CIS4360 – Security Fundamentals **Spring 2025**

Homework 1: Deadline Monday 3/17

Instructor: Viet Tung Hoang

1. (**DoS attacks**) (60 points)

a) (30 points) You want to perform a DoS attack against some host with a known IP address. You have become aware that a mis-configured sub-network, corresponding to the range `w.x.y.z/24`, allows for external access to its *broadcast address*, i.e., traffic sent to `w.x.y.255` reaches *all* hosts simultaneously on that sub-network. Note that neither you nor your target are on this sub-network.

Describe as clearly as possible how you can take advantage of the sub-network to perform a denial-of-service attack on the target.

b) (30 points) The network time protocol (NTP) is used to synchronize Internet devices to within a few milliseconds of UTC time. The current version of the protocol, NTPv4, is an evolution of the protocol described in RFC 5905, and is built on top of UDP, i.e., requests to NTP servers are via UDP packets.

Earlier versions of NTP had servers accept a command called "monlist" for monitoring purposes. It returns the addresses of up to the last 600 machines that the NTP server has interacted with.

Briefly explain how to use the monlist feature of NTP for a DoS attack.

2. (65 points) (**Reuse of one-time pad**) In this problem all characters are represented as 8-bit bytes with the usual US-ASCII encoding (e.g. "A" is encoded as 0x41). Here are two 8-character English words (that you can find in a dictionary such that /usr/share/dict/words in Unix) encrypted with the *same* "one-time pad". What are the words?

```
e9 3a e9 c5 fc 73 55 d5
f4 3a fe c7 e1 68 4a df
```

Describe how you figured out the words. (You should implement a program for this task but don't have to submit the code.)