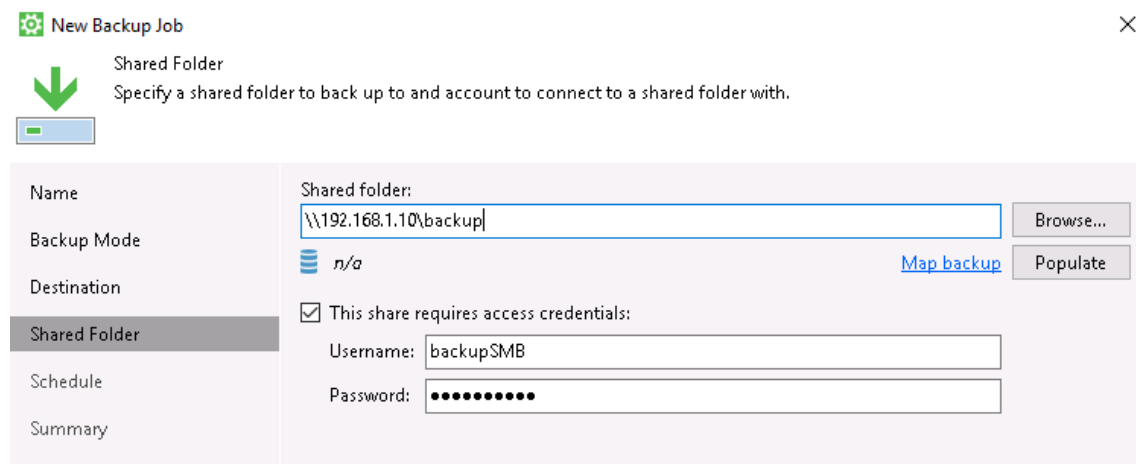
VPN / OpenVPN / Servers						
Servers	Clients	Client Specific Overrides	Wizards	Client Export	Shared Key Export	
OpenVPN Servers						
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions	
WAN	UDP / 1196 (TUN)	10.0.8.0/24	Mode: Remote Access ( SSL/TLS + User Auth ) Data Ciphers: AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN SERVER TM		

## SISTEMAS DE BACKUP

### VEEAM

Hemos configurado Veeam para hacer una copia incremental diariamente y una completa semanalmente del sistema operativo completo. A parte se reemplazan las copias de la semana anterior por las nuevas, ahorrando espacio en disco.

Luego hemos seleccionado el destino de las copias en nuestro servidor NAS:



**New Backup Job** [Close]

Shared Folder  
Specify a shared folder to back up to and account to connect to a shared folder with.

Shared Folder

Name: Shared folder:

Backup Mode:  [Map backup](#)

Destination: ☒ This share requires access credentials:

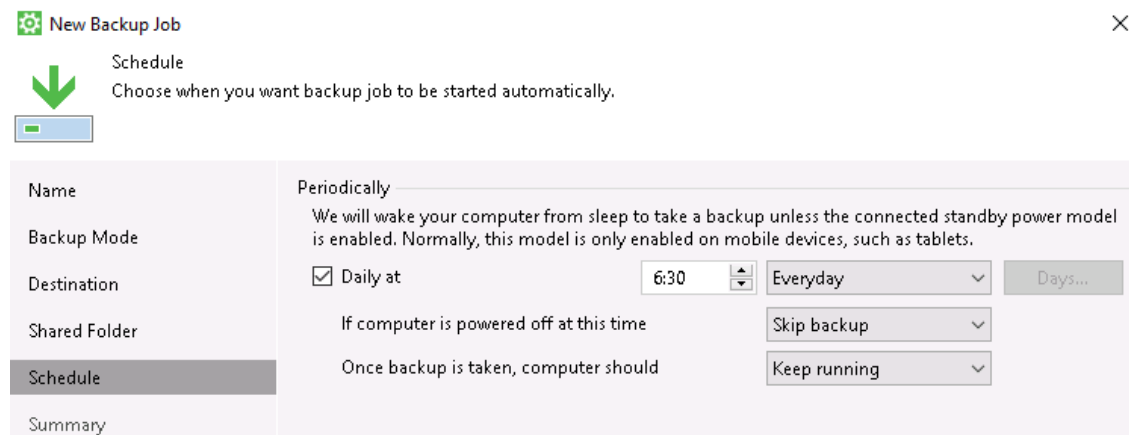
Username:

Password:

Schedule

Summary

Seguidamente hemos configurado que las copias se hagan a las 6:30 de la madrugada. Luego hemos seleccionado que los domingos se haga la copia completa.



**New Backup Job** [Close]

Schedule  
Choose when you want backup job to be started automatically.

Schedule

Name: Periodically

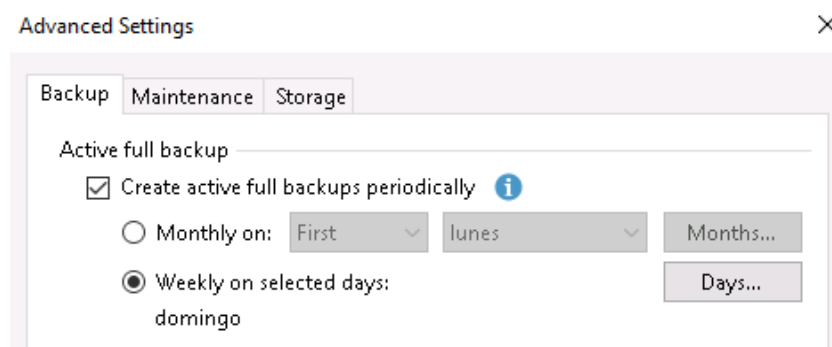
Backup Mode: We will wake your computer from sleep to take a backup unless the connected standby power model is enabled. Normally, this model is only enabled on mobile devices, such as tablets.

Destination: ☒ Daily at

Shared Folder: If computer is powered off at this time

Schedule: Once backup is taken, computer should

Summary



**Advanced Settings** [Close]

Backup Maintenance Storage

Active full backup

☒ Create active full backups periodically

☐ Monthly on:

☒ Weekly on selected days:

domingo



Y finalmente al terminar la configuración, hemos hecho la primera copia completa.

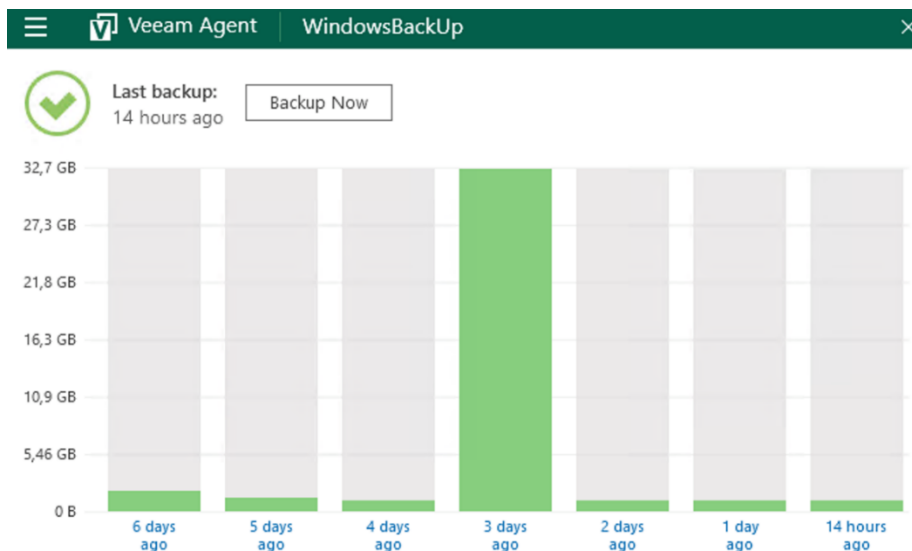
← Restore point details WindowsBackUp ×

Backed up items: n/a  
Backup duration: 0:01:01  
Restore point size: 0 B

Total backup size: n/a  
Average backup duration: 0:00:00  
Free disk space: 582 GB

