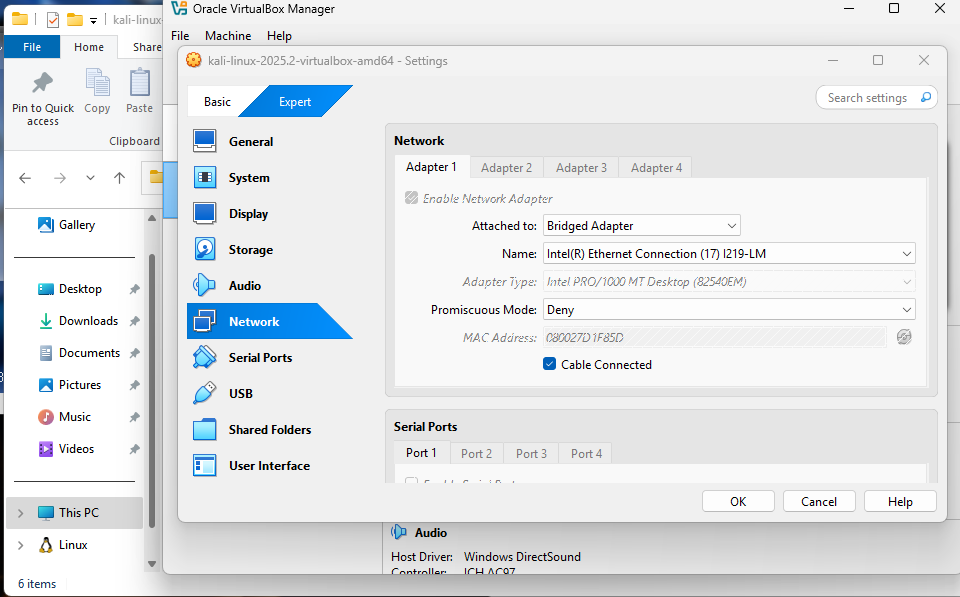
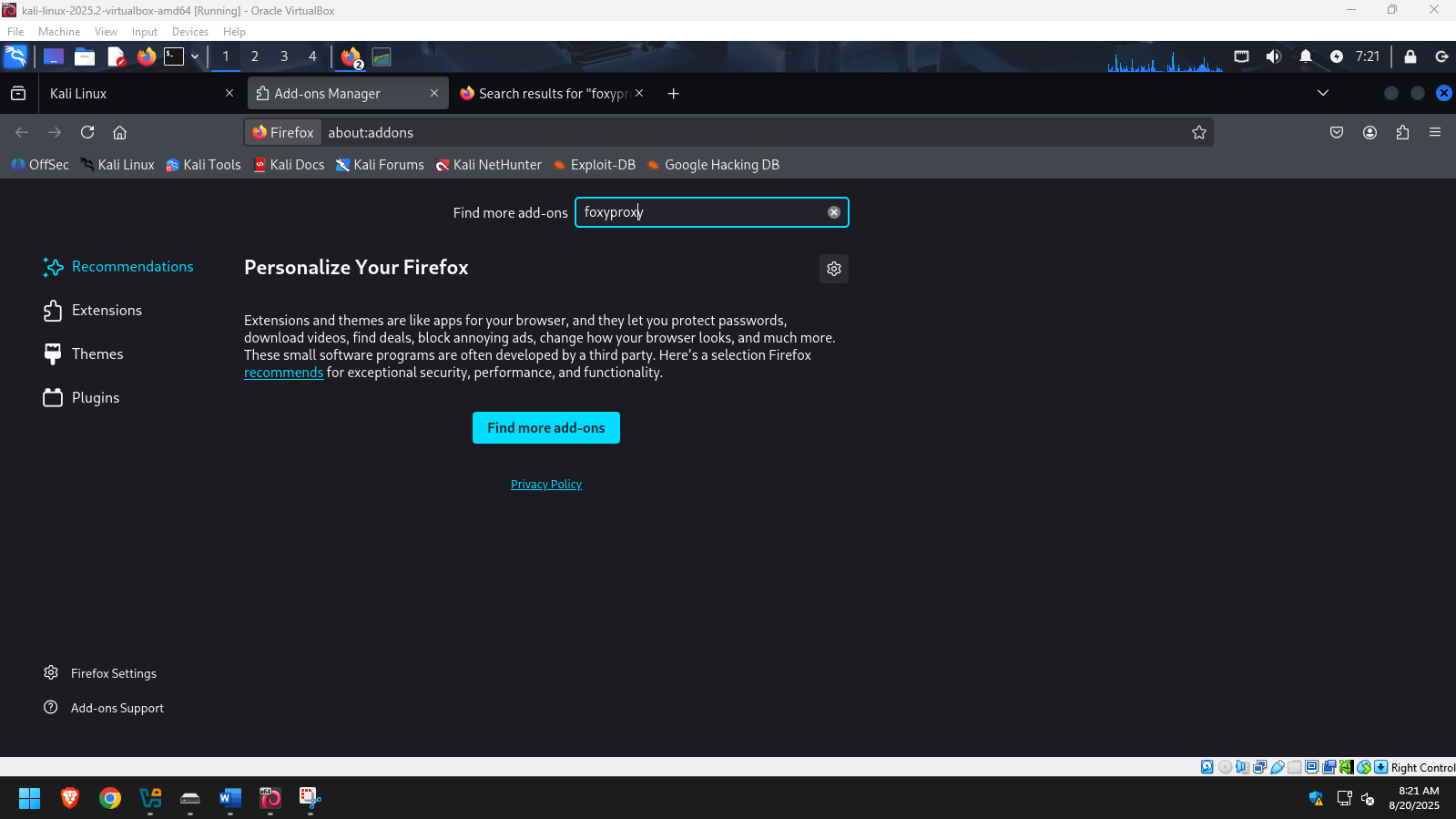
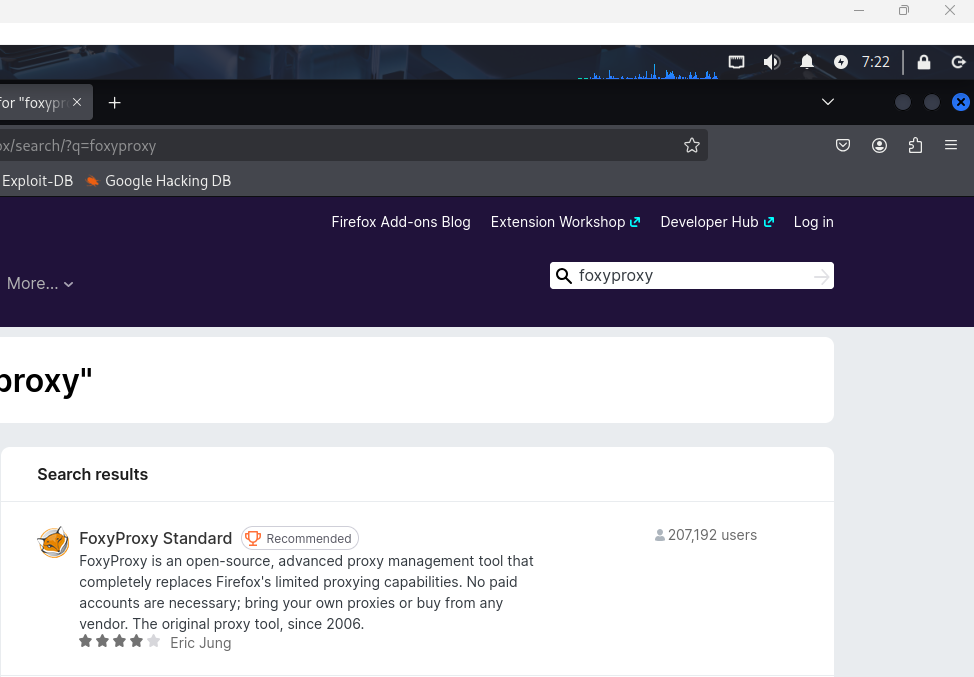
1# - No Kali:

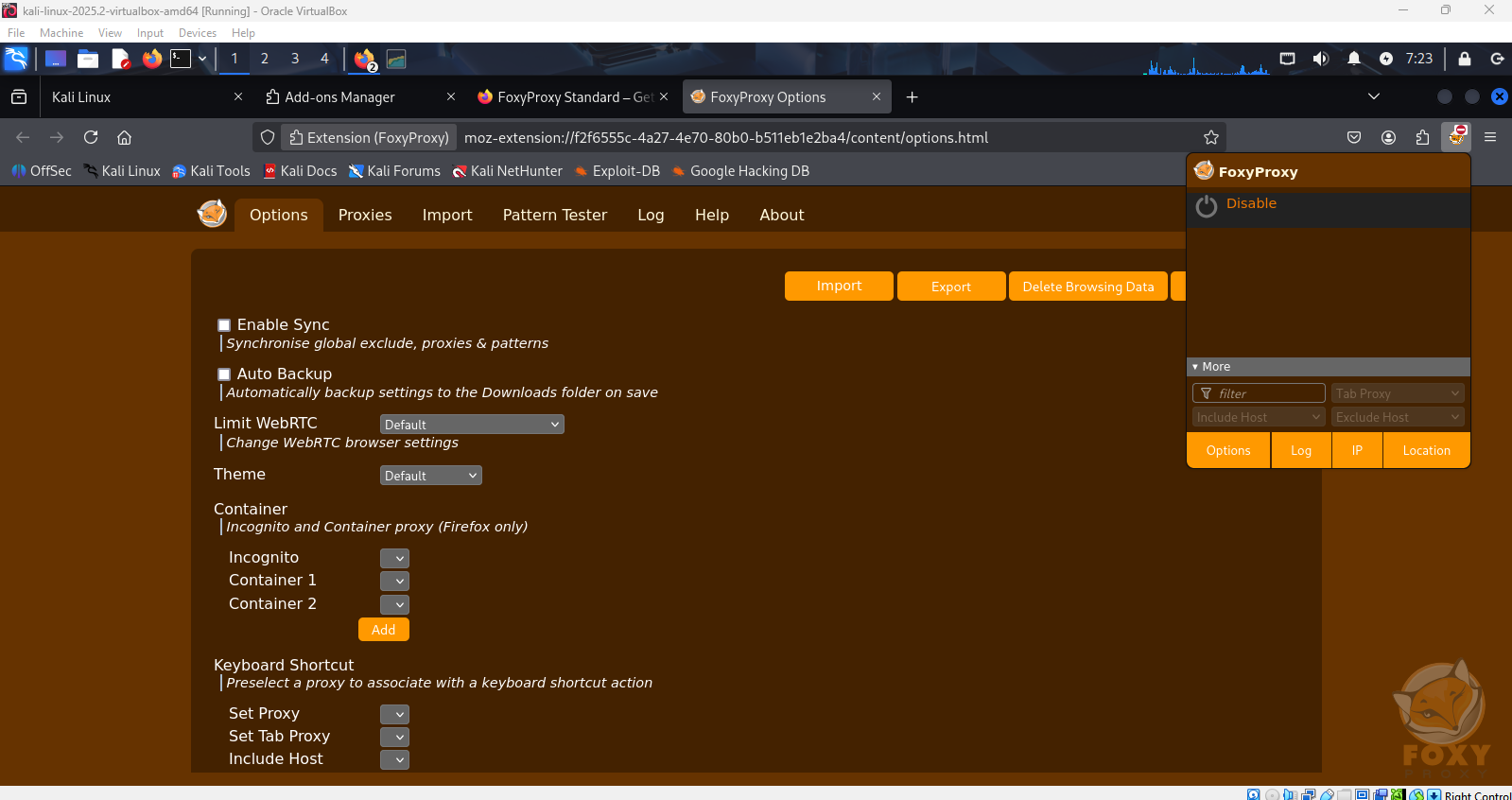
2# - \*Mudaremos o adaptador 1 para NAT num primeiro momento porque a fiap não funciona.



