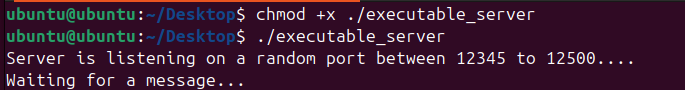
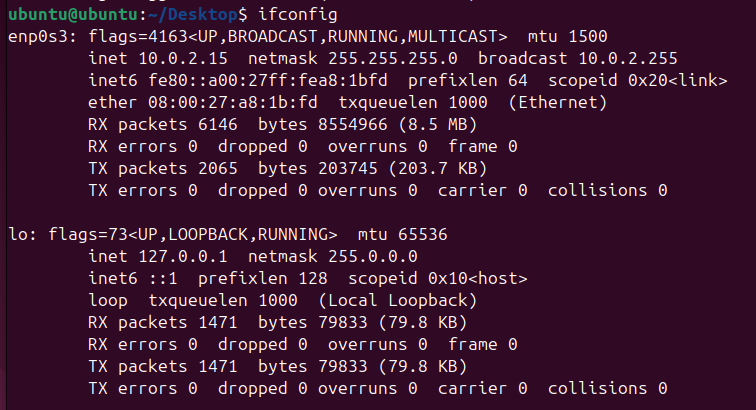
CSCI369 – Assignment, Question 4

UOW ID: 7770029

1. To run the server program provided with this specification on the Ubuntu VM by typing ./executable\_server on the terminal.

* ‘chmod +x ./executable\_server’, is used to change the permissions of the file named executable\_server to make it executable as I couldn’t run the file on the terminal straight.

To begin, check the IP address of the system using ‘ifconfig’

Scans for open port using **Nmap**. Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a network.

*sudo nmap -sT -sU -p 12345-12500 -v 10.0.2.15*

* ‘sudo’ to run the command with root privilege when dealing with UDP scans as it involves sending and receiving raw network packets and ‘nmap’ needs the permissions to perform the scan accurately.
* ‘nmap’ specifies the scanning tool used to identify open ports on the target server.
* ‘-sU’ specifies a UDP scan.
* ‘-sT’ specifies a TCP scan.
* ‘-p 12345-12500’ specific the range of port to scan
* ‘-v’, verbose mode, to get detailed feedback as the scan progresses as ‘nmap’ scans each port.
* ‘10.0.2.15’ the ip address of the Ubuntu VM.

A computer screen shot of a computer program

Description automatically generatedAs seen from the terminal output, an UDP open port was identified, port 12441.

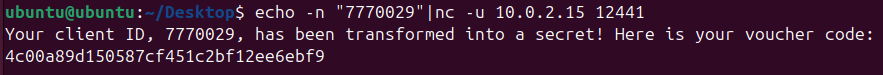
1. Based on the UDP port discovered, to obtain the gift voucher code a UDP client tool is used to send the ClientID to the identified port using tools like **Netcat**.

Netcat is a versatile networking tool used for reading from and writing to network connections using TCP or UDP protocols.

*echo -n "7770029" | nc -u 10.0.2.15 12441*

* ‘echo -n’ is used to output the text that follows in a new line and not to append it to the output.
* ‘7770029’ is the ClientID, generated from my student ID (UOW ID).
* ‘|’ pipe is used to take the output of the command on its left and uses it as the input for the command on its right.
* ‘nc’, Netcat is used to communicate with the server that generates gift voucher codes.
* ‘-u’ specifies that ