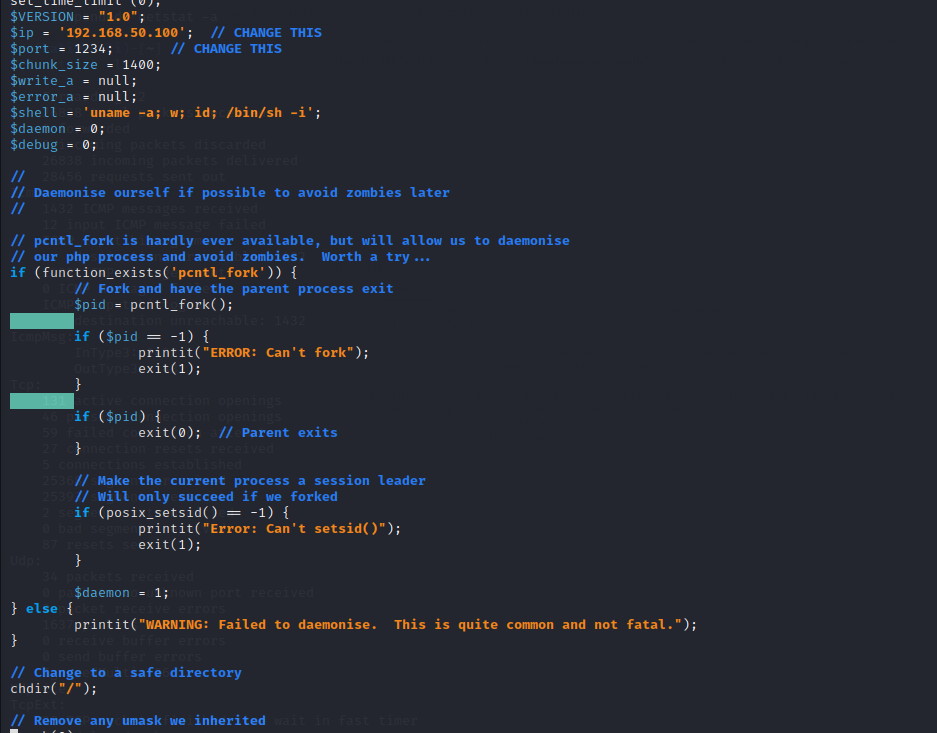
**Report reverse shell**

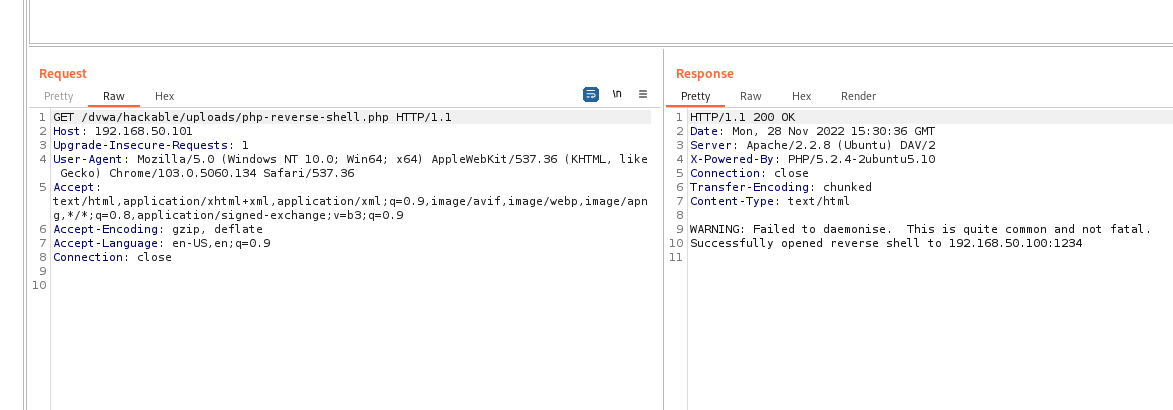
La task odierna richiedeva di sfruttare un file upload sulla DVWA, caricando una shell in php. Gli step verrando monitorati tramite il tool kali linux Burpsuite.

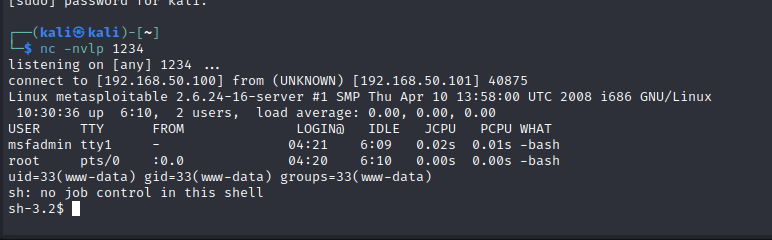
Ci assicuriamo innanzitutto che Metasploitable e Kali linux siano in comunicazione tramite ping.

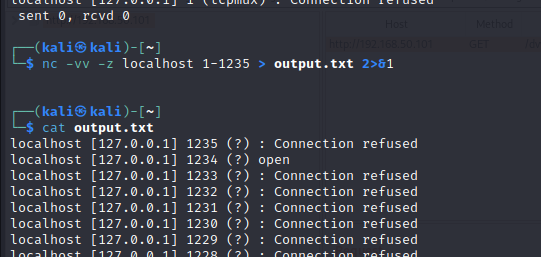
Scarichiamo quindi una reverse shell (<https://github.com/pentestmonkey/php-reverse-shell> , in questo caso specifico)



(Sample della reverse shell in cui andremo opportunamente a cambiare Ip e numero della porta, in questo caso è stato inserito l’ip di kali ed una porta di default).

Sfruttiamo quindi la vulnerabilità della DVWA che permette l’upload di un file, caricando la reverse ed intercettettando l’invio tramite BurpSuite, ripetendo l’operazione una volta che sarà stato attivato il comando d’ascolto sulla porta.





Ipoteticamente ciò permetterebbe ad un utente malintenzionato di stabilire una connessione remota tra il proprio server e quello del target.