Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

GamingServer – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | GamingServer – Gabriel F. Sabino |
| **N° Revisão** |  |
| **Data de publicação** | 08/09/2025 |
| **Link** | https://tryhackme.com/room/gamingserver |

|  |  |  |
| --- | --- | --- |
| **Redação** | Gabriel F. Sabino | Estudante |
| **Revisão** |  |  |
| **Aprovação** |  |  |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 08/09/2025 | Gabriel F. Sabino |
| **1** |  |  |
| **2** |  |  |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Exploração web, Escalação de Privilégio, Containers |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

What is the user flag 3

What is the root flag 7

[Conclusão](#_heading=h.1t3h5sf) 9

[Referências](#_heading=h.4d34og8) 10

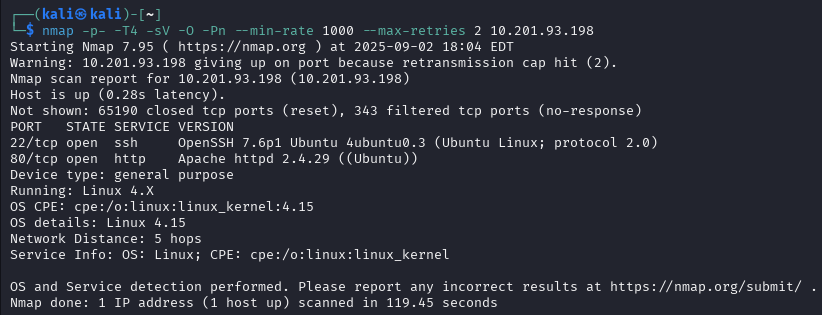
**Contextualização**

O CTF "Gaming Server" do TryHackMe é um desafio visando testar habilidades de webhacking, como exploração web e escalação de privilégio.

**Desenvolvimento**

**What is the USER flag?**

Iniciamos fazemos um scan usando nmap:



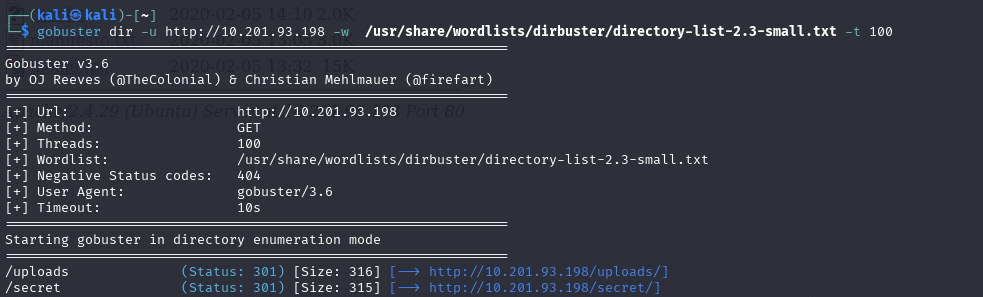
Observa-se que há duas portas, vamos analisar a porta http primeiro. Indo até ele, vemos um site para um jogo:



Analisando o código fonte da página encontramos uma mensagem no final dela:



Conseguimos um possível login (john), agora utilizando o gobuster para encontrar diretórios, descobrimos apenas 2:



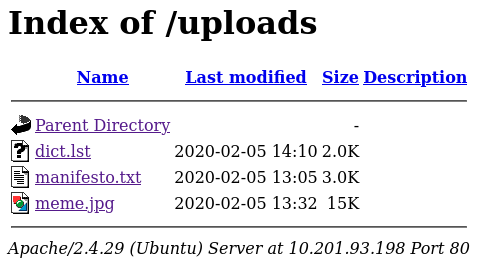
Vamos primeiro ir até o /secret:



Abrindo o arquivo secretKey, temos uma chave RSA:

