Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF de estudo – Nome do realizador |
| **N° Revisão** | 1 |
| **Data de publicação** | 25/10/2025 |
| **Link** | https://tryhackme.com/room/tomghost |

|  |  |  |
| --- | --- | --- |
| **Redação** | Vinícius Takashi | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 25/10/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | PrivEsc, CVE e Criptografia |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

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

[Pergunta 2 3](#_heading=h.2et92p0)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

O CTF Tomghost envolve a exploração de alguns conceitos de webhacking, como PrivEsc, exploração de uma CVE e criptografia.

**Desenvolvimento**

**Pergunta 1**

O passo inicial de todo desafio é o reconhecimento, então, o primeiro comando utilizado foi o nmap, a imagem a seguir mostra o resultado obtido:

Figura 1 – nmap   
Texto

O conteúdo gerado por IA pode estar incorreto.

Em seguida, foi realizada uma busca por exploits na versão do Apache Tomcat. Após algumas pesquisas, é possível encontrar várias formas de explorar uma CVE existente para essa versão (CVE-2020-1938), então, foi utilizado um exploit disponível no github. Então, a resposta desse exploit foi:

Figura 2 – exploit CVE-2020-1938

Texto

O conteúdo gerado por IA pode estar incorreto.

Então, a resposta obtida é um arquivo disponibilizado em um servidor vulnerável a falha. Nesse arquivo havia credenciais expostas do user skyfuck. Então, ao fazer a conexão ssh no ip pelo user: skyfuck, foi possível se conectar na máquina como usuário “skyfuck”.

Figura 3 – ssh conquistado



Então, ao explorar os diretórios é possível encontrar a primeira flag:

Figura 4 – flag user.txt



Ao explorar os diretórios, foi possível perceber indícios de que existe outro usuário a ser comprometido. No diretório raiz do usuário “skyfuck” havia alguns arquivos que pareciam ser chaves criptografadas. Então com ajuda do john the ripper e do comando “gpg” foi possível descriptografar e conseguir o acesso ao usuário “merlin”. As imagens a seguir mostram as etapas do processo de descriptografia:

Figura 5 – John the ripper

Tela de computador com fundo preto

O conteúdo gerado por IA pode estar incorreto.

Figuta 6 – uso do comando “gpg”

Texto

O conteúdo gerado por IA pode estar incorreto.

Então, com acesso ao usuário “merlin”, talvez seja possível a execução de um PrivEsc, pois com o user “skyfuck” não era possível fazer a elevação de privilégio, pelo menos não com o “sudo -l”.

**Pergunta 2**

Com acesso ao usuário “merlin”, o primeiro passo é descobrir com qual comando é possível fazer a elevação de privilégios. A imagem a seguir mostra com quais comandos, é possível fazer a elevação:

Figura 7 – sudo -l  
Texto

O conteúdo gerado por IA pode estar incorreto.

Então, com a ajuda do gtfobins, foi possível concluir a elevação e pegar a flag, como as imagens a seguir ilustram:

Figura 8 – PrivEsc

Texto

O conteúdo gerado por IA pode estar incorreto.

Figura 9 – flag root.txt



**Conclusão**

O CTF foi bom para relembrar as técnicas aprendidas durante as capacitações e praticar conceitos de criptografias diferentes.

**Referências**

<https://github.com/00theway/Ghostcat-CNVD-2020-10487>  
<https://gtfobins.github.io/gtfobins/zip/>