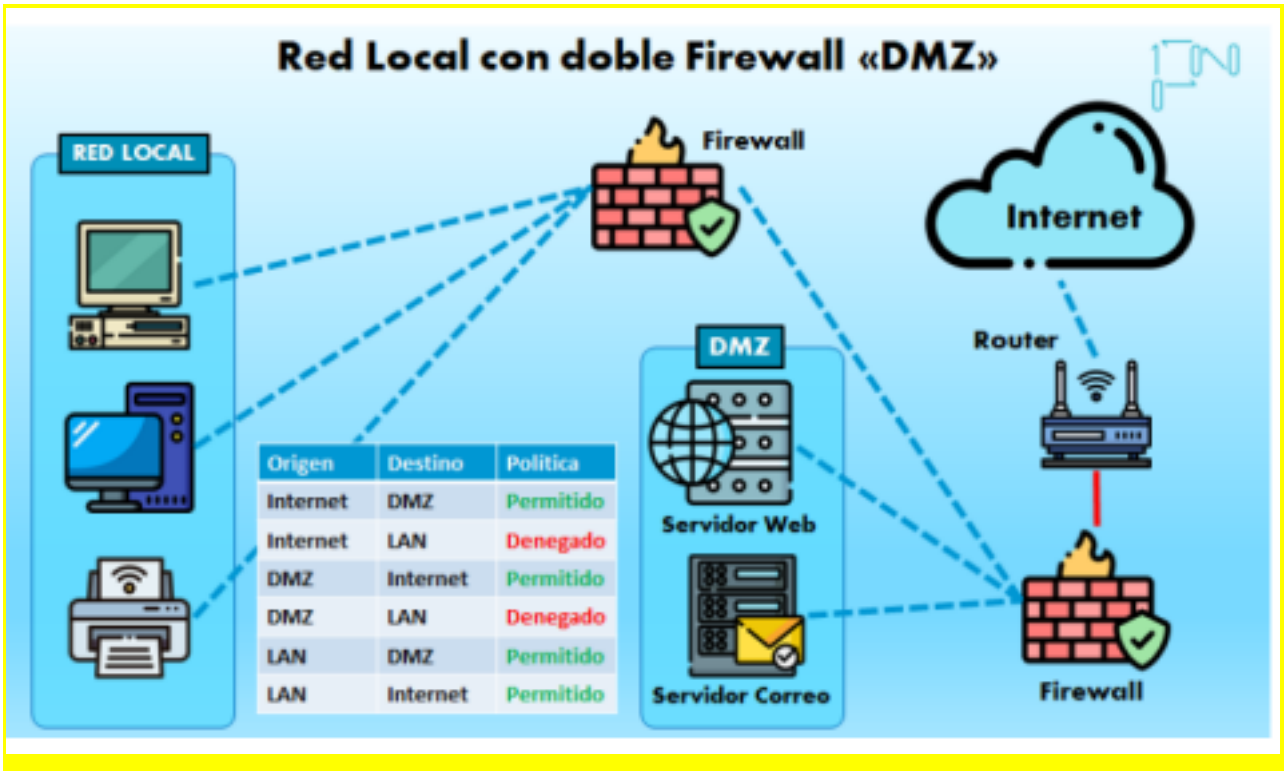
PRÁCTICAS OBLIGATORIAS BASTIONAJE DE REDES Y SISTEMAS

Revisado 19/05/2025 (09:00 horas) (Fco. Javier Melero López)

EN CONSTRUCCIÓN TODO EL CURSO



NORMAS A TENER EN CUENTA EN LA REALIZACIÓN DE CADA PRÁCTICA.

LEER CADA VEZ QUE SE REALICE LAS PRÁCTICAS

1. Se subirá un archivo de Google Docs compartido, para que yo pueda realizar anotaciones sobre el mismo documento (nada de fichero WORD, fichero PDF).
2. Hay que leer toda la práctica completamente antes de empezar a realizar nada.
3. En la presentación de cada práctica hay que **dejar el enunciado** en **color negro** tal y como yo os la entrego sin cambiar NADA-tamaño, tipo letra, etc.) de cada apartado, junto a sus capturas **concluyentes** o respuestas en color rojo, que creáis oportunas.
4. Las capturas concluyentes son imágenes obtenidas por vosotros donde se **marque** (con color amarillo y rectángulo/flecha) lo que yo tengo que fijarme para concluir que os habéis enterado del ejercicio/apartado en cuestión. En clase se dicen muchos ejemplos, pero podéis añadir las que creáis oportunas. Por ejemplo, una marca que siempre hay que realizar en el nombre del usuario, para que yo observe que es vuestra práctica. 5. Los terminales deben estar con fondo blanco y letra en negra.
6. Las capturas **concluyentes** tienen que ser claras y concisas de lo que se pregunta, en muchas ocasiones hay que demostrar de lo que se puede y de lo contrario, o mostrar el antes y el después para que se observe el cambio. En todas las capturas tiene que haber evidencia del usuario (**XXxx, pXXxx,fXXxx,dXxxx**) que realiza la acción.
7. Cada **ejercicio** empezará en una página y se intentará en la medida de lo posible que ocupe una única hoja (siempre y cuando las capturas se vean con claridad, y no sea necesaria varias capturas). Si hay un subapartado hay que ponerlo junto a su captura o su respuesta, no todo el enunciado al principio.
8. En la inmensa mayoría de los ejercicios/apartados no hay que escribir nada (a menos que ponga en palabras), sólo **CAPTURAS**. Vale más una captura concluyente, que muchas capturas que no digan nada. De hecho, en la inmensa mayoría de los ejercicios no es necesario escribir una palabra, sólo capturas.
9. Cuando un ejercicio/apartado no se realiza, hay que dejar siempre el enunciado y poner con claridad en color rojo EJERCICIO NO REALIZADO. Adicionalmente podéis añadir el motivo por el cual no se realiza. 10. Demuestre en todo momento sus conocimientos desde la bash del sistema operativo (operadores graves, &&, tuberías (|), tail -f, comandos adecuados, etc.) para realizar las evidencias. No quiero capturas del nano, y menos capturas completas sin marcas.
11. Firmar digitalmente (al principio) cada práctica entregada y realice la entrega mediante un archivo PDF. 12. En los diferentes enunciados ejercicios os encontrareis algunos textos en color rojo, son pistas para las evidencias (hacer todas las que dicen). Que no aparezca estos textos no significa que no se haga, si no que de vez en cuando os doy pistas, para que no se olviden.
13. Se recomienda realizar SNAPSHOT antes de empezar la práctica y al terminal la misma, y no estará nada mal en situaciones intermedias.

Se penalizará negativamente cada apartado/ejercicio en caso de no tenerse en cuenta estas normas. En caso de que sean muchas las penalizaciones no se corregirá directamente la práctica, obteniendo un valor de cero.

PRÁCTICA 1 (XXxx-practica1)
U.D.1. SSH. AUTENTICACIÓN. CONTROL DE ACCESO Y SEGURIDAD. (PARTE Nº 1)

CONEXIONES CIFRADAS USANDO CIFRADO ASIMÉTRICO, CONEXIÓN CLIENTE-SERVIDOR. HERRAMIENTAS PARA CONTROLAR LAS CONEXIONES.

1. Explique **con sus propias palabras** en relación al cifrado, poniendo ejemplos reales explicados en clase y algunas imágenes descriptivas, cuando lo crea oportuno: ***(0,5 puntos)***
    a. ¿En qué consiste el cifrado asimétrico?
    b. ¿En qué se basa la seguridad del cifrado asimétrico, para que se lleve usando durante muchos años y haya hecho posible el avance de Internet en las últimas décadas?
    c. ¿En qué se diferencia del cifrado simétrico? Ponga ejemplos de uso.
    d. ¿Para qué se usa el cifrado asimétrico en las conexiones con servidores SSHD?

2. Realice la instalación de servidor openssh-server en Servidor Ubuntu Server. *(#apt get install openssh-server)*, y realice las siguientes evidencias: **(0,5 puntos cada uno)**
    a. Use comandos adecuados para comprobar que el servidor SSHD está funcionando y está escuchando en el puerto por defecto 22. *(#netstat -putan | grep 22 && systemctl status ssh)*, y demuestre que ningún cliente está conectado. Posteriormente, realice la instalación de apache2, mysql-server y vsftpd y demuestre que esos servicios están escuchando *(netstat -putan | grep LISTEN).*

    b. Conecte desde un cliente ssh GUI Windows anfitrión (putty, BitTunnelier, MobaTerm.) por primera vez usando el usuario XXxx (no es necesario en este caso introducir la contraseña para comprobar el ejercicio:
        - Demuestre que hay un usuario conectado desde el cliente de Windows, con diferentes herramientas. *(ifconfig, netstat -putan | grep 22 | grep ESTABLISHED (en el cliente y en el servidor), tcpdump port 22, tcpdump port 22 and host XX, iptraf-ng).*
        - ¿En qué fichero y directorio se descarga esa llave pública/fingerprint? Liste el contenido del fichero y marque cual es longitud en número de bits y algoritmo.
        - ¿Qué pasa si borramos este fichero o borramos su contenido? Borre y comprueba que ocurre.

    c. Responda a lo mismo que en el ejercicio anterior, pero ahora desde un equipo **cliente en modo comando (POWERSHELL o CMD).** En este caso puede loguearse con el usuario XXxx:
        - Muestre dicha conexión realizada con diferentes herramientas.
        - ¿Qué características tiene esa llave pública (longitud-nº de bits y algoritmo)?
        - ¿Dónde se ha guardado esa key/llave pública en el equipo cliente?
        - ¿Qué pasa si borramos este fichero o borramos su contenido? Borra y comprueba que ocurre.

d. Realice una conexión desde el cliente en modo comando desde Ubuntu Desktop y demuestre que se ha producido la conexión.

e. ¿Es la misma key/llave pública la que se ha descargado en los tres clientes diferentes? Responda con palabra: ¿Por qué ocurre eso? ¿en qué equipo y en qué lugar se queda siempre la key/clave/llave privada?

REFORZANDO CONOCIMIENTO COMUNICACIONES CIFRADAS USANDO CIFRADO ASIMÉTRICO CON HTTPS

3. En relación a los servidores webs en Internet y su protocolo https, realice una conexión al servidor https://www.unicajabanco.es/, desde un **navegador web** predeterminado. Demuestre a las siguientes preguntas relacionadas con el cifrado asimétrico de la conexión con UNICAJA: **(1 punto)**

▪ **RELACIONADO CON LA CONEXIÓN A SERVIDOR https://www.unicajabanco.es**

a. ¿Versión y número de serie del certificado digital?
b. ¿Qué autoridad certificado internacional certifica esta llave pública? Busque alguna información relevante en relación a esta empresa (con palabras).
c. ¿Con qué algoritmo y número de bytes se ha firmado el certificado?
d. En relación a la clave/key/llave **pública**:
    a. Algoritmo usado.
    b. Tamaño en número de bytes.
    e. ¿Cuándo fue emitido y cuando caduca? ¿Está en vigor entonces?
    a. ¿Cuál es la llave pública? Demuestre que el nº de bytes que aparece coinciden.
f. En relación a la **huella digital** o fingerprint (hash con el que se firma la llave pública).
    a. Algoritmo usado.
    b. Tamaño en número de bytes.
    c. Fingerprint
g. A continuación, realice la conexión desde otros dos navegadores distinto al anterior (Opera, Firefox Chrome, etc.), y demuestre mediante una única captura, que todas las llaves públicas que aparece son iguales en cada navegador. ¿Por qué cree que ocurre esto *(palabras)*? ¿Le recuerda esto algo a lo que ha ocurrido con el cifrado en comunicaciones SSH *(con sus palabras)*?
h. ¿Qué diferencias hay entre la "la descarga de la llave pública del servidor ssh, y la de "servidor https"?

****** Lea las medidas de seguridad que el banco Unicaja.es les proporciona a los usuarios. Son muy interesante.***

REDUCIENDO LAS PROBABILIDADES DE EXPOSICIÓN ATAQUES. CONEXIÓN CLIENTE SERVIDOR

4. Sobre el fichero de configuración del servidor Ubuntu Server *(/etc/ssh/sshd_config)* modifique las siguientes opciones y realice diferentes conexiones variadas (cliente Windows (CMD/Powershell), GUI de

Windows) para demostrar lo que realiza cada una de las opciones. Los cambios a realizar son **(0,5 puntos cada opción)**:

a. Active el banner (Banner /etc/issue.net) para que muestre información cada vez que se conecte y escriba en dicho fichero el siguiente contenido (Bienvenido al servidor Ubuntu server del módulo de Bastionaje

de redes, del alumno XXxx. Está prohibida la conexión si no es Administrador de este sistema informático).

b. Pruebe a conectarse desde cualquier cliente con el usuario root. Haga todo lo necesario para que pueda conectarse con el usuario root antes y después de cambiar las opciones. *(PermitRootLogin) (iptraf-ng, # tcpdump port 22)*

c. Sólo se permite dos intentos para loguearse (*MaxAuthTries 2*). Pruebe a realizar tres intentos (fallando la contraseña 3 veces).

d. Demuestre para que vale la opción. Use comando date para evidenciar. *(LoginGraceTime 60) e.* Sólo se permiten **dos** bash abiertas a la vez. (MaxStartups 2). Cuidado con algunos programas GUI que abren varias sesiones a la vez. *(netstat putan | grep 22 | grep ESTABLISHED,iptraf-ng)*

REDUCIENDO LA PROBABILIDADES DE EXPOSICIÓN DE ATAQUES. SEGURIDAD DEL SERVICIO DIRECTAMENTE.

Siguiendo con las opciones de configuración del servidor SSHD de Ubuntu Server: **(1 punto cada opción)** ******* En estos tres ejercicios es importante evidenciar desde la IP del cliente que se realiza la conexión.***

5. Demuestra que permita conectarse desde una determinada IP (por ejemplo, equipo IP anfitrión), pero no desde otra IP (Ubuntu Desktop), y al revés, jugando además con diferentes usuarios (XXxx, root, pXXxx, etc.). *(AllowUsers y DenyUsers)* ~~*(GroupUsers y Denygroups)*~~. Se deja al alumno que elija la configuración que desee de IP/red/usuario, adaptada a las IPs de su casa/trabajo.
6. Cambie el puerto de escucha del servidor SSHD a 2222 para conexiones vía localhost y 22 para conexiones externas (ListenAddress) (tarjeta de red) (#netstat -putan | grep 22 | grep LISTEN , tcpdump -i lo port 2222, iptraf-ng, etc.). Realice las evidencias suficientes para demostrar este hecho para conexiones exitosas y no exitosas.
7. Configure /etc/hosts.deny (ALL:ALL), y realice algunas actuaciones usando acl de TCP-Wrappers (/etc/hosts.allow, /etc/hosts.deny), para permitir algunos equipos (se deja libertad al alumno desde el número de hosts clientes desde donde probar). Las actuaciones tienen que mostrar que se "juega" con:
   a. Comprobar que esta activada TCP-Wrappers para los servicios SSHD y vsftfp, pero no para mysql server y apache2).
   b. Servicio SSHD con hosts individuales, subredes, localhost.
   c. Servicio vftpd con hosts individuales, subredes, localhost.
   d. Retoque el fichero /etc/hosts.deny, para Denegar alguna conexión pero loguear el acceso de un intento de "ataque" (poner mensaje personalizado). *(tail -f ficheroXXxx.log).*

DOBLE FACTOR DE AUTENTIFICACIÓN (2FA) USANDO TOTP (Time-based one-time Password)

8. Realice todo lo necesario para que se pueda entrar al servidor SSHD de Ubuntu Server mediante usuario/contraseña doble Autenticación (TOTP, contraseña de un sólo uso por tiempo), usando para ello la herramienta Google Authentificator. **(0,5 puntos)**. Se deja al alumno que realice las capturas de evidencias que desee (no realizar manual, sólo demostrar que os funciona, fichero de configuración, app).

CRITERIOS DE EVALUACIÓN	
2.b	Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.
2.c	Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
2.d	Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques
3.b	Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
3.c	Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.c	Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

PRÁCTICA 2 (XXxx-practica2)
U.D.1. SSH. AUTENTICACIÓN. CONTROL DE ACCESO Y SEGURIDAD. (PARTE Nº 2)

CIFRADO ASIMÉTRICO: AUTENTIFICACIÓN MEDIANTE CIFRADO ASIMÉTRICO

Relacionado con el servidor SSHD de Ubuntu Server, realice las siguientes operaciones:

1. Genere un único par de llaves (XXxx, XXxx.pub***, será usado por usted durante todo el curso***) en el S.O. Ubuntu Server, de 2048 bits, sin contraseñas y las guarda inicialmente en el directorio /root/keys/ e introduzca dicha llave pública para poder realizar conexiones SSH a este servidor Ubuntu Server (cat XXxx.pub >> /root/.ssh/authorized_keys, cat XXxx.pub >>/home/XXxx/.ssh/authorized_keys). **(0,5 puntos cada uno)**. Compruebe que puede conectarse al servidor Ubuntu server, usando la llave privada, desde:
    a. Localhost. (No es necesario copiar la llave privada en ningún lugar, ya que la tenemos), tanto como usuario XXxx comoo root *(ssh -i /root/keys/llaveprivada XXxx@localhost, ssh -i*

/root/keys/llaveprivada root@locahost) (netstat -putan |grep ESTABLISHED)

b. Cliente Microsoft Windows mediante comando. Recuerde que previamente hay que copiar la llave privada en Windows) (#scp XXxx.pub root@IP:/root/keys/llaveprivada c:\Usuarios\Desktop\MisKeys\llaveprivada)

c. Cliente Microsoft Windows (GUI) (Mobeterm) desde el usuario root. Recuerde que tiene que importar la llave privada en la aplicación GUI Mobaterm.

d. Cliente Ubuntu Desktop en modo comando. Recuerde que previamente hay que copiar la llave privada en algún directorio de Ubuntu Desktop (le recomiendo /root/MisKeys/)

e. Cliente APP de su smartphone (Juice SSH, o la que desee) desde usuario XXxx. Recuerde que tiene que importar la llave privada en la aplicación de su APP.

*****Como has podido comprobar la llave pública sólo la hemos puesto en el servidor al cual nos conectamos (fichero authorized_keys) una única vez. Sin embargo, es la llave privada la que va con nosotros en todo momento, y la que tendremos que tener mucho cuidado con ella.***

2. A continuación, vamos a dotar a todos los demás S.O del servicio SSHD, además del servidor Ubuntu Server. Para ello, usaremos la misma llave pública (y por tanto la misma llave privada para poder autentificarnos). Instale SSHD y modifique el fichero authorized_keys (de la forma que cree oportuno), para que podamos conectarnos mediante un cliente a los servidores siguientes.

   a. Servidor SSHD en Ubuntu Desktop **(1 punto)**
   b. Servidor SSHD de Windows. **(1,5 puntos)**
   c. Smartphone. **(1 punto).**

   Aclaración: Es la primera tarea que hay contenidos no explicados en clase (instalación de servidor SSHD en Windows y smartphone), pero en la mayoría de los casos es muy fácil realizarlo. El fichero de configuración se suele llamar de igual forma.

Para evidenciar este ejercicio, elija las capturas que crea oportuno para demostrar que:

- Se ha instalado correctamente. (netstat, ss, systemctl …., etc.).
- Podemos loguearnos mediante usuario/contraseña (tcpdump, netstat, iptraf, etc.). • Se ha introducido correctamente el contenido de la llave pública en authorized_keys del servidor en cuestión.
- Se ha hecho una conexión desde otro cliente (comando, GUI) para probar que funciona la autentificación mediante la llave privada.

******* Tendrá que realizar esta operación cada vez que tengamos un nuevo servidor en este curso. Puede usar el comando ssh-copy-id desde Ubuntu Server, para meter la clave pública en cada uno de estos nuevos servidores SSHD. Aunque se recuerda que hay muchas más formas (scp, winscp, cat ….).. .***

CIFRADO ASIMÉTRICO: AUTENTIFICACIÓN MEDIANTE LLAVES Y DOBLE FACTOR DE AUTENTIFICACIÓN (2FA)

3. Realice todo lo necesario para que se pueda entrar al servidor SSHD, usando a la vez llave privada y usando

doble Autenticación (TOTP, contraseña de un sólo uso por tiempo), usando para ello la herramienta Google Authentificator (KbdInteractiveAuthentication yes).

Se deja al estudiante que elija las capturas necesarias para demostrar que le funciona correctamente. Se recomienda que siga los pasos del material proporcionado al alumno. **(0,5 punto)**

REDUCIENDO LAS PROBABILIDADES DE EXPOSICIÓN ATAQUES. CONEXIÓN CLIENTE SERVIDOR

4. Cambie (sólo en el servidor Ubuntu Server) para que se pueda únicamente autentificar mediante el uso de cifrado asimétrico, no por usuario/contraseña (demuestre que no se puede). A partir de ahora, no se puede entrar con usuario/contraseña en todo el curso. (PasswordAuthentication no) **(0,5 puntos)**

SACANDO PROVECHO A HERRAMIENTAS VARIAS RELACIONADAS CON CLIENTE SSH.

5. Realice las siguientes comprobaciones siempre **desde cliente SSH Ubuntu Desktop (no desde otro equipo)** en modo comando conectándose al servidor SSHD de Ubuntu Server, usando **siempre** autenticación por cifrado asimétrico. **(0,25 puntos cada uno)**

   a. Compruebe que puede copiar *(# scp -i llaveprivada …..)* un archivo desde un cliente al servidor(XXxx.iso). b. Compruebe que puede copiar (*#scp -i llaveprivada …..*) un archivo desde el servidor al cliente (XX.xx 1.iso). Al revés, que en el ejercicio anterior.

   c. Realice la actualización de fuentes, actualizar el S.O, instalar apache2 y reiniciar el servicio de apache2, sin tener que entrar al sistema operativo, usando un único comando (&&). Posteriormente, compruebe que puede conectarse al servidor web (http://IP, wget), para saber que ha tenido éxito.

   d. Compruebe que puede montar mediante sshfs el sistema de archivos completo del servidor Ubuntu Server. (ls -al, ll, y df -ah, cat /etc/mtab). Desmonte el sistema de archivo montado en el apartado anterior y vuelva a comprobar.

PROBANDO TODO LO APRENDIDO CON HERRAMIENTAS DE SSH. AUTOMATIZACIÓN DE TAREAS (DEMONIO CROND). ATACANDO A MUCHOS EQUIPOS A LA VEZ.

6. Realice un script de Linux (/root/Bucle/XXxx-SSH.sh) que se ejecute en un S.O. Linux (por ejemplo, Ubuntu Desktop) que gestione como **mínimo** dos servidores (Ubuntu Server y crear otro S.O. para esta práctica) y que usando **siempre** autenticación por cifrado asimétrico (NO CONTRASEÑA) y usando un fichero de texto ipXXxx.txt, realice las siguientes tareas: **(0,25 puntos cada apartado)**

   a. Actualizará fuentes, actualizará los S.O y mostrará los dos últimos usuarios (/etc/passwd) que se han creados en ese S.O.

   b. Comprobará el tamaño de disco duro libre (únicamente del disco duro raíz, no otros) que tiene y la memoria RAM que está usando actualmente.

   c. Copiará (#scp …) desde el equipo que se ejecuta el script, un fichero (por ejemplo, este mismo script) a esos S.O remotos.

   d. Copiará (#scp ….) el fichero /var/log/auth de esos S.O. remotos a este S.O. (para que no machaque unos

con otros hay que cambiar auth**IP**.log)

e. Montará (#sshfs . . . .) el directorio /root de cada uno de los S.O. remotos en el equipo que se ejecuta el script. Hay que crear el directorio con la IP (#mkdir …… 2>/dev/null) donde se montará dicho directorio remoto.

f. Cambiará una opción del fichero de configuración del servidor apache de los S.O. (por ejemplo, cambiar el puerto de escucha, reiniciar el sistema y comprobar que funciona en el nuevo puerto) (# sed XXXXXX). g. Como medida de seguridad adicional, cada vez que se ejecute este script se generará un par de keys/llaves (privada/pública) nuevas e incluirá la llave pública generada en el fichero authorized_keys de S.O. remoto (#ssh-id-copy….). Realice una nueva prueba para comprobar que se puede autentificar con la **nueva** llave privada generada.

h. Enviará un mensaje de correo electrónico (estará en el fichero ipXXxx.txt) con lo que se ha realizado correctamente y con lo que no ha funcionado.

Se tendrá en cuenta para la nota de este ejercicio:

- Uso técnico en la explicación del script y Calidad del video explicativo **(0,5 puntos)**
- Claridad en el diseño del script, uso de variables, uso de mensajes clarificadores, etc.

Este ejercicio se corregirá montando un video (**NO grabado con móvil, use Canta**)

donde:

• El vídeo tendrá **máximo 5 minutos** de grabación y el alumno debe explicar (tiene que escucharse) todas las comprobaciones que realiza el script.

• Aparezcan varios terminales donde se demuestre los resultados y comprobaciones. • Existen algunos "echo" en el script para explicar que se está realizando o que no se ha realizado. • Introducir paradas (sleep) para que dé tiempo a ir explicando correctamente lo que va realizando. Hacer lo más personal (XXxx, etc.) posible el script.

• **En ningún momento** puede solicitar por pantalla al usuario, ya que supuestamente este script se ejecutará sin intervención de un usuario.

• Se debe intentar que las comprobaciones sean hechas en el mismo script, por ejemplo, cuando se monta por sshfs, que aparezca el df del servidor remoto, etc., haciendo uso de && y ||.

En el video se debe explicar y en este orden:

• Partes del script que no te ha funcionado o no se ha realizado.
• Muestra del fichero script y fichero con las IP's con los correos electrónicos.
• Mostrar el script e ir explicando cada opción con las comprobaciones que se han realizado en cada apartado.

CRITERIOS DE EVALUACIÓN	
2.b	Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las

	principales vulnerabilidades y tipos de ataques.
2.c	Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
2.d	Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques
3.b	Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c.	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs) de un cortafuegos.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.c	Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

PRÁCTICA 3 (XXxx-practica3)
U.D.2. REDES DE COMPUTADORAS SEGURAS (I). SEGURIDAD A NIVEL DE HOST. FIREWALL DE SERVIDOR

SCRIPTS. HOST SIN CORTAFUEGOS. CONOCIENDO LA TARJETA LOOPBACK.

1. **(SERVICIOS INNECESARIOS, MONITORIZACIÓN)** Partiendo de un servidor Ubuntu Server recién instalado, actualizado, con la hora correctamente (y huso horario), realice las siguientes operaciones: a) Instalación de SSHD (configurado para entrar con llave privada por su comodidad), apache, vsftpd, mysql-server (se permitirá conexiones desde el exterior, no sólo localhost). Se deberá mostrar evidencias de que están escuchando (netstat -putan | grep LISTEN) dichos servicios instalados. ¿Podrías decir con tus palabras si hay algún otro servicio/demonio más instalado en este servidor, y a qué se dedica cada uno de esos servicios? **(0,5 puntos)**

   b) Evidencia de que desde cliente Ubuntu Desktop se produce conexiones remotas (netstat -putan | grep ESTABLISHED, ss, tcpdump, iptraf-ng) a cada uno de estos servicios del servidor Ubuntu Server instalados en apartado anterior, además de poder hacerle ping. Intentar realizar un script que haga todas las comprobaciones desde el cliente o use && para las evidencias. **(0,5 puntos)**

   c) Evidencia qué desde Ubuntu Server, actuando como **cliente**, puede: **(0,5 puntos)**

      i. Resolver dns con servidores remotos ($ ping www.diariosur.es)
      ii. Actualizar hora del S.O y de hardware. (#ntpdate hora.rediris.es && sleep 10 && hwclock -h)
      iii. Hacer ping a un equipo exterior ($ ping 8.8.8.8).
      iv. Descargarse una web remota (# wget ..)
      v. Enviar un correo (#echo hola | mailx -s "Asunto" XXx@gmail.com) (puerto 25).
      vi. Conectarse por ssh algún equipo remoto, como por ejemplo Ubuntu Desktop/Windows/Smartphone.
      vii. Entrar en el servidor mysqld vía **localhost**. (netstat -putan | grep ESTABLISHED, ss, tcpdump,

iptraf-ng)

**** Haga un snapshot a la máquina virtual Ubuntu Server, con el nombre XXxx-Dia y escriba lo que contiene esos cambios. Muestre dicho snapshot,*

INICIANDONOS EN IPTABLES y SCRIPTS. CORTAFUEGOS DE SERVIDOR. CONOCIENDO LA TARJETA LOOPBACK.

