Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

NetSecChallenge – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | NetSecChallenge – Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 13/11/2024 |
| **Link** | https://tryhackme.com/r/room/netsecchallenge |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 05/11/2024 | Produção |
| **1** | 13/11/2024 | Revisão |
| **2** | 13/11/2024 | Aprovação |

**Sumário**

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

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

[What is the highest port number being open less than 10,000? 3](#_heading=h.3znysh7)

[There is an open port outside the common 1000 ports; it is above 10,000. What is it? 3](#_heading=h.2et92p0)

[How many TCP ports are open? 3](#_heading=h.tyjcwt)

[What is the flag hidden in the HTTP server header?](#_heading=h.3dy6vkm) 4

What is the flag hidden in the SSH server header? 4

We have an FTP server listening on a nonstandard port. What is the version of the FTP server? 4

We learned two usernames using social engineering: **eddie** and **quinn**. What is the flag hidden in one of these two account files and accessible via FTP?Parte superior do formulário

5

Browsing to **http://10.10.243.195:8080** displays a small challenge that will give you a flag once you solve it. What is the flag? 5

[Conclusão 3](#_heading=h.1t3h5sf)

**Contextualização**

Neste desafio da plataforma TryHackMe, é possível aplicar as habilidades adquiridas no módulo de Segurança de Redes da trilha *Jr Penetration Tester*. Todas as perguntas deste desafio podem ser resolvidas usando apenas as ferramentas *NMAP*, *TELNET* e *HYDRA*.

**Desenvolvimento**

**What is the highest port number being open less than 10,000?**

Para começar, verificamos o endereço de ip da máquina e utilizamos o comando *nmap* com alguns parâmetros.

***Comando usado:*** nmap -sC -sV -p- -T4 --min-rate=9326 <ip\_machine>

**-sC**: executa scripts específicos no alvo e verifica tudo o que pode ocorrer lá

**-sV**: verifica as versões

**-p-**: verifica todas as portas

**-T4**: serve para acelerar o processo (o máximo é T5)

**-vv**: modo verbose

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

***Resposta:*** 8080

**There is an open port outside the common 1000 ports; it is above 10,000. What is it?**

Com o mesmo comando da pergunta anterior, podemos descobrir esta porta.



***Resposta:*** 10021

**How many TCP ports are open?**

Analisando um pouco mais o resultado do *nmap*, encontram-se diversas portas tcp, sendo elas porta 80, 22, 139, 445, 8080 e 10021

***Resposta:*** 6

**What is the flag hidden in the HTTP server header?**

Acessando a porta 80, temos uma flag escondida.

Texto

Descrição gerada automaticamente

***Resposta:*** THM{web\_server\_25352}

**What is the flag hidden in the SSH server header?**

Analisando a porta 22:

Texto

Descrição gerada automaticamente

***Resposta:*** THM{946219583339}

**We have an FTP server listening on a nonstandard port. What is the version of the FTP server?**

Agora na porta 10021, podemos procurar pelo versionamento.

Texto

Descrição gerada automaticamente

***Resposta:*** vsftpd 3.0.5

**We learned two usernames using social engineering: eddie and quinn. What is the flag hidden in one of these two account files and accessible via FTP?**

O Tryhackme criou um cenário onde já possuímos os nomes dos nossos alvos, então vamos usar o *Hydra* para realizar um *bruteforce* no serviço ftp. Crie um arquivo .txt e coloque o nome de ambos os usuários fornecidos.

***Comando usado:*** hydra -L nomes.txt -P /usr/share/wordlists/rockyou.txt <ftp://10.10.243.195:10021>

***Interface gráfica do usuário, Texto

Descrição gerada automaticamente***

Agora basta acessar o ftp, baixar o arquivo e abri-lo.

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

***Resposta:*** THM{321452667098}

**Browsing to http://<IP\_Machine:8080 displays a small challenge that will give you a flag once you solve it. What is the flag?**

Acessando a URL, percebemos que o site serve para testar se o seu scan vai ser detectado pelo sistema. Haverá um botão, aperte ele e então volte para o terminal e execute o comando *nmap*.

***Comando usado:*** nmap -sN

**Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente**

***Resposta:*** THM{f7443f99}

**Parte superior do formulário**

**Conclusão**

O desafio é muito simples de ser realizado, apesar de ser apresentado como nível de dificuldade intermediário na plataforma Tryhackme. Com apenas um scan do servidor é possível responder grande parte das perguntas.