Remote Script Execution AWS EC2 Win

Vijay Philip

Version

0.1 - Created on 10/03/12 by Vijay Philip

Requirements

- Download the PsExec program from http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx Or download PsExec.exe version 1.98 posted here.

- PsExec.exe - remote process execution tool published by Mark Russinowich that allows an administrator to run processes on a remote system.

- Download the batch script, PsExecRemote.bat - script that automates the PsExec with ec2 information to remotely run the exe/batch script.

Remote EC2 Instance Setup / Info

- IPA
- Username
- Password
- Path to the batch/exe
- Open TCP port 445 on the remote EC2 instance for traffic.

Edit PsExecRemote.bat Source

- **SET IPA=*23.22.11.10* (Remote EC2 IP Address)**
- **SET USER=*Administrator* (Remote EC2 Account Username)**
- **SET PSWD=*"abcd1234"* (Remote EC2 Account Password)**
- **SET EXE=*"C:\script.bat"* (Path on Remote EC2 Instance to script/exe)**

Please note that **PSWD** & **EXE** variables enclosed in quotations.

Some non-alphanumeric characters like "&" or spaces can cause the batch file to fail.

Enclosing them in quotations is safe way to pass these parameters within the batch script.

Final Notes

- Run the batch file, check to see the results.log for output of the run.
- You can automate the batch file call via your publishing program.
- TCP Port 445 has been opened for traffic in the AWS security group and on the EC2 instance.
- It is advisable to restrict the TCP port 445 rule on AWS security group to connections only to your specific endpoints.