README.txt written by Jeffrey Harnois

Mission 2

This project is contained in a zip file which includes:

1. README.pdf
2. Mission_2_Report.pdf
3. Mission2_1
   a. Decode.py - our decoding function using RSA that we import into our encryption script
   b. Encode.py - encoding function using RSA that we imported into our decryption script
   c. DNSresolv.py - sends out the actual DNS request
   d. Index.html - our example webpage
   e. Encryption.py - script that used decryption to resolve where the ip is for the query sent
   f. Private_pem.pem - the private key of the client for RSA decryption
   g. Public.pem - the public key of the DNS for decryption
   h. Server.py - the script that runs the webserver
   i. encryption_attack .py - does not encode or decode, just sends out the DNS and resolves the response (for attack phase, encryption is for the defense phase)
4. Mission2_2
   a. Index.html - sample html page
   b. Encrypt.py - for defense, receives a packet and sends right back
   c. Server.py - script to run the web server
5. Mission2_4
   a. db.www.bombast.com - DNS record (zone file) for bombast
   b. db.www.carter.com - zone for carter
   c. Named.conf - description of all the named.conf files to look at when resolving DNS
   d. Named.conf.local - list of all the zone files for DNS resolve
   e. Named.conf.options - all the optional configurations of DNS
   f. Named.con.default-zones - Did not need to include but default if DNS did not fine alternatives like the ones above
6. Mission2_5
   a. Router.py - runs the man-in-the-middle attack (only run during the blackhole phase)
7. Mission2_6
   a. Decode.py - same as in 1
   b. Encode.py - same as in 1

c. Encrypt_attack.py - same as in 1
d. generateRSA.py - did not need to include but generated the 2048 key
e. encrypt .py - same as 2
f. Encrypt_attack.py - same as 1
g. Named.conf.default-zones - same as 4
h. Named.conf.local - same as 4, only difference is that it is empty, so there needs to be a recursive call
i. Named.conf.options - same as 4
j. Private.pem - the DNS server's private key for RSA encryption
k. Public_pem.pem - the public key of the client for RSA encryption

Tools:
Scapy - a library in Python that allows us to sniff and modify packers
NFQueue - a tool that allows us to put packets into a queue to send that allows us to drop the first packet in the queue due to the fact that the packet is not written
RSA - a library in Python that allowed us to generate RSA private and public keys for part of our defense
Bind9 - a Linux tool that allows DNS servers to be set up on specific computers