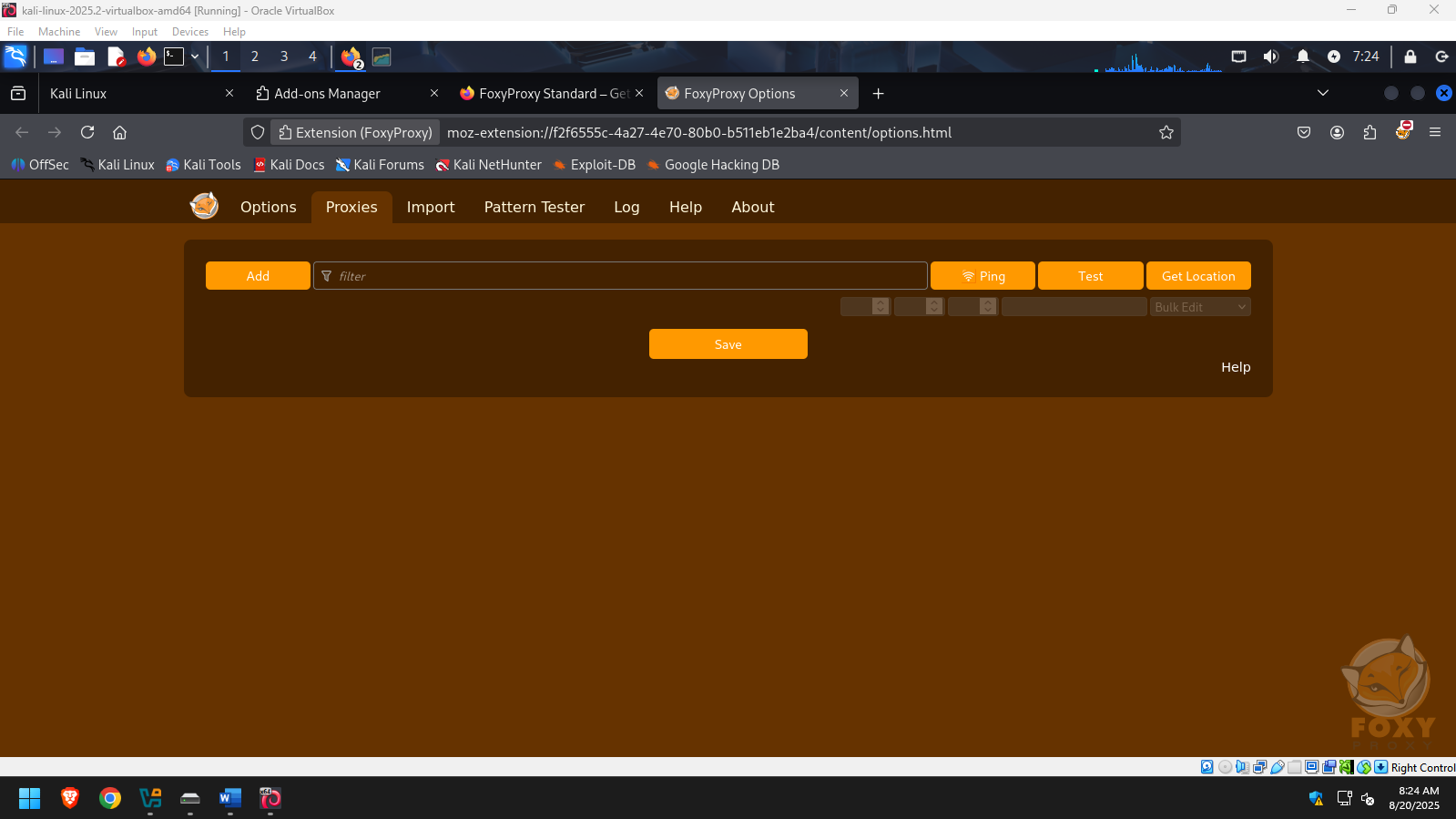
3# - Pesquise pelo foxproxy na aba de extensões



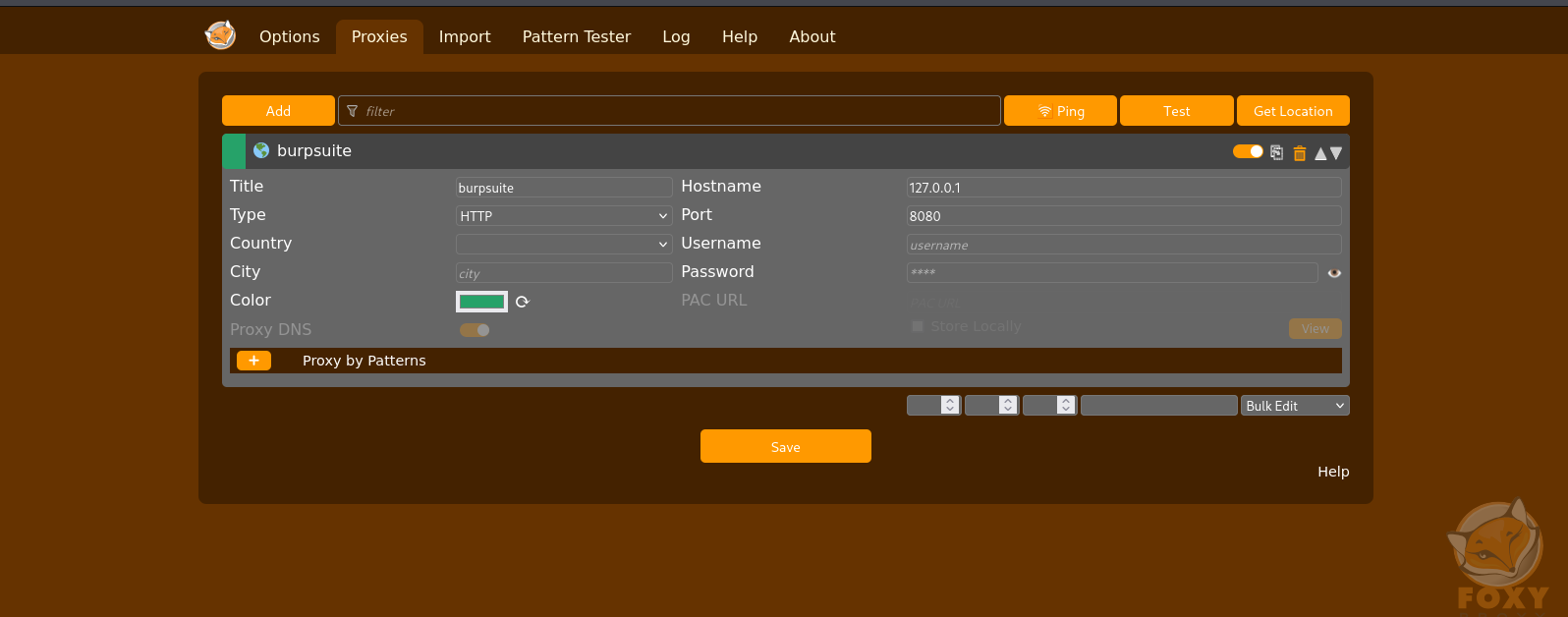
4# - Instalaremos o standard edition, lembre-se de fixa-lo nos atalhos.



