**12/05/2024 - OVERPASS**

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

1. Escaneamento com Nmap

Texto

Descrição gerada automaticamente

1. Exploração com Gobuster

Texto

Descrição gerada automaticamente

1. Analisando JavaScript e cookies
   1. o login seta o cookie e direciona para /admin novamente – ideia: setar um cookie aleatório para ser redirecionado para tela de admin
   2. setar cookie com qualquer coisa e dar refresh entra na tela de admin

Texto

Descrição gerada automaticamente



Texto, Carta

Descrição gerada automaticamente

1. Conexão com chave RSA
   1. quebrando criptografia da chave com ssh2john.py
   2. usando usuário james e chave

Texto

Descrição gerada automaticamente com confiança média

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Testando linpeas para escalar privilégio
   1. arquivo /etc/hosts da para alterar
   2. SUIDs e SGIDs

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Arquivo todo.txt na home
   1. “automated build script” – cronjobs

Texto

Descrição gerada automaticamente

1. Explorando cronjobs
   1. faz curl no buildscript.sh de forma root – ideal para privilegie escalation
   2. mudança no /etc/hosts para mudar o “DNS” para a minha máquina
   3. reverse shell por meio do servidor python na máquia

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente