19/07/2023 – TryHackMe – Ignite

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

1. Fazendo um Port Scanning, tem-se:

Texto

Descrição gerada automaticamente

1. Verificando que está rodando uma aplicação web na porta 80, ao analisa-la, tem-se:

Tela de celular com aplicativo aberto

Descrição gerada automaticamente

1. Analisando o site, pode ser descoberto duas informações importantes para a resolução do CTF. Primeiro um endpoint de login, e segundo um diretório de configurações, armazenados em um database, onde pode ser observado usuários e senhas:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Verificando o endpoint encontrado, com o usuário e senha encontrados, tem-se:

Tela de celular

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Site

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Ao verificar a documentação, tem-se:

Interface gráfica do usuário, Texto, Email

Descrição gerada automaticamente

1. Com a versão do CMS, é possível pesquisar um exploit no site <https://www.exploit-db.com/> :

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Analisando o “[Fuel CMS 1.4.1 - Remote Code Execution (3)](https://www.exploit-db.com/exploits/50477)”, tem-se:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Baixando o arquivo python encontrado, e executando-o, tem-se:

Texto

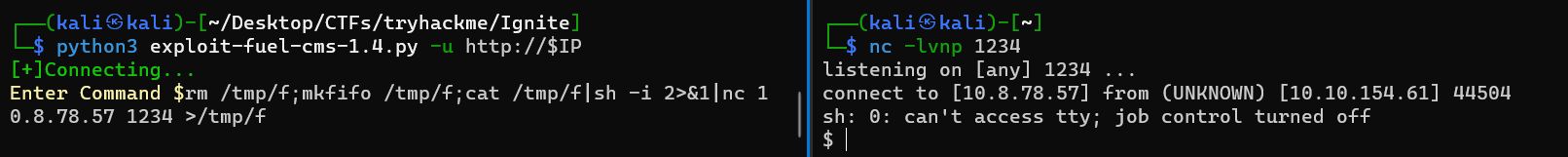
Descrição gerada automaticamente

1. Com isso, é possível explorar o sistema, porém utilizando este terminal fica “ruim” de se explorar. A partir deste RCE, é possível tentar explorar um Reverse Shell para atingir o objetivo supracitado. Com isso, procurando no site <https://www.revshells.com/> , e testando possibilidades de reverse shell, descobre-se o seguinte comando:

Tela de celular com publicação numa rede social

Descrição gerada automaticamente

1. Abrindo uma porta na máquina do atacante, e executando o comando via RCE (respectivamente), tem-se:



1. Possuindo a shell, é possível fazer um Spawn Shell para conseguir executar alguns comandos (como troca de usuários), que com o terminal que se tem não é possível. Procurando possibilidades de Spawn Shell no link <https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html> , encontra-se o seguinte comando:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Executando o comando no terminal:



1. Sabendo que no arquivo “database.php”, encontrado anteriormente, se tem dados sensíveis, é interessante verificá-lo. Com isso:

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente

1. Ao analisar o arquivo, encontra-se:

Texto

Descrição gerada automaticamente com confiança média

1. Com este usuário e senha do root, é possível trocar de usuário (possibilitado pelo Spawn Shell feito). Com isso, trocando de usuário, tem-se:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Logo, é possível encontrar as flags. De fato, é possível encontrar a primeira flag estando com o usuário padrão (www-data), porém esta resolução escolheu encontrar as flags após se tornar root. Com isso, encontrando a primeira flag no diretório “/home”, tem-se:

Texto

Descrição gerada automaticamente

1. Encontrando a segunda flag no diretório “/root” (necessariamente exigindo que o usuário seja root), tem-se:

Texto

Descrição gerada automaticamente com confiança média