Consideraciones a tener en cuenta:

- En este ejercicio además de los "sensores" usados en prácticas anteriores, tendréis que tener en cuenta #iptables -L -n -v –line-numbers, #iptables -L -n -v | grep …. , tail -f /var/log/kern….
- Realice un script (firewall-XXxx.sh) para la ejecución de las reglas de iptables.
- **Este es típico ejercicio que hay que probar que se puede y que no se puede.** Ajustar a cada ejercicio esta consideración.

- Es importante poner comentarios mediante -m comment --comment "Comentarios ….", para evidenciar cada apartado.
- En alguno de los apartados (a elección del alumno) hay que demostrar el uso de los contadores para evidenciar lo que está ocurriendo.

2. **(INICIANDO SCRIPTS)** Realice (y ejecute para evidenciar) un script de Linux (firewall-XXxx.sh) que se arranque en el inicio del S.O del servidor Ubuntu Server (con /etc/rc.local o mejor como un servicio) con las siguientes consideraciones **(0,5 puntos cada uno)**

   a) Se borren los contadores (-Z) y todas las reglas (-F) que estuvieran cargadas en el kernel del S.O. b) Las políticas por defecto sean DROP tanto en INPUT, OUTPUT y FORWARD en todo momento. En este momento de la práctica todo lo evidenciado en el ejercicio número 1 debe fallar. Demuestre esto con los contadores de DROP.

   c) Se permite al interfaz loopback conexiones entrantes y salientes al servicio mysqld, pero **no** a ningún otro servicio (ssh, web, vsftpd, ping). **Dejar posteriormente que se permita todo por la tarjeta loopback.** d) No se permitirá **conexiones entrantes,** pero se logueará (-j LOG) con el prefijo ("Intentos-ataque-SSH Server-XXxx", "Intentos-ataque-Web-Server-XXxx", "Intentos-ataque-mysql-XXxx") en el fichero /var/log/iptablesXXxx.log. Provocar dichas conexiones "fallidas" mediante hping3, nmap -S, ssh, ftp, wget, etc., desde cliente Ubuntu Desktop. Realizar conexiones para que se llene el fichero log.

****** Haga un backup de este script final (Firewall-XXxx-v1.0.sh). Muestre, aunque no se valorará. ******
Haga un nuevo snapshot para tener guardado este nuevo estado. Muestre, aunque no se valorará.

3. **(REGLAS DE FILTRADO OUTPUT)** Continuando con el script anterior y con las **respuestas (INPUT)** a las conexiones salientes(respuestas a esos OUTPUT),tienen que ser **exclusivamente** para conexiones establecidas o relacionadas, demostrar paso a paso que: **(0,5 puntos cada uno)**

   a) Únicamente puede hacer ping (ICMP) al exterior, pero no permite descargar web, resolver DNS, ni poder actualizar la hora (# ntpdate).

b) Resuelve DNS y ping, pero que no deja actualizar el S.O ni puede actualizar la hora del S.O. c) Resuelve DNS y ping y permite actualizar el S.O. **exclusivamente** (IP servidores de Ubuntu), pero no permite descargar ninguna web, ni puede actualizar la hora del S.O.

d) Resuelve DNS y ping, y que se puede actualizar el S.O. y descargar web (http/https) pero no se permite actualizar la hora del S.O.

e) Además, que se permita actualizar la hora del S.O., pero **exclusivamente** con un servidor por su IP (elija usted dos servidores horarios, uno de España y otro de fuera de España).

f) Además, que se permita enviar correos salientes con el comando mailx o el que desee.

***** Haga un backup de este script final (Firewall-Xxxx-v2.0.sh). Muestre, aunque no se valorará. ******
Haga un nuevo snapshot para tener guardado este nuevo estado. Muestre, aunque no se valorará.

4. **(REGLAS DE FILTRADO INPUT)** Continuando con el script anterior y que las **respuestas (OUTPUT)** a las conexiones entrantes tienen que ser **exclusivamente** para conexiones establecidas o relacionadas. Se **recomienda** que se prepare un script para Linux (XXxx-cliente.sh) para ejecutar la prueba completa de servicios para conexiones OUTPUT. Demostrar paso a paso.

a) Que se puede realizar ping a este servidor. **(0,5 puntos).**

b) Demostrar que se permite la conexión al servidor SSHD (no web ni vsftpd, ni mysql, ni apache), pero de la siguiente manera (cada apartado se demuestra por separado:

i. Desde la IP concreta de un determinado cliente. **(0,5 puntos)**
ii. Lo mismo que el anterior, pero que además se permita sólo 3 conexiones de esa IP. **(0,5 puntos)**
iii. Desde la MAC concreta de un determinado cliente. **(0,5 puntos)**
iv. Desde la red concreta en la que se encuentra Ubuntu Server. **(0,5 puntos)**
v. A una determinada fecha y hora del día (inventarse dicho horario). **(0,5 puntos)**

Por último, deje que permita la conexión desde cualquier cliente y a cualquier hora del día

c) Que se permita también conexiones al servidor web (http), vsftpd y mysql. **(0,5 puntos)**

**** Haga un backup de este script final (Firewall-XXxx-v3.0.sh).*
**** Sería bueno realizar un snapshot final de este servidor Ubuntu Server. Muestre, aunque no se valorará.*

AMPLIACIÓN/INVESTIGACIÓN

- Realizar el mismo script (.bat), pero ejecutando desde un cliente Microsoft Windows, "atacando" los dos equipos (o más Linux).
- Realizar el mismo ejercicio, pero sobre S.O. Windows 10/11 o Windows Server. Puede implementar otros protocolos interesantes (RDP, VNC, SAMBA, etc.).
- Configuración y uso de HoneySSH.
- Uso de Snoopy.
- Cualquier cosa relacionada con lo visto en esta práctica, que no haya sido explicado por el profesor. Otros tipos de ataques, etc.
- Eliminación de protocolos innecesarios en S.O. Microsoft Windows.

CRITERIOS DE EVALUACIÓN

5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c.	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.a	Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
7.c	Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

PRÁCTICA 4 (XXxx-practica4)
U.D.2. REDES DE COMPUTADORAS SEGURAS (I). SEGURIDAD A NIVEL DE HOST. FIREWALL DE SERVIDOR. IDS

***** En esta práctica, el alumno debe realizar TODAS las comprobaciones que conozca y se hayan implementado a lo largo del curso. No bastará con comprobaciones simples. Se trata de demostrar todo lo que se sepa a lo largo del curso.**

IPTABLES CON PORT-KNOCKING. HERRAMIENTA ESPECÍFICA.

1. **(2,5 puntos)** Usando exclusivamente iptables, configure el servicio sshd de Ubuntu Server, para que se active llamando a los puertos 7777, 8888, 9999. Se deja al alumno que muestre las evidencias necesarias (netstat, watch iptables -L -n -v, creación de reglas, apertura de puertos poco a poco, etc).

2. **(1,5 puntos)** Haciendo uso de la herramienta port-knocking, configure el servicio sshd de Ubuntu Server, para que se active llamando a los puertos 7770, 8880, 9990 y se desactive realizando la llamada en orden inverso. Se debe configurar un timeout máximo de 30 minutos una vez abierto el servicio.

OTRAS HERRAMIENTAS RELACIONADAS CON IPTABLES

3. **(FailToBan-IDS)** Usando la herramienta failtoban, realice las siguientes actuaciones en el servidor de Ubuntu Server, para evitar problemas de ataque. Mínimo tiene que demostrarse:

   a) Instalación y comprobación de servicio fail2ban. **(0,5 puntos)**
   b) Haciendo uso de la configuración por defecto (/etc/fail2ban/jail.conf): **(2 puntos)**

      i. Evidenciar que se produce un bloqueo después de X intentos fallidos desde Windows anfitrión mediante comando ssh manualmente (o bucle), según configuración por defecto. Fichero /var/log/auth, cliente de fail2ban (fail2ban-client status sshd).
      ii. Evidenciar que se produce un desbloqueo automáticamente pasado el tiempo determinado en el

fichero por defecto.

iii. Evidenciar el bloqueo de nuevo, y desbloquear mediante comando (#fail2ban-client unban). b) Haciendo uso de una configuración personalizada (/etc/fail2ban/jail.local) (nº de intentos de 10 por cada minuto y banear durante 3 minutos, usando iptables (#watch iptables -L -n -v): **(2 puntos)** i. Evidenciar que se produce un bloqueo después de 10 intentos mediante fuerza bruta (#nmap - -script ssh-brute -p 22 <IP>) desde Ubuntu Desktop y se añaden reglas de iptables (#watch iptables -L –n -v), Fichero /var/log/auth, cliente de fail2ban (fail2ban-client status sshd). ii. Evidenciar que se produce un desbloqueo automáticamente pasado el tiempo determinado en el fichero por defecto.

iii. Evidenciar el bloqueo de nuevo, y desbloquear mediante comando (#fail2ban-client unban IP). iv. Realice lo anterior para quitar la regla usando comando iptables manualmente.

c) **Investigar** y evidenciar, la configuración para proteger mediante fail2ban contra fuerza bruta en autenticación básica vía web (http/https), mediante el filtro auth-filter **(1,5 puntos).**

CRITERIOS DE EVALUACIÓN	
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c.	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.d	Se han implementado contramedidas frente a comportamientos no deseados en una red.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.c	Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
7.d	Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.

PRÁCTICA 5 (XXxx-practica5) – UD 4. U.D.3. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). SEGURIDAD PERIMETRAL. IPTABLES.

SEGMENTACIÓN DE RED FÍSICA Y ENRUTAMIENTO ENTRE REDES. ZONA DMZ. PRACTICA 5.1

1. **(2 puntos) (EQUIPO FIREWALL)** Montaje de un servidor Ubuntu Server (conexión únicamente por SSHD y conexión por key pública), con cuatro tarjetas de red con las siguientes características:
   - Nombre del servidor: firewall-XXxx. Para simplificar XXxx puede ser covadonga, zambrana, alvaro, etc. - Nombre de interfaz para **usar en los scripts** (wan?, lan?, wlan? y dmz? – donde ? es el número de clase, previamente informado al alumno en clase (/etc/udev/rules.d/70-persistent-net.rules).

- Las Ip ((ifconfig, ping, dmesg, fichero de configuración)/Redes del firewall-XXxx, serán las siguientes: ▪ (Modo Bridge) Red WAN, red roja o Internet, por DHCP o IP fija si se encuentra usted en casa (tracepath, route)
  - ▪ (Red 1) Red DMZ, red naranja, ip fija 10.0.10?.1/24. (Red Privada Tipo A)
  - ▪ (Red 2) Red Intranet, red verde o zona lan. ip fija 172.16.10?.1/24. (Red Privada Tipo B)
  - ▪ (Red 3) Red WLAN, red azul, 192.168.10?.1/24. (Red Privada Tipo C).

2. **(EQUIPOS DE LAS SUBREDES)**
   - **(2 puntos)** Montaje de **tres** máquinas virtuales Ubuntu Server (uno por cada red, 512 MB de RAM), con servicio SSHD instalado con autentificación por cifrado asimétrico, net-tools instalados, actualizadas, en redes privadas (LAN segment de VM) con las siguientes IP y con los siguientes servicios adicionalesinstalados.
     - ▪ Red 1: nombre (dmz-US-Xxxx), IP (10.0.10?.2/24), Gateway (10.0.10?.1) (ifconfig, route, fichero de configuración)
       - Servidor apache2 escuchando en el puerto 80, con php instalado.
       - Página web personalizada dónde aparezca nombre y apellidos del alumno, número de clase, y que aparezca la IP del servidor (**obtenga del S.O., nada fijo**), y la IP del cliente que solicita la página web.
     - ▪ Red 2: nombre (intranet-US-Xxxx), IP (172.16.10?.2/24), Gateway (172.16.10?.1). (ifconfig, route, fichero de configuración)
       - Servidor apache2 escuchando en el puerto 80, con php instalado.
       - Página web personalizada dónde aparezca nombre y apellidos del alumno, número de clase, que aparezca la IP del servidor (**obtenga del S.O., nada fijo**), y la IP del cliente que solicita la página web.
       - Servidor mysql-server instalado y configurado para poder acceder desde la red, no sólo desde localhost.
       - Servidor vsftpd instalado.
     - ▪ Red 3: nombre (wlan-US-Xxxx), IP (192.168.0.10?.2/24), Gateway (192.168.10?.1). (ifconfig, route, fichero de configuración)
   - **(1 punto)** Montaje de una máquina virtual Microsoft Windows en la red 2 (intranet), con nombre (intranet MS-XXxx), IP fija (172.16.10?.3/24), Gateway (172.16.10?.1). (ifconfig, route, traceroute)

   - **(1 punto)** Montaje de una máquina virtual Ubuntu Desktop en la red 2 (intranet), con nombre (intranet-UD XXxx), IP fija (172.16.10?.3/24), Gateway (172.16.10?.1).
3. **(1 punto)** Comprobaciones de que se puede acceder desde el cortafuegos a todas las máquinas de cada subred, mediante ping y ssh, y wget/curl a los servidores webs (red dmz, red intranet).
4. **(1 punto)** Comprobación de que se puede acceder desde cada equipo de red, al firewall (ping, ssh**), pero no** se puede acceder a internet (actualizar, ping, o lo que prefiera).
5. Realizar un script (firewall.sh) que.
   - **(1 punto)** Permita enmascarar desde la red DMZ (naranja), intranet (verde) y wlan (azul) hacía la red wan (roja). Evidenciar qué desde cualquier máquina de esa red, se permite acceder a equipos de la zona wan, es decir internet (ifconfig, ping, apt-get update, wget, dns y ntpdate).
   - **(1 punto)** No se permita enmascarar (-j LOG, para ver que se está intentando acceder, aunque no enmascare), desde:
     - ▪ Equipos de la red lan a equipo de la red wlan.

▪ Equipos de la red lan a equipo de la red dmz.

**** Sería bueno realizar un snapshot final de cada de este servidor Ubuntu Server, con explicación de lo que hace. Muestre, aunque no se valorará.*

**** Este es el escenario inicial que se recomienda para tener para todo el curso.*

CRITERIOS DE EVALUACIÓN	
4.a	Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

PRÁCTICA 6 (XXxx-practica6) – UD 4.
U.D.3. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). SEGURIDAD PERIMETRAL. IPTABLES.

COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). SEGURIDAD PERIMETRAL. IPTABLES.

En esta práctica hay que usar toda la estructura creada en el ejercicio anterior, pero en este caso vamos a realizar la seguridad perimetral de toda nuestra empresa que recae en el servidor firewall.XXxx y por supuesto de la seguridad de host de la misma (INPUT/OUTPUT) de nuestra empresa, que está formada por tres zonas (dmz, lan y wlan), y los equipos que hemos ubicado en cada zona. Esta estructura (y algunos equipos más que pondremos) los vamos a usar durante todo el año, así que es muy importante la estabilidad de la misma.

La práctica tiene que ir creciendo (en cuanto a las reglas), por tanto, no pueden aparecer reglas que todavía no se hayan preguntado, aunque se pregunten en prácticas siguientes.

CARACTERÍSTICAS GENERALES DE FIREWALL y DE LA PRÁCTICA.

- El script de iptables se arrancará en el inicio de la máquina (/etc/rc.local) o mediante servicio. • Usar comentarios en las mismas reglas de iptables, sobre todo en las de FORWARD, que son las nuevas. • Uso de funciones, variables para facilitar el entendimiento y su modificación.
- Cuando se muestre iptables -L, como la opción line-numbers, para que yo os puedo comentar las capturas por una línea determinada.

1. **(0,5 puntos).** Opciones por defecto y preparación del mismo.
   a) **Único** servicio instalado en la máquina, servicio SSHD.
   b) Reglas defecto DROP para la tabla filter en el firewall para INPUT/OUTPUT/FORWARD en las reglas de la tabla FILTER. Reglas de borrado por defecto.
   c) Firewall consigo mismo se permitirá todo (loopback).
   d) El script de iptables se arrancará en el inicio de la máquina (/etc/rc.local) o mediante servicio.

2. **(1 punto)** Reglas de INPUT. Vamos a asegurar nuestro servidor de posibles ataques desde las cuatro tarjetas de red, para ello se configurará de la siguiente forma**.**

a) Se puede hacer ping al firewall desde cualquier sitio LAN, WLAN y DMZ, pero no desde WAN. Dejar después que se pueda hacer ping desde todas las subredes.

b) Se puede acceder al firewall vía ssh desde todas las interfaces menos desde la zona WLAN, es decir, desde LAN, DMZ y WAN.

c) No se permitirá **nada** más.

3. Reglas de OUTPUT, de la siguiente forma**.**

a) **(0,5 puntos)** Por todas las tarjetas de red, podrá:

• Realizar ping a todas las subredes a cualquier equipo que haya en dicha subred.

• Conectarse por ssh a cualquier equipo de la red wan, y únicamente a las IP (que tenemos ahora, habrá que ir añadiendo a lo largo del curso, caso de que haga falta) de la zona DMZ, LAN y WLAN.

b) **(0,5 puntos)** Por la tarjeta wan, únicamente como es obvio, podrá:

• Actualizarse (DNS, HTTP, HTTPS) y descargar páginas web (wget, curl, etc.)

• Actualizar su hora.

• Enviar email (puerto smtp 25).

• Conectarse por ssh a todos los equipos de todas las zonas, menos a la WAN.

4. **Reglas Filter Forward y NAT:** Accesos a la zona DMZ desde exclusivamente wan:

a) **(1,5 puntos)** Se puede acceder al servidor Web de la zona DMZ en los puertos 80 y 443.

b) **(1,5 puntos)** Desde la zona WAN y desde únicamente los equipos de vuestra confianza (por ejemplo, mac de vuestro equipo anfitrión, etc), se podrá acceder al servidor SSH en la zona DMZ, por el puerto que se desee, ya que os recuerdo que el 22 está ocupado para el cortafuegos (INPUT). Se recomienda uso de variable.

5. **(2 puntos) Filter Forward y NAT desde LAN y WLAN**. Accesos desde la zona LAN/WLAN a Internet (wan) permitidos (hay que usar para cara regla su interfaz correspondiente) y únicamente a los equipos que existan actualmente instalados en las diferentes zonas por su IP (172.16.10?.2, 172.16.10?.3, 192.168.0.10?.2), usando para ello dos **bucles (uno para LAN y otro para WLAN)** que lea de un fichero donde estarán escritas esas IP y que habrá que ir añadiendo a lo largo del curso cuando aparezcan más equipos, y que únicamente se permitirá los siguientes accesos:

• Actualizarse (apt-get) y visitar páginas web (80 y 443) mediante dns

• Hacer ping.

• Actualizar su hora del sistema.

6. **Filter Forward y NAT desde DMZ** Accesos desde la zona DMZ a Internet (wan) permitidos: • **(1 punto)** Actualizarse (apt-get) y visitar páginas web (80 y 443) mediante dns, exclusivamente al único equipo que hay actualmente en dicha zona.

• **(0,5 puntos)** Actualizar la hora del sistema operativo.

• **(1 punto)** No se permitirá la conexión a https://facebook.com, https://www.marca.com.

CRITERIOS DE EVALUACIÓN	
4.a	Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.

5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.a	Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.

PRÁCTICA 7 (XXxx-practica7)
U.D.3. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). PROXY APLICACIÓN WEB.

Antes de describir lo que hay que realizar se van a explicar una serie de normas a tener en cuenta para cada apartado que:

- Se deja al alumno que en cada ejercicio realice las capturas concluyentes que desee, pero **NUNCA** debe faltar:
  - Fichero de configuración de squid que muestra lo que se desea probar.
  - Evidencias de los contadores de las reglas relacionadas (PREROUTING, INPUT, y si la página envía a https FORWARD), para comprender por donde pasan los diferentes paquetes. (iptables -L -n – v – line number, iptables -t nat -L -n -v –line-number)
  - La ejecución de comando wget/curl con las evidencias del número de respuesta (2??, 3??,4??), respuesta del proxy, reenvio a otras páginas ya sea por https o por qué el proxy nos envía a otro web.
  - Las líneas del fichero access.log exactamente relacionada con esa comprobación, que evidencia la aceptación o denegación del mismo, y que tienen que coincidir con la anterior.
- Uso de squid -k parse para comprobar que no hay errores en la configuración de las directivas. • **Para cada** HTTP_ACCESS y HTTP_REPLY_ACCESS tiene que haber un deny_info personalizado donde aparezca nombre alumno XXxx, número de clase del alumno, el nombre de la ACL que prohíbe y un texto que explica el motivo por el cual se deniega. Dichas páginas web deben estar en el servidor DMZ (10.0.?.2).

SEGURIDAD PERIMETRAL

1. **(2,5 puntos)** Instalaciones y configuraciones previas:
   a) **(0,75 puntos)** Instalación del servicio squid, configuración en modo transparente para las dos zonas LAN (puerto 3128) y WLAN (3129), no realizando dicha configuración directamente sobre fichero squid.conf, si no en fichero en el directorio ".conf.d/XXxx-squid.conf". (netstat, systemctl, etc.)
   b) **(0,5 puntos)** Adaptación del script del cortafuegos para prohibir la regla de FORWARD de http desde las dos zonas en modo DROP (esto lo haremos para tener la certeza de que no debe pasar nada por esa regla en todo el ejercicio) y para correcto funcionamiento para http en squid.
   En este momento no debería funcionar nada relacionado con http, ya que http_access deny all (única directiva configurada), lo cortaría todo, pero si con https.

Además, se deben realizar evidencias con netstat, tcpdump e iptraf-ng, para demostrar que existen conexiones **establecidas** en los puertos de escucha de squid.

c) **(0,25 puntos)** Deny_info personalizado para la **acl all** y evidencia de su funcionamiento. d) **(0,25 puntos)** Personalice la opción visible_hostname (proxyXXxx.es) y el fichero access.log (accessXXxx squid.log) y evidencia de su funcionamiento.

e) **(0,25 puntos)** Evidenciar de que no se deja rastros de la IP del cliente, únicamente desde la red. Reestablezca para que siempre guarde la IP del cliente web.

f) **(0,5 puntos)** Además configurar para que haya dos ficheros más de log, una con la opción combined (accessXXxx-combined.log) y uno con un formato realizado por vosotros con todas las opciones posibles (accessXXxx-personalizado.log).

HERRAMIENTAS DE MONITORIZACIÓN

2. **(2 puntos, Investigación)** Realice la instalación y posterior configuración de 2 loganizadores de proxy web entre los siguientes:
   a) Sarg.
   b) Awstats.
   c) Squid Analyzer.
   d) Calamaris.
   e) Fiddler
   f) Burp Suite.

***** Se realiza la instalación en este apartado para qué al realizar el ejercicio al completo, podáis recoger capturas de toda la información que está recogiendo cada loganizador.), en función de la configuración de vuestra práctica. Por tanto, realice el ejercicio completo y ponga aquí las capturas de todo lo loganizado (equipos conectados, sitios top, accesos denegados, etc.**

**** Se recomienda un snapshot, con explicación de lo que hace. Muestre, aunque no se valorará.*

SEGURIDAD PERIMETRAL

3. (2,5 puntos) Filtros HTTP_ACCESS BÁSICOS.

A continuación, se deja al alumno que elija los ejemplos, orden que tiene que tener las directivas http_access en el fichero de configuración y las capturas que desee para evidenciar directivas relacionadas con (deben funcionar todas a la vez, el enunciado está redactada de forma que vaya creciendo):

a) **(0,5 puntos)** Restricciones por la directiva url_regex por ciertas palabras en las dos subredes. b) **(0,5 puntos)** Restricciones en el uso de los navegadores (user-agent) en las dos subredes c) **(0,5 puntos)**

Restricciones en el uso de ciertos dominios en las dos subredes, a partir de un fichero de texto.

d) **(0,5 puntos, AND)** Se permitirá todas las restricciones anteriormente (a, b, c) a una determinada hora (a elegir por el alumno, que dependerá de cuando se realice el ejercicio) de que denominemos descanso, es decir en ese horario no se aplicará ninguna de las restricciones, pero **sólo** en la red LAN. Por tanto, en wlan en ese mismo rango de horas se debe cortar.

e) **(0,5 puntos)** Sin embargo para una MAC concreta (la de equipo Windows), siempre se podrá acceder a todo (no hay restricciones).

4. (1,5 puntos) OTROS Filtros HTTP_ACCESS y HTTP_REPLY_ACCESS

Las siguientes restricciones se pueden demostrar individualmente. Si no se indica nada al respecto, se deja que el alumno decida el ejemplo de lo que se quiere restringir.

a) **(0,5 puntos)** Restricciones por la directiva method, por ejemplo, que no se permita paquetes mediante método GET. Se debe mostrar evidencias de lo que ocurre mediante FIREBUG o herramientas de desarrollador.

b) **(0,5 puntos)** Restricciones por la directiva browser (se aconseja cortar el navegador APT).

c) **(0,5 puntos)** Restricciones por la directiva rep_mime_type.

5. (1,5 puntos) PROXY EN MODO TRANSPARENTE.

b) **(0,75 puntos)** Establezca ahora que en la zona LAN el proxy web funciona en modo no transparente y muestre las evidencias que usted crea necesario. No se olvide de evidenciar de que funciona correctamente la actualización en Ubuntu (apt-get).

c) **(0,75 puntos)** Configure proxy web para que solicite usuario/contraseña mediante htpasswd.

***** Una vez terminado este apartado número 5 reestablezca para que quede en modo no transparente.**

CRITERIOS DE EVALUACIÓN	
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

PRÁCTICA 8 (XXxx-practica8)

U.D.3. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). PROXY INVERSO.

Evidenciar toda esta práctica, mediante dos videos, ejercicio número 2 y 3 (videoXXxx-1-2) y ejercicio número 4 (videoXXxx-3), no superior a 3 minutos cada uno (si es posible). Se debe evidenciar cada una de las opciones que aparecen abajo. Si algún apartado/ejercicio no se ha realizado debe ponerse en este enunciado que no se ha realizado.

1. (1 punto) Modificaciones en el firewall perimetral para que lo que llegue por wan en el puerto 8080 (haproxy) y 8404 (estadística de haproxy), sea reenviado al servidor DMZ (10.0.?.2). Servidor donde convivirán tanto el servicio apache (puerto 80) como el servicio haproxy (8080). Es obligatorio mostrar movimiento en contadores.

2. (6 puntos) Shell script lo más personalizado posible (**./XXxx-arranque.sh**) para arrancar 5 microservicios de una misma imagen (ubuntu+php+apache2) usando para ello un bucle, y del arranque de servicio haproxy (sin dockerizar) configurado para los 5 nodos de forma equitativa. Se valorará de la siguiente forma:

   a) (1,5 puntos) Hay evidencias en la misma ejecución del script de que se ha producido el arranque de los 5 microservicios dockerizados y del servicio haproxy, tanto de escuchas como evidencias de establecimiento de la conexión. Enviar mensajes de que se ha producido correctamente el arranque del script.
   b) (1,5 puntos) Script lo más personalizado (XXxx, variables) posible con XXxx todo lo que pueda del script (nombre de contenedores, hash de los contenedores, nombre del alumno, nombre de nodos de haproxy, variables, comentarios). Se valorará la claridad, explicación y funcionalidad del script.
   c) (1,5 puntos) Hacer una web con php/node lo más personalizable posible donde aparezca la IP que solicitó la petición de la página, día y hora de la conexión, microservicio que ha proporcionado el servicio (nombre del nodo (contenedor) con su IP y puerto) y todo lo que se te ocurra para personalizar y hacer más profesional el ejercicio. d) (1,5 puntos) En relación a la web de estadística de haproxy (IP/haproxy?stats):
      - Fichero de configuración de haproxy personalizado.
      - Evidencia donde se comprueba que se ejecuta correctamente en el puerto adecuado y que existen conexiones establecidas tanto desde el cliente como desde el lado del servidor.
      - Evidencia de que funciona correctamente el balanceo de carga con todos los nodos/contenedores (se aconseja el uso de un bucle para probar el funcionamiento). Evidencia de que si se para **uno** o **varios** contenedores, sigue funcionando el balanceador de carga haproxy sin problemas.
      - Evidencia de que sí se para **todos** los contenedores, no se puede descargar la web solicitada, ya que no existen microservicios arrancados.
      - Evidenciar que el nodo número 1, responde más veces que el resto de los otros nodos (opción weight).

3. (1 punto) Shell script para la parada y borrado (**./XXxx-paradaborrado.sh)** de los 5 microservicios y parada del servicio haproxy y evidencias en el mismo script de que se ha parado los contenedores y el servicio haproxy. Se deja al alumno que muestre las capturas que se necesite para evidenciar dicho apartado.

4. (2 puntos) Modificación de los dos scripts anteriormente creados (**./XXxx-arranque.sh número)** (**./XXxx-parada.sh número)** para que se le pase como opción el número de nodos a arrancar/parar. El número representa el número de contenedores y de nodos del servicio haproxy. Antes de arrancar haproxy habrá que construir previamente el fichero haproxy.cfg con el número de nodos indicado como parámetro (pero no manualmente).

Por ejemplo, se puede probar que se crean 20 contenedores y se adapta el fichero de configuración haproxy.cfg para dichos microservicios. Se deja al alumno que muestre las capturas que necesite para evidenciar que los scripts funcionan correctamente (web de la estadística, ps, netstat, fichero de configuración, conexión desde cliente, etc.). Debe aparecer en la

comprobación, que se arranca 20, que posteriormente se borran esos 20, y que después se arranca 15 y se vuelven a parar.

Todo ello sin **interrupción** y lanzado mediante los scripts que se han preparado.

NORMAS PARA TODA LA PRÁCTICA.

- **No** se puede usar docker-compose en la práctica.
- Se deja a elección del alumno el número de los puertos para arrancar los diferentes contenedores. • Uso de volúmenes **obligatoriamente** para la web de los contadores.
- Los **nombres (--name)** de los contenedores tienen que tener **obligatoriamente** de la siguiente forma (XXxx-web1). • En cada apartado no pueden faltar capturas sobre systemctl, tcpdump, netstat, iptraf-ng y por supuestos de todos los comandos/opciones (docker container …).
- Personalización lo máximo posible de los diferentes scripts, como son uso de variables, comentarios, comandos para mostrar evidencias en el mismo script (&&, ficheros de configuración, etc). Personalizar lo máximo posible de la web (nombre alumno, contenedor que responde, desde donde se conecta el cliente, etc.).

CRITERIOS DE EVALUACIÓN	
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

PRÁCTICA 9
PKI, CA. CERTIFICADOS. SERVIDORES SEGUROS SSL-TLS (HTTPS y FTPS).

Tener en cuenta para las evidencias de este ejercicio, que se debe **personalizar lo máximo** posible cada propiedad de los certificados creados, los nombres de cada uno de los ficheros, información de CA, etc.

1. **(0,5 puntos)** Instalación de servidor Ubuntu servers, denominado intranet-PKI-XXxx en la zona de intranet, mediante IP fija. (172.16.?.5). Se recomienda que se configure SSHD para que acepte la autentificación mediante cifrado asimétrico. Igual tiene que realizar alguna actuación en el firewall para que este equipo pueda conectarse a Internet (wan) o que se puede entrar al mismo desde el firewall.
2. **(0,5 puntos)** Creación de PKI y CA, lo más personalizados posible (fichero vars). Se debe configurar como mínimo: • CN. Nombre Común o commonName (CA XXxx).
   - CountryName, stateOrProvinceName, localityName, emailAddress.
   - OU. Unidad organizativa
   - Fecha de validez de la entidad certificadora.
   - Fecha de validez de los certificados autofirmados.
   - Algoritmo de firma de certificado (SHA-512).
   - Otros dos que creáis oportuno (tamaño keys, etc.) para personalizar más vuestro CA a partir del fichero vars. 3. **(2 puntos)** Creación de 3 pares de llaves (.key y .crt) para **servidores** sin contraseña que usaremos a lo largo de todo el curso.

   a) Servidor Apache (Https) (XXxx-https.key y XXxx-https.crt). **(0,5 puntos)**

   b) Servidor vsftpd (ftps) (XXxx-ftps.key y XXxx-ftps.crt) **(0,5 puntos)**

c) Servidor OpenVPN (XXxx-vpn.key y XXxx-vpn.crt) **(0,5 puntos)**

d) Evidencie que las diferentes llaves públicas autofirmadas por nuestra CA contienen: **(0,5 puntos)** • **Cada uno** de los cambios personalizados obligatorios realizados en fichero vars en apartado número dos. • Los dos cambios realizados por vosotros.

• Números de serie que tiene cada certificado público (.crt). ¿Por qué se crean con esta numeración? 4. **(1 punto)** Creación de 2 pares de llaves (.key y .crt) para 2 **clientes** (una con contraseña y otra sin contraseña) que posteriormente usaremos para identificarnos en diferentes servidores a lo largo del todo el curso.

a) Cliente número 1 sin contraseña (XXxx-cliente1.key y XXxx-cliente1.crt). Cree fichero XXxx-cliente1.p12 mediante comando openssl y evidencie su contenido (openssl pkcs12 -export -out mi_certificado.p12 -inkey mi_clave.key -in mi_certificado.crt -certfile ca_intermedio.crt). **(0,25 puntos)**

b) Cliente número 2 con contraseña, (XXxx-cliente2.key y XXxx-cliente2.crt). Cree fichero XXxx-cliente2.p12 mediante comando easyrsa y evidencie su contenido (./easyrsa export-p12 nombre_cliente --password=clave_secreta). **(0,25 puntos)**

c) Cliente número 3 con contraseña, (XXxx-cliente3.key y XXxx-cliente3.crt). Cree fichero XXxx-cliente3.p12 **(0,25 puntos)**

d) Evidencie que las diferentes llaves públicas para clientes autofirmadas por nuestra CA contienen: **(0,25 puntos)** • **Cada uno** de los cambios personalizados obligatorios realizados en fichero vars en apartado número dos. • Los dos cambios realizados por vosotros.

• Números de serie que tiene cada certificado público (.crt) de cada cliente.

5. **(3 puntos) (APACHE CON HTTPS)** Configuración de servidor Apache en zona DMZ (10.0.?.2), para que escuche por https (conexión cifrada). Se debe evidenciar lo siguiente:

a) Cambios en la configuración de ficheros de configuración de apache y habilitación del módulo SSL. **(0,25 pt).** b) Creación de página personalizadas (index.html) para http y otra para https. Estarán en directorios diferentes directorios de trabajo (DocumentRoot). **(0,25 pt).**

c) Ubicación de las diferentes llaves (XXxx-https.key, XXxx-https.crt, ca.crt). **(0,25 pt).**

d) Servicio arrancado y servicio escuchando en el 80 y 443. **(0,25 pt).**

e) Conexión desde **cliente web GUI** ubicado en la zona WAN tanto en el puerto 80 como por el puerto 443, donde se demuestre.

- e.1. Cambios de los contadores de iptables tanto de la tabla NAT como de la tabla FILTER (FORWARD) al lanzar peticiones por los dos puertos. **(0,25 pt).**
- e.2 Conexión establecida tanto en el lado del cliente como en el lado del servidor (netstat), por los dos puertos. **(0,25 pt).**
- e.3 Tcpdump en el lado del servidor dmz que está escuchando conexiones tanto del 80 y 443. ¿Se observa alguna diferencia en lo que se ha reportado? **(0,25 pt).**
- e.4 Iptraf-ng en el lado del servidor. **(0,25 pt).**
- e.5 Relacionado con **https** en el lado del **cliente** web GUI (navegador web). Evidencie que cambios ha ocurrido en su navegador. ¿Por qué dice que no es seguro, si hemos tenido que aceptar una llave pública? **(0,25 pt).**

f) Conexión desde terminal del servidor DMZ (wget,curl) en modo comando de la descarga tanto del 80 y 443 por localhost. ¿Qué ha ocurrido con el certificado público ahora? **(0,25 pt).**

g) Realice cambios en el fichero de configuración del servidor apache para qué lo que llegue por el puerto 80, sea redireccionado automáticamente al puerto 443 del mismo servidor. Demuestre que funciona correctamente. **(0,50 pt).**

6. **(1 punto) (FTPS)** Configuración del servidor FTP ubicado en la zona DMZ (10.0.?.2) para que las conexiones establecidas se hagan de forma segura (ftps). Se deja al alumno que evidencie con las capturas que desee, pero deben parecerse mucho a las usadas en el ejercicio número 5 para https. Debe aparecer evidencias tanto en modo comando como desde cliente GUI (Filezilla, etc.)

7. **(1 punto) (APACHE CON AUTENTIFICACIÓN DE LOS CLIENTES MEDIANTE CERTIFICADOS)** Configuración adicional en el servidor Apache en zona DMZ, para que los diferentes clientes que quieran ver contenidos del servidor web, les obligue el servidor a tener que autentificarse (ficheros XXxx-cliente1.p12, ..) con el certificado de cliente generados en el apartado número 4.

   Se deja al alumno que evidencie con las capturas que necesite tanto en el lado del cliente como en el lado del servidor. Tiene que haber evidencias con comando wget/curl y con navegador web GUI.

8. **(1 punto) (REVOCACIÓN DE CERTIFICADOS)**. Revoque el certificado de **cliente número dos** con contraseña, realice todos los cambios oportunos que deba realizar y **evidencie** que este cliente ya no puede hacer autentificarse en el servidor apache, tal y como se ha comprobado en el apartado anterior, que sí se podía.

CRITERIOS DE EVALUACIÓN	
2.c	Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
3.a	Se han identificado los tipos de credenciales más utilizados.

3.b	Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
3.c.	Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.
3.d.	Se han comparado certificados digitales válidos e inválidos por diferentes motivos.

PRÁCTICA 10
TUNELES SEGUROS CON SSH. REENVIO DE PUERTOS LOCALES

1. **(5 puntos)** Desde la zona wan usando un cliente Linux en modo terminal y autenticándonos con **llave privada al servidor firewall,** realice la conexión mediante un túnel SSH con el servidor SSHD de la zona (172.16.?.2). Se deja a elección del alumno el puerto usado para realizar el túnel. Se deberá mostrar las siguientes evidencias:
   a) Conexiones establecidas (netstat e iptraf-ng) una vez realizado el túnel y antes de acceder al servicio final (172.16.?.2). Se mostrará una única captura con los dos terminales abiertos en elsiguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el túnel, firewall al cual le hacemos la conexión ssh). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.
   b) Conexiones establecidas (netstat, iptraf-ng y tcpdump) mostrando **una única captura** con los tres

terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el tunel, firewall al cual le hacemos conexión ssh, servidor final en la zona LAN 172.16.?.2). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.

2. **(2,5 puntos, investigación)** Realice el mismo ejercicio número 1, pero usando en este caso un cliente SSH GUI (putty, bitTunnelier, etc). Además, de las evidencias descritas en el apartado anterior, se tiene que mostrar la configuración realizada en el cliente GUI.
3. **(2,5 puntos)** Desde la zona wan usando un cliente Linux en modo terminal y autenticándonos con **llave privada al servidor firewall,** realice la conexión mediante un túnel SSH con el servidor apache (puerto 80 o puerto 443) de la zona (10.0.?.2). Se deja a elección del alumno el puerto usado para realizar el túnel. Se deberá mostrar las siguientes evidencias:
    a) **(1,25 puntos)** Conexiones establecidas (netstat e iptraf-ng) una vez realizado el túnel y antes de acceder al servicio final (10.0.?.2). Se mostrará una única captura con los dos terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el túnel, firewall al cual le hacemos la conexión ssh). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.
    b) **(1,25 puntos)** Conexiones establecidas (netstat, iptraf-ng y tcpdump) mostrando **una única captura** con los tres terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el tunel, firewall al cual le hacemos conexión ssh, servidor final en la zona LAN 10.0.?.2). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.

CRITERIOS DE EVALUACIÓN	
4.e	Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

PRÁCTICA 11
VPN. VPN ENTRE SEDES GEOGRÁFICAMENTE SEPARADAS.

Antes de empezar con el ejercicio, debe tener en cuenta que las reglas de iptables y de configuración del servidor tienen que ir apareciendo poco a poco, no vale ponerlas y ejecutarlas al principio del ejercicio. No se corregirá la práctica si se realiza esto. Use funciones en el script de iptables, como por ejemplo vpn-general, vpn-lan, vpn-dmz, vpn-wan, etc.

INSTALACIÓN DE SERVIDOR VPN

1. **(1 punto)** Realice la instalación del servidor VPN en el servidor firewall en la red 172.18.?.0, usando certificados creados

en práctica de PKI, CA, y usando como nombre del dispositivo tun-XX (donde Xx, alias que queráis). Ejemplo (tun-cova), que una vez conectado será tun-cova-0. Evidencie.

a. Configuración del fichero server.conf mínima, no mostrando comentarios, para que sea más elegible su contenido.

b. Servido arrancando y escuchando por tarjeta tun-XX0.

c. Configuración del cortafuegos mínima para que el servidor escuche por la tarjeta wan. Muestre que los contadores de la regla iptables están inicializadas.

d. Nmap donde se observe que el servidor firewall tiene el puerto abierto UDP.

CLIENTE VPN – TO – SERVER VPN

2. **(1,5 puntos)** Conexión **desde cliente LINUX** usando comando openvpn y del fichero .ovpn con el certificado cliente.crt sin contraseña, **del cliente número 1** creado en nuestra CA. Se debe mostrar como mínimo las siguientes capturas. a. Fichero de configuración del fichero clienteXXxx1.ovpn, donde se demuestre que ha sido creado por vuestra entidad certificadora.

b. Realice primera conexión con cliente openvpn y muestre movimiento de contadores de iptables (INPUT). c. Ip asignadas a la tarjeta virtual del cliente linux y del servidor.

d. Captura de fichero del servidor donde aparece que está IP se ha asignado correctamente. e. Tcpdump en servidor firewall vpn de la conexión vpn realizada.

f. Captura de la salida systemctl status en el cliente, explicando con sus palabras algunas de los mensajes que salen, relacionándolo con las diferentes opciones de configuración.

