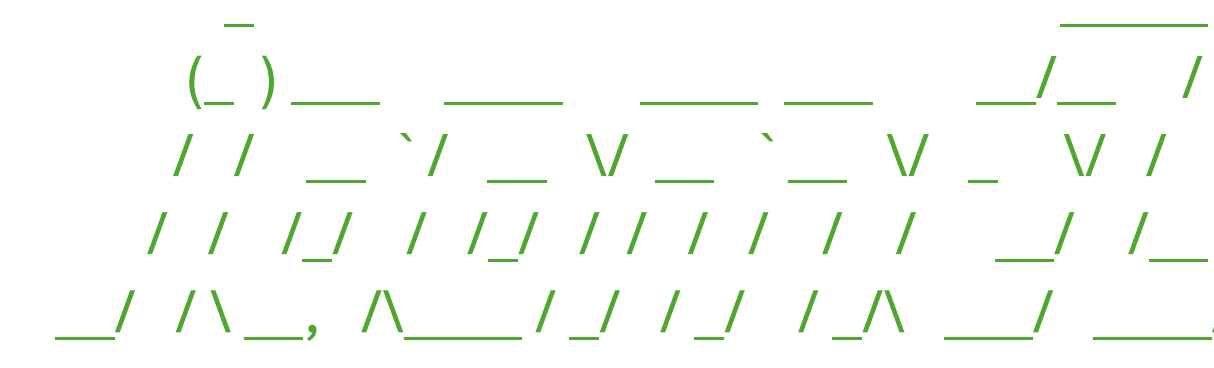
Laboratorio de Hardening Defensivo - Servidor Rocky Linux 9.6



by Jonathan Gomez - 6c 6c 65 76 61 6d 6f 73 20 75 6e 20 6d 75 6e 64 6f 20 6e 75 65 76 6f 20 65 6e 20 6e 75 65 73 74 72 6f 73 20 63 6f 72 61 7a 6f 6e 65 73

Índice

Contents

---

1. Introducción y Objetivos

⚠ **Nota Educativa**: Este laboratorio se realizó en un entorno controlado con fines educativos. Las técnicas mostradas deben utilizarse únicamente en sistemas con autorización explícita.

Objetivos:

- Identificar vulnerabilidades en un servidor Rocky Linux 9.6 sin hardening.
- Aplicar medidas defensivas mediante firewall (firewalld).
- Implementar protección contra ataques de fuerza bruta con fail2ban.
- Validar la efectividad de las configuraciones mediante pruebas controladas.

2. Estado Inicial del Servidor

Escaneo de Puertos y Servicios

Resultado del escaneo Nmap

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.5

22/tcp open ssh OpenSSH 8.7

80/tcp open http Apache httpd 2.4.62

3306/tcp open mysql MariaDB 10.3.23 o anterior

Vulnerabilidades Identificadas

1. **Ping Permitido** (ICMP echo request/reply)
2. **Fuerza Bruta SSH Posible**
3. **FTP Anónimo Habilitado**
4. **Servicios Expuestos Sin Restricciones**

Pruebas Iniciales desde maquina Parrot OS

#Permite ping

ping 192.168.0.104

64 bytes from 192.168.0.104: icmp_seq=1 ttl=64 time=1.10 ms

64 bytes from 192.168.0.104: icmp_seq=2 ttl=64 time=1.90 ms

64 bytes from 192.168.0.104: icmp_seq=3 ttl=64 time=2.22 ms

#Permite ping grandes

ping -s 1000 192.168.0.104

1008 bytes from 192.168.0.104: icmp_seq=1 ttl=64 time=2.26 ms

1008 bytes from 192.168.0.104: icmp_seq=2 ttl=64 time=2.65 ms

1008 bytes from 192.168.0.104: icmp_seq=3 ttl=64 time=2.37 ms

#Ataque de fuerza bruta con hydra permite múltiples intentos

hydra -l root -P /usr/share/wordlists/rockyou.txt -t 4 -vV -f -o hydra_results.txt ssh://192.168.0.104

