UNIVERSIDAD POLITECNICA DE VALENCIA

DEPARTAMENTO DE COMUNICACIONES

Máster Universitario en Tecnologías, Sistemas y Redes de Comunicaciones

Diseño, Implementación y Validación de un Cyber Range

Autor: Víctor Javier Garrido Peñalver

Director: Manuel Esteve Domingo

Fecha de comienzo: Marzo 2017

Lugar de trabajo: Laboratorio de Sistemas de Tiempo Real Distribuidos

Objetivos – El objetivo del trabajo es llevar a cabo la implementación de un **Cyber Range**, cuyo propósito principal es el desarrollo y entrenamiento de las habilidades de profesionales, así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías, técnicas y tácticas en materia de ciberseguridad y ciberdefensa. Para ello se emplea un entorno real simulado que dispone de todos los servicios y servidores que formen parte de una organización, tales como servidores de correo, servicios web, administración de dominios, etc. Al ser un entorno virtual es posible experimentar y probar con nuevas herramientas y métodos de seguridad sin poner en peligro la integridad de los equipos de nuestra organización.

Metodología – En el desarrollo del Cyber Range se emplea principalmente la **virtualización**, que es el proceso de creación de una representación basada en software de cualquier recurso físico. En el Cyber Range se virtualizan, a través de la plataforma de virtualización VMware, todos los recursos de un equipo físico (almacenamiento, memoria, adaptadores, etc,). Mediante está técnica se simulan los servidores y herramientas de seguridad que emplea una empresa u organización para gestionar sus recursos y dar servicio a los clientes.

Desarrollos teóricos realizados – En materia de seguridad,se han investigado los diversos tipos de arquitecturas de red para organizaciones o empresas. Además se ha estudiado los principales ataques cibernéticos e intrusión a cualquier servicio de los que se han implementado, tales como phishing, ransomware, spoofing, etc. Así como de las distintas herramientas para la detección y prevención de estos ataques.

Desarrollo de prototipos y trabajo de laboratorio – Se desarrolla un Cyber Range sobre un servidor físico (host), en el que se han virtualizado en total, 11 máquinas virtuales, correspondientes a los servicios que posee una organización, así como algunas herramientas de seguridad para la monitorización y protección de estos recursos. Todo ello se ha implementado sobre una red que dispone de tres zonas (Externa, Interna y Desmilitarizada) delimitadas por un firewall que aplica reglas adaptadas a las características de cada zona.

Resultados – Al finalizar este trabajo se han cumplido los objetivos propuestos desde el principio. Se implementó y configuró el Cyber Range con todas los servidores propuestos, activos y cumpliendo sus funciones, con acceso a la red configurada y siguiendo las reglas establecidas por el firewall. Además también se han realizado algunos análisis para comprobar que la herramienta de monitorización OSSIM, reconoce todas las máquinas y es capaz de rastrear y analizar el tráfico que pasa por ella, así como los logs que mandan cada una de las máquinas virtuales donde se ha configurado un agente OSSEC.

Líneas futuras – El trabajo que se prevé realizar a partir del desarrollo de este Cyber Range es mejorar y dotarlo de una mayor seguridad, a través de herramientas software de seguridad, implementando nuevos sensores y directivas que permitan una mayor detección de amenazas. También se pretende incorporar elementos hardware como un firewall de última generación, que proporciona una mayor visibilidad y control de lo que ocurre en la red.

Abstract – This paper describe the implementation and development of a prototype of Cyber Range, it is based on a virtual system that simulates a real environment in which, simulates the technological architecture of any organization with their network infrastructure, servers and services. What is intended with the Cyber Range is provide a training camp for cybersecurity, where professional and not so professional can acquire and develop skills on Cybersecurity and Cyberdefence matter, as well as testing and experiment with new tools.

Autor: Víctor Javier Garrido Peñalver email: vicgarp2@teleco.upv.es
Director: Manuel Esteve Domingo, email:mesteve@dcom.upv.es
Fecha de entrega: 30-02-07

Índice

Índice de figuras

1. Introducción

En esta primera parte del trabajo se va a introducir algunos conceptos sobre Ciberseguridad y su situación actual en empresas. A continuación, se explicará que es un Cyber Range, en que consiste y cuales son sus características principales.

1.1. Ciberseguridad

El uso de Internet ha ido creciendo exponencialmente con la introducción de las nuevas tecnologías y se extiende cada vez más, siendo parte imprescindible en el día a día de cualquier persona. En la sociedad actual es importante estar conectado en cualquier sitio y a cualquier hora del día, ya sea para estar al tanto de las últimas noticias, conocer el tiempo o colgar fotos en redes sociales.

Como muestra de ello en la figura 1, se observan unos datos sobre el uso de internet y sus usuarios en España. En este estudio [1], realizado en Enero de 2017 por **We Are Social**, se aprecia que la tasa de penetración de Internet es del 82 %, un crecimiento de 2 millones de usuarios, lo que supone un 6 % más que el año anterior.

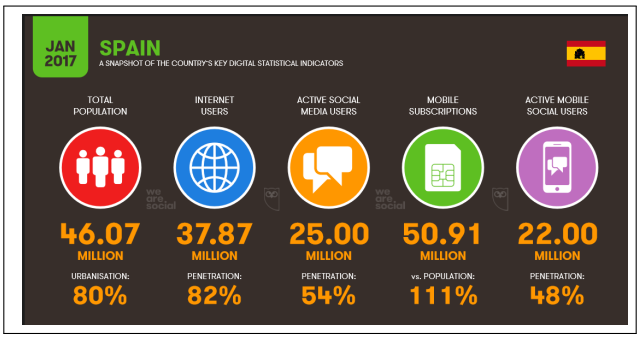

Figura 1: Estudio sobre el uso de Internet en España

Esto, ocurre a nivel global pero si se habla de organizaciones y empresas, se observa que Internet ha cambiado totalmente la imagen que se tenía de puesto de trabajo tradicional. Esto es debido a que el uso de la tecnología como apoyo a los procesos de negocio reduce los costes además de hacer más eficiente y eficaz la operación corporativa.

El uso de Internet en cualquier organización no solo proporciona un valor añadido si no que es necesario para poder competir con otras empresas del sector donde la competencia es cada vez mayor.

Aunque visto de esta forma puede parecer que el uso de Internet solo trae consigo ventajas, que van desde beneficios económicos sustantivos, facilidad de uso para el acceso rápido o acceso a servicios o productos independientes de la situación geográfica, lo cierto es que también propone desafíos importantes. Uno de estos desafíos es que las organizaciones o empresas con presencia digital en línea son muy susceptibles a la ciberdelincuencia o ataques cibernéticos. Cada vez es mayor el número de empresas que son víctimas de estos ataques, independientemente del tamaño de la organización, y es un problema que preocupa notablemente, pues puede suponer un peligro para la continuidad de estas.

Según el informe sobre Ciberseguridad anual de **Cisco** en 2017 (figura 2), el 29 % de profesionales dedicados a la ciberseguridad exponen que sus organizaciones han experimentado pérdidas de ingresos como resultado de ataques cibernéticos. Dentro de este grupo el 38 % reporta que las pérdidas de ingresos fueron del 20 % o más.

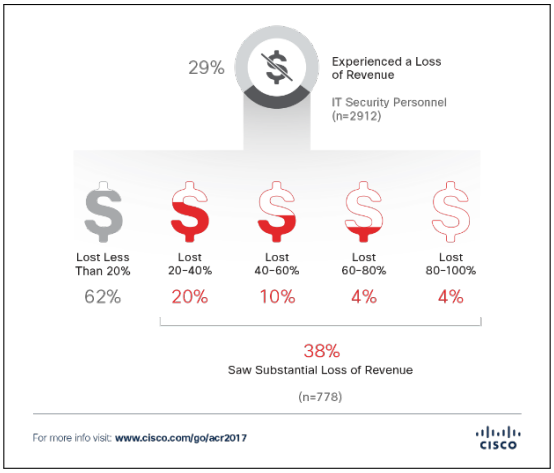

Figura 2: Porcentaje de perdida de ingresos como resultado de un ataque

El principal objetivo de la seguridad informática es garantizar la **disponibilidad, integridad y confidencialidad** de la información para que los clientes confíen en la organización y aumentar el número de clientes.

Aunque, lo cierto es que evitar ataques cibernéticos es prácticamente imposible, la digitalización ha causado que el número de vulnerabilidades que los atacantes pueden explotar para atacar una empresa sea mayor y, aunque no se pueda evitar al 100 %, si que se puede luchar para que las posibilidades de que los ataques tengan éxito sean reducidas. Y esto se consigue, entre otras posibilidades, reduciendo las vulnerabilidades. Claro está que no es una tarea sencilla pues proteger los sistemas y la infraestructura de una organización requiere de una protección activa y monitorizada continuamente, lo que precisa de tiempo y dedicación. Para llevar a cabo esta tarea de forma adecuada lo recomendable es dividir el proceso en varios pasos [2], de forma que sigan un orden secuencial, estos pasos se detallan a continuación:

- **Recolección de información:** consiste en la recolección de todos los logs de eventos de los sistemas. Sin logs de eventos sería difícil detectar cuando un sistema ha sido comprometido o cuando se ha producido un intento de intrusión. Por lo que es importante configurar estos sistemas para que generen dichos logs.

- **Análisis**: es la parte del proceso donde se analizan los logs extraídos en el paso anterior. Los análisis pueden ser manuales o automatizados. Los análisis manuales sirven para hacer informes o para investigar algún evento en concreto, pero son mas tediosos y lentos. Mientras que los análisis automáticos se suelen basar en patrones y reglas basados en tecnologías **SIEM (Security Information and Event Ma-**

nagement), los cuales se pueden configurar para qué nos avisen de determinados eventos, aumentando así la eficiencia.

- **Respuesta:** cuando se produce una alerta, es el turno de responder frente a ella. Es la parte más complicada del proceso, pues hay que estudiar la alarma (grado de impacto, procedencia, objetivos, etc.). Al igual que los análisis, se puede configurar una respuesta activa frente a diversos patrones de ataques, pero cuando se trata de ataques específicos o de los que no se tiene conocimiento, es necesaria la acción humana que intentará minimizar al máximo el impacto de dicho ataque.

