MITRE TEST

This code was used to deploy the Atomic red Team framework based on the mitre ATT&CK framework on a windows machine.

How to

to deploy this you need 2 machines that can ping each other:

- a windows machine with the agent installed
- a machine with ansible installed (I used a debian machine)

in the inventory file you need to change the following entries:

- `ansible_user` with the username of you windows machine
- `ansible_password` with the password of your windows machine
- `hosts` with the ip of the windows machine

also you need to add the agent installer in *roles/atomic/files* and rename it `edrinstaller.msi`|`edrinstaller.exe` depending on the extension.

this playbook will install the atomic red scripts on the windows machine and add 2 script one to install all the prerequirement and the other to run all windows test. Both can take some time.

you can use the following command to execute the playbook:

- `ansible-playbook mitre-playbook.yml -v --skip-tag "install_exe"` to install the .exe file
- `ansible-playbook mitre-playbook.yml -v --skip-tag "install_msi"` to install the .msi file

after the successful installation you cann connect to your windows machine and run the `run-all-prereqs.ps1` script as administrator inside the **C:\tools** directory, if this fail you need to run `Set-ExecutionPolicy Unrestricted` as administrator.

and after you can run the `run-all-techniques.ps1` script.