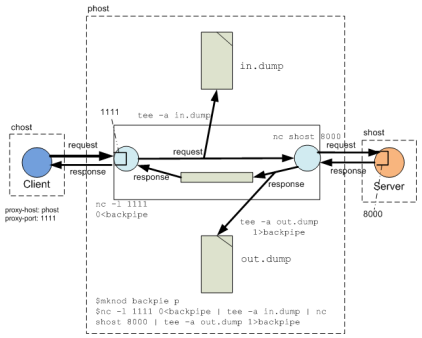
Pankaj Kumar's Weblog

Random thoughts, musings, experiences, ideas, and opinions

Using netcat to view TCP/IP traffic

There are times when you do want to see what bytes are flowing over wire in HTTP communication (or any TCP/IP communication). A good tool on Unix/Linux to use for this purpose is netcat (it is available as command **nc**), as long as you have the ability to set proxy host and post at the client side. This is best explained by the following diagram:



Let us say your client program running on machine **chost** is talking to the Server program running on machine **shost** and listening for connections at port 8000. To capture the request and response traffic in files, you need to do two things:

1. Setup a netcat based proxy either on a third machine **phost** or any of the client or server machines. The commands are shown in the above diagram (click to enlarge). The first command **mknod backpipe p** creates a FIFO. The next command **nc -l 1111 0<backpipe | tee -a in.dump | nc shost 8000 | tee -a out.dump 1>backpipe** does a number of things: (a) runs a **netcat** program that listens for incoming connections at port 1111, writes output to **stdout** and reads input from FIFO **backpipe**; (b) runs a **tee** program that write a copy of the previous netcat output to file **in.dump**; (c) runs a second **netcat** program that reads the output of the first netcat program, connects to the server program running on shost at port 8000 and forwards all data to the newly established connection. the response messages from this connection are written back to the **stdout** of this program; (d) runs a second tee program that sends the output of the second netcat program (ie; the response messages from the server program) to FIFO **backpipe** and also appends a copy to file out.dump. Data bytes written to FIFO **backpipe** are read by the first **netcat** program and returned to the client program as response message.
2. Specify the proxy host and port for the client. This can often be done without modifying the program. For example, most Browsers have GUI options to set proxy host and post; Java programs allow setting **http.proxyHost** and **http.proxyPort** system properties; and CURL based PHP programs have option **CURLOPT_PROXY**.

The request message gets captured in file in.dump and response message in out.dump

LINKS

- Home Page
- Professional Blog
- J2EE Security
- Self Publications
- Master Archive Index

SEARCH

Search this blog:
Search

ABOUT

This page contains a single entry from the blog posted on **May 17, 2010 5:49 PM**.

The previous post in this blog was My Experience being a MATHCOUNTS Coach.

The next post in this blog is Statistical Analysis of JEE 2009 Results.

Many more can be found on the main index page or by looking through the archives.

Subscribe to this blog's feed [What is this?]

Powered by Movable Type 3.33

on the machine where netcat based capturing proxy is running.

Posted on May 17, 2010 5:49 PM | Permalink

COMMENTS (3)

Hi, Nice to read about Netcat at your blog. I need help in using this procedure.

I want to capture request and response of a particular site at the client system for which I am trying to do the following.

To access internet in my browser's proxy settings I have 192.168.1.100:8080 as proxy ip and port number.

Now from terminal, I executed the command ,
#nc -l -p 12345 < pipe | tee outgoing.log | nc yahoo.com 80 | tee pipe incoming.log

Then in browser, I changed the proxy settings to localhost:12345 and accessed, yahoo.com, Immediately I see a request header on terminal as output to the netcat command,

I am now struck at this point. My yahoo.com page in browser is continuesly loading and not showing me any page, since localhost:12345 doesn't have internet may be.

Now how should I configure my netcat to send this request to my proxy 192.168.1.100:8080 and get the yahoo page in my browser as well capture the response in my log file.

Is this possible through this method which you are explaining?

Please guide me in achieving the above.

Please note: I am not doing anything illegal, for learning purpose only I am trying to do this.

Thanks
Indra

Posted by Indraveni Chebolu | June 21, 2012 1:40 AM

Hi, Nice to read about Netcat at your blog. I need help in using this procedure.

I want to capture request and response of a particular site at the client system for which I am trying to do the following.

To access internet in my browser's proxy settings I have 192.168.1.100:8080 as proxy ip and port number.

Now from terminal, I executed the command ,
#nc -l -p 12345

Then in browser, I changed the proxy settings to localhost:12345 and accessed, yahoo.com, Immediately I see a request header on terminal as output to the netcat command,

I am now struck at this point. My yahoo.com page in browser is continuesly loading and not showing me any page, since localhost:12345 doesn't have internet may be.

Now how should I configure my netcat to send this request to my proxy 192.168.1.100:8080 and get the yahoo page in my browser as well capture the response in my log file.

Is this possible through this method which you are explaining?

Please guide me in achieving the above.

Please note: I am not doing anything illegal, for learning purpose only I am trying to do this.

Thanks
Indra

Posted by Indraveni Chebolu  | June 21, 2012 1:42 AM

Hi, Nice to read about Netcat at your blog. I need help in using this procedure.

I want to capture request and response of a particular site at the client system for which I am trying to do the following.

To access internet in my browser's proxy settings I have 192.168.1.100:8080 as proxy ip and port number.

Now from terminal, I executed the command ,
#nc -l -p 12345

Then in browser, I changed the proxy settings to localhost:12345 and accessed, yahoo.com, Immediately I see a request header on terminal as output to the netcat command,

I am now struck at this point. My yahoo.com page in browser is continuesly loading and not showing me any page, since localhost:12345 doesn't have internet may be.

Now how should I configure my netcat to send this request to my proxy 192.168.1.100:8080 and get the yahoo page in my browser as well capture the response in my log file.

Is this possible through this method which you are explaining?

Please guide me in achieving the above.

Please note: I am not doing anything illegal, for learning purpose only I am trying to do this.

Thanks
Indra

Posted by Indraveni Chebolu  | June 21, 2012 1:42 AM

POST A COMMENT

You are not signed in. You need to be registered to comment on this site. Sign in

(If you haven't left a comment here before, you may need to be approved by the site owner before your comment will appear. Until then, it won't appear on the entry. Thanks for waiting.)