Assignment I: Breaking established TCP connections with RST

CS3006D Computer Networks

CSED NIT Calicut

Group Submission Due date: January 19, 2022

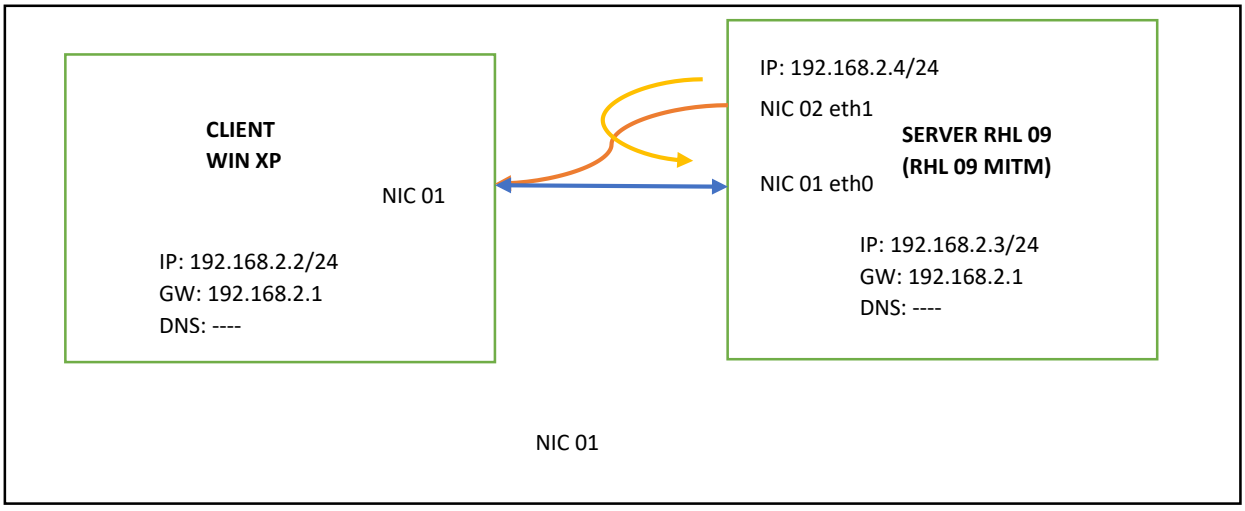
Video Submission due Date & Online Quiz: February 06 & 14, 2022 (Tentative).

Acknowledgement/Source: This assignment question is taken from Prof. Sandeep Kumar, who was my faculty. He is presently working in VMWare, USA. For those who are interested in his research in Cyber Security, please refer his Ph.D. thesis from link.

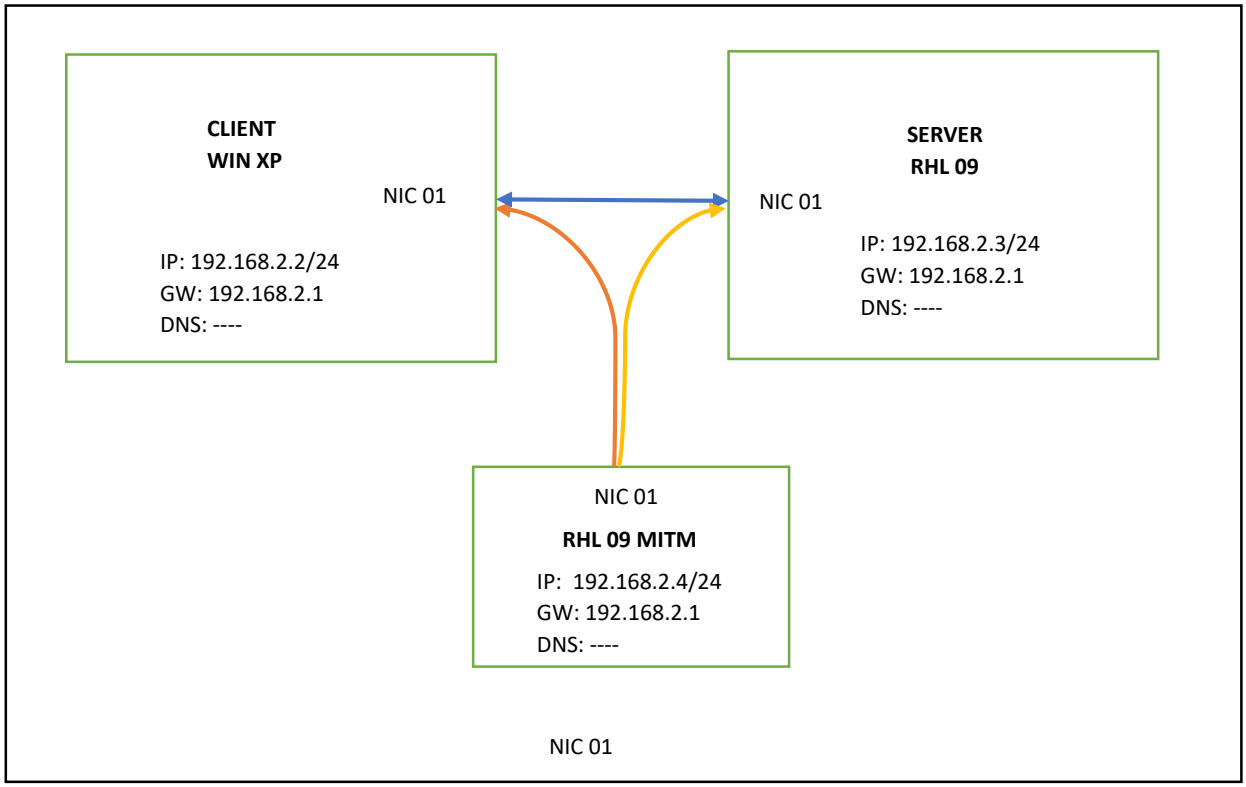
This assignment could be done in groups of size 1 to 3. I prefer you to do it individually in each of your laptop, if your laptop configurations supports it, so that you get a clear understanding. The assessment evaluation would be done based on the video that you records and submit, that demonstrates breaking an active TCP connection, followed by an Online Quiz, where the questions relating to the assignment will be asked. There is no written material to be returned with this assessment. The video has to be shared via google drive, by attaching it as email. I will be posting the details later.

After completing this assignment, you will get a feel for how to generate TCP packets and push that into network. There are powerful libraries available for the creation and injection of arbitrary packets into the network, which can be used to significantly simplify the coding effort needed to create such attacks. One such library is the libnet (http://www.packetfactory.net/projects/libnet) packet creation and injection library written by Mike Schiffman. While you won't be required to code using the library in this lab, you will profit considerably from understanding how to use the API (in your spare time), perhaps by writing a general-purpose traffic generator with it.

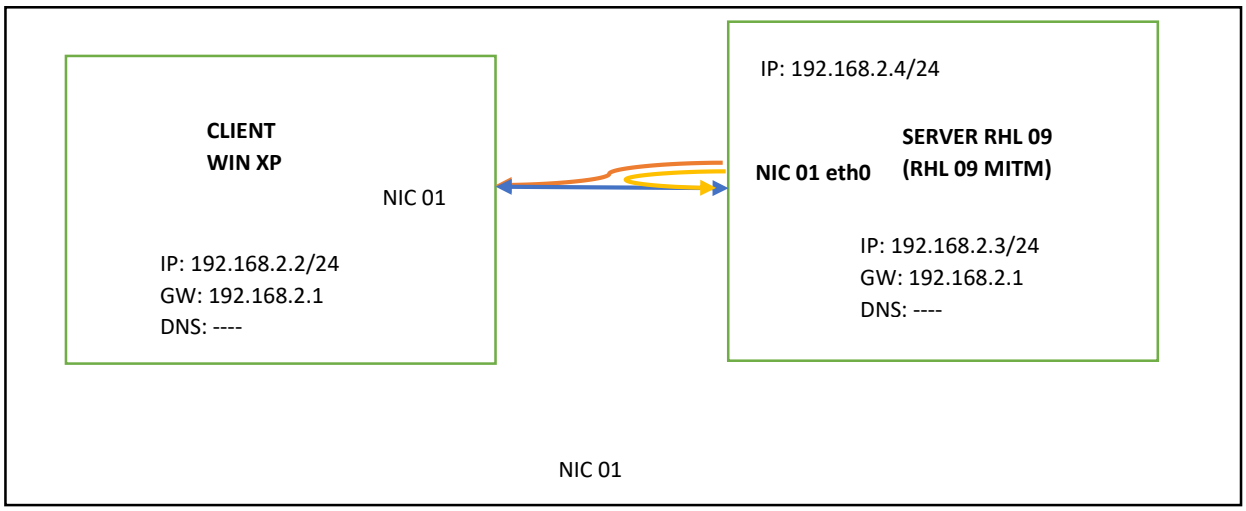
Network Diagram – with Static IP addressing (Basic for systems with less RAM)