Se deduce de lo expuesto en las líneas anteriores que se requiere de tiempo y dedicación, esto, unido a que las amenazas de ciberseguridad se vuelven cada vez más complejas, dirigidas y persistentes, plantean un desafío constante para cualquier organización. Para solventar esta situación no solo son suficientes productos hardware y software. La ciberdefensa moderna requiere de operaciones de seguridad pro activas dirigidas por personal altamente entrenado con la experiencia y pericia para detectar y eliminar dichas amenazas. Así, se llega a la conclusión de que el personal es parte fundamental cuando se refiere a la seguridad de una empresa. Es importante contar con personal cualificado y con habilidades en el campo de la Ciberseguridad que sepan desenvolverse en situaciones complejas que puedan afectar a la integridad de una empresa.

En la actualidad, el número medio de empleados dedicados a la Seguridad Informática es de 33 empleados por organización [3]. El 19 % de organizaciones tienen entre 50 y 99 empleados dedicados a estas tareas y el 12 % a más de 200. Aunque, como se aprecia en la figura 3, el número de empleados dedicados a la Seguridad ha aumentado con respecto a otros años, sigue siendo un porcentaje bajo para importancia que supone la seguridad para una organización.

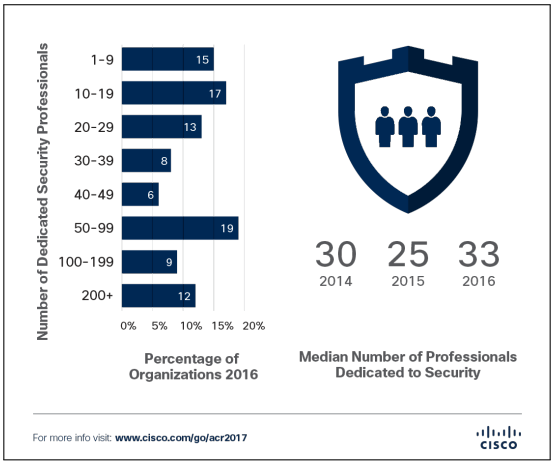

Figura 3: Estudio Cisco sobre el número de profesionales de la seguridad en organizaciones

Por otra parte, los trabajadores de una empresa constituyen el eslabón más débil de una infraestructura de red, es decir, muchos de los ataques son producidos debidos a

imprudencias o desconocimiento de estos trabajadores. Es por ello por lo que es necesario que todos los empleados cuyas funciones requieran de acceso a Internet tenga un mínimo de conocimientos sobre seguridad.

A continuación se detalla como se pretende lidiar con estos problemas o por lo menos reducirlos a través del sistema desarrollado, objeto de este trabajo.

1.2. Cyber Range

En este documento se expone el desarrollo de un Cyber Range, un "campo de maniobras" para ciberseguridad, en él se va a detallar como se ha desarrollado y cuáles pueden ser sus funciones principales dentro de cualquier empresa u organización. Pero para comenzar es importante hacerse la siguiente pregunta: **"¿Qué es un Cyber Range?"**.

Existen varias y diversas definiciones de que es un Cyber Range. Pero para entenderlo de una forma sencilla y clara se escoge la siguiente:

"Un Cyber Range es una capacidad estratégica basada en una plataforma virtual que permite simular entornos operativos reales- estáticos o desplegables, clasificados o no clasificados- para la formación y el entrenamiento- individual o colectivo- de profesionales, así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa."

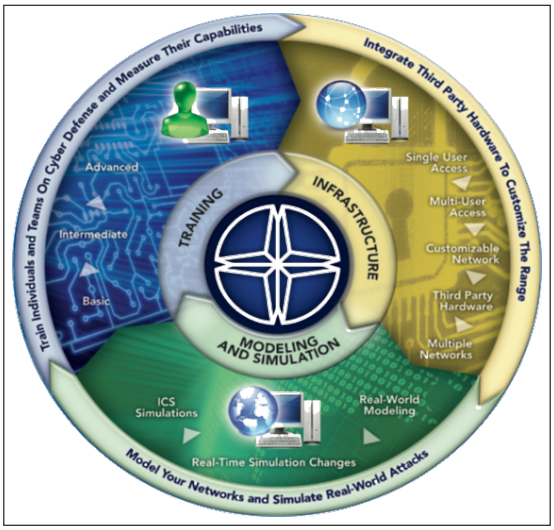

Figura 4: Características Cyber Range

Como la propia definición refleja, en un Cyber Range se simulan entornos reales, adaptados a los servicios de cualquier empresa, que sirven como apoyo para que tanto el personal de seguridad de una empresa como cualquier empleado, construya sus habilidades y experiencias necesarias para combatir las amenazas actuales. Por lo tanto, sirve como campo de entrenamiento de la ciberseguridad, sin poner en riesgo la integridad de la organización. Un Cyber Range proporciona:

- Experiencia de entornos reales para respuesta y defensa contra ataques cibernéticos sencillos y complejos, incluidas las **APTs** (Amenazas persistentes avanzadas).

- Aprendizaje de las principales metodologías, operaciones y procedimientos de seguridad.
- Habilidades avanzadas en la implementación de modelos de protección y en el uso de las últimas técnicas y herramientas de seguridad.
- Experiencia para construir trabajo en equipo y gestión de la responsabilidad para equilibrar la carga de trabajo y enfocar las competencias básicas.
- Una base para garantizar que, en el equipo de respuesta de ciberseguridad, todos los miembros adquieren las mismas habilidades técnicas.

Por todo ello la solución Cyber Range va ganando atención como aliado clave para apoyar programas de formación rentables tanto en contextos civiles y militares.

El Cyber Range que se ha desarrollado cuenta con equipos simulados, como servidores web, de archivos, de correos, servidores DNS, etc., que bien podrían ser los de cualquier organización, aunque estos pueden varias según el tipo de organización. A continuación, se detalla el entorno donde ha sido implementado y los elementos que lo componen.

2. Escenario de pruebas del Cyber Range

El Cyber Range se basa en tres capas, como se muestra en la figura 5:

- **Capa física:** es la capa inferior donde residen los servidores (en el caso de estudio, un servidor), el almacenamiento y la arquitectura de red, que como se verá más adelante, en este caso es híbrida, una parte de red es física mientras la otra parte es virtual.
- **Capa virtual:** en esta capa se encuentra la zona virtual. Se emplean servidores ESXi de VMware donde se encuentra el procesamiento y almacenamiento virtual, y por encima de estos, se encuentran todas las máquinas virtuales con sus distintos sistemas operativos y aplicaciones.
- **Capa de Gestión:** es la capa superior que se compone de plataformas de gestión como vCenter (VMware), con la que se controlan varios servidores ESXi y que contiene funcionalidades de Alta disponibilidad, tolerancia a fallos, etc.

Cada una de estas partes se describen en detalle en los siguientes apartados.

En cuanto a la red sobre la que se ha desarrolla el Cyber Range sigue el modelo de estructura típico de cualquier empresa u organización con un mínimo nivel de seguridad, como muestra la figura 6. Este tipo de estructura permite, por un parte estar conectado a Internet y protegido de conexiones entrantes del exterior en los servicios internos de la organización, y por otra parte tener ciertos servicios accesibles desde el exterior de la organización, sin poner en peligro los demás servicios. Esto se consigue disponiendo de firewall en el que se configuran tres zonas bien diferenciadas:

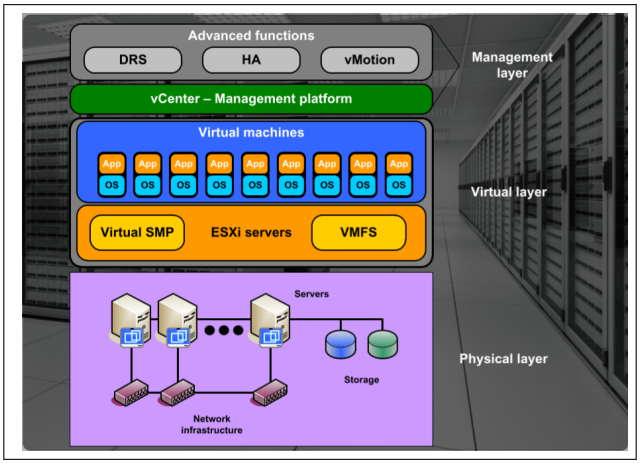

Figura 5: Arquitectura Cyber Range

- ***Internet o Zona exterior:*** es la zona que está directamente conectada a la gran red (Internet) y en ella solo se encuentra el router de acceso.
- ***DMZ o Zona desmilitarizada:*** es la zona que se encuentra a continuación de la frontera de Internet. En esta zona se configuran los servicios que deben estar accesibles desde el exterior de la red.
- ***Intranet o Zona interna:*** es la zona en la que se encuentran todos los equipos y servicios internos de la organización y que no son accesibles desde fuera de esta red, como por ejemplos los ordenadores de los trabajadores de la empresa o los servidores de archivos.

Existen varias configuraciones para esta estructura de red. En el escenario de pruebas del Cyber Range se ha empelado un **Router OS** con firewall con tres adaptadores de red, uno para cada subred.

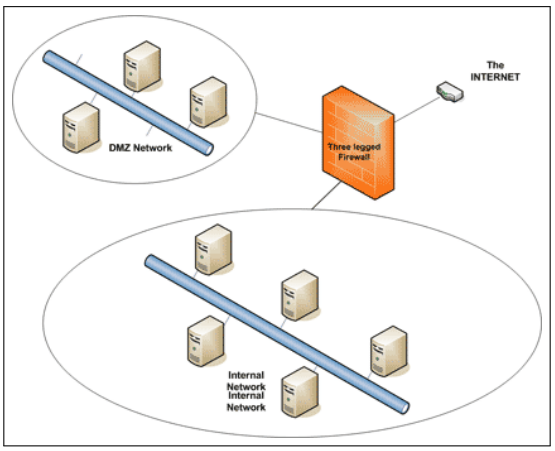

Figura 6: Arquitectura red DMZ

La diferencia reside básicamente en las reglas que se configuran el firewall para cada subred. Así, las reglas más restrictivas y por tanto la zona más segura contra las amenazas será la Interna, mientras que la DMZ dispone de un número de puertos abiertos mayor para los servicios accesibles desde el exterior y, por lo tanto, será más susceptible a los ataques cibernéticos.

En el caso de Cyber Range la zona externa es física, mientras las zonas DMZ e Interna sobre los que se alojan los servidores y equipos Administradores y clientes, se realizan mediante virtualización, es decir, se dispone de un servidor en el cuál se crean las máquinas virtuales necesarias y deseadas para su implementación. A continuación, se explica en detalle cada uno de los componentes que conforman el Cyber Range.

2.1. Hardware

Como se ha introducido en la sección anterior, el servidor es el componente que alberga todas las máquinas virtuales que forman el Cyber Range, por lo que es la parte fundamental del desarrollo. Además, debe contar con los recursos necesarios para soportar todas las máquinas virtuales con las que debe trabajar, ofreciendo a su vez un rendimiento óptimo. En este caso, el servidor con el que se ha trabajado ha sido un **HPE Pro Liant ML110 Generation 9** con las siguientes características principales:

Figura 7: HPE Pro Liant ML110 Gen 9

Núcleos CPU	8 CPU x 2.097 GHz
Procesador	Intel Xeon CPU E5-2620
RAM	74 GB
Almacenamiento	2 TB
Adaptadores de red	Broadcom 5717 Dual-port 1GbE

Tabla 1: Recursos hardware servidor

Todas las características y configuraciones del modelo de este servidor se encuentran disponibles en [4].

2.2. Software

En la parte referente al software del Cyber Range, como se ha comentado anteriormente, se decide utilizar **virtualización** por las ventajas que estas conlleva, algunas de ellas son:

- Disminuye los costes de equipos físicos.
- Crear máquinas virtuales es un proceso sencillo y rápido, además de poder crear una gran cantidad de ellas en un solo servidor.
- Aislamiento: en caso de ocurrir cualquier fallo o error en alguna máquina, solo afecta a esa máquina en concreto y no afecta a las demás.
- Flexibilidad: Es posible guardar las máquinas con su estado actual para recuperarlas más tarde o para implementar en otros sistemas.
- Centralización: Gestión de todas las máquinas de forma centralizada.

Estas ventajas son beneficiosas en el caso concreto del Cyber Range ya que al ser un campo de entrenamiento para ciberseguridad es posible crear y modificar todas las máquinas que se deseen o probar distintas configuraciones sin temor a dañar el sistema.

La plataforma elegida para la virtualización es VMware, que además de los beneficios anteriormente señalados, trae consigo otras ventajas propias de esta plataforma que se verán a continuación, así como sus características principales.

2.2.1. Hypervisor vSphere ESXi

El Hypervisor ESXi se instala directamente en el servidor físico y es el componente que se encuentra al nivel inferior de la capa de virtualización, sobre el que funcionan las máquinas virtuales con los distintos sistemas operativos y sus aplicaciones (figura 8). Está compuesto de un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software hipervisor, y los servicios y servidores que permiten la interacción con el software de gestión y administración y las máquinas virtuales.

En este caso se ha implementado la versión **ESXi 6.0** que permite acceder a la interfaz gráfica mediante un cliente para sistemas operativos Windows o bien por medio de la interfaz gráfica web. Así pues, se pueden visualizar todas las máquinas implementadas y gestionarlas de una manera sencilla e intuitiva. Además, proporciona funcionalidades [5] como:

- Monitorización de los recursos utilizados en tiempo real.
- Permite guardar y recuperar el estado de una máquina virtual en un punto específico del tiempo (Snapshots)
- Permite crear switchs virtuales con el fin de simplificar y optimizar la red de máquinas virtuales.

- Permite crear más de 1000 máquinas virtuales por host.
- Permite realizar acciones en caliente como: ampliar la CPU, memoria o almacenamiento a las máquinas virtuales, conectar dispositivos virtuales de almacenamiento o de red, etc.

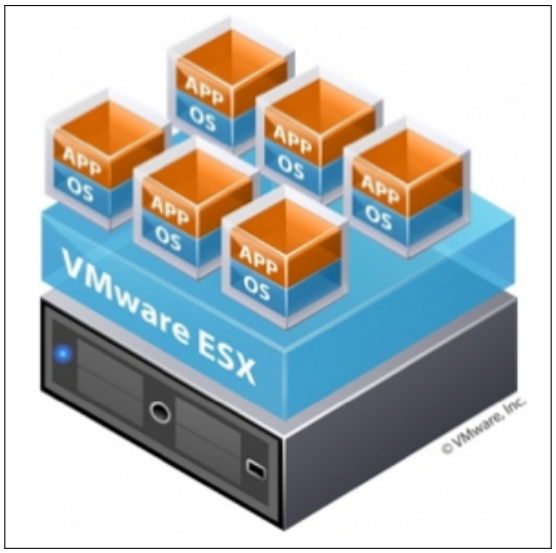

Figura 8: Arquitectura Hypervisor ESXi

2.2.2. vCenter Server

vCenter Server proporciona un sistema de gestión centralizado que permite controlar varios servidores físicos (varios vSphere ESXi) y sus máquinas virtuales desde una sola interfaz gráfica. Una sola instancia de vCenter Server soporta un **máximo de 1000 hosts ESXi y 15000 máquinas virtuales**[6].

vCenter Server además de proporcionar las mismas funcionalidades que vSphere ESXi, añade nueves funcionalidades [5] como:

- **VMware HA (Alta Disponibilidad):** permite reiniciar automáticamente máquinas virtuales en otro servidor físico si ocurre un error o fallo en el servidor en el que se encuentran alojadas, minimizando el tiempo de caída
- **VMware DRS (Balanceo de carga):** permite balancear las cargas de trabajo entre recursos que estén disponible en un cluster de hosts. Así, si la carga de trabajo de una o más máquinas virtuales cambia drásticamente, se redistribuye las máquinas virtuales entre los servidores físicos.
- **Fault Tolerance (Tolerancia a fallos):** se crea una instancia duplicada de una máquina virtual que siempre se mantiene actualizada respecto a la máquina virtual principal. En caso de un fallo de hardware, vShpere FT activa automáticamente la

conmutación por error y, a continuación, crea una nueva máquina virtual secundaria con el fin de proteger de forma continua la aplicación.

- **vMotion (Migración de máquinas):** permite trasladar máquinas virtuales en funcionamiento de un servidor físico a otro, sin tiempo de inactividad. Con lo que es posible realizar el mantenimiento de cualquiera de los servidores sin pérdida de funcionamiento.

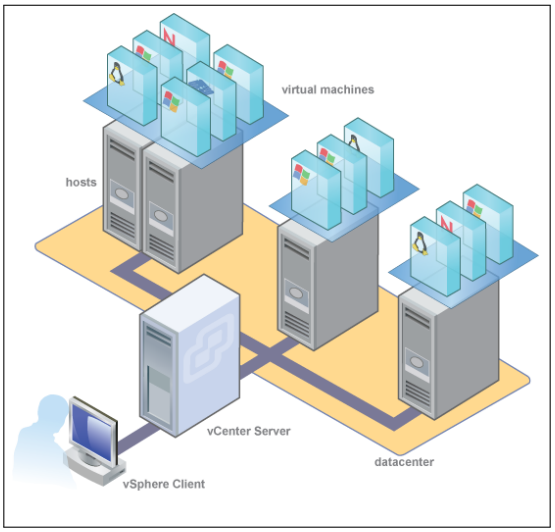

Figura 9: Arquitectura Hypervisor ESXi

Como el vSphere ESXi, también se ha instalado la versión 6.0 de la herramienta vCenter, ya que es la última versión que permite utilizar el cliente de vmware para Windows, las versiones siguientes a las 6.0 de vCenter, solo se pueden ejecutar mediante la interfaz web.

3. Diseño de la arquitectura de red

Una vez se ha visto el software utilizado para la implementación del Cyber Range, se pasa a estudiar el diseño de su arquitectura. Como se ha introducido en la sección 2, la arquitectura de red se basa en tres zonas, delimitadas por un firewall con tres adaptadores de red.

En concreto, la arquitectura diseñada se compone de los siguientes elementos:

- **Servidor físico** con IP pública 158.42.188.114 conectado al Gateway de la **Universidad Politécnica de Valencia** (158.42.188.250) que proporciona el acceso a Internet.
- **Router físico** en la red 10.0.0.1/24, el cual puede ser utilizado como punto de acceso para intrusos que puedan comprometer nuestro sistema por medio de ataques cibernéticos.

- **Distributed Switch virtual** donde se conecta el vCenter, al que también se le asigna una ip pública (158.42.188.163) y poder conectar entre sí los distintos servidores físicos.
- **Router OS con Firewall**, encargado de conectar y dar direcciones privadas a las distintas subredes, además de configurar las políticas de seguridad según las características de cada subred.
- **Subred DMZ o zona desmilitarizada** (10.0.1.0/24) que proporcionan los servicios que requieren acceso a Internet, pero desde estos equipos no se tiene acceso a la red Interna para no poder así comprometer su seguridad.
- **Subred Interna o Intranet** (192.168.0.0/24), donde se alojan todos los servidores Internos virtuales a los que solo se pueden acceder dentro de la subred. Además, estos equipos SI pueden tener acceso a los servicios de la DMZ.

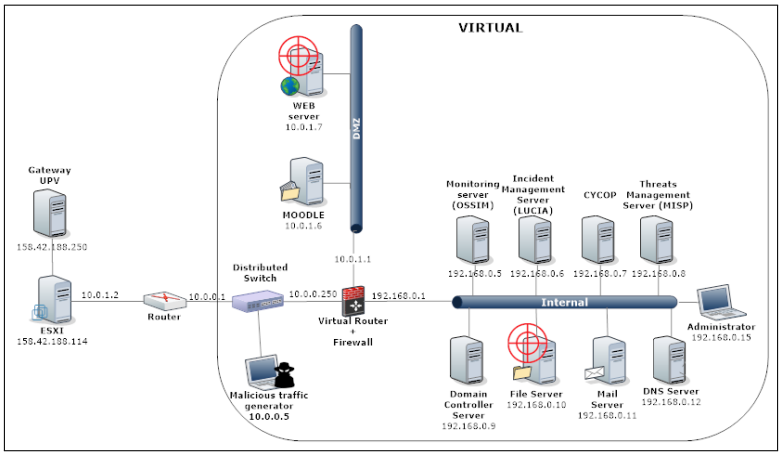

Figura 10: Diseño Arquitectura de red Cyber Range

Posteriormente al diseño de la arquitectura de red, se procede a la implementación del Cyber Range con todas las subredes y máquinas virtuales expuestas en la figura 10.

4. Implementación Cyber Range

En esta sección se expone de forma detallada la función de cada uno de los elementos de nuestra arquitectura (servidores, routers, firewall, etc.) así como la implementación y configuración de cada uno de ellos.

Como se ha explicado anteriormente se trabaja mediante la plataforma de virtualización de VMware y, por tanto, todos los desarrollos y configuraciones se realizan a través del cliente vSphere para Windows.

