Hint 2

ARP spoofing/ poisoning (http://en.wikipedia.org/wiki/ARP_spoofing) is a technique which can be used for man in the middle (http://en.wikipedia.org/wiki/Man-in-the-middle_attack) attacks. You can use **Cain** for arp-poisoning and performing man-in-the–middle attacks. Once you are in the middle of the two chatting PCs you can easily sniff their traffic and get the encrypted message. One tool called **wireshark** can be used for sniffing the TCP packet (**64 bytes** of data) that flows between the chatting PCs.

The main problem is that you, can only poison and perform man-in-the –middle attacks if the PCs lie in your local area network. However the chatting PCs are in a different VLAN, so you must hack the telnet interface (configured with a weak password) of the switch and then change you VLAN to enter the chatting PC's VLAN, ie VLAN-PC. Again the password can be easily brute forced.

Note however that Brutus should be configured properly to brute force telnet interface of cisco switch. You should note the behaviour of switch when one telnet's it using telnet <switch's IP>. It asks for password thrice and then shows *%Bad Passwords*. This is known as authentication sequence. You can feed this authentication sequence in Brutus and crack the password or there's an easy way out using BAD files or preconfigured files. Download this file (for cracking cisco) from internet and import it in Brutus and perform the attack.

These commands can be used to **change your VLAN**, once you obtain the password

Switch# conf t
Switch(config)# Interface gigabitEthernet 1/0/x
Switch(config-if)#switchport access vlan 30
Where x = team number

Then change your ip address to 192,168.30.y
Where y> 4

Then apply **chatting server.bat** to access internet again..