SELECTED STADIUM
SOLUTIONS

Category: Network Traffic Analysis
Bracket: Bronze
Title: Telnet Challenge **SOLUTION**

This challenge evaluates the participant's ability to understand a packet capture containing Telnet traffic - https://www.dropbox.com/s/ydd6mqhkoerxtfz/NCL-2015-Telnet.pcap?dl=0. During the game, it was suggested to use the Wireshark program to solve the challenge.

1. What is the username that was used?	**test**
2. What is the password that was used?	**capture**
3. What command was executed once the user was authenticated?	**uname**
4. In what year was this capture created?	**2011**
5. What is the hostname of the machine that was logged in to?	**cm4116**
6. What CPU architecture does the remote machine use?	**armv4tl**

Questions 1-6 can be solved by following the TCP stream on any of the packets. Keep in mind that telnet will echo back what is typed (except for passwords). Following the TCP stream yields the following:

```
........... ..!.."..'.....#.... ..#..’

.....#.....'.............P......

.38400,38400....#.Sandbox:0.0....'..DISPLAY.Sandbox:0.0......xterm...
...login: tteesstt
.
Password: capture
.
$ uunnaammee --aa
.
Linux cm4116 2.6.30.2-uc0 #3 Tue Feb 22 00:57:18 EST 2011 armv4tl unknown
$ ...
$ eexxiitt
.
logout
```