**12/05/2024 – Brute It**

<https://tryhackme.com/r/room/bruteit>

1. Varredura com Nmap
   1. -A – agressivo (versões e SO)
   2. -Pn – pula etapa de ping no servidor

Texto

Descrição gerada automaticamente

1. Escaneamento com Gobuster

Texto

Descrição gerada automaticamente

1. Descoberta do usuário e senha com Hydra e Rockyou
2. -V – verboso

Texto

Descrição gerada automaticamente]

1. Quebra da chave privada RSA utilizando John
   1. armazenamento da chave em um txt para usar John
   2. utilização da wordlist rockyou



Texto

Descrição gerada automaticamente

1. Conexão com SSH

Texto

Descrição gerada automaticamente

1. Privesc com /etc/passwd e /etc/shadow
   1. /etc/passwd – encontra os usuários
   2. /etc/shadow – senhas criptografadas
   3. usar comando unshadow entre o arquivo /etc/passwd e /shadow
   4. john para decriptografar senha
   5. transformar usuário em superusuário com senha: su root

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Site

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente