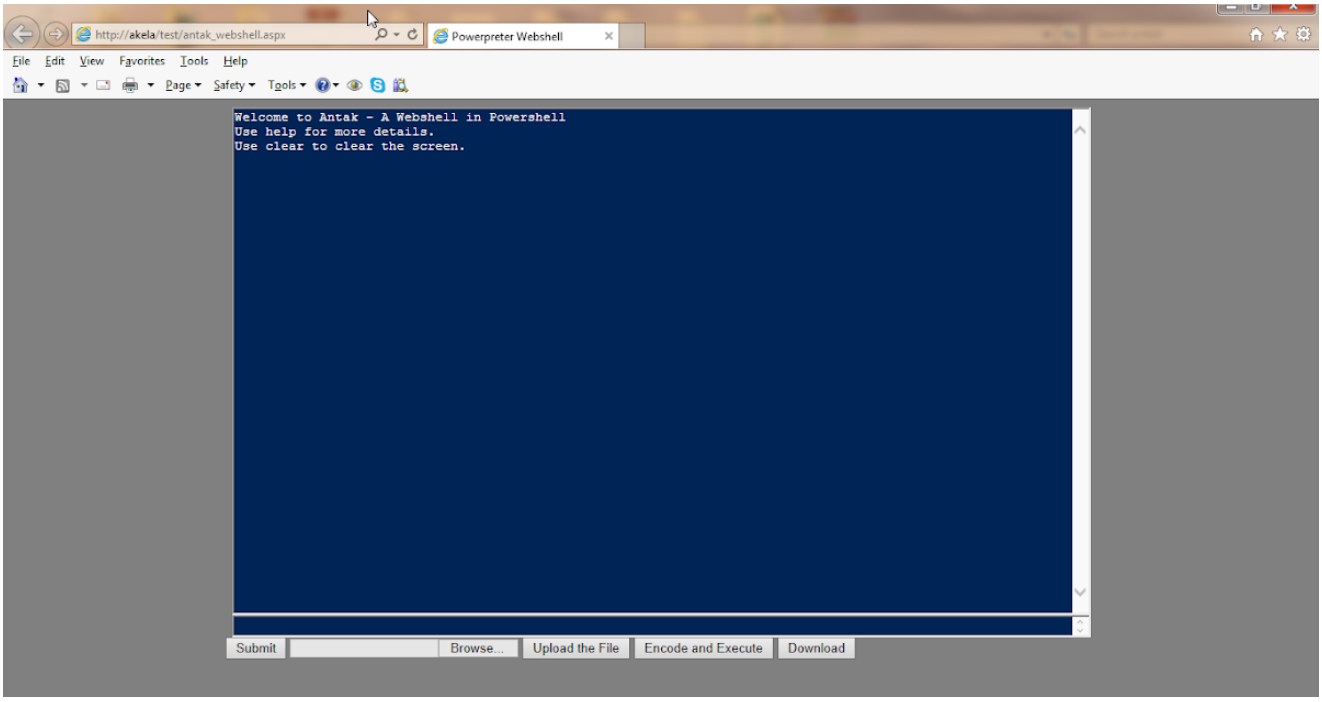
Introducing Antak - A webshell which utilizes powershell

labofapenetrationtester.com/2014/06/introducing-antak.html

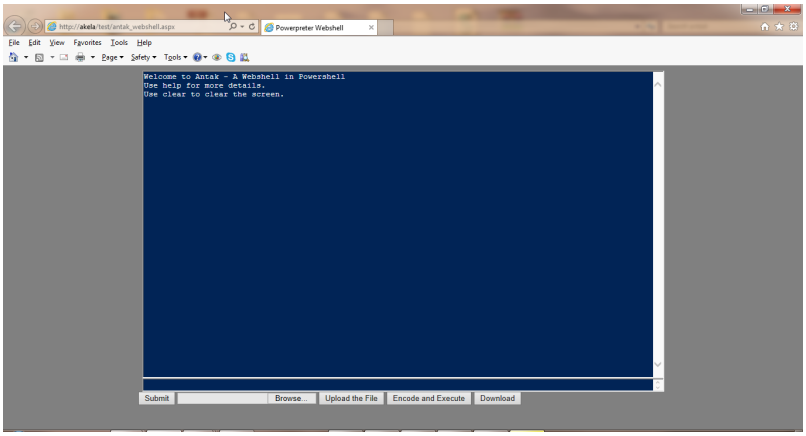


Duing penetration tests, I always wanted to have a simple yet powerful webshell. For that, I wrote Antak last year, demonstrated it at Defcon 21 but never released for I was busy in other things :)

