Open in app ↗

Sign up   Sign in

Medium   🔍 Search   ✎ Write   👤

Pentesting and .hta (bypass PowerShell Constrained Language Mode)

✕

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

through application whitelisting rules and we can do lots of interesting things using the extra scripting languages, specifically *vbscript*.

Lets say you're in an environment where you don't have access to the command prompt or PowerShell and you want to do something simple, like ping a PC. You could use a hta file with the following contents:
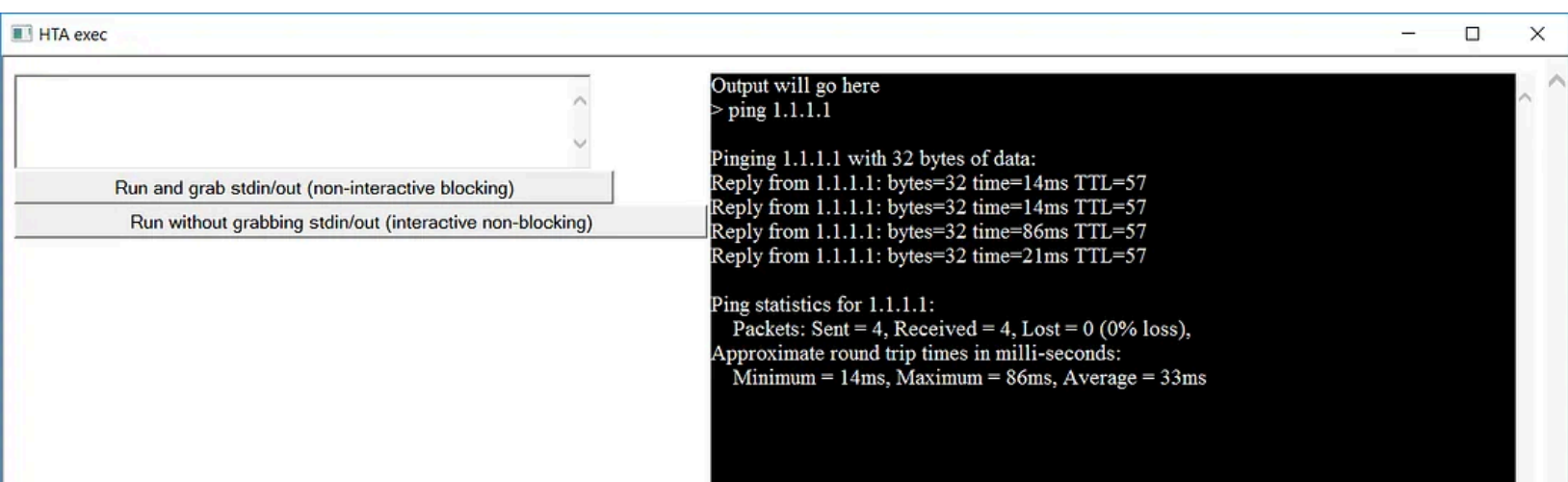
Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

to create said executable using another built in windows binary, *csc.exe,* which can be used to compile arbitrary C# code (this resource is useful for application whitelist bypasses). Doing this manually is a pain and too hard to remember so we use a .hta to wrap the mundane steps. The hta will perform the following steps:

1. Write some C# to a file, the C# contains an uninstall hook

2. Compile the C# from step 1 into a .exe using csc.exe

3. Write the PowerShell commands you want to run to a file. The C#

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

tools without a file ever hitting disk.

```
mshta.exe javascript:"<script
language=vbscript>createobject(\"WScript.Shell\").run(\"calc\")\r\
nclose()</script>
```

Persistence

In Windows 10 (and Windows Server 2016 I think), Windows restarts a selection of applications that were running before you shut down the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app