10/07/2023 – TryHackMe – RootMe

Link: <https://tryhackme.com/room/rrootme>

1. Realizando portscanning no alvo:

Texto

Descrição gerada automaticamente

**Scan the machine, how many ports are open?: 2**

**What version of Apache is running?: 2.4.29**

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

1. Usando gobuster para fazer directory Discover:

Texto

Descrição gerada automaticamente

**What is the hidden directory?: /panel/**

1. Verificando tal endpoint:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Com a extensão Wappalyzer, identifica-se que está sendo utilizdo php:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Com isso, supõe-se que deve ser realizado um PHP Reverse Shell. Dentro do kali, tem-se o arquivo /usr/share/webshells/php/php-reverse-shell.php. Adaptando ele para o IP e porta escolhidas onde está comentado //CHANGE THIS:

Texto

Descrição gerada automaticamente

1. Abrindo a porta 3333 por meio do Netcat:



1. Fazendo upload do arquivo no endpoint, verifica-se uma restrição por conta da extensão .php:

Interface gráfica do usuário, Site

Descrição gerada automaticamente

1. Como esta restrição é feita pelo Backend da API, não é possível se utilizar do BurpSuite para alterar a requisição. Logo, será alterado a extensão para uma compatível com o .php. como o .php5. Fazendo isso, observa-se que a API aceita o novo arquivo:



Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

Descrição gerada automaticamente

1. Ao clicar em “veja”, o arquivo é executado e verifica-se o sucesso do Reverse Shell:

Texto

Descrição gerada automaticamente

1. Buscando pelo arquivo “user.txt” (como dito no enunciado) com o comando find, encontra-se o seguinte:

Texto

Descrição gerada automaticamente

1. Chegando no diretório do arquivo e verificando-o com o comando cat, tem-se:

Texto

Descrição gerada automaticamente com confiança baixa

Portanto, a primeira flag é: $flag

1. Sabendo que deve-se realizar uma escalação de privilégios, deve-se procurar (como dito no enunciado da próxima questão) um arquivo “estranho”. Ao rodar o seguinte comando, encontra-se o python com permissão SUID:

Texto

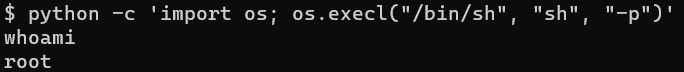
Descrição gerada automaticamente

**Search for files with SUID permission, which file is weird?: /usr/bin/python**

1. Com isso, se utilizando do site <https://gtfobins.github.io/gtfobins/python/>, encontra-se uma maneira de ganhar acesso ao usuário root, rodando o seguinte comando:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente



1. Com isso, é possível acessar o diretório /root e, assim, encontrar a flag:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário

Descrição gerada automaticamente com confiança baixa

Portanto, a última flag é: $flag