3. **(1 punto)** Conexión **desde cliente Windows GUI (openVPN Connect)** usando fichero .ovpn con el certificado del cliente número 3 (cree certificados pero no muestre este proceso) creado en nuestra CA. Evidencie:

a. Fichero de configuración del fichero clienteXXxx2.ovpn, donde se demuestre que ha sido creado por vuestra entidad certificadora.

b. Realice primera conexión con cliente openvpn **(openVPN Connect)** y muestre movimiento de contadores de iptables (INPUT). Muestre información que aparece en el cliente GUI, y compare con lo que aparece en el servidor VPN. Demuestre que se solicita contraseña.

c. Ip asignadas a la tarjeta virtual del cliente windows y del servidor. Captura de fichero del servidor donde aparece que está IP se ha asignado correctamente. Debería aparecer como segunda.

d. Tcpdump en servidor firewall vpn de la conexión vpn realizada.

e. Realice cambios en el fichero de configuración del servidor VPN, para que los diferentes clientes VPN conectados, puedan verse entre ellos. Evidencie que pueden verse con un ping y con ssh.

4. **(1 punto)** Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectado, pueda alcanzar el servidor VPN con ping y ssh. Evidencie:

a. Cambios en el fichero de configuración del servidor VPN para permitir conexiones.

b. Reglas de iptables **concretas** para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

c. Capturas de la conexión realizada (contadores) y establecidas (netstat y tcpdump) correctamente, donde se demuestre que se alcanza mediante ping al servidor VPN por la tarjeta tun-XXxx0, usando el cliente Linux vpn. Muestre que se han creado las rutas para alcanzar dicha red (ip route).

d. Capturas de la conexión realizada (contadores) y establecidas (netstat y tcpdump) correctamente, donde se

demuestre que se alcanza mediante ping al servidor VPN por la tarjeta tun-XXxx0 usando el cliente Openvpn GUI de Windows.

CLIENTE VPN – TO – CLIENTES RED LAN

5. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectados, pueden alcanzar el equipo 172.16.?.2 de la red lan (ping y ssh). Evidencie:

a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones. b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

c. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 172.16.?.2, mediante un ping. Muestre que se han creado las rutas para alcanzar dicha red (ip route)

d. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 172.16.?.2, mediante una conexión por ssh.

CLIENTE VPN – TO – CLIENTES RED DMZ

6. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectados, pueden alcanzar el equipo 10.0.?.2 de la red lan (ssh y web (80 y 443). Evidencie:

a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones. b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

c. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 10.0.?.2, mediante un ping, usando el cliente vpn linux.

d. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión al equipo 10.0.?.2, mediante una conexión por ssh, usando el cliente openvpn GUI de Windows.

CLIENTE VPN – TO – CLIENTES RED WAN o INTERNET

7. (1 punto) Realice los cambios necesarios en el fichero de configuración del servidor VPN y de las reglas de iptables, para que se permita que los diferentes clientes openvpn una vez conectados, pueden alcanzar la red wan. Evidencie: a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones. b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.

c. Capturas de éxito (contadores de iptables y traceroute) de la conexión a cualquier equipo de la zona WAN por su IP (ping). Muestre que se han creado las rutas para alcanzar dicha red (ip route)

d. Capturas de éxito (contadores de iptables, tráfico en tcpdump, netstat) de la conexión a cualquier equipo de la

zona WAN por su nombre dns (servidor web de internet), usando el cliente OpenVPN GUI de Windows.

8. **(1 punto)** Realice los cambios necesarios en el fichero de configuración de squid y de las reglas de iptables, para que se pueda alcanzar la red WAN desde cliente VPN haciendo uso del squid en modo transparente por el puerto 3130, cortando la página http://httpforever.com y direccionándola con deny_info personalizado para la red VPN/denegación, como por ejemplo la Web solicitada desde la red VPN con la IP ----, no puede ser descargada.

   a. Cambios **exclusivos** en el fichero de configuración del servidor VPN para permitir dichas conexiones. b. Reglas de iptables concretas para esta tarjeta de red, añadidas exclusivamente para este apartado, momento antes de la conexión.
   c. Capturas de éxito (contadores de iptables tanto en tabla filter como en tabla nat, tráfico en tcpdump, netstat) de la conexión a cualquier equipo de la zona WAN por su nombre dns (servidor web de internet), usando el cliente OpenVPN Connect de Windows o terminal (wget,curl), donde se demuestre que el tráfico está siendo interceptado, direccionado y gestionado por el squid en el puerto 3130.
   d. Capturas de que se produce la denegación de la web deny_info, muestra en access.log de la denegación a la IP de la red VPN, etc.)

CONEXIÓN CLIENTE WINDOWS VPN DESDE INTERNET a SERVIDOR VPN en vuestra casa

9. **(0,5 puntos) (investigación)** En este caso el cliente VPN tiene que estar en Internet (no por delante del servidor VPN), para ello podéis hacer uso de un cliente VPN de algún compañero (tendréis que proporcionales un par de llaves y los ficheros necesarios.
   a. Cambios **exclusivos** en el fichero de configuración del cliente (fichero .ovpn) (cambia la opción remote IP) y del servidor para permitir dichas conexiones y configuración realizada en el router de vuestra casa para que se haga NAT desde la zona WAN a vuestro servidor VPN.
   b. Se deja a elección del alumno que el tráfico viaja desde el cliente, al router y posteriormente al servidor VPN, y que se produce la conexión adecuadamente (capturas de apartados del router, netstat, tcpdump, etc.).

   Caso de que no sea posible realizar estas configuraciones en el router de Casa, se puede cambiar este ejercicio por realizar una conexión como cliente desde un Smartphone/Tablet.

PARTE LAN-TO-LAN 2. CONEXIÓN DE SEDES CENTRALES Y SUCURSALES.

10. **(1 punto) (investigación)** En este caso tendréis que configurar dos firewalls (central y sucursal/franquicia de una empresa). O se monta dos infraestructuras o se hace uso de la infraestructura (sede) de un compañero de clase.

    a. Captura del fichero de configuración del servidor VPN central con las opciones concretas para realizar LAN-TO LAN.
    b. Pruebas de funcionamiento tal y como aparece en el manual con la sede (únicamente conexiones con redes de la sede principal, no con otras sedes ya que estas implican tener más de dos sedes).

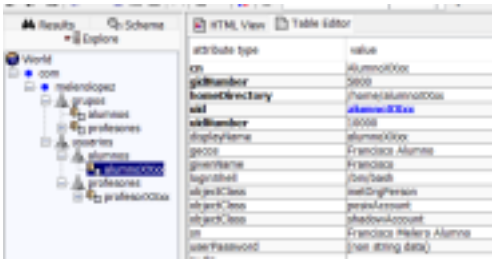
CRITERIOS DE EVALUACIÓN	
4.e	Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.

5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

PRÁCTICA 12
SERVIDOR FREERADIUS. WPA2-ENTERPRISE. INTEGRACIÓN CON SERVIDOR LDAP

INSTALACIÓN DE SERVIDOR FREERADIUS SIN MYSQL NI LDAP

1. **(1 punto)** Realice la instalación del servidor FreeRadius en un nuevo equipo (radiuslapXXxx) (para evitar configuraciones de iptables, etc.) mediante S.O. Ubuntu Server en la zona WAN (bridge) para permitir el acceso a un cliente radius vía localhost para realizar pruebas (personalice la contraseña por defecto). Además, cree un usuario en la forma XXxx con la contraseña XXxx para pruebas locales. Evidencie.
   a. Ficheros modificados y contenido de lo modificado.
   b. Servicio arrancado y comprobación de que está funcionando (systemctl, netstat, nmap)
   c. Pare el servicio y arranque mediante comando freeradius -X y evidencie pruebas en modo local con comando radtest con el usuario/contraseña **correctamente** y la salida del comando freeradius -X. Capture el momento de la conexión con tcpdump.
   d. Evidencie pruebas en modo local, es decir vía locahost sin ningún AP con cliente radius, usando para ello el comando radtest, poniendo usuario mal, contraseña mal y contraseña del cliente mal.



INSTALACIÓN DE SERVIDOR LDAP EN LINUX. OPENLDAP

2. **(1 punto)** Realice la instalación del servidor OpenLDAP en el mismo servidor que FreeRadius usando el nombre del dominio XXxx.com. Evidencie.
   a. Servicio arrancado y comprobación de que está funcionando (systemctl, netstat, nmap)
   b. Conexión mediante cliente JXPLORER en Windows, evidencia de conexión establecida y captura con el comando tcpdump que puede capturar usuario y contraseña en texto plano (ldap no seguro).
   c. (fichero-ou.ldif) Añada una estructura mínima con cuatro unidades organizativas (usuarios, usuarios/alumnos, usuarios/profesores y grupos) mediante comando ldapadd. Compruebe mediante cliente GUI en Microsoft Windows SOFTERRA LDAP BROWSER.
   d. (fichero-grupos.ldif) Añada dos grupos de LINUX en la unidad organizativa grupos con los nombres grupoalumnos y grupoprofesores (adapte GID) mediante comando ldapadd. Compruebe mediante JXPLORER. e. (fichero-servicios.ldif). Añada un servicio en la unidad organizativa servicios, previamente creada. f. (fichero-hosts.ldif). Añada un par de equipos en la unidad organizativa equipos, previamente creada. g. (fichero-usuarios.ldif) Añada 2 usuarios con uid profesorXXxx y alumnoXxxx con las siguientes características: i. En su correspondiente unidad organizativa (usuarios/alumnos, usuarios/profesores)
      ii. Que tenga Shell

iii. Con directorio de trabajo (/home/profesorXXxx, /home/alumnoXXxx)
iv. Con contraseña en formato SSHA (use comando slappasswd)
v. Adapte UID y GID (según sea profesor o alumno).

Evidencie:
vi. Contraseñas generadas.
vii. Su creación con comando ldapadd.
viii. Uso del comando ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:///
ix. Uso del comando ldapsearch -x -H ldap://127.0.0.1 -b dc=XXxx,dc=com
x. JXPLORER y la estructura de los diferentes usuarios creada tal y como aparece en el enunciado.

CONFIGURACIÓN SERVIDOR LDAP SEGURO (LDAPS)

3. **(1 punto)** Realice la configuración del servidor OpenLDAP para que la conexiones sean cifradas (puerto 636) usando para ello use el certificado autogenerado por nuestra CA en prácticas anteriores o creando uno para esta práctica (ldap.crt y ldap.key). Se debe evidenciar:
   a. Netstat, ss, tcpdump e iptraf.
   b. Conexión con Softerra LDAP Browser de forma anónima y SSL+user+password por el puerto 636. Demostrar que te solicita descargar la llave pública y comprobar donde se guarda (mostrar información de ese certificado en el software).
   c. No es posible capturar la información de conexión con usuario cn=admin, al realizar la conexión (SSL+user+password) de forma segura.
   d. Deshabilite ahora que se pueda loguear mediante LDAP no seguro (389) pero si funcione mediante LDAP seguro (636). Deje al final que se puedan permitir la conexión con LDAP y LDAPS.

NO USAR JXPLORER ya que tiene problemas con SSL.

AUTENTIFICACIÓN EN FREERADIUS A TRAVÉS DE SERVIDOR OPENLDAP

4. **(1,5 punto)** Realice la integración de FreeRadius con el servidor OpenLDAP (inicialmente 389). Se debe evidenciar: a. Configuración realizada en servidor FreeRadius inicialmente con puerto 389 para la integración. b. Haciendo uso del arranque de freeradius con la opción -X y del comando radtest, realice las siguientes comprobaciones.
   • Prueba de funcionamiento en modo local con usuario alumnoXXxx y contraseña correctamente. • Apague el servidor Openldap y realice prueba de funcionamiento en modo local con usuario (alumnoXXxx) y contraseña correctamente. ¿Qué ocurre ahora?
   • Evidencia de conexionado en modo local con usuario alumnoXXxx y contraseña incorrectamente.
   • Evidencia de conexionado en modo local con usuario profesorXXxx y contraseña incorrectamente.
   c. Configuración realizada en servidor FreeRadius inicialmente con puerto 636
   d. Haciendo uso del arranque de freeradius con la opción -X y del comando radtest, realice las siguientes comprobaciones.
      i. Prueba de funcionamiento en modo local con usuario alumnoXXxx correctamente.
      ii. Prueba de funcionamiento en modo local con usuario alumnoXXxx incorrectamente.

iii. Prueba de funcionamiento en modo local con usuario profesorXXxx correctamente.

INTEGRACIÓN DE RADIUS CON MYSQL

5. **(1 puntos)** Realice la integración de FreeRadius con un servidor Mysql. Se deja al alumno que presente las evidencias que desee para comprobar su funcionalidad. Puede valer los mismos apartados que ejercicios anteriores. El usuario que creéis que se llame (mysql-alumno-XXxx).

INTEGRACIÓN DE SQUID CON SERVIDOR FREERADIUS

6. **(1 punto)** Realice la integración del servidor squid (modo no transparente) con el servidor OpenLDAP. Se deja al alumno que presente las evidencias que desee para comprobar su funcionalidad. Puede valer los mismos apartados que ejercicios anteriores.

INTEGRACIÓN DE UBUNTU SERVER (SSH, SU) CON SERVIDOR FREERADIUS. PAM

7. **(1,5 punto)** Realice la integración de un sistema operativo Ubuntu Server (puede hacerse vía localhost para no tener que usar otro sistema operativo) con FreeRadius (que a su vez ya está integrado con servidor LDAP). Se deja al alumno que realice las capturas oportunas para demostrar que se ha integrado correctamente el S.O.
    a. Ficheros modificados para su integración con PAM. En el caso de usuarios, únicamente pueden hacer uso los usuarios que estén en la unidad organizativa profesores, no alumnos (mostrar que se puede integran b. Uso de comandos tipo getent, tanto con usuarios, grupos, hosts y equipos, para demostrar que la integración es correcta
    c. Inicio de sesión con usuario de freeradius directamente y un usuario alumno (no debería) y usuario profesor mediante comando switch user (su).
    d. Inicio de sesión con usuario de freeradius directamente y un usuario alumno (no debería) y usuario profesor mediante comando ssh.

