Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

GamingServer – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | GamingServer – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 22/04/2025 |
| **Link** | https://tryhackme.com/room/gamingserver |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 22/04/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | *Port Scanning*, Enumeração web, *Brute-Force, Privilege Escalation* via containers. |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_Toc196242830)

[Desenvolvimento 3](#_Toc196242831)

[What is the user flag? 3](#_Toc196242832)

[What is the root flag? 9](#_Toc196242833)

[Conclusão 10](#_Toc196242834)

[Referências 10](#_Toc196242835)

Contextualização

O CTF Gaming Server, é um desafio do TryHackMe de nível fácil, onde aborda temas como enumeração de IP e diretórios web, exploração de uma máquina via SSH, quebra de senhas, e escalonamento de privilégios com contêineres LXD.

Desenvolvimento

What is the USER flag?

Para começar, execute o **Nmap** para fazer um *Port Scanning* na máquina desejada.

Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta apontou que a porta 22 e a porta 80 estão abertas, executando serviços de SSH para conexão remota e HTTP para hospedagem web respectivamente.

No navegador, investigue a página web.

Interface gráfica do usuário, Site

O conteúdo gerado por IA pode estar incorreto.

Ao inspecionar o código HTML, é possível encontrar o possível desenvolvedor do site, chamado ‘John’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Para continuar, enumere os diretórios presentes no site com a ferramenta **Gobuster** ou **Dirb**.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta aponta que há alguns diretórios desconhecidos, como ‘/robots.txt’, ‘/secret’ e ‘/uploads’. Investigue cada path do site.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

O diretório ‘/secret’ possui um arquivo chamado “secretKey”.

Texto

O conteúdo gerado por IA pode estar incorreto.

Esse arquivo contém uma chave privada para uma possível conexão SSH.

Copie e cole essa chave em um novo arquivo na máquina local.

Texto

O conteúdo gerado por IA pode estar incorreto.

Investigue o endpoint ‘/uploads’:

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Entre os arquivos presentes, o mais interessante é o ‘dict.lst’.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Esse arquivo contém diversas senhas que podem ser usadas para realizar um *Brute-Force*, esse tipo de arquivo é comumente chamado de “wordlists”.

Faça o download desse arquivo usando o comando ‘wget’ na máquina local.

Forma

O conteúdo gerado por IA pode estar incorreto.

Agora, deve-se fazer a conexão SSH (Conexão remota) com a máquina de ‘john’ usando o arquivo ‘rsaKey’ como chave. Mas que será pedido uma palavra-chave para continuar.

Então, será necessário descobrir essa palavra-chave a partir de ‘rsaKey’. Para isso, use o ‘ssh2john’ para transformar a key em uma hash e transferindo para um arquivo de texto. E então, use o **JohnTheRipper** para quebrar o hash da palavra-chave, usando a wordlist que foi encontrada(dict.lst) para fazer o *Brute-Force*.

Texto

O conteúdo gerado por IA pode estar incorreto.

Com isso, obtém-se conexão à máquina de ‘john’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Use o comando Linux ‘ls’ para listar os arquivos que estão contidos no diretório atual e então, use o comando ‘cat’ para visualizar a flag ‘user.txt’.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

What is the ROOT flag?

Para descobrir a flag root, será necessário fazer um *Privilege Escalation* ou escalonamento de privilégios. Para isso, verifique as permissões de usuário de ‘john’.



Enumerando a máquina com o comando ‘id’, é possível ver que esse usuário possui permissões suspeitas, e pertence a um grupo chamado ‘lxd’. Isso permite ao usuário interagir com o daemon do Linux Containers (LXD). Ou seja, criar e usufruir de ambientes de testes chamados de containers, utilizados para testes e virtualização.

Com isso, é possível criar um contêiner com permissões de usuário ‘root’. Para isso, faça o download de uma imagem Linux e hospede o arquivo usando o python com o comando ‘python3 -m http.server’ e na máquina do John, faça o download do arquivo com o ‘wget’. Texto

O conteúdo gerado por IA pode estar incorreto.

Monte a imagem da distribuição Linux e dê permissões de super usuário ao contêiner, e então monte a imagem no diretório ‘/mnt’. Após isso, execute o contêiner recém-criado em uma nova shell. Texto

O conteúdo gerado por IA pode estar incorreto.

E então, será conquistado privilégios de root. Navegue até o diretório ‘/root’ dentro do disco de montagem e lá estará a flag final do desafio.

Texto

O conteúdo gerado por IA pode estar incorreto.

Conclusão

Esse CTF é um desafio de nível simples de *Web Hacking*, onde novos ingressantes no mundo da segurança cibernética podem resolver. Além disso, o desafio em questão, demonstra a importância da configuração correta de um contêiner em um sistema, e seus possíveis vetores de ataque.

Referências

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

<https://book.hacktricks.wiki/sr/linux-hardening/linux-privilege-escalation-checklist.html>

<https://www.kali.org/tools/john/>