Scan the target ip, find some weird smtpd caked Haraka on it, so we’ll search for it in searchsploit (3)

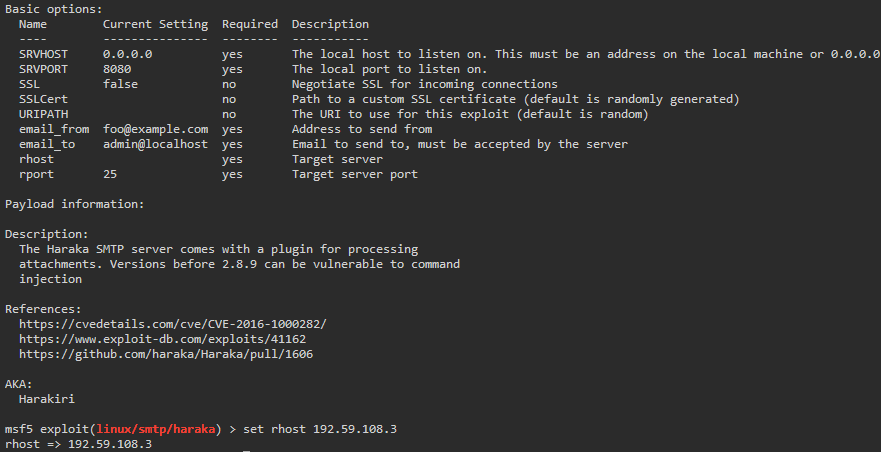
Then, we have a path (4) showing us the Metasploit moule associated with it.



…

Some basic info about the haraka remote command execution.

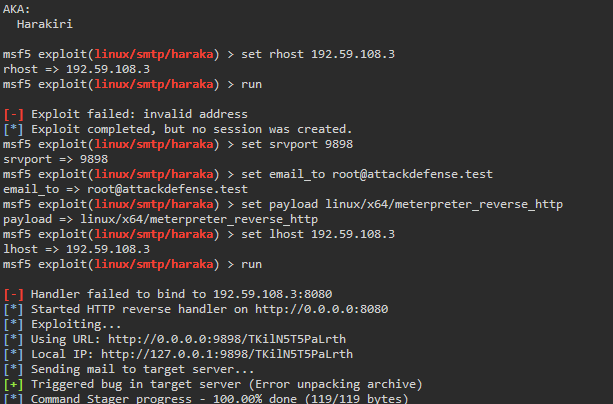
Let’s set the rhost to the target



Running it fails. Set a srv port, an email, and a payload.

You just gotta magic your way into knowing the payload is this metrepeter reverse shell and that all the other stuff like an lhost is needed, since the instructors sucked at explaining the significance of these elements or how we know how to fill them out.

So, just do it, I guess.



…

This would create a session if things were solid, but no methodology is explained, so an actual solution to this exception cannot be resolved.

What a failure, I guess.

