Table Of Contents	1,	/3

## **Table Of Contents**

Table Of Contents	1
Further readings:	2

Further readings: 2/3

# nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format <a href="http://www.cyberciti.biz/">http://www.cyberciti.biz/</a>

Home > Faq > Security

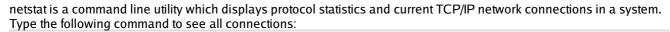
### Detecting DoS / DDoS Attack on a Windows 2003 / 2008 Server

Posted by Vivek Gite <vivek@nixcraft.com>

Question: How do I detect a DDOS (Distributed denial of service) / DOS attack on a Windows Server 2003 / 2000 / 2008? Can I use <u>Linux netstat command syntax to detect</u> DDoS <sup>[2]</sup> attacks?

Answer: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

You can always use netstat command to get list of connections under Windows. Open command prompt by visiting Start > Run > Type "cmd" in box.



netstat -noa

#### Where,

- 1. n: Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
- 2. **o**: Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager.
- 3. a: Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

You can use find command as filter to searches for a specific string of text in a file. In the following example you are filtering out port 80 traffic:

```
netstat -ano | find /c "80"
```

Find the IP address which is having maximum number of connection and block it using Cisco firewall or IPSec. Another protective measurement is to harden the TCP/IP stack [3].

## Further readings:

- More information about DDoS [4]
- FIND [5] and NETSTAT [6] command help pages.

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our <u>daily email</u> newsletter or <u>weekly newsletter</u> to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: http://www.cyberciti.biz/faq/

URL to article: http://www.cyberciti.biz/faq/detect-ddos-dos-attack-on-windows-server/

URLs in this post:

- [1] Image: http://www.cyberciti.biz/faq/category/windows/
- [2] Linux netstat command syntax to detect DDoS: http://www.cyberciti.biz/tips/netstat-command-tutorial-examples.html
- [3] harden the TCP/IP stack: http://msdn.microsoft.com/en-us/library/aa302363.aspx
- [4] More information about DDoS: http://en.wikipedia.org/wiki/Denial-of-service\_attack



Further readings: 3/3

- [5] FIND: http://technet.microsoft.com/en-us/library/bb490906.aspx
- [6] NETSTAT: http://technet.microsoft.com/en-us/library/bb490947.aspx

Copyright © 2006-2010 <u>nixCraft</u>. All rights reserved. This print / pdf version is for personal non-commercial use only. More details <a href="http://www.cyberciti.biz/tips/copyright">http://www.cyberciti.biz/tips/copyright</a>.