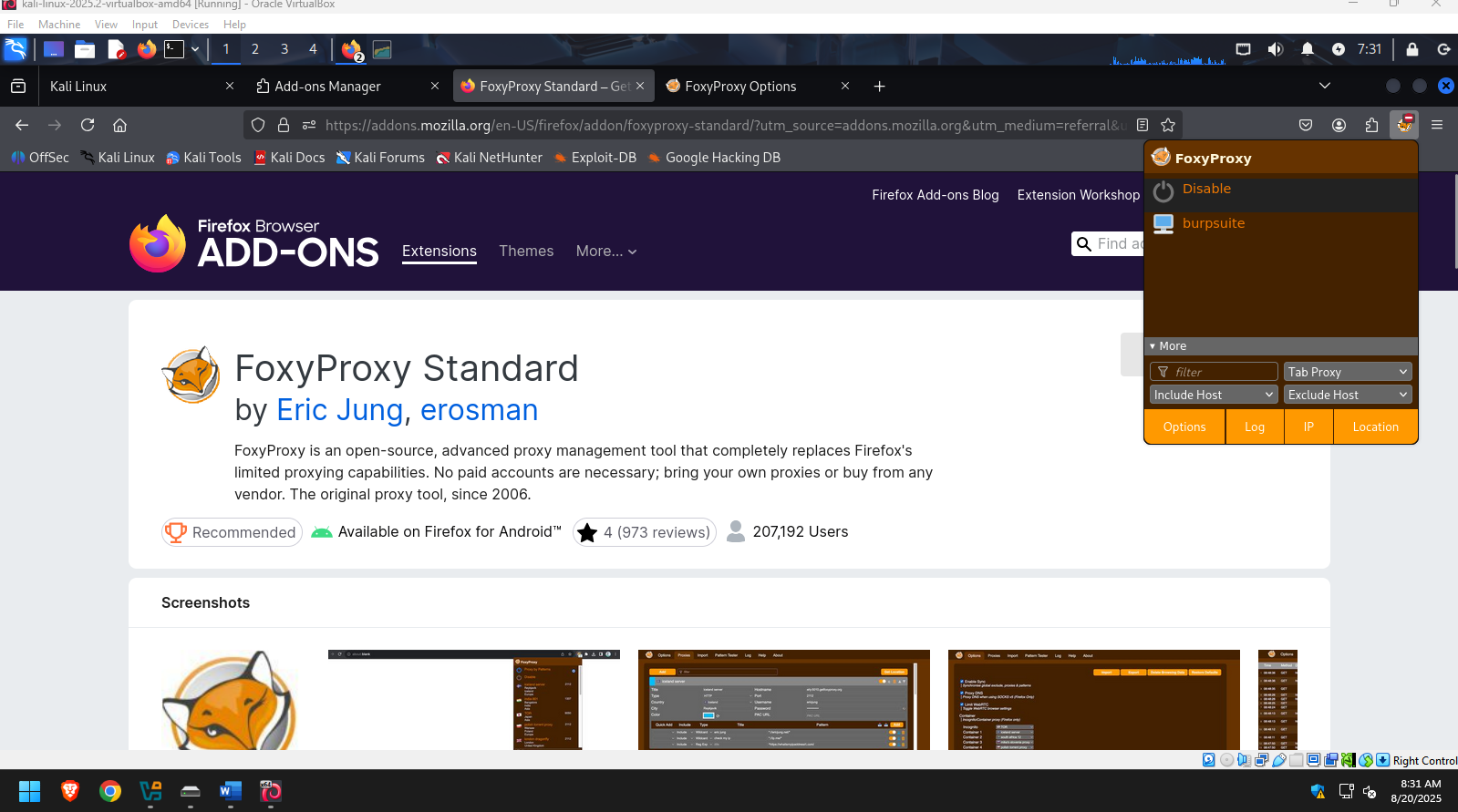
5# - Clique em options

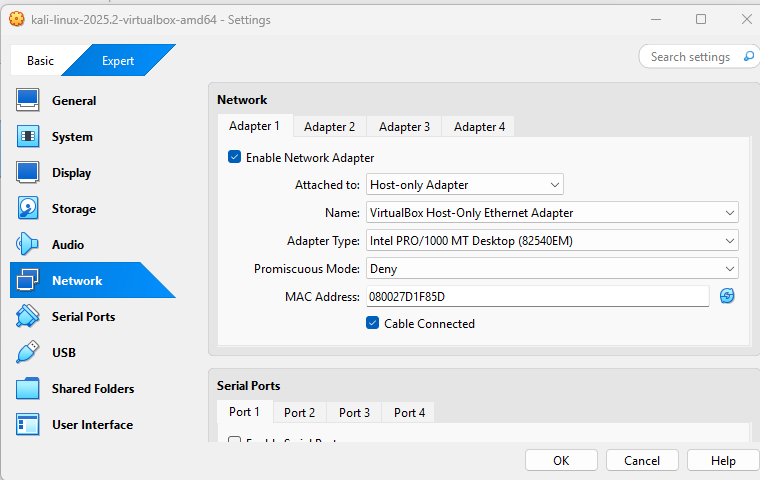


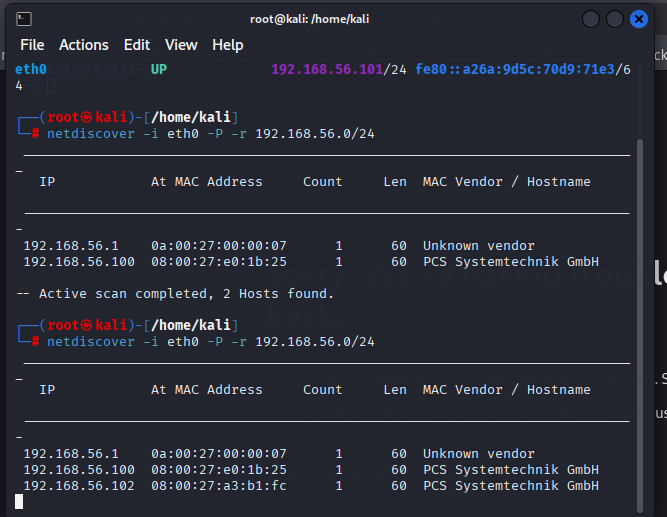
6# - Clique em proxies



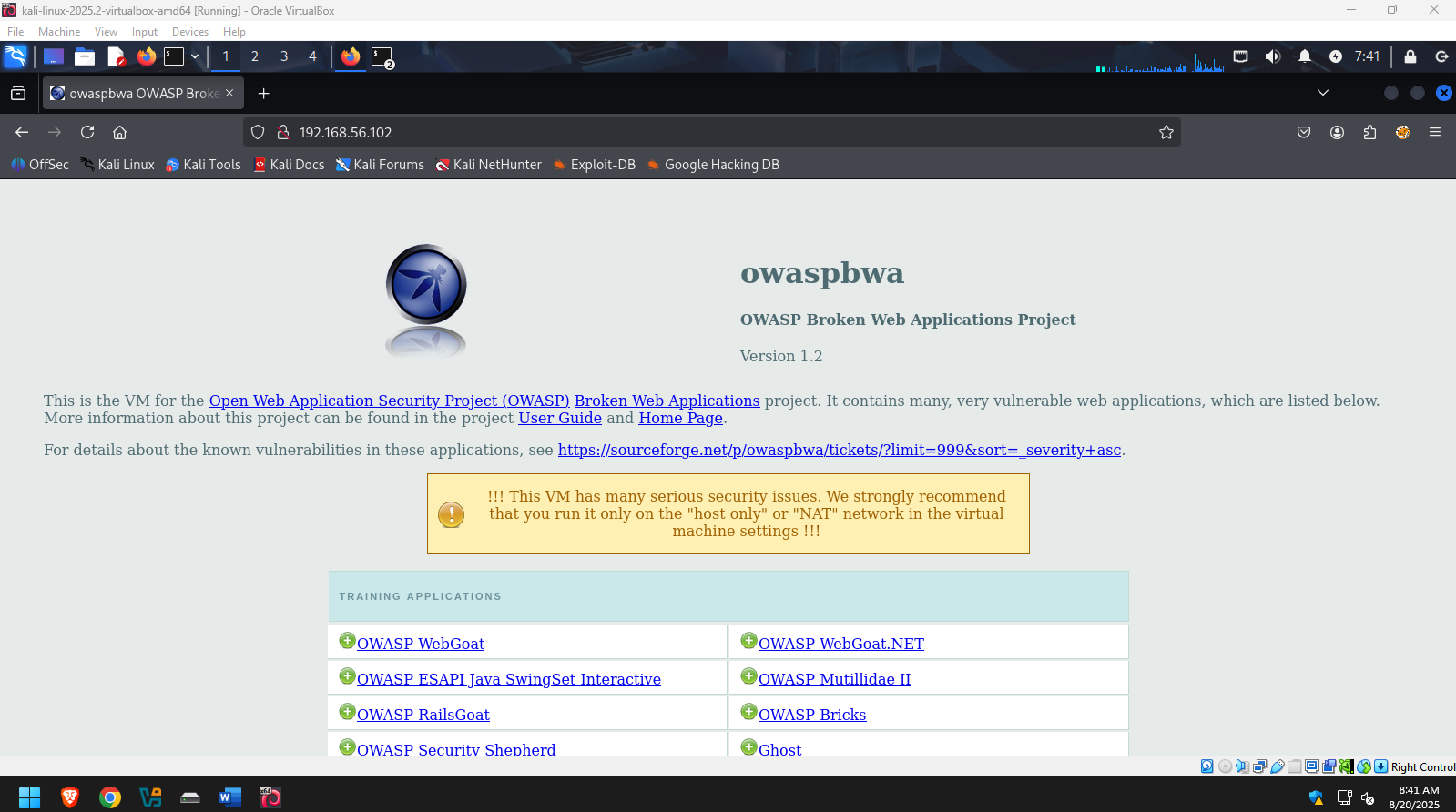
7# - Salve



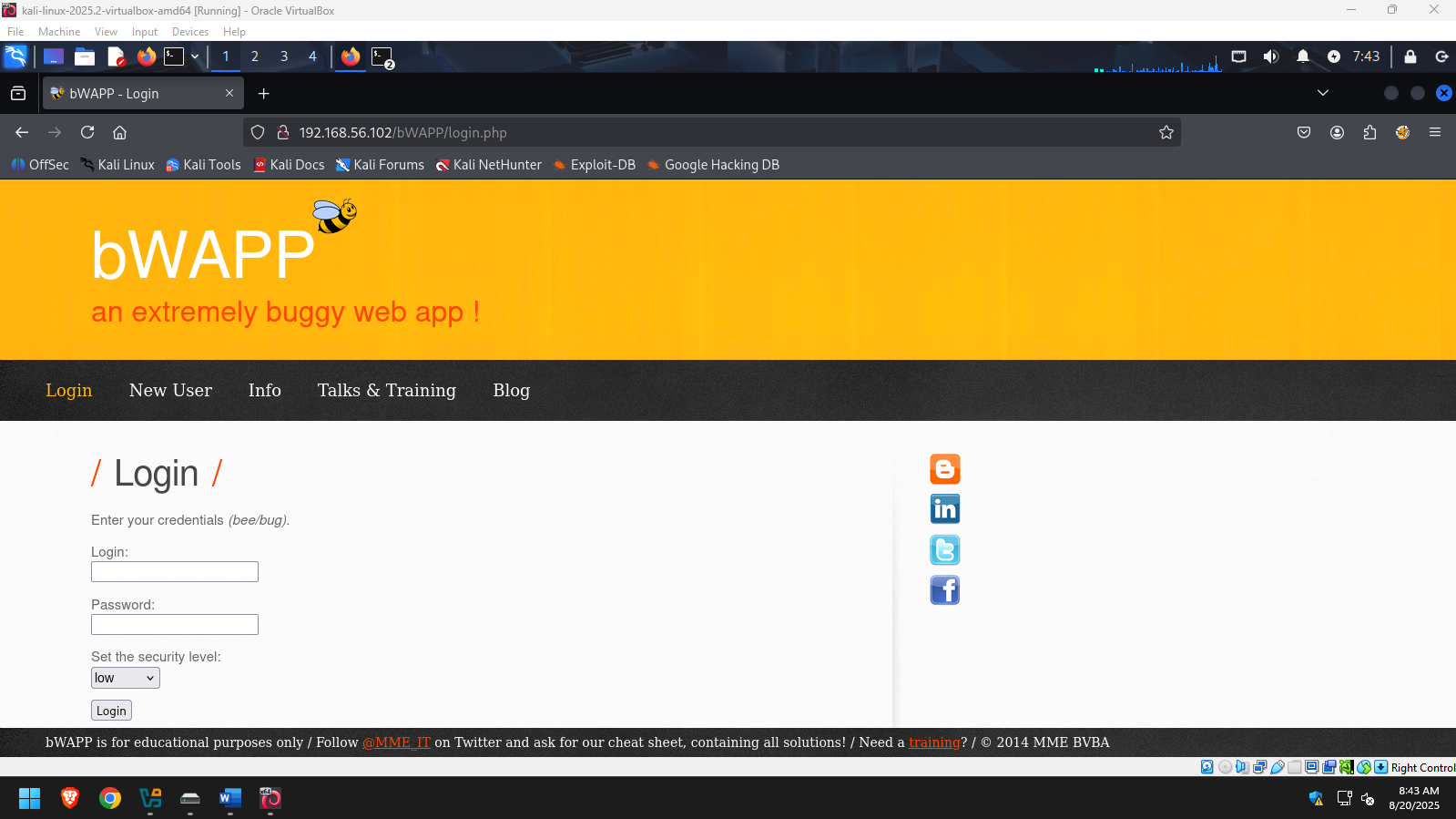
8# - Voltamos para o host-only (Tudo isso era só pra baixar o burp suíte)  


9# - Ligue o servidor OWASP  
10# - No kali:  
  
o primeiro netdiscover foi antes do servidor da OWASP subir, o segundo é depois.

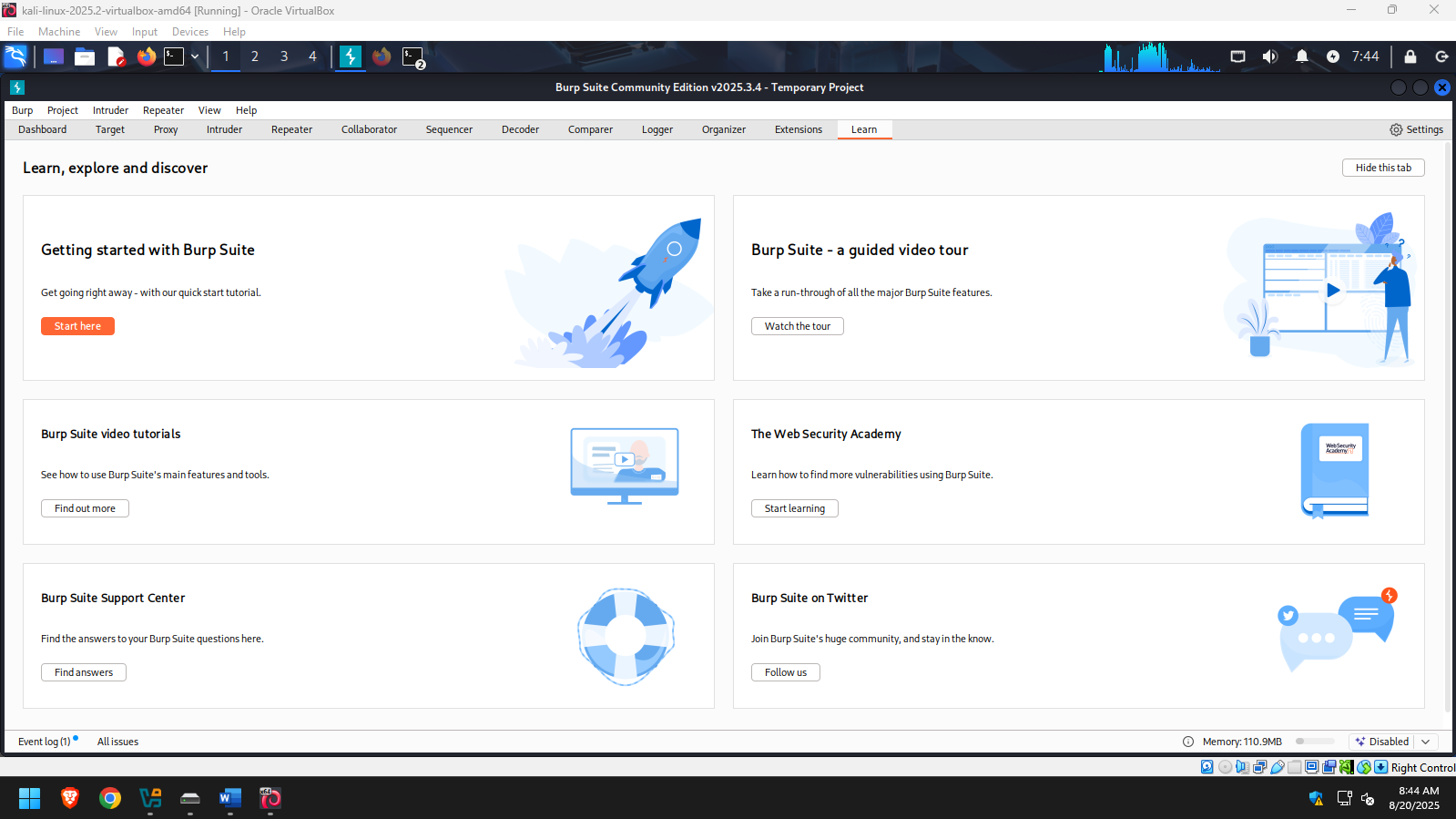
11# - pesquise 192.168.56.102 no Firefox.



