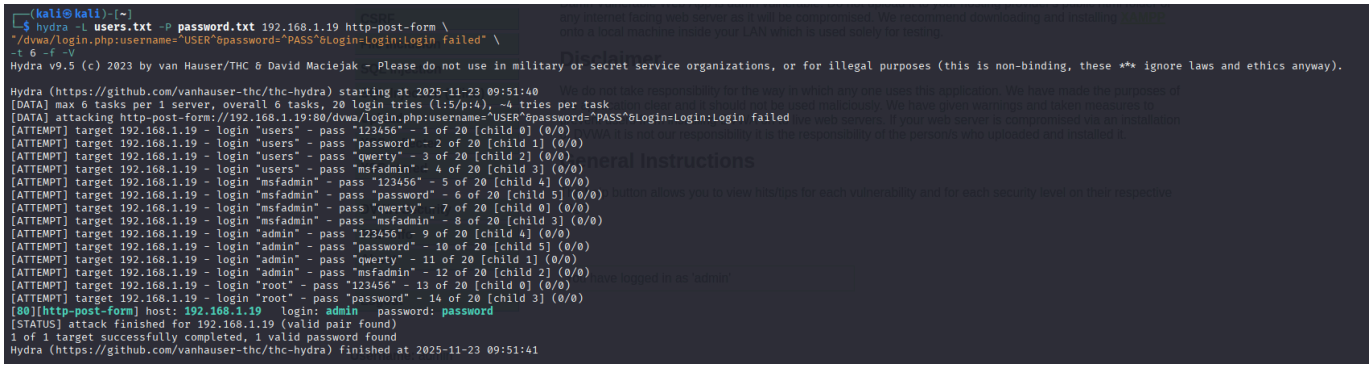
Realizando Ataque Brute Force a um formulário Web vulnerável intencionalmente através da máquina Metasploitable

Inspecionando o site e tentando fazer login na página eu vejo como é o corpo da requisição POST na hora de fazer um request de login, e verifico também que o formulário de login não possui bloqueio após determinadas tentativas de login falhadas (rate limiting).

Utilizei o Hydra para realizar ataque de força bruta no formulário de login da aplicação web em /dwwa/login.php. O ataque explorou a ausência de rate limiting testando combinações de credenciais através de requisições POST simultâneas.



Após o ataque descobrimos o nome de usuário e senha do sistema.
Esse ataque é muito simples e tem como o objetivo destacar como formulários básicos que possuem baixa ou nenhuma segurança podem ser um porta de entrada para ataques maiores.

Uma política de senha fortes deveria ser aplicada ao sistema para garantir uma maior segurança exigindo números, letras, caracteres especiais, evitando uso de informações pessoais e sequências numéricas. Além disso as vulnerabilidades aqui encontradas podem ser facilmente corrigidas adicionando um rate limiting, um captcha após determinadas tentativas de logins e bloqueio de ip após muitas tentativas consecutivas. Para uma camada de segurança ainda maior poderia ser adicionado um MFA ou 2FA, para validar a identidade de quem está acessando o sistema.