TCP/UDP Port Scanning Using Python/Scapy

1.0 Objective

TCP and UDP port scanning is a method of determining what applications a host is running. You will develop 2 Python programs using the SCAPY module to scan TCP and UDP ports on the external router **rtr** (10.10.111.1) in VLAB.

For TCP you will scan all the ports from 0 to 100. You will collect the responses and sort them by their status of OPEN, CLOSED, FILTERED. i.e. OPEN:1, 2, 3, ...; CLOSED: 8, 9, ...;FILTERED: 11, 12, ... You should account for dropped packets. If you send out a TCP/SYN packet and get no response you should send out another as the packet may have been dropped.

For UDP you will also scan all the ports from 1 to 100 and collect the responses by their status of OPEN and CLOSED. Remember to account for packets being dropped. With UDP, no response means either the port is OPEN or the packet was dropped. You should send out additional UDP packets to verify.

For an open UDP port found OPEN on rtr, lookup the service name associated with the port number and send a well-formed UDP packet using scapy for that service to the port to verify it is running a service and what that service is. Look up service names and transport protocol numbers from the number registry in iana.org. You only need to do this for ports that you found OPEN on rtr. http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Tip: Use wireshark or tcpdump may assist you in writing your program.

2.0 Lab Setup

Turn on the router **rtr** and the **backtrack5** machine. You will be scanning the **rtr** computer. You will code your program on the backtrack5 machine using Python and SCAPY. The start of your program should be:

```
import sys
from SCAPY.all import *
```

3.0 What to Submit

Write a lab report describing your results. Each Python program should be submitted as a Python program i.e. ***<name>.py***, followed by a screen shot showing the output of the Python program. You may submit all programs as one file.

- [30 pts] Your Python TCP scanning program.
- [30 pts] Your Python UDP scanning program.
- [30 pts] Your Python/SCAPY program for UDP service name discovery.
- [10 pts] Screenshots of the output of all programs.

Note: A lab report descripting describing all your activities and detailed workings of the code is required.