**[How to Crack Online Passwords with Tamper Data & THC Hydra](https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-passwords-with-tamper-data-thc-hydra-0155374/)**

* By [**occupytheweb**](https://creator.wonderhowto.com/occupythewebotw/)
* 05/27/2016 2:20 am
* [Password Cracking](https://null-byte.wonderhowto.com/how-to/password-cracking/)

Welcome back, my tenderfoot hackers!

Not too long ago, I showed how to find [various](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-targets-using-shodan-the-worlds-most-dangerous-search-engine-0154576/) [online](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-any-routers-web-interface-using-shodan-0154660/) [devices](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-webcams-across-globe-using-shodan-0154830/) using [Shodan](https://null-byte.wonderhowto.com/how-to/shodan/). As you remember, Shodan is a different type of search engine. Instead of indexing the content of websites, it pulls the banner of web servers on all types of online devices and then indexes the content of those banners.

This info can be from any type of device including web servers, routers, webcams, SCADA systems, home security systems, and basically anything that has a web interface, which in 2014, means just about everything.

I mentioned in [my first Shodan tutorial](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-targets-using-shodan-the-worlds-most-dangerous-search-engine-0154576/) that you can often access these devices by simply using the default username and password, as administrators are often lazy and neglectful. The question we want to address in this tutorial is—what do we do when the site requires credentials and the defaults don't work?

There is tool that is excellent for cracking online passwords and it is called [THC-Hydra](https://www.thc.org/thc-hydra/). Fortunately, it is built into [our Kali distribution](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/), so we don't need to download, install, or [compile](https://null-byte.wonderhowto.com/how-to/hack-like-pro-compile-new-hacking-tool-kali-0155229/) anything to use it.

[](https://img.wonderhowto.com/img/original/67/46/63537989329975/0/635379893299756746.jpg)

*Image via* [*Shutterstock*](http://www.shutterstock.com/pic-10322398/stock-photo-binary-code-goes-to-a-keyhole.html)

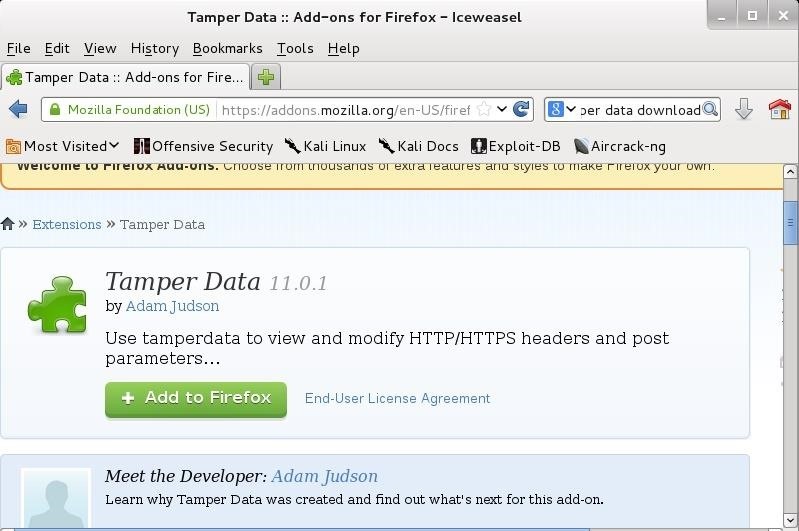
**Step 1Download & Install Tamper Data**

Before we start with THC-Hydra, let's install another tool that complements THC-Hydra. This tool is known as "Tamper Data", and it is a plug-in for Mozilla's Firefox. Since our IceWeasel browser in Kali is built on the open source Firefox, it plugs equally well into Iceweasel.

Tamper Data enables us to capture and see the HTTP and HTTPS GET and POST information. In essense, Tamper Data is a web proxy similar to Burp Suite, but simpler and built right into our browser.

Tamper Data enables us to grab the information from the browser en route to the server and modify it. In addition, once we get into more sophisticated web attacks, it is crucial to know what fields and methods are being used by the web form, and Tamper Data can help us with that as well.

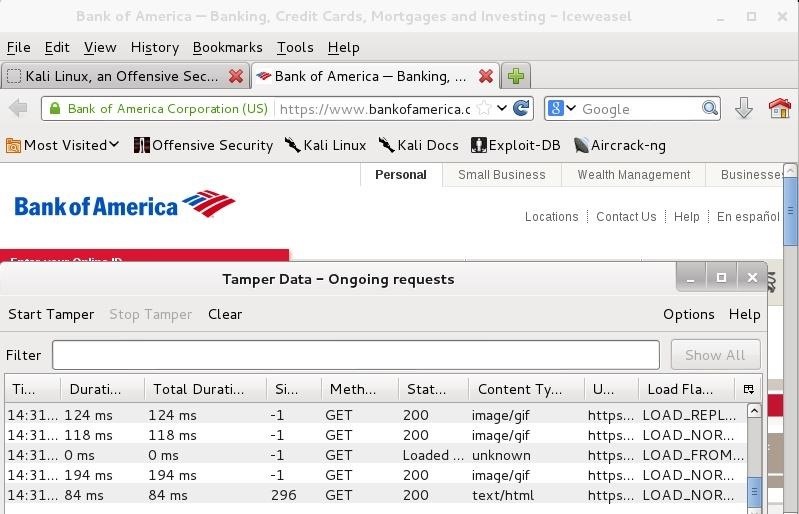
Let's [download it from here](https://addons.mozilla.org/en-US/firefox/addon/tamper-data/) and install it into Iceweasel.

[](https://img.wonderhowto.com/img/original/13/62/63537564557013/0/635375645570131362.jpg)

Install the Tamper Data Firefox add-on in Iceweasel.

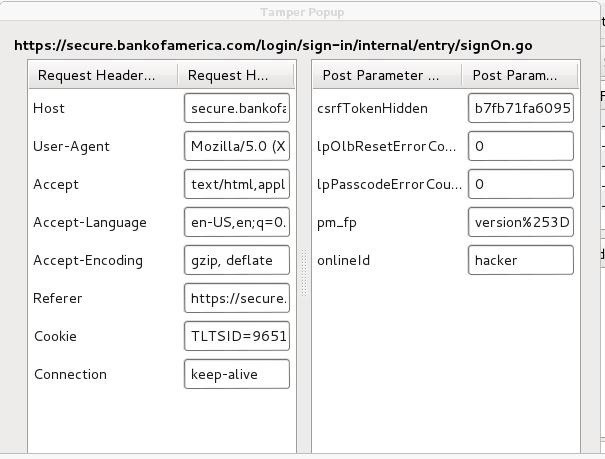
**Step 2Test Tamper Data**

Now that we have Tamper Data installed into our browser, let's see what it can do. Activate Tamper Data and then navigate to any website. Below you can see that I have navigated to Bank of America and Tamper Data provides we with each HTTPS GET and POST request between my browser and the server.

[](https://img.wonderhowto.com/img/original/90/17/63537564829231/0/635375648292319017.jpg)

HTTPS GET and POST requests for BOA.

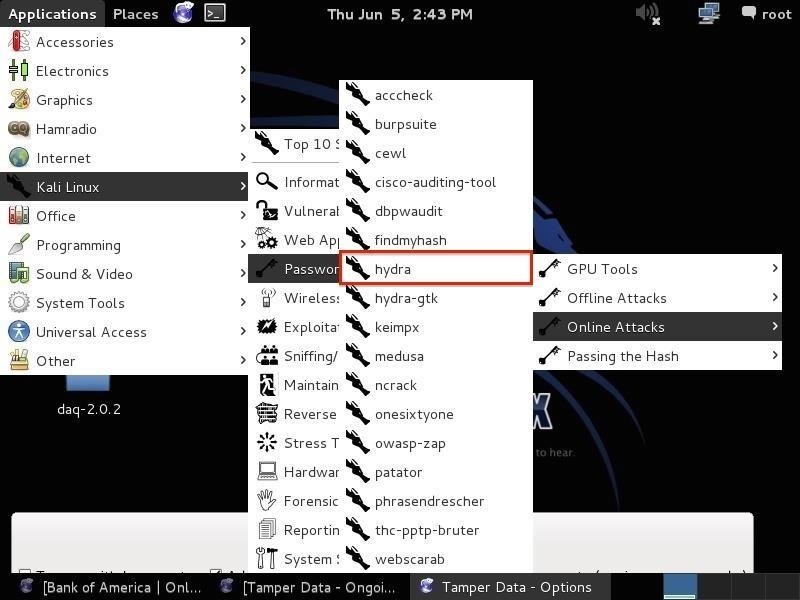
When I try to login to the site with the username "hacker", Tamper Data returns to me all the critical info on the form. This information will be useful when we begin to use Hydra to crack online passwords.

[](https://img.wonderhowto.com/img/original/89/21/63537565265903/0/635375652659038921.jpg)

Tamper Data information for BOA login.

**Step 3Open THC Hydra**

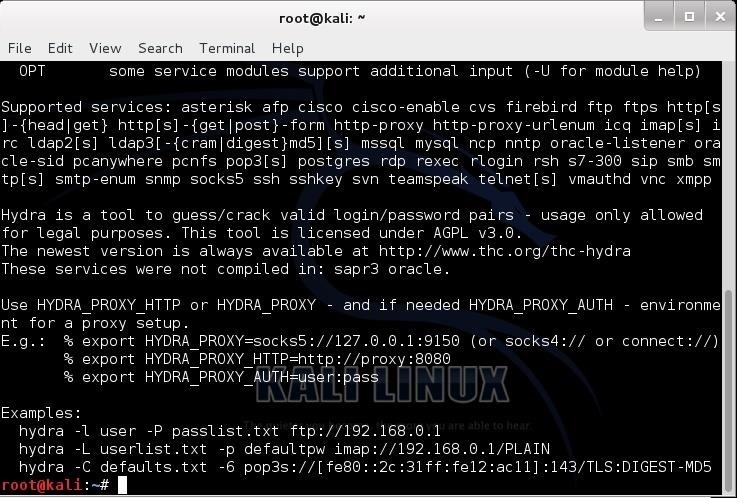
Now that we have Tamper Data in place and working properly, let's open Hydra. You can find it at *Kali Linux* -> *Password* -> *Online Attacks* -> *Hydra*. You can see it about midway among the list of online password cracking tools.

[](https://img.wonderhowto.com/img/original/61/23/63537987330476/0/635379873304766123.jpg)

Select the "hydra" tool.

**Step 4Understand the Hydra Basics**

When we open Hydra, we are greeted with this help screen. Note the sample syntax at the bottom of the screen. Hydra's syntax is relatively simple and similar to other password cracking tools.

[](https://img.wonderhowto.com/img/original/15/79/63537565634263/0/635375656342631579.jpg)

The initial help screen for Hydra.

Let's take a look at it further.

**hydra -l username -p passwordlist.txt target**

The **username** can be a single user name, such as "admin" or username list, **passwordlist** is usually any text file that contains potential passwords, and **target** can be an IP address and port, or it can be a specific web form field.

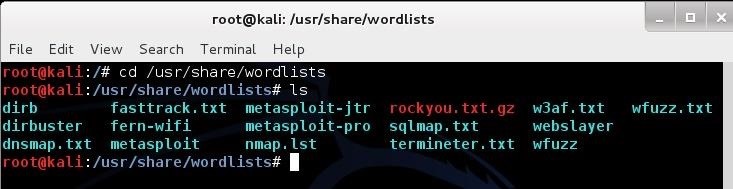
Although you can use ANY password text file in Hydra, Kali has several built in. Let's change directories to */usr/share/wordlists*:

**kali > cd /usr/share/wordlists**

Then list the contents of that directory:

**kali > ls**

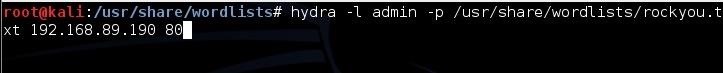
You can see below, Kali has many word lists built in. You can use any of these or any word list you download from the web as long as it was created in Linux and is in the .txt format.

[](https://img.wonderhowto.com/img/original/82/14/63537566090325/0/635375660903258214.jpg)

The default word lists available in Kali.

**Step 5Use Hydra to Crack Passwords**

In the example below, I am using Hydra to try to crack the "admin" password using the "rockyou.txt" wordlist at 192.168.89.190 on port 80.

[](https://img.wonderhowto.com/img/original/66/59/63537568270950/0/635375682709506659.jpg)

An example of using Hydra.

**Using Hydra on Web Forms**

Using Hydra on web forms adds a level of complexity, but the format is similar except that you need info on the web form parameters that Tamper Data can provide us.

The syntax for using Hydra with a web form is to use <url>:<formparameters>:<failure string> where previously we had used the target IP. We still need a username list and password list.

Probably the most critical of these parameters for web form password hacking is the "failure string". This is the string that the form returns when the username or password is incorrect. We need to capture this and provide it to Hydra so that Hydra knows when the attempted password is incorrect and can then go to the next attempt.

In my next Hydra tutorial, I will show you how to use this information to brute-force any web form including all those web cams, SCADA systems, traffic lights, etc. that we can find on [Shodan](https://null-byte.wonderhowto.com/how-to/shodan/).