IIT PALAKKAD

COMPUTER SCIENCE AND ENGINEERING
Indian Institute of Technology, Palakkad
CS3210: Computer Networks Lab
Lab 2 (HTTP, FTP and SSH)

05 Aug, 2019

Time: 3 hrs

1. Set up the virtual network for this lab. This network has 8 VMs namely **h1**, **h2**, **h3**, **h4**, **h5**, **r1**, **r2** and **r3**. The first 5 VMs are hosts and the rest are routers. In this lab, you only have access to machine **h1**, and the goal is find out a message stored in host **h4**.

   (a) Connect to host **h1**. Ensure that you are able to ping ***x***.*virtnet.com* for all $h \in \{h2, h3, h4, h5\}$. Send 5 ping packets to each of these hosts and report the respective average round-trip time. [10]

   (b) Host **A** is running a FTP server, whereas Host **B** is simultaneously running two HTTP servers on port numbers in the range 8000 to 9000. Identify hosts **A** and **B**. What are the incoming ports of the HTTP servers on host **B**? [10]
   Can be seen using "nmap -p- h2.virtnet.com"
   A = h2.vi... B = h3.vi... and Port 8143, 8534.

   (c) Let us call the HTTP servers running on host **B** as **S1** and **S2**. On each of these servers there are two text files (within some directory). Download these files. *Hint: directory listing is enabled on these servers.* Each of these files contains one half of the password needed to log into the FTP server on host **A**. Write down this password. [10]
   wget h3.virtnet.com:port/dir
   Pass = "use" + "r@487"

   (d) One of the HTTP server on host **B** runs *HTTP/1.0* and the other runs *HTTP/1.1*. Match the port number of the servers to corresponding HTTP versions. [10]
   "wget --server-response --spider h3.virtnet.com:Port" Spider is used to avoid downloading.

   (e) Using command **lftp**, FTP into host **A** using username "tc" and the password obtained in step (c). There is a file called "sol.txt" (within a directory) on this machine. Download it and look at its contents. This file contains the password for user "tc" on host **h5**. Write down this password. [10]
   Simply using lftp

   (f) SSH into host **h5** using username "tc" and the password obtained in the previous step. There is file with the extension ".pcapng" in the home directory of user "tc". What is the name of this file? [10]

   (g) Download this file to your physical host machine (*Hint: host **h5** can be accessed via SSH on port 14505 on the loopback IP address of the physical host*) and open it with wireshark. [10]
   scp -P 14505 tc@localhost:my_capture.pcopy ~/Desktop

   (h) What you now see in wireshark is a sample packet capture. During the capture, a website was pinged, which host was pinged? What was the IP returned after DNS resolution? How many ping response packets were received? What was the minimum response time for these packets? [10]

   (i) During the capture, a website was also visited using a browser. What is the hostname of this website? A file was also downloaded from this website. What was the name of this file? The password of host **h4** for user "tc" is embedded within HTTP GET requests send during the packet capture. Find out and write down this password. [10]

   (j) Connect to **h1**, and then ssh to host **h4** with the user name "tc" and the password obtained from the previous step. The final message is placed within a text file in the home directory of user "tc". What is this message? [10]

End of paper