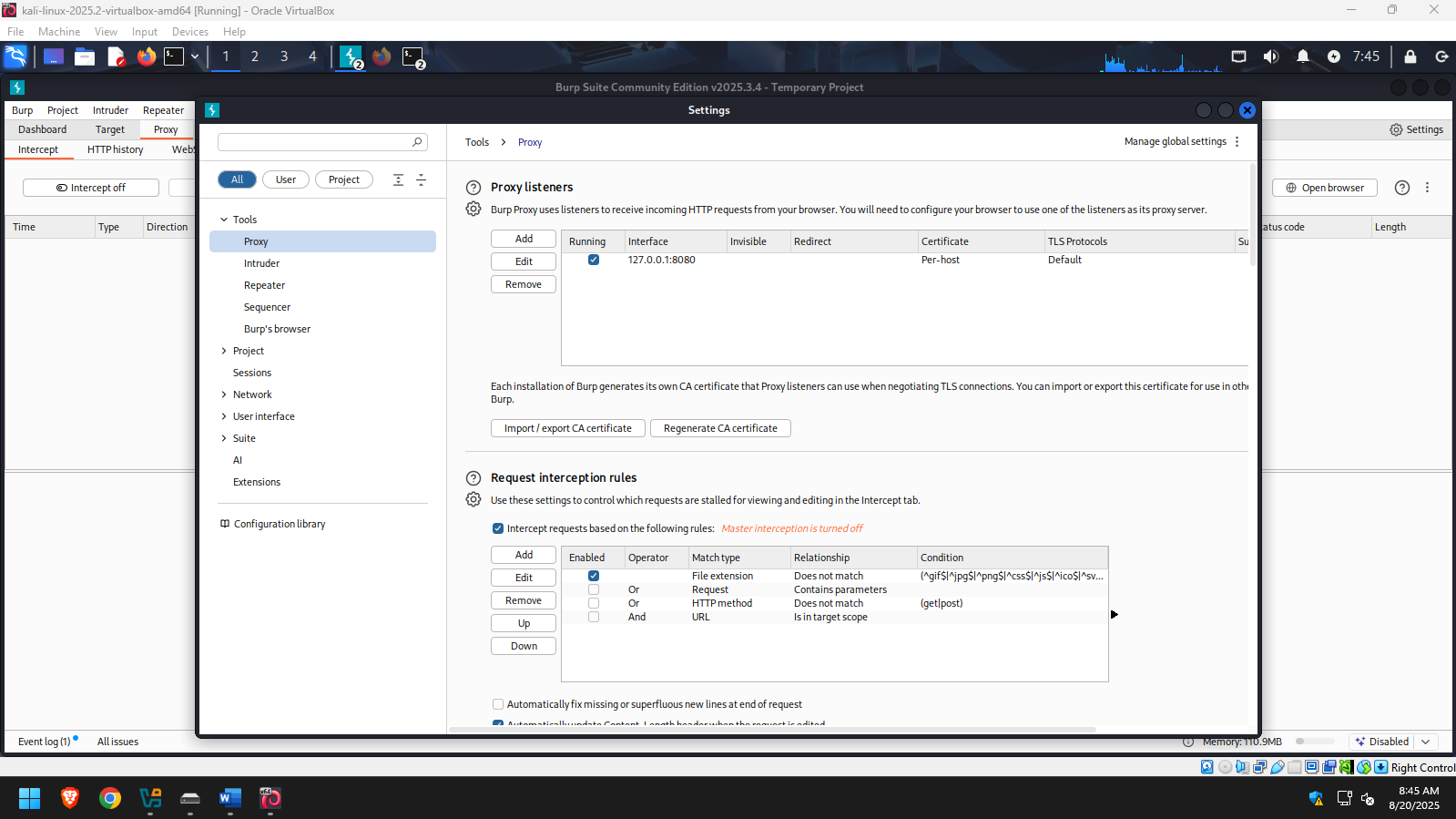
12# - selecione BWAPP



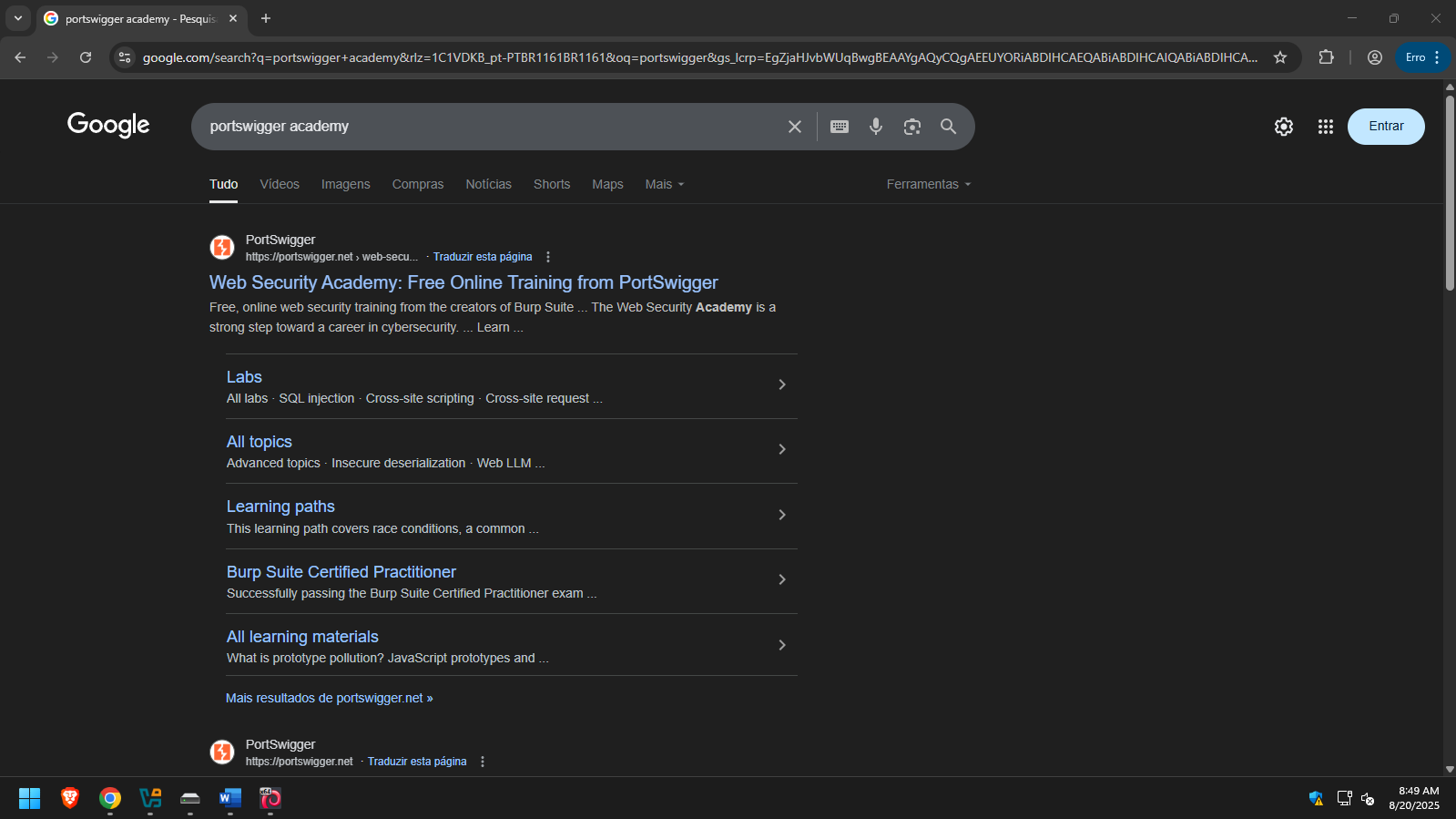
13# ABRA O BURP SUITE. (De next e start em tudo)



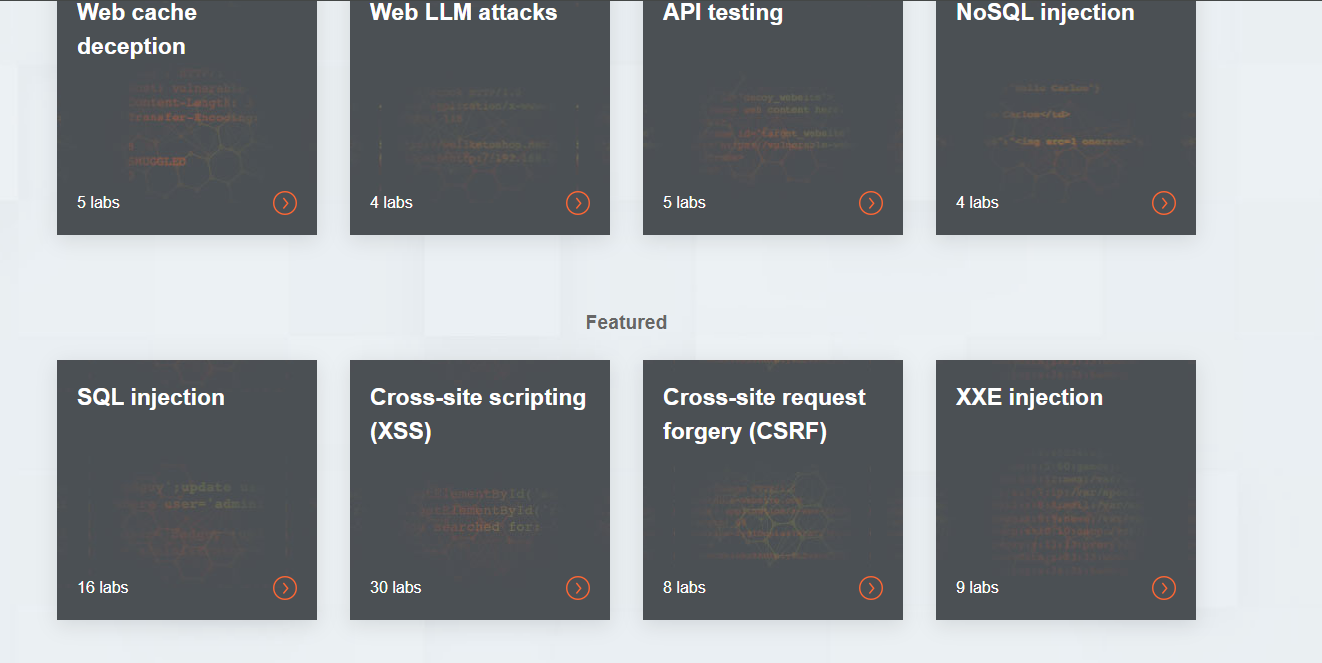
14# - Clique em proxy settings



O IP no foxyproxy deve ser o mesmo do proxy listener.