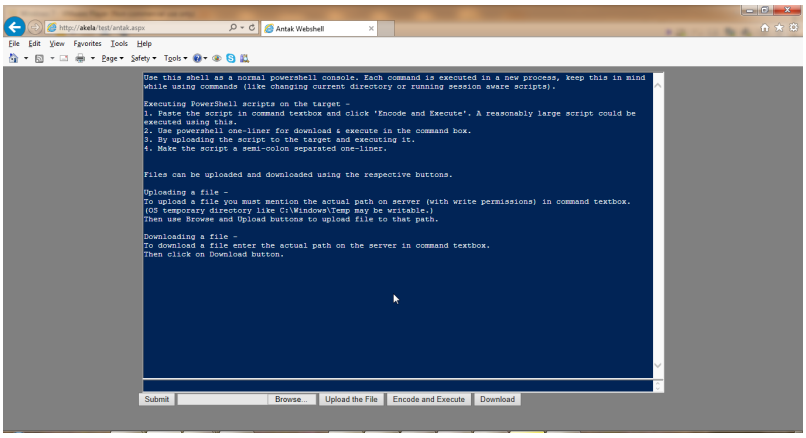
Antak stands for God of Death in Indian mythology, popularly known as Yamraj. Muhahaha

The webshell is a part of Nishang now. It is written in ASP.Net.

Antak's UI has been designed to resemble a powershell console.



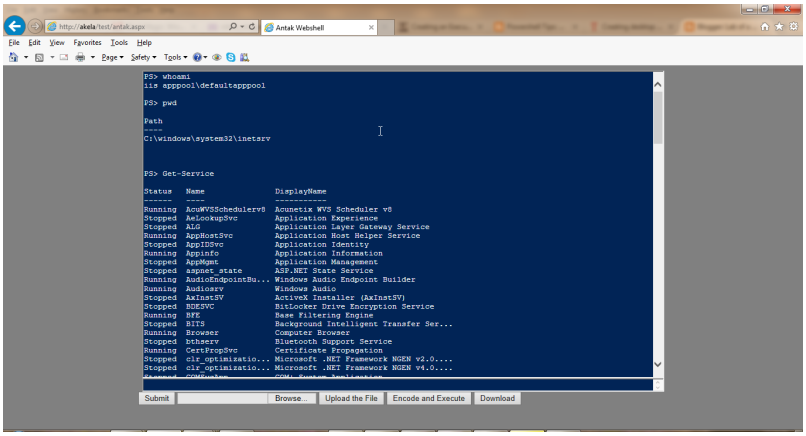
Use *clear* to clear the output box. Use *help* to see the built-in help.



Lets see some of its features.

Running Commands

To run commands on the target machine, just type those in the command text box and press enter or click on submit.



Each command is executed in a separate powershell process. To run multiple commands in a single process, use semi-colon (;) separated commands like *cd..;pwd;ls*

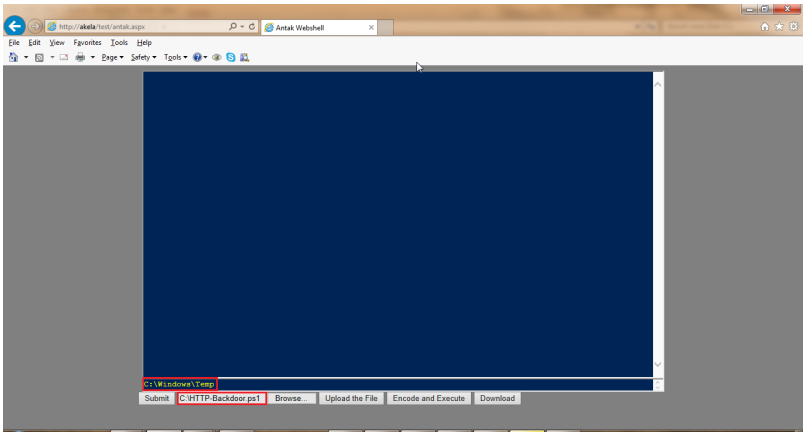
You are effectively sitting on a powershell prompt with *-noninteractvie* and *-executionpolicy bypass* parameters. So all powershell commands would run. Great!

