Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Bountyhacker – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | boutnyhacker– Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 15/10/2024 |
| **Link** | https://tryhackme.com/r/room/cowboyhacker |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 15/10/2024 | Produção |
| **1** | 22/10/2024 | Revisão |
| **2** | DD/MM/AAAA | Aprovação |
| **3** | 04/11/2024 | 2° Revisão |

**Sumário**

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

[Subtítulo caso necessário 3](#_heading=h.30j0zll)

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

[Find open ports on the machine 3](#_heading=h.3znysh7)

[Who wrote the task list?](#_heading=h.2et92p0) 5

[What service can you bruteforce with the text file found?](#_heading=h.tyjcwt) 6

What is the user Password? 6

[user.txt](#_heading=h.3dy6vkm) 6

root.txt 7

[Conclusão](#_heading=h.1t3h5sf) 7

[Referências](#_heading=h.4d34og8) 7

**Contextualização**

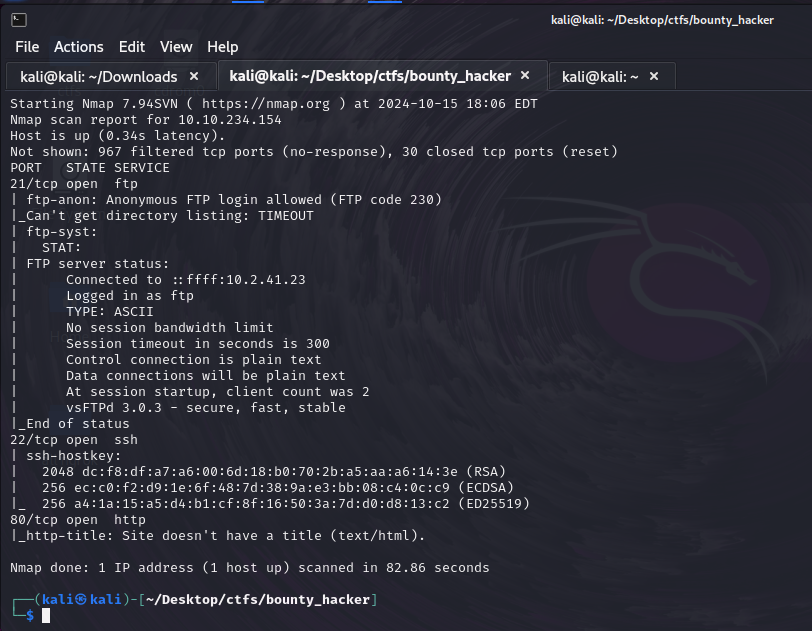
Este CTF foi feito em inspiração do anime/mangá Cowboy Bebop. O percurso começa com port scanning, usando ferramentas como Nmap para mapear a rede e identificar serviços e portas abertas na máquina-alvo. A exploração pode incluir **SQL Injection (SQLi)** para manipular consultas de banco de dados e obter informações sensíveis. Em seguida, os jogadores enfrentam a **escalada de privilégios (Privilege Escalation)**, aproveitando **cronjobs** mal configurados ou explorando binários SUID para obter acesso elevado.

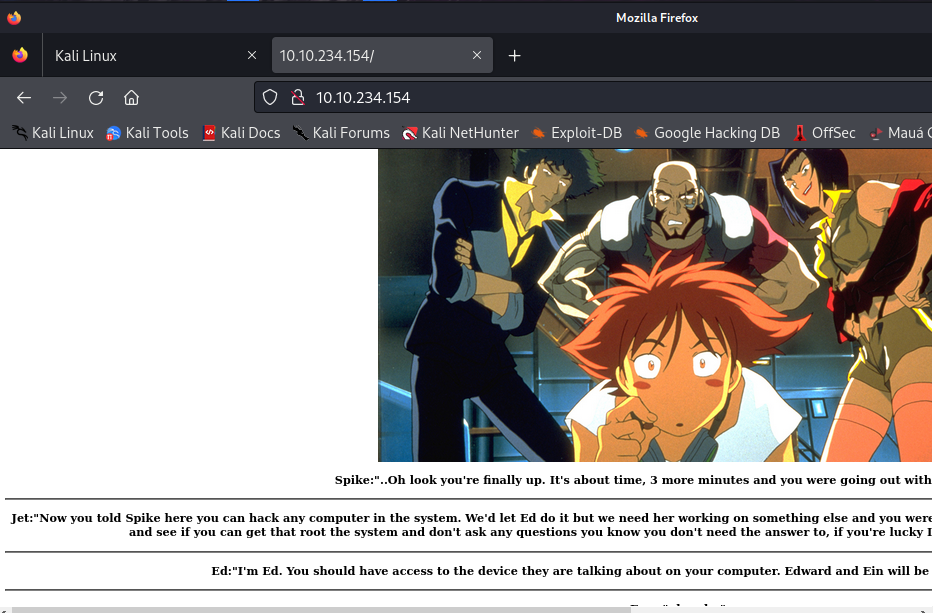
**Desenvolvimento**

**Find open ports on the machine**

Para começar é preciso usar o NMAP, para listar as portas que há na máquina.

***Comando usado***: sudo nmap –sS –sC <ip\_target>

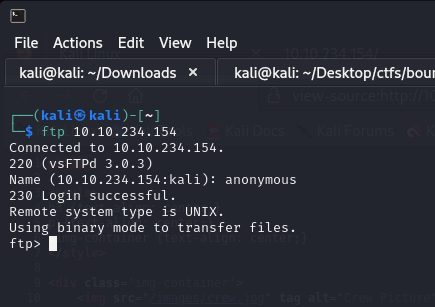
 Há 3 portas abertas, a porta 21 que é direcionada para o serviço FTP, a porta 80 para o serviço HTTP, e a porta 22 para o serviço de SSH. Então o ideal é começar pela porta 80.

****

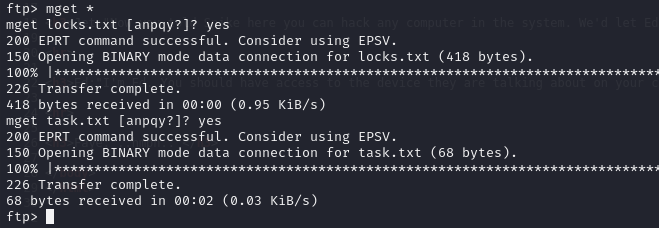
Após analisar, é possível ver que não há nada de informação útil nem nada que vá ajudar, nem mesmo no código fonte da página.

Agora, o foco será para o serviço FTP, na porta 21. No resultado do NMAP da para perceber que é possível acessa-lo com a falha do anonymous.

***Comando usado***: ftp <ip\_target>

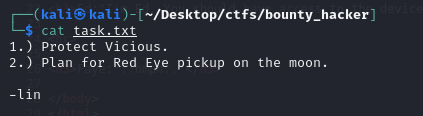
****

No FTP, é possível ver que há dois arquivos txt, agora, o ideal é baixar ambos.

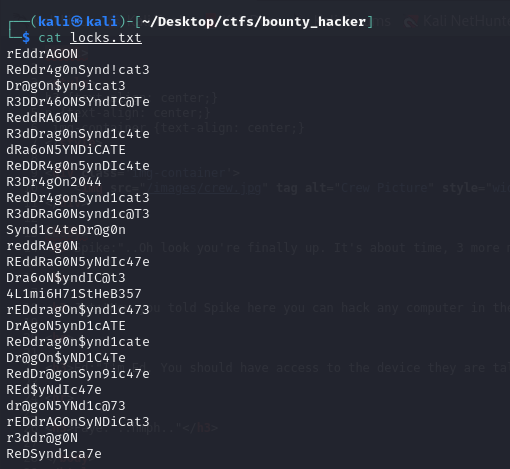
****

**Who wrote the task list?** Parte superior do formulário

Abra o arquivo “task.txt”, nele há o nome “lin”, ele será bem útil no futuro.

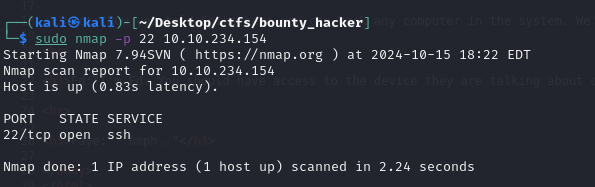


E no outro arquivo há uma wordlist que provavelmente é de senhas que também irá ser útil.

.

**What service can you bruteforce with the text file found?**

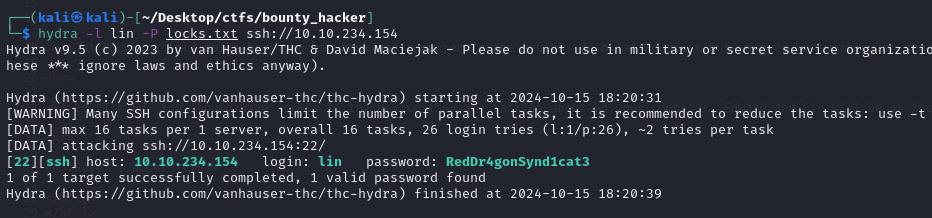
Foco agora será no serviço ssh, aonde um bruteforce será realizado.



**What is the users password?**

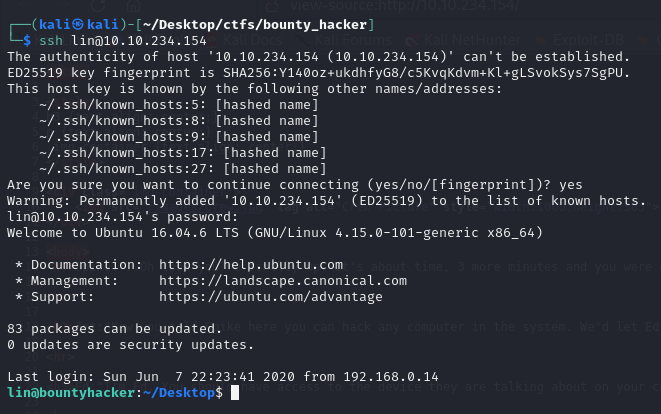
Com o hydra, o será possível realizar o bruteforce, com as informações dos dois arquivos.

***Comando usado***: hydra -l lin -P locks.txt ssh://<ip\_target>



**user.txt**

Adentrando o ssh, o acesso está liberado, agora, só vasculhar os arquivos, de diretório por diretório, mas por sorte, já está no diretório atual

****

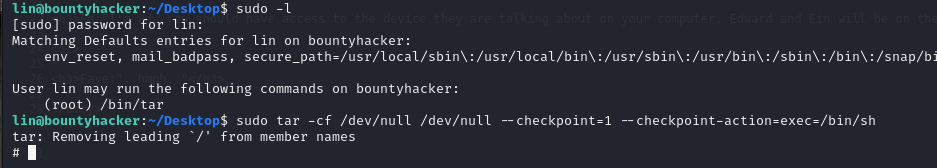
****

**root.txt**

Com o comando sudo –l é possível ver qual comando em sudo o usuário “lin” pode utilizar, e já fazer a busca no GTFobins para achar algum código que consiga entregar o maior privilégio. Após isso, entrar no diretório root com facilidade. Assim, finalizando o CTF.

***Comando usado:*** sudo -l

***Comando usado:*** sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

****

**Conclusão**

O Bounty Hacker é bom para ter uma noção básica de privilege escalation, algumas falhas tranquilas como anon login e bruteforce, que é muito útil. Com um tema muito interessante

.

**Referências**

https://gtfobins.github.io/