Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Mr Rbobot CTF– Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 18/08/2024 |
| **Link** | https://tryhackme.com/r/room/mrrobot |

|  |  |  |
| --- | --- | --- |
| **Redação** | EIke G. Barbosa | Estudante |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 18/08/2024 | Produção |
| **1** | 18/08/2024 | Revisão |
| **2** | 18/08/2024 | Aprovação |

**Sumário**

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

[Desenvolvimento 3](#_heading=h.30j0zll)

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

[What is key 1? 3](#_heading=h.3znysh7)

[What is key 2? 3](#_heading=h.2et92p0)

[What is key 3? 3](#_heading=h.tyjcwt)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

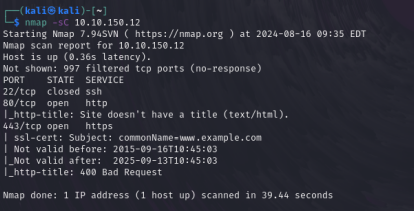
Neste CTF se encontra escaneamento de portas e serviços, enumeração de diretórios, escalonamento de privilégios e exploração web.

**Desenvolvimento**

**What is key1?**

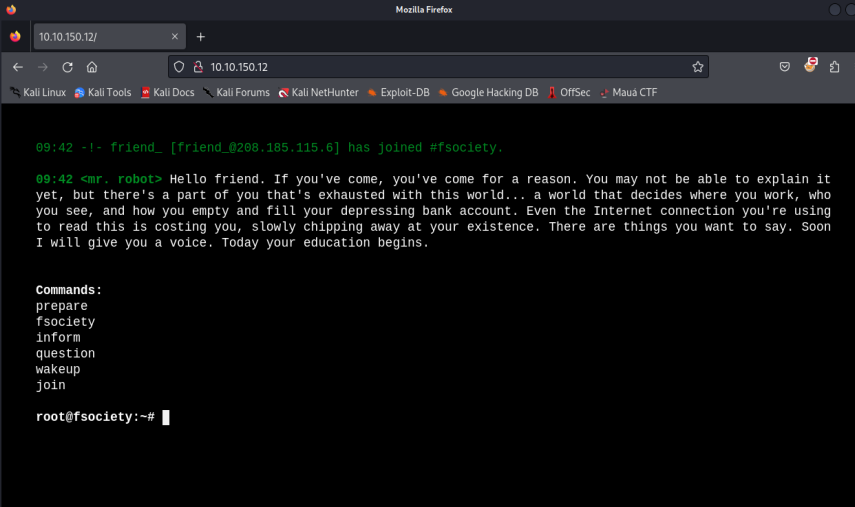
Começamos usando o nmap, para listar as portas que há no servidor.

Comando usado: ***nmap –sC <target IP>***.



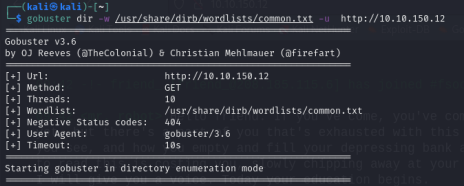
Descobrimos as portas 22, 80 e 443 abertas, que estão rodando os serviços HTTP, SSH e HTTPS.

Acessando o site, ele nos da diversos comandos para serem usados. Informando diversas coisas sobre a iniciativa da “fsoceity”, porém, nada muito importante.



Agora, utilizaremos o programa GOBUSTER, para poder listar os diversos diretórios que há no site.

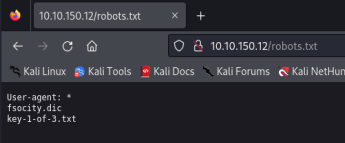
Comando usado: ***gobuster dir –w /usr/share/dirb/wordlists/common.txt –u*** ***http://<target IP>.***



Até acharmos o diretório “robots.txt” ou apenas “robots”.



