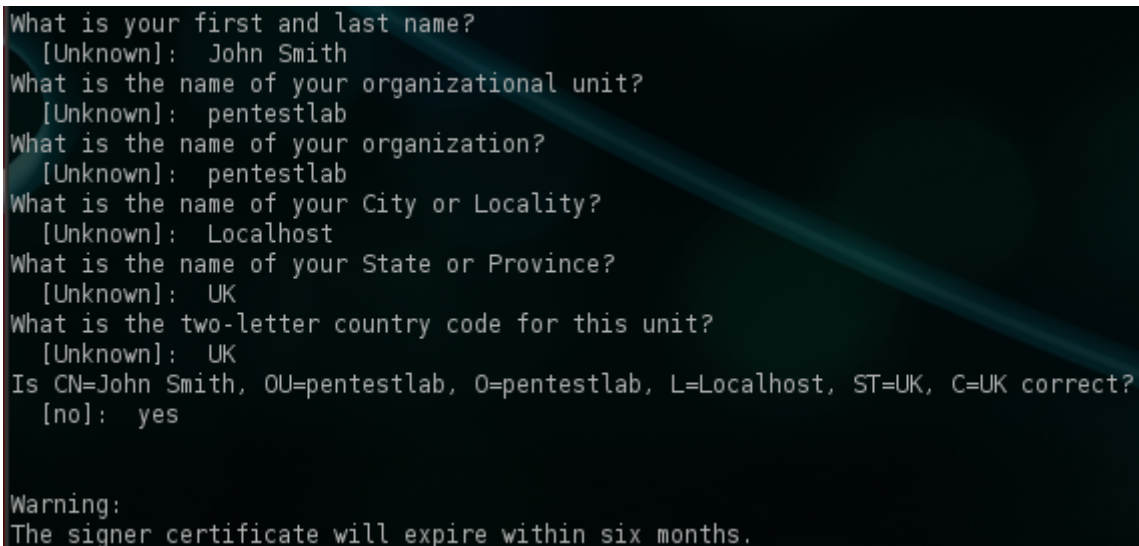


Configuring The Social Engineering Toolkit



```
What is your first and last name?
[Unknown]: John Smith
What is the name of your organizational unit?
[Unknown]: pentestlab
What is the name of your organization?
[Unknown]: pentestlab
What is the name of your City or Locality?
[Unknown]: localhost
What is the name of your State or Province?
[Unknown]: UK
What is the two-letter country code for this unit?
[Unknown]: UK
Is CN=John Smith, OU=pentestlab, O=pentestlab, L=localhost, ST=UK, C=UK correct?
[no]: yes

Warning:
The signer certificate will expire within six months.
```

One of the best tools for conducting social engineering attacks is SET which was developed by Dave Kennedy. The social engineering toolkit is already pre-configured to use some default settings in order to make it more easier for its users. However these settings can be altered in order to cover the needs of the scenario that the penetration tester will create. The changes that we can make are endless so in this article we will cover only the basic.

In Backtrack SET is located in the following directory:

/pentest/exploits/set

So we need to browse to that directory first and then to find the **set_config** file which is located in the directory called config inside the SET folder. This file contains all the setting that it can be made in the social engineering toolkit.

By default SET is configured to use Gmail as the default email provider for sending emails to other users through SET. If we want to use other providers such as Yahoo and Hotmail we just change the following setting:

EMAIL_PROVIDER=Yahoo

One of the most popular web-based attacks that the social engineering toolkit is also using is the Java applet attack. If we try to use this attack we will notice that SET is configured to use Microsoft as the publisher name. If we want to use a different publisher we can change the following setting to ON.

SELF_SIGNED_APPLET=ON

SET will require from us additional information so we will import the information accordingly to the scenario that we have develop. You can see in the next image a sample of the information that we have to provide:

```
What is your first and last name?
[Unknown]: John Smith
What is the name of your organizational unit?
[Unknown]: pentestlab
What is the name of your organization?
[Unknown]: pentestlab
What is the name of your City or Locality?
[Unknown]: Localhost
What is the name of your State or Province?
[Unknown]: UK
What is the two-letter country code for this unit?
[Unknown]: UK
Is CN=John Smith, OU=pentestlab, O=pentestlab, L=Localhost, ST=UK, C=UK correct?
[no]: yes

Warning:
The signer certificate will expire within six months.
```

SET – Java Applet Self Signed Certificate

Another one important configuration that we can play with is the **AUTO_DETECT** option. When this option is set to **ON** the social engineering toolkit will detect automatically our local IP address and it will use it for the reverse connection of our attacks. If this option is set to **OFF**, the social engineering toolkit will ask for our public IP address. This can be used in a scenario that we are behind NAT and we want to use SET over the Internet.

AUTO_DETECT=OFF

```
set:webattack>l
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:█
```

SET asks for public IP when AUTO_DETECT option is OFF

Also the web-based attack vectors like the credential harvester can be used in combination with email phishing in order to improve the success rate of the attack. The option that we have to configure is the following:

WEBATTACK_EMAIL=ON

```
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter

set:webattack> Select a template:2

[*] Cloning the website: https://gmail.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[!] I have read the above message.

Press <return> to continue

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
```

Email support in combination with credential harvester attack

As we can see and from the image above SET will include as well in the attack and the email support in order to be able to send email directly to users after the launch of the attack.

Conclusion

Social engineering toolkit provides a variety of options in his configuration file which can be altered in order to meet our needs. However in this article we saw only some of the basic configurations that we can do to change the behavior of SET and to make it work more efficiently.