TALLER SR – PRÁCTICA 24 – Servizo WEB – Apache

Control de acceso: Autentificación HTTP-BASIC, ficheiros .htaccess

NÚMERO DE GRUPO	FUNCIÓNS	Apelidos, Nome
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

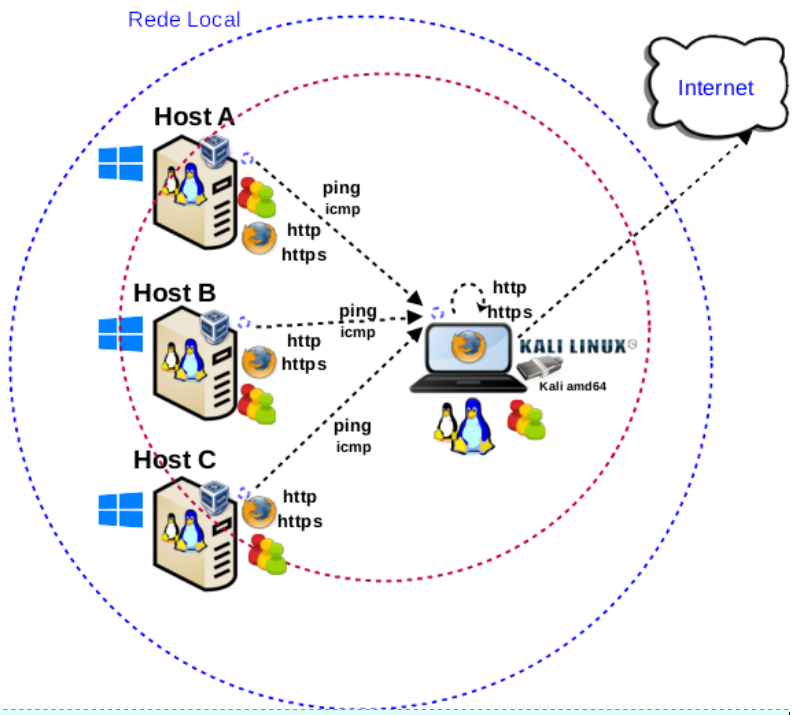
ESCENARIO:

Portátil:
Intranet

USB
Live Kali amd64

Hosts A, B, C:
∈ Intranet
⊃ Máquina virtual
Cliente DHCP
Servidor Web Apache

Máquinas virtuais GNU/Linux:
⊂ Host
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: NAT
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
ISO: Kali Live amd64
Cliente DHCP
Cliente Web (Navegador)



Material necesario	Práctica: Servizo WEB – Apache – Control de acceso Autentificación HTTP-BASIC, ficheiros .htaccess
■ Portátil ■ Regleta ■ Switch 5-Port Gigabit ■ USB Live amd64 Kali ■ Hosts alumnado ■ Cableado de rede ■ [1] Apache (v2.4) ■ [2] Práctica SI Apache ■ [3] Debian Handbook – Apache ■ [4] Debian Wiki - Apache ■ [5] Práctica 1 ■ [6] Práctica SI HTTP-BASIC ■ [7] Práctica 23 ■ [8] .htaccess	(1) Prerrequisito: Ter realizada a Práctica 1 [5] e a Práctica 23 [7] (2) Conectar portátil e hosts do alumnado ao switch. (3) Conectar o switch á roseta da aula. (4) Portátil: a) Arrancar co USB Live amd64 Kali. b) Revisar configuración de rede. c) Activar Apache (HTTP e HTTPS) e crear virtualhosts. d) Control de acceso: HTTP-BASIC [6], .htaccess [8] e) Solicitar contido web mediante HTTP e HTTPS (5) Hosts alumnado: a) Crear máquinas virtuais coa rede en modo “NAT” e especificacións según escenario. b) Arrancar máquina virtual e comprobar conectividade co portátil. c) Solicitar contido mediante HTTP e HTTPS

Procedemento:

(1) Conectar no mesmo segmento de rede o portátil e os hosts do alumnado.

(a) Conectar a regleta á corrente eléctrica na vosa zona de traballo.

(b) Conectar o switch á regleta.

(c) Conectar o portátil ao switch.

(d) Conectar co cableado de rede creado na Práctica 1 [5] os vosos equipos de alumnado ao switch.

(e) **Conectar o switch á roseta da aula.**

(2) Portátil:

(a) Arrancar co USB Live Kali amd64.

(b) Comprobar que tedes acceso á rede local e a Internet. Abrir unha consola e executar:

```
$ setxkbmap es #Configurar teclado en español
$ ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar a configuración de rede para a NIC eth0
$ ip route #Amosar a táboa de enrutamento.
$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
$ ping -c4 www.google.es #Enviar 4 paquetes ICMP ECHO_REQUEST a www.google.es, solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia Internet e ao servidor de google.
```

Cubrir a seguinte táboa:

Host	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)
Portátil				

(c) Avisar ao docente para a revisión. ☐[1]

(d) Activar servidor Web Apache. Executar na anterior consola:

```
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
# /etc/init.d/apache2 start #Iniciar o servidor web Apache.
# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
# nc -vz IP_Portatil 80 #Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Mediante o comando nc(netcat) comprobar se o porto 80 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 80 é o porto TCP a escanear.
```

No caso da distribución Kali xa temos instalado o servidor web Apache, pero nunha distribución baseada en Debian poderiamos instalalo do seguinte xeito:

```
# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
# apt search apache2 #Buscar calquera paquete que coincida co patrón de búsqueda apache2
# apt -y install apache2 #Instalar o paquete apache2, é dicir, instalar o servidor web apache2. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

(e) Activar configuración e certificado https (módulo SSL, porto TCP 443) en Apache. Executar na anterior consola:

```
# a2ensite default-ssl #Habilitar o VirtualHost default-ssl, que configura o acceso a través de https (porto TCP 443)
# a2enmod ssl #Habilitar o módulo ssl que permite activar a configuración do VirtualHost default-ssl, que configura o acceso a través de https (porto TCP 443)
# /etc/init.d/apache2 restart #Reiniciar a configuración do servidor web Apache.
# nc -vz IP_Portatil 443 #Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Mediante o comando nc(netcat) comprobar se o porto 443 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 443 é o porto TCP a escanear.
```

(f) Avisar ao docente para a revisión. ☐₂

(3) Portátil: Xerar virtualhost baseados en nome.

Veremos como poder aloxar páxinas de distintos dominios no mesmo servidor web mediante a configuración de hosts virtuais ou virtualhosts.

Os virtualhosts basicamente o que fan é permitir que un mesmo servidor web poida aloxar múltiples dominios, así configurando hosts virtuais podemos aloxar: `exemplo1.local`, `exemplo2.local`..., `exemploN.local` no mesmo servidor web. Cada empresa terá o seu virtualhost único e independente das demais.

Aínda que como se comentou anteriormente cada virtualhost é único e independente dos demais, todo aquilo que non estea incluído na definición de cada virtualhost herdarase da configuración principal: `/etc/apache2/apache2.conf`, así, se se quere definir unha directiva común en tódolos virtualhost non se debe modificar cada un dos virtualhost introducindo esa directiva senón que se debe definir esa directiva nun arquivo de configuración dentro de `/etc/apache2/conf-available` e empregar o comando `a2enconf` para habilitar esa configuración no servidor web Apache, de tal forma que todos os virtualhost herdarán esa directiva. Por exemplo en `/etc/apache2/conf-available/security.conf` pódese atopala directiva `ServerSignature On`, que engade unha liña contendo a versión do servidor e o nome do VirtualHost.

Existe tres tipos de virtualhost: baseados en nome, baseados en IP e baseados en varios servidores principais. Imos centrarnos nos virtualhost baseados en nome.

(a) Engadir no directorio `/etc/apache2/sites-available/` os seguintes bloques de configuración de virtualhosts. Cada bloque pertence a un arquivo .conf:

Arquivo empresa1.conf (/etc/apache2/sites-available/empresa1.conf)