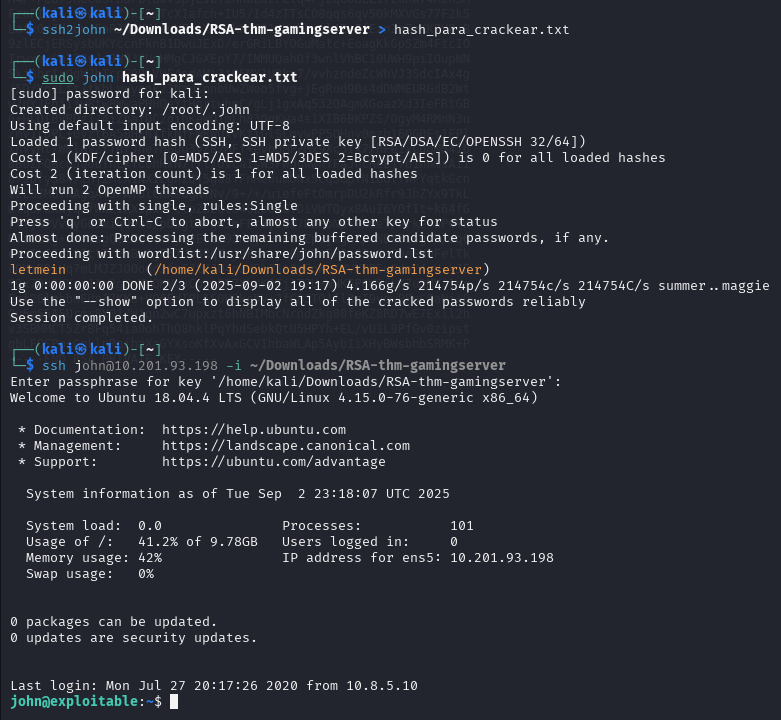


Agora indo até /uploads temos:

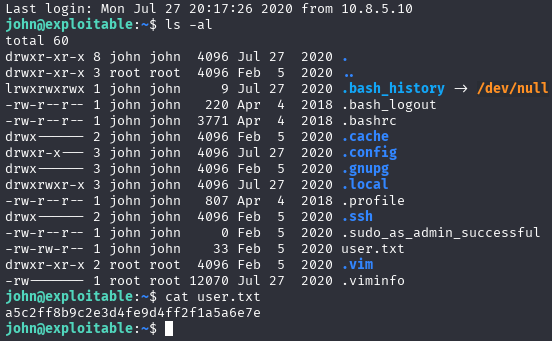


Tanto o meme.jpg quanto o manifesto.txt não parecem ter nada, analisando dict.lst parece ser uma lista de palavras, talvez para ser usada como wordlist?

Vamos tentar agora entrar no ssh, usando a wordlist não funcionou, vamos tentar descriptografar a chave RSA com o johnthereaper:



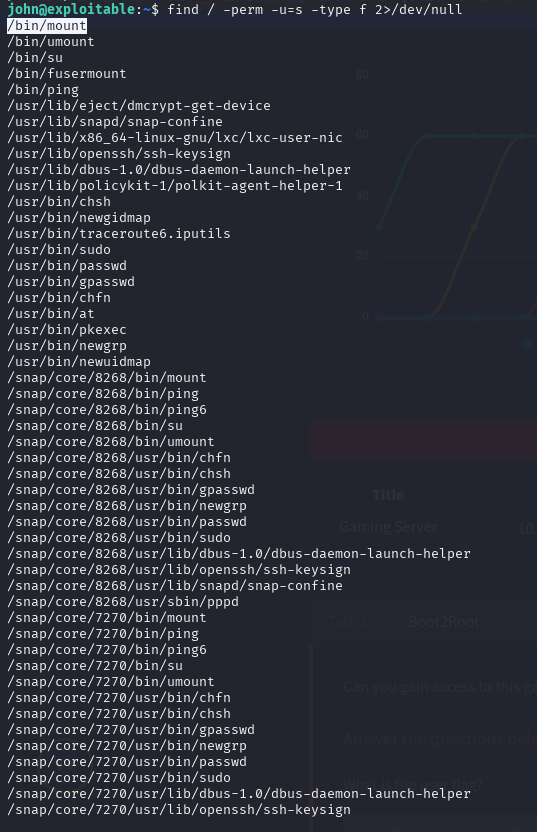
Conseguimos encontrar a senha do ssh (letmein), agora com ela conseguimos entrar como John, vamos ver o que temos:



Encontrando o arquivo user.txt parece promissor, abrindo ele, encontramos a user flag.

**What is the ROOT flag?**

Para acessarmos como root, vamos tentar por SUID primeiro, usando o comando find, vemos quais comandos temos permissão para usar:



Fazendo uma busca no GTFOBins, vemos que o /mount pode ser exploitado, mas ao tentar, ele utiliza sudo e pede a senha do usuário John, que não temos, impossibilitando assim seguirmos por esse caminho:



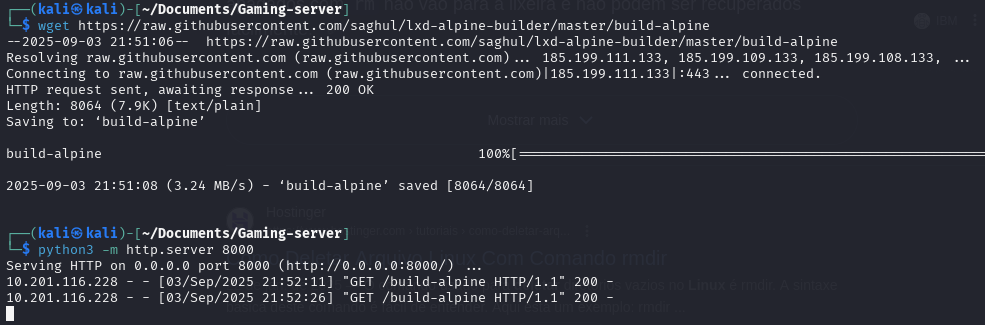
Tentaremos então o comando id para ver se existe algum grupo que se destaca ou que pode ser vulnerável:

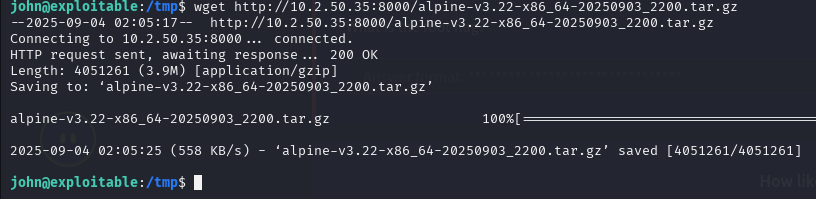


Vemos que existe o grupo lxd, ele é uma extensão do lxc.

O lxc (LinuX Containers) é um container, um ambiente separado, mas que roda códigos usando o mesmo host e kernel do host.

Buscando na internet, descobrimos que o lxc possui exploits, mas precisamos colocar a distribuição Alpine para poder exploitar o lxc. Entretanto, não conseguimos colocar diretamente arquivos no alvo, então temos que baixar na nossa máquina e depois transferir ao alvo:

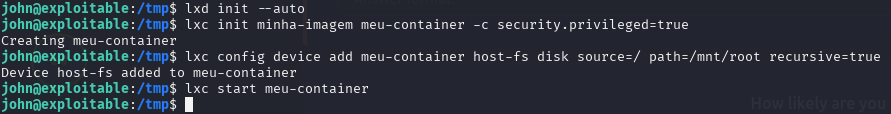




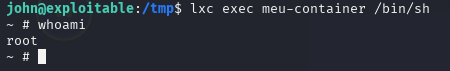
Agora que o Alpine está no alvo, vamos importar uma imagem para o lxc:



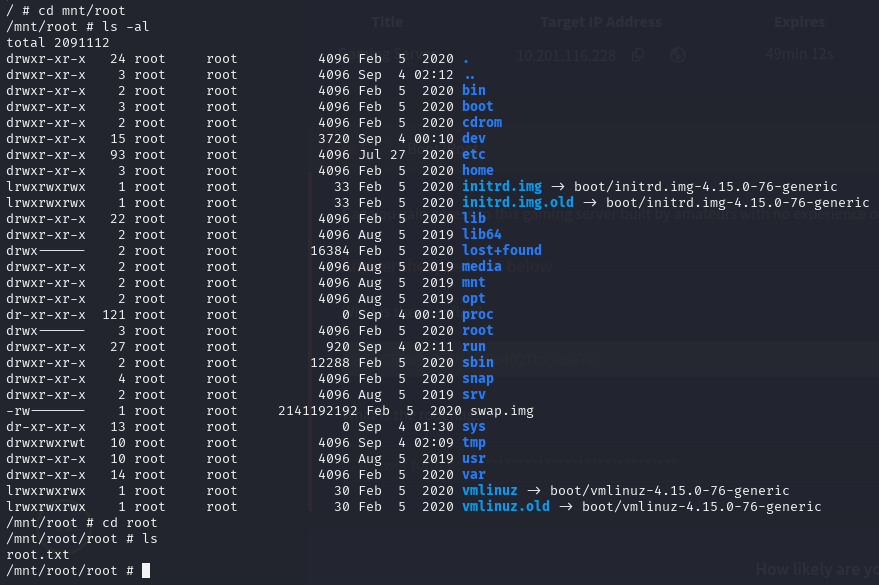
Com a imagem no lxc, inicializamos ele e, em seguida, criamos e configuramos o container para que ele tenha permissão root:



Feito isso entramos no container que acabamos de criar e nós nos tornamos root no container:



Devemos conseguir entrar no diretório da máquina mantendo o privilégio root:



Abrindo o arquivo root.txt obtemos a segunda e última flag:



**Conclusão**

Este CTF é uma boa porta de entrada para containers, já que não se aprofunda muito no tema mas faz o usuário buscar um pouco sobre para conseguir entender como funciona e como se aproveitar dele, além disso as partes de exploração web não são de grande dificuldade e possibilitam o usuário praticar suas habilidades no tema.

**Referências**

<https://chatgpt.com/>

<https://www.redhat.com/pt-br/topics/containers/whats-a-linux-container>

<https://gtfobins.github.io/gtfobins/mount/>

<https://linuxcontainers.org/lxc/introduction/>