1 Intro

Der iCTF (international Capture The Flag) wird jährlich von der University of California, Santa Barbara veranstaltet und ist der gröSSten Hackerwettbewerbe dieser Art. Der iCTF integriert Angriff und Verteidigung zugleich. Die Teilnehmer müssen gleichzeitig Flaggen von fremden Servicen klauen, sowie ihre eigenen Service patchen um diese unangreifbar zu machen. Dieses Jahr fand der Wettbewerb am 04.12. statt und ca. 40 Teams nahmen daran Teil. Dabei belegte unser Team (in23canation) den 22. Platz. Die Dauer des Wettbewerbs wurde mit 24 Stunden angekündigt jedoch kurz vor dem iCTF auf 8 Stunden reduziert. Die Stimmung beim Wettbewerb war durchgehend positiv und insgesamt war der CTF ein groSSer Erfolg. Durch etwas Werbung vorab war es möglich eine groSSe Teilnehmerzahl aus allen Semestern zu begeistern sich unserer Gruppe anzuschlieSSen. Schon bei den zwei vorangehenden Informationsveranstaltungen waren ungefähr 60 Studenten anwesend. Beim iCTF selber waren rund 25 Teilnehmer aktiv dabei.

1.1 Network-Setup

The setup of the iCTF 2015 is shown in the graphic 1.1. The Router has a private VPN running, tunneling all traffic through the THI-Network. Also the Router creates 2 sub-networks. The ”bad network”(shown in red) holds the iCTF-Router and vulnerable VM, as well as some attacker PCs, which will run the exploits against other teams. In the ”good network”(shown in green) are the participants, who have a local copy of the vulnerable Image and develop patches and exploit. It’s to mention, that the router has ip-tables-rules specified, so the ”bad network”can not communicate with the ”good network”. Also, the Attacker-PCs have to route their traffic through the CTF-Router. This should be solved differently in the upcoming CTFs, since the separation of the 2 networks needed a lot of time to be configured.

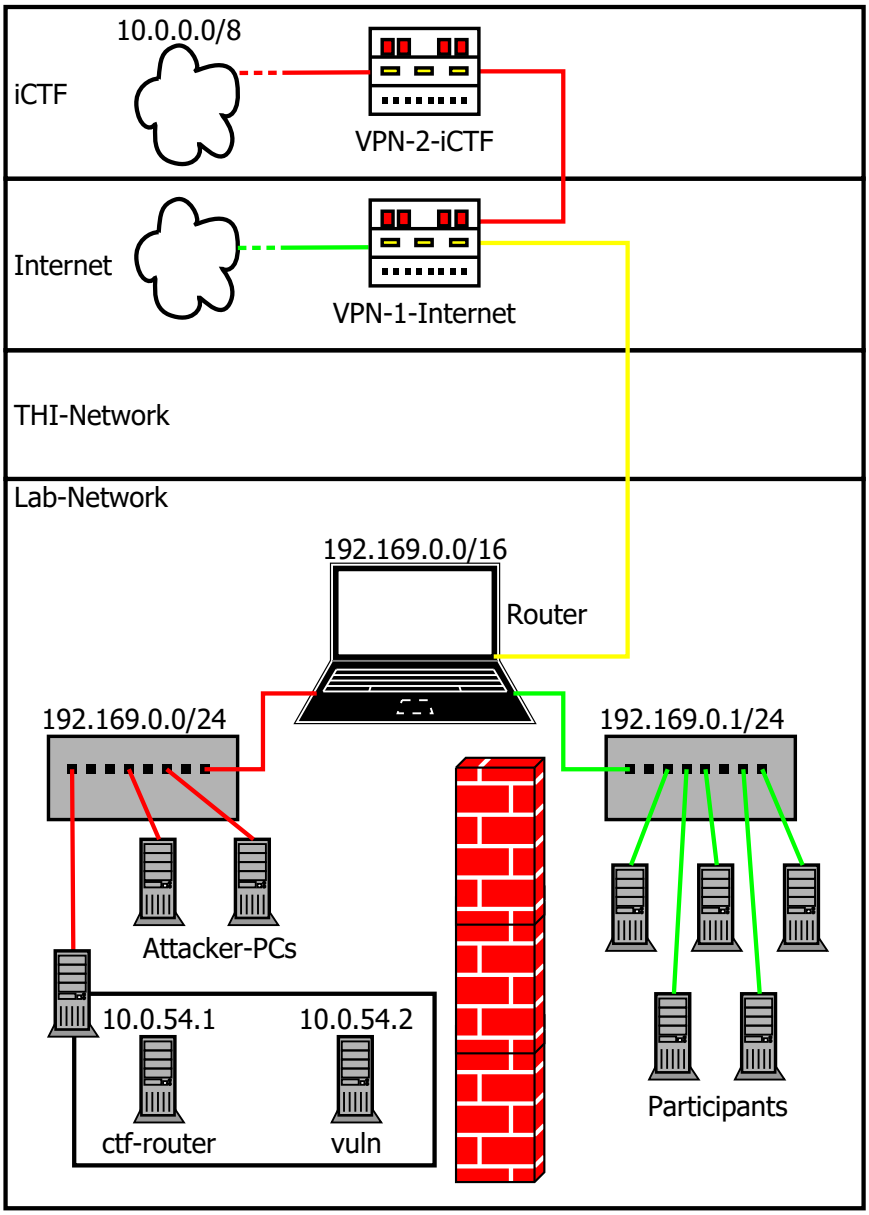

Abbildung 1.1: Network-Setup iCTF 2015

2 Dungeon

2.1 Services: Dungeon

The Dungeon service was a consoleservice which presented a litte game. The player needs to run through the dungeon to finally kill a dragon in the end. To do this, two items are needed. Firstly a golden sabre and second a magic shield. If either of the items is missing the player will die to the dragon. To get the sabre the player needs to find a secret room and in there has to get the name of an airplane picture right. If he does he will get the sabre. Now the player will get in a room with a dwarf. He says if you get the number i guess you will get my shield. But the number he has is random generated and nearly impossible to get right. Also if you get the number right he will tell you that he gives you the shield but the variable HAVE_SHIELD will not change. To achive the shield the player has to go to a room with a gnome which asks the player's name and then says Hi! playername. In this function there is an adress returned with the variable HAVE_SHIELD. So the player need to type in anycharacter than %n so that the adress will be overwritten with 0x1. If the player encounters the dragon with both items he can slay the dragon with the command "kill dragon". After that he will be asked what his name is. Here comes the tricky part. With a Bufferoverflow it is possible to alter the return adress so that the function will jump to the secret treasure room where the flag can be optained. To do this the player have to type 88 random characters followed by 0xDEADBEEF in ASCII than 8 random characters again and then the adress to the storage room. The 0xDEADBEEF is needed because a value is checked for change. If you overwrite it with the bufferoverflow the service will disconnect the player. Both 0xDEADBEEF and the return adress have to be turned because little Endian is used.