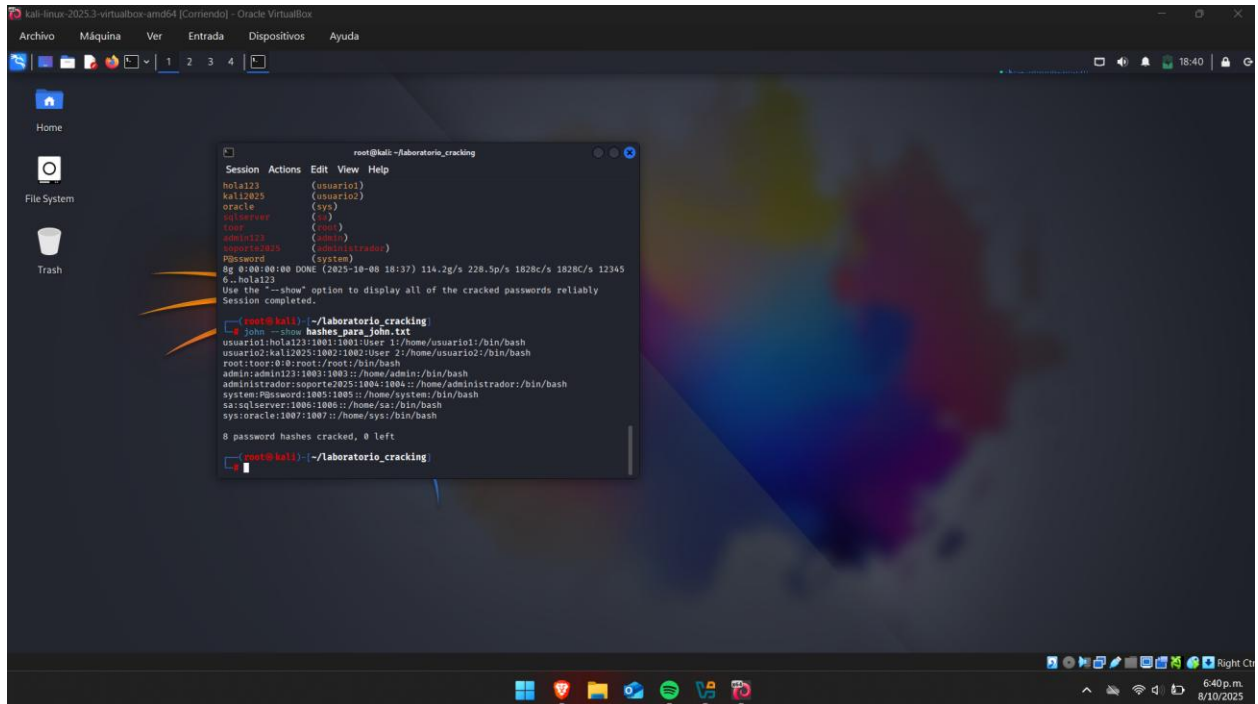


HACKEAR CONTRASEÑAS

John the reaper (offline)

