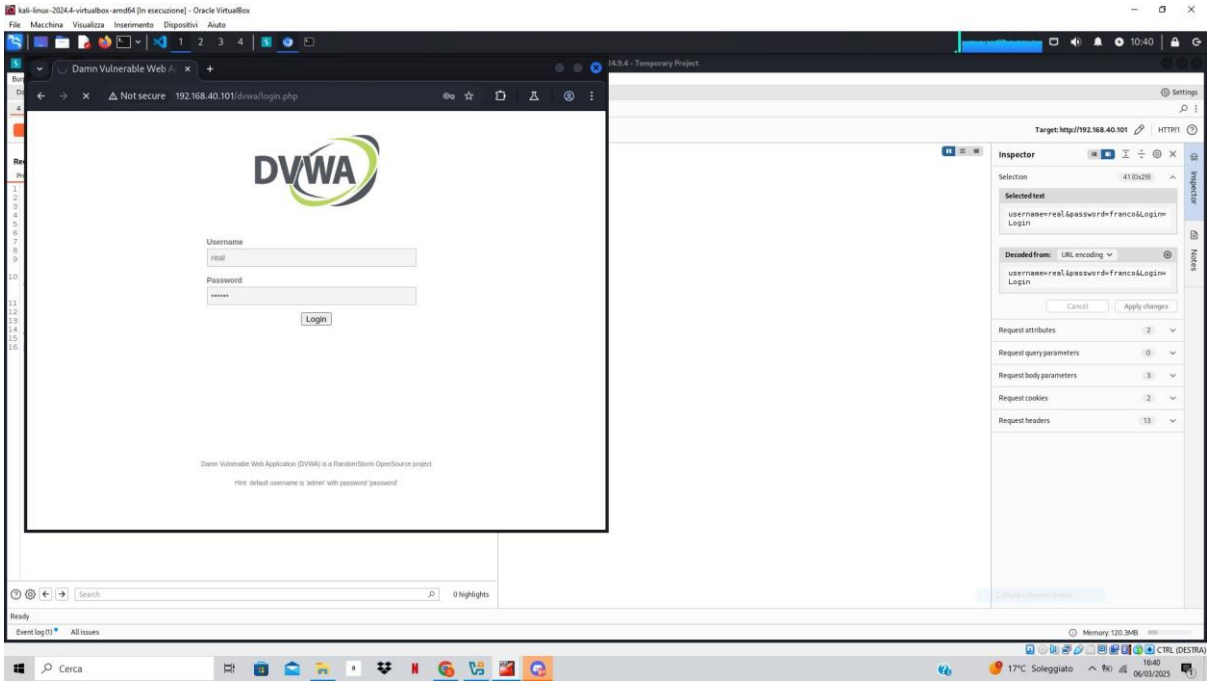
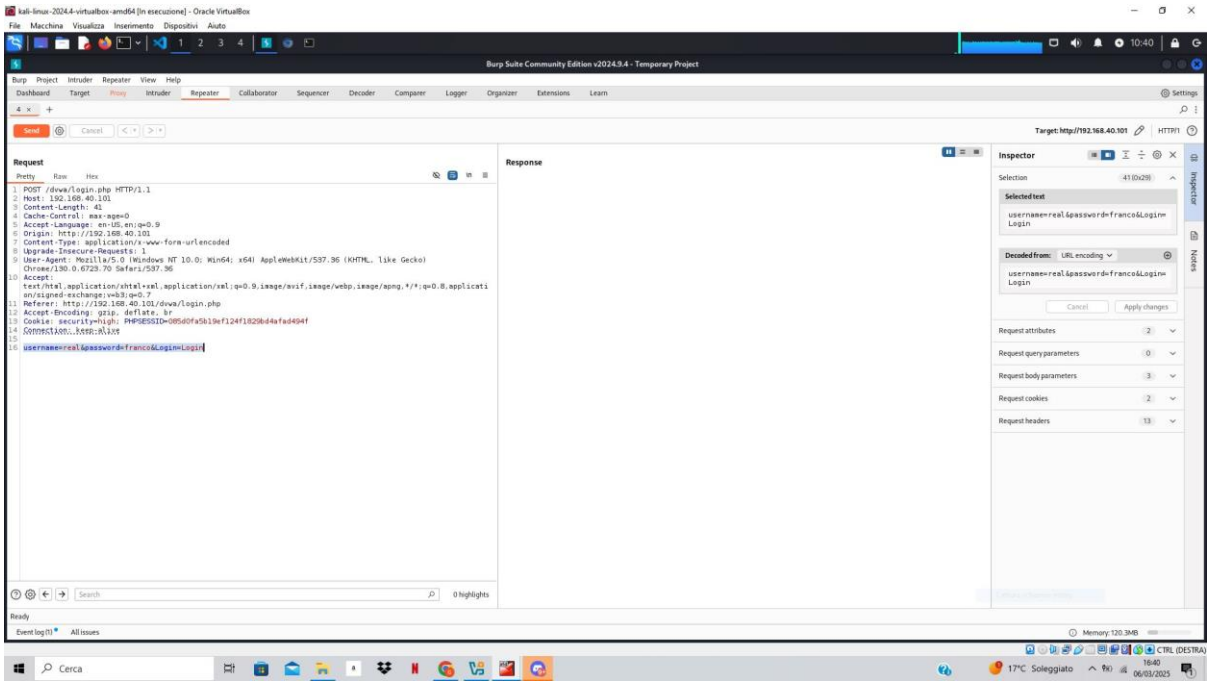
ESECIZIO DI OGGI SPIEGAZIONE