4.1. Servidor ESXi

El servidor ESXi es el elemento central de la arquitectura y pieza fundamental, en él se realiza la creación y mantenimiento de todas las máquinas virtuales. La interfaz principal de la herramienta muestra una descripción de los componentes hardware de nuestro sistema, así como el estado de los recursos, las redes de las que dispone, etc.

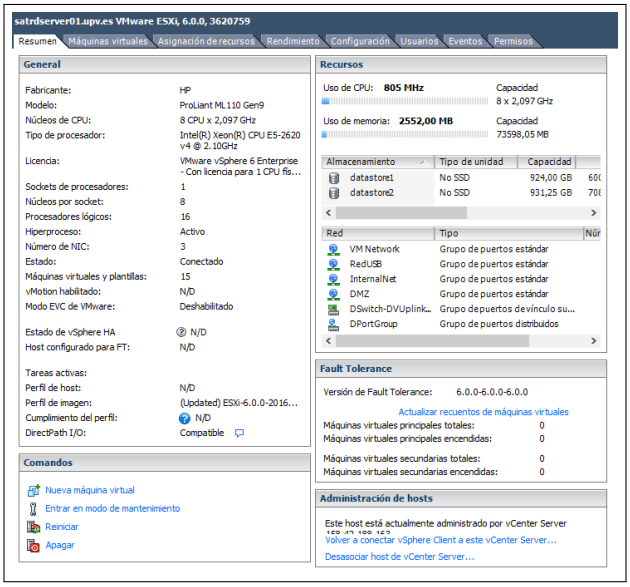

Figura 11: Interfaz principal ESXi

Además, muestra un listado de todas las máquinas virtuales alojadas en el sistema como muestra la figura 12. Se dispone de dos grupos de recursos: uno llamado Cyber Range que alberga todas las máquinas virtualmente directamente relacionadas con la estructura y otra de denominada Management, la cual dispone de máquinas utilizadas para la gestión del Cyber Range. En total se crean **11 máquinas virtuales en Cyber Range y 4 máquinas virtuales en Management**.

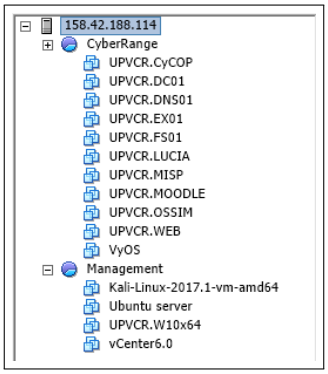

Figura 12: Listado Máquinas virtuales

Una de las funcionalidades que proporciona vSphere ESXi es la de mostrar de forma

gráfica la conexión entre las distintas máquinas virtuales, ya sea conexión de red o conexión a los almacenes de datos, lo que permite ver de forma gráfica y sencilla la disposición de todas las máquinas y recursos de los que se disponen.

En la figura 13 se muestra como todas las máquinas virtuales cuelgan de la red a la que pertenecen y que todas ellas se encuentran en el mismo servidor.

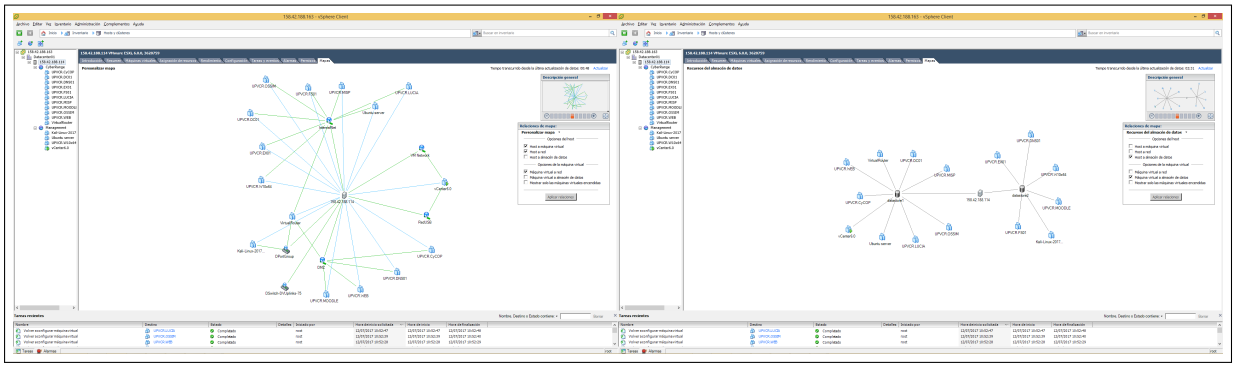

Figura 13: Mapa arquitectura Cyber Range

En esta otra imagen se puede apreciar cómo se reparten las máquinas virtuales en los dos almacenamientos de datos de los que está provisto el servidor.

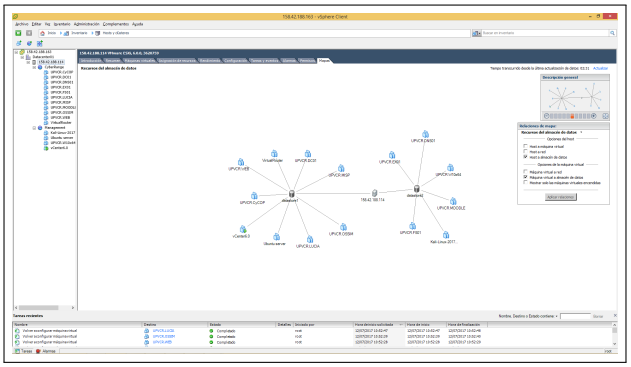

Figura 14: Mapa datastores Cyber Range

Además, vSphere permite la monitorización del rendimiento y los recursos que están utilizando en cada momento cada máquina.

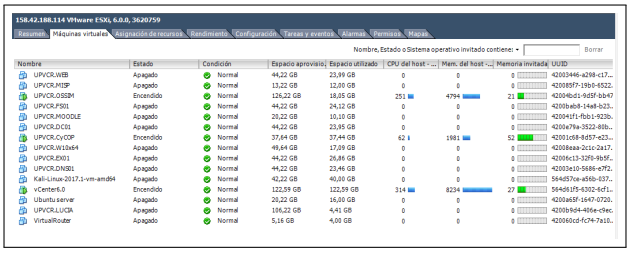

Figura 15: Interfaz uso recursos

Aunque si se desea un informe más detallado es posible exportar un archivo Excel que presenta los datos del rendimiento del disco, energía, uso de la CPU, uso de la red, etc, en el intervalo de tiempo deseado.

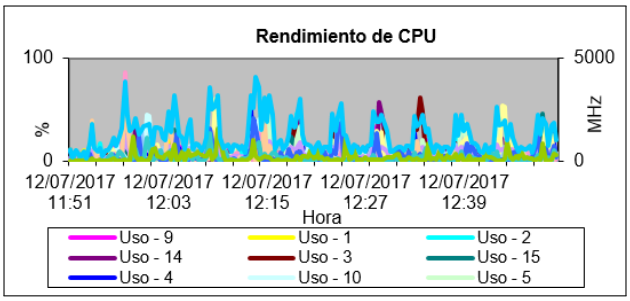

Figura 16: Gráfica informe rendimiento CPU

En cuanto a la red se refiere, mediante vSphere se crean los distintos Switch virtuales que servirán como subredes a los que se conectarán las máquinas virtuales. En este caso se disponen de los siguientes.

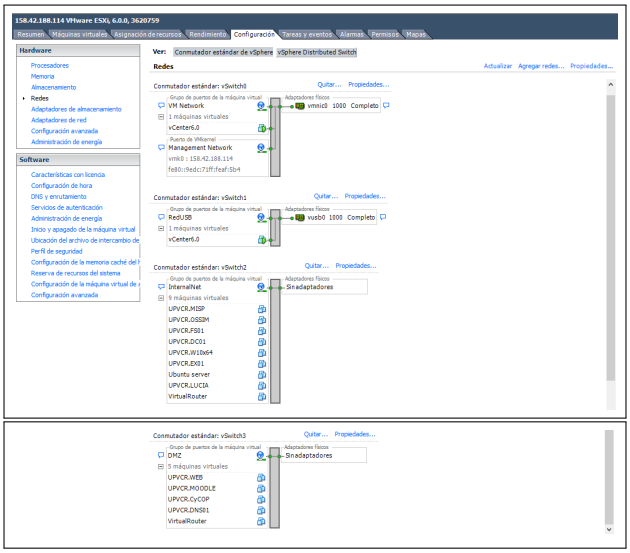

Figura 17: Switch virtuales Cyber Range

Switch virtual	Red	Adaptador de red	Función
0	VM Network	Gigabit Ethernet	Proporciona el acceso a Internet
1	RedUSB	Gigabit Ethernet	Conectar los distintos servidores entre sí mediante vCenter
2	InternalNet	Virtual	Aislar la red Interna
3	DMZ	Virtual	Aislar la red DMZ

Tabla 2: Switch virtuales y adaptadores de red

Las funcionalidades mencionadas anteriormente son las principales con las que se trabaja, aunque VMware vSphere tiene multitud de funcionalidades más, algunas de ellas se irán viendo conforme se vaya detallando la implementación de las distintas máquinas virtuales.

4.2. Router Virtual

El elemento utilizado para interconectar las diferentes subredes y proporcionar las direcciones IPs privadas ha sido un router virtual. En este caso se ha hecho uso de un **Router OS (Router Operating System)**, que es una parte del software encargado de gestionar los recursos del router mediante el control y la asignación de la memoria o de priorizar las solicitudes y procesos del sistema. En concreto, se implementado un **VyOS Router** [7], desarrollado por la empresa **Brocade Communications**. VyOS es un sistema operativo de red de fuente abierta, basado en GNU/Linux, con una interfaz en línea de comandos que proporciona capacidades de enrutamiento, firewall y VPN.

VyOS se configura para que disponga de tres interfaces de red; el primero conectado al Switch distribuido, el segundo a la red DMZ y el tercero a la red Interna, tal y como se muestra en la imagen.

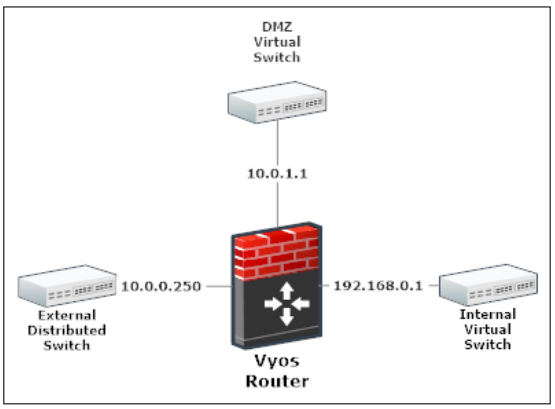

Figura 18: Interfaces Router Virtual

Así, todos los equipos de la DMZ tendrán como puerta de enlace la dirección 10.0.1.1, los equipos de la red Interna la dirección 192.168.0.1 y los pertenecientes a la red externa la IP 10.0.0.250.

Con el fin de proporcionar direcciones IPs a los equipos que se conecten a las distintas redes, se configura el servicio DHCP, y para que sea posible la conexión a Internet, los servicios NAT, DNS forwarding, Port forwarding, etc.

Además, como se ha comentado anteriormente el software de VyOS, también incorpora servicios de firewall, lo que permite configurar las reglas para aportar la seguridad necesaria a cada zona de red.

El firewall se configura teniendo en cuenta que las reglas se cumplen de arriba a abajo, por lo que se sigue un orden:

1. Bloquear las conexiones a redes no autorizadas
2. Aceptar tráfico ICMP
3. Aceptar servicios deseados/necesarios
4. Bloquear otros servicios no deseados

Así, se definen las siguientes reglas en cada red:

Reglas de la DMZ

En el adaptador de la red DMZ (10.0.1.1) se bloquea el tráfico que tenga como dirección la red interna, y se permite el tráfico hacia la red Exterior a aquellos servicios que desde la red DMZ, necesitan de acceso a Internet. Además, se permite el tráfico ICMP a cualquier destino.

Fuente	Destino	Servicio/Puerto	Acción
DMZ	OSSIM (LAN)	SSH, SMB, OSSIM/ 22, 445, 1514	Permitir
DMZ	Interna	Cualquiera	Bloquear
DMZ	Exterior	ICMP	Permitir
DMZ	Exterior	IMAP/143	Permitir
DMZ	Exterior	SMTP/25	Permitir
DMZ	Exterior	POP/110	Permitir
DMZ	Exterior	DNS/53	Permitir
DMZ	Exterior	FTP/21	Permitir
DMZ	Exterior	HTTP/80	Permitir
DMZ	Exterior	HTTPS/443	Permitir

Tabla 3: Reglas firewall DMZ

Reglas de la Red Interna

En el adaptador de la red interna (192.168.0.1) se permite el tráfico a los servicios usados por los servidores y usuarios de esta red. Además se permite el tráfico ICMP a cualquier destino.

Fuente	Destino	Servicio/Puerto	Acción
OSSIM (Interna)	OSSIM (LAN)	SSH, SMB, OSSIM/ 22, 445, 1514	Permitir
Interna	Interna	ICMP	Permitir
Interna	DMZ		Permitir
Interna	Interna	FTP/21	Permitir
Interna	Interna	SMTP/25	Permitir
Interna	Interna	POP3/110	Permitir
Interna	Interna	DNS/53	Permitir
Interna	Interna	IMAP/143	Permitir
Interna	Interna	SMB/445	Permitir
Interna	Interna	SSH 22	Permitir
Interna	Interna	Netbios/137,138,139	Permitir
Interna	Interna	HTTP/80	Permitir
Interna	DMZ	HTTP/443	Permitir

Tabla 4: Reglas firewall Red Interna

Reglas de la Red Externa

En el adaptador de la red Externa (10.0.0.250) se permite el tráfico a los servicios de la DMZ que deben estar disponibles desde Internet. Además, se bloquea el tráfico a la red Interna o a cualquier otro puerto no necesario en la red DMZ. En este caso no se permite el tráfico ICMP.

Fuente	Destino	Servicio/Puerto	Acción
Interna	Interna		Bloquear
Interna	DMZ	FTP/21	Permitir
Interna	DMZ	SMTP/25	Permitir
Interna	DMZ	POP3/110	Permitir
Interna	DMZ	DNS/53	Permitir
Interna	DMZ	IMAP/143	Permitir
Interna	DMZ	HTTP/80	Permitir
Interna	DMZ	HTTP/443	Permitir
Externa	DMZ	Cualquiera	Bloquear

Tabla 5: Reglas firewall Red Externa

4.3. Servicios de la red Externa

La red externa es la red que se conecta al **Switch Distribuido virtual** de vSphere. En esta red no se aloja ningún servicio ni equipo perteneciente a la organización, pero es la red que proporciona el acceso a Internet, ya que se encuentra conectada a la puerta de enlace de la Universidad.

Podría ser un punto vulnerable de acceso de cualquier intruso, por lo que para comprobar la seguridad se implementa una máquina virtual con sistema operativo **Kali-Linux 2017.1**. Kali Linux Se basa en una distribución **Debian** de Linux y es utilizado por muchos pentester de seguridad ya que viene provista de multitud de herramientas para controlar el nivel de seguridad, realizar escaneos de vulnerabilidades, explotar dichas vulnerabilidades, comprobar el tráfico en nuestra red, etc [8].

En el Cyber Range se ha implementado para realizar estas comprobaciones de seguridad y realizar pequeños ensayos de ataques a los servicios alojados en las redes Internas y DMZ, para así estudiar el comportamiento de estas máquinas frente a los ataques. Posteriormente en este documento se documentan algunas de las pruebas que se han realizado con esta herramienta.

4.4. Servicios de la red DMZ

La red DMZ es la zona que se encuentra entra la red interna y la red externa. Su objetivo es permitir el acceso desde las redes internas y externas, mientras que las conexiones desde la red DMZ solo se permiten a la red externa y no a la interna. Con esto se consigue que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen a la red Interna en caso de intrusión[9].

La red DMZ normalmente alberga aquellos servicios que necesitan ser accesibles desde fuera de nuestra red. Un ejemplo de ello sería la página web corporativa de la empresa a la que pueda acceder cualquier internauta. En el caso del Cyber Range, el rango de direcciones que se le ha asignado a esta red es 10.0.1.0/24.

Los servicios y máquinas disponibles en la red DMZ del Cyber Range son:

Servicio	Dirección IP	Sistema Operativo
MOODLE	10.0.1.5	Ubuntu 16.10
Servidor WEB	10.0.1.6	Windows Server 2008 R2

Tabla 6: Servicios de la red DMZ

A continuación, se va a detallar la función de cada una de las máquinas, así como su implementación.

4.4.1. MOODLE

En el entorno de pruebas del Cyber Range se realiza la implementación de un Moodle. Moodle es una herramienta de carácter académico para la gestión virtual de cursos, de

distribución libre, en los cuales los educadores se ayudan para subir material y crear comunidades de aprendizaje en línea.

Esta implementación se realiza sobre la máquina virtual **UPVCR.MOODLE**, con sistema operativo **Ubuntu 16.10** y se le asigna la dirección IP 10.0.1.6. Este servicio requiere de acceso a Internet, para que, usuarios fuera de nuestra organización puedan acceder a los recursos que se cuelguen en la plataforma Moodle.

Moodle utiliza como servidor web Apache, MySQL para la gestión de las bases de datos y PHP como lenguaje de programación, por lo que antes de proceder a la instalación de Moodle es necesario instalar sus librerías correspondientes y configurar estos servicios en la máquina virtual de Ubuntu.

Una vez implementado y corriendo sobre el servidor Apache, se accede a la interfaz gráfica mediante la dirección local del servidor en cualquier navegador, donde se gestionan los cursos y material virtual, como se observa en la figura 19.

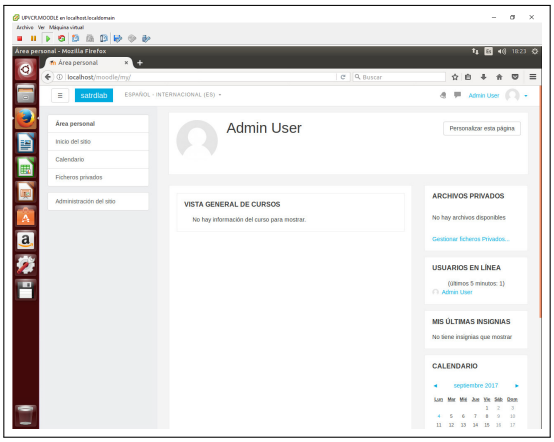

Figura 19: Interfaz gráfica Moodle

4.4.2. Servidor WEB

La mayoría de organizaciones disponen de una página web corporativa en la que se dan a conocer, cuelgan sus productos o suben sus noticias. Para el desarrollo de una página WEB es necesario disponer de un Servidor que almacene su contenido y responda a las peticiones HTTP.

La implementación del Servidor WEB en el Cyber Range se realiza sobre la máquina virtual **UPVCR.WEB**, mediante el sistema operativo **Windows Server 2008 R2** y se le asigna la dirección IP 10.0.1.7. Este servidor estará disponible tanto para la red del exterior como para la interior.

Se realiza la implementación de forma sencilla con Windows Server agregando la función de **"Servidor Web IIS"**, y una vez instalada la funcionalidad, nos permite crear y administrar la página web mediante una gran variedad de herramientas y opciones de seguridad.

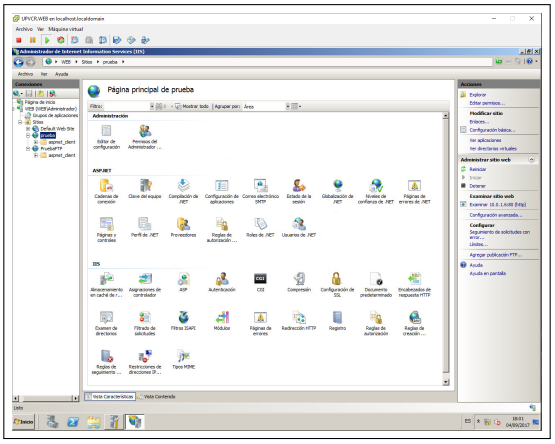

Figura 20: Servidor Web IIS Windows Server

4.5. Servicios de la red Interna

En la Red Interna se alojan todos los servicios necesarios de la organización a los que solo se tiene acceso dentro la misma red y se deniega a toda conexión entrante fuera de la misma.

