UTSA
The University of Texas at San Antonio™

Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

Lab 1 – Deciphering Secret Messages

Lab Description and Instructions:

Imagine that you are a special agent for your country's defense services. Your primary job is to eavesdrop on encrypted communications originating from foreign adversaries and to decode/decipher them as quickly as possible. One day at job, you intercept the following encrypted message sent out by a spy working for a foreign adversary:

```
yfafjge wzl fa fwnwdw ls cuslls
```

This message originated from a machine with the domain `range.secretlab.page` (which resolves to the IPv4 address 69.61.103.44). You do not know the details of the encryption algorithm (or details of the secret key used) to encrypt this message. However, you are aware that the spy is running this encryption service on `range.secretlab.page` port 39000, and he uses this service to encrypt all his messages before sending out. You can access this service using a raw TCP connection (e.g., using telnet or nc) as follows: *`nc range.secretlab.page 39000`*. In other words, you can use this service as a "Blackbox" to encrypt any number of plaintext messages of your choice and observe the corresponding ciphertexts. You can then use this knowledge of how the encryption service (or algorithm) generates the ciphertext for each plaintext you provided in order to decipher the ciphertext in question.

Your task is to decrypt the above encrypted message and reveal the secret being transmitted by the foreign spy. More importantly, you need to figure out the encryption algorithm, and the key used for encryption, so that all future encryptions can be decrypted. Timely decipherment of this message is critical, as strategic decisions relying on the information you provide need to be made! You can assume that the encrypted message is written in English language.

Guidelines and Deliverables:

Each student must complete this lab assignment during the lab session and then complete the associated homework before the due date.

Homework (Due: 9AM Tuesday, June 25th, 2024):
Upon further investigation you also noticed that `range.secretlab.page` is offering another similar text encryption service at port 39001. Your mission to is identify this second "Blackbox" encryption algorithm on your own and report it back by the due date! You may upload a 1-2 page report describing this second encryption algorithm in a PDF file (with your first and last names in the filename) here:
https://cloud.secretlab.page/s/PmYJEZyACJ7HDSj

PuTTY: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html