Recomendação de curso do professor ^



<https://portswigger.net/web-security/sql-injection>

CP -4

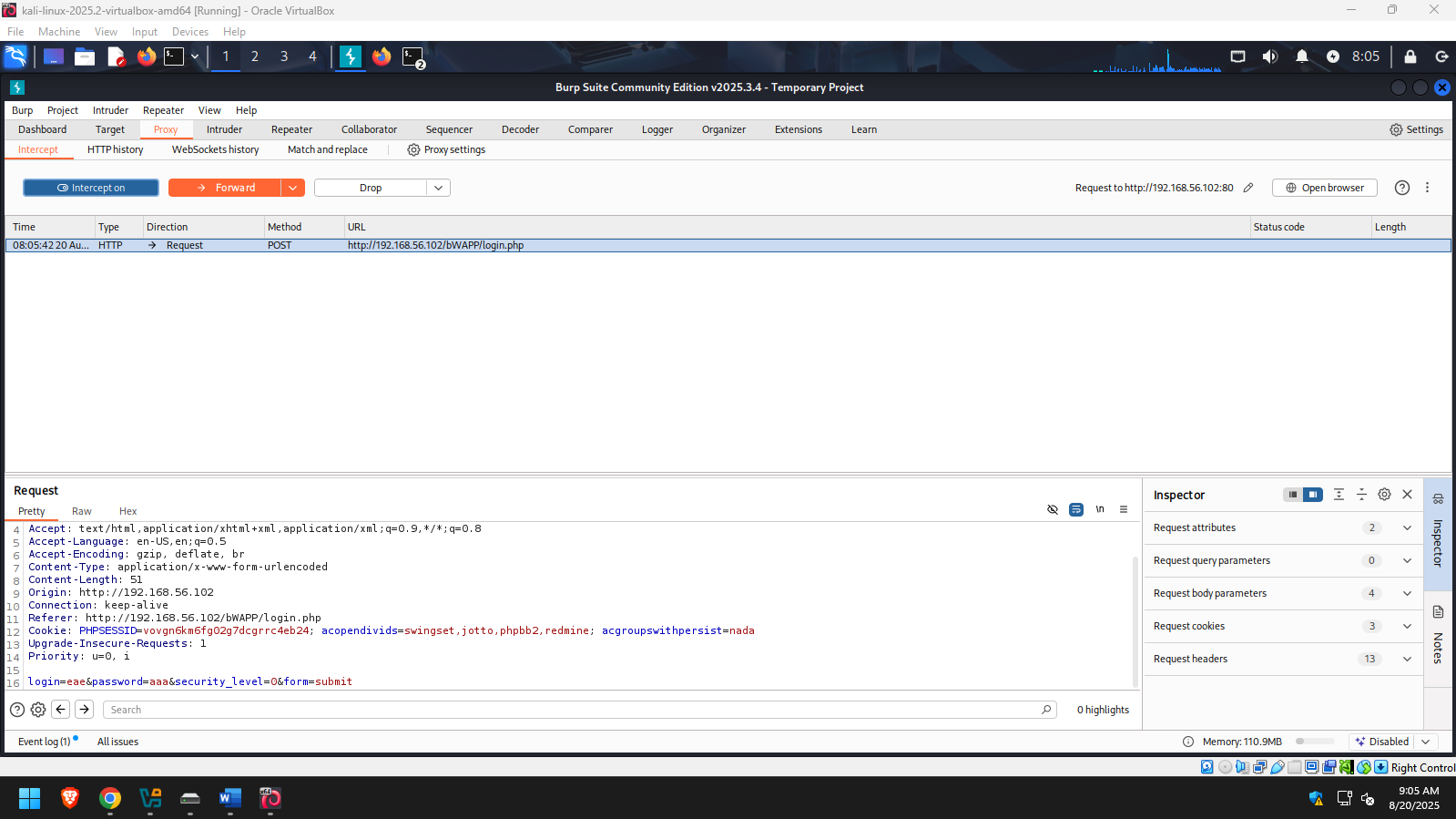
Chave publica/privada.

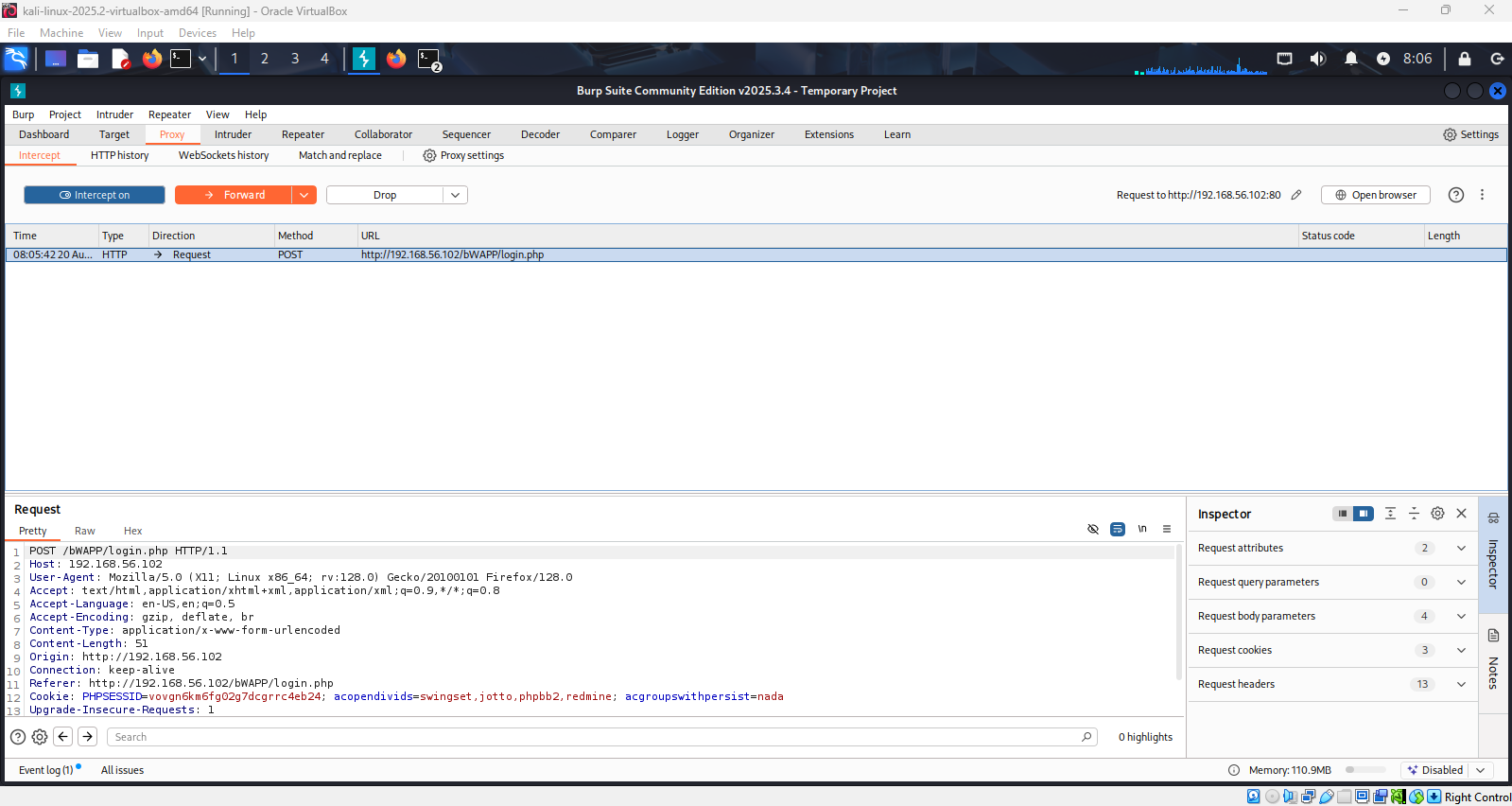
SSH.

Error Response.

15# - Auth by-pass:  
  
<https://github.com/payloadbox/sql-injection-payload-list/tree/master/Intruder/exploit>

16# ligue o intercept e o proxy.

17# tente logar  




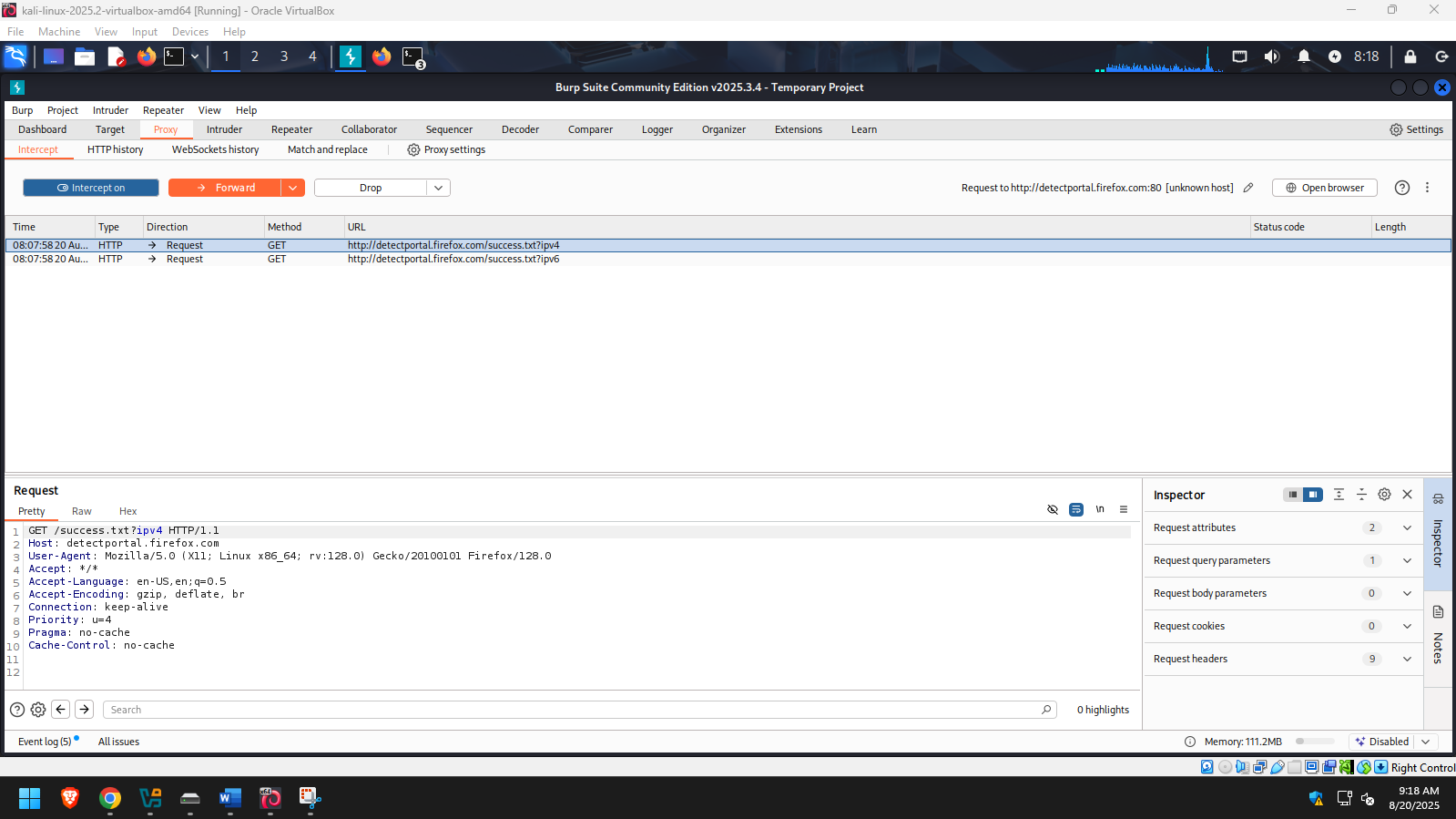
A primeira linha da imagem se trata do caminho e no qual a requisição é enviada (essencialmente o curl)

