Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Kiba – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Kiba – Gabriel F. Sabino |
| **N° Revisão** |  |
| **Data de publicação** | 10/10/2025 |
| **Link** | https://tryhackme.com/room/kiba |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 10/10/2025 | Gabriel F. Sabino |
| **1** |  |  |
| **2** |  |  |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Exploração Web, Escalação de Privilégio, Prototype Pollution, Capabilities |
| **Plataforma** | Tryhackme |
| **Área** | Red |

Sumário

[Contextualização 3](#_Toc211032568)

[Desenvolvimento 3](#_Toc211032569)

[What is the vulnerability that is specific to programming languages with prototype-based inheritance? 3](#_Toc211032570)

[What is the version of visualization dashboard installed in the server? 3](#_Toc211032571)

[What is the CVE number for this vulnerability? 5](#_Toc211032572)

[Compromise the machine and locate user.txt 5](#_Toc211032573)

[How would you recursively list all of these capabilities? 7](#_Toc211032574)

[Escalate privileges and obtain root.txt 7](#_Toc211032575)

[Conclusão 8](#_Toc211032576)

[Referências 8](#_Toc211032577)

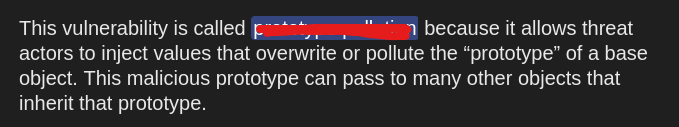
Contextualização

O CTF "Kiba" do TryHackMe é um desafio visando testar habilidades de webhacking, como exploração web e escalação de privilégio, além de aprender um pouco sobre o servidor Kibana e algumas de suas vulnerabilidades.

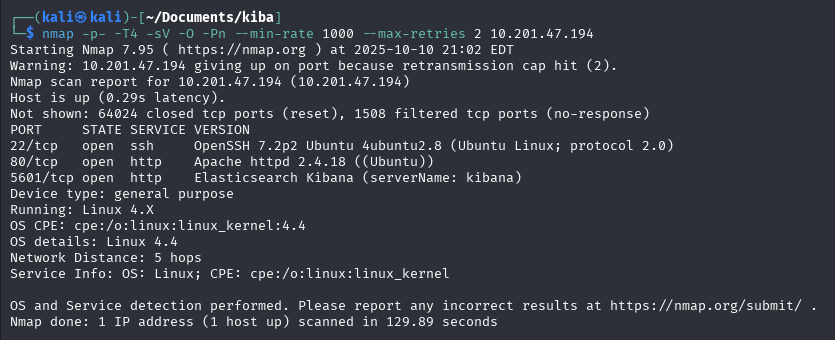
Desenvolvimento

What is the vulnerability that is specific to programming languages with prototype-based inheritance?

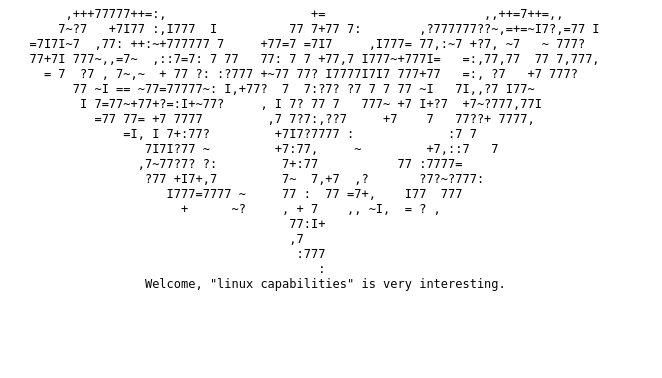
Buscando a pergunta no google, já encontramos a resposta:



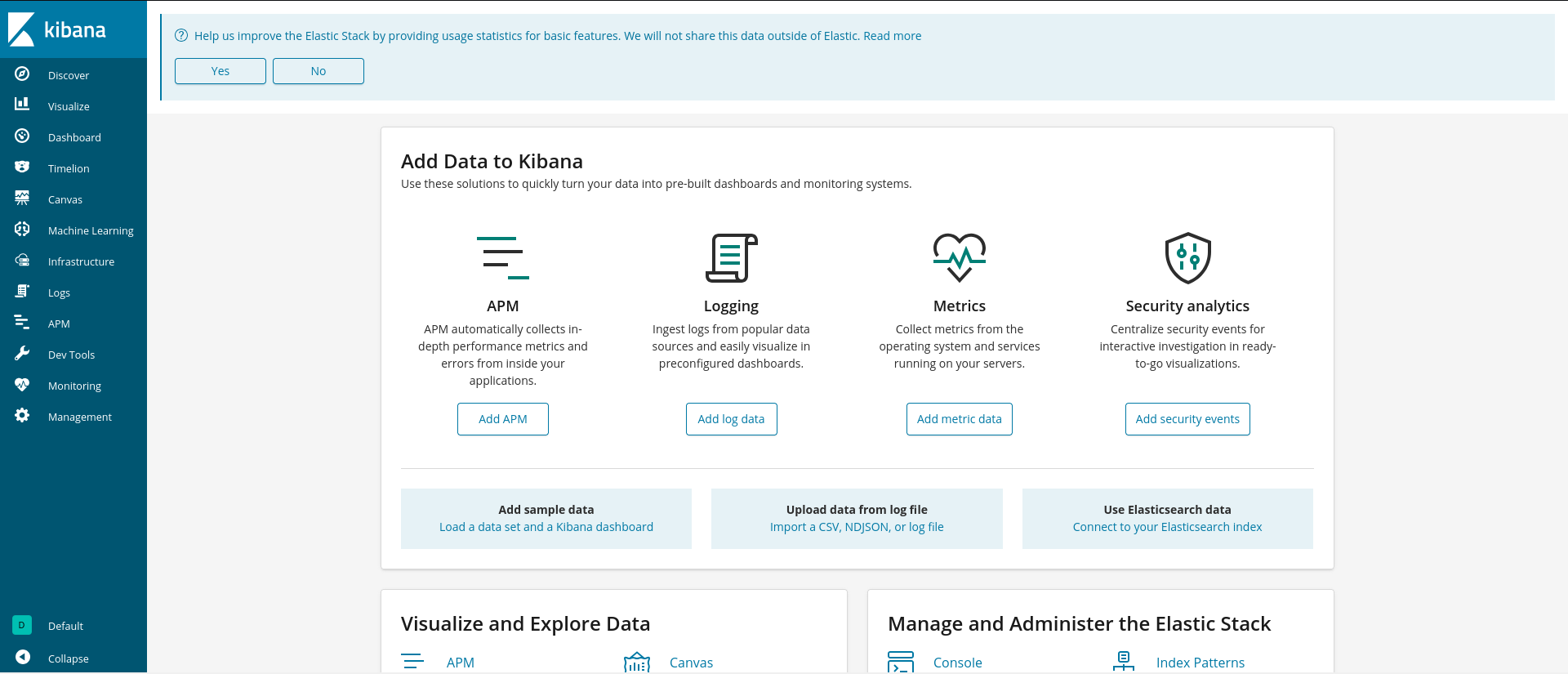
What is the version of visualization dashboard installed in the server?

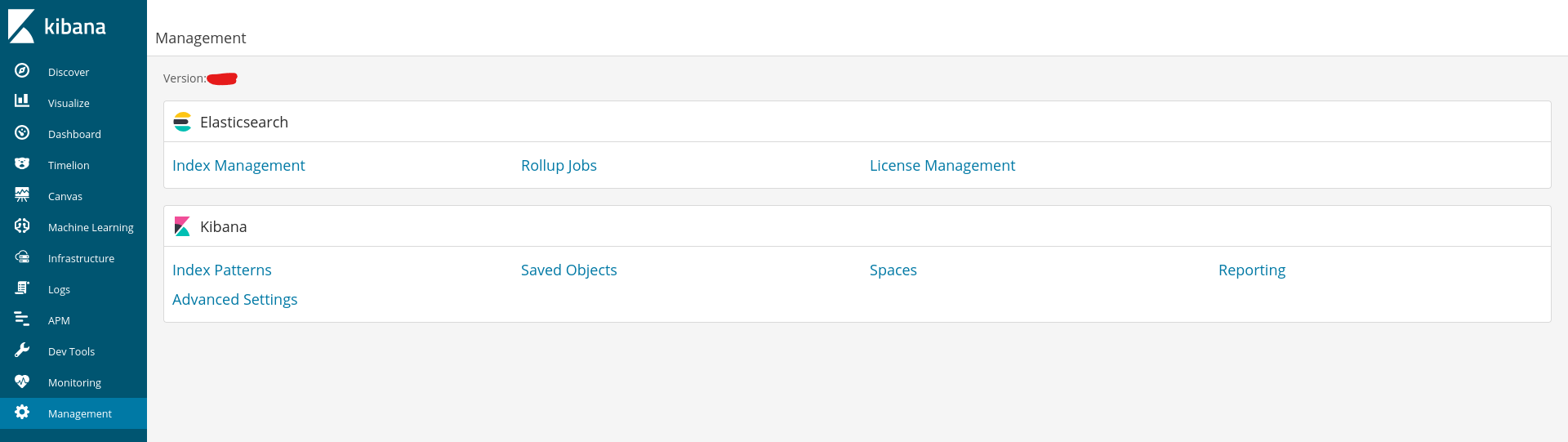
Iniciamos o CTF com nmap: 

