Write-up SIMOC

- enumeração, acha ssh, http 80 e tcp/111
- acessando browser, meme do cachorro hacker
- enumerando diretórios web, acha /robots.txt, nele está a primeira flag [FLAG!]
- nessa enumeração identifica o diretório da aplicação, em /company
- index é igual a started.php, o código-fonte dessa página mostra mensagem de dev mencionando parâmetro file sendo incluído
- identifica que file consegue ler arquivos e está vulnerável a path traversal
- identifica que o access.log do Apache está logando User-Agent, e ao injetar um payload php nesse cabeçalho o mesmo é interpretado pelo php na chamada
- com isso, é possível, por exemplo, criar um argumento que executa chamadas no sistema
- pode-se chamar um shell reverso
- aplicação web roda como www-data, ao obter um shell reverso é possível descobrir a flag em /var/www [FLAG!]
- enumerando usuários do sistema, é identificado o usuário viper
- em /var existe um diretório backups, que contém cópias de arquivos de log do sistema. No auth.log de lá, constam erros de autenticação, como se o usuário tivesse digitado a senha no campo de login... ?V1p3r2020!?
- ao testar login viper e esta senha, foi possível logar... no home do viper está a flag [FLAG!]
- no home do viper existe um subdir backup_site, nele existe um binário em assets/vendor/weapon/run
- este binário executa o perl e com cap_setuid habilitado , da para chamar o perl passando argumento de bin/bash foi pego o argumento no GTfobins,depois foi so receber shell root (essa informação do cap_setuid pode ser descoberta pelo linpeas, por exemplo)

- flag dentro do /root [FLAG!]