

Forum:[Hack Forums](#)

Thread: [\[TuT\]Personal VPN -- Taking over the Router](#)

slober - April 12, 2015, 7:22 am

Personal VPN -- Taking over the Router

Tutorial
So?
Destroy Everything?
Small SOHO

Pre Tutorial

Please you should know what a vpn is what it does and what the risks are.
a few months ago I made a tutorial explaining this ^-^ take a look ?
<https://hackforums.net/showthread.php?tid=4402894>

So?
There are two types of attacks we could use both of them require searching a lot

Attacks:
Small Soho routers NO FLASH (N16R)
Small Soho routers FLASH (DD-WRT based ex. E1200 E2000,...)

Destroy everything?
No please don't destroy the routers you found if you found one you should even secure it better
maybe try to flash it to DD-WRT
enhancing the security on the router is only beneficial for your experience and beneficial for the
Users connected to the device.
after you setup the VPN connection you should consider putting the router back in the intranet and
kicking it out of the Internet
stop forwarding that ugly 80 port. it's the least you could do remember your using it as your VPN xD

Small SOHO?
Find a SOHO router (SOHO stands for SmallOffice HomeOffice)
aka the house routers (and smallOffice routers xD)

Finding it.
Shodan.io
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))

PHP Code

```
<?php
//some dorks:
RT-N16 port:"80"
E2000 port:"80" country:"UK"
E1200 port:"80"
WNR4000 port:"80"
```

PHP Code

```
<?php
//common default usernames:passwords
admin:admin //LINKSYS
admin: //D-LINK
admin:password //NETGEAR
root:admin //DD-WRT
root:root
root:
:
```

after you found a router you can flash it with DD-WRT enabling VPN shouldn't be a problem ^^

DD-WRT compatibility:

<http://www.dd-wrt.com/site/support/router-database>

- some routers have built-in VPN options like the RT-N16

Setting it up in windows:

Spoiler ([Click to View](#))

password: 1234567890

username: sam

It's for testing ^^

Step1:

Step2:

Step3:

Step4:

This can also be done on larger cisco routers but I'm Strongly sugesting you don't try this unless you are following a CCNA course (and you passed routing and switching)

More information about that:

<https://hackforums.net/showthread.php?tid=4470857>

-

ex VPN. location

China:

[IMG]http://www.speedtest.net/result/4284811776.png[/IMG]

Netherlands:

[IMG]http://www.speedtest.net/result/4284819082.png[/IMG]