12/09/2023 – TryHackMe – tomghost

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

1. Fazendo port Scanning no alvo:

Texto

Descrição gerada automaticamente

1. Fazendo port Scanning mais específico nas portas encontradas:

Texto

Descrição gerada automaticamente

1. Verificando “Apache Tomcat 9.0.30”, tentará-se encontrar alguma vulnerabilidade nela utilizando o Metasploitable:  
   Texto

   Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Verificando o exploit “4”, por conta do nome do ctf, será utilizado:



Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente

1. Encontrado um usuário “skyfuck:8730281lkjlkjdqlksalks”, utilizá-lo para conectar no serviço ssh:

Texto

Descrição gerada automaticamente

1. Explorando os diretórios



Texto

Descrição gerada automaticamente com confiança média

1. Ao pegar os arquivos “credential.pgp” e “tryhackme.asc”, é possível tentar usar de bruteforce para acessar o conteúdo destes arquivos. Utilizando a ferramenta nativa do kali chamada *gpg2john:*

Texto

Descrição gerada automaticamente

1. Usando a ferramenta *john*  para fazer o ataque de força bruta, tem-se:

Texto

Descrição gerada automaticamente

1. Abrindo o arquivo *credentials.pgp*, sabendo da chave encontrada:

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Tendo a senha, agora deve ser realizado a troca de usuário:



1. Verificando permissões “sudo”:

Texto

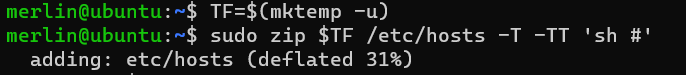
Descrição gerada automaticamente

1. Verificando possibilidades do binário “zip” no site <https://gtfobins.github.io/gtfobins/zip/#sudo> :

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Executando os comandos passados:



Texto

Descrição gerada automaticamente

1. Lendo o arquivo buscado:

Uma imagem contendo Texto

Descrição gerada automaticamente