[INFO] Successful, password authentication is supported by ssh://192.168.0.104:22

[ATTEMPT] target 192.168.0.104 - login "root" - pass "123456" - 1 of 14344399 [child 0] (0/0)

[ATTEMPT] target 192.168.0.104 - login "root" - pass "12345" - 2 of 14344399 [child 1] (0/0)

[ATTEMPT] target 192.168.0.104 - login "root" - pass "123456789" - 3 of 14344399 [child 2] (0/0)

[ATTEMPT] target 192.168.0.104 - login "root" - pass "password" - 4 of 14344399 [child 3] (0/0)

[ATTEMPT] target 192.168.0.104 - login "root" - pass "iloveyou" - 5 of 14344399 [child 3] (0/0)

#Ataque de fuerza bruta con hydra permite múltiples intentos

ftp 192.168.0.104

220 Servicio FTP Empresa

Name (192.168.0.104:user): anonymous

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp>

#MySQL servicio expuesto

mysql -u usuario_prueba -p -h 192.168.0.104

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 142

Server version: 10.3.23-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

3. Configuración Defensiva con Firewall

Política Base y Configuración Inicial

Establecer política por defecto DROP

sudo firewall-cmd --set-default-zone=drop

sudo firewall-cmd --permanent --zone=drop --add-interface=enp0s3

sudo firewall-cmd –reload

Reglas Específicas por Servicio

SSH - Acceso Restringido

Solo permitir desde IP administrativa

sudo firewall-cmd --permanent --add-rich-rule='

rule family="ipv4"

source address="192.168.0.100"

port port="22"

protocol="tcp"

accept'

Bloquear SSH desde otras IPs

sudo firewall-cmd --permanent --add-rich-rule='

rule family="ipv4"

source address="0.0.0.0/0"

port port="22"

protocol="tcp"

reject'

FTP - Red Local Only

FTP y puertos pasivos solo para red local

sudo firewall-cmd --permanent --add-rich-rule='

rule family="ipv4"

source address="192.168.0.0/24"

port port="21"

protocol="tcp"

accept'

sudo firewall-cmd --permanent --add-rich-rule='

rule family="ipv4"

source address="192.168.0.0/24"

port port="30000-31000"

protocol="tcp"

accept'

HTTP/HTTPS - Acceso Público Controlado

sudo firewall-cmd --permanent --add-service=http

sudo firewall-cmd --permanent --add-service=https

Limitar tasa de conexiones anti-DDoS

sudo firewall-cmd --permanent --add-rich-rule='

rule family="ipv4"

port port="80"

protocol="tcp"

limit value="25/m"

accept'

MySQL - Solo Red Local

sudo firewall-cmd --permanent --add-rich-rule='

rule family="ipv4"

source address="192.168.0.0/24"

port port="3306"

protocol="tcp"

accept'

Bloqueo ICMP y Puertos Innecesarios

Bloquear ping

sudo firewall-cmd --permanent --add-icmp-block=echo-request

sudo firewall-cmd --permanent --add-icmp-block=echo-reply

Cerrar puertos no utilizados

sudo firewall-cmd --permanent --remove-port=8080/tcp

sudo firewall-cmd --permanent --remove-port=9090/tcp

Ocultar Versión FTP

sudo tee -a /etc/vsftpd/vsftpd.conf <<EOF

ftpd_banner=Servicio FTP Empresa

hide_ids=YES

EOF

sudo systemctl restart vsftpd

---

4. Protección de Servicios con Fail2Ban

Instalación y Configuración Base

sudo dnf install epel-release -y

sudo dnf install fail2ban fail2ban-firewalld -y

sudo systemctl enable fail2ban

sudo systemctl start fail2ban

(no se debe configurar directamente jail.conf)