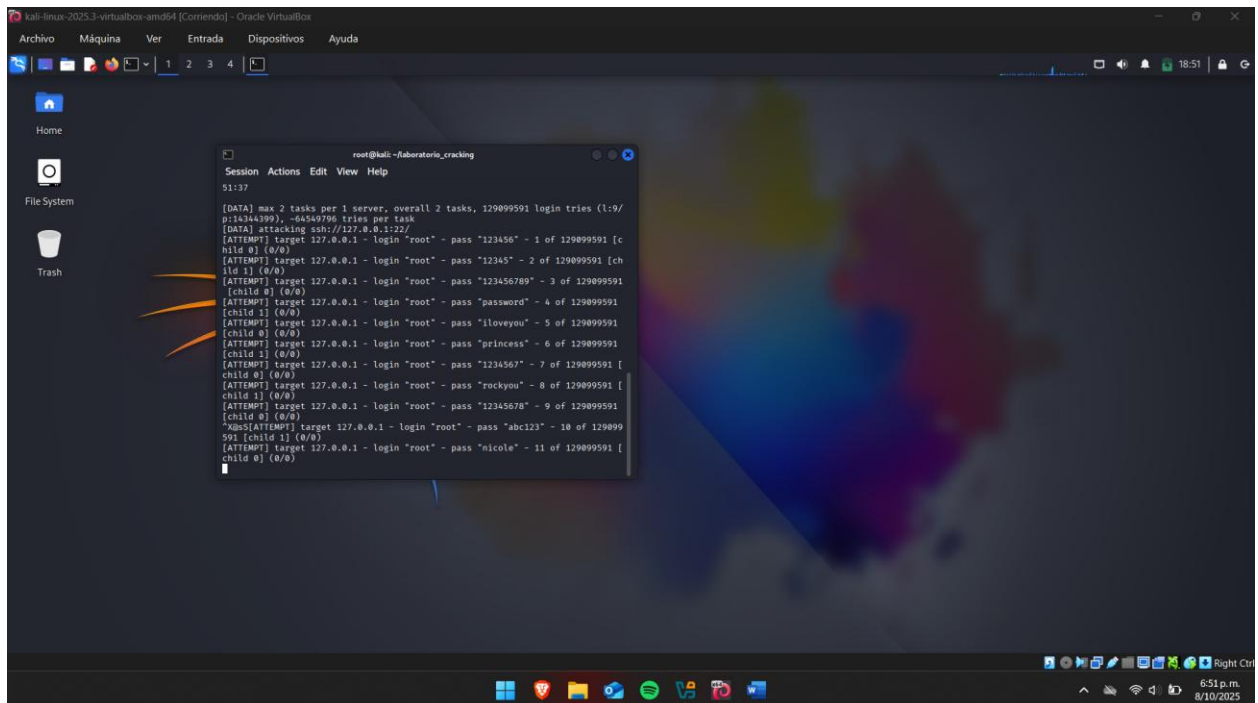


The screenshot shows a Kali Linux virtual machine with a terminal window titled 'root@kali: ~ - laboratorio_cracking'. The terminal displays the output of the 'john --show hashes para_john.txt' command. The output lists several cracked passwords and their corresponding hashes, including 'usuario1', 'usuario2', 'sys', 'root', 'admin', 'support', and 'system'. The terminal also shows the progress of the cracking process, indicating that 8 password hashes were cracked out of 8 left.

```
root@kali: ~ - laboratorio_cracking
Session Actions Edit View Help
john --show hashes para_john.txt
usuario1:holai23:1001:1001:User 1:/home/usuario1/bin/bash
usuario2:holai23:1002:1002:User 2:/home/usuario2/bin/bash
root:toor:0:root:/root/bin/bash
admin:admin123:1003:1003:/home/admin/bin/bash
administrador:supporte2025:1004:1004:/home/administrador/bin/bash
system:Password:1005:1005:/home/system/bin/bash
sa:sqlserver:1006:1006:/home/sa/bin/bash
sys:oracle:1007:1007:/home/sys/bin/bash

8 password hashes cracked, 0 left
```

Hydra (online)



The screenshot shows a Kali Linux virtual machine with a terminal window titled 'root@kali: ~ - laboratorio_cracking'. The terminal displays the output of the 'hydra' command, showing the progress of the cracking process. The output indicates that 10 password hashes were cracked out of 10 left, including 'usuario1', 'usuario2', 'sys', 'root', 'admin', 'support', and 'system'. The terminal also shows the progress of the cracking process, indicating that 10 password hashes were cracked out of 10 left.

```
root@kali: ~ - laboratorio_cracking
51:37
[DATA] max 2 tasks per 1 server, overall 2 tasks, 129099591 login tries (1:9/
p134344399), ~64549796 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "root" - pass "123456" - 1 of 129099591 [c
hild 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "12345" - 2 of 129099591 [c
hild 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "123456789" - 3 of 129099591
[child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "password" - 4 of 129099591
[child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "iloveyou" - 5 of 129099591
[child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "princess" - 6 of 129099591
[child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "1234567" - 7 of 129099591 [
child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "rockyou" - 8 of 129099591 [
child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "12345678" - 9 of 129099591
[child 0] (0/0)
[XB5S[ATTEMPT] target 127.0.0.1 - login "root" - pass "abc123" - 10 of 129099
591 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "nicole" - 11 of 129099591 [
child 0] (0/0)
```