Hacking scenario

In here you will find the code for the automation of the different machines and each step of the attack.

prepare the environment

for this test you need up to 6 machines (for the architecture check the Guide point **3.2.2.1**).

- attacker machine:
  - A windows machine with visual studio to compile the C# code and windows defender disabled.
  - A linux machine preferably Kali Linux with the metasploitable framework installed (you can also install it on the windows machine if you want)
- test machines (with the same username and password):
  - a windows OS machine for the initial access.
  - a windows server which will work as Domain controller.
  - a windows server to install the agent on all machines.
  - a machine (windows or Linux) with ansible and running in the same network.

To create the environment you just need to copy the code in automation inside the ansible machine and you need to change the following things:

- *inventory.yml*
  - hosts IP address of all 3 machines to there corresponding IPs
- *group_vars/windows.yml*
  - `ansible_user` with the common username of all three machines.
  - `ansible_password` with the common password of all three machines.
  - `domain_name` with the domain name you want.
- copy the agent installer in *roles/winserver/files*

after changing the different setting you can run the command `ansible-playbook mitre-playbook.yml -v --skip-tags install_msi` if you have a .exe agent installer or `ansible-playbook mitre-playbook.yml -v --skip-tags install_exe` if you have an .msi agent installer.

after the successful execution of ansible you can create a GPO that install the agent on all machine. You can also change the password of a domain admin and give local admin right to a user in your domain and change the password of both.

To make the attack simpler you can add the password of the domain admin in the comments or log the user in the windows machine.

check the video **Prepare hacking enviroment** to see the process.

Hacking steps

for the whole attack you can check the video or follow the instruction down here.

⚠️ change the *{path to this folder}* and the ** to the IP of you Kali and to where you copy the scripts

1. Create the payload

Kali Linux machine execute `create_reverse_shell.sh` (change the IP indide the script with yours) to create a meterpreter payload for the hiden payload.

Evil Windows machine copy the created file on you windows machine, you can use the python http.server for this.

2. Create the injected

Evil Windows machine Download the cotent of the payload and copy it inside the `Executable_gen.cs` and execute `csc Executable_gen.cs`

after that you can host it with python http.server

3. Run the backdoor

Kali Linux machine copy the script 00* to 04 and both autorun script to your document folder.

execute the following command `msfconsole -q -r 00_impersonate_github.rc` and change the value of `{path to impersonate_ssl file}` inside the different script to the location of the pem file

run the following command `resource 01_create_backdoor.rc` this will create the listener of your backdoor.

Windows machine Login with the user with local admin privileges

download the malicious file with the payload and execute it

Kali Linux machine result of the connection

4. create privilege escalation

Kali Linux machine run the command `resource 02_create_priv_esc.rc` this will create the privilege escalation move to a privileged process and execute bloodhound (a AD scanner)

after that you can dezip the zip file created during the escalation step if you want and run bloodhound but this is not required since you know which user to use.

5. create persistence

Kali Linux machine run the command `resource 04_create_persistence_listener.rc` to create the listener for your persistance and run `ressource 03_create_persistence.rc` to create the persistance

6. lateral mouvement

Kali Linux machine for the lateral mouvement you will use the following script in your msfconsole `resource 05_lateral_mouvement.rc` don't forget to change the parrameter in the file. This will create a new session on your AD.