IP do Kali:

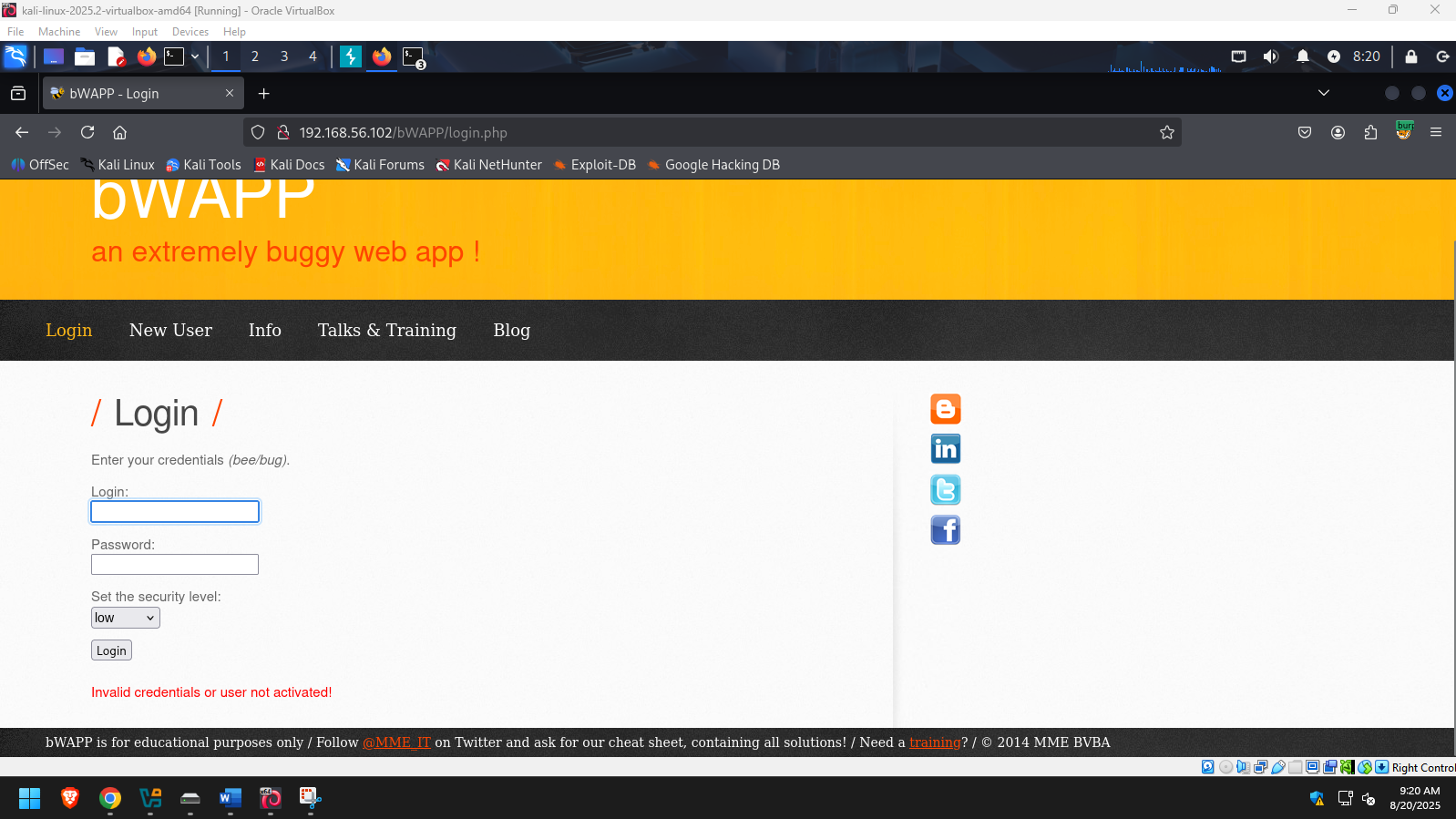


IP do OWASP:  

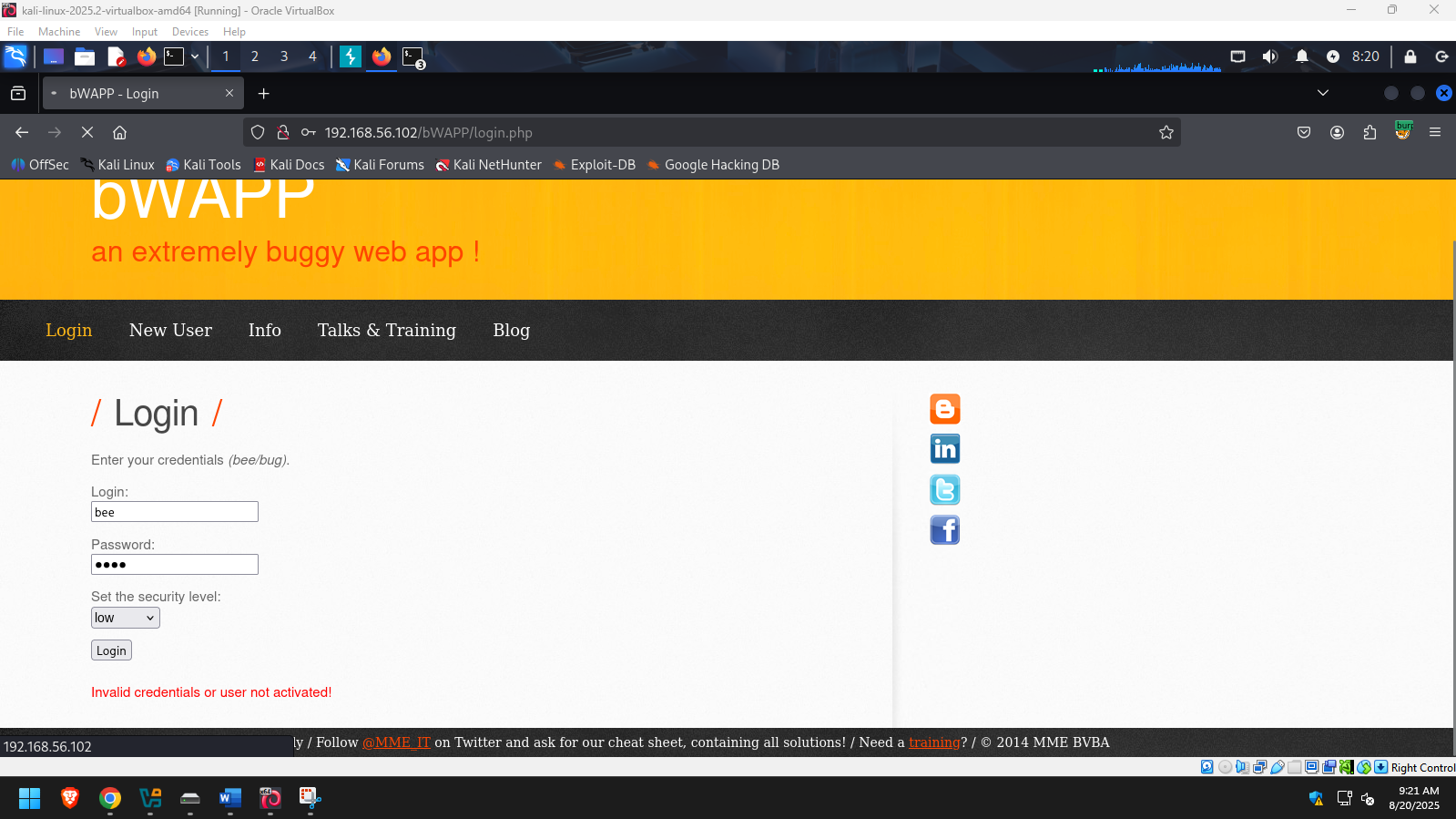

18# - Clique em forward



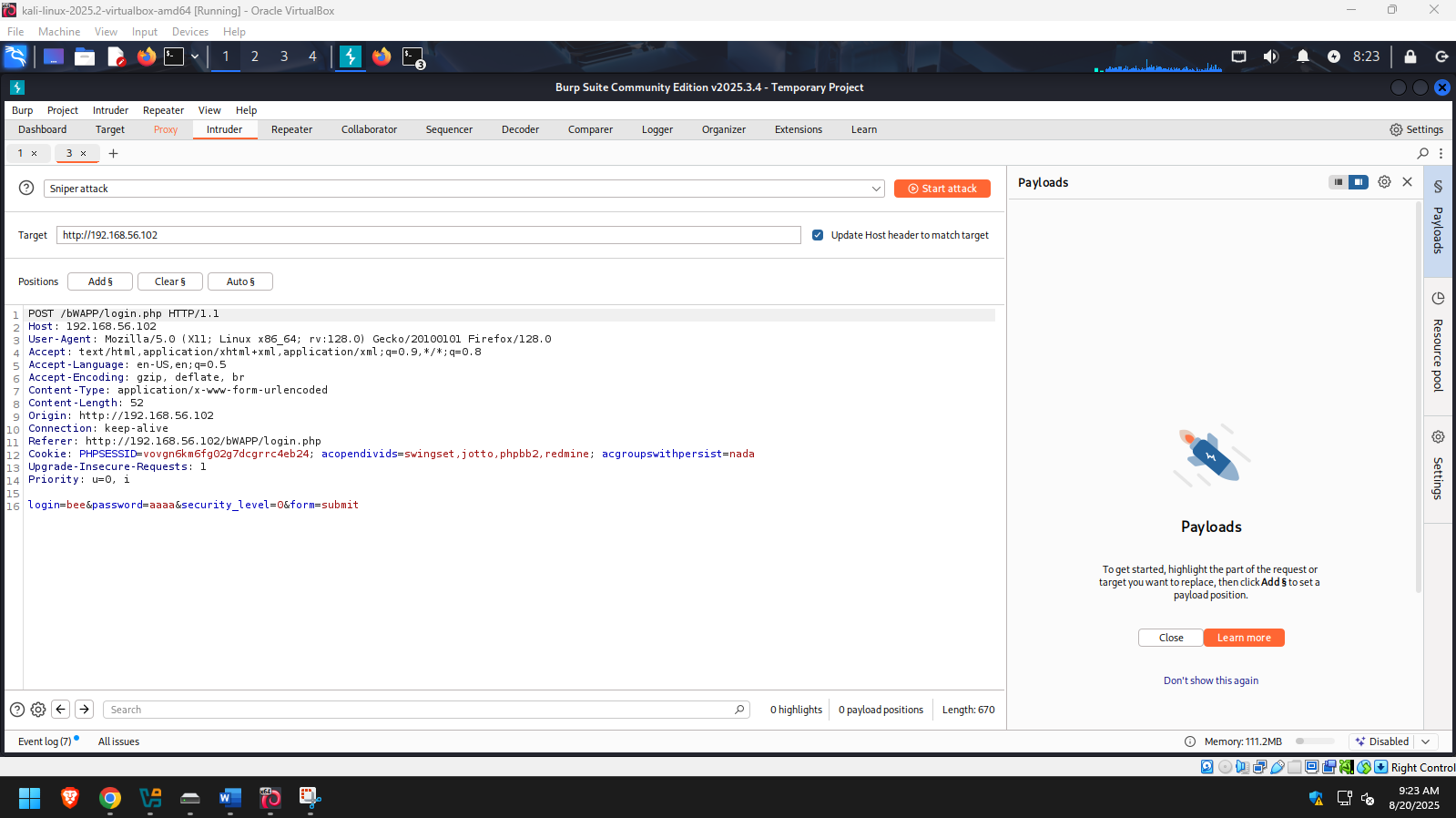
O burp cria uma copia do estado do servidor



