INTRODUCCIÓN

Se realizó una prueba de penetración a la máquina vulnerable Metasploitable con IP 10.0.2.7 desde una máquina atacante Kali Linux con IP 10.0.2.5 con el objetivo de encontrar y explotar vulnerabilidades.

METASPLOTABLE

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:7f:c0
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:7fc0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:35 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4664 (4.5 KB)  TX bytes:7116 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

KALI LINUX

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::3016:49cf:f5c7:f88e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ad:25:87  txqueuelen 1000  (Ethernet)
        RX packets 1677453  bytes 2522283637 (2.3 GiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 146264  bytes 9349040 (8.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IDENTIFICACIÓN DE VULNERABILIDADES

El primer paso fue escanear la máquina Metasploitable usando la herramienta nmap (**nmap -sV 10.0.2.7**). Me arrojó puertos abiertos, los servicios que corren y sus versiones.

```
Nmap scan report for 10.0.2.7
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:39:7F:C0 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.95 seconds
```

Los resultados arrojan muchos puertos abiertos con servicios corriendo y sus respectivas versiones. Aquí hablaremos sobre algunos de ellos y de sus respectivas vulnerabilidades:

Puerto 21/TCP - SERVICE: ftp - VERSION: vsftpd 2.3.4

Puerto 22/TCP - SERVICE: ssh - VERSION: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

La versión 4.7p1 es vulnerable a múltiples fallos, como ataques de fuerza bruta debido a configuraciones débiles (por ejemplo, permitir autenticación por contraseña).

Puerto 23/TCP - SERVICE: telnet - VERSION: Linux telnetd

Telnet transmite datos sin cifrar, lo que lo hace extremadamente inseguro. Credenciales y datos pueden ser fácilmente interceptados por atacantes.

Puerto 25/TCP - SERVICE: smtp - VERSION: Postfix smtpd

Versiones antiguas de Postfix pueden ser vulnerables a ataques como buffer overflow o remote code execution (RCE).

Puerto 80/TCP - SERVICE: http - VERSION: Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Apache 2.2.8 es una versión antigua y ha alcanzado su fin de soporte, por lo que contiene multiples vulnerabilidades.

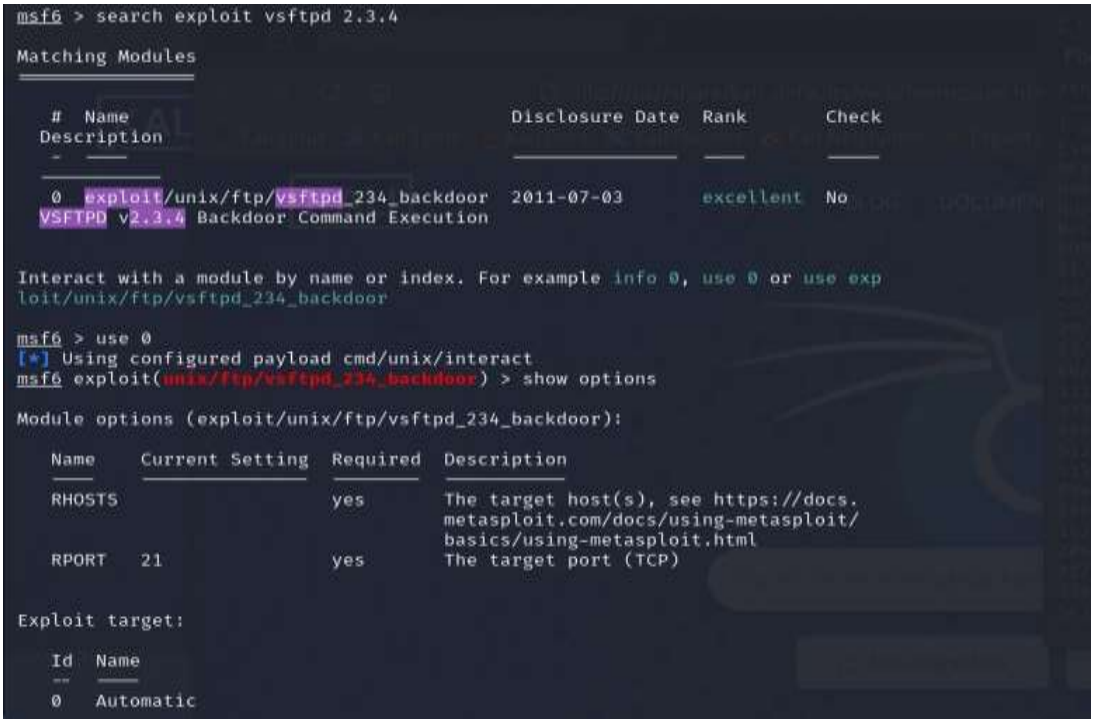
Puerto 5432/TCP – SERVICE: postgresql – VERSION: PostgreSQL DB 8.3.0 – 8.3.7