INVESTIGACIÓN

8. **(2 puntos)** Ejercicio número 8. Investigación

• Portal Cautivo con FreeRADIUS, OpenLDAP y CoovaChilli. **(Frank Castello, Alvaro, Jose Luis)** • Integración de FreeRADIUS + OpenLDAP con VPN (OpenVPN).(**Frank Moreno, Eugenia, Hernan).** • Implementar autenticación multifactor (2FA) para reforzar la seguridad de los accesos mediante OTP (One-Time Passwords). **(Covadonga, Miguel, Alvaro, Alberto)**
• Bloqueo de Usuarios tras Múltiples Intentos Fallidos (Fail2Ban + FreeRADIUS) **(Cristian, David).**

	CRITERIOS DE EVALUACIÓN
3.b	Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
3.e	Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)

PRÁCTICA 13
SEGURIDAD EN REDES INALÁMBRICAS

PUNTO DE ACCESO DE MI ROUTER CASA

En esta ocasión se elegirá el router de casa para trabajar con las diferentes funcionalidades del punto de acceso integrado en el interior del mismo. En el caso de que no tenga alguna funcionalidad se puede solicitar al profesor algún punto de acceso independiente o router de ISP (tipo LiveBox, etc.). En esta práctica se deja vía libre al alumno que demuestre con capturas concluyentes lo que se solicita, teniendo que hacer uso de capturas del interfaz GUI vía web, software wifi analyzer (vía smartphone/portátil), otros softwares, ***etc****. Se valorará positivamente el uso de opciones diferentes que aparezcan en su dispositivo, uso de software diferente, etc.*

Marca y modelo del dispositivo usado: _____

1. **(3 puntos) (Protocolo de cifrado)** Demuestre los diferentes protocolos de cifrado para contraseñas que incorpora el punto de acceso desde el menos seguro (WEP) hasta el más seguro (WPA-3), evidenciando su correcta conexión al mismo desde móvil/portátil/tablet (ipconfig /all, coamndo de consola en Windows y Linux, canal usado, logs vía web del punto de acceso, GUI de windows/Linux).

2. **(2 puntos) (Buscando en el aire)** Usando el software/app wifi analyzer y/o propio analizador del punto de acceso o software similar, evidencie.
   a. (interfaz web) Configuración preestablecida en el dispositivo en relación a canales/ancho de banda/etc. b. Entorno de señales vecinas wireless tanto en 2.4 GHz y 5 GHz, el canal que está usando, la intensidad (dBm) al cual usted se encuentra. ¿Crees que deberías cambiar de canal su dispositivo para tener mejor señal en su casa? c. Haga cambios en la configuración del canal para demostrar que su dispositivo emite de forma diferente ahora, por ejemplo:
      i. Cambio de canal de forma manual
      ii. Activación/desactivación de Wi-fi de 2.4 GHz/5 GHz, etc.

3. **(5 puntos) (Buenas prácticas).** Evidencie el correcto funcionamiento de las siguientes buenas prácticas relacionadas con la seguridad en redes inalámbricas en puntos de acceso.
   a. **(0,5 puntos)** Cambio del nombre de SSID por defecto del dispositivo.
   b. **(0,5 puntos)** Posibilidad de añadir 2 SSID con diferente protocolo de cifrado. Una puede ser la opción por defecto de Wi-fi de invitados, típica en routers casa de ISP.
   c. **(0,5 puntos)** Ocultación del SSID y configuración manual de SSID, etc. en un cliente de forma manual. d. **(0,75 puntos)** Filtrado de algún dispositivo por MAC (allow list y black list)
   e. **(0,75 puntos)** Modificación del rango de direcciones IP por DHCP.
   f. **(0,75 puntos)** Deshabilitar DHCP del dispositivo y asignación manual a los dispositivos clientes Wireless. g. **(0,75 puntos)** Control horario del dispositivo. Probar que hay alguna restricción horaria en el momento de hacer la práctica.
   h. **(0,25 puntos)** Desactivar WPS.
   i. **(0,25 puntos)** Cambio de contraseña del router/punto de acceso.

En casos excepcionales, donde la opción no aparezca en su dispositivo, demuestre con capturas de como se haría de otro dispositivo.

Curso 2025-2026. Ejercicio relacionado con soluciones comerciales UBIQUITI-UNIFI. Enunciado.

	CRITERIOS DE EVALUACIÓN
4.d	Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, punto de acceso, etc.)

PRÁCTICA 14
DISEÑO DE REDES DE COMPUTADORES. REDES PRIVADAS VIRTUALES (VLAN). SOFTWARE CISCO PACKET TRACER.

SOFTWARE PACKET TRACER. VLAN

Usando la herramienta Packet tracer realice las siguientes configuraciones adicionales y realice comprobaciones de funcionamiento y de configuración (CLI, capturas del interfaz GUI). Personalice lo máximo posible lo que vaya apareciendo (nombre del dispositivo, nombre de las vlan, etc.). Se deja a elección del alumno donde conectar los diferentes dispositivos.

1. **(1 puntos)** Red con un switch (switch1-XXxx) y dos end-points (ordenador y un portátil) con IP manuales en la red 172.16.1??.1/27 y 172.16.1??.2/27. Haga comprobaciones de ping.
2. **(1 punto)** Añada otro switch (switch2-XXxx) con otros dos end-points (ordenador y un portátil) con IP manuales consecutivas a las anteriores, y conecte ambos switches. Haga comprobaciones de ping entre dispositivos de diferentes switches.
3. **(2 puntos)** En la empresa, se decide que los equipos ordenadores pertenezcan a una vlan (1??) (vlan-lanXXxx) y los de portátiles (1??+1) (vlan-wlanXXxx) pertenezcan a otra vlan. Rehaga toda la configuración para establecer dicha configuración y haga comprobaciones de ping.
4. **(4 puntos)** Añada otro switch a la empresa (switch3-XXxx), conecte a los otros dos switchs, y añada a ese switch dos servidores (servidor1XXxx-lan y servidor2XXxx-wlan). Cada servidor será únicamente visto por los equipos de sus diferentes vlans. Dicha configuración hay que realizarla mediante CLI (terminal). En cada uno de los servidores se configurará lo siguiente:
    - Servidor Web en los dos servidores.
    - Servidor ftp en los dos servidores.
    - Servidor DHCP de vlan-lanXXxx con red tipo A, con un pool de direcciones de únicamente 8 equipos. Los diferentes equipos de esa VLAN recibirán la IP de forma dinámica.

• Servidor DHCP de vlan-wlanXXxx con red tipo B, con un pool de direcciones de únicamente 16 equipos. Los diferentes equipos de esa VLAN recibirán la IP de forma dinámica.

5. **(2 puntos)** (Investigación). Añada un router (router-XXxx) con simulación salida de internet (equipo cloudXXxx) conectado al switch3, para que puedan salir a internet los diferentes dispositivos de la vlan-lanXX.

	CRITERIOS DE EVALUACIÓN
4.b	Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).

PRÁCTICA 15
DISEÑO DE REDES DE COMPUTADORES. SEGMENTACIÓN. SUBNETTING. VLSM. REDES PRIVADAS VIRTUALES (VLAN). SOFTWARE CISCO PACKET TRACER.

Recientemente se nos ha contratado en una empresa como administradores de redes, la labor que nos han encomendado es optimizar lo máximo posible y securizar la red informática de toda la empresa, pero manteniendo en la medida de lo posible el direccionamiento usado.

1. Nuestro punto de partida es una red de clase C con direccionamiento 192.168.3.0/24 en la que todos los departamentos tienen direcciones IPs de esa red sin ningún tipo de agrupación y los dispositivos de red como switches tienen una configuración plana sin VLANs, aunque soportan dicha funcionalidad.
2. Se dispone de switchs de 24 puertos, distribuidos como indica el mapa.
3. La empresa realizó una clasificación de departamentos y obtuvo el listado que debemos de usar a la hora de crear nuestras agrupaciones mediante VLANs.
4. La empresa ha hecho especial hincapié en que la red I+D no se debe de permitir conectar ningún dispositivo aparte de los ordenadores que ya están conectados, para ello, se ha elaborado un listado con las direcciones MAC de los dispositivos, que tendrán que asignarse a cada puerto del switch.

DEPARTAMENTO Nº de HOSTS	
Comercial	5
Administrativo	6
I + D	12
Desarrollo	28
Wifi Corporativo	60
Wifi Invitados	25
DMZ	20
Red Gestión	18
VozIP	30

LISTADO MACs I+D
2A:1D:DC:70:EE:01
2A:1D:DC:70:EE:02
2A:1D:DC:70:EE:03
2A:1D:DC:70:EE:04

…
2A:1D:DC:70:EE:12

5. Además, tenemos el siguiente listado de los servidores de la empresa con sus servicios asociados.

	Nombre Servidor Dirección IP Servicio Activo Puerto Externo		
Servidor Web	192.168.3.98	http, https y ssh	80, 443
Servidor Correo	192.168.3.99	pop, imap, smtp yssh	110, 143, 25

Servidor Contabilidad	192.168.3.100	https y RDP	
Servidor FTP	192.168.3.101	ftp y ssh	20, 21
NAS	192.168.3.102	Samba, nfs y ssh	

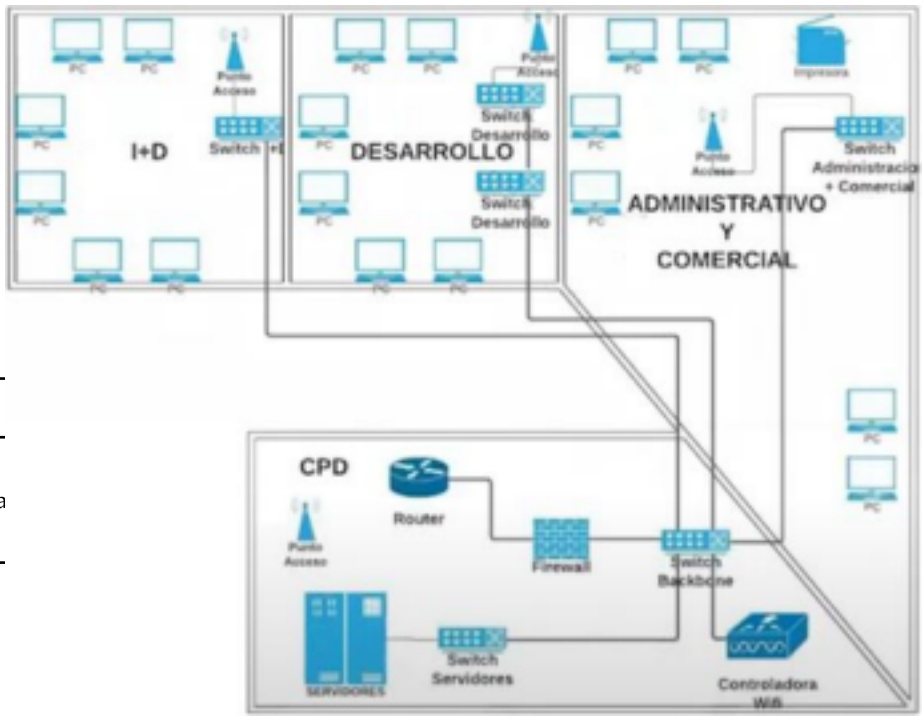
6. Por otra parte, los siguientes departamentos contarán con líneas de teléfono VoIP:

	DEPARTAMENTO Nº de Líneas
I + D	9
Desarrollo	10
Administrativo	6
Comercial	5

7. Se proporciona una hoja de cálculo (classroom) para su mayor compresión, que se debe entregar junto al ejercicio y un fichero inicial con switches de packet tracer.

No es necesario poner en el fichero todos los equipos o comprobaciones que aparecen. Es suficiente con demostrar uno/dos. La IP de los teléfonos IP hay que asignarlos dinámicamente.

En esta ocasión, y por primera vez en el curso se deja al alumno **mostrar las evidencias** del desarrollo de la configuración de los switches con sus correspondientes vlan, asignación de IP a diferentes equipos, evidencias CLI y configuración GUI, etc.



	CRITERIOS DE EVALUACIÓN
4.a	Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y

	utilizando técnicas y dispositivos de enrutamiento.
4.c	Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.

PRÁCTICA Nº 16 SISTEMAS DE COPIA DE SEGURIDAD. RSYNC. CRON. SCRIPTS DE BACKUP. HERRAMIENTAS INTEGRADAS (BAREOS, BACULA)

En este ejercicio y posiblemente en todos los que quede hasta el final del curso, se dejará libremente que el alumno presente todas las evidencias que demuestre lo que se pide. Por tanto, el alumno elegirá las capturas, la forma del ejercicio, las demostraciones a realizar, etc. Debe leer todo el enunciado al completo antes de empezar la práctica.

BACKUP CON COMANDOS DE LINUX DE DIRECTORIOS

1. **(3,5 puntos)** Realice la simulación del sistema de copia de seguridad completo/diferencial/incremental de una empresa durante una semana al completo que cumpla con los siguientes requisitos:
   a) El backup tiene que realizarse de los directorios /home, /etc, /var/log, /datos/XXxxpracticaBackup. Este último donde el alumno realizará cambios manualmente, como son creación de nuevos ficheros, modificación de los mismos, eliminación o simplemente que no haya cambios, antes de cada backup.
   b) Los diferentes backups deben respetar los usuarios, grupos propietarios, permisos y fechas de los mismos. c) **(1,5 puntos) (Backup Local, backup nº 1) (tar, find, cron)** El alumno elige un día y una hora de la semana para que realice el backup completo (/BackupLocal/Xxxx-completo.tar.gz). Desde ese día se irán creando backups diferenciales (ejemplo /BackupLocal/diferencial-miercolesXX.tar.gz, …) y backups incrementales (ejemplo /BackupLocal/incremental-miercolesXX.tar.gz), hasta que llegue de nuevo la fecha del completo. Es decir, después de pasar una "semana" debería haber 13 ficheros (1 completo, 6 diferenciales y 6 incrementales). Realizar las configuraciones adecuada en el servicio cron y para no estar esperando a cada día, id cambiando la fecha del sistema (por ejemplo 5 minutos antes) operativo y de hardware (**date, hwclock**) para que no esperar un día, y cron realice su trabajo adecuadamente.
   d) **(0,5 puntos)** Demostrar evidencias de que se sabe las diferencias entre backups incrementales y diferenciales. e) **(0,5 puntos)** (Backup remoto o nube, backup nº 2) (rsync) Posteriormente a la realización del backup completo/incremental/diferencial de cada día, se realizará la sincronización de todos los backups en algún servidor remoto, a elección del alumno en el directorio (/root/BackupRemotoXXxx/) de la zona LAN, usando cifrado asimétrico para la autentificación.
   f) **(1 punto)** Active los logs de cron para que haya evidencias de que se ha ejecutado el script adecuado en las fechas y horas adecuadas.

RESTAURACIÓN DE BACKUP COMPLETO.