Indo na porta 80 temos:



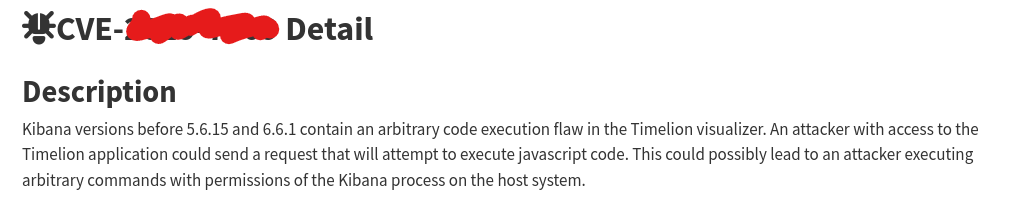
Não aparenta ter nada importante, vamos então à porta 5601 que é diferente das portas que geralmente são usadas:



Parece que somos levados à página de um server, indo na aba Management, encontramos a versão escrita do servidor: 

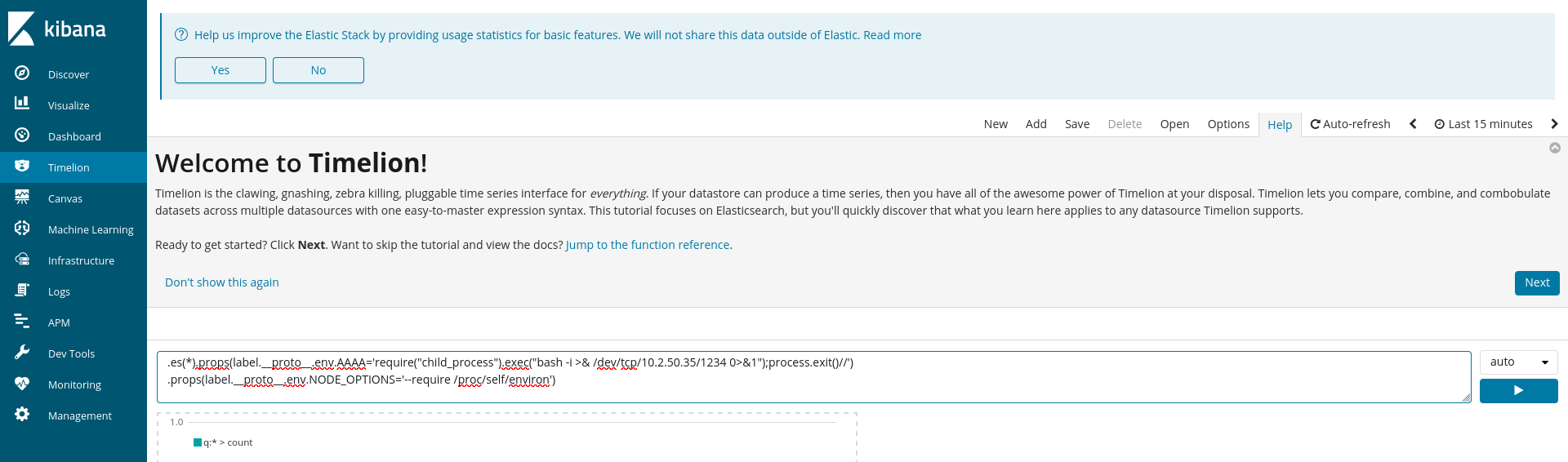
What is the CVE number for this vulnerability?

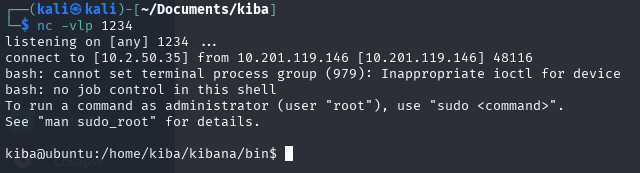
Fazendo uma busca no google por “kibana version 6.5.4 vulnerability”, encontramos uma vunerabilidade que foi corrigida apenas na versão 6.6.1:



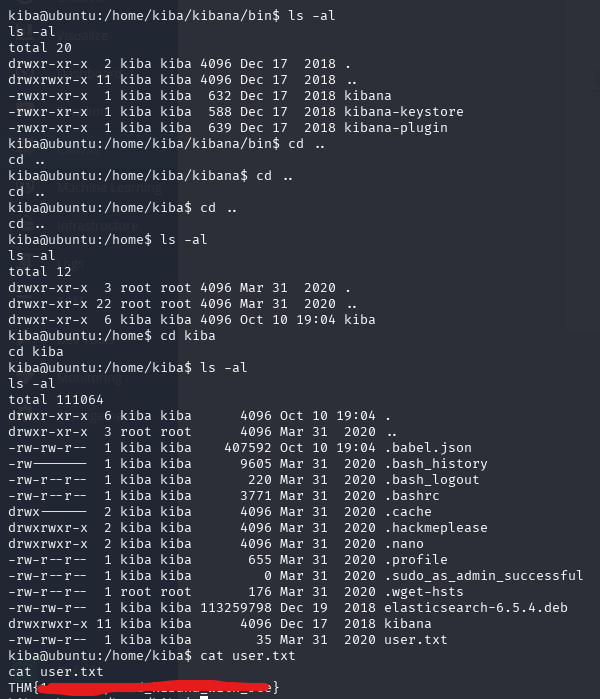
Compromise the machine and locate user.txt

Indo até a aba Timelion e colocando o comando da vulnerabilidade encontrada e rodando o comando “nc” para escutar uma porta:



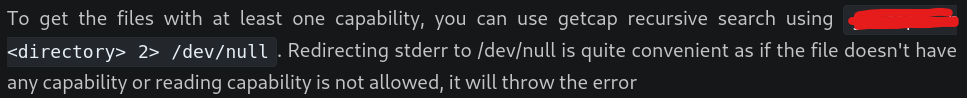


Conseguimos acesso ao servidor, buscando a flag temos:

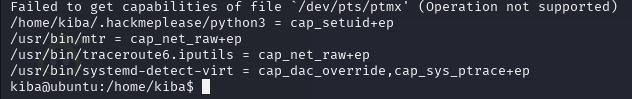


How would you recursively list all of these capabilities?

Fazendo uma busca no google, encontramos um site que explica sobre “Linux Capabilities Exploits”, nele obtemos a resposta:

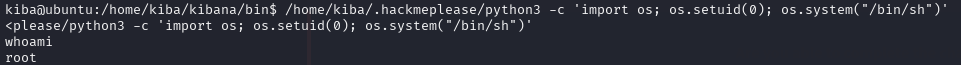


Escalate privileges and obtain root.txt

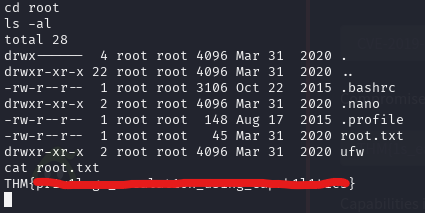
Rodando o comando para listar as capabilties: 

A linha .hackmeplease parece interessante, vamos nos aprofundar mais nela. Buscando possíveis exploits no GTFObins, um deles parece ser aplicável: 

Rodando o comando, conseguimos acesso root:



Agora resta apenas encontrar a flag:



Conclusão

Este CTF leva a pessoa a saber sobre Kibana e uma de suas vulnerabilidades, além de um pouco de capabilities. É uma boa porta de entrada para esses conteúdos, já que com apenas buscas simples no google consegue-se encontrar facilmente conteúdos relevantes, além de não se aprofundar muito nos temas.

Referências

<https://chatgpt.com/>

<https://nvd.nist.gov/vuln/detail/cve-2019-7609>

<https://github.com/mpgn/CVE-2019-7609>

<https://tbhaxor.com/exploiting-linux-capabilities-part-1/>

[https://gtfobins.github.io/gtfobins/python/#capabilities](https://gtfobins.github.io/gtfobins/python/%23capabilities)