02/09/2023 – TryHackMe – Basic Pentesting

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

1. Salvando o IP da máquina alvo na seguinte variável:



1. Usando o nmap para reconhecimento de portas, tem-se:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. É retornado que o serviço “smb” está vulnerável. Após uma pesquisa rápida, é possível descobrir que SMB é um protocolo de compartilhamento de arquivos usado para compartilhar recursos em redes de computadores. Pesquisando por vulnerabilidades neste serviço, chega-se no seguinte vídeo: <https://www.youtube.com/watch?v=IDnhJ3Ysvvo> . Nele, está descrito passos de como explorar o protocolo. Inicialmente, será utilizado a ferramenta smbmap para analisar o a porta 445 (que está rodando um smp server):

Texto

Descrição gerada automaticamente

1. Com isso, é possível verificar que o disco “Anonymous” está aberto para leitura. Com isso, será verificado os arquivos neste disco com o seguinte comando:

Texto

Descrição gerada automaticamente

1. Existe um arquivo “staff.txt” que pode ser útil na investigação. Portanto, de fato será acessado o serviço com a ferramenta “smbclient”, utilizando nenhuma senha:

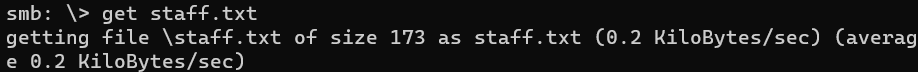
Texto

Descrição gerada automaticamente com confiança média

1. Verificando os arquivos no disco:

Texto

Descrição gerada automaticamente com confiança média

1. Importando o arquivo “staff.txt”: 
2. Lendo o arquivo:

Texto

Descrição gerada automaticamente

1. Existem 2 nomes que podem ser utilizados como usuário: Jan e Kay. Como não há mais nada de interessante por aqui, será analisado o serviço HTTP na porta 80. Ao analisar o site, tem-se:

Tela de celular com publicação numa rede social

Descrição gerada automaticamente

1. Como está descrito que existe uma seção de dev, será feito a enumeração de diretório para encontrar esta seção:

Texto

Descrição gerada automaticamente

1. Acessando o diretório /development:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

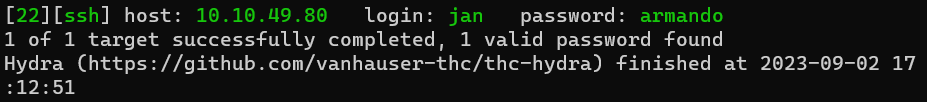
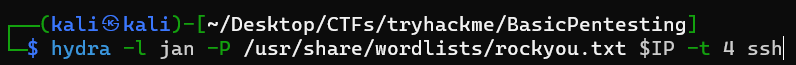
1. Lendo os arquivos:

Tela de celular com publicação numa rede social

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente

1. Lendo os comentários do arquivo “j.txt”, verifica-se que a “J” foi notificada a não utilizar credenciais fracas. Portanto, supondo que “J” seja de “Jan”, será feito um bruteforce com a senha dela no serviço “ssh” (verificado na enumeração de portas feitas com o nmap). Para isto, será utilizado a ferramenta “hydra”:



1. Acessando via ssh no usuário “jan” de senha “armando”:

Texto

Descrição gerada automaticamente

1. Verificando os arquivos ocultos:

Texto

Descrição gerada automaticamente

1. Verificando existência do “wget”:

Interface gráfica do usuário, Texto

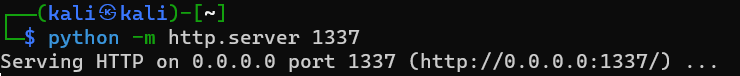
Descrição gerada automaticamente

1. Importando o arquivo <https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh> para analisar escalação de privilégio na minha máquina:

Texto

Descrição gerada automaticamente

1. Rodando um server http via python:



1. Importando o arquivo LinEnum na máquina alvo estando no diretório /tmp:

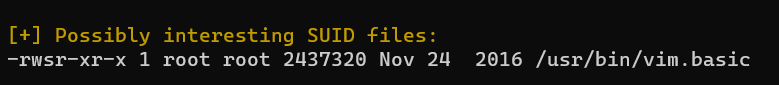
Texto

Descrição gerada automaticamente

1. Dando permissão de execução e logo após rodando o script:



1. Lendo o terminal:



1. Verificando no link <https://gtfobins.github.io/gtfobins/vim/> sobre escalação de privilégios utilizando vim:

Texto

Descrição gerada automaticamente com confiança baixa

1. Realizando o comando indicado, substituindo “py” por “py3”





Texto

Descrição gerada automaticamente

1. Por fim, explorando o servidor é possível encontrar a senha:

Texto

Descrição gerada automaticamente