Code snip for command execution:

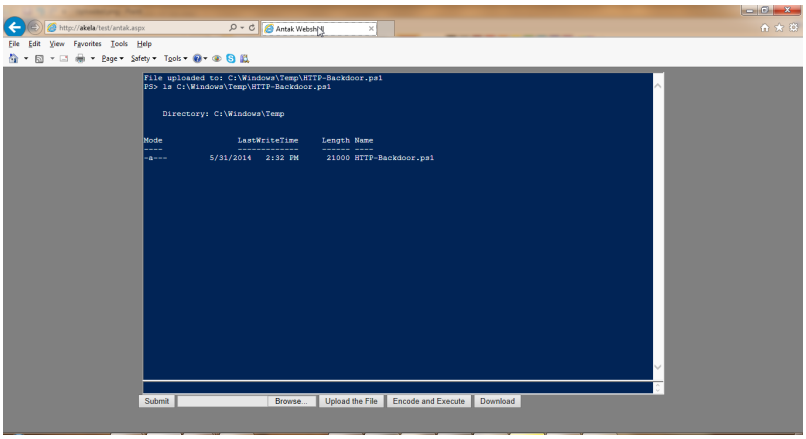
Upload a file

To upload a file using Antak:

1. Write the path writable directory in command box. Usually, at least C:\Windows\Temp should be writable.
2. Use the browse button to locate the file on your local machine.



3. Click on "Upload the file" button.
Also, lets verify if the file has been uploaded.

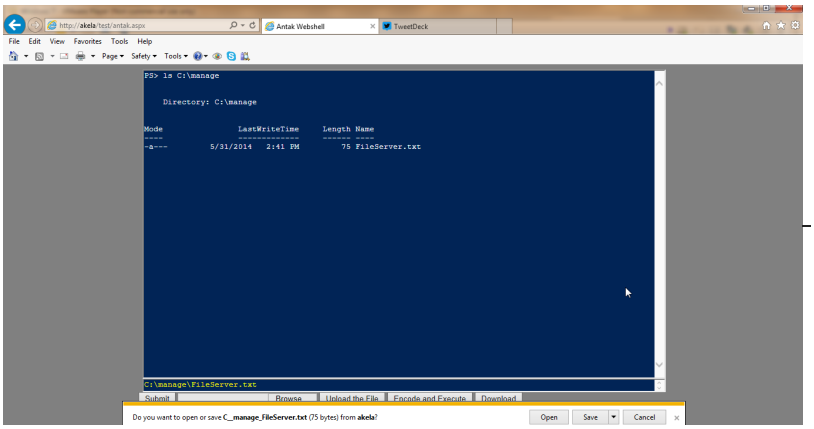


Nice! The file has been uploaded.

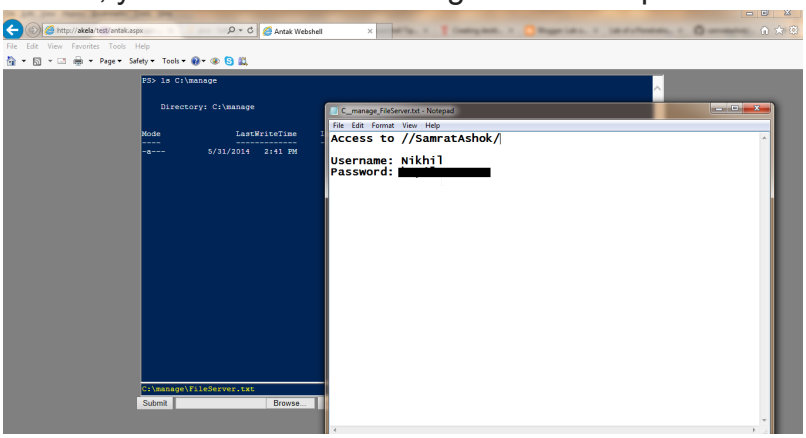
Code for this:

Download a file

To download a file, just write/copy its complete path in command box and click on the "download" button.



And this downloaded text file contains username and password to another machine. Of course, you won't find such things in an enterpreise envirоonment (pun intended) :D



Code for download:

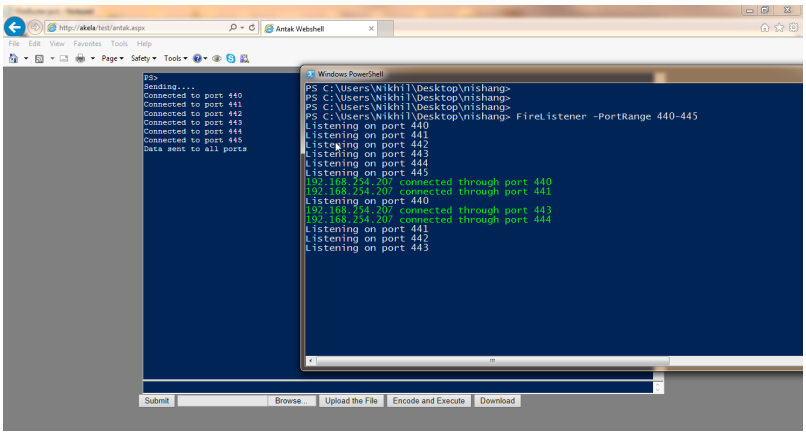
Executing Scripts

There are many ways how a script could be executed using Antak.

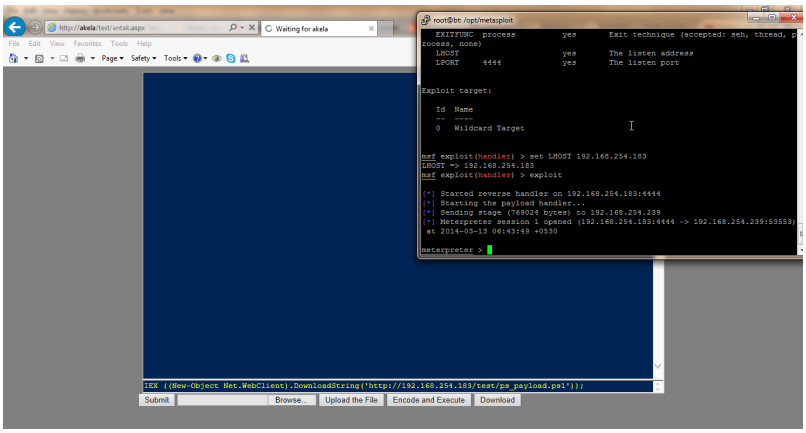
UPDATE: In methods 1 and 2 below the script does not touch disk (someone asked me this).

1. Paste the script in command box and click "Encode and Execute".

Lets try this with the egress testing script *Firebuster.ps1*

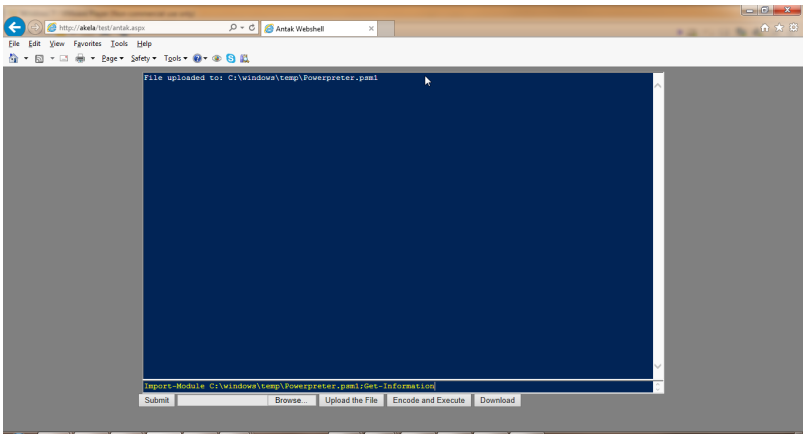


2. Using powershell one-liner for download & execute. Paste the one-liner in command box and click on execute.
Lets try this with powershell payload generated using msf.



The one liner which could be used is:

3. An uploaded script could be executed in the usual way.
Lets upload *powerpreter* on the target and use *Get-Information* function.



Handy!

Remoting/Pivoting

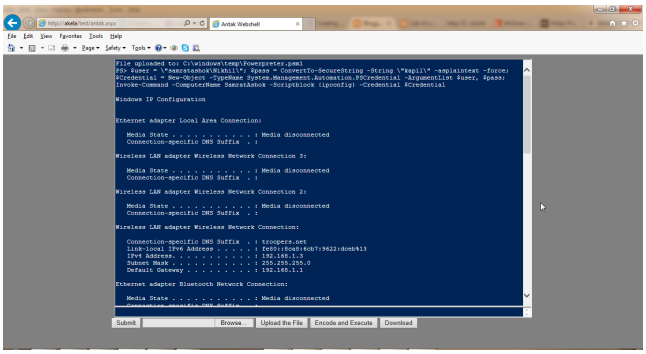
Recall that we are practically on a powershell prompt. So lets try to use powershell remoting to execute commands on remote machines. Two things which are required for using powershell remoting from Antak are:

1. Administrative credentials for the target remote system.
2. Powershell remoting must already be enabled between system where Antak is residing and the target machine. As it is not possible to change any settings due to low privileges under which Antak runs.

Recall that we downloaded a plain-text credential for a remote machine. That could be used now.

Following semi-colon(;) separated commands could be used to achieve this. This command takes username and password in plain and exeucte ipconfig on the target.

Lets use this :)


Great! We are able to execute commands on the remote machine.

That is it for Antak, hope you liked it. It is a part of Nishang and could be found here: https://github.com/samratashok/nishang

If you would like to see Antak in action, you may like to see the webcast I did for Garage4hackers:

I look forward to feedback, bugs and feature requests.