```
#Configuración virtualhost: empresa1
<VirtualHost *:80>
DocumentRoot /var/www/empresa1/
ServerName www.empresa1.com
ServerAlias empresa1.com empresa1.es www.empresa1.es
</VirtualHost>
```

Arquivo empresa2.conf (/etc/apache2/sites-available/empresa2.conf)

```
#Configuración virtualhost: empresa2
<VirtualHost *:443>
DocumentRoot /var/www/empresa2/
ServerName www.empresa2.com
ServerAlias empresa2.com empresa2.es www.empresa2.es
</VirtualHost>
```

Explicación bloques configuración virtualhost:

- `<VirtualHost *:80>` ➜ Inicio etiqueta virtualhost. Calquera IP do servidor WEB no porto TCP 80 está en estado `listen` para este virtualhost.
- `DocumentRoot /var/www/empresa1/` ➜ Definición da ruta onde está aloxada a páxina web no servidor, neste caso: `/var/www/empresa1/` mediante a directiva `DocumentRoot`.
- `ServerName www.empresa1.com` ➜ Definición do nome DNS que buscará a páxina aloxada na ruta anterior do servidor mediante a directiva `ServerName`. É o nome que escribes no navegador para visitar a páxina.
- `ServerAlias empresa1.com` ➜ A directiva `ServerAlias` permite definir outros nomes DNS para a mesma páxina.
- `</VirtualHost>` ➜ Fin da etiqueta VirtualHost: fin da definición deste virtualhost para empresa1.

(b) Xerar os directorios `/var/www/empresa1` e `/var/www/empresa2`, os ficheiros `index.html` dentro deles e establecer permisos para que Apache poida acceder a eses ficheiros `index.html`. Executar na anterior consola:

```
# mkdir /var/www/empresa1 /var/www/empresa2 #Crear os directorios /var/www/empresa1 e /var/www/empresa2

# echo 'empresa1 contido' > /var/www/empresa1/index.html #Crear o ficheiro /var/www/empresa1/index.html co contido: empresa1 contido

# echo 'empresa2 contido' > /var/www/empresa2/index.html #Crear o ficheiro /var/www/empresa2/index.html co contido: empresa2 contido

# chown -R www-data. /var/www/empresa1 /var/www/empresa2 #Cambiar usuario propietario www-data e grupo propietario www-data a toda a árbore de ficheiros e directorios que colgan dos directorios /var/www/empresa1 e /var/www/empresa2
```

(c) Actualizar a configuración de Apache para ter en conta os novos cambios. Executar na anterior consola:

```
# a2ensite empresa1 #Comando que permite habilitar a configuración do VirtualHost empresa1, é dicir, comando que permite habilitar o ficheiro do VirtualHost empresa1 situado no directorio /etc/apache2/sites-available/empresa1.conf engadindo a ligazón correspondente dende /etc/apache2/sites-enabled/empresa1.conf a /etc/apache2/sites-available/empresa1.conf

# a2ensite empresa2 #Comando que permite habilitar a configuración do VirtualHost empresa2, é dicir, comando que permite habilitar o ficheiro do VirtualHost empresa2 situado no directorio /etc/apache2/sites-available/empresa2.conf engadindo a ligazón correspondente dende /etc/apache2/sites-enabled/empresa2.conf a /etc/apache2/sites-available/empresa2.conf
```

(d) Actualizar o arquivo `/etc/hosts`. Executar na anterior consola:

```
# echo 'IP_Portatil www.empresa1.com empresa1.com empresa1.es www.empresa1.es' >> /etc/hosts
#Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) os nomes www.empresa1.com, empresa1.com, empresa1.es e www.empresa1.es para que atendan á IP_Portatil

# echo ' IP_Portatil www.empresa2.com empresa2.com empresa2.es www.empresa2.es' >> /etc/hosts
#Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) os nomes www.empresa2.com, empresa2.com, empresa2.es e www.empresa2.es para que atendan á IP_Portatil
```

(e) Recargar a configuración do servidor Apache. Executar na anterior consola:

```
# /etc/init.d/apache2 reload #Recargar a configuración do servidor web Apache.
```

(f) Lanzar un navegador e visitar as URLs:

I. `http://IP_Portatil/empresa1/index.html`

II. `https://IP_Portatil/empresa1/index.html`

III. `http://IP_Portatil/empresa2/index.html`

IV. `https://IP_Portatil/empresa2/index.html`

V. `http://empresa1.es/index.html`

VI. `https://empresa1.es/index.html`

VII. `http://empresa2.es/index.html`

VIII. `https://empresa2.es/index.html`

Substituír `IP_Portatil` polo seu valor (ver táboa apartado 2b) .

Indicar que acontece e o por que nos apartados anteriores (dende o I ata o VIII).

(g) Avisar ao docente para a revisión. ☐3

(4) Portátil: Control de acceso

Imos tratar o tipo de control de acceso: autentificación `http basic`[6] e os arquivos tipo `.htaccess`[8]

HTTP proporciona un método de autenticación básico de usuarios: `basic`. Este método ante unha petición do cliente(navegador web) ao servidor cando se solicita unha URL amosará un diálogo pedindo usuario e contrasinal. Unha vez autenticado o usuario, o cliente volverá facer a petición ao servidor pero agora enviando o usuario e contrasinal, en texto claro (sen cifrar) proporcionados no diálogo. É recomendable entón se se emprega este método que se faga combinado con conexión SSL (HTTPS).

Na autenticación `HTTP Basic`[6] é moi típico utilizar arquivos `.htaccess`[8] nos directorios que queremos controlar o acceso. Os arquivos `.htaccess`[8] son ficheiros de configuración do propio directorio onde exista. Para usar arquivos `.htaccess`[8], necesítase ter unha configuración no servidor que permita poñer directivas de autenticación nestes arquivos, mediante a directiva `AllowOverride`, tal como segue: `AllowOverride AuthConfig`

NOTA:
Visitar o seguinte enlace para ver unha explicación, máis polo miúdo, sobre á autenticación `http basic`: Autenticación y autorización

(a) Executar na anterior consola:

```
# a2dissite empresa2 #Comando que permite deshabilitar a configuración do VirtualHost empresa2, é dicir, comando que permite deshabilitar o ficheiro do VirtualHost empresa2 situado no directorio /etc/apache2/sites-available/empresa2.conf eliminando a ligazón correspondente dende /etc/apache2/sites-enabled/empresa2.conf a /etc/apache2/sites-available/empresa2.conf
# /etc/init.d/apache2 reload #Recargar a configuración do servidor web Apache.
```

(b) Modificar arquivo `/etc/apache2/conf-available/security.conf` e engadir o seguinte bloque:

```
<Directory /var/www/empresa2>
AllowOverride Authconfig
</Directory>
```

(c) Crear usuarios para autentificación `HTTP Basic`[6]. Estes usuarios non existen como usuarios do sistema no host servidor, é dicir, non posúen conta como usuarios para facer login no sistema operativo do servidor, son usuarios virtuais soamente empregados para este control de acceso en Apache.

- Crear o contrasinal para o usuario `ana` no ficheiro de contrasinais `/etc/apache2/web.htpasswd`:

```
# htpasswd -c /etc/apache2/web.htpasswd ana #Pór 123456 como contrasinal do usuario ana
```

- Crear o contrasinal para o usuario `brais` no ficheiro de contrasinais `/etc/apache2/web.htpasswd`:

```
# htpasswd /etc/apache2/web.htpasswd brais #Pór 654321 como contrasinal do usuario brais. OLLO!: Non empregar a opción -c para non voltar a crear o ficheiro web.htpasswd e así eliminar as credenciais do usuario ana.
```

(d) Configuralo servidor para o acceso sexa permitido mediante autenticación: usuario/contrasinal empregando un arquivo `.htaccess`[8]. Así, engadir no directorio `/var/www/empresa2/` o seguinte arquivo:

Arquivo /var/www/empresa2/.htaccess