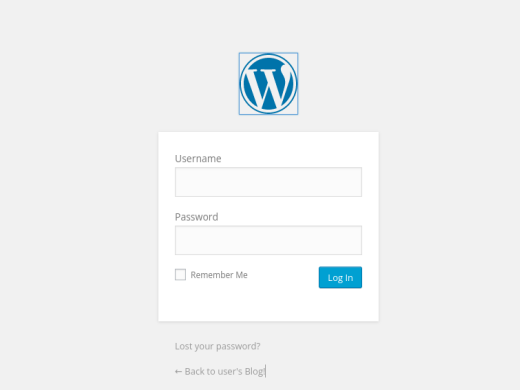
Acessando então o diretório do robots.txt, acharemos a 1º flag e também um arquivo chamado fsocity.dic.



**What is key 2?**

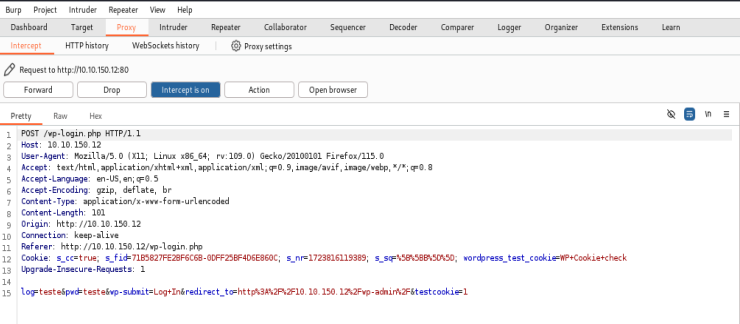
Baixando esse arquivo, poderemos obter uma wordlist.

Entrando no diretório “wp-login.php” podemos ver que há uma página de login de um wordpress. Com a wordlist encontrada, poderemos realizar um ataque de força bruta utilizando o Hydra.



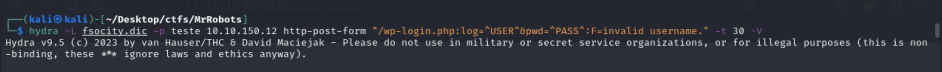
Para utilizarmos o Hydra, precisamos de diversos parâmetros de login.

Abrindo o BurpSuite para coletar essas informações que são necessárias para a realização do Brute force



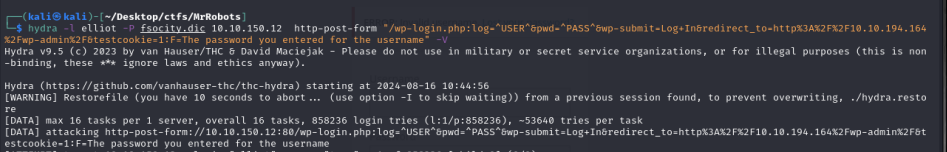
Então agora poderemos utilizar o Hydra.

Comando usado: ***hydra –L fsocity.dic –p teste <target IP> http-post-form “/wp-login.php:log=^USER^&pwd=^PASS^:F=invalid username.” –V.***



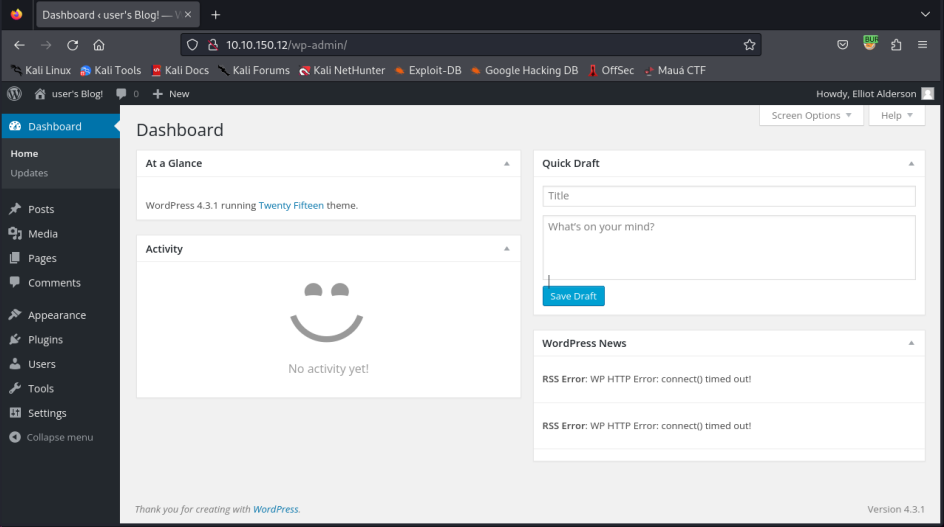


Assim descobrimos que o usuário é o “Elliot”. Agora para acharmos a senha, é o mesmo caminho.

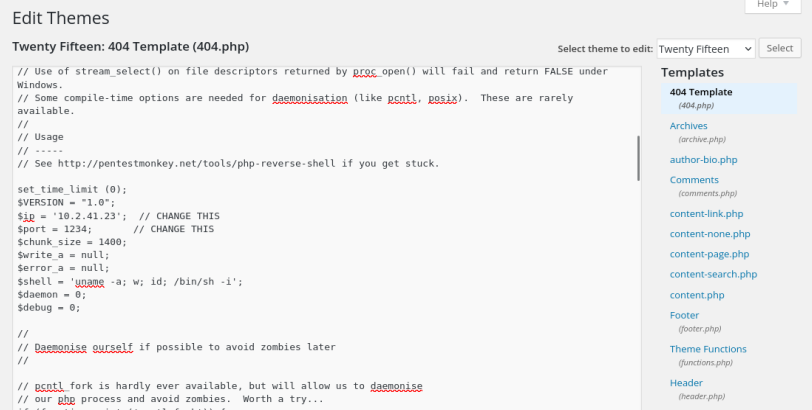




Então assim conseguimos acessar a página wordpress.



Agora, entrando em “Appearance” depois “Editor” e acessando na direita o template “404.php” podemos ter acesso ao código. Pegando alguma reverse shell que temos no nosso sistema ou <https://pentestmonkey.net/> podemos colar a reverse shell dentro do código, mudando o IP <Machine IP> e a Porta que você vai utilizar, no meu caso utilizei a porta 1234.



Salve o arquivo e então utilizando o programa NetCat, abriremos uma porta em nosso host local com a porta 1234.

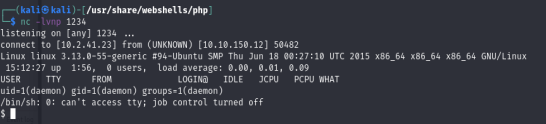
Comando usado: ***nc –lvnp 1234.***



E acessando o link:

***http://<target IP>/wp-content/themes/twentyfifteen/404.php***

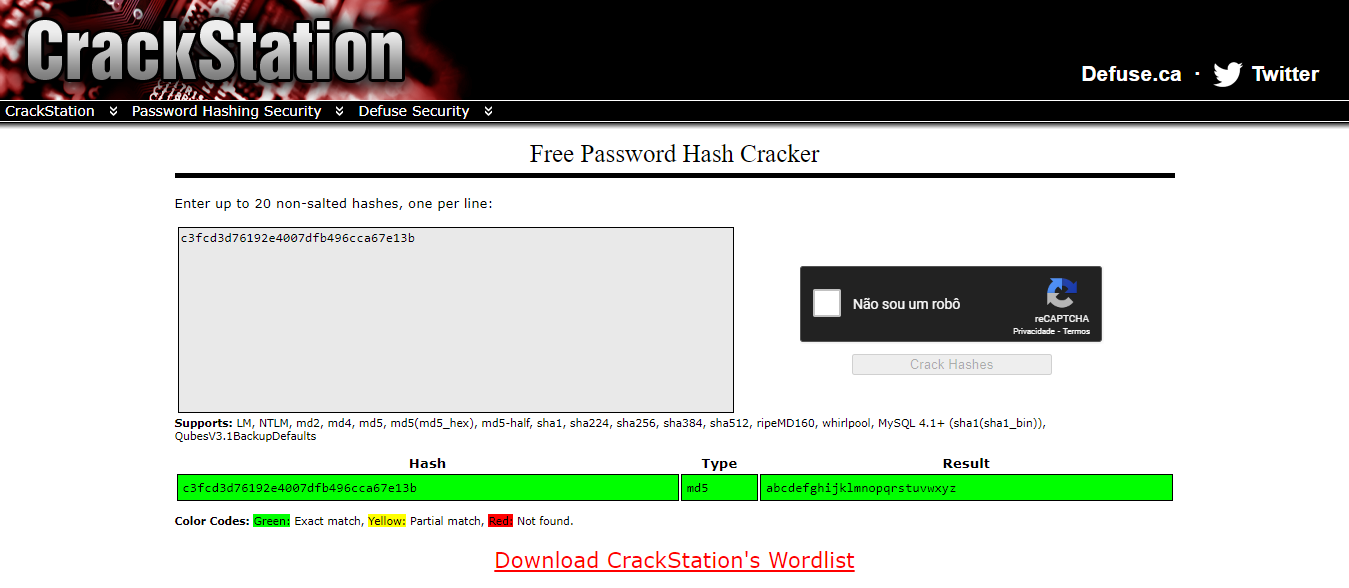
Conseguimos acessar a shell.



