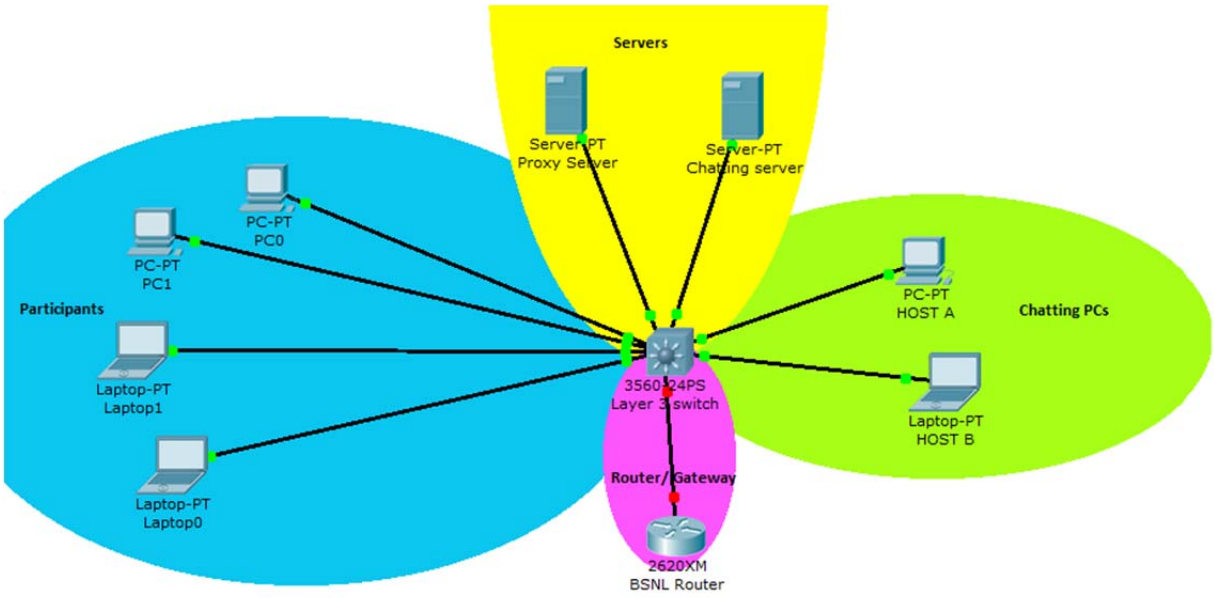
Hello sir,

Every year in Charvyuh as well as in Aranya we have events related to coding like knight codes, bug debugging, reverse gear etc. Organizers as well as participants learn a lot from these successful events. We wish to expand this learning horizon to networking and are planning to set a new trend in university by organising an overnight hacking event. For that I have come up with an idea and want to consult with you for feasibility in regard to permission, equipment required or any other issues. Apart from that kindly help us with you suggestions or some other idea, if possible.

This is the scenario.

1. We will take a layer 3 cisco switch and configure 4 VLANs (named as P, S, PS, CS) on it. Inter VLAN routing is enabled. The scenario will be roughly as below.



Two PCs are chatting with each other using 32-bit encryption key which is impossible to break. These PCs have got their common key from chatting server which has a web interface. The users wanting to participate in chat are given a 'chat name' and 'password', which they can share. People who have this password can get the 32-bit encryption key and participate in chat. Careless users A and B created a chat with just a small insecure password.

2. Participants are expected to break this password using brute forcing. Having obtained the key, they will log in layer-3 switch (again break password of router using brute force). After logging in they will reconfigure their port and add themselves to VLAN of two chatting PCs (VLAN CP). Then they will do ARP poisoning to render the switch as a HUB and listen to traffic of chatting PCs. Having obtained they will decrypt the data using 32bit key.

3. Decrypted data will contain another 32bit key which is used for login of router interface. The goal is to edit the access control list in router and unban the otherwise banned site (www.yahoo.com). But the router logs in all details of logged PCs. So the administer can catch them afterwards.

4. To make them safe they will search for a victim (There's a careless proxy server lying). The hackers should intrude through the proxy server into the router web interface and change settings there to unban the banned site. So they wont be caught.

Requirements:

We will make an isolated network with a switch and participants will bring their own laptops and plugin their LAN wires into the switch.

1. We will require a Cisco layer 3 switch.
2. For router I have a BSNL router, I hope it will work.
3. We will manage LAN wires as well.
4. We can manage servers as well.

To make the event a learning experience, we will drop hints regularly (say every hour) in a proper manner (in the form of pdf documents containing diagrams etc) which will help them in the event. The hints will be such that at the end of event everyone will be able to complete the task and learn from it.

What students will learn from the event?

1. Organizers/ participants will practically configure cisco switch.
2. People will get a basic idea of intrusion and how they passwords can be brute forced and why should one have a strong password.
3. How does network work in a whole and how can one sniff network for passwords.