10/07/2023 – TryHackMe – Hydra

Link: <https://tryhackme.com/room/hydra>

1. Usando nmap para análise de portas (o CTF já informava os serviços que devem-se explorar, mas para ter certeza de quais portas foram usadas, se utilizou do nmap):

Texto

Descrição gerada automaticamente

1. Respondendo primeira pergunta (serviço web). Verificando o serviço http:

Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente

1. Verificando o que acontece quando se insere uma senha incorreta:

Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente

1. Verificando no BurpSuite quais são os parâmetros do “POST”:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Utilizando a lista “rockyou.txt” e utilizando como incorreto o texto “Your username or password is incorrect”:

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente

1. Logando como “molly” de senha “sunshine”:

Tela de computador com imagem de personagem de desenho animado

Descrição gerada automaticamente com confiança média

Portanto, a primeira flag é $flag

1. Utilizando o hydra para ssh:

Tela de computador

Descrição gerada automaticamente

1. Fazendo a conexão ssh com a senha “butterfly”:

Texto

Descrição gerada automaticamente

1. Verificando os arquivos e encontrando a flag:

Tela preta com letras brancas

Descrição gerada automaticamente

Portanto, a segunda flag é: $flag