2. Borre/modifique todo el contenido del directorio /datos/XXxxpracticaBackup, y realice la restauración haciendo uso de:
   a) **(0,5 puntos)** Backup Completo local.
   b) **(0,5 puntos)** Vuelva a borrar el contenido y restaure desde un Backup Completo remoto.

RESTAURACIÓN DE BACKUP PARCIALES

3. Restauraciones parciales.

   a) **(0,75 puntos)** Simule la restauración un backup diferencial a partir del backup local.
   b) **(0,75 puntos)** Simule la restauración de un backup incremental a partir del backup local.

BACKUP DE DISPOSITIVOS

4. **(1 punto)** (dd) Realice el backup cifrado (BootXX-xx.img) del dispositivo donde se guarda el arranque del sistema (/boot, normalmente en /dev/sda1) y posteriormente cifrado (gpg). Simule la creación del backup cifrado, el borrado de algún fichero y su posteriormente restauración. Se ha elegido dicho dispositivo ya que es pequeño en tamaño.

SISTEMAS DE COPIA DE SEGURIDAD INTEGRADO (BACULA, AMANDA, BAREOS, UrBackup)

Bacula (Miguel, Covadonga, Alberto)
Bareos (Alvaro, Frank Moreno, Frank Ruiz, David)
Amanda (Hernan, Adrian, José Luis)
UrBackup (Alvaro Hueto, Eugenia, Cristian)

5. **(3 puntos)** Realización completa de la simulación del funcionamiento de un sistema de backup completo mediante cliente/servidor. En las evidencias tiene que aparecer:
   • La configuración de backup completo y backup incremental o diferencial (no son necesarios los dos) • La comprobación de que se han realizado correctamente los diferentes backups y la restauración de los mismos.
   • Correcto funcionamiento entre el cliente y el servidor. Correcto funcionamiento del servicio. • Logs generados en la herramienta donde se compruebe que se han creado y restaurado backups. • Utilidad gráfica (vía web) de la herramienta si la tuviera.
   • Todo aquello que crea preciso para evaluar que se comprende perfectamente el funcionamiento del mismo.

PRÁCTICA Nº 17
CONFIGURACIÓN DE DISPOSITIVOS PARA LA INSTALACIÓN DE SISTEMAS INFORMÁTICOS MINIMIZANDO LAS PROBABILIDADES DE EXPOSICIÓN A ATAQUES.

PRACTICA Nº 17-A, BIOS. MEDIOS DE ARRANQUE.

1. **(10 puntos)** Demuestres las siguientes evidencias sobre máquina real.
   a. (BIOS) Se solicita contraseña para entrar en la BIOS del S.O. (Opción set). Configuración y solicitar contraseña. b. (BIOS) Se solicita contraseña para dar acceso a un medio de arranque en la BIOS del S.O. (Opción set). Configuración y solicitar contraseña.
   c. (BIOS) Dejar los dos apartados que no soliciten contraseñas (Opción clear).
   d. Realiza las mismas actuaciones sobre UEFI.

CRITERIOS DE EVALUACIÓN	
6.a	Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.

PRACTICA Nº 17-B, BIOS-UEFI-SECUENCIA DE ARRANQUE.

Ejercicio de enunciado y resolución abierto teniendo en cuenta el criterio de evaluación 6.c.

CRITERIOS DE EVALUACIÓN	
6.c	Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.

PRACTICA Nº 17-C, ARRANQUE DEL SISTEMA OPERATIVO.

Ejercicio de enunciado y resolución abierto teniendo en cuenta el criterio de evaluación 6.b.

CRITERIOS DE EVALUACIÓN	
6.b	Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.

PRACTICA Nº 17-D, PARTICIONADO DE DISCOS DUROS INTERNOS Y EXTERNOS PARA MINIMIZAR RIESGOS DE SEGURIDAD.

(10 puntos) Realice el siguiente ejercicio sobre cualquier S.O. Ubuntu Desktop en máquina virtual.

1. **(1 punto)** Realice los siguientes montajes especiales:
   a. **(0,5 puntos)** Monte un pen-drive en /root/XXxx/USB-write en modo escritura y vea la información que contiene. Cree un archivo de texto y vea sus propiedades y por último desmonte. Desmonte el pen-drive y monte ahora en modo lectura, comprobando que está el contenido creado anterior, pero no puede añadir nada ahora.

   b. **(0,5 puntos)** Monte un archivo ISO (.iso) que usted elija en /root/XXxx/ISO) (mount -t iso9660 -o loop /home/fichero.ISO), vea su información y desmonte. Compruebe que el fichero ISO descargado es correcto (checksum) usando la función hash adecuada (md5, sha, etc.)
2. **(1 punto)** Añada 1 disco duro de 10 GB más (/dev/sdb), usando el modo gráfico **GPARTED y los comandos que cree necesario para sus evidencias**, realice:

   a. Crea tabla de particionado MBR (msdos).
   b. Intente crear 8 particiones primarias (da igual el sistema de archivos, no vamos a formatearlo). ¿Qué ha sucedido? c. Demuestre como crear 3 particiones primarias, 1 extendida, y 5 particiones lógicas. Elija adecuadamente el tamaño.
   d. Elija la partición número 8:
      - Formatee en ext4.
      - Monta en /root/Xxxx/Ejercicio4/

- Desmonta.
- Haga que se pueda montar automáticamente.

3. **(1 punto)** Añada 1 disco duro de 10 GB más (/dev/sdc), usando el modo gráfico **GPARTED y los comandos que cree necesario para sus evidencias**, realice:

   a. Crea tabla de particionado **GPT** (modo BIOS UEFI).
   b. Intente crear 8 particiones primarias (da igual el sistema de archivos, no vamos a formatearlo). ¿Qué ha sucedido? c. Demuestre que puede crear 8 particiones o más. Elija adecuadamente el tamaño.
   d. Elija la partición número 6:
      - Formatee en ext4.
      - Monta en /root/Xxxx/Ejercicio4/
      - Desmonta.
      - Haga que se pueda montar automáticamente.
4. **(1 punto)** Añada 1 disco duro de 30 GB (/dev/sdd) y usando comando **fdisk** particione en 3 particiones (/dev/sdd1, /dev/sdd2 y /dev/sdd3) (ext4, ext2 y NTFS)
   a. Montar en /root/XXxx/Disco4-ext4. Cree un archivo de texto y vea las propiedades.
   b. Montar en /root/XXxx/Disco4-ext2. Cree un archivo de texto y vea las propiedades.
   c. Montar en /home/XXxx/Disco4-NTFS. Cree un archivo de texto y vea las propiedades.
   d. Monte las 3 particiones en el arranque del S.O. (/etc/fstab) con las siguientes características: primera partición (se puede escribir), segunda partición 2 (se puede leer únicamente), tercera partición 3 (no se puede ejecutar un fichero con permisos de ejecución).

5. **(1 punto)** (/dev/md0, /etc/mdadm/mdadm.conf, espejo RAID 1) con los discos duros número (/dev/sde) y (/dev/sdf). a. Asegúrese de que los discos duros están limpios para evitar conflictos (wipefs).
   b. Cree un sistema de archivos (ext3) y cree algunos directorios y ficheros en su interior.
   c. Realice el montaje manual (/mnt/XXxx-discoraid1) y cree directorios/ficheros.
   d. Realice el montaje automático en el arranque del S.O.
   e. Desconecte uno de los discos duros y compruebe que no se ha perdido ninguna información.

Realice el siguiente ejercicio sobre cualquier S.O. Microsoft Windows en máquina virtual.

6. **(1 punto)** (Movernos y mostrar información de disco “simples”, no por volúmenes) Realice las siguiente las siguientes comprobaciones y responda a lo que se le pregunta.

   a. Ejecute la aplicación DISKPART en modo comando desde PowerShell y muestre la ayuda de todos los comandos/opciones de esta aplicación.
   b. Muestre los diferentes discos que existe en su equipo, mostrando cual es el disco focalizado, indicando los disco dinámicos y GPT.

7. **(1 punto)** (Movernos y mostrar información de volúmenes) Realice las siguiente las siguientes comprobaciones y responda a lo que se le pregunta.
   a. Muestre/comente todos los volúmenes que tiene su ordenador, evidenciando cuales son cada uno de ellos (debe aparecer todos los realizado en la práctica anterior), cual volumen tiene el foco y si la información concuerda con lo realizado en la práctica anterior.
8. **(1 punto)** (Un único disco) Sobre el disco duro donde se encuentra el S.O (que tiene particiones), realice las siguiente

las siguientes comprobaciones y responda a lo que se le pregunta.

a. Muestre/comente las particiones que tiene el disco duro del S.O.

b. Seleccione la partición donde se encuentra instalado el S.O y explique con sus palabras toda la información que se muestra (además de la captura) (¿Qué es el asterisco que aparece, que letra y etiqueta tiene, que tipo de partición, que tamaño y si es de arranque o no?

c. Selecciona la partición que se encripto, muestre/comente detalle.

d. ¿Qué sistema de archivo soporta dicha partición?

9. **(2 puntos)** (Crear, borrar, formatear y redimensionar) Sobre un disco duro comprado (500 MB) realice las siguiente las siguientes comprobaciones y responda a lo que se le pregunta.

a. Inicialice con comando DISKPART el disco con GPT (convert GPT) muestre información del mismo (tipo de disco, GPT/MBR, tamaño, hay volúmenes, etc).

b. Seleccione/enfoque dicho disco duro y muestre información de las particiones/volúmenes que existen actualmente. ¿Por qué hay una partición ya creada y qué guarda?

c. Limpie el disco duro y muestre de nuevo las particiones ¿Qué ha sucedido con la partición que había? Vuelva a convertir a GPT.

d. Cree la estructura de la imagen con 6 particiones sin formatear y los tamaños indicados (comando create).

```
DISKPART> list partition

  Núm Partición  Tipo            Tamaño   Desplazamiento
  -------------  --------------  -------  --------------
  Partición 1    Reservado         32 MB    17 KB
  Partición 2    Principal        100 MB    32 MB
  Partición 3    Principal        200 MB   132 MB
  Partición 4    Principal         50 MB   332 MB
  Partición 5    Principal         50 MB   382 MB
  Partición 6    Principal         50 MB   432 MB
```

e. Formatee todas las particiones creadas, las de 50 MB con FAT32 y las otras con NTFS. Ponga la etiqueta TamañoXXxx a cada partición (por ejemplo, partición 5, 50XXxx-3 (el tres es xq hay tres particiones de 50 MB), asigne una letra (assign letter) (desde la Q: en adelante a cada una de ellas). (muestro un ejemplo, el tres ya que es la tercera de 50 MB con la letra U, formateado con FAT32).

```
Partición 6
Tipo             : ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
Oculta           : No
Necesaria        : No
Atrib.           : 0000000000000000
Desplaz. bytes: 453050368

  Núm Volumen Ltr  Etiqueta     Fs     Tipo        Tamaño   Estado     Info
  ---------- ---  -----------  -----  ----------  -------  ---------  --------
* Volumen 9     U   50XXXX-3    FAT32  Partición     50 MB  Correcto
```

f. Evidencie que puede crear archivos y directorios en cada una de estas particiones/volúmenes. g. Seleccione/Enfoque la partición número 6 y extiendo su tamaño hasta el total de espacio libre ¿Has podido y por qué?

h. Borre todas las particiones FAT32 (delete partition) creadas en los apartados anteriores.

i. Extienda la partición de 200 MB en 100 MB más (extend size) y posteriormente extienda el tamaño hasta el total del tamaño libre.

CRITERIOS DE EVALUACIÓN	
6.e	Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

PRACTICA Nº 17-E, CIFRADO DE DISCOS DUROS, PARTICIONES, DIRECTORIOS Y FICHEROS REGULARES.

(10 puntos) A partir de una máquina virtual **nueva** preparada para la instalación de S.O. Ubuntu Server con cinco discos duros (20 GB, 10 GB, 1 GB, 1 GB, 500 MB), realice las siguientes actuaciones:

1. **(2,5 puntos)** (Disco nº 1, /dev/sda) Instalación de S.O. en disco duro de 20 GB, cifrando el disco duro al completo y guardando fichero de recuperación. Demuestre con evidencias:
    a. ¿Qué solicita contraseña para desencriptar en el arranque?
    b. Compruebe que todos los discos duros se han cargado en el inicio del S.O., que algunos tienen sistemas, pero que la mayoría no lo tienen.
    c. Información en /etc/crypttab que aparece.
    d. Demostrar número de particiones que se han creado con cada uno de los siguientes comandos (df -h, parted -l, fdisk, lsblk) y tamaño de cada una
    e. ¿Qué contiene cada uno de ellos de esas particiones? ¿Con qué sistemas de archivo se ha formateado? ¿Tipo de tabla de partición creada?
    f. Que podemos recuperar contraseña de cifrado con fichero de recuperación.
2. **(2,5 puntos)** (Disco nº 2, /dev/sdb1) (LUKS + cryptsetup, /etc/crypttab, blkid) Usando todo el disco duro nº 2, prepare el mismo como volumen cifrado (XXxx-discoduro2_cifrado).
    a. Abra el volumen cifrado, formatee, realice el montaje manual en /mnt/XXxxdiscoduro2 y cree directorios/ficheros en su interior.
    b. Compruebe que el tipo de partición es crypto_LUKS (blkid).
    c. Reinicie S.O., y vuelva a montar el volumen cifrado (XXxx-discoduro2_cifrado) manualmente. d. Configure /etc/crypttab para que se realice el montaje del volumen cifrado en el arranque del S.O. y solicite la contraseña al iniciar el S.O. de este nuevo volumen cifrado.
3. **(2,5 puntos)** (Disco número 5, /dev/sde) Usando el disco duro número 5.
    a. Realice el particionado, formateo del sistema de archivos en **ext3 obligatoriamente**, montaje en /mnt/XXxxdiscoduro5/.
    b. Compruebe el tipo de tabla de partición. ¿Qué problemas cree que tendrías?
    c. Cree 1 directorio (XXxxDirectorioACifrar) y cifre y descifre (fscrypt). ¿Por qué no es posible cifrar? Realice los cambios necesarios para poder encriptar y demuestre que ha sido posible.
    d. Cree 1 archivo regular (XXxxFicheroACifrar.txt), cifre y descifre (gpg).
4. **(2,5 puntos)** En S.O. Windows virtual, añada un disco duro, formatee y cifre con herramienta bitlockers.

CRITERIOS DE EVALUACIÓN	
6.d	Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.