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

sudo systemctl status fail2ban

Configuración de Jails

SSH Protection

sudo nano /etc/fail2ban/jail.d/sshd.local

[sshd]
enabled = true
port = ssh
logpath = /var/log/secure
maxretry = 3
findtime = 300
bantime = 600
ignoreip = 127.0.0.1/8 192.168.0.100

FTP Protection

sudo nano /etc/fail2ban/jail.d/vsftpd.local

[vsftpd]
enabled = true
port = ftp,ftp-data,ftps,ftps-data
logpath = /var/log/vsftpd.log
maxretry = 3
findtime = 300
bantime = 600

Apache Protection

sudo nano /etc/fail2ban/jail.d/apache.local

[apache-auth]
enabled = true
port = http,https
logpath = /var/log/httpd/error_log
maxretry = 3
bantime = 600

[apache-badbots]
enabled = true
port = http,https
logpath = /var/log/httpd/access_log
maxretry = 2
bantime = 86400

MySQL Protection

sudo nano /etc/fail2ban/jail.d/mysql.local

[mysqld-auth]
enabled = true
port = 3306

logpath = /var/log/mysqld.log
maxretry = 3
bantime = 600

Ver los estados de las jaulas

sudo fail2ban-client status
sudo fail2ban-client status sshd

sudo fail2ban-client status vsftpd

sudo fail2ban-client status apache-auth

sudo fail2ban-client status

Status

|- Number of jail: 3

`- Jail list: apache-auth, sshd, vsftpd

Pruebas de Protección

SSH - Fuerza Bruta Bloqueada

sudo fail2ban-client status sshd

Status for the jail: sshd

|- Filter

| |- Currently failed: 0

| |- Total failed: 0

| ` - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session

` - Actions

|- Currently banned: 0

|- Total banned: 0

` - Banned IP list:

 # Intentos fallidos resultan en baneo

sshpass -p "wrongpass1" ssh testuser1@192.168.0.104

sshpass -p "wrongpass2" ssh testuser2@192.168.0.104

sshpass -p "wrongpass3" ssh testuser3@192.168.0.104

Verificar baneo

[root@localhost ~]# sudo fail2ban-client status sshd

Status for the jail: sshd

|- Filter

| |- Currently failed: 0

| |- Total failed: 3

| ` - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session

` - Actions

|- Currently banned: 1

|- Total banned: 1

` - Banned IP list: 192.168.0.54

#Comando para desbanear ip
sudo fail2ban-client set sshd unbanip 192.168.0.54

Apache - Autenticación Protegida

Crear directorio protegido

sudo mkdir -p /var/www/html/protected

sudo htpasswd -c /etc/httpd/.htpasswd testuser

Intentos de acceso no autorizado

curl -u wronguser:wrongpass http://192.168.0.104/protected/

---

5. Resultados Post-Hardening

Escaneo Final

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.5 (solo desde red local)

80/tcp open http Apache httpd 2.4.62

Mejoras Implementadas

1. ✅ **ICMP Bloqueado**: Ping y ping grandes filtrados
2. ✅ **SSH Restringido**: Solo desde IP administrativa
3. ✅ **FTP Seguro**: Anónimo deshabilitado, solo red local
4. ✅ **HTTP Limitado**: Protección contra DDoS
5. ✅ **MySQL Local**: Acceso solo desde red interna
6. ✅ **Fail2Ban Activo**: Protección multi-servicio

Verificación de Estado

bash

Estado general de fail2ban

sudo fail2ban-client status

Reglas de firewall

sudo firewall-cmd --list-all

🎯 Conclusión

Este laboratorio demostró la efectividad de un enfoque defensivo por capas:

- **Capa 1**: Firewall para control de acceso básico
- **Capa 2**: Configuración segura de servicios
- **Capa 3**: Fail2Ban para protección dinámica

📚 **Nota Final**: Este material es educativo y debe adaptarse a entornos productivos considerando políticas organizacionales y requisitos específicos de cada servicio.

Laboratorio Defensivo - Rocky Linux 9.6
Entorno Controlado - Fines Educativos