```
AuthType Basic
AuthName "Web con Autenticacion Basic"
AuthBasicProvider file
AuthUserFile /etc/apache2/web.htpasswd
#Require valid-user
Require user ana
```

(e) Establecer permisos:

```
# chown -R www-data. /var/www/empresa2 #Cambiar usuario propietariowww-data e grupo propietario www-data a toda a árbore de ficheiros e directorios que colgan do directorio/var/www/empresa2
# chmod 400 /var/www/empresa2/.htaccess #Cambiar a só lectura ospermisos ugo do ficheiro .htaccess situado en /var/www/empresa2, é dicir, establecer os permisos r--------(soamente lectura para o usuario propietario)
```

(f) Activar o VirtualHost `empresa2`:

```
# a2ensite empresa2 #Comando que permite habilitar a configuración do VirtualHost empresa2, é dicir, comando que permite habilitar o ficheiro do VirtualHost empresa2 situado no directorio /etc/apache2/sites-available/empresa2.conf engadindo a ligazón correspondente dende /etc/apache2/sites-enabled/empresa2.conf a /etc/apache2/sites-available/empresa2.conf
```

(g) Actualizar a configuración de Apache para ter en conta os novos cambios:

```
# /etc/init.d/apache2 reload #Recargar a configuración do servidor web Apache.
```

(h) Realizar de novo o apartado (3f). Indicar que acontece e por que.

NOTA: Se é necesario limpa as cookies para probar a autentificación cos 2 usuarios: `ana` e `brais`.

(i) Avisar ao docente para a revisión. ☐ 4

(5) Hosts alumnado:

(a) Crear unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):

- RAM ≥ 2048MB
- CPU ≥ 2
- PAE/NX habilitado
- Rede: Soamente unha tarxeta activada en modo NAT
- ISO: Kali Live amd64
- Nome: Practica24-Cliente-WEB

(b) Arrancar a máquina virtual.

(c) Comprobar a conectividade co portátil e co servidor WEB. Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español
$ ping -c2 IP_Portatil #Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Comprobar mediante o comando ping a conectividade coa interface de rede do portátil
$ nc -vz IP_Portatil 80 #Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Mediante o comando nc(netcat) comprobar se o porto 80 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 80 é o porto TCP a escanear.
$ nc -vz IP_Portatil 443 #Substituír IP_Portatil polo seu valor (ver táboa apartado 2b). Mediante o comando nc(netcat) comprobar se o porto 443 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 443 é o porto TCP a escanear.
```

(d) Realizar de novo os apartados (3d), (3e) e (3f). Indicar que acontece e por que.

NOTA: Se é necesario limpa as cookies para probar a autentificación cos 2 usuarios: `ana` e `brais`.

(e) Avisar ao docente para a revisión. ☐ 5

(6) Razoa e contesta brevemente:

(a) Modificamos o arquivo `.htaccess` do apartado (4d) descomentado a liña referente a `valid-user` e comentando a liña referente ao usuario `ana`, tal que así:

```
Require valid-user
#Require user ana
```

Que acontece se realizamos de novo o apartado (3f) dende o portátil e as máquinas virtuais xeradas nos hosts do alumnado? Por que?

NOTA: Se é necesario limpa as cookies para probar a autentificación cos 2 usuarios: `ana` e `brais`.

(b) Modificamos o arquivo `.htaccess` do apartado (4d) descomentado a liña referente a `valid-user` e comentando a liña referente ao usuario `ana`, tal que así:

```
Require valid-user
#Require user ana
```

Unha vez modificado recargamos a configuración do servidor Web Apache:

```
# /etc/init.d/apache2 reload #Recargar a configuración do servidor web Apache.
```

Que acontece se realizamos de novo o apartado (3f) dende o portátil e as máquinas virtuais xeradas nos hosts do alumnado? Por que?

NOTA: Se é necesario limpa as cookies para probar a autentificación cos 2 usuarios: `ana` e `brais`.

(c) Avisar ao docente para a entrega e revisión da práctica. ☐ 6

Revisión:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6