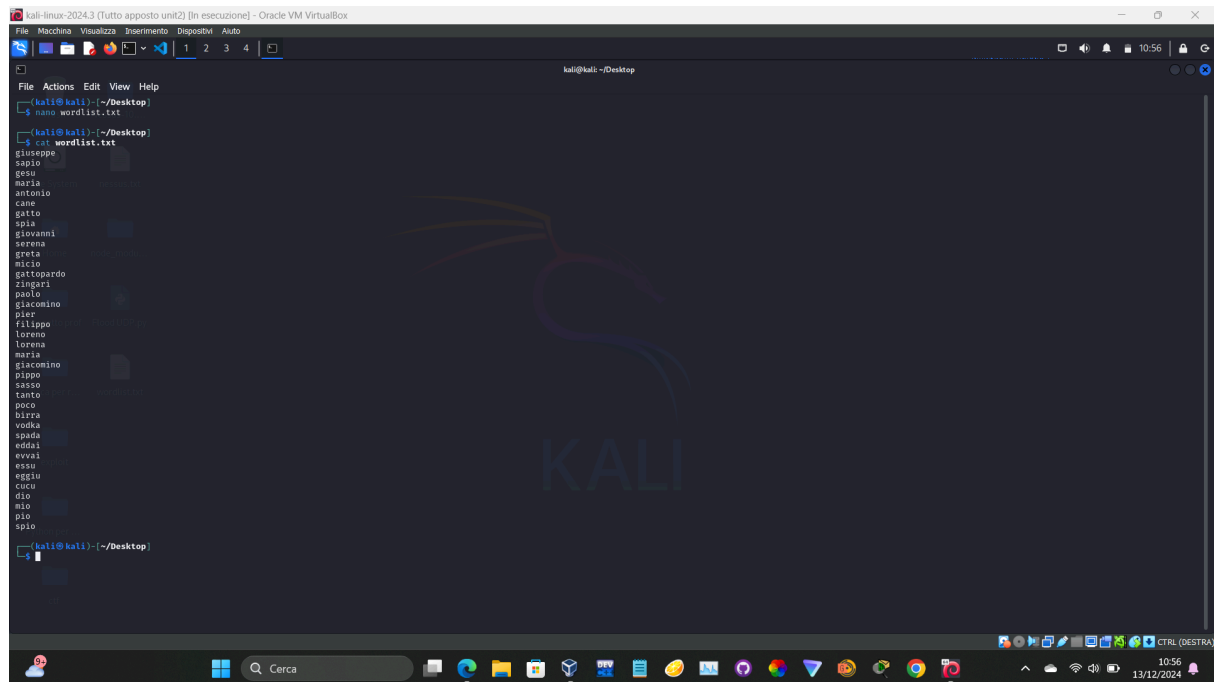


Oggi ho craccato la psw di un utente fatto da me sulla mia stessa macchina. Ho proceduto col crearlo e lo chiamo **giacomino** e come psw gli ho dato sempre **giacomino**, ho proceduto con l'attivare la comunicazione ssh dal file config che ho trovato nella path `/etc/ssh/sshd_config`. Dopodichè ho verificato se potevo connettermi al mio user tramite ssh ci son riuscito posto qua lo screen.

