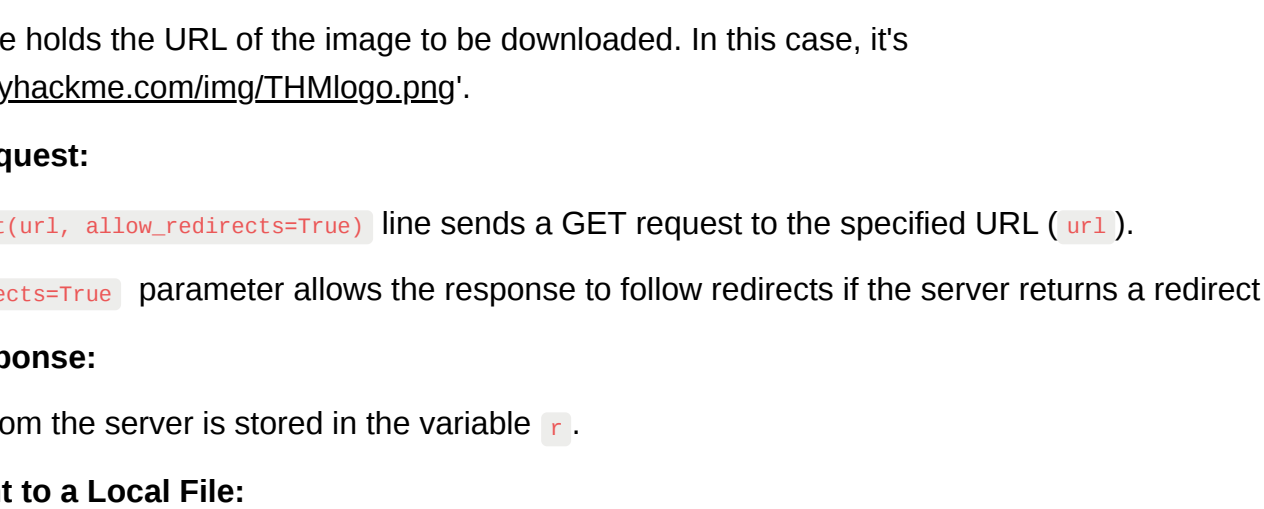
File_Downloader

```
import requests

# URL of the image to download
url = 'https://assets.tryhackme.com/img/THMlogo.png'

# Send a GET request to the URL and retrieve the content
r = requests.get(url, allow_redirects=True)

# Write the content of the response to a local file named 'THMlogo.png'
open('THMlogo.png', 'wb').write(r.content)
```

Explanation:

1. **Importing the `requests` Module:**
   - The code starts by importing the `requests` module, which is a popular Python library for making HTTP requests.
2. **Defining the URL:**
   - The `url` variable holds the URL of the image to be downloaded. In this case, it's 'https://assets.tryhackme.com/img/THMlogo.png'.
3. **Sending a GET Request:**
   - The `requests.get(url, allow_redirects=True)` line sends a GET request to the specified URL (`url`).
   - The `allow_redirects=True` parameter allows the response to follow redirects if the server returns a redirect status.
4. **Receiving the Response:**
   - The response from the server is stored in the variable `r`.
5. **Writing the Content to a Local File:**
   - The `open('THMlogo.png', 'wb').write(r.content)` line opens (or creates) a local file named 'THMlogo.png' in binary write mode (`'wb'`).
   - It then writes the content of the HTTP response (`r.content`) to the local file.
   - This effectively downloads and saves the image from the specified URL to the local file system.

PSexec
allow system administrators to run commands on remote Windows systems.
We see that PSexec is also used in cyber attacks as it is usually not
detected by antivirus software. You can learn more about PSexec
here and read ***this*** blogpost about its use by attackers.



`PsExec` is a legitimate Microsoft Sysinternals tool that is
often misused by attackers for lateral movement and remote code
execution on Windows systems. It is typically associated with the

"Execution" and "Command and Control (C2)" stages of the Cyber Kill Chain:

Therefore, `PsExec` is commonly associated with the later stages of the Kill Chain, particularly in the phases involving execution and command and control. It's important to note that while `PsExec` is a legitimate tool, its misuse by attackers can be a sign of malicious activity. Organizations often monitor for unusual or suspicious use of tools like `PsExec` as part of their security measures.