Networks and Systems Security - Winter 2019

Sambuddho Chakravarty

April 15, 2019

Homework Assignment 5 (total points:40)

Due date: April 30. Time: 23:59 Hrs. (No extensions)

1 Simple TCP port scanner (Mandatory) (total ponints: 40)

The final assignment is primarily to familiarize you with two important things – NMAP network reconnaissance tool and Linux/FreeBSD Raw Sockets. You need to start out by reading and trying out the NMAP tool (site:`https://nmap.org/`) and about how to craft your own packets using SOCK_RAW sockets. The following resources may come in handy:

`http://man7.org/linux/man-pages/man7/raw.7.html`
`https://opensourceforu.com/2015/03/a-guide-to-using-raw-sockets/`

The objective for you is to create your small little rudimentary port scanner which should emulate two different TCP port scans supported by NMAP. You need to test its functionality on a VM. You require to test it by probing another VM using the former, using your own tool. The latter VM should have some TCP services (*e.g.* web, SSH or some other service running).

1.1 How you would be graded:

1. Correctly compiled programs (both client and server) (via a Makefile) – 5 points.
2. Correct functioning of the port scanner using the SOCK_RAW API and should produce the same outcomes as that of NMAP program – 30 points.
3. Documentation describing the system design and the assumptions made – 5 points.

2 Extra Credit Problem 1 (points: 20)

You need to a add the functionality of UDP scanning your above tool. UDP does not support the control messages or flags relevant in TCP. You need to

thus figure our how to identify open and available UDP services on a target host using your tool. NMAP has built-in support for identifying UDP ports. You need to determine how that works and need to implement your own UDP scanner (as a part of your own rudimentary port scanner).

3 Extra Credit Problem 2 (points: 20)

In you lab exercise 6 you worked with L2TP and managed to integrate it with IPSec. You would now require to send configure PPTP to run over Tor and make sure the PPTP client communicate so the PPTP server over a private Tor network which you need to set-up with VMs. The private Tor network would require three VMs, each one acting as entry, middle and exit nodes respectively. Further, you would also require two directory server nodes and VMs as client, servers and PPTP client and server, as shown in figure 1

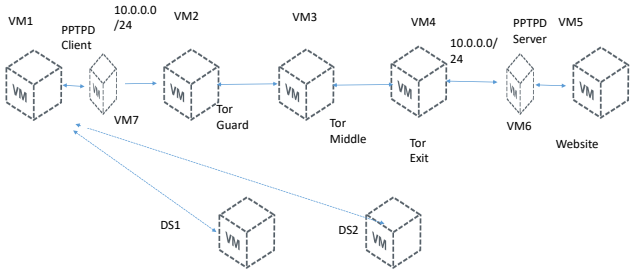

Figure 1: PPTP tunnel over Tor Circuit