HOME ASSIGNMENT 1 Deadline: 6. March. YOUR NAME: NEPTUN CODE:

Task 1

Construct a TCP port scanner from TCP port 1 to TCP port 2000 and observe which ports are open. Verify your findings also with the *netstat* command!

Useful tips:

1. For unknown concepts or terminology use the Google and Wikipedia :)
2 Get two routers in GNS3 and connect them!
3 Give IP addresses to each of them
4 Send TCP SYN packets from one computer to another using Scapy. Use for example a *for* cycle to send multiple packets with one complex command. When the other computer answers you can tell if the port was open or not (depending on the answer if it is a TCP SYN+ACK (S.) or TCP RST+ACK (R.)).

+1. If you use the *sr* command with the *dport* option (giving multiple port numbers separated with commas or an interval) then the task can be made even more simple.

+2. You can verify your final result by checking the receiving computer on the opened ports by using the *netstat* command

Task 2

Perform a TCP SYN attack against another computer in GNS3. Analyze the packet using the tools *tcpdump* and *netstat*!

Useful tips:

2. For unknown concepts or terminology use the Google and Wikipedia :)
1. Get two routers in GNS3 and connect them!
2. Give IP addresses to each of them
3. Check the receiving computer about opened TCP ports (*netstat -atn*), or open a port by yourself (use the *nc* command)
4. Send the appropriate TCP packets (i.e. the SYN packets) using Scapy!
5. Check carefully the packet that the receiver sent back: If it sends the flags: “R.” , than it means the port was closed, so the attack did not complete. The right answer is “S.”!

+1. You have two options: IF you give a fake source IP address when sending the SYN packet, than you have nothing to do further, BUT IF you let it unchanged, then when you send a TCP SYN packet from computer *A* to computer *B*, then computer *B* send back a SYN ACK in response. Now the IP protocol stack in computer *A* surprises as it did not send any SYN packet (as you did using Scapy), so it answers with a TCP RST. In that way, however, computer *B* closes the TCP channel properly, so the SYN attack is not succeeded. To avoid that you should filter out that TCP RST message on the output port of computer *A* by using the following firewall command:

```
iptables -t raw -A OUTPUT -p tcp --tcp-flags RST RST -j DROP
```

A sample topology (it is suggested to use the given OpenWrt routers in GNS3 for both computers, although it would work for any computers that has an IP protocol stack):