**Capture the flag exercise: Analyze PowerShell scripts**

For this exercise, search for and download tools to your VM to perform this activity. Hints are provided throughout the module and in the questions below. For help, refer to the Capture the Flag exercise demo video in Module 2.

From re\_exercises.zip, you will analyze:

MegaProject.ps1

**Answer the following questions and capture the flag:**

A screenshot of a computer

Description automatically generated

**VirusTotal**

**A screenshot of a computer

Description automatically generated**

* What is the SHA256 hash of the file?

**cab3224df17971790cd56131e0629b766868a336072496b2901e7f3d14827b2d**

* Where does this program externally connect to? (Hint: use tools like FakeNet-NG, Wireshark, BurpSuite)

**https://a\_non\_existent\_powershell\_test\_site.com/pub/hacked/malware.bin**

* What is the flag? (Hint: Debug and check the variables to get the flag. Be careful with the IEX command, it immediately executes code passed to it. But you can also statically analyze and use Cyberchef.)

**SUP3R\_P0W3RSH33L\_X-Force**

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated