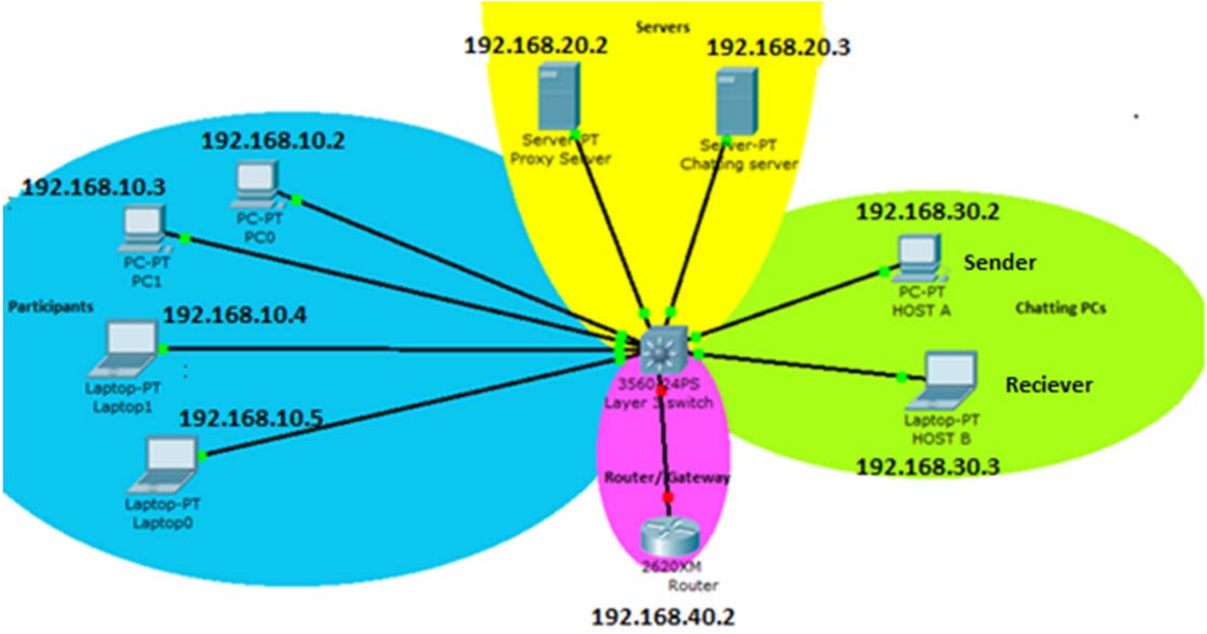
Hack Pack – Overnight Hacking Event

Scenario



The network in the LAB is topological similar to the figure above. There are four VLANs (see the references section for a brief description of VLAN)

- P – **P**articipants VLAN
- S – **S**erver's VLAN
- CP – **C**hatting **P**Cs VLAN
- R – **R**outer's VLAN

These VLANs are created on Catalyst 3750 series (Cisco Layer-3 switch) with inter-VLAN routing enabled, which means you will be able to ping all PCs in the scenario. The router hooked in VLAN-R will make your way to internet as well.

In the participants VLAN you are hooked on an interface of an L-3 (layer-3) switch which is of the form of

GigabitEthernet 1/0/{your team number}

Suppose if your **team number is 3**, the interface of the router on which you are connected is

GigabitEthernet 1/0/3

Problem

The router connected in VALN R, which makes your way to internet, may implement many constraints like banning some sites or implement access lists. So this gateway router is of prime interest to a hacker. The hacker managing to gain access to this router can make things go as per his will.

The problem is that as in practical scenarios the administrator has protected the router with a strong password (almost impossible to crack). This router has a web interface and a telnet interface whose user name is *admin*. Your job is to obtain password of this admin account of the router and gain admin rights for this router.

Now as stated, the password is this account is almost impossible to break. So the hacker has to try an alternate route for obtaining the password. The PC of the administrator is attached in the VLAN-CP, who sometimes chats with other technicians and tell them the router's password. The message reads as ----

hello bob the password is ***********

If the hacker can somehow intercept this message he can obtain the router's password from the message. But there is another problem, the administrator happens to be clever here. He is using a secured chat service, which **encrypts** the chat with **Serpant CBC algorithm** whose output is **encoded** with **base64 algorithm**, which is again impossible to break.

After intriguing a bit, the hacker finds out that the chat service, which gives the strong key to the administrator, is located nearby labelled as **Chatting Server**. Chatting server has a web interface and provides chatting candidates **a strong random key** for each session (common for all participants of the chat) with the help of which they can chat securely. This key is obtained by the chat client automatically, when the chat starts. The chat client can obtain the key only after authentication with the chat server, so people who know the chat password can let their clients obtain the key and participate in chat.

Luckily the administrator threw precautions in the air and created a chat with a weak password, which can be easily cracked using dictionary based attacks. This is the chat that the administrator created ---

Uname – **chat1** (all chats are created with similar names)
Pass – unknown but can be cracked

The hacker can crack the password and enter the web interface of the Chat Server (try opening web interface of chat server, see ip address in the figure). Having entered, the hacker will obtain the key with the help of which he can easily decrypt (there are online tools available) the message of the administrator and obtain the router's password from it.

Now the hacker can enter the router and play with the configuration as per his needs. But the hacker needs to be careful because the router/gateway (as in many practical scenarios) **logs** access to it. These logs and help the administrator to trace the hacker and get him caught. The hacker can look around for some victims, possibly people who have misconfigured their PCs and intrude through them.

Furthermore, cisco L3 switch (check its ip-adderss in the figure) used in the problem has a telnet interface. Unfortunately again life is not so simple, the telnet interface is protected with a password but the password is weak and can be cracked. The administrator has not enabled any privilege mode password on the router and the after the telnet login, the privilege mode is returned straight.

Possible steps that can be followed for cracking the problem

1) Crack the password of the chatting server and obtain the **key**.
2) Having obtained the key, trick the administrator by sniffing the message.
3) Having obtained the message, decrypt it and get the router password.
4) Search for the possible victim and get into the configuration of the router.

Directions/ Rules

1) You are not supposed to hinder other's movement by performing DOS (Denial of Service) attacks against other participants or infrastructure (servers, etc.).
2) After each step you can inform organizers, so that we can make a note of time.