**14/05/2024 – Mr Robot**

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

1. Exploração com Nmap

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Exploração com Gobuster
   1. site aparenta ser wordpress – wpscan

Texto

Descrição gerada automaticamente

1. Procurando vulnerabilidades com wpscan

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Acessando robots.txt
   1. fsociety.dic – wordlist com diversas palavras

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

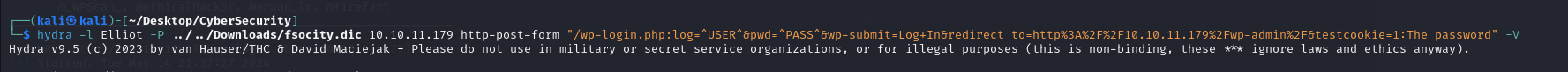
1. Brute force com wordlist dada
   1. o texto para erro de nome de usuário e para nome de senha são diferentes
   2. descobrir primeiro o usuário depois a senha
   3. hydra ou wpscan – wpscan mais rápido
   4. a senha está no final da lista (bastante tempo) - ER28-0652

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Site

Descrição gerada automaticamente



1. Reverse shell no Appearence
   1. injetando código malicioso no 404 template
   2. acessando: /wordpress/wp-content/themes/twentyfifteen/404.php

Texto

Descrição gerada automaticamente

1. Privesc
   1. sudo não é permitido
   2. listando SUIDs
   3. nmap é promissor para fazer privesc

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente