Network Traffic Analysis

Telnet (Easy)

This challenge evaluates the contestant's ability to understand a packet capture containing network traffic using the HTTP protocol. It was suggested to use the Wireshark program to solve the challenge.

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
```

Question	Answer
What is the username that was used?	test
What is the password that was used?	capture
What command was executed once the user was authenticated?	uname
In what year was this capture created?	2011
What is the hostname of the machine that was logged in to?	cm4116
What CPU architecture does the remote machine use?	armv4tl

© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.