PostgreSQL en las versiones 8.3.0 a 8.3.7 es antigua y contiene múltiples vulnerabilidades conocidas que podrían comprometer la base de datos y el sistema subyacente. Estas son las principales amenazas:

Para esta práctica, se eligió explotar la vulnerabilidad asociada al servicio ftp con versión vsftpd 2.3.4 que, **según el CVE-2011-2523, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp.**

EXPLOTACIÓN DE VULNERABILIDADES

Se inició metasploit framework en la terminal de la máquina atacante, se buscó el exploit asociado a la vulnerabilidad señalada y se configuró con la IP de la máquina objetivo. Finalmente, se le dio “run”.



PROPUESTA DE MITIGACIÓN

Actualizar servicios y sistemas:

- Mantener los servicios y sistemas operativos actualizados con las últimas versiones y parches de seguridad.
- Usa herramientas como Unattended Upgrades en Debian/Ubuntu para automatizar las actualizaciones.

Control de acceso:

- Implementa un firewall (como UFW o iptables) para permitir el acceso solo desde direcciones IP específicas.
- Usa una VPN para proteger el acceso a servicios críticos.

Cifrado de datos:

- Habilita SSL/TLS para servicios como HTTP, SMTP y PostgreSQL para proteger las transmisiones de datos.

Supervisión y auditoría:

- Implementa sistemas de monitoreo como Nagios, Zabbix o ELK Stack para registrar la actividad de los servicios.
- Configura alertas para actividades sospechosas, como intentos de fuerza bruta o accesos no autorizados.

Deshabilitar servicios innecesarios:

- Si algún servicio (como Telnet o WebDAV) no es requerido, desactívalo para reducir la superficie de ataque.

Seguridad en contraseñas:

- Aplica políticas de contraseñas robustas (mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos).
- Deshabilita la autenticación basada en contraseñas en servicios como SSH y utiliza claves públicas/privadas.

CONCLUSIONES

- **La obsolescencia de software aumenta los riesgos**:
Los servicios identificados (vsftpd 2.3.4, OpenSSH 4.7p1, Apache 2.2.8, PostgreSQL 8.3.7) utilizan versiones desactualizadas que contienen vulnerabilidades conocidas. Actualizar a versiones compatibles y soportadas es crítico para mantener la seguridad del sistema.

- **La exposición innecesaria de servicios es peligrosa**:
Servicios como **Telnet** y **FTP**, que transmiten datos en texto plano, son inherentemente inseguros y deben ser desactivados o reemplazados por alternativas modernas como **SSH** y **SFTP**.

- **La falta de cifrado compromete la confidencialidad de los datos**:
Los servicios HTTP y SMTP no cifrados facilitan ataques de intercepción (MITM) y la exposición de credenciales. Implementar SSL/TLS en todos los servicios es esencial para proteger las comunicaciones.

- **La configuración predeterminada expone al sistema a ataques**:
Malas configuraciones, como servidores SMTP configurados como relays abiertos o permisos laxos en WebDAV, permiten a los atacantes abusar del sistema para sus fines. Es vital revisar y endurecer las configuraciones de cada servicio.

- **La falta de controles de acceso aumenta la superficie de ataque**:
Sin restricciones en los archivos de configuración de PostgreSQL o reglas de firewall, cualquier atacante puede intentar explotar vulnerabilidades desde la red. Limitar accesos a direcciones IP específicas reduce significativamente este riesgo.

- **La supervisión y auditoría son cruciales**:
Sin un monitoreo constante, los sistemas pueden ser explotados sin detección. Herramientas de monitoreo y registro como **Fail2Ban**, **Nagios**, o **SIEM** ayudan a identificar actividades sospechosas y responder a ellas rápidamente.

- **La seguridad es un proceso continuo**:
No basta con implementar mitigaciones una vez. Es fundamental realizar auditorías periódicas, aplicar parches regularmente y mantenerse actualizado sobre nuevas amenazas.