1.Estrarre rockyou.txt da wordlists

2.Hydra

Ho usato hydra per provare tutte le combinazioni username/password su un sito web locale (`192.168.40.101`). E o utilizzato BurpSuite per prendere il post-form per dare il comando a hydra;



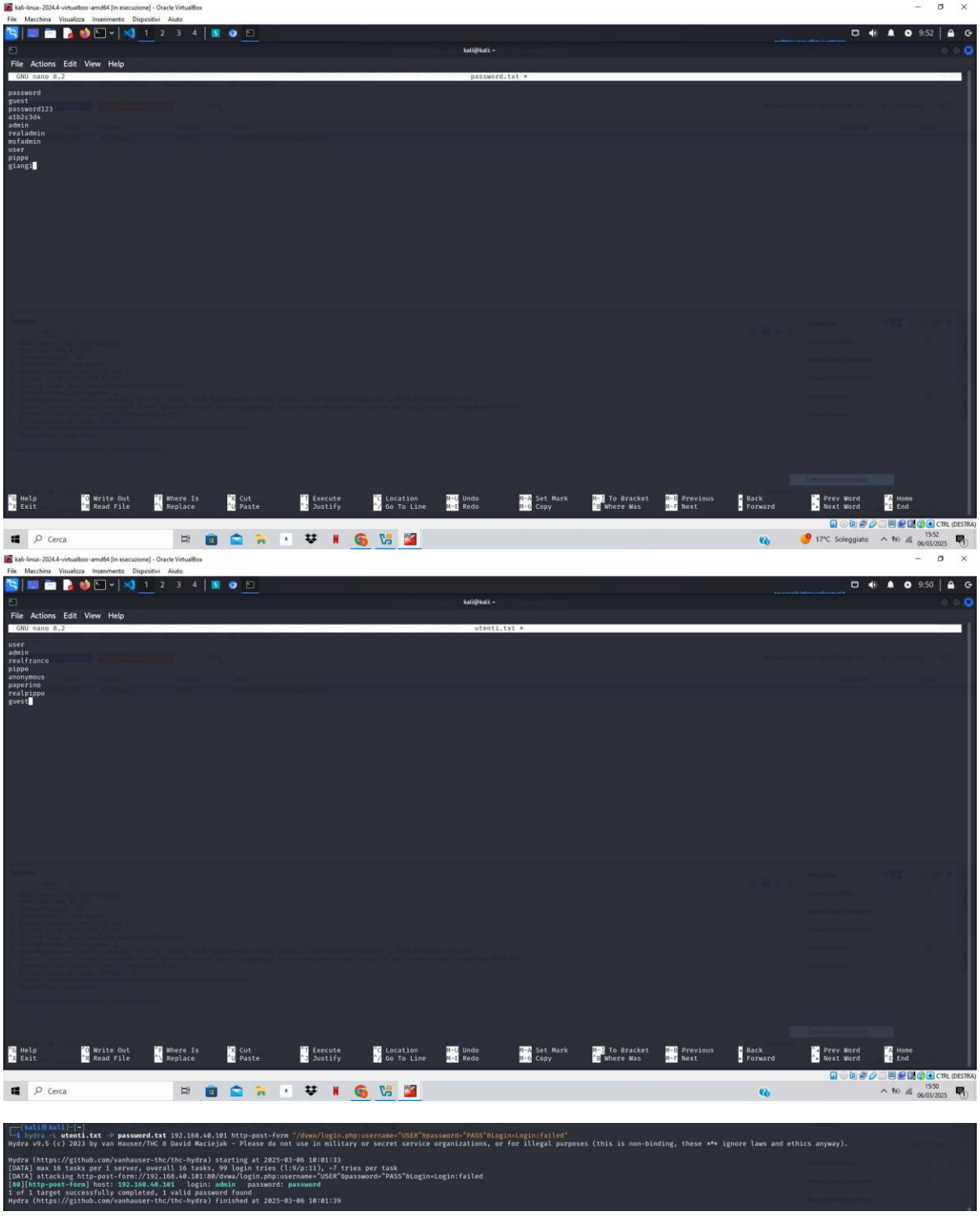



```
Examples:
 "/login.php:user=^USER^&pass=^PASS^:incorrect"
 "/login.php:user=^USER64^&pass=^PASS64^&colon=colon\:escape:S=result=success"
 "/login.php:user=^USER^&pass=^PASS^&mid=123:authlog=.*failed"
 "/:user=^USER&pass=^PASS^:H=Authorization\: Basic dT1w:H=Cookie\: sessid=aaaa:h=X-User\: ^USER^:H=User-Agent\: wget"
 "/exchweb/bin/auth/:F=failedowaauth.dll:destination=http%3A%2F%2F<target>%2Fexchange&flags=0&username=<domain>%5C^USER^&password=^PASS^&SubmitCreds=x&trusted=0:C=/exchweb":reason=

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ nano utenti.txt

┌──(kali㉿kali)-[~]
└─$ nano password.txt
```



Hydra ha trovato che l'utente **admin** aveva la password **password**.

3.John the Ripper

Ho generato un hash MD5 di una password (`passw0rd:password`) usando `md5sum`, poi ho salvato l'hash in un file (`dvwapasshash.txt`), e infine usato John the Ripper per tentare di decifrare l'hash MD5.