10/07/2023 – TryHackMe – Boiler CTF

Link: <https://tryhackme.com/room/boilerctf2>

1. Fazendo Port Scanning com nmap:

Texto

Descrição gerada automaticamente

1. Identificou-se que na porta 21 o perfil anonymous está liberado. Portanto, logar com este perfil

Texto

Descrição gerada automaticamente

1. Verificando o arquivo escondido “.info.txt” e, para isso, baixando o arquivo na máquina:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Verificando o tipo de criptografia: <https://www.dcode.fr/cipher-identifier>

Interface gráfica do usuário

Descrição gerada automaticamente com confiança média

1. Descriptografando por meio do <https://www.dcode.fr/rot-13-cipher>:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Dica: fazer enumeração de privilégios. Usando o gobuster para encontrar diretórios na porta 80. Sabendo que é um Apache, será usado uma wordlist com as extensões .php, .txt e .html:

Texto

Descrição gerada automaticamente

1. Verificando o /joomla, identifica-se uma página da aplicação web:

Interface gráfica do usuário

Descrição gerada automaticamente

1. Fazendo enumeração de diretórios a partir deste endpoint, só que utilizando a ferramenta dirb:

Texto

Descrição gerada automaticamente

1. Muitos desses diretórios possuem “pegadinhas” (como no robots.txt), mas ao analisar o \_test, verifica-se o seguinte:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Pesquisando o que é esse “sar2html”, chega-se em:

Interface gráfica do usuário, Texto, Site

Descrição gerada automaticamente

1. Portanto, provavelmente esta ferramenta tem falhas documentadas. Verificando as ferramentas, se encontra a seguinte: https://raw.githubusercontent.com/AssassinUKG/sar2HTML/main/sar2HTMLshell.py
2. Utilizando-a, é possível obter uma shell, abrindo um terminal escutando com *nc*:

Texto

Descrição gerada automaticamente

1. Procurando pelo servidor, encontra-se um arquivo *log.txt* com credenciais:

Texto

Descrição gerada automaticamente

1. Para utilizá-las, deve-se abrir um terminal com o comando: *python -c 'import pty;pty.spawn("/bin/bash")'*
2. Ao trocar de conta, tem-se:

Texto

Descrição gerada automaticamente

1. Procurando mais arquivos interessantes, tem-se:

Texto

Descrição gerada automaticamente

1. Utilizando as credenciais encontradas, tem-se:

Texto

Descrição gerada automaticamente

1. Procurando por binários com permissão SUID, tem-se:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Procurando *find* em <https://gtfobins.github.io/gtfobins/find/#suid>:

Texto

Descrição gerada automaticamente