Las máquinas del Cyber Range que se implementan en esta red son las siguientes:

Servicio	Dirección IP	Sistama Operativo
OSSIM (Monitorización)	192.168.0.5	Linux
LUCIA (Gestión de Incidentes)	192.168.0.6	CentOS
CyCOP	192.168.0.7	Windows 10
MISP (Gestión de Amenazas)	192.168.0.8	Ubuntu 14.04
Controlador de dominios	192.168.0.9	Windows Server 2008 R2
Servidor de Archivos	192.168.0.10	Windows Server 2008 R2
Servidor de Correo	192.168.0.11	Windows Server 2008 R2
Servidor DNS	192.168.0.12	Windows Server 2008 R2

Tabla 7: Servicios de la red Interna

En este caso, se deciden implementar las máquinas anteriores con el objetivo de asemejarse lo máximo posible a cualquier organización, además de algunas otras herramientas para trabajar en materia de ciberseguridad. A continuación, se detalla cada una de las máquinas implementadas y sus principales características.

4.5.1. OSSIM

El primero de los servicios a implementar en el Cyber Range es **OSSIM** (Open Source Security Information Management. OSSIM se basa en un conjunto de herramientas Open Source integradas para formar una infraestructura de monitorización de seguridad.

El objetivo de OSSIM es mejorar las capacidades de detección de eventos de seguridad. Esto lo consigue principalmente gracias a la correlación. Mediante la correlación es posible obtener una visibilidad de todos los eventos de los sistemas en un punto y con un mismo formato, y gracias a ello relacionar y procesar la información proveniente de los distintos sensores o monitores, para que permita detectar, monitorizar, priorizar y organizar la seguridad de nuestra red.

La implementación de OSSIM en el Cyber Range se realiza sobre la máquina virtual **UPVCR.OSSIM**, sobre el sistema Linux y se le asigna la dirección IP 192.168.0.5.

OSSIM se instala mediante línea de comandos en Linux, y una vez instalado y configurado se accede a su interfaz gráfica a través del navegador. OSSIM ofrece multitud de opciones en su plataforma, nada más acceder a ella, muestra un Dashboard resumen con gráficos del número de alarmas, el tipo de alarmas más ocasionales, los sistemas en los que se han producido más alarmas, etc.

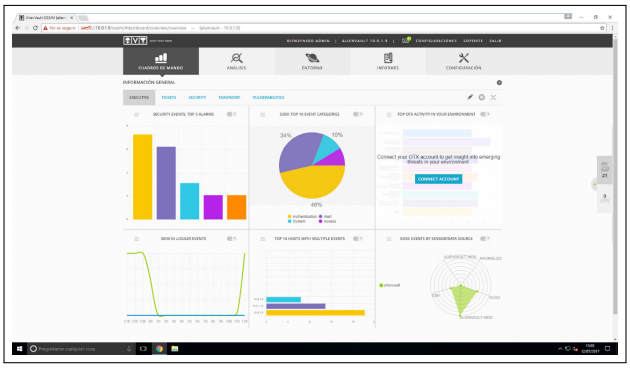

Figura 21: Dashboard OSSIM

Además, monitoriza constantemente la red para descubrir nuevos equipos que se conecten a nuestra red y poder comprobar así, si se produce alguna intrusión o equipo no deseado accediendo a la red de nuestra organización.

OSSIM permite crear grupos de activos para organizar la información que se obtiene mediante la monitorización, por lo que para el Cyber Range se crea un grupo de activos con las máquinas que lo componen para acceder de una forma más clara y sencilla a la información exclusiva de nuestro sistema (fig 22).

Una de las funcionalidades interesantes y que se han realizado es la de implementar agentes OSSEC en cada una de las máquinas que componen el Cyber Range. OSSEC es un sistema de detección de intrusos a nivel de host (HIDS), es decir, monitoriza los registros de Windows, analiza la integridad de sus ficheros, detecta rootkits, etc.

Mediante el **agente OSSEC** se crean los logs y se envían al servidor OSSIM para su análisis. Como se ve en la figura 23 se ha implementado un agente en cada máquina virtual del Cyber Range y OSSIM nos da información de los agentes conectados o desconectados, el número de eventos analizados, etc.

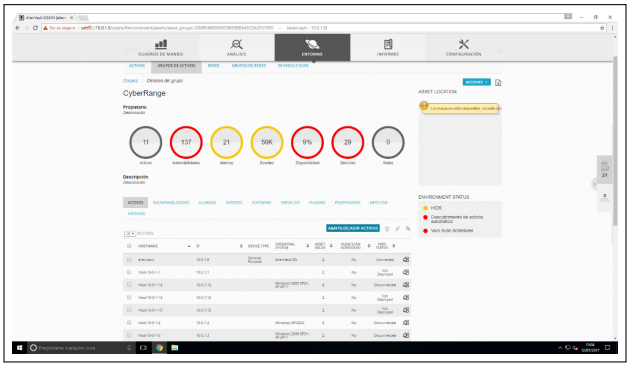

Figura 22: Grupo de Activos Cyber Range

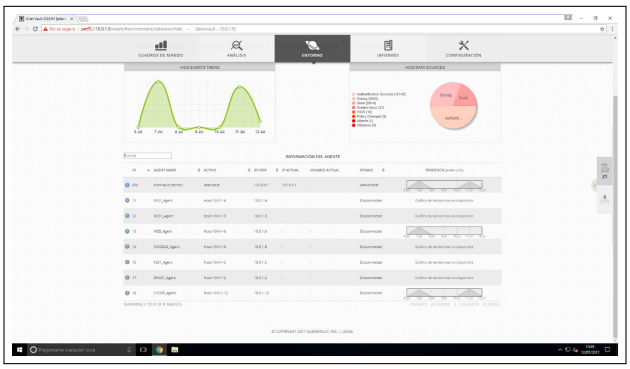

Figura 23: Agentes OSSEC desplegados

4.5.2. LUCIA

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta desarrollada por el **CCN-CERT** (Centro Criptológico Nacional) para la gestión de ciberincidentes en las entidades participantes en el Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora[10].

Ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados. Con la herramienta LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:

- Los incidentes propios del Organismo
- Los provenientes del Sistema de Alerta Temprana de RED SARA (SAT-SARA)
- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET)

Además, el uso de LUCIA aporta numerosos beneficios para una organización como son los siguientes:

- Mejora la coordinación entre el CCN-CERT y todos los organismos a los que ofrece sus servicios mediante la Integración de los incidentes de seguridad con el CCN-CERT
- Mejora el intercambio de información de incidentes de seguridad.
- Mantener la trazabilidad y seguimiento del incidente
- Mejora en los procesos de gestión
- Automatiza tareas y permitir su integración con otros sistemas
- Construir bases de datos de conocimiento
- Mejora de gestión de los proyectos SAT-SARA y SAT-INET

Por todo ello, se decide hacer uso de LUCIA, que se implementa en el Cyber Range sobre la máquina virtual **UPVCR.LUCIA**, identificada con la dirección IP 192.168.0.6, provista de sistema operativo **CentOS**.

4.5.3. CyCOP

CyCOP (Cyber Common Operational Picture) es una herramienta desarrollada por el Grupo de sistemas de Tiempo Real Distribuidos para el mando y control de la ciberdefensa. El principal objetivo de CyCOP es proporcionar una mejor **Situational Awareness**, para ello dispone de un módulo que fusiona la información de dominio cibernético como amenazas, ataques, vulnerabilidades, etc.) obtenidos con herramientas SIEM, con información georreferenciada de los sistemas de mando y control de dominio físico, obteniendo así lo que se denomina **CyHSA** (Cyber Hybrid Situation Awareness).

Los casos de uso generales de CyCOP son:

- Obtención de información externa ciber:
  - Assets
  - Alarmas
  - Vulnerabilidades
  - Amenazas
  - Incidentes
- Generación de SA
  - Ciber
  - Física (C2)
  - Híbrida
- Análisis

- Fusión de Información
- Inserción manual de datos
- Exportar Información

CyCOP se conecta y recibe información de otras herramientas implementadas. Por ejemplo para información de Assets, Alarmas y Vulnerabilidades las obtiene de la herramienta OSSIM, las Amenazas de la herramienta MISP o por inserción manual y la información de Incidentes a través de LUCIA o como en el caso de las Amenazas, por inserción manual de los usuarios. Esta información se fusiona y almacena en un modelo de datos que constituye el núcleo del sistema. Además, existe un módulo que permite realizar análisis sobre los datos, crudos o fusionados. Con dicha información se puede, en todo momento, alimentar al otro componente fundamental del sistema: la parte de visualización. Esta puede realizarse en una visualización 2D clásica, con múltiples técnicas más canónicas o bien más novedosas, o bien utilizando el módulo de visualización con realidad virtual inmersiva con la intención de explorar en cuánto mejoran la SA.

Para el testeo de la herramienta CyCOP en un Cyber Range,se ha implementado sobre la máquina virtual **UPVCR.CyCOP**, identificada con la dirección IP 192.168.0.7, funcionando sobre el sistema operativo **Windows 10**. Además se conectará con las máquinas virtuales de OSSIM, MISP y LUCIA.

4.5.4. MISP

MISP (Malware Information Sharing Platform & Threat Sharing) es una solución de Software libre creada para compartir, almacenar o distribuir indicadores o amenazas de ciberseguridad encontradas en análisis. Su principal objetivo es el de fomentar el intercambio de información estructurada dentro de la comunidad de seguridad. MISP proporciona funcionalidades para apoyar el intercambio de información, pero también para el consumo de información para **NIDS (Network Detection Intrusion System)**, **LIDS**, pero también para herramientas de análisis de logs, **SIEM**. Las características principales de MISP [11]son:

- Búsqueda de correlación automática de relaciones entre atributos e indicadores de malware, ataques de campañas o análisis.
- Funcionalidad de compartición integrada para facilitar el uso compartido de datos mediante diferentes modelos de distribución.
- Almacenamiento de datos estructurado (permitiendo el uso automatizado de bases de datos para varios propósitos).
- Exportación: generación de IDS, OpenIOC, texto sin formato, CSV, MISP XML o JSON para la integración con otros sistemas (NIDS o HIDS).
- Importación: importación conjunta, por lotes, importación desde OpenIOC, GFI sandbox, ThreatConnect CSV.

- API flexible para integrar MISP en soluciones propias. MISP está incluido en PyMISP, que es una biblioteca de Python flexible para buscar, agregar o actualizar atributos de eventos, manejar muestras de malware y etiquetar eventos siguiendo sus propios esquemas de clasificación.

