CISC 367 – Spring 2016

1 Port Scanning in Nmap

Refer to Port Scanning Techniques and set up necessary (Linux and/or Windows) VMs to demonstrate the following scans.

- TCP SYN scan
- TCP connect scan
- UDP scan
- TCP NULL, FIN, and Xmas scans (with target Windows VM)
- TCP ACK scan
- TCP Window scan
- IDLE scan
- IP protocol scan
- FTP bounce scan

2 Extra credit: Implementing IDLE Scan in Python

Study the TCP Idle Scan (-sI) of Nmap and implement the same fuynctionality in Python, and demonstrate your implementation via Linux VMs.

You may need to investigate IP spoofing in Python.