19# - coloque o usuário certo (bee)

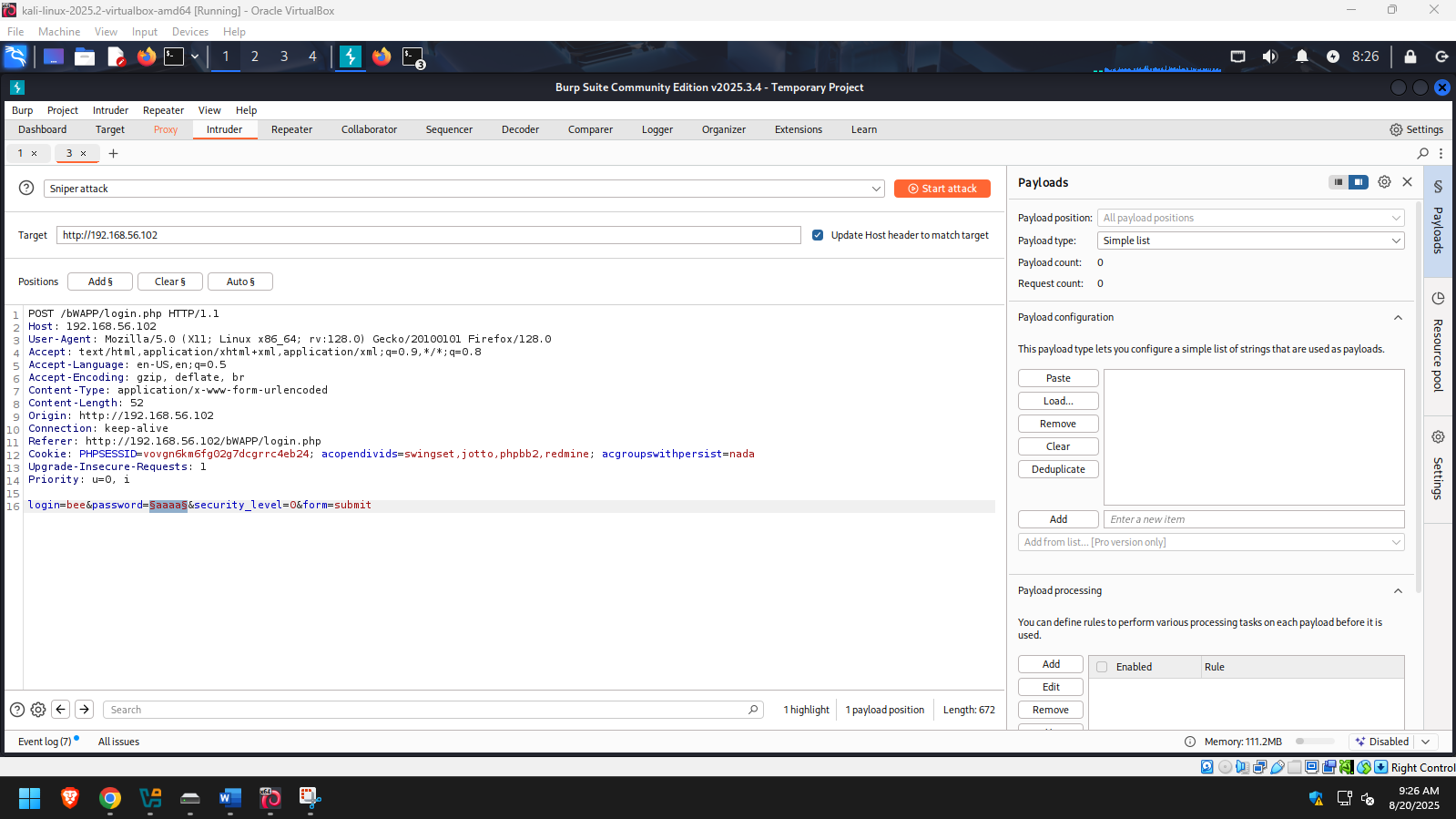


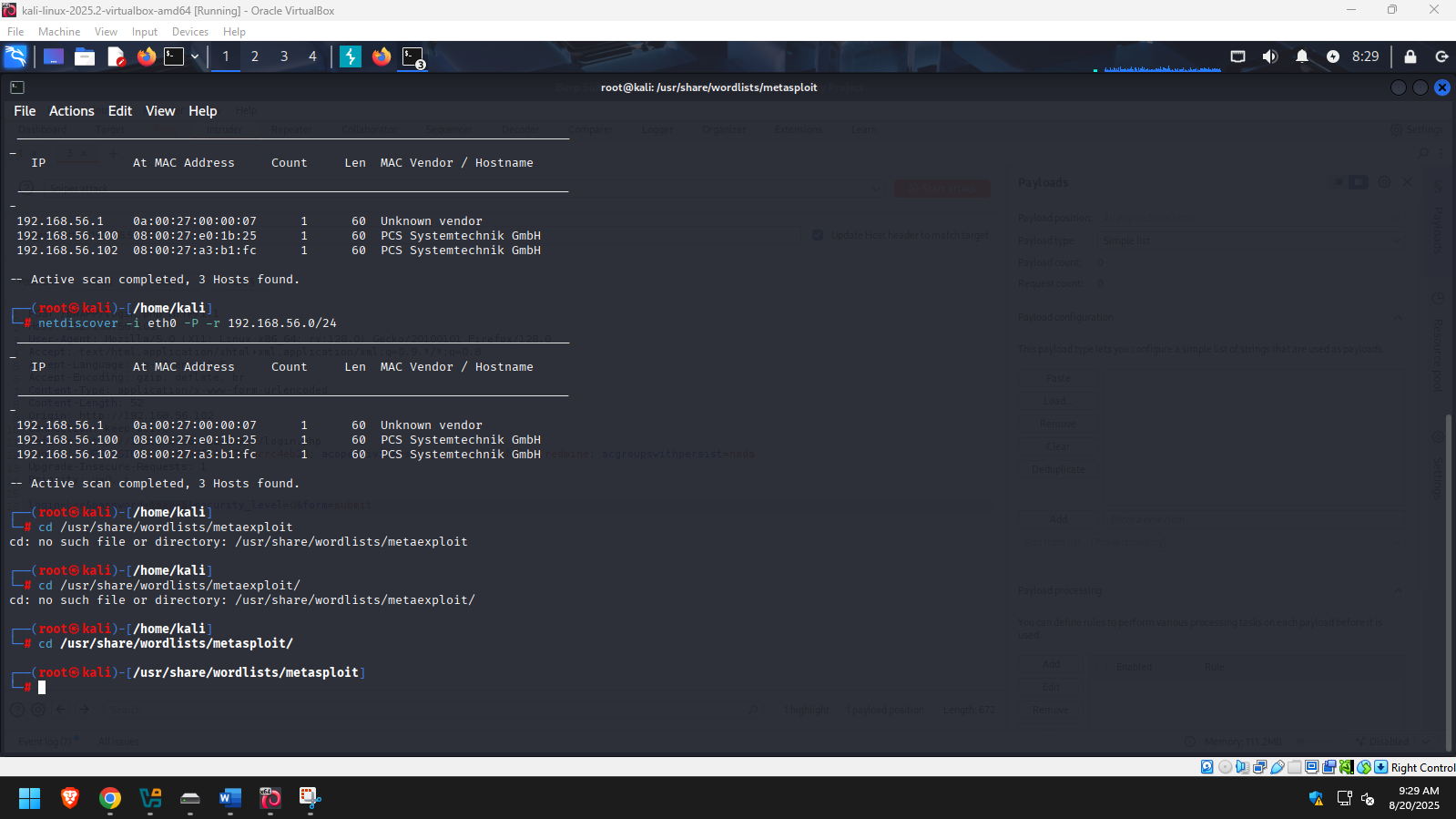
20# - envie a requisição capturada para o intruder

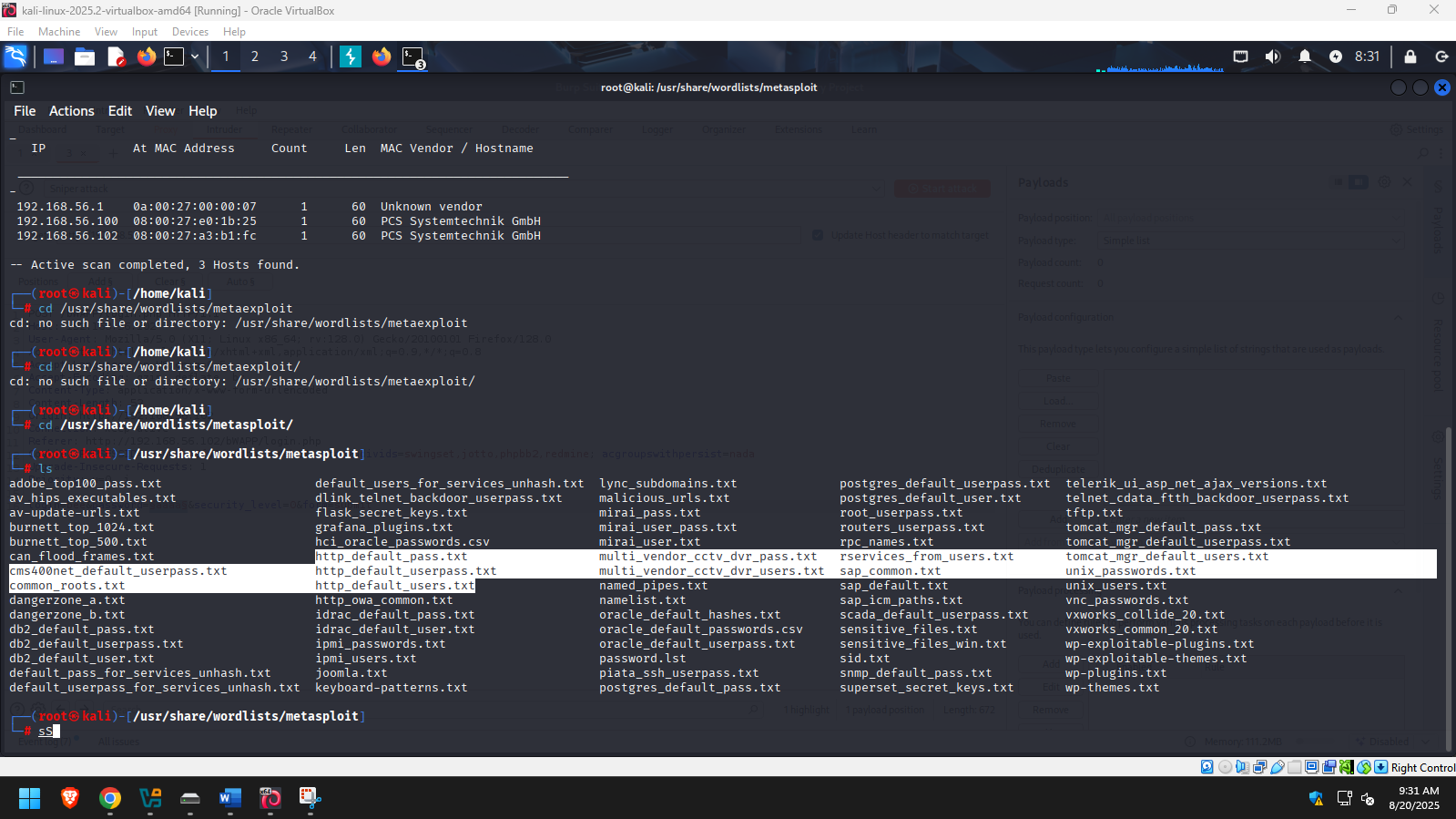


Sniper para um campo de ataque apenas (Login ou senha)