Action	Duration
✓ Initializing	
✓ Preparing for backup	0:00:11
✓ Backup file will be encrypted	
▶ Creating VSS snapshot	0:00:03

Al cabo de unos días, vemos que las copias se van realizando correctamente:



En cambio en el resumen de la copia completa podemos ver que ha copiado 32 GB en unos 16 minutos:

← Restore point details WindowsBackUp ×

Backed up items: Recuperación;EFI system partition..  
Backup duration: 0:16:35  
Restore point size: 32,7 GB

Total backup size: 98,4 GB  
Average backup duration: 0:07:13  
Free disk space: 476 GB

En el resumen de la copia incremental vemos que ha copiado menos de 1GB en unos 5 minutos:

← Restore point details WindowsBackUp ×

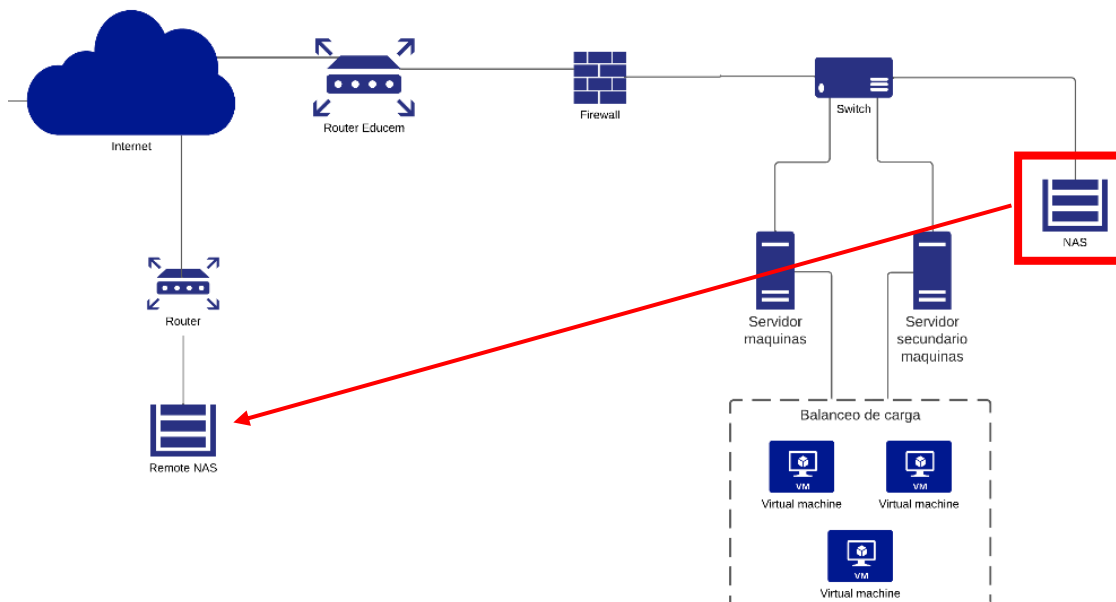
Backed up items: Recuperación;EFI system partition..  
Backup duration: 0:05:41  
Restore point size: 0,98 GB

Total backup size: 101 GB  
Average backup duration: 0:07:13  
Free disk space: 476 GB

Finalmente vemos que la copia de seguridad entera es de 101 GB.

## COPIAS REMOTAS POR FTP

Como vimos al principio en el esquema, tenemos un NAS remoto, el cual hacemos también copias de seguridad, ya que en un entorno real es importante tener copias en otra localización geográfica.



Estas copias, se hacen directamente del NAS que tenemos en el educem a un NAS que tenemos en casa de un componente del grupo, las copias se hacen por FTP. Debido al software que tenemos en el NAS remoto, que es un software antiguo, no podemos enviar archivos por sFTP o algún otro medio que tenga cifrado, para solucionar esto, hemos cifrado la copia manualmente en el origen.

Hemos seleccionado que haga la copia de la carpeta WindowsBackUp:

**Paso 1: seleccione el origen de la copia de seguridad**

Especifique el contenido de la copia de seguridad. La ruta de la que desea realizar la copia de seguridad puede ser compartida de este dispositivo (un disco USB conectado a este dispositivo aparecerá como recurso compartido) o una ubicación remota. El origen y destino de la copia de seguridad no pueden ser ambos recursos compartidos re

Recurso compartido: backup ▼

Host:

Ruta:

Inicio de sesión:  Contraseña:

Luego hemos configurado el servidor de destino:

**Paso 2: seleccione el destino de la copia de seguridad**

Especifique dónde desea guardar los datos de la copia de seguridad. Como el origen de la copia de seguridad, la ruta puede ser un recurso compartido en este dispositivo o una ruta de un PC o dispositivo remoto.

Remoto: sitio FTP ▼ Host: 85.48.53.\*\*\*  
Ruta: /home/backup/veeamWindows Browse  
Inicio de sesión: backupUsr Contraseña: .....  
Prueba de conexión

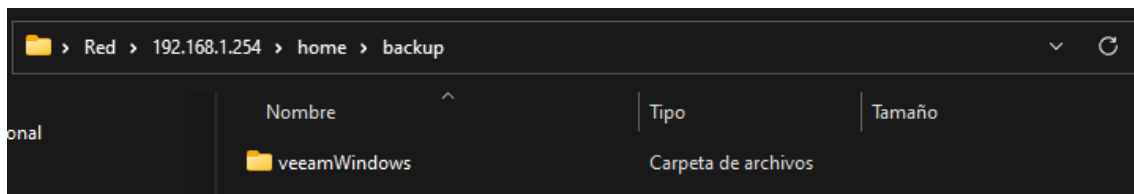
Luego hemos seleccionado que haga la copia los domingos a las 10 am:

**Paso 3: seleccione la programación de la copia de seguridad**

Seleccione cuándo desea realizar la copia de seguridad.

☒ Realice una copia de seguridad cada 24 ▼ horas entre 10:05 ▼ y 20:05 ▼  
☒ Dom ☐ Lun ☐ Mar ☐ Mié ☐ Jue ☐ Vie ☐ Sáb Selecionar todos los días

Finalmente el domingo a las 10 am copio los datos correctamente al servidor remoto.



## MYSQL DUMP

En el servidor web, para hacer copias de seguridad, hemos decidido usar MySQL Dump, que nos permitirá copiar las bases de datos, que es donde tenemos la información más importante de nuestra web.

Como tenemos el servidor web conectado por VPN al educem, podemos copiar la base de datos directamente al NAS, por NFS.

Aquí está el script que hemos usado para copiar la base de datos:

```
#!/bin/sh
FILE=minime.sql.`date +%Y%m%d`
DBSERVER=127.0.0.1
DATABASE="webapp"
USER="backup"
PASS="Backup12354.!"

unalias rm      2> /dev/null
rm ${FILE}      2> /dev/null
rm ${FILE}.gz   2> /dev/null

mysqldump --opt --user=${USER} --password=${PASS} ${DATABASE} >
${FILE}

gzip $FILE

echo "${FILE}.gz se creo correctamente:"
ls -l ${FILE}.gz
```

Vemos que se ejecuta correctamente y genera un archivo.sql comprimido:

```
josep@localhost:~$ sudo ./scripts/backupDB.sh
mysqldump: [Warning] Using a password on the command line interface can be insecure.
minime.sql.20220523.gz se creo correctamente:
-rw-r--r-- 1 root root 4094 May 23 13:40 minime.sql.20220523.gz
josep@localhost:~$
```

```
josep@localhost:~$ cat minime.sql.20220523
-- MySQL dump 10.13 Distrib 8.0.28, for Linux (x86_64)
--
-- Host: localhost    Database: webapp
--
-- Server version      8.0.28-0ubuntu0.20.04.3

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

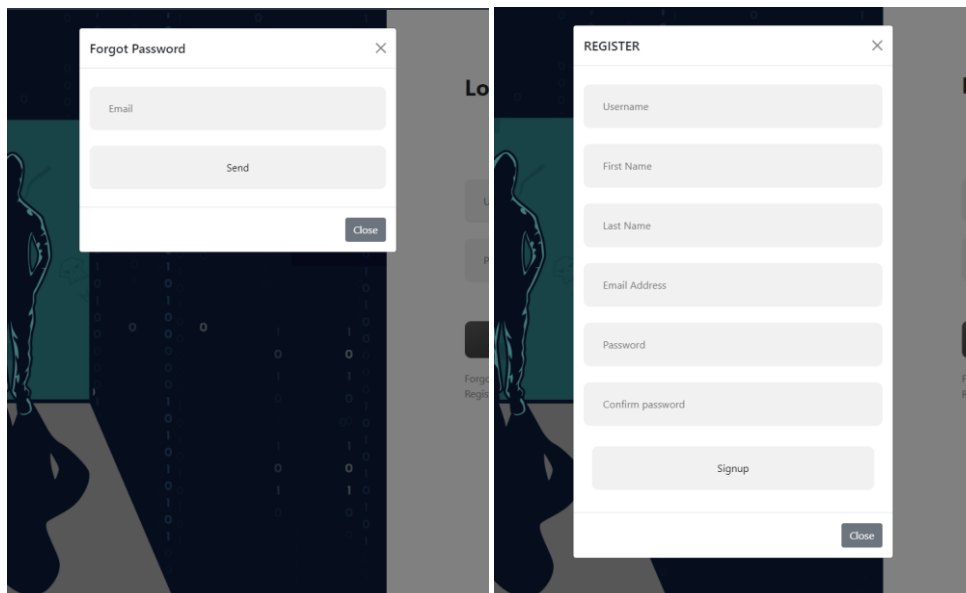
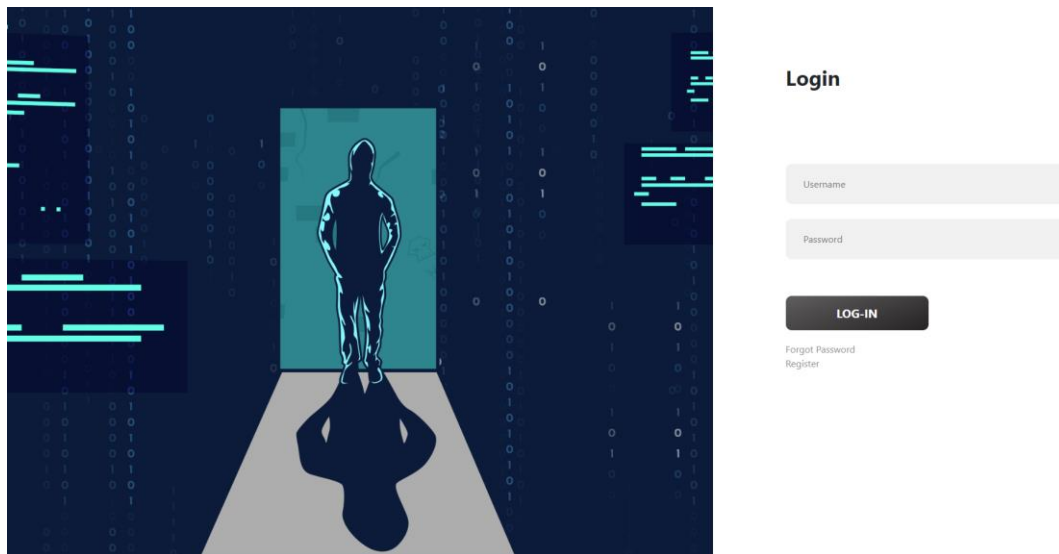
--
-- Table structure for table `categoria`
--
DROP TABLE IF EXISTS `categoria`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `categoria` (
  `nom` varchar(50) NOT NULL,
  `descripcio` varchar(150) NOT NULL,
  PRIMARY KEY (`nom`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;
```

## APLICACIÓN WEB

Una vez instalado y configurado el hardware y software adecuado, podemos llevar a cabo nuestra aplicación web. Como hemos explicado previamente, vamos a crear una plataforma educativa de Cyberseguridad y Hardening, donde tendremos disponibles máquinas con sistemas vulnerables, a parte también tendremos retos CTF.

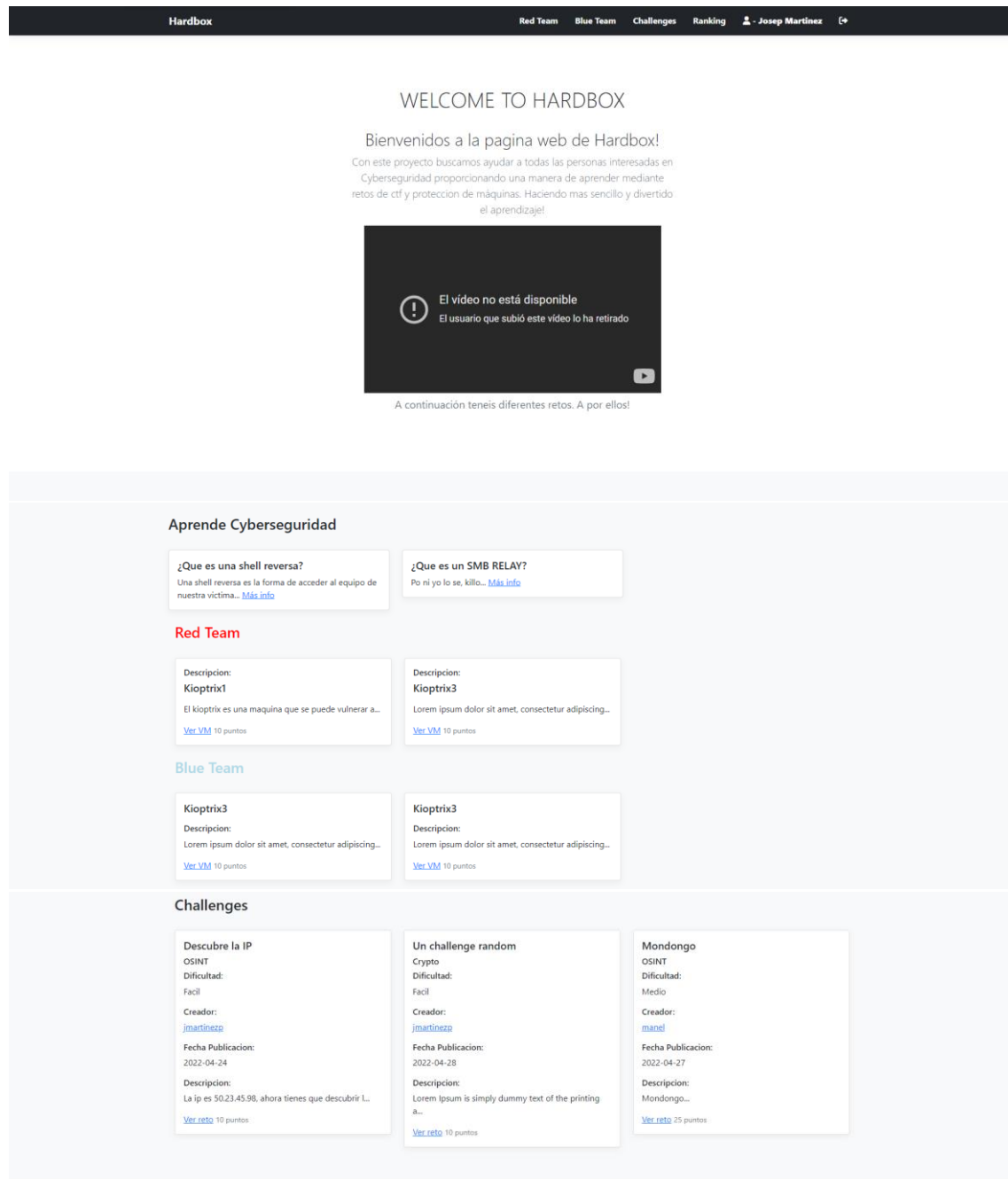
## DISEÑO

La página de login esta hecha de la siguiente manera, veremos una imagen en un lado y el login en el otro, a parte tambien tendremos el formulario de registro y de cambio de contraseña, esta pagina al entrar, tiene unas pequeñas animaciones hechas con javascript:



El diseño de nuestra pagina, es un diseño minimalista en blanco y negro, tenemos una barra de navegación en la parte superior, donde podemos movernos entre paginas, con los iconos de perfil y de cerrar sesión.

Seguidamente tenemos el temario y si continuamos bajando están las máquinas y los retos CTF disponibles.



La página de las máquinas o de los retos tienen el mismo estilo y es donde sale toda la información de la máquina o del reto en cuestión.

Hardbox

Red TeamBlue TeamChallengesRankingJosep Martinez

Descubre la IP

La ip es 50.23.45.98, ahora tienes que descubrir la ip, con la info que te he dado.

Creador: jmartinezp

Fecha de creación: 2022-04-24 09:08:04

Categoría: OSINT

Dificultad: Fácil

Puntuacion maxima: 10

Archivos adjuntos: No

Flag:  Enviar

Hardbox ga © 2022

Finalmente tenemos la página del perfil, donde tenemos nuestra información, los retos que hemos creado, también podemos descargar el fichero de VPN y cambiar de contraseña.

Hardbox

Red TeamBlue TeamChallengesRankingVPNJosep Martinez

Josep Martinez

Nombre de usuario: jmartinezp

Nombre: Josep

Apellidos: Martinez

Miembro desde: 2022-04-24

Correo electronico: Jo\*\*\*\*\*@gmail.com

Contraseña: \*\*\*\*\*

Reset PasswordDownload VPN file

Your Challenges:

Descubre la IP

OSINT

Dificultad: Fácil

Creador: jmartinezp

Fecha Publicacion: 2022-04-24 09:08:04

Description

Un challenge random

Crypto

Dificultad: Fácil

Creador: jmartinezp

Fecha Publicacion: 2022-04-28 09:55:12

Description

fichero test

Forensics

Dificultad: Fácil

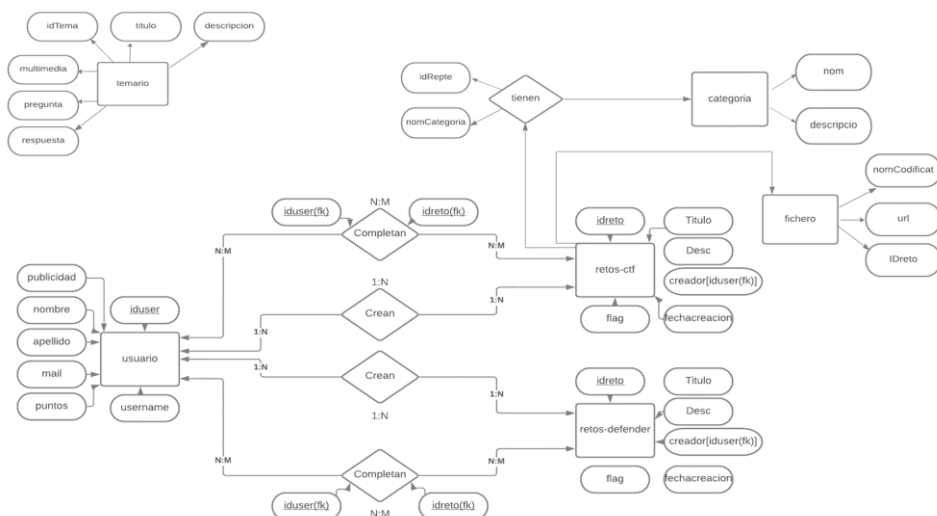
Creador: jmartinezp

Fecha Publicacion: 2022-05-10 14:42:01

Description

22

## DIAGRAMA RELACIONAL



Reto		
ID	Int NOT NULL AI	PK
creador	varchar(50) NOT NULL	FK
nombreReto	varchar(100) NOT NULL	
descripcion	text NOT NULL	
puntuacion	tinyint unsigned NOT NULL	
flag	varchar(50) NOT NULL	
fechaPub	datetime NOT NULL	

Categoria		
nombre	varchar(50) NOT NULL	PK
Descripcion	varchar(150) NOT NULL	

Fichero		
nomCodificat	varchar(100) NOT NULL	PK
url	varchar(100) NOT NULL	
IDrepte	int NOT NULL	FK

Categoria-Reto		
idReto	int NOT NULL	PK FK
nomCateg	varchar(50) NOT NULL	PK FK

Puntuaciones		
IDuser	int NOT NULL AI	PK FK
IDrepte	int NOT NULL	PK FK
intentosFallidos	tinyint unsigned	
puntuacionObtenida	tinyint unsigned	

Usuarios		
idUser	int NOT NULL AI	PK
mail	varchar(50) unique	
username	varchar(16) unique	
passHash	varchar(60)	
userFirstName	varchar(60)	
userLastName	varchar(120)	
creationDate	Datetime	
removeDate	Datetime	
lastSignIn	Datetime	
active	tinyint(1)	
activationDate	datetime	
activationCode	char(64)	
resetPassExpiry	datetime	
resetPassCode	char(64)	

Maquinas		
idMaquina	int NOT NULL	PK
nomMaquina	varchar(50) NOT NULL	
descripcion	text NOT NULL	
puntuacion	tinyint unsigned	
active	tinyint(1)	
ip	varchar(15)	
tipo	varchar(10)	

Temario		
idTema	int NOT NULL AI	PK
titulo	varchar(100) NOT NULL	
descripcion	text NOT NULL	
pregunta	varchar(200)	
respuesta	varchar(100)	



## DOMINIO

Para tener nuestra página accesible por cualquier persona, hemos tenido que contratar un dominio público, este paso lo hemos hecho en **freenom** que es una página donde puedes obtener dominios, entre otros, \*.tk y \*.ga de forma gratuita.

Nosotros hemos obtenido el dominio [hardbox.ga](https://hardbox.ga) y aquí alojaremos nuestros servicios abiertos al público, como la página web y nuestro servicio de envío de correos.

A continuación lo explicamos más detalladamente, pero hemos cambiado los servidores DNS de nuestro dominio, que eran los servidores de Freenom, por los servidores DNS de Cloudflare, que nos ofrecerán otros servicios para nuestro dominio.

## CLOUDFLARE


Cloudflare tiene un papel muy importante en nuestro proyecto, ya que se encarga de gestionar el acceso de nuestros clientes a nuestra página web y de los buzones de correo electrónico.

### DNS

Como estábamos diciendo anteriormente, hemos usado los DNS de Cloudflare para nuestro dominio, de momento hemos configurado 3 registros, dos de ellos son para el servicio web y están protegidos por el proxy, el otro es simplemente para poner nombre a la VPN y apunta a la IP pública del Educem.