The image shows a Kali Linux terminal window. At the top, the title bar reads "kali-linux-2024.3 (Tutto apposto unito) [In esecuzione] - Oracle VM VirtualBox". The terminal interface includes a menu bar with "File", "Macchina", "Visualizza", "Inserimento", "Dispositivi", and "Aiuto". Below the menu is a toolbar with icons for file operations and a tab bar showing tabs numbered 1 through 4, with the first tab selected. The terminal prompt is "giacomino@kali: ~". The user enters "File Actions Edit View Help" and then "ssh giacomino@192.168.1.8". The terminal displays the SSH connection process, including the host's authenticity, key fingerprint (SHA256:58jE1tEWc2jsBG2C5AzLI4ILSL6j0v/ZgA/09xOgv5w), and a warning to permanently add the host to the list of known hosts. The user confirms by entering "yes". The terminal then shows the Kali GNU/Linux version (6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64) and the programs included with the system. The user then enters "ifconfig eth0 up" and "ip netns exec ns1 ip netns exec ns2 ip netns exec ns3 ip netns exec ns4 ip netns exec ns5 ip netns exec ns6 ip netns exec ns7 ip netns exec ns8 ip netns exec ns9 ip netns exec ns10 ip netns exec ns11 ip netns exec ns12 ip netns exec ns13 ip netns exec ns14 ip netns exec ns15 ip netns exec ns16 ip netns exec ns17 ip netns exec ns18 ip netns exec ns19 ip netns exec ns20 ip netns exec ns21 ip netns exec ns22 ip netns exec ns23 ip netns exec ns24 ip netns exec ns25 ip netns exec ns26 ip netns exec ns27 ip netns exec ns28 ip netns exec ns29 ip netns exec ns30 ip netns exec ns31 ip netns exec ns32 ip netns exec ns33 ip netns exec ns34 ip netns exec ns35 ip netns exec ns36 ip netns exec ns37 ip netns exec ns38 ip netns exec ns39 ip netns exec ns40 ip netns exec ns41 ip netns exec ns42 ip netns exec ns43 ip netns exec ns44 ip netns exec ns45 ip netns exec ns46 ip netns exec ns47 ip netns exec ns48 ip netns exec ns49 ip netns exec ns50 ip netns exec ns51 ip netns exec ns52 ip netns exec ns53 ip netns exec ns54 ip netns exec ns55 ip netns exec ns56 ip netns exec ns57 ip netns exec ns58 ip netns exec ns59 ip netns exec ns60 ip netns exec ns61 ip netns exec ns62 ip netns exec ns63 ip netns exec ns64 ip netns exec ns65 ip netns exec ns66 ip netns exec ns67 ip netns exec ns68 ip netns exec ns69 ip netns exec ns70 ip netns exec ns71 ip netns exec ns72 ip netns exec ns73 ip netns exec ns74 ip netns exec ns75 ip netns exec ns76 ip netns exec ns77 ip netns exec ns78 ip netns exec ns79 ip netns exec ns80 ip netns exec ns81 ip netns exec ns82 ip netns exec ns83 ip netns exec ns84 ip netns exec ns85 ip netns exec ns86 ip netns exec ns87 ip netns exec ns88 ip netns exec ns89 ip netns exec ns90 ip netns exec ns91 ip netns exec ns92 ip netns exec ns93 ip netns exec ns94 ip netns exec ns95 ip netns exec ns96 ip netns exec ns97 ip netns exec ns98 ip netns exec ns99 ip netns exec ns100 ip netns exec ns101 ip netns exec ns102 ip netns exec ns103 ip netns exec ns104 ip netns exec ns105 ip netns exec ns106 ip netns exec ns107 ip netns exec ns108 ip netns exec ns109 ip netns exec ns110 ip netns exec ns111 ip netns exec ns112 ip netns exec ns113 ip netns exec ns114 ip netns exec ns115 ip netns exec ns116 ip netns exec ns117 ip netns exec ns118 ip netns exec ns119 ip netns exec ns120 ip netns exec ns121 ip netns exec ns122 ip netns exec ns123 ip netns exec ns124 ip netns exec ns125 ip netns exec ns126 ip netns exec ns127 ip netns exec ns128 ip netns exec ns129 ip netns exec ns130 ip netns exec ns131 ip netns exec ns132 ip netns exec ns133 ip netns exec ns134 ip netns exec ns135 ip netns exec ns136 ip netns exec ns137 ip netns exec ns138 ip netns exec ns139 ip netns exec ns140 ip netns exec ns141 ip netns exec ns142 ip netns exec ns143 ip netns exec