Dando uma olhada nos diretórios, podemos acessar /home/robot aonde há 2 arquivos, o primeiro que aparenta ter a segunda flag: key-2-of-3.txt, porém não conseguimos acessar este, pois precisamos de uma senha. E o segundo, que é: password.raw.md5.

robot: c3fcd3d76192e4007dfb496cca67e13b

Pegando essa hash, entramos no site da <https://crackstation.net/> e jogamos ela lá.



Então agora temos a senha do robot (abcdefghijklmnopqrstuvwxyz).



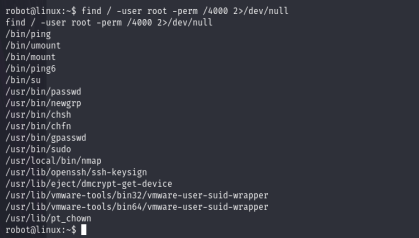
Assim agora conseguindo pegar a 2º flag

**What is key 3?**

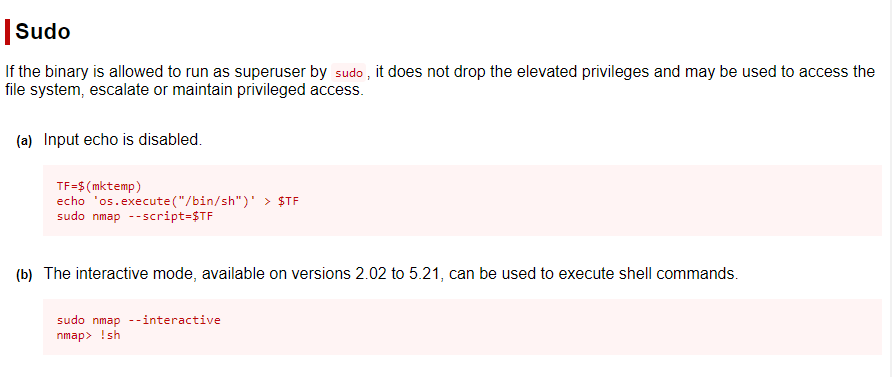
*Escalação de privilégio*

Fazendo uma busca por arquivos que tem permissão SUID, para que eu consiga utilizar em root mesmo com o meu usuário atual.

Comando usado: ***find / -user root -perm /4000 2>/dev/null***



Então vemos que podemos utilizar o nmap par a escalação de privilégio. Utilizando o site <https://gtfobins.github.io/> pesquisamos o nmap.



Utilizando a alternativa **b)** , podemos então ter acesso ao root.



Agora, podemos então entrar no diretório /root e pegar a 3º flag.

**Conclusão**

O CTF do Mr Robot é adequado para iniciantes a intermediários, pois trata de conceitos básicos, mas inclui alguns desafios um pouco mais avançados que precisam um pouco de prática.

**Referências**

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

<https://crackstation.net/>

<https://pentestmonkey.net/>