

RETO 1: SEGURIDAD EN SISTEMAS Y RED

INTRODUCCION

- Repositorio [Vulnhub](#)

Repositorio que recoge máquinas virtuales vulnerables por autor/nombre para poder practicar habilidades de seguridad. Pueden ser de escritorio o móvil. Varían en dificultad.

- Propuesta: realizar el **análisis y explotación de sus vulnerabilidades**. Informe de todo el proceso, y sus resultados.
- Máquina: [METASPLOITABLE 1](#), de una serie de dos máquinas.
- Ataque: vamos a realizar una ataque explotando una vulnerabilidad conocida en la versión 3.0.20 de samba para conseguir permisos de administrador y poder ejecutar comandos en la máquina. Una vez conseguido el acceso y los permisos cambiaremos la página web del servidor.

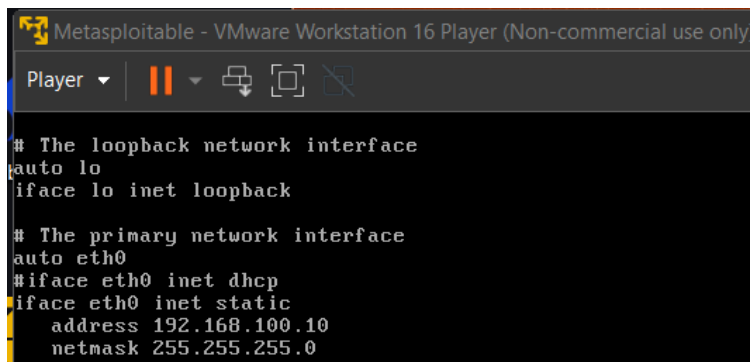
ENTORNO DE VIRTUALIZACIÓN

- Máquina Atacante: kali Linux 192.168.100.20/24
- Máquina víctima - metasploitable: Ubuntu 8.04 192.168.200.10/24

Ninguna puerta de enlace en las máquinas

En primer lugar, los comandos para cambiar la configuración de red

```
> Sudo nano /etc/network/interfaces
> Sudo /etc/init.d/networking restart
```



```
Metasploitable - VMware Workstation 16 Player (Non-commercial use only)
Player
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.100.10
netmask 255.255.255.0
```

Verificamos que ambas máquinas se pueden ver y están dentro de la misma red haciendo ping.


```
root@kali: /home/kali
File Actions Edit View Help
nmap 192.168.100.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 07:01 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.10
Host is up (0.0018s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:8B:F4:5B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Figura 1

1. Nmap -sV -sC < ip >

Ahora profundizamos más en el escaneo de puertos, lo que proporciona este comando es una lista de los softwares y su versión de los puertos que están disponibles en el servidor. Además, como vemos en varios de los puertos, por ejemplo, en el puerto 25, donde se está conectando a SMTP, el script *smtp-commands* de nmap ha podido hacer una lista de comandos que el servidor SMTP acepta tras una conexión, ayudándonos a entender que posibles comandos se pueden utilizar, y darnos pistas por qué camino podemos continuar el ataque.

COMANDOS DE NMAP

https://www.csirtcv.gva.es/wp-content/uploads/2020/05/NMAP-6_Listado-de-comandos.pdf

2. -sS

Al añadir este comando, el escaneo de puertos y servicios se convierte en una tarea menos intrusiva para la máquina víctima, además con esto también se puede añadir el comando *-spoofmac*, que permite cambiar la dirección MAC de mi máquina atacante.

El resultado del análisis lo vemos en las figuras 2,3,4.

Figura 2

```
Nmap scan report for 192.168.100.10
Host is up (0.0040s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ ssl-date: 2025-05-08T12:37:11+00:00; +27s from scanner time.
```

Figura 3

```
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10
with Suhosin-Patch)
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosi
n-Patch
|_ http-methods:
|_ Potentially risky methods: TRACE
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
|_ mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 8
|_ Capabilities flags: 43564
|_ Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, Speaks41Prot
ocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SupportsC
ompression
|_ Status: Autocommit
|_ Salt: j-g>8o+$q2D<An,-<'M0
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-date: 2025-05-08T12:37:11+00:00; +27s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat/5.5
```

