**... - BLOG**

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

1. Varredura com Nmap
   1. -A – opção agressiva, detecta SO e versões
   2. CMS - site feito em wordpress - <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress>

Texto

Descrição gerada automaticamente

1. WordPress exploits
   1. checagem dos usuários do WordPress
   2. procura por vulnerabilidades utilizando wpscan – gerar token de api no site do wpscan
   3. descoberta da versão

Texto

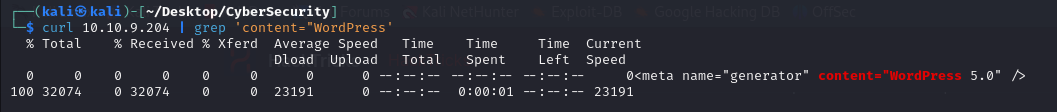
Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente



1. Busca das senhas com wpscan

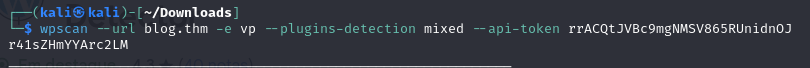
Texto

Descrição gerada automaticamente

Texto

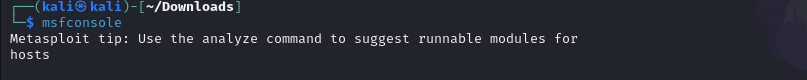
Descrição gerada automaticamente

1. Explorando vulnerabilidade WordPress 5.0.0
   1. <https://www.exploit-db.com/exploits/49512>
   2. wpscan para descobrir theme
   3. msfconsole - use exploit/multi/http/wp\_crop\_rce (https://www.rapid7.com/db/modules/exploit/multi/http/wp\_crop\_rce/)



Texto

Descrição gerada automaticamente



Texto

Descrição gerada automaticamente

1. Explorando os diretórios
   1. arquivo fake user.txt em /home/bjoel

Uma imagem contendo Texto

Descrição gerada automaticamente