**23/05/2024 - IGNITE**

<https://tryhackme.com/r/room/ignite?ref=skerritt.blog>

1. Análise do website no navegador
   1. utilizando cms Fuel CMS

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

* 1. site rodando em servidor Apache

Texto

Descrição gerada automaticamente

* 1. acesso de admin (o usuário e a senha foram mantidos padrão admin e admin)

Texto

Descrição gerada automaticamente

1. Escaneamento das portas com Nmap
   1. escaneamento de todas as portas com -p- (sem detectar versões ou SO ainda, apenas serviço e status da porta)

Texto

Descrição gerada automaticamente

* 1. apenas porta 80 (http) encontrada – escaneamento profundo com -A

Texto

Descrição gerada automaticamente

* 1. sem porta com serviços de conexão remota
  2. presença de robots.txt

1. Analisando Robots.txt
   1. apenas o diretório /fuel já descoberto anteriormente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Procurando exploit pelo CMS (Fuel)
   1. código para execução de código remoto (útil para reverse shell): <https://github.com/ice-wzl/Fuel-1.4.1-RCE-Updated/blob/main/Fuel-Updated.py>
   2. execução do código passando ip da máquina, meu ip e porta a ser escutada

Texto

Descrição gerada automaticamente

* 1. utilização do netcat para conexão

Texto

Descrição gerada automaticamente

1. Procurando pela flag User.txt
   1. procurando pelos diretórios – indo para pasta home (onde tem os usuários geralmente) e entrando na pasta www-data encontra-se uma flag.txt

Texto

Descrição gerada automaticamente com confiança média

1. Privilege Escalation
   1. utilizando linpeas
   2. disponibilizando servidor para puxar arquivo linpeas

Texto

Descrição gerada automaticamente

* 1. puxando linpeas.sh com wget



* 1. alterando permissão de execução do linpeas e executando

Uma imagem contendo Diagrama

Descrição gerada automaticamente

* 1. indicação de uma senha no arquivo database.php

Texto

Descrição gerada automaticamente

* 1. visualizando o conteúdo descobre-se que a senha mememe é do usuário root

Texto

Descrição gerada automaticamente com confiança média

* 1. tentando trocar de usuário com su root

Interface gráfica do usuário, Texto

Descrição gerada automaticamente com confiança média

* 1. gerando terminal interativo com python (python -c 'import pty; pty.spawn("/bin/bash")')

Texto

Descrição gerada automaticamente

* 1. encontrando a flag

Texto

Descrição gerada automaticamente