```

MAC Address: 00:0C:29:BB:F4:5B (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2025-05-08T08:37:03-04:00
|_clock-skew: mean: 1h00m26s, deviation: 2h00m00s, median: 26s
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

```

figura 4

* **Nombres activos:** **METASPLOITABLE** y **WORKGROUP** son grupos de trabajo y máquinas activos que están siendo detectados en la red

En la larga lista de información, vamos a fijarnos en lo que nos interesa para este ataque. El puerto TCP 139 está abierto y ejecuta Samba smbd (versiones 3.x a 4.x), proporcionando servicios SMB a través del protocolo NetBIOS Session Service (netbios-ssn) dentro del grupo de trabajo WORKGROUP. Samba se utiliza para comunicar máquinas Linux dentro de una red windows y smbd es la parte de archivos e impresoras, y netbios es la API que se utiliza para comunicar máquinas en redes windows. Permite a los ordenadores identificarse con un nombre.

> nmap -v -sV 192.168.100.10 -p 139

-v es para obtener todos los pasos en detalle del análisis al puerto 139.

```

L$ nmap -v -sV 192.168.100.10 -p 139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-15 17:18 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 17:18
Scanning 192.168.100.10 [1 port]
Completed ARP Ping Scan at 17:18, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:18
Completed Parallel DNS resolution of 1 host. at 17:18, 13.02s elapsed
Initiating SYN Stealth Scan at 17:18
Scanning 192.168.100.10 [1 port]
Discovered open port 139/tcp on 192.168.100.10
Completed SYN Stealth Scan at 17:18, 0.05s elapsed (1 total ports)
Initiating Service scan at 17:18
Scanning 1 service on 192.168.100.10
Completed Service scan at 17:18, 11.03s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.100.10.
Initiating NSE at 17:18
Completed NSE at 17:18, 0.01s elapsed
Initiating NSE at 17:18
Completed NSE at 17:18, 0.01s elapsed
Nmap scan report for 192.168.100.10
Host is up (0.00078s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:BB:F4:5B (VMware)

Read data files from: /usr/share/nmap

```

```
> Nmblookup -A 192.168.100.10
```

```
$ nmblookup -A 192.168.100.10
Looking up status of 192.168.100.10
METASPLOITABLE <00> - B <ACTIVE>
METASPLOITABLE <03> - B <ACTIVE>
METASPLOITABLE <20> - B <ACTIVE>
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE>
WORKGROUP <00> - <GROUP> B <ACTIVE>
WORKGROUP <1d> - B <ACTIVE>
WORKGROUP <1e> - <GROUP> B <ACTIVE>

MAC Address = 00-00-00-00-00-00
```

Esto permite obtener los nombres de trabajo asociados a la ip utilizando la herramienta nmblookup. Metasploitable es el nombre del host y los sufijos de la derecha son para indicar que es el servidor de mensajes (03) y servidor de archivos (20). MS Browser indica que es el navegador principal que tiene los nombres de la red. GROUP es el nombre de dominio del grupo de trabajo

