Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | SuitGuy |
| **N° Revisão** | 1 |
| **Data de publicação** | 31/08/2020 |
| **Link** | https://tryhackme.com/room/gamingserver |

|  |  |  |
| --- | --- | --- |
| **Redação** | Murilo O. Marchezzane | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Enumeração e Análise de Aplicações Web |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Pergunta 1](#_heading=h.3znysh7) 5

[Pergunta 2](#_heading=h.2et92p0) 6

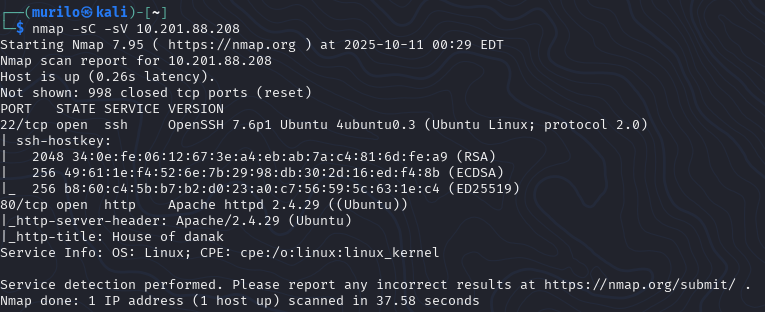
[Conclusão](#_heading=h.1t3h5sf) 7

**Contextualização**

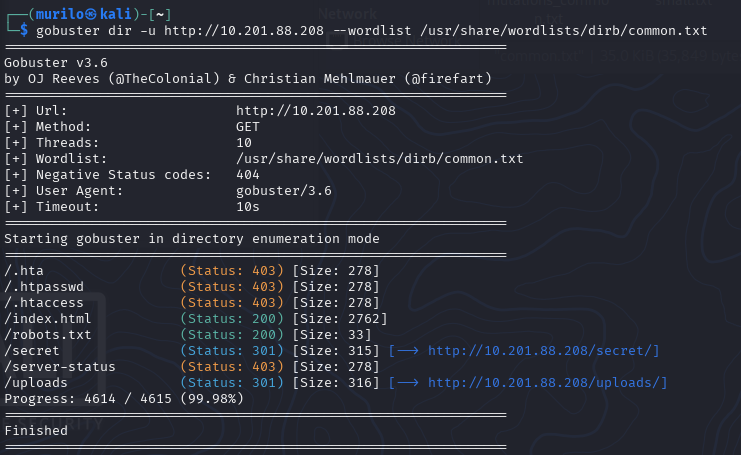
Bem-vindo ao meu write-up para a room gamingserver do TryHackMe. O objetivo aqui é explorar as fraquezas de um servidor de jogos construído por desenvolvedores inexperientes. O foco da análise e do ataque será o seu sistema de *deployment*, que se mostrará o caminho para obter acesso inicial à máquina.

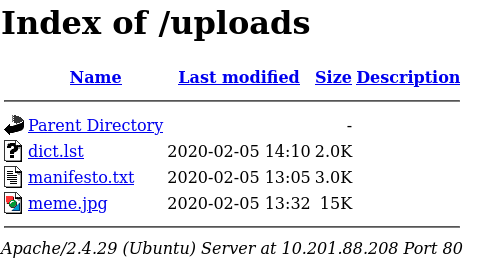
**Desenvolvimento**

para começarmos utilizamos o comando “nmap -sC -sV -p- 10.201.25.95” onde procuramos todas as devidas portas:



Após isso utilizo o gobuster para saber qual diretórios há:



Abrindo o “<http://10.201.88.208/uploads/>” nós damos de cara com: 

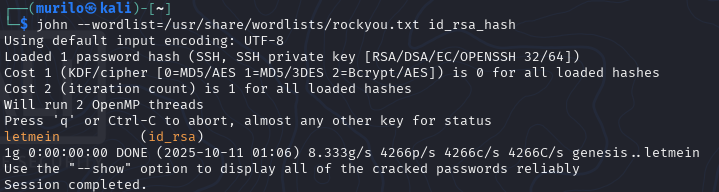
E o “<http://10.201.88.208/secret/>” temos uma chave SSH Encriptado:



