10/07/2023 – TryHackMe – Pickle Rick

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

1. Fazendo um Port Scanning no alvo utilizando o nmap:

Texto

Descrição gerada automaticamente

1. Observando o serviço HTTP pelo navegador:

Interface gráfica do usuário, Site

Descrição gerada automaticamente

1. Inspecionando a página:

Interface gráfica do usuário

Descrição gerada automaticamente

1. Com isso, descobriu-se o nome de usuário: R1ckRul3s. Como está rodando um servidor apache, utilizar o gobuster para descobrir os possíveis diretórios:

Texto

Descrição gerada automaticamente

1. Rodando o endpoint /robots.txt:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Portanto, descobriu-se o valor Wubbalubbadubdub. Observando o endpoint /login.php:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Utilizando o usuário e “Wubbalubbadubdub” como senha:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Como tem-se um command panel, verificar a possibilidade de um RCE, utilizando o comando “ls”:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Ao tentar ler o arquivo “Sup3rS3cretPickl3Ingred.txt” com o comando “cat”:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Ao utilizar o comando “less”:

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

Descrição gerada automaticamente

1. Portanto, esta é a primeira flag. Ao ler o arquivo “clue.txt” com o mesmo comando:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Com isso, para acessar mais facilmente o sistema, se utilizará de reverse shell para conectar com o servidor web. Verificando a existência de alguma ferramenta que possibilita isso, como python3:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Com isso, deve-se abrir alguma porta. Utilizando o Netcat para isso:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Pesquisando no site <https://www.revshells.com/> reverse shells usando python3 no ip 10.8.78.57 (dado pelo openvpn do tryhackme) na porta escolhida 3333:

Tela de celular com aplicativo aberto

Descrição gerada automaticamente

1. Ao rodar o comando

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

verifica-se no terminal que a conexão foi estabelecida:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente com confiança média

1. Verificando diretórios anteriores, encontra-se o diretório “/home”. Nele, se encontra o suspeito diretório “/rick”. Entra-se nele:

Texto

Descrição gerada automaticamente

1. Ao verificar o que ele possui com o comando ls:

Texto

Descrição gerada automaticamente

1. Imprimindo o resultado na tela:

Texto

Descrição gerada automaticamente

Com isso, está descoberta a segunda flag.

1. Supondo que deve-se fazer uma escalação de privilégios, observar quais comandos o usuário utilizado pode realizar com “sudo”, pelo seguinte comando:

Texto

Descrição gerada automaticamente

1. Da maneira que está mostrada, qualquer comando pode ser executado com “sudo”, ou seja, a partir dele tem-se privilégios de um usuário “root”. Com isso, é possível acessar o usuário “root”:

Texto

Descrição gerada automaticamente

1. Agora, é possível entrar no diretório “root”:

Texto

Descrição gerada automaticamente

1. Verificando o terceiro ingrediente:

Texto

Descrição gerada automaticamente

Logo, a última flag é $flag