LPIC2 2021 Sesión 15 (2021-03-23)

Documentación relacionada:

- Manual Certificacion LPIC-2.pdf, pag XX
- Material Practicas LPIC-2/LPIC-202/
- Presentaciones/2020/202/
- gdrive://

Clase

- DOC: Material Practicas LPIC-2/LPIC-202/7-System Security/
  - NMAP: Guia_Avanzada_Nmap.pdf
  - metasploit https://metasploit.com

fail2ban

- DOC: Proteger SSH VSFPD con fail2ban.pdf
- **ignoreip**
  - incluir 127.0.0.1 y la IP del server
- **bantime**: tiempo que está un servidor bloqueado
- **findtime**: en que periodo de tiempo se mira para ver si ha llegado al maxretry
- **maxretry**: número de intentos fallidos

- /etc/jail2ban/jail.d/sshd.local

```
[sshd]
enabled = true
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
sendmail-whois[name=SSH, dest=root, sender=fail2ban@example.com]
logpath = /var/log/secure
maxretry = 5
```

  - requiere **firewalld** activo
- `fail2ban-client status sshd`
- `fail2ban-client set sshd unbanip IPADDRESS`
- `fail2ban-client set sshd banip IPADDRESS`
- `fail2ban-client get sshd maxretry|bantime`
- configurar desde línea de comando (no persistencia?):
  - `fail2ban-client set sshd findtime <TIME>`
  - `fail2ban-client set sshd bantime <TIME>`

iptables

- DOC: Laboratorio Iptables.doc.pdf
- DOC: iptables scripts.zip
- tablas:
  - FILTER

        - cadenas:
            - INPUT
            - OUTPUT
            - FORWARD
    - NAT:
        - cadenas:
            - PREROUTING
            - POSTROUTING
            - OUTPUT
- cerramos todo por defecto y habilito aquello que me interesa
    - BOGON: https://en.wikipedia.org/wiki/Bogon_filtering

firewall-politica-drop.sh

```
#!/bin/bash
echo -n Aplicando Reglas de Firewall...
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
## Establecemos politica predeterminadas
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
## Denegacion BOGON NETS
iptables -A PREROUTING -s 0.0.0.0/8 -j DROP
iptables -A PREROUTING -s 10.0.0.0/8 -j DROP
iptables -A PREROUTING -s 169.254.0.0/16 -j DROP
iptables -A PREROUTING -s 172.16.0.0/12 -j DROP
iptables -A PREROUTING -s 192.88.99.0/24 -j DROP
iptables -A PREROUTING -s 198.18.0.0/15 -j DROP
iptables -A PREROUTING -s 198.51.100.0/24 -j DROP
iptables -A PREROUTING -s 203.0.113.0/24 -j DROP
iptables -A PREROUTING -s 224.0.0.0/4 -j DROP
iptables -A PREROUTING -s 240.0.0.0/4 -j DROP
## Se permite accesos full a la loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
## Reglas de entrada
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
# Solo se permite acceso a 443 y 10000 con origen la 1.2 (registrado)
iptables -A INPUT -p tcp -s 192.168.1.2 -m multiport --dports 443,10000 -j LOG
--log-prefix 'Acceso HTTPS/Webmin' --log-level 4
iptables -A INPUT -p tcp -s 192.168.1.2 -m multiport --dports 443,10000 -j
ACCEPT
iptables -A OUTPUT -p tcp -d 192.168.1.2 -m multiport --sports 443,10000 -j
ACCEPT
## Reglas de salida a DROP. No se permite tráfico saliente originado en el
equipo
## Revisar con "iptables -nvL --line-numbers"
```

- abrimos todo por defecto. Me ahorro las «vueltas» (OUTPUT). Cerramos al final

; firewall-politica-accetp.sh

```
#!/bin/bash
## SCRIPT de IPTABLES - ejemplo del manual de iptables
## Ejemplo de script para proteger la propia máquina
#echo -n Aplicando Reglas de Firewall...
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
## Empezamos a filtrar
# El localhost se deja (por ejemplo conexiones locales a mysql)
/sbin/iptables -A INPUT -i lo -j ACCEPT
# A w7 acceeso a putty -22
iptables -A INPUT -s 192.168.1.105 -p tcp --dport 22 -j ACCEPT
#Permitir a w2003
iptables -A INPUT -s 192.168.1.7 -p icmp --icmp-type echo-request -j ACCEPT
# A nuestra IP le dejamos todo
iptables -A INPUT -s 192.168.1.5 -j ACCEPT
# Denegamos a r6 acceder a apache de r5
iptables -A OUTPUT -d 192.168.1.6 -p tcp --dport 80 -j DROP

# A w2003 entra a  mysql
iptables -A INPUT -s 192.168.1.7 -p tcp --dport 3306 -j ACCEPT

# A R5 dejamos consultar nuestro DNS
iptables -A INPUT -s 192.168.1.6 -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -s 192.168.1.6 -p udp --dport 53 -j ACCEPT

# A w2003 le dejamos usar el FTP
iptables -A INPUT -s 192.168.1.7 -p tcp --dport 20:21 -j ACCEPT
# A w2003 le dejamos acceso al Apache.
iptables -A INPUT -s 192.168.1.105 -p tcp --dport 80 -j ACCEPT
# A w7 accede a webmin
iptables -A INPUT -s 192.168.1.105 -p tcp --dport 10000 -j ACCEPT


#Cerramos rango de los puertos privilegiados. Cuidado con este tipo de
# barreras, antes hay que abrir a los que si tienen acceso.
iptables -A INPUT -p tcp --dport 1:65000 -j DROP
iptables -A INPUT -p udp --dport 1:65000 -j DROP
#Si ponemos la opción REJel servidor da mensaje de que no se puede acceder.
iptables -A INPUT -s 0.0.0.0/0 -p icmp --icmp-type echo-request -j REJECT
```

- https://www.pfsense.org/
  - https://www.bellera.cat/josep/pfsense/installacio_cs.html

OpenVPN