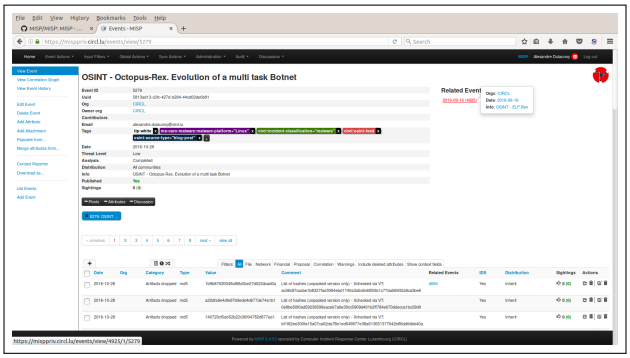

Figura 24: Ejemplo indicador de amenaza

En nuestro entorno de pruebas Cyber Range se ha implementado sobre la máquina virtual **UPVCR.MISP** corriendo sobre un sistema operativo **Ubuntu 14.04** con dirección IP 192.168.0.8.

4.5.5. Controlador de Dominios

Si se desea una mayor supervisión de los usuarios y equipos en nuestra red, es necesario implementar un **controlador de dominios** cuya función principal es la **autenticación**: garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente para ello se hace uso de las contraseñas. Por lo que el controlador de dominios es el encargado de almacenar los usuarios y sus respectivas contraseñas de una red para su posterior autenticación.

La implementación del controlador de dominios en el Cyber Range se realiza sobre la máquina virtual **UPVCR.DC01** con sistema operativo **Windows Server 2008 R2**, a la que se le asigna la dirección IP 192.168.0.9.

Se realiza de forma sencilla activando el rol de Active Directory integrado en este sistema operativo. El dominio creado corresponde con el nombre **"UPV.CR"** y desde las funcionalidades disponibles en el Active Directory se puede administrar los equipos y usuarios que se encuentran dentro del dominio creado.

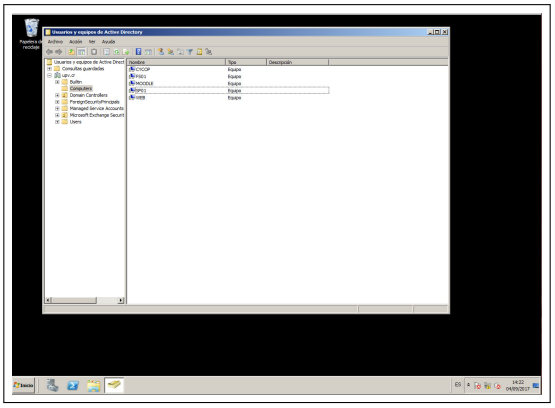

Figura 25: Equipos en el dominio UPV.CR

En esta otra imagen se ve como en las propiedades del sistema el equipo FS01 (Servidor de Archivos) se añade al dominio mencionado anteriormente en vez de pertenecer a un grupo de trabajo que es como se encuentra inicialmente.

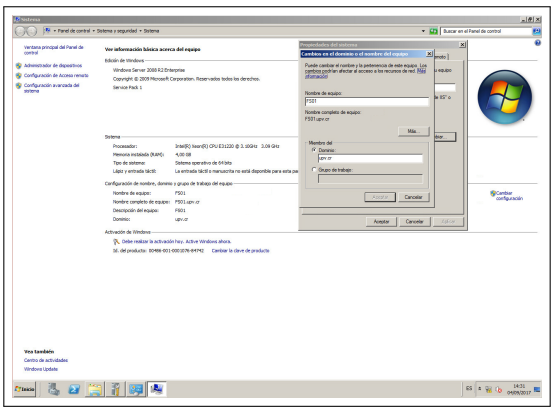

Figura 26: Añadiendo equipo al dominio UPV.CR

4.5.6. Servidor de Archivos

Cualquier organización dispone de una unidad en red donde subir y descargar archivos de forma centralizada, en la que es posible personalizar los privilegios según las necesidades de cada grupo de usuarios o su posición en la empresa.

Esta funcionalidad necesita estar debidamente controlada y supervisada pues se comparten archivos confidenciales dentro de una organización. La implementación del servidor de archivos en el Cyber Range se realiza en la máquina virtual **UPVCR.FS01** sobre un sistema operativo **Windows Server 2008 R2**, la cual está identificada por la dirección IP 192.168.0.110.

Con este sistema operativo es posible crear una carpeta compartida en red a la que el Administrador le concede los privilegios que requiera cada usuario o grupo de usuarios. En la figura 27 refleja como se ha particionado el disco de almacenamiento en dos para crear

una unidad de 10 GB (Unidad E), donde se compartan los archivos deseados y conceder los privilegios para cada usuario o grupo de usuarios.

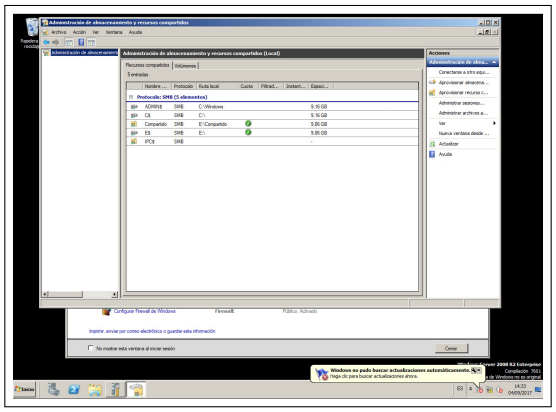

Figura 27: Unidad compartida de archivos

4.5.7. Servidor de Correo

Además de todos los servicios descritos anteriormente, se implementa un Servidor de Correo, con el que es posible realizar el intercambio de correos de la organización. Para su implementación se utiliza el servidor de correo **Microsoft Outlook Exchange 2010** sobre la máquina virtual **UPCR.EX01**, sobre un sistema operativo **Windows Server 2008 R2**, identificada por la dirección IP 192.168.0.111.

Al finalizar la instalación, se dispone de una consola de Gestión de Exchange (fig 28), donde se gestionan todas las configuraciones de este servidor y se da de alta a los usuarios, además es posible configurar los roles de acceso administrativo para los usuarios o grupos de usuarios. Esta consola también permite configurar el Mailbox, el acceso a clientes y una vez registrados, es necesario configurar el cliente Exchange en cada uno de los equipos que vayan a hacer uso de este servicio y poder intercambiar correos.

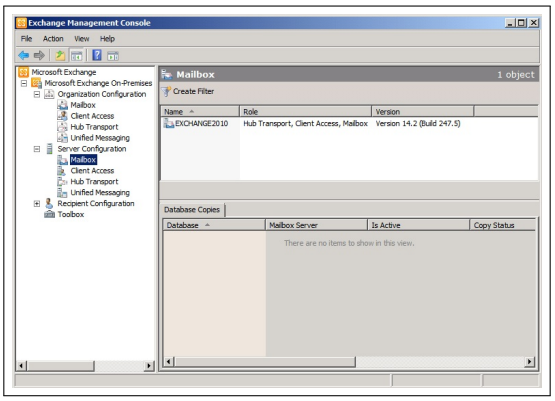

Figura 28: Unidad compartida de archivos

4.5.8. Servidor DNS

Este servidor proveerá a los usuarios del interior de la red corporativa la resolución de nombres. Disponer de este servicio en el interior de la red corporativa eleva el nivel de seguridad y hace más difícil que los usuarios sufran un ataque de **DNS Spoofing**, mediante el cual se alteran las direcciones IP de los servidores DNS de las víctimas ara que apunten a servidores maliciosos y poder tener el control sobre las consultas que se realizan.

El servidor DNS se configura sobre la máquina virtual **UPVCR.DNS**, provista con el sistema operativo **Windows Server 2008 R2**, con la dirección IP 192.168.0.12,

En Windows Server 2008 el servicio de servidor DNS está asociado al rol de **servidor Active Desktop**, por lo que en primer lugar se realiza la instalación y configuración del citado rol. Esta instalación se inicia desde el panel de administración del servidor, con la opción de agregar una nueva función.

Una vez agregada esta funcionalidad, se crea una zona de búsqueda directa para que el servidor DNS resuelva los nombres de los hosts a direcciones IP, y una zona de búsqueda inversa, encargada de realizar la conversión contraria.

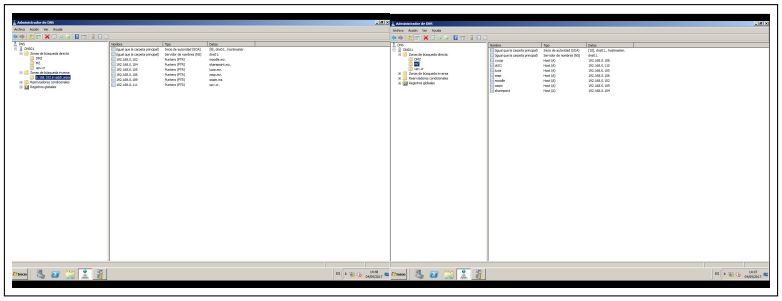

Figura 29: Búsqueda Directa e Inversa del Servidor DNS

5. Validación y pruebas del Cyber Range

Una vez se han implementado todas las máquinas y servidores con sus respectivos roles, la arquitectura queda de la siguiente manera con el router virtual como elemento central.

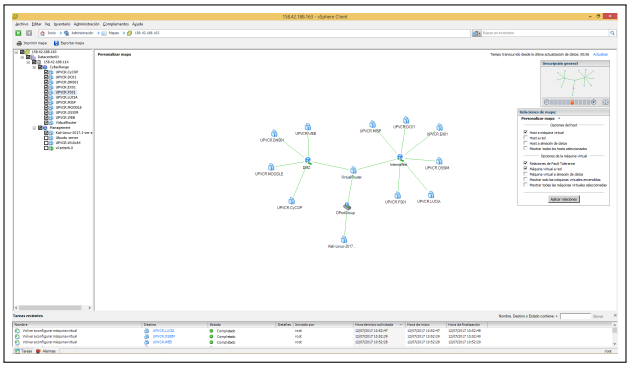

Figura 30: Conexión maquinas virtuales

El siguiente paso es realizar una comprobación para ver que el router virtual está desempeñando su función y está asignado las direcciones IP correctamente.