Tipo	Nombre	Contenido	Estado de proxy	TTL	Acciones
CNAME	www	hardbox.ga	 Redirigido por proxy	Automático	<a href="#">Editar</a> ▶
A	vpn	185.107.106.57	 Solo DNS	Automático	<a href="#">Editar</a> ▶
A	hardbox.ga	212.227.168.123	 Redirigido por proxy	Automático	<a href="#">Editar</a> ▶

También hemos configurado los registros del servicio de correo, donde tenemos el SPF, y el DMARC, a parte del servidor SMTP:

A	smtp	198.251.65.219	 Solo DNS	Automático	<a href="#">Editar</a> ▶
TXT	_dmarc	v=DMARC1; p=quarantine; rua...	Solo DNS	Automático	<a href="#">Editar</a> ▶
TXT	_dmarc.smtp	v=DMARC1; p=quarantine; rua...	Solo DNS	Automático	<a href="#">Editar</a> ▶
TXT	hardbox.ga	v=spf1 include:_spf.mx.cloudflare...	Solo DNS	Automático	<a href="#">Editar</a> ▶
TXT	smtp	v=spf1 include:_spf.mx.cloudflare...	Solo DNS	Automático	<a href="#">Editar</a> ▶

Y para el reenviador de correos hemos indicado los servidores de correo:

MX	hardbox.ga	route3.mx.cloudflare.net	<b>95</b> Solo DNS	Automático	<a href="#">Editar</a> ▶
MX	hardbox.ga	route2.mx.cloudflare.net	<b>14</b> Solo DNS	Automático	<a href="#">Editar</a> ▶
MX	hardbox.ga	route1.mx.cloudflare.net	<b>57</b> Solo DNS	Automático	<a href="#">Editar</a> ▶

## WAF

Hemos configurado el WAF que nos ofrece cloudflare, este servicio es un firewall inverso para nuestra pagina web, el cual lo hemos configurado de momento para que solo admita conexiones de España, de esta forma evitamos la mayoría de bots que escanean nuestra página, esto lo podemos ver en las estadísticas que también nos ofrece.

Tan solo 8h despues de activar el firewall, ya vemos que hay muchas peticiones de otros paises bloqueadas, esto nos indica que este servicio esta haciendo bien su función.

Eventos de firewall					<a href="#">+ Crear una regla de firewall</a> <a href="#">Descargar datos</a>
<a href="#">+ Agregar filtro</a>					24 horas anteriores
Registro de actividades					<a href="#">Editar columnas</a>
Fecha	Acción realizada	País	Dirección IP	Servicio	
> 17 abr., 2022 10:25:44	Bloquear	China	42.193.23.161	Reglas de firewall	
> 16 abr., 2022 11:59:58	Bloquear	Russian Federation	89.175.184.250	Reglas de firewall	
> 16 abr., 2022 12:00:06	Bloquear	Singapore	151.106.120.184	Reglas de firewall	
> 16 abr., 2022 11:32:37	Bloquear	United States	52.55.244.91	Reglas de firewall	
> 16 abr., 2022 15:22:40	Bloquear	United Kingdom	51.254.49.98	Reglas de firewall	
> 16 abr., 2022 13:28:35	Bloquear	France	51.255.62.8	Reglas de firewall	

## MAILING

Para el registro de nuestra página, los usuarios deben activar sus cuentas a traves del correo electrónico y para esto necesitamos un dominio y un servidor de envio de correos (Postfix), el cual ya lo hemos configurado previamente.

Para el envio de correos hemos utilizado PHPMailer y enviamos los correos des de:

[accounts\\_no-reply@hardbox.ga](mailto:accounts_no-reply@hardbox.ga)

Como ya hemos visto en la configuración del servicio de correo, los correos se encriptan con un certificado TLS y al haber configurado en nuestro DNS el registro SPF y DMARC, los correos llegan de forma correcta a la bandeja de entrada.

### Mensaje original

ID de mensaje	<pB8pKSx7hke3wOGDj4y9LIMxKIGhCWINYXVA3A1ao@www.hardbox.ga>
Creado a las:	24 de abril de 2022, 10:56 (entregado en 3 segundos)
De:	HARDBOX <accounts_no-reply@hardbox.ga> Con PHPMailer 6.5.3 ( <a href="https://github.com/PHPMailer/PHPMailer">https://github.com/PHPMailer/PHPMailer</a> )
Para:	HARDBOX <Josepmp02@gmail.com>
Asunto:	Activacion cuenta Eduhacks
SPF:	PASS con la IP 198.251.65.219 <a href="#">Más información</a>
DMARC:	'PASS' <a href="#">Más información</a>

## SPF

El registro SPF sirve para que los correos de nuestro dominio solo puedan ser enviados desde los servidores que nosotros elijamos. De esta forma, si nuestro servidor de correo está bien configurado, los correos falsos que se envíen en nuestro nombre no llegarán a la bandeja de entrada. Este registro se configura en el servidor DNS de nuestro dominio.

Nosotros para configurar el SPF, hemos ido al servidor DNS de nuestro dominio y hemos indicado el siguiente registro TXT vinculado a todo el dominio:

**“v=spf1 include:\_spf.mx.cloudflare.net ip4:198.251.65.219 ~all”**

TXT	hardbox.ga	v=spf1 include:_spf.mx.cloudfla...	Solo DNS	Automático	Editar▼
Tipo	Nombre (obligatorio)		TTL		
<b>TXT</b>	<input type="text" value="hardbox.ga"/>	<input type="button" value="Automá..."/>			
Utilice @ para la raíz					
Contenido (obligatorio)					
<input type="text" value="v=spf1 include:_spf.mx.cloudflare.net ip4:198.251.65.219 ~all"/>					

## DMARC

El DMARC, es un registro DNS, que sirve para definir lo que queremos hacer con los correos fraudulentos de nuestro dominio. En nuestro caso le hemos definido “quarantine” que quiere decir que si hay un problema lleve el correo al SPAM.

Nuestro registro DNS es el siguiente:

**“v=DMARC1; p=quarantine; rua=<mailto:oriel-listens-0v@icloud.com>”**

TXT	_dmarc	v=DMARC1; p=quarantine; rua...	Solo DNS	Automático	Editar▼
Tipo	Nombre (obligatorio)		TTL		
<b>TXT</b>	<input type="text" value="_dmarc"/>	<input type="button" value="Automá..."/>			
Utilice @ para la raíz					
Contenido (obligatorio)					
<input type="text" value="v=DMARC1; p=quarantine; rua=mailto:oriel-listens-0v@icloud.com"/>					

Con este registro también nos envían informes de como está funcionando. Estos informes se envían a la dirección que hemos puesto, en nuestro caso hemos puesto una dirección que nos reenvía el correo a nuestro correo de verdad.

## MAIL FORWARDING

Hasta ahora hemos visto que podemos enviar correos, pero de momento no podemos recibirlos, así que hemos configurado otro servicio que nos ofrece Cloudflare, para poder reenviar nuestros correos del dominio a una bandeja de correo real.

### Enrutamiento de correos electrónicos Beta





Cree direcciones de correo electrónico personalizadas para su dominio y redirija los mensajes entrantes a su buzón de correo preferido.

#### Direcciones personalizadas

Cree direcciones de correo electrónico personalizadas y defina la acción que se realizará con los correos electrónicos recibidos.

Crear dirección

Dirección personalizada creada.

Dirección personalizada	Acción	Estado	
info@hardbox.ga	Enviar a <b>josep.martinezp@educem.net</b>	 Activo	<a href="#">Editar</a> ▶
support@hardbox.ga	Enviar a <b>josep.martinezp@educem.net</b>	 Activo	<a href="#">Editar</a> ▶
manel@hardbox.ga	Enviar a <b>manel.mayoralc@educem.net</b>	ⓘ Verificación pendiente	<a href="#">Editar</a> ▶
ahnuar@hardbox.ga	Enviar a <b>ahnuarramirez@gmail.com</b>	ⓘ Verificación pendiente	<a href="#">Editar</a> ▶
maya@hardbox.ga	Enviar a <b>marti.reyesg@educem.net</b>	ⓘ Verificación pendiente	<a href="#">Editar</a> ▶
josep@hardbox.ga	Enviar a <b>josep.martinezp@educem.net</b>	 Activo	<a href="#">Editar</a> ▶
admin@hardbox.ga	Enviar a <b>josep.martinezp@educem.net</b>	 Activo	<a href="#">Editar</a> ▶

De esta forma ya podemos enviar y recibir los correos de nuestro dominio.

## CONTENIDO

En nuestra web, tenemos diferente contenido para comenzar, tenemos temarios, donde podrán consultar los clientes para aprender los conceptos básicos de las máquinas, tenemos máquinas de defensa y de ataque y por último tenemos retos CTF que pueden ser creados por los usuarios de la web.

## TEMARIO

Tema
Permisos - Ficheros Sudoers y Shadow
Automatizacion de tareas - Cron Tab
Firewall – IPTables

## MAQUINAS

Las máquinas de defensa están vinculadas a los temarios, de esta forma el usuario final se puede informar antes de resolver la máquina.

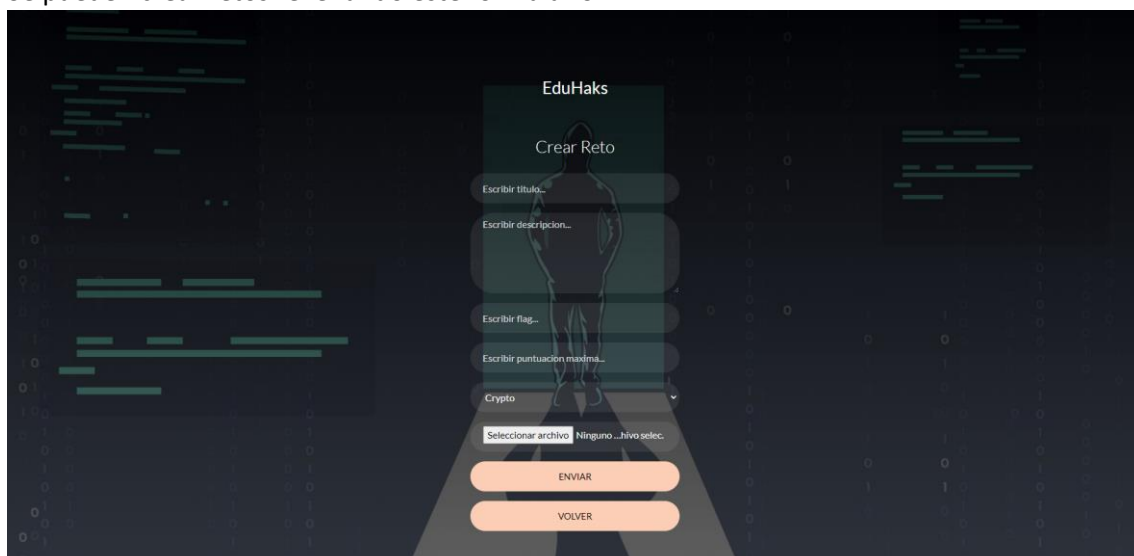
Maquinas de defensa
Fallo en los permisos
Demasiadas tareas automatizadas
Firewall incompleto

Maquinas Ataque
ASIX
Mr. Robot

## RETOS

Los retos los puede crear la comunidad de HardBox, así que cada día habrá más retos de diferentes temáticas.

Se pueden crear retos rellenando este formulario:



## GATEWAY CLIENTES

Para que los clientes puedan acceder a nuestras máquinas, se tienen que conectar por VPN, para ello tenemos una máquina virtual en red interna con las máquinas vulnerables para que los clientes puedan conectarse y acceder a los sistemas vulnerables.

Máquinas virtuales							
Nombre	Acción en c...	Uso de CPU	Memoria asignada	Tiempo activo	Estado	Versión de c...	Mantenimient...
ASIX	ejecutando	0 %	512 MB	2:19:07:50		9.0	No aplicable
MRRBOT	ejecutando	0 %	512 MB	1:23:51:07		9.0	No aplicable
Ubuntu	ejecutando	0 %	1024 MB	13:09:17:34		9.0	No aplicable

Esta máquina es la que se encarga de la conexión de los clientes, como vemos tiene las 2 interfaces de red.

Ubuntu			
Adaptador	Conexión	Direcciones IP	Estado
Adaptador de red (MAC dinámica: 00:15:5...	adaptador puente		Aceptar
Adaptador de red (MAC estática: 00:15:5...	RED INTERNA		Aceptar

Si hacemos un “ip a” podemos ver que hay 4 ip distintas:

```
joseph@dhcp:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:03:09 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.30/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 6747sec preferred_lft 6747sec
    inet6 fe80::215:5dff:fe01:309/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:03:0a brd ff:ff:ff:ff:ff:ff
    inet 10.0.255.1/24 brd 10.0.255.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe01:30a/64 scope link
        valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1/24 brd 10.8.0.255 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::5bab:a4d9:ffb8:a316/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
joseph@dhcp:~$ _
```

**lo:** es la dirección de localhost.

**Eth0:** es la interfaz donde tenemos acceso a internet.

**Eth1:** es la red interna la cual tenemos conexión con las máquinas vulnerables.

**Tun0:** es la red donde se conectarán los clientes de la VPN.

## DHCP

Esta máquina, al estar en red interna, hará de servidor DHCP para las máquinas vulnerables para que tengan una IP para que se conecten los clientes. Hemos configurado el rango 10.0.255.0/24.

```
GNU nano 4.8 /etc/dhcp/dhcpd.conf
subnet 10.0.255.0 netmask 255.255.255.0 {
    range 10.0.255.10 10.0.255.254;
    option routers 192.168.1.1;
    option domain-name-servers 1.1.1.1;
}
```

## SCRIPTS

### ACTUALIZAR LAS MAQUINAS DE LA WEB

```
function getID {
    param (
        $nombre
    )
    $nombre = $nombre.ToString()
    $id = ''
    if($nombre -like "*MRROBOT*"){
        $id = 1
    }elseif($nombre -like "*ASIX*"){
        $id = 2
    }elseif($nombre -like "*maquinaY*"){
        $id = 3
    }elseif($nombre -like "*maquinaZ*"){
        $id = 4
    }elseif($nombre -like "*maquinaH*"){
        $id = 5
    }elseif($nombre -like "*maquinaA*"){
        $id = 6
    }elseif($nombre -like "*maquinaN*"){
        $id = 7
    }else{$id = -1}
    return $id
}

$maquina = Get-VM | Where-Object {$_.State -eq 'Running'}
$VM1 = '' $VM2 = '' $VM3 = '' $VM4 = '' $maquinaFormat = ''

for($i = 0; $i -lt $maquina.length; $i++){
    if($maquina[$i] -notlike "*Ubuntu*"){
        $maquinaFormat = ($maquina[$i] | select Name | Format-Table -
HideTableHeaders | Out-String).Replace("`n","")
        if($i -eq 0){ $VM1 = getID($maquinaFormat) }
        if($i -eq 1){ $VM2 = getID($maquinaFormat) }
        if($i -eq 2){ $VM3 = getID($maquinaFormat) }
        if($i -eq 3){ $VM4 = getID($maquinaFormat) }
    }
}

$url =
"https://hardbox.ga/php/updateMachines.php?nombre1=$VM1&nombre2=$VM2&nombre3=$V
M3&nombre4=$VM4&code=Change-Makina12354"
$url = $url.ToString()
#Guardar LOG en un fichero
$fecha = Get-Date -UFormat "%m/%d/%Y %R"
echo $fecha " | URL --> " $url.Replace("`n","") "-----`n" | Out-File -FilePath
"D:\log\updateWeb_log.txt" -Append
#Actualizar la web con esta peticion
Invoke-WebRequest -URI $url
```

## BACKUPS DE LA BASE DE DATOS

```
#!/bin/sh

FILE=minime.sql.`date +%Y%m%d`
DBSERVER=127.0.0.1
DATABASE="webapp"
USER="backup"
PASS="Backup12354.!"

unalias rm      2> /dev/null
rm ${FILE}      2> /dev/null
rm ${FILE}.gz   2> /dev/null

mysqldump --opt --user=${USER} --password=${PASS} ${DATABASE} > ${FILE}

gzip $FILE

echo "${FILE}.gz Se creo correctamente:"
ls -l ${FILE}.gz
```



## SOCKETS

### ENVIO DE DATOS

Este script lo hemos utilizado en el servidor web para enviar la orden de crear un usuario VPN al servidor VPN:

```
#!/bin/bash

if [[ $1 == 'vpn' ]]
then
    echo 'newvpn,$2 > /dev/tcp/192.168.1.30/3030'
elif [[ $1 == '--help' ]]
then
    echo "./sendReq.sh [tipo] [dato]"
    echo "Ejemplo:"
    echo "./sendReq.sh newvpn usuarioVPN"
fi
```

### RECIBO DE DATOS

Y este es el script del servidor VPN que hemos usado para recibir y tramitar la orden del servidor web.

```
#!/bin/bash

log () {
    echo $1 >> requests_log.txt
}

vpnUser () {
    /home/ahnuar/createuser.sh $1
}

while [ True ]
do
    req=$(nc -nvlp 3030)

    reqType=$(echo $req | cut -d "," -f 1)
    reqData=$(echo $req | cut -d "," -f 2)

    log $req

    if [[ $reqType == 'newvpn' ]]
    then
        vpnUser $reqData
    fi
done
```

## IPTABLES:

### REDIRECCIONAR PAQUETES A LA RED INTERNA

Con estas reglas de firewall hemos usado este ubuntu como router, así las máquinas virtuales en red interna pueden conectarse a internet.

```
#!/bin/bash
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

iptables -A FORWARD -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
iptables -nL
iptables -nL -t nat
```

### BLOQUEAR CONEXIONES VPN A SERVIDORES

Con este script, bloqueamos las conexiones de los clientes web hacia nuestros servidores, para que solo se puedan conectar a las máquinas de la red interna.

```
#!/bin/bash
#Admitir trafico de TUN (vpn) a ETH1 (Red Interna)
iptables -A FORWARD -i eth1 -o tun0 -j ACCEPT -m comment --comment "VPN FORWARD Allow ETH1 --> TUN0"
iptables -A FORWARD -i tun0 -o eth1 -j ACCEPT -m comment --comment "VPN FORWARD Allow TUN0 --> ETH1"
#Bloquear trafico de TUN (vpn) a ETH0 (Red de los servers)
iptables -A FORWARD -i tun0 -o eth0 -d 192.168.1.2 -j DROP -m comment --comment "Deny vpn to server 192.168.1.2"
iptables -A FORWARD -i tun0 -o eth0 -d 192.168.1.3 -j DROP -m comment --comment "Deny vpn to server 192.168.1.3"
iptables -A FORWARD -i tun0 -o eth0 -d 192.168.1.10 -j DROP -m comment --comment "Deny vpn to server 192.168.1.10"
#Mas reglas pa que funcione el forward de la VPN a la red interna
iptables -A FORWARD -i eth1 -o tun0 -m state --state RELATED,ESTABLISHED -j ACCEPT -m comment --comment "vpn lan"
iptables -A FORWARD -i tun0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT -m comment --comment "vpn lan"

iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE -m comment --comment "vpn lan"
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE -m comment --comment "vpn lan"

iptables -nL
iptables -nL -t nat
```

## ADMITIR EL ACCESO WEB SOLO POR CLOUDFLARE

Con este script, hemos restringido el acceso web a todas las ip que no sean de cloudflare, haciendo que los clientes de la web tengan que entrar por nuestro dominio.

```
#!/bin/bash

iptables -F

cloudflare=$(cat /home/josep/firewall/rangosIPcloudflare.txt)

for rangeIP in $cloudflare; do
    iptables -A INPUT -p tcp -s $rangeIP -m multiport --dports 80,443 -j
    ACCEPT
done

iptables -A INPUT -p tcp -m multiport --dports 80,443 -j DROP
```

Rangos IP de cloudflare:

```
173.245.48.0/20
103.21.244.0/22
103.22.200.0/22
103.31.4.0/22
141.101.64.0/18
108.162.192.0/18
190.93.240.0/20
188.114.96.0/20
197.234.240.0/22
198.41.128.0/17
162.158.0.0/15
104.16.0.0/13
104.24.0.0/14
172.64.0.0/13
131.0.72.0/22
```

## INFORMACION DE DISPOSITIVOS Y USUARIOS

RED EDUCEM	Tipo	IP Externa	IP Interna	MAC	Usuario	Contraseña	Nombre dominio	Observaciones
<b>FIREWALL</b>	Fisico	10.0.11.201	192.168.1.1	08:5B:0E:3D:5C:8C	admin	gongongon	firewall.hardbox.hbx	Direccion de acceso: <a href="https://10.0.11.201">https://10.0.11.201</a> Puerto 1197
<b>Server Maquinas</b>	Fisico	-	192.168.1.3	ec:b1:d7:49:01:dc	nombre	JMA!123	vms.hardbox.hbx	Servidor de maquinas
<b>Server Maquinas 2</b>	Fisico	-	192.168.1.2	18:a9:05:2d:ae:68	nombre	JMA!123	vms2.hardbox.hbx	Servidor web
<b>NAS</b>	Fisico	-	192.168.1.10	00:22:3f:a9:a5:df	admin	netgear1	storage.hardbox.hbx	Servidor de archivos y copias de seguridad

INTERNET	Tipo	IP Externa	Nombre dominio		Usuario	Contraseña		Observaciones
<b>SERVER SMTP</b>	VPS	198.251.65.219	<a href="mailto:smtp.hardbox.ga">smtp.hardbox.ga</a>		-	-		Servidor de correo VPS
<b>ServerWeb</b>	VPS	212.227.168.123	<a href="http://www.hardbox.ga">www.hardbox.ga</a>		-	-		Server web
<b>NAS Remoto</b>	Fisico	Dinamica			-	-		NAS Remoto de back Up

VPN USERS	User	Password		VEEAM ENCRYPT	password
Josep	jmartinez	Josep!123		Webserver	Backup!123WEB

Marti	mreyes	Marti!123
Ahnuar	aramirez	Ahnuar!123
Manel	mmayoral	Manel!123
web server	webserver	WebServer!123

NAS NETGEAR	User	Password
	admin	netgear1
	backupSMB	Backup!123

NAS REMOTO	User	Password
	admin	-
	backup	Backup12354..

Maquinas server	Backup!123Mak
-----------------	---------------

VPS Web User	webeditor	GuebSurmano!123
--------------	-----------	-----------------

<u>MySQL Web Srv</u>	User	Password
root	root	mYsql!123
user de php	php	!phpW3bPass

Correos Electronicos	Correo dominio	Correo Forward
Info	info@hardbox.ga	josep.martinezp@educem.net
Support	support@hardbox.ga	josep.martinezp@educem.net
Manel	manel@hardbox.ga	manel.mayoralc@educem.net
Ahnuar	ahnuar@hardbox.ga	ahnuarramirez@gmail.com
Maya	maya@hardbox.ga	marti.reyesg@educem.net
Josep	josep@hardbox.ga	josep.martinezp@educem.net
Admin	admin@hardbox.ga	josep.martinezp@educem.net

## MEMORIA

Aquí deberemos explicar que estamos haciendo, qué problemas hemos tenido y cómo los hemos solucionado. Nos servirá, tanto para nosotros tener controlado el proyecto como para redactar la memoria final y que nos sume puntos que siempre son necesarios.

### NUESTROS INICIOS:

Empezamos ideando el proyecto con un brainstorming entre los cuatro integrantes del grupo. Al principio surgieron varias ideas, como un control de flotas de diferentes tipos de vehículos hasta una empresa que vendería USB para auditorías. Finalmente, nos decantamos por realizar este proyecto, ya que ayudaría a muchos alumnos aprender técnicas de hardening.

### MONTANDO EL FIREWALL:

Gracias a que Josep y Manel vieron utilizar un Fortinet en sus empresas de prácticas. Se decidió seleccionar el firewall Fortigate. Al principio se descubrió cómo configurar la VPN rápidamente gracias a que era muy intuitivo y fácil de acceder y usar. Sin embargo, al tener un fallo en el disco duro, no se podía formatear y debido a que algunas configuraciones eran del grupo del año anterior, no pudimos seguir usándolo.

En su defecto decidimos montar un servidor que contuviera un PFSense.

### MONTANDO EL SERVIDOR:

Una vez montado el firewall y configuradas las reglas NAT para tener internet en nuestra red local, comenzamos instalando un proxmox en el servidor grande, un servidor muy potente que nos había proporcionado el centro, el servidor tenía doble CPU, 16GB de ram. Pero comenzamos a tener algunos problemillas con el sistema. Cuando conseguimos ponerlo en marcha vimos que el servidor se reiniciaba solo, resulta que había un problema de alimentación. Entonces tuvimos que cambiar de servidor usando 2 ordenadores de sobremesa, uno de ellos para la web y otro para las máquinas virtuales.

Más adelante, debido a que era muy complicado virtualizar las máquinas con el Ubuntu, instalamos un Windows Server para evitar los problemas de compatibilidad que surgían en linux.

### CONFIGURANDO EL SERVIDOR WEB:

Para tener nuestro servicio web activo lo que hicimos fue instalar el apache detrás de un docker para que esté aislado del sistema. Además, hemos configurado un proxy inverso para filtrar las conexiones según el dominio que solicita el usuario.

Pero pensando mejor la idea del proyecto, vimos que sería mejor que la web fuese pública a internet y no estuviese detrás de una VPN, así que al final hemos alojado nuestra web en un servidor VPS como hemos visto, con un dominio real.

## CONFIGURANDO EL SERVIDOR DE MÁQUINAS VIRTUALES:

Hemos instalado un Windows Server 2019, que funciona con Hyper V para virtualizar las máquinas. Primero instalamos el Windows y agregamos un rol y característica de Hyper V.

Teníamos 3 discos duros un SSD y 2 HDD de 300 GB y pensamos en unir los HDD de la administración de discos para que sea una unidad única de 600 GB y que sea fácil su gestión. Esta unidad servirá únicamente para guardar las máquinas virtuales y el SSD para el sistema operativo en general.

Una vez instalado reiniciamos el servidor y desde la herramienta administrativa de Hyper V fuimos creando máquinas virtuales.

## CREACIÓN DE MÁQUINAS VIRTUALES:

Primeramente, hemos cogido todas las máquinas virtuales que hemos vulnerado a lo largo del curso en M7 y las hemos pasado a la unidad antes comentada. Al ser ".ova" hemos tenido que adaptarlas a ".VHD" que es el formato que soporta Hyper V. Para ello lo primero que tuvimos que hacer es coger la ova y descomprimir su contenido, y con un programa externo llamado 2Tware convert VHD transformamos los archivos descomprimidos en VHD.

Con este archivo, en el administrador de Hyper V crear una nueva máquina y seleccionar un disco duro existente, es decir, el archivo VHD. Y así las fuimos generando todas.

## APARTADO WEB:

Más adelante, Maya encontró un bootstrap que se empezó a editar entre él y Manel.

Sin embargo, nos dimos cuenta de que usando la web del proyecto de PHP podía quedar bien, ya que eran webs de casi la misma temática, aunque tuvimos que modificar bastante código HTML, CSS... Y añadir más código PHP para las nuevas funcionalidades que tiene nuestro proyecto, como la resolución de máquinas vulnerables, la descarga del fichero VPN y más opciones.

## COMUNICACIÓN ENTRE MÁQUINAS

Llegado a este punto teníamos casi todo listo, pero faltaba juntarlo para que funcionara bien, teníamos, por un lado, en la red del educem un Windows server con máquinas virtuales y por otro un servidor VPN con la web. Necesitábamos que la web se comunicase con el servidor de máquinas, para publicar en la web las máquinas activas, etc.

Aquí estuvimos pensando como hacerlo y caímos en que podíamos conectar el servidor web por VPN a nuestra red local y de esta forma ya podríamos enviar información entre los diferentes sistemas. Para enviar dicha información hemos utilizado TCP sockets en pequeños scripts que hemos visto anteriormente en el trabajo.

## CONCLUSIONES

En este proyecto, hemos luchado contra varios retos que se nos han ido poniendo en nuestro camino, desde sistemas de virtualización incompatibles hasta la creación de scripts para automatizar los diferentes sistemas y la actualización de nuestra página web. También hemos pasado por fallos de hardware, que ya hemos explicado anteriormente en la memoria y debido a los fallos de hardware hemos tenido que optimizar las máquinas virtuales para que puedan trabajar bajo poca memoria RAM.

Creemos que hemos hecho un buen trabajo, teniendo en cuenta la faena y el tiempo invertido en la configuración y sincronización de todos los servicios que hemos utilizado, para que nuestra plataforma web pueda trabajar con máquinas virtuales, dando el servicio a los clientes.

También, hay que añadir, que en nuestro proyecto hemos estado motivados por el simple hecho de transmitir conocimientos a nuestros usuarios y que puedan aprender y probar técnicas de hacking y de hardening sobre un entorno controlado, ya que pensamos que la ciberseguridad va a ser fundamental en los próximos años en el mundo de la informática.

Finalmente, hemos aprendido mucho en este proyecto, debido a que cada fallo que cometíamos o cada error que había, eran unas horas de búsqueda de información sobre el error o sistemas similares. También queremos añadir, que las copias de seguridad, han sido nuestra salvación, porque hemos tenido fallos que de no tener configuradas las copias, tendríamos que haber estado mucho más tiempo volviendo a instalar programario.



## BIBLIOGRAFIA

Hemos obtenido información de los siguientes enlaces:

Virtualizacion de contenedores:

<https://www.digitalocean.com/customers/hack-the-box>

Portainer:

<https://docs.portainer.io/v/ce-2.9/start/install/server/docker/linux>

Traefik:

<https://www.cloudcenterandalucia.es/blog/traefik-proxy-inverso-y-balanceador-de-carga-parte1/#:~:text=Traefik%20es%20un%20proxy%20inverso,mediante%20Docker%20y%20docker%20compose%20>

Balanceo de carga:

<https://seguridadzero.com/balanceo-de-carga-swarm-y-docker-compose>

Dockers:

[https://linuxhint.com/setup\\_docker\\_machine\\_virtualbox/](https://linuxhint.com/setup_docker_machine_virtualbox/)

Veeam:

<https://www.veeam.com/linux-backup-free.html>

<https://community.hetzner.com/tutorials/getting-started-with-veeam/installing-the-veeam-agent-for-linux>

Doker backup:

<https://docs.docker.com/desktop/backup-and-restore/>

Estilos Web:

<https://getbootstrap.com/docs/4.0/components/modal/>

<https://themewagon.com/themes/free-bootstrap-one-page-template-download/>

<https://themewagon.com/themes/free-bootstrap-responsive-personal-portfolio-template-djoz/>

<https://bootsnipp.com/builder>

TCP sockets:

<https://learntutorials.net/es/powershell/topic/5125/comunicacion-tcp-con-powershell>

<https://www.jesusninoc.com/01/02/server-and-client-sockets-tcp/>

Backup MySQL:

<https://alvinalexander.com/mysql/mysql-database-backup-dump-shell-script-crontab/>

CODIGO FUENTE DE LA WEB: <https://github.com/JosepMP02/HardBox>

WEB: <https://hardbox.ga/>