Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Cyborg – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Cyborg – Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 14/08/2024 |
| **Link** | https://tryhackme.com/r/room/cyborgt8 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico Santarelli | Membro |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 14/08/2024 | Produção |
| **1** | 14/08/2024 | Revisão |
| **2** | 14/08/2024 | Aprovação |

**Sumário**

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

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

[Scan the machine, how many ports are open? 3](#_heading=h.3znysh7)

[What service is running on port 22? 3](#_heading=h.2et92p0)

[What service is running on port 80? 3](#_heading=h.tyjcwt)

[What is the user.txt flag? 3](#_heading=h.3dy6vkm)

[What is the root.txt flag? 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

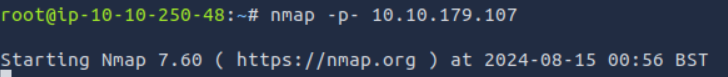
**Contextualização**

A sala aborda os conceitos de escaneamento de portas e serviços, enumeração de diretórios, exploração web, entendimento de logs, criptografia, exploração do BorgBackup (programa de backups), leitura de programas e escalonamento de privilégios.

**Desenvolvimento**

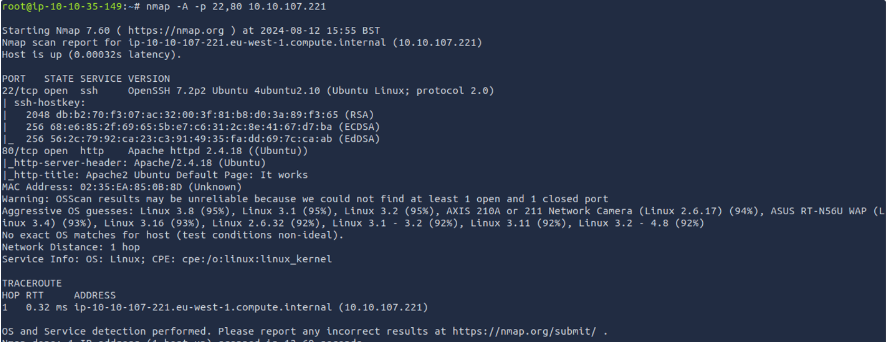
**Scan the machine, how many ports are open?**

Primeiramente, vamos realizar um Port Scanning usando Nmap com a tag -p- para verificar todas as portas possíveis.



**What service is running on port 22?**

Agora, vamos executar um Port Scanning buscando mais informações. Para isso, vamos usar o Nmap com a flag -A, responsável por verificar versões, serviços, sistema operacional e executa scripts.



**What service is running on port 80?**

Para essa questão utilizamos o mesmo escaneamento da pergunta anterior.

**What is the user.txt flag?**

O próximo passo é realizar a enumeração dos diretórios do servidor web procurando por arquivos html e php.

Texto

Descrição gerada automaticamente

Os resultados mostram dois diretórios interessantes: /admin e /etc.

No diretório de admin há um website relacionado com músicas.

Interface gráfica do usuário, Site

Descrição gerada automaticamente

No diretório /etc há uma pasta squid com dois arquivos: “passwd” e “squid.conf”.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

**Texto

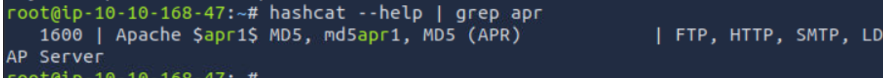
Descrição gerada automaticamente**

O arquivo de passwd mostra uma possível senha criptografada. Utilizando o site hashes podemos identificar o algoritmo utilizado no texto, nesse caso Apache $apr1$ MD5. Ref: <https://hashes.com/en/tools/hash_identifier>

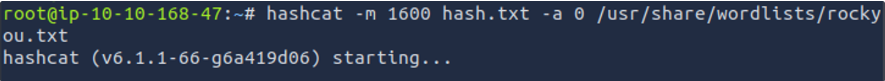
Padrão do plano de fundo

Descrição gerada automaticamente

Na sequência podemos utilizar o hashcat para descriptografar o hash. Primeiro, então vamos buscar o número que identifica o algoritmo no hashcat.

****

Logo, descobrimos a senha com o hashcat utilizando a wordlist Rockyou que é “squidward”.

****

**Texto

Descrição gerada automaticamente**

Para dar continuidade devemos explorar as abas da página web. Na aba “Archive” podemos baixar uma pasta.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Explorando a pasta temos diversos arquivos. Mais especificamente, no arquivo README há informação de que a pasta utiliza o backup Borg. Ref: <https://borgbackup.readthedocs.io/en/stable/quickstart.html#restoring-a-backup>

Texto

Descrição gerada automaticamente

Na documentação há uma parte de extração de informações, para isso é necessária uma senha, que já foi encontrada anteriormente. Ao extrair nos deparamos com o diretório do usuário alex.

Texto

Descrição gerada automaticamente

Nos documentos do usuário há um arquivo .txt com a senha do usuário em questão.

Texto

Descrição gerada automaticamente

Usando SSH podemos nos conectar ao alvo com o usuário e senha encontrados.

Texto

Descrição gerada automaticamente

No diretório do usuário há a flag procurada do usuário.

Tela de celular com letras

Descrição gerada automaticamente

**What is the root.txt flag?**

Procurando os possíveis comandos que o usuário pode usar sudo temos um arquivo .sh.

Texto

Descrição gerada automaticamente

Analisando o arquivo temos um código que faz backups de arquivos, mas também executa na shell o comando adicionado na flag -c

Texto

Descrição gerada automaticamente

**Interface gráfica do usuário, Texto

Descrição gerada automaticamente**

Diante disso, podemos executar qualquer comando como root ao executar o arquivo como sudo.

Texto

Descrição gerada automaticamente

**Conclusão**

Este CTF possui um nível fácil para intermediário, já que aborda conceitos iniciais, porém com algumas sacadas um pouco mais complexas.

Eu indicaria essa sala para aqueles que desejam consolidar e botar em prática conceitos primários.

**Referências**

* <https://borgbackup.readthedocs.io/en/stable/quickstart.html#restoring-a-backup>
* <https://hashes.com/en/tools/hash_identifier>