Write-up SIMOC

Box 10 - Write Up

- enumeração mostra serviços de ftp, ssh e web rodando
- pagina inicial da web possui imagem do gumball, nela é possível extrair a bandeira em keywords com exiftool [FLAG!]
- enumerando web com gobuster, encontramos a página /hidden
- esta página sinaliza manutenção, e possui um link no "Obrigado" que leva para um arquivo QR Code
- ao decodificar o QR Code, encontra bandeira, além de um pequeno script em bash que conecta ao ftp com as credenciais do usuário carlos [FLAG!]

USER=carlos PASSWORD=C@rL0$@1111

- Ao conectar no ftp com Carlos, existe um arquivo info.txt e listas.txt... o info trata-se de uma msg do carlos para o claudio indica um brute force de ssh pra logar como claudio com a pequena wordlist

claudio:8@zeZZz

- ao logar como claudio, obter a flag em seu /home [FLAG!]
- sudo -l do claudio mostra bash script feedback.sh que pode ser executado com o usuario joao, este arquivo executa o comando que for passado no input de feedback
- com isso, é possível ganhar um shell como joao, a flag dele está em seu home [FLAG!]
- joao é membro do grupo docker, chamando docker image ls já existe uma imagem do alpine
- é possível ganhar acesso root explorando uma chamada do alpine com chroot para volume montado, no GTfobins tem todo passo a passo
- como root, a flag está em /root/root.txt [FLAG!]