ns144 ip netns exec ns145 ip netns exec ns146 ip netns exec ns147 ip netns exec ns148 ip netns exec ns149 ip netns exec ns150 ip netns exec ns151 ip netns exec ns152 ip netns exec ns153 ip netns exec ns154 ip netns exec ns155 ip netns exec ns156 ip netns exec ns157 ip netns exec ns158 ip netns exec ns159 ip netns exec ns160 ip netns exec ns161 ip netns exec ns162 ip netns exec ns163 ip netns exec ns164 ip netns exec ns165 ip netns exec ns166 ip netns exec ns167 ip netns exec ns168 ip netns exec ns169 ip netns exec ns170 ip netns exec ns171 ip netns exec ns172 ip netns exec ns173 ip netns exec ns174 ip netns exec ns175 ip netns exec ns176 ip netns exec ns177 ip netns exec ns178 ip netns exec ns179 ip netns exec ns180 ip netns exec ns181 ip netns exec ns182 ip netns exec ns183 ip netns exec ns184 ip netns exec ns185 ip netns exec ns186 ip netns exec ns187 ip netns exec ns188 ip netns exec ns189 ip netns exec ns190 ip netns exec ns191 ip netns exec ns192 ip netns exec ns193 ip netns exec ns194 ip netns exec ns195 ip netns exec ns196 ip netns exec ns197 ip netns exec ns198 ip netns exec ns199 ip netns exec ns200 ip netns exec ns201 ip netns exec ns202 ip netns exec ns203 ip netns exec ns204 ip netns exec ns205 ip netns exec ns206 ip netns exec ns207 ip netns exec ns208 ip netns exec ns209 ip netns exec ns210 ip netns exec ns211 ip netns exec ns212 ip netns exec ns213 ip netns exec ns214 ip netns exec ns215 ip netns exec ns216 ip netns exec ns217 ip netns exec ns218 ip netns exec ns219 ip netns exec ns220 ip netns exec ns221 ip netns exec ns222 ip netns exec ns223 ip netns exec ns224 ip netns exec ns225 ip netns exec ns226 ip netns exec ns227 ip netns exec ns228 ip netns exec ns229 ip netns exec ns230 ip netns exec ns231 ip netns exec ns232 ip netns exec ns233 ip netns exec ns234 ip netns exec ns235 ip netns exec ns236 ip netns exec ns237 ip netns exec ns238 ip netns exec ns239 ip netns exec ns240 ip netns exec ns241 ip netns exec ns242 ip netns exec ns243 ip netns exec ns244 ip netns exec ns245 ip netns exec ns246 ip netns exec ns247 ip netns exec ns248 ip netns exec ns249 ip netns exec ns250 ip netns exec ns251 ip netns exec ns252 ip netns exec ns253 ip netns exec ns254 ip netns exec ns255 ip netns exec ns256 ip netns exec ns257 ip netns exec ns258 ip netns exec ns259 ip netns exec ns260 ip netns exec ns261 ip netns exec ns262 ip netns exec ns263 ip netns exec ns264 ip netns exec ns265 ip netns exec ns266 ip netns exec ns267 ip netns exec ns268 ip netns exec ns269 ip netns exec ns270 ip netns exec ns271 ip netns exec ns272 ip netns exec ns273 ip netns exec ns274 ip netns exec ns275 ip netns exec ns276 ip netns exec ns277 ip netns exec ns278 ip netns exec ns279 ip netns exec ns280 ip netns exec ns281 ip netns exec ns282 ip netns exec ns283 ip netns exec ns284 ip netns exec ns285 ip netns exec ns286 ip netns exec ns287 ip netns exec ns288 ip netns exec ns289 ip netns exec ns290 ip netns exec ns291 ip netns exec ns292 ip netns exec ns293 ip netns exec ns294 ip netns exec ns295 ip netns exec ns296 ip netns exec ns297 ip netns exec ns298 ip netns exec ns299 ip netns exec ns300 ip netns exec ns301 ip netns exec ns302 ip netns exec ns303 ip netns exec ns304 ip netns exec ns305 ip netns exec ns306 ip netns exec ns307 ip netns exec ns308 ip netns exec ns309 ip netns exec ns310 ip netns exec ns311 ip netns exec ns312 ip netns exec ns313 ip netns exec ns314 ip netns exec ns315 ip netns exec ns316 ip netns exec ns317 ip netns exec ns318 ip netns exec ns319 ip netns exec ns320 ip netns exec ns321 ip netns exec ns322 ip netns exec ns323 ip netns exec ns324 ip netns exec ns325 ip netns exec ns326 ip netns exec ns327 ip netns exec ns328 ip netns exec ns329 ip netns exec ns330 ip netns exec ns331 ip netns exec ns332 ip netns exec ns333 ip netns exec ns334 ip netns exec ns335 ip netns exec ns336 ip netns exec ns337 ip netns exec ns338 ip netns exec ns339 ip netns exec ns340 ip netns exec ns341 ip netns exec ns342 ip netns exec ns343 ip netns exec ns344 ip netns exec ns345 ip netns exec ns346 ip netns exec ns347 ip netns exec ns348 ip netns exec ns349 ip netns exec ns350 ip netns exec ns351 ip netns exec ns352 ip netns exec ns353 ip netns exec ns354 ip netns exec ns355 ip netns exec ns356 ip netns exec ns357 ip netns exec ns358 ip netns exec ns359 ip netns exec ns360 ip netns exec ns361 ip netns exec ns362 ip netns exec ns363 ip netns exec ns364 ip netns exec ns365 ip netns exec ns366 ip netns exec ns367 ip netns exec ns368 ip netns exec ns369 ip netns exec ns370 ip netns exec ns371 ip netns exec ns372 ip netns exec ns373 ip netns exec ns374 ip netns exec ns375 ip netns exec ns376 ip netns exec ns377 ip netns exec ns378 ip netns exec ns379 ip netns exec ns380 ip netns exec ns381 ip netns exec ns382 ip netns exec ns383 ip netns exec ns384 ip netns exec ns385 ip netns exec ns386 ip netns exec ns387 ip netns exec ns388 ip netns exec ns389 ip netns exec ns390 ip netns exec ns391 ip netns exec ns392 ip netns exec ns393 ip netns exec ns394 ip netns exec ns395 ip netns exec ns396 ip netns exec ns397 ip netns exec ns398 ip netns exec ns399 ip netns exec ns400 ip netns exec ns401 ip netns exec ns402 ip netns exec ns403 ip netns exec ns404 ip netns exec ns405 ip netns exec ns406 ip netns exec ns407 ip netns exec ns408 ip netns exec ns409 ip netns exec ns410 ip netns exec ns411 ip netns exec ns412 ip netns exec ns413 ip netns exec ns414 ip netns exec ns415 ip netns exec ns416 ip netns exec ns417 ip netns exec ns418 ip netns exec ns419 ip netns exec ns420 ip netns exec ns421 ip netns exec ns422 ip netns exec ns423 ip netns exec ns424 ip netns exec ns425 ip netns exec ns426 ip netns exec ns427 ip netns exec ns428 ip netns exec ns429 ip netns exec ns430 ip netns exec ns431 ip netns exec ns432 ip netns exec ns433 ip netns exec ns434 ip netns exec ns435 ip netns exec ns436 ip netns exec ns437 ip netns exec ns438 ip netns exec ns439 ip netns exec ns440 ip netns exec ns441 ip netns exec ns442 ip netns exec ns443 ip netns exec ns444 ip netns exec ns445 ip netns exec ns446 ip netns exec ns447 ip netns exec ns448 ip netns exec ns449 ip netns exec ns450 ip netns exec ns451 ip netns exec ns452 ip netns exec ns453 ip netns exec ns454 ip netns exec ns455 ip netns exec ns456 ip netns exec ns457 ip netns exec ns458 ip netns exec ns459 ip netns exec ns460 ip netns exec ns461 ip netns exec ns462 ip netns exec ns463 ip netns exec ns464 ip netns exec ns465 ip netns exec ns466 ip netns exec ns467 ip netns exec ns468 ip netns exec ns469 ip netns exec ns470 ip netns exec ns471 ip netns exec ns472 ip netns exec ns473 ip netns exec ns474 ip netns exec ns475 ip netns exec ns476 ip netns exec ns477 ip netns exec ns478 ip netns exec ns479 ip net

Ho proseguito creando una mia wordlist che daremo ad Hydra



Successivamente col parametro **-I** gli ho specificato il nome utente dell'user e con **-P** la wordlist per craccare le psw e per finire l'indirizzo di loopback (127.0.0.1) dato che era un attacco rivolto a me stesso, un'alternativa poteva essere come detto dalle slide il parametro **-L** per usare la wordlist anche per craccare il nome utente ci ho riprovato anche con questa formula ma ormai avevo già usato il metodo elencato qui sopra e non rielaborava il cracking, un'altra alternativa valida poteva essere spostare il servizio ssh di giacomino su un'altra porta per scagliare l'attacco usando l'ip della mia macchina e non il loopback, ho proceduto col primo metodo perchè è quello che mi è venuto in mente per primo in caso di autotest di seguito provo quanto ho scritto!

