

LPIC2 2021 Sesión 15 (2021-03-23)

Documentación relacionada:

- Manual Certificación 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

OpenVPN

From:
<https://miguelangel.torresegea.es/wiki/> - **miguel angel torres egea**

Permanent link:
<https://miguelangel.torresegea.es/wiki/info:cursos:pue:lpic2-2021:s15?rev=1616524953>

Last update: **23/03/2021 11:42**