Network Diagram – with Static IP addressing - MITM Attack –Ideal Scenario (Recommended)



Network Diagram – with Static IP addressing (Minimum Architecture for systems with less RAM)



You have to use **Internal Network (intnet)**, for setting up this network. Any updates/package download to the VMs has to be done using Bridge / NAT setting. Before trying for this attacks, the virtual network between the VMs has to be totally isolated from internet. You should use only **Internal Network setting** while doing this attack/demo.

For this lab, you will use hping2 / hping3 to generate a TCP packet that breaks a quiescent TCP connection. When a TCP connection is in the ESTABLISHED state, a RST packet received by either endpoint's TCP within the receiver's receive window signals that the other end wants to immediately break the connection. If an active attacker knows or can guess details about a TCP connection's current

window, then he can break it by generating a spurious RST packet and sending it to either the source or the destination. You will download and install hping2 from http://www.hping.org/hping2.0.0-rc3.tar.gz on the **RHL 09 MITM** machine for your use with the lab. Figure out the command line arguments for hping2 that will generate a TCP Packet with help of hping documentation from https://cyberwar.nl/d/cheatsheets/hping3_cheatsheet_v1.0-ENG.pdf.

What you will do

Create a TCP connection between two machines, say A (a Linux box) and B (a Windows box) or both Linux boxes. A TCP connection can be made by either telnetting from one to the other or by logging in using ssh. Run Wireshark on one of the machines (here always in Windows) to determine the sequence number of the next expected datagram from A -> B / B->A when the connection is quiescent. Invoke hping2 with appropriate arguments to break the TCP connection (ORANGE and YELLOW lines demonstrate how the RESETING has to be done). You should be able to break the connection at A's end in first demonstration and at B's end in second demonstration. Explain what's going on. Do you need a special value for each of the header fields in the TCP packet, or does any value work? If you need a special value, what are the values conceptually?

Review questions

You don't have to submit answers to these in writing, but you must be prepared to answer them and other similar questions in the scope of this assignment.

1. What is the kind of attack you are performing in this assignment referred to in the computer network literature?
2. TCP understands six code bits: URG, ACK, PSH, RST, SYN, FIN. Explain the purpose of each.
3. Why do we need the src_ip and src_pt numbers when constructing the attack RST packet? Why isn't it enough to just send a RST packet to the correct destination and port number? Will the RST packet generated, without giving the source ip and source port works in any of the above scenario?
4. What is the importance of window size in the above attack? What is the range of value that I could select from the window size for generating RST attack? How it impact the attack?
5. Why do we need to estimate the sequence number of data traffic in one direction (any direction is fine) before generating the packet? Why doesn't an arbitrarily constructed RST packet work?
6. Describe the purpose of the DF and MF bits in the IP header?
7. Describe how the ping of death datagram can be constructed.
8. In SYN cookies, describe how the ISN is generated by the receiver (server). Note that the ISN from the client is ignored when computing the cookie value. Does it matter? When the client sends the final ACK, he can change his initial ISN. Does it matter?
9. Why are there ACK storms in Laurent Joncheray's TCP hijacking scheme?

Link for downloading earlier version of Redhat Linux 9 is http://archive.download.redhat.com/pub/redhat/linux/9/en/iso/i386/. It just requires 256 MB of RAM, so anyone who have 512 MB of Extra RAM could do this assignment easily without any headaches / issues.