```
> nmap --scripts="all" 192.168.100.10 -p139 -N
```

```
| Workstation
|_ METASPLOITABLE 0.0 metasploitable server (Samba 3.0.20-Debian)
| smb-ls: Volume \\192.168.100.10\msfadmin
| SIZE    TIME                               FILENAME
| <DIR>   2025-05-12T07:52:18 .
| <DIR>   2010-04-16T06:16:02 ..
| <DIR>   2010-04-28T03:44:17 vulnerable
| <DIR>   2010-04-28T06:48:36 vulnerable\samba
| <DIR>   2010-04-28T07:12:05 vulnerable\mysql-ssl
| <DIR>   2010-04-16T20:37:02 vulnerable\twiki20030201
| <DIR>   2010-04-19T23:43:18 vulnerable\tikiwiki
|
| Volume \\192.168.100.10\opt
| SIZE    TIME                               FILENAME
| <DIR>   2025-05-12T07:52:18 .
| <DIR>   2010-04-28T21:25:52 ..
| 0       2025-05-12T06:03:55 5278.jsvc_up
| 260     2025-05-12T07:52:15 nmap-test-file
|
| Volume \\192.168.100.10\print$
| SIZE    TIME                               FILENAME
| <DIR>   2010-04-28T06:51:21 .
| <DIR>   2010-04-28T06:51:22 ..
| <DIR>   2010-04-28T06:33:43 W32X86
| <DIR>   2010-04-28T06:33:43 WIN40
|
| Volume \\192.168.100.10\tmp
| SIZE    TIME                               FILENAME
| <DIR>   2025-05-12T07:52:20 .
| <DIR>   2010-04-28T21:25:52 ..
| 0       2025-05-12T06:03:55 5278.jsvc_up
| 260     2025-05-12T07:52:15 nmap-test-file
```