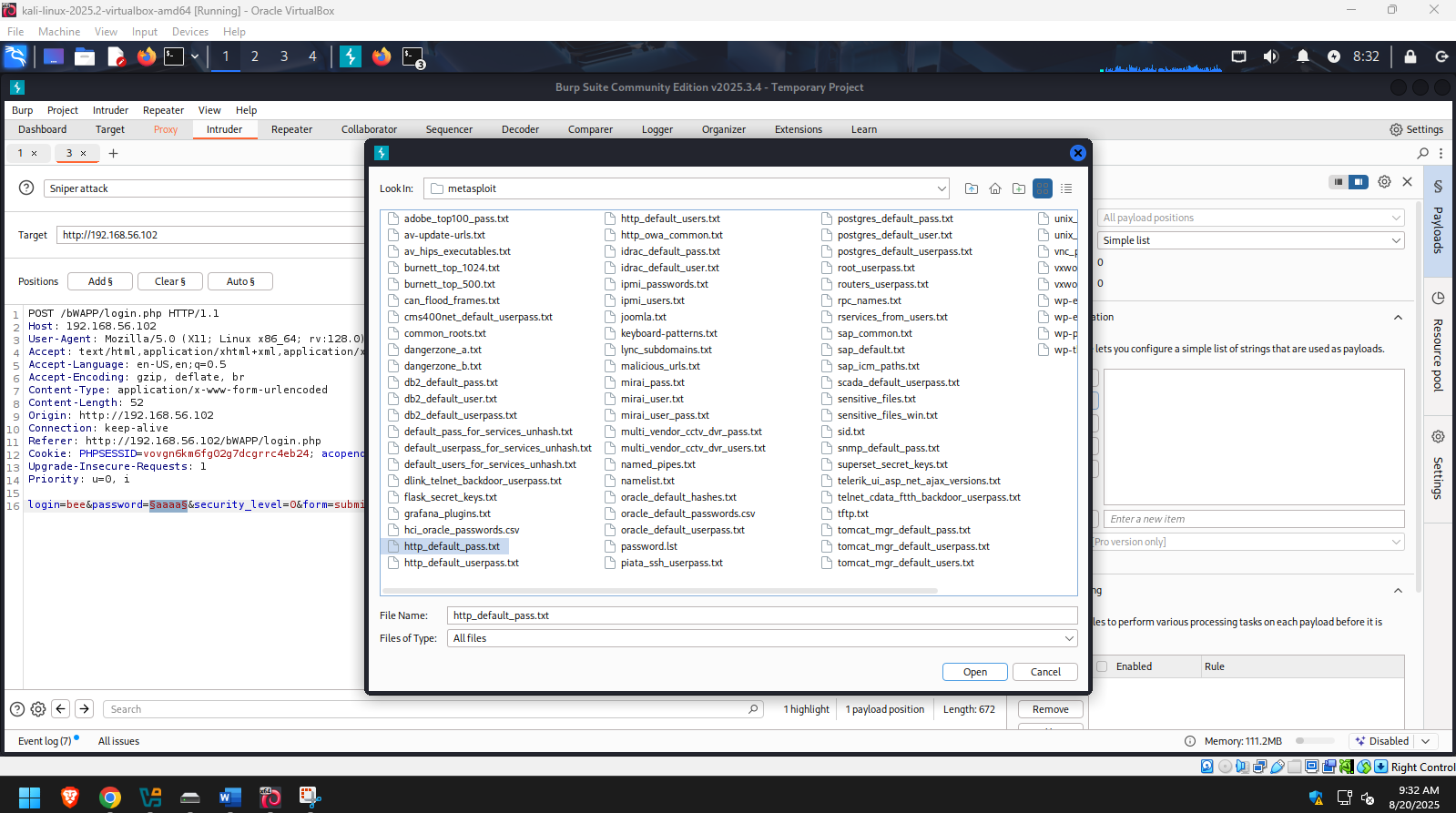
Sem nenhum dos dois usamos Cluster bomb

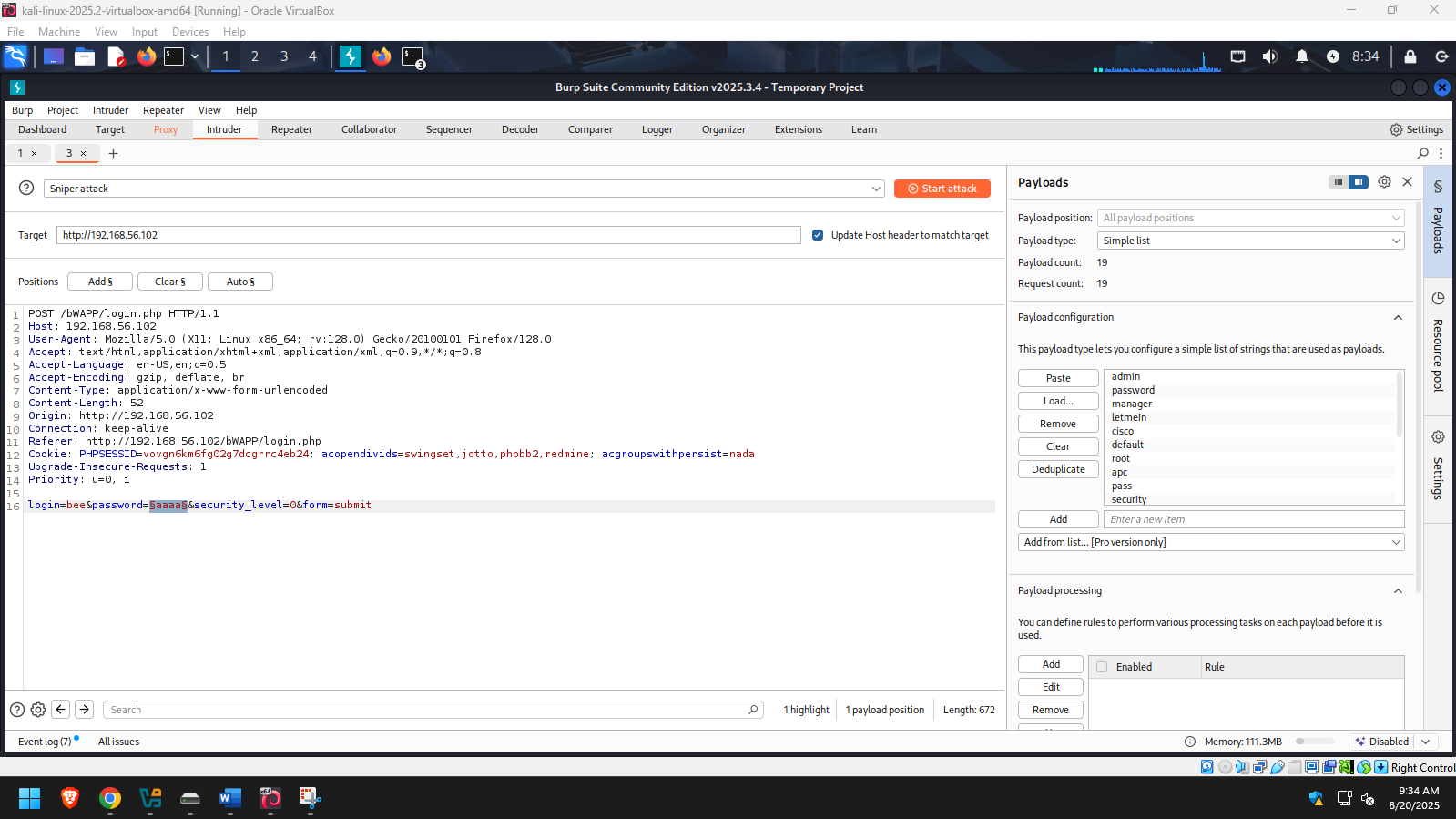
21# - selecione add  


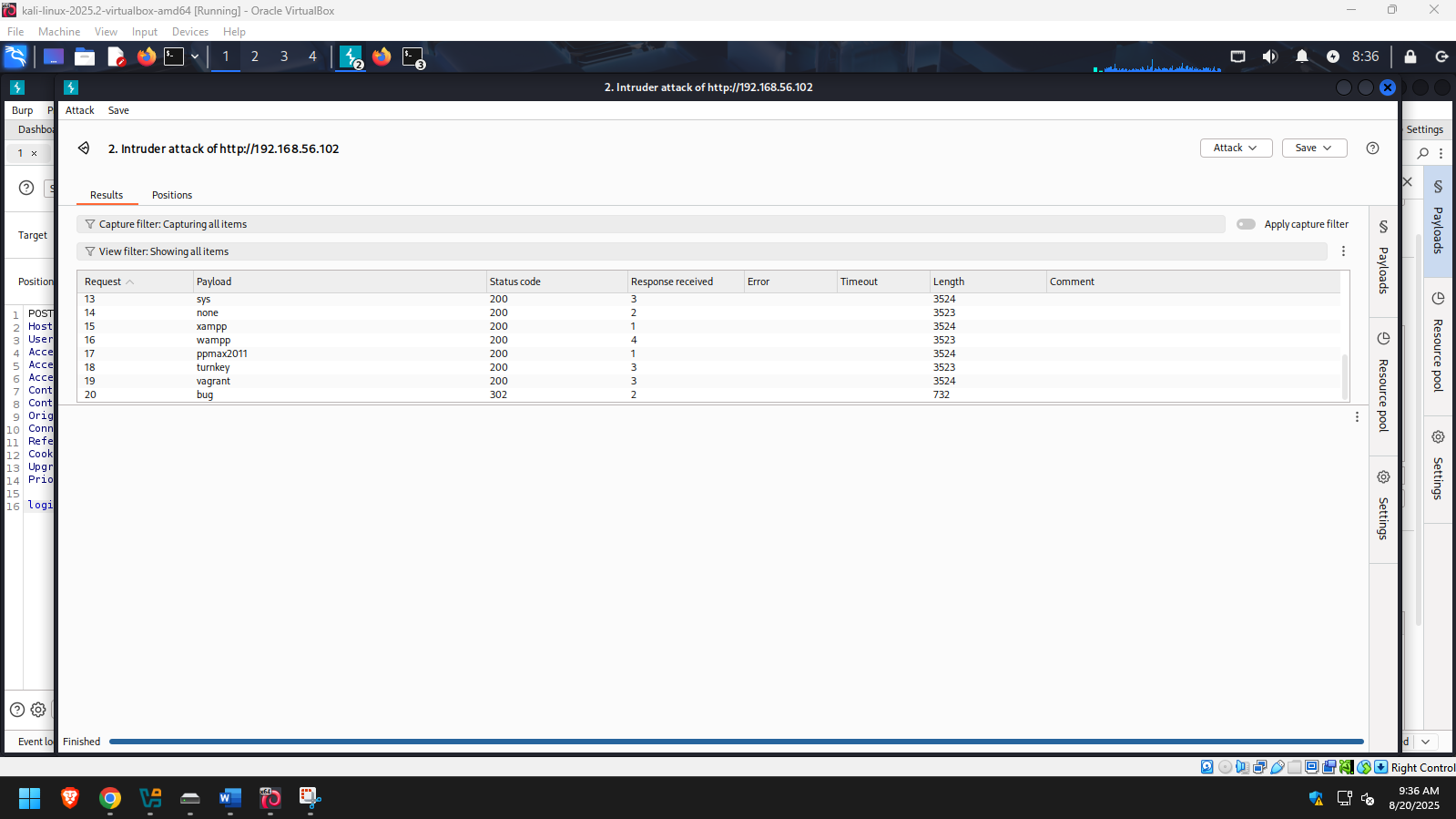










Inicie o Ataque:  


200 normalmente significa que esta batendo no servidor, mas nesse caso esta batendo na copia.

302 significa que achamos a senha.

Além disso podemos notar que o tamanho do payload é significativamente diferente.