**Experiment 2:**

**Perform an experiment to grab a banner with telnet and perform the task using Netcat**

**Banner Grabbing**

Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. Tools commonly used to perform banner grabbing are [Telnet](http://en.wikipedia.org/wiki/Telnet), which is included with most [operating systems](http://en.wikipedia.org/wiki/Operating_systems), and [Netcat](http://en.wikipedia.org/wiki/Netcat).

**What is Telnet?**  
Telnet is a user command and an underlying [TCP/IP](http://searchnetworking.techtarget.com/definition/TCP-IP) [protocol](http://searchnetworking.techtarget.com/definition/protocol) for accessing remote computers. Through Telnet, an administrator or another user can [access](http://whatis.techtarget.com/definition/0,,sid9_gci211510,00.html) someone else's computer remotely. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific [application](http://searchsoftwarequality.techtarget.com/definition/application) and [data](http://searchdatamanagement.techtarget.com/definition/data) on that computer.

**Steps for banner grabbing using telnet:**

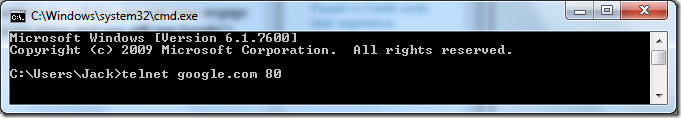
**Step1:**

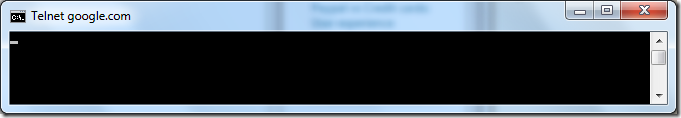
1. Go to Command Prompt
2. Type telnet followed by IP Address

Example:

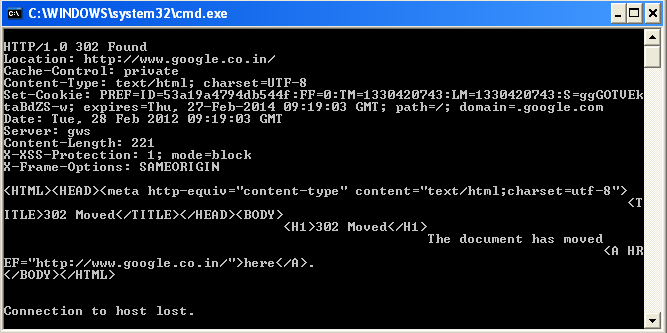
telnet google.com 80

As an example lets see if Google.com has port 80 (HTTP) open …

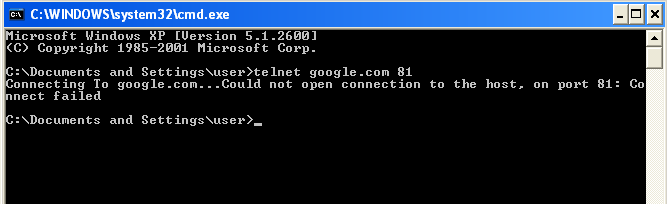
[](http://jack.ukleja.com/wp-content/uploads/image2.png)

[](http://jack.ukleja.com/wp-content/uploads/image3.png)

1. If you get a blank screen with a blinking cursor you have successfully connected to that TCP port.
2. Now type following request **GET HTTP** and press enter and you will see Google’s home page being sent to you.



On the other hand if the TCP port is not open or not reachable you will see this:

****

**Steps for Banner Grabbing using Netcat :**

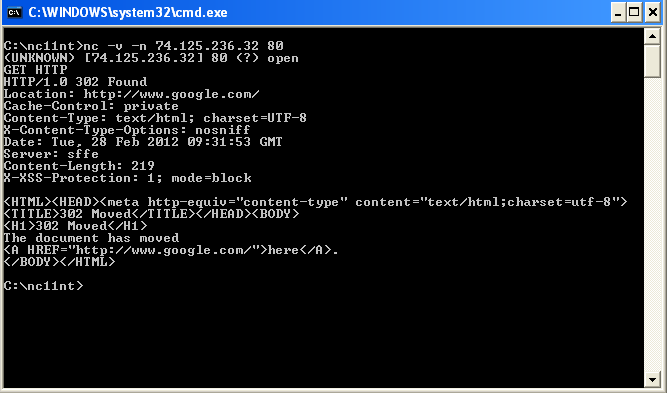
**Netcat:Netcat is a featured networking utility which reads and writes data across n/w connections.,using the TCP/IP protocol.It is designed to be a reliable “back-end “ tool that can be used directly or easily driven by other programs and scripts.**

**Step1:**

How to work with Netcat:

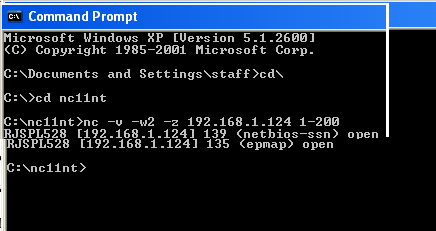
1. Go to Command Prompt
2. Copy the folder nc11nt to c:/ from the netcat s/w
3. In (C:\nc11nt\)
4. Type nc –v –n 74.125.236.32 (google.com) 80
5. You will get a blinking cursor that you have successfully connected to that TCP port.
6. Type **GET HTTP.**

We can see the details of our target web server.



Example 2:

C:\nc11nt\nc –v -w2 –z 192.168.1.124 1-200



**Netcat command options:**

1-e prog inbound program to exec [dangerous!!

2 -i secs delay interval for lines sent, ports scanned

3 -n numeric-only IP addresses, no DNS

4 -o file hex dump of traffic

5 -p port local port number

6 -r randomize local and remote ports

7-s addr local source address

8-t answer TELNET negotiation

9-u UDP mode

10-v verbose [use twice to be more verbose]