```
smb: \vulnerable\> ls
.                D      0 Tue Apr 27 23:44:17 2010
..               D      0 Mon May 17 21:44:45 2010
samba            D      0 Wed Apr 28 02:48:36 2010
mysql-ssl        D      0 Wed Apr 28 03:12:05 2010
twiki20030201    D      0 Fri Apr 16 16:37:02 2010
tikiwiki         D      0 Mon Apr 19 19:43:18 2010
```

Este comando es genial para cuando no sabes que estás buscando exactamente durante el análisis de la máquina pero tu objetivo es un puerto en específico. Ejecuta cada uno de los scripts de nmap contra el puerto 139. Es un poco ir a lo loco, y seguramente no sea una práctica muy utilizada en entornos reales, sin embargo en este contexto no está mal utilizado. Además, extraemos un montón de información: usuarios y contraseñas que se pueden conectar a la máquina user:user y msfadmin:msfadmin, la versión exacta de samba que se está utilizando en el servidor.

Sabiendo todo esto podemos hacer varias cosas: una, y la que hice en primer lugar, fue empezar a moverme por los directorios en busca de archivos de configuración o archivos que tuviesen buena pinta. Es verdad que esto, en mi opinión, lo haría si tuviese mucho tiempo o supiese que el acceso que yo he ganado al servidor no lo pudiesen detectar con facilidad, ya que, es un proceso muy lento en el que más que “atacar” tu objetivo es estudiar el lugar al que has ganado acceso. Además, cuando conseguía meterme a recursos compartidos con el usuario msfadmin conseguía acceder a todos los servicios como samba, mysql-ssl... y podía descargarme archivos. Intente modificar algunos como my.cnf de mysql-ssl, y aunque podía ver usuario y contraseña para poder acceder a la base de datos, no conseguía conectarme y tampoco con los permisos de msfadmin podía reiniciar el servidor. Claro **que cuando hacía esto estaba dentro de smbclient, lo que tiene sentido que no pueda hacer nada desde ahí.**

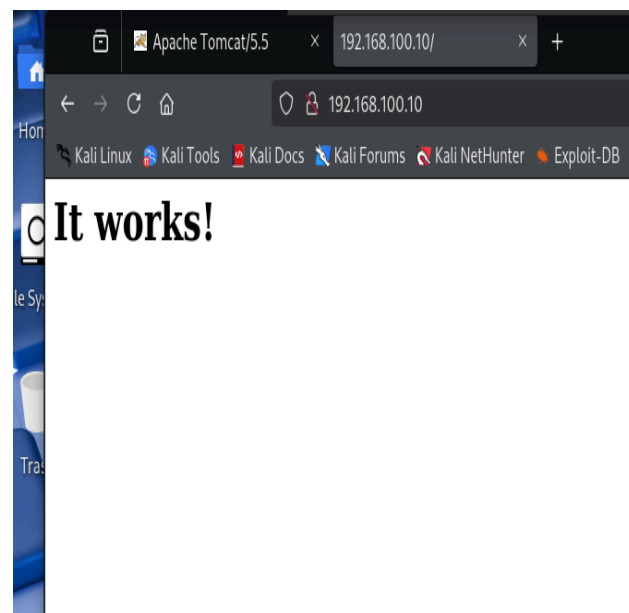
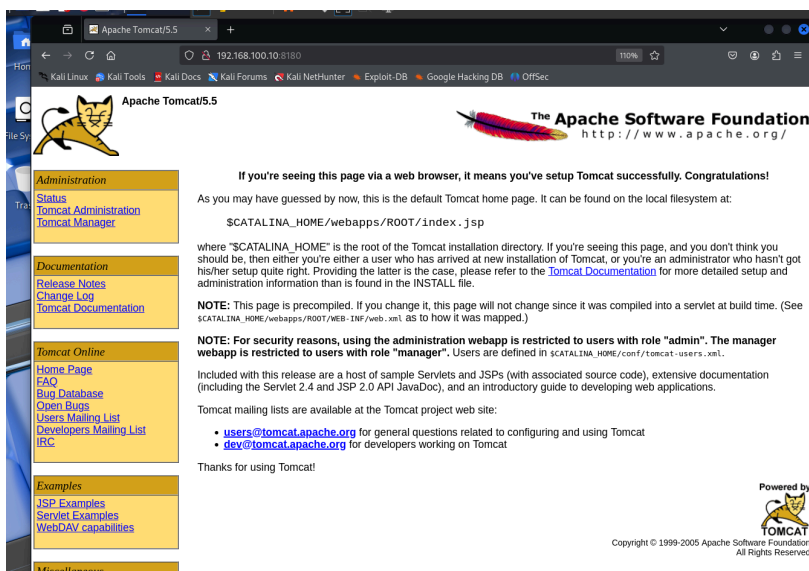
La otra cosa que se puede hacer, en vez de jugar a “¿qué comando funciona aquí?”, es que sabiendo las versiones de cada uno de los servicios disponibles en el servidor podemos buscar vulnerabilidades conocidas y usar **msfconsole**, **exploitable**.

Con esta herramienta explotamos la vulnerabilidad Samba "username map script" Command Execution 2007-05-14