Agora O objetivo é realizar a quebra da senha da chave privada RSA criptografada. Para isso, utilizaremos o utilitário ssh2john para extrair o hash da chave do arquivo (que foi salvo como id\_rsa). Em seguida, o John the Ripper (John) será empregado para realizar um ataque de força bruta ou dicionário contra o hash extraído, a fim de descobrir a *passphrase* original. Então utilizo essa série de código:

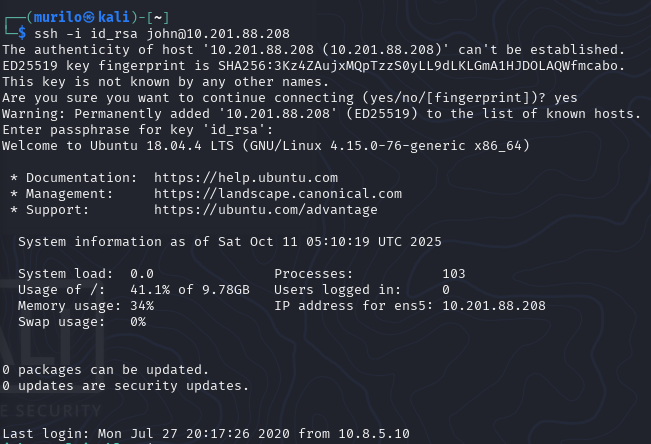






Após tento fazer a conexão com o ssh, então utilizo essa série de comando:





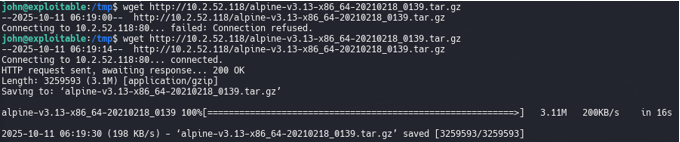
**Pergunta 1 - What is the user flag?**

Após fazer o Login, faço um ls e vejo que tem um arquivo user.txt: ao fazer um “cat” recebo a resposta:

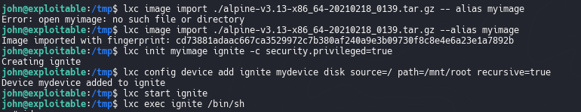


**Pergunta 2 - What is the root flag?**

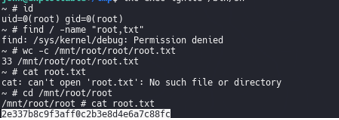
começamos utilizando o wget para fazer o download do alpine:



após isso utilzamos o lxc para criar o conteiner e ter acesso a flag. O conteiner que criamos se chama iginite:



então ao executarmos o sistema procuramos o root.txt e encontramos a resposta da flag:



**Conclusão**

O desafio "gamingserver" demonstrou a importância de práticas de segurança robustas, mesmo em ambientes desenvolvidos por amadores. Iniciamos a fase de reconhecimento com o nmap, o que nos permitiu mapear os serviços em execução e identificar portas abertas cruciais para a exploração. Em seguida, a enumeração de diretórios via gobuster foi fundamental, revelando dois pontos de interesse: o diretório /uploads/ e, mais criticamente, o diretório /secret/, onde encontramos uma chave privada SSH encriptada.

Este achado direcionou a próxima etapa, que consistiu na quebra da senha da chave. Utilizando o ssh2john para extrair o hash da chave RSA e, posteriormente, o John The Ripper para realizar o ataque de dicionário, fomos capazes de recuperar a passphrase e autenticar-nos com sucesso no servidor via SSH, obtendo acesso ao primeiro nível de comprometimento.

O sucesso desta invasão ressalta duas falhas de segurança críticas: a exposição de credenciais sensíveis (a chave SSH) em um diretório acessível via web e a vulnerabilidade do sistema de deployment, insinuada na introdução do desafio. Ao obter acesso como usuário, alcançamos o objetivo imediato de capturar a user flag.

Em suma, este cenário serviu como um excelente exercício prático para o fluxo de trabalho em testes de penetração, desde a enumeração de rede e web até a exploração de credenciais fracas ou mal armazenadas, preparando o terreno para a próxima fase de escalonamento de privilégios.