13/07/2023 – TryHackMe – MrRobot

Link: [https://tryhackme.com/room/mrrobot#](https://tryhackme.com/room/mrrobot)

1. Fazer varredura de portas utilizando o nmap:

Texto

Descrição gerada automaticamente

1. Ao verificar o serviço HTTP na porta 80, tem-se:

Texto

Descrição gerada automaticamente

1. Nesse diretório principal não tem nada de útil para encontrar as flags. Ao testar o endpoint /robots.txt, padrão em muitas aplicações, tem-se:

Interface gráfica do usuário, Texto

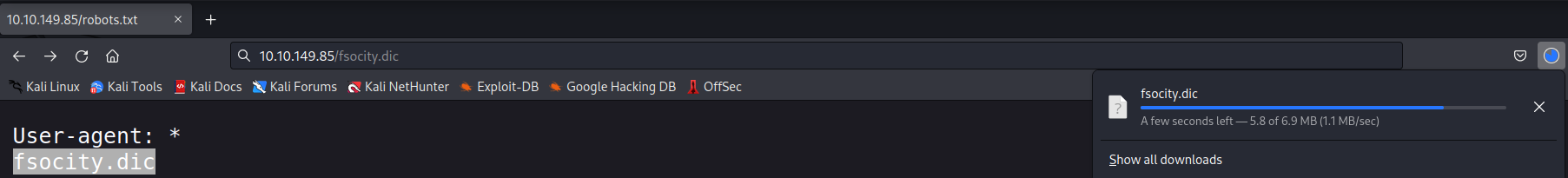
Descrição gerada automaticamente

1. Ao verificar o arquivo “key-1-of-3.txt”, tem-se:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Portanto, a primeira flag é: $flag. Ao verificar o segundo arquivo, tem-se:



1. Ao analisar o arquivo baixado, tem-se:

Texto

Descrição gerada automaticamente

1. Ao usar gobuster para listar mais diretórios, tem-se:

Texto

Descrição gerada automaticamente

1. Verificando o endpoint “/wp-login.php”, redirecionado por “/login”, tem-se:

Interface gráfica do usuário, Site

Descrição gerada automaticamente

1. Ao testar um usuário qualquer, tem-se:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Para encontrar um usuário válido, será utilizado o hydra juntamente com o wordlist encontrado previamente. Para isso, necessita-se saber os nomes dos parâmetros que referenciam o username e o password no body da request do login. Ao utilizar o BurpSuite para verificar tais parâmetros, tem-se:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Com isso, é possível encontrar um usuário válido com o hydra da seguinte forma:





1. Ao testar este username com um password qualquer, tem-se:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Utilizando a mesma wordlist para procurar uma senha válida, tem-se:

Texto

Descrição gerada automaticamente

1. Vale ressaltar que a wordlist “wc\_pass\_non\_dec.txt” é uma sublista da wordlist original, retirando as senhas duplicadas (que são muitas), e as senhas que se iniciam com um valor numérico. Isso acelera a busca pela palavra-chave correta, porém não invalida a utilização direta da wordlist original. O recomendado é realmente tirar as duplicatas, que aumentam drasticamente o tempo em que se encontra a senha correta. Fazendo o login, tem-se:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Ao explorar o site, verifica-se uma aba possível de se aplicar php-reverse shell (observando a ferramenta Wappalyzer): Tela de computador com texto preto sobre fundo branco

   Descrição gerada automaticamente
2. Ao abrir uma porta por meio do Netcat:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Ao pegar o arquivo de php-reverse shell do link: <https://github.com/pentestmonkey/php-reverse-shell>, e adicionando o IP da máquina atacante, juntamente com a porta que está sendo escutada pelo Netcat na máquina do atacante, tem-se:

Texto

Descrição gerada automaticamente

1. Colando o conteúdo do arquivo em “404.php” do site, tem-se:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Acessando o site, será possível efetivar o reverse-shell ao gerar um erro. Dessa forma:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Explorando o sistema, tem-se:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Ao tentar ler o arquivo com a flag, verifica-se que não se tem permissão:

Texto

Descrição gerada automaticamente

1. Ao abrir o arquivo com a senha, tem-se:



1. Utilizando a ferramenta <https://www.dcode.fr/md5-hash> para decryptar a senha, tem-se:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Trocando para o usuário robot (por conta do nome do diretório acessado), com a senha encontrada, tem-se:



1. Para transformar para terminal, fazendo um shell upgrade, rodar os seguintes comandos:

Texto

Descrição gerada automaticamente

1. Acessando o usuário robot, tem-se:

Texto

Descrição gerada automaticamente

1. Abrindo o arquivo com a flag, tem-se:



1. Provavelmente para encontrar a última flag deve-se acessar o usuário root. Para isso, verificar binários com permissão SUID da seguinte forma:

Texto

Descrição gerada automaticamente

1. Sabendo que o “nmap” é um binário com permissão SUID, é possível explorá-lo da seguinte maneira:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente