**[MITM Automated Suite That Looks Just Lame.](https://null-byte.wonderhowto.com/how-to/subterfuge-mitm-automated-suite-looks-just-lame-0156845/)**

* By [**Ciuffy**](https://creator.wonderhowto.com/ciuffy/)
* 08/11/2014 7:34 pm
* [MitM](https://null-byte.wonderhowto.com/how-to/mitm/)

Remember when MITMing people to pentest webapps and log-ins you had to fire Ettercap,Arpspoof, SSLstrip, then look for credentials in the captured packets?

No more thanks to (or fault of?) "Subterfuge".

Surprisingly, there's nothing about Subterfuge here on Null Byte (is it?), so I decided to share this awesome tool presented at DEFCON 20.

Subterfuge is an automated suite for MITM attacks that includes a lot of useful features and tools (like SSLstrip) that will make your pentest easier and more efficient. Not only it includes SSLstrip (completely automated), but the creators have added some features to make it more powerful and reliable.

Here's the DEFCON speech on YouTube:

And here's the download link:

[**Downloads - subterfuge - Automated Man-in-the-Middle Attack Framework - Google Project Hosting**](http://code.google.com/p/subterfuge/downloads/list)

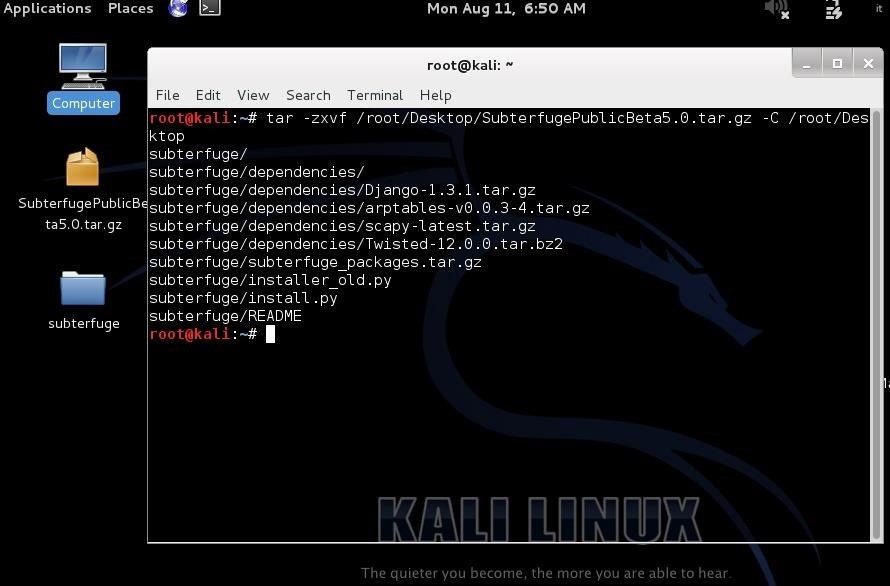
So let's see how-to install and setup it on Kali Linux and let's explore some of its amazing features.

**Step 1Download the Packages**

Go to the download link above and choose your download.  
For efficiency purposes, I'm going to download the SubterfugePublicBeta5.0.tar.gz package.  
Place it in the Desktop and that's it for this step.

**Step 2Extract the Packages**

There are plenty of ways to extract a .tar.gz in Linux:  
Open the Terminal and type:  
**tar -zxvf /root/Desktop/SubterfugePublicBeta5.0.tar.gz -C /root/Desktop**  
It will extract the contents of the compressed file in the Desktop, in a folder called "subterfuge".

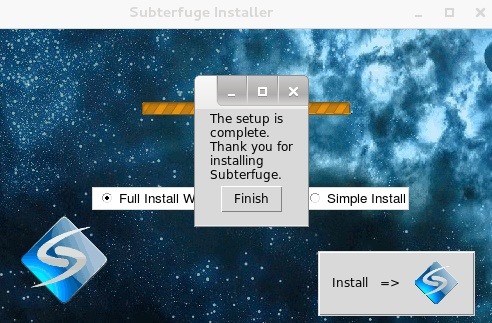
[](https://img.wonderhowto.com/img/original/02/33/63543325877838/0/635433258778380233.jpg)

**Step 3Setup Subterfuge**

Type in the Terminal:  
**cd /root/Desktop/subterfuge**  
to navigate to the folder,  
and:  
**python install.py**  
to start the installer.  
Something like this will be prompted:

[](https://img.wonderhowto.com/img/original/55/45/63543326073253/0/635433260732535545.jpg)

Check "Full Install with Dependencies" and click the Install button.  
The installer is super verbose, wait until this will prompt:

[](https://img.wonderhowto.com/img/original/76/33/63543326272525/0/635433262725257633.jpg)

Click finish, now you can close the Terminal.

**Step 4Start Subterfuge (And Credential Harvester Modules)**

From now on you'll only have to type "subterfuge" in the Terminal to start our new friend, then go to Iceweasel and type in the URL space "127.0.0.1".

There you go:

[](https://img.wonderhowto.com/img/original/26/81/63543329576109/0/635433295761092681.jpg)

Now you can press the button "start" and the Credential Harvester Module will automatically start, capturing all the passwords that people type in your LAN, including SSLstrippded ones.

Before we continue with some other modules, I want to tell you why SSLstrip isn't reliable anymore (almost).

HTTPS SSLstrip vulnerability has been patched with HSTS Headers, so that first time someone connects to a HTTPS page that he never visited, it is stored as HTTPS, and when you visit that page again the HTTPS request will be inevitable, and SSLstrip won't be effective (it would only if it's running the first time that the victim visits the page, but some browsers implemented a list of default HSTS headers for popular sites, so yeah).

HSTS is supported by most of the browsers out there (latest versions) except IE (surprised?), which is said to implement it in version 11.

**Other Interesting Subterfuge Features and Modules**

First, you may say: "what if I want to MITM only one host?"  
Subterfuge->Settings

Here you can customize the settings, that otherwise Subterfuge will tell you to do it for you (this is also automated, how nice!).

Just enter the single client in "Arp single clients".

A little description on the other modules that Subterfuge supports (some of those are NOT supported in the public beta, you'll have to download the official .deb file, which is even easier to install):

1)Network View:"allows you to quickly and easily launch advanced attack vectors".  
2)Session Hijacking:steals the cookies of the compromised session to authenticate into a web service.  
3)HTTP code injection:"allows the user to inject payloads directly into a compromised session".  
4)Evilgrade:evilgrade is a tool built for update hijacking, you can find documentation online.