Esta vulnerabilidad se basa en los scripts para mapear usuarios. Lo que hacen es traducir estos usuarios y grupos de Linux a los equivalentes en windows y viceversa. El error que se aprovecha es que no se valida de forma correcta la entrada en los scripts. Cuando se realiza una petición al servidor Samba para autenticarse o pedir recursos y entonces realiza una inyección de comandos: usermap-script "usuario; rm -rf /tmp/ataque"
Estamos dentro, en la carpeta raíz con permisos de administrador. Además de que podemos parar y reiniciar los servicios cuando queramos.



He navegado por los directorios y como anteriormente había visto index.html con el siguiente msfadmin al smbclient, además de que durante el escaneo de puerto y listado de directorios puedes ver que se aloja una página web. Como ya se como ganar acceso al servidor, una vez lo consiga quiero hacer algo más. Decidi cambiar su página web:



Ahora solo toca buscarlo. He buscado dentro del root, donde se me ha ocurrido mirar porque en srv no había nada. Habría supuesto que es services. En el archivo log que hay aparecen todos mis accesos. Este archivo se puede borrar y se debe, tras el ataque para no dejar rastro. Pregunte a chat gpt donde podía encontrar típicamente en un servidor web la página index.html y me dijo:

EN QUE DIRECTORIO SUEKE ESTAR ALOJADA UNA PAGINA WEB
INDEX.HTML CUANDO TENGO EL APACHE2

Cuando tienes instalado **Apache2** en un sistema Linux (como Ubuntu, Debian o derivados), la página web `index.html` suele estar alojada en un directorio predeterminado. Este directorio es donde Apache busca los archivos de las páginas web para servirlos a los usuarios.

En sistemas basados en Debian/Ubuntu:

El directorio predeterminado para los archivos de la página web (incluyendo `index.html`) es:

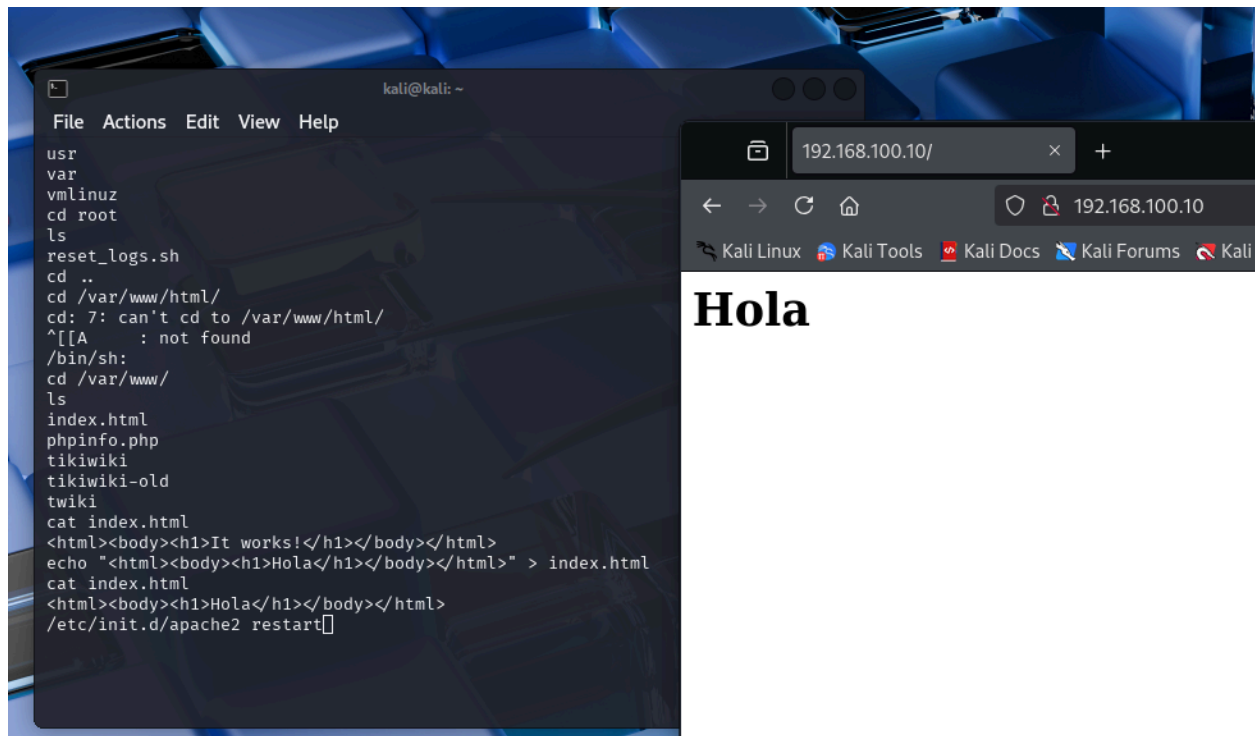
```
bash
```

 Copiar

```
/var/www/html/
```



Entonces, ya solo me falta modificar el código HTML. PERO aquí me encuentre con otro problema: lo que estaba utilizando el script para poder ganar acceso al servidor con permisos de root no implicaba que yo podía acceder a los recursos de la máquina, como por ejemplo el editor nano o vim. Por lo tanto, se me ocurrió utilizar el comando **echo “<html>” > index.html** para **sobreescribir en él**.



- METASPLOIT

Es una herramienta creada en 2003 por H.D Moore de código abierto que se utiliza para analizar y explotar las vulnerabilidades que encontramos en un sistema. Tiene una base de datos de exploits para vulnerabilidades conocidas CVE. Tiene una arquitectura modular. La línea de comandos se llama MSFconsole.