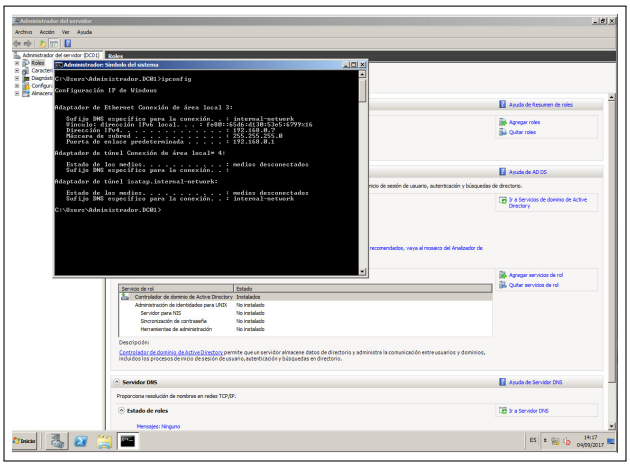

Figura 31: Asignación dirección IP a máquina virtual

Como se ve en la imagen 31 mediante el comando **"ïpconfig"** en una de las máquinas virtuales, el router le ha asignado una dirección IP dentro del rango 192.168.0.0/24 y nos indica que pertenece a la red interna. Otro punto importante para comenzar a incrementar la seguridad de las máquinas del Cyber Range es realizar un análisis de vulnerabilidades de los equipos. Esto se realiza de una forma sencilla con una de las funcionalidades de OSSIM.

Es importante que nuestros equipos tengan el menor número de vulnerabilidades posibles, ya que estas vulnerabilidades son las que aprovechan los intrusos para acceder a

los sistemas por medio de herramientas de explotación y hacerse con el control de nuestro equipo o bien para sustraer información.

OSSIM realiza un escaneo de cada equipo en busca de vulnerabilidades que posee en sus bases de datos y que se van actualizando periódicamente. Estos análisis se pueden realizar de forma sistemática cada cierto tiempo de intervalo designado o mediante una sola ejecución en ese momento, además es posible indicar las máquinas que a las que se quiere realizar el análisis de todas las que componen la organización.

Como ejemplo de ello, se procede a realizar el análisis de una máquina virtual, en concreto de la máquina WEB server, con sistema operativo Windows Server 2008 R2. Este proceso suele tardar entre 10-15 minutos en una solo sistema.

Una vez finalizado el análisis, se ofrece en informe en varios formatos para su visualización o descarga: html, csv, pdf, etc. En este informe nos indica entre otras cosas, la fecha a la que se ha realizado el análisis, los equipos analizados y el número de vulnerabilidades encontradas como se ilustra en la figura 32

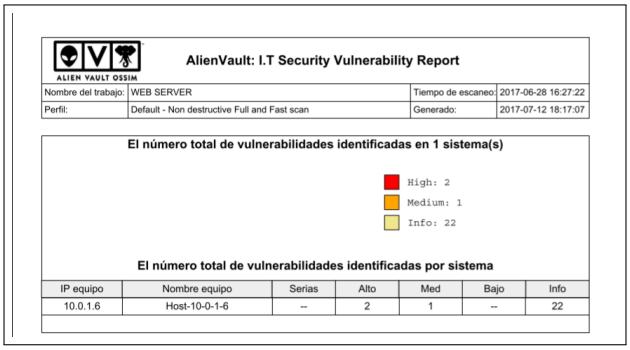

Figura 32: Informe vulnerabilidades Servidor Web

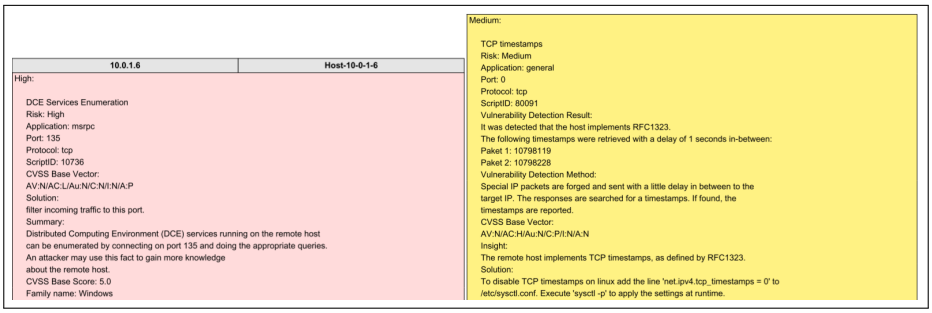

Figura 33: Vulnerabilidades detectadas Servidor Web

Como se indica en el informe (figura 33), se encuentran dos vulnerabilidades de riesgo alto (rojo), una de riesgo medio (amarillo) y las demás son advertencias o información que no suponen un riesgo para nuestro sistema.

Además, se detalla en la descripción que tipo de vulnerabilidad es, a que elementos afecta e incluso unas pequeñas recomendaciones de como solventarlas.

Otra de las pruebas que se llevan a cabo, es una de las técnicas que suelen aplicar los hackers en la primera fase de un ataque y es obtener información de la máquina o red a la que están atacando. Algunos de ellos utilizan **Zenmap**, que es una potente herramienta de Kali Linux que realiza un barrido de puertos, indicando cuales de estos puertos están abiertos, cerrados o indica el sistema operativo empleado, etc. Informaciones que puede resultar muy útiles a los hackers a la hora de preparas sus ataques.

En esta prueba se realiza un escáner al mismo equipo (Servidor Web), en apenas unos minutos la herramienta nos muestra los resultados (figura 34) con los siguientes datos obtenidos:

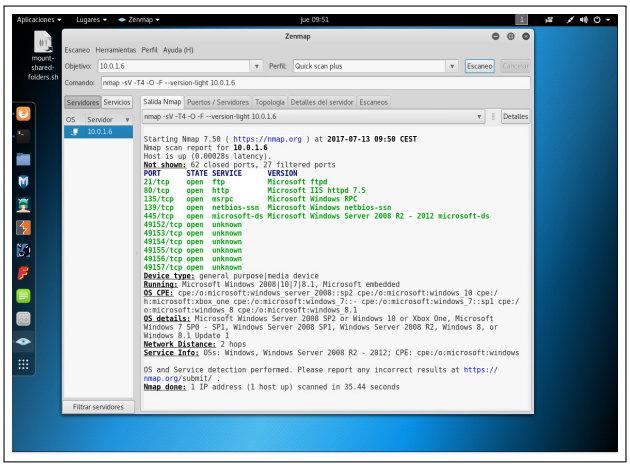

Figura 34: Escáner Zenmap a Servidor Web

- Listado de puertos abiertos con sus servicios asociados: 62 puertos cerrados, 27 filtrados y 11 abiertos.
- Sistema operativo detectado: Windows Server 2008 R2.
- Distancia de red: el equipo se encuentra a dos saltos de distancia.

Estas pruebas son importantes realizarlas a nuestros equipos para ver los puertos que tenemos abiertos y cerrar aquellos que no sean necesarios para las funciones de cualquier equipo y también para ver que es lo que se podría encontrar un intruso que intentase acceder a nuestros equipos y limitar así, los vectores de ataques que estamos proporcionando.

6. Conclusiones

Se ha implementado las fases iniciales del desarrollo de un Cyber Range completo, que se traducen en una gran cantidad de conocimientos adquiridos en diversas ramas tanto de la seguridad como en la informática.

Se han realizado multitud de tareas de virtualización mediante la plataforma VMware, con la implementación de todas las máquinas virtuales, además de virtualizar elementos de red como switchs, firewall o routers.

Se han llevado a cabo la creación y configuración de equipos informáticos como de servidores de correo, DNS, WEB, Administrador de dominios, servidor de archivos, etc.

En el campo de las comunicaciones, se ha realizado la implementación de una arquitectura red de tres zonas con políticas de seguridad adaptadas a cada zona. En la cual el elemento central es un router virtual al que se le han configurado todos los servicios necesarios de DHCP, NAT, DNS Forwarding, etc. Además de establecer las reglas y políticas del firewall para que se cumplan las reglas de acceso a las diferentes zonas de la red.

Se han configurado y testeado software de seguridad como la herramienta de monitorización OSSIM, mediante el análisis de vulnerabilidades, análisis de eventos SIEM, etc. Así como, la distro Kali Linux, plataforma creada para el pentesting y la seguridad de equipos, realizando distintas pruebas con la gran variedad de herramientas que proporciona.

En definitiva, se ha creado un Cyber Range operativo, escalable y flexible. Simulando un entorno real basado en la arquitectura de cualquier organización para el entrenamiento y desarrollo de habilidades de profesionales de seguridad así como para el testeo y validación de herramientas de seguridad.

Ha sido una tarea compleja y duradera debido a que los conocimientos previos a la realización del trabajo en estas materias eran escasos, pero ha sido gratificantes a la hora de ver los resultados obtenidos en el trabajo y el buen dominio de la herramienta y las técnicas para hacerlo posible.

7. Agradecimientos

En primer lugar, agradecer al director del presente trabajo, D. D. Manuel Esteve Domingo, por permitirme la posibilidad de realizar este interesante proyecto de investigación que me ha permitido adquirir una gran cantidad de conocimientos en diversas materias. Además darle las gracias por su apoyo y motivación.

Agradecer también al equipo de *Sistemas de Tiempo Real Distribuidos* por acogerme como uno más, resolver todas mis dudas y enseñarme parte de los extensos conocimientos de los que poseen, en especial dar las gracias a Francisco José Pérez Carrasco, sin duda su ayuda ha sido esencial en el desarrollo de este proyecto.

Para finalizar, acordarme de toda mi familia y amigos, que también han sido parte esencial llevar acabo este proyecto gracias a su apoyo y motivación. ¡Gracias a todos!

8. Referencias

Referencias

[1] Hootsuite. A study of internet, social media, and mobile use throughout the region. Technical report, We Are Social, 2017.

[2] Cyril Onwubiko. Security monitoring for protecting business and supporting cyber defense strategy. 2015.

[3] Annual cybersecurity report. Technical report, Cisco, 2017.

[4] Hewlett Packard Enterprise. Quickspecs hpe proliant ml110 generation9 (gen9)). https://www.hpe.com/h20195/v2/GetPDF.aspx/c04545445.pdf.

[5] Vmware vsphere datasheet. https://www.vmware.com/files/es/pdf/vsphere/VMW-vSPHR-Datasheet-6-0.pdf.

[6] Jose María González. Todo lo que necesitas saber sobre vmware vcenter server. https://www.josemariagonzalez.es/2013/11/20/todo-necesitas-saber-vmware-vcenter-server.html, 2013.

[7] Router os vyos. https://vyos.io/es/.

[8] Concise Courses. Hacker tools top ten. https://www.concise-courses.com/hacking-tools/top-ten/, 2017.

[9] Wikipedia. Zona desmilitarizada. https://es.wikipedia.org/wiki/Zona_desmilitarizada, 2017.

[10] CCN-CERT. Lucia. https://www.ccn-cert.cni.es/en/tools/lucia.html, 2017.

[11] GitHub. Misp (malware information sharing platform and threat sharing). https://github.com/MISP/MISP.