

Ciao Valerio insieme a questo documento troverai anche il programmino in py del bruteforce richiesto dalla traccia.

[illegible]

Questo è lo screen che hai richiesto della prima prova. Purtroppo per questioni di tempo sono solo potuto arrivare al livello 20.

Per quanto riguarda il programmino ti allego anche qui uno screen oltre al programma zero e proprio su git.

```
import paramiko

def test_authentication(username, hostname, password):
    client = paramiko.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

    (method def set_missing_host_key_policy(policy: type[MissingHostKeyPolicy] | MissingHostKeyPolicy) -> None
    cli Set policy to use when connecting to servers without a known host key.
    pri Specifically:
    ret
        • A policy is a "policy class" (or instance thereof), namely some subclass of .MissingHostKeyPolicy such as .RejectPolicy (the default), .AutoAddPolicy ,
        • .WarningPolicy , or a user-created subclass.
    except
    pri
    ret
        • A host key is known when it appears in the client object's cached host keys structures (those manipulated by load_system_host_keys and/or
        load_host_keys ).

Parameters
cli policy: .MissingHostKeyPolicy
cli the policy to use when receiving a host key from a previously-unknown server

# Prova una lista di password finché una funziona

passwords = ["password", "123554", "password2", "kali", "ciaociao", "1231234123", "udsaiodu"]
for p in passwords:
    if test_authentication("kali", "192.168.50.100", p):
        break

# Interrompe se trova la password giusta
```

Spero sia tutto corretto e nel caso contrario mi scuso in anticipo... Grazie mille e buon proseguimento