Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Startup – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Startup – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 07/11/2024 |
| **Link** | https://tryhackme.com/r/room/startup |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/11/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 3](#_Toc179216044)

[Desenvolvimento 3](#_Toc179216045)

[User flag: 3](#_Toc179216046)

[Root flag: 5](#_Toc179216047)

[Conclusão 6](#_Toc179216048)

[Referências 6](#_Toc179216049)

Contextualização

O Startup CTF é divertido de resolver e aborda temas variados. Como por exemplo, *Port Scanning*, enumeração de diretórios e arquivos, *Reverse Shell*, vulnerabilidades e escalonamento de privilégios.

Desenvolvimento

What is the secret spicy soup recipe?

Parte superior do formulário

Inicie usando o **Nmap** para fazer um *Port Scanning* na máquina com o parâmetro *Agressive* (-A):

Texto

Descrição gerada automaticamente

O **Nmap** indica que há 3 portas abertas, a porta 21 (FTP), a 22 (SSH para conexão remota) e a porta 80 (HTTP). Além disso, o resultado indica que a conexão FTP pode ser feita usando o usuário ‘anonymous’ sem a exigir uma senha para autenticação.

Consultando a página HTTP não aparenta ter nenhuma informação importante:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Continue a enumeração conectando-se a porta FTP para checar os arquivos da máquina alvo:

Texto

Descrição gerada automaticamente

Entre os diretórios FTP, é possível notar uma pasta que há permissão para todos os privilégios Linux, como executar, ler e escrever arquivos.

Usando a ferramenta **Gobuster** para enumerar os diretórios web, descobre-se um diretório chamado ‘/files’ que tem como destino as mesmas pastas FTP.

Texto

Descrição gerada automaticamente

Com isso, é possível fazer um upload de um arquivo PHP de reverse shell e executar esse arquivo no diretório ‘/files/ftp’.

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Para prosseguir, execute o **NetCat** na máquina local para escutar a porta escolhida no arquivo da *Reverse Shell* e então execute o arquivo PHP no site.

Lembre-se de trocar o IP para a máquina local no arquivo PHP.

Uma imagem contendo Texto

Descrição gerada automaticamente

Dessa forma, obtém-se acesso à máquina alvo. Porém, sem a permissão para acessar diretórios de outros usuários.

Texto

Descrição gerada automaticamente com confiança média

Na pasta raiz da máquina, existem alguns arquivos incomuns, entre esses arquivos é possível encontrar a receita secreta:

Uma imagem contendo Texto

Descrição gerada automaticamente

What are the contents of user.txt?

Para encontrar o arquivo ‘user.txt’ será preciso ter acesso ao usuário “lennie” primeiro. Na pasta ‘Documents’ há um recado em relação aos registros de incidentes, uma pasta que está exposto na máquina alvo.

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Para ter acesso a esse arquivo, é interessante iniciar um servidor local python nesse diretório para transferir esse arquivo para a máquina local.

Texto

Descrição gerada automaticamente

Então, abra esse arquivo com a ferramenta **WireShark** para ter acesso aos pacotes de rede registrados. Entre esses pacotes, um deles é responsável por registrar os comandos executados no terminal, e entre esses comandos, um deles expõe a senha do usuário ‘lennie’.

Interface gráfica do usuário, Aplicativo, Tabela

Descrição gerada automaticamente

Interface gráfica do usuário

Descrição gerada automaticamente

Agora, é possível obter acesso a esse usuário, então realize uma conexão SSH com a máquina utilizando as credenciais obtidas, e no diretório ‘/home/lennie’ estará contido o arquivo ‘user.txt’:

Texto

Descrição gerada automaticamente

What are the contents of root.txt?

Ao enumerar os arquivos de lennie, será possível encontrar alguns scripts que executam a partir de um crontab. Texto

Descrição gerada automaticamente

O script ‘planner.sh’ copia o valor da variável ‘LIST’ e cola no arquivo de texto ‘startup\_list’ em seguida executa o script ‘print.sh’, que por sua vez, exibe no terminal o texto “Done!”. Porém, o usuário ‘lennie’ possui acesso para editar, ler e escrever no arquivo ‘print.sh’, que será executado como root.

Então, digite um comando que fará um segundo comando ser copiado para o arquivo ‘print.sh’, o segundo comando irá copiar e ler o arquivo ‘/root/root.txt’ para o diretório ‘/home/lennie’. Dessa forma, será possível visualizar a flag final e finalizar o desafio.

Texto

Descrição gerada automaticamente

Conclusão

Esse CTF pode ser considerado de nível fácil, visto os conhecimentos prévios que ele exige. Porém, o escalonamento de privilégios dele pode ser um pouco desafiador no início. Portanto, pode ser um bom desafio para treinar os conceitos básicos de pentesting e comandos do terminal Linux.

Referências

* <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>
* <https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/full-ttys>
* <https://github.com/pentestmonkey/php-reverse-shell>