Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Boiler CTF – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Boiler – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 16/08/2024 |
| **Link** | https://tryhackme.com/r/room/boilerctf2 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Sérgio Guidi Trovo | Estudante |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 16/08/2024 | Produção |
| **1** | 16/08/2024 | Revisão |
| **2** | 16/08/2024 | Aprovação |

**Sumário**

[Contextualização 3](#_Toc174353000)

[Desenvolvimento 3](#_Toc174353001)

[Pergunta 1 - File extension after anon login 3](#_Toc174353002)

[Pergunta 2 - What is on the highest port? 5](#_Toc174353003)

[Pergunta 3 - What's running on port 10000? 5](#_Toc174353004)

[Pergunta 4 - Can you exploit the service running on that port? 5](#_Toc174353005)

[Pergunta 5 - What's CMS can you access? 6](#_Toc174353006)

[Pergunta 6 - Keep enumerating, you'll know when you find it. 6](#_Toc174353007)

[Pergunta 7 - The interesting file name in the folder? 9](#_Toc174353008)

[Pergunta 8 - Where was the other users pass stored (no extension, just the name)? 9](#_Toc174353009)

[Pergunta 9 - user.txt 11](#_Toc174353010)

[Pergunta 10 - What did you exploit to get the privileged user? 12](#_Toc174353011)

[Pergunta 11 - root.txt 13](#_Toc174353012)

[Conclusão 13](#_Toc174353013)

[Referências 13](#_Toc174353014)

Contextualização

O Boiler CTF foi um CTF introduzido ao longo da capacitação para a entidade. Trata-se de um CTF de dificuldade intermediária.

Desenvolvimento

Pergunta 1 - File extension after anon login

Primeiramente foi realizado um *PortScanning* agressivocom o comando *nmap -A*:

Texto

Descrição gerada automaticamente

Foram encontradas três portas abertas com os serviços *ftp* e *http*.

Utilizando o login FTP anônimo e verificando os diretórios e files:

Texto

Descrição gerada automaticamente

Verificou-se que a extensão da file é *.txt*.

Pergunta 2 - What is on the highest port?

Fazendo nmap de todas as portas:

Texto

Descrição gerada automaticamente

Verificando a porta 55007 encontrada:

Texto

Descrição gerada automaticamente

Verifica-se que o serviço rodando na maior porta é ssh.

Pergunta 3 - What's running on port 10000?

Como visto no primeiro *nmap* a porta 10000 está rodando *webmin httpd*.

Pergunta 4 - Can you exploit the service running on that port?

Não é possível exploit o serviço da porta 10000.

Pergunta 5 - What's CMS can you access?

Enumerando as páginas do serviço web com o comando *gobuster*:

Texto

Descrição gerada automaticamente

Foi encontrado o CMS *joomla*.

Pergunta 6 - Keep enumerating, you'll know when you find it.

Continuando a enumeração a partir do diretório joomla:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Verificando os diretórios foi encontrado algo diferente em */­­\_test*:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Pesquisando sobre *sar2html*:

Texto, Carta

Descrição gerada automaticamente

Utilizando o comando encontrado para listar os diretórios:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Pergunta 7 - The interesting file name in the folder?

Como visto a file tem nome *log.txt*.

Pergunta 8 - Where was the other users pass stored (no extension, just the name)?

Utilizando o comando *cat* para verificar o conteúdo da file *log.txt*:



Interface gráfica do usuário, Texto, Aplicativo, Word

Descrição gerada automaticamente

Encontrado o usuário *basterd* com a pass *superduperp@$$*.

Utilizando a conexão ssh na porta encontrada anteriormente com as credenciais encontradas:

Texto

Descrição gerada automaticamente

Verificando e acessando os diretórios presentes:

Texto

Descrição gerada automaticamente

Encontrado outro usuário chamado *stoner* com senha *superduperp@$$no1knows* na file backup.sh.

Pergunta 9 - user.txt

Acessando o servidor com o novo usuário:

Texto

Descrição gerada automaticamente

Verificando os diretórios e files:

Texto

Descrição gerada automaticamente

Acessando a file .secret:



Pergunta 10 - What did you exploit to get the privileged user?

Verificando os comandos executáveis com SUDO:

Texto

Descrição gerada automaticamente

Verificando os comandos executáveis com SUID:





Utilizando o comando *find* para alterar as permissões do diretório root:



Pergunta 11 - root.txt

Acessando a file root.txt:

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

Conclusão

Por meio da realização do Boiler CTF foi possível aplicar muitos conceitos aprendidos na capacitação para a entidade. Esse CTF passa pelas três etapas do *pentesting* e possuí diversos *rabbit holes* que dificultam a sua execução.

Referências

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

<https://www.exploit-db.com/exploits/47204>

<https://book.hacktricks.xyz/>