

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] CISCO/Routers and switches gaining TELNET access Basics Questions just ask](#)

slober - October 1, 2014, 11:10 am

CISCO/Routers and switches gaining TELNET access

ShodanHQ
The Dorks
The steps
Access granted!

ShodanHQ

WikiMan Wrote:Shodan is a search engine that lets the user find specific types of computers (routers, servers, etc.) connected to the internet using a variety of filters.

Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client.

This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.

Shodan collects data mostly on web servers at the moment (HTTP port 80), but there is also some data from FTP (21), SSH (22) Telnet (23), SNMP (161) and SIP (5060) services.

It was launched in 2009 by computer programmer John Matherly, who, in 2003, conceived the idea of searching devices linked to the Internet.[4] The name Shodan is a reference to SHODAN, a character from the System Shock video game series.From:

[http://en.wikipedia.org/wiki/Shodan_\(website\)](http://en.wikipedia.org/wiki/Shodan_(website))

Thanks Wikipedia man ?

So why does it help me?

Let's take a closer look to what the WikiMan said:

Quote:Shodan is a search engine that lets the user find specific types of computers (routers, servers, etc.) connected to the internet using a variety of filters.

Simplified:

If we are search a Router or switch using the right keywords and some imagination :

Router/Switch telnet OR SSH acces

Gaining information(depending!)

Disclosing possible security gaps

Explaining with pictures: [\(Click to View\)](#)

from: <https://i.imgur.com/97oMlju.png>

Point of entry:

HTTP

Duh using the Dork

PHP Code

```
<?php
cisco OK country:"BE"
cisco OK country:"US"
cisco OK country:"NL"
cisco OK country:"FR"
```

we will enter the vulnerable Router/switch through our webbrowser enabling the Telnet access later on

Explaining with pictures: [\(Click to View\)](#)

from: <https://i.imgur.com/q9srgJq.png>

Telnet

after typing some shizle in config mode we will gain access to Telnet ^-^

from: <https://i.imgur.com/dNzgawS.png>

SSH

Same only more typing needed just stay with Telnet ^-^

The dangers:

Don't be a (...) send the admin a mail or reset the configuration back to normal otherwise risk of getting in trouble xD

Jail,Fine,.... just use common sense please ^-^

The steps

like mentioned earlier you should use the search engine ShodanHQ using prefixes like country:"FR" you could filter your results in this example i use cisco OK and the country Belgium

Cisco = Type/vendor of the device Switch or Router

OK = Reply from the web server OK means no authorization required on this site so a

(Possible)clean entry ^-^

country:"DE" = filter on country

Find a result you should need/seek for something like this:

Explaining with pictures: [\(Click to View\)](#)

from: <https://i.imgur.com/axvKnoM.png>

press configure you need this configuration mode to change the config files the following command should give you Telnet access:

```
Code line vty 0 15
```

```
password what578
```

```
login
```

```
exit
```

```
enable secret what5788
```

after you filled in all the commands you should have access ^-^

from: <https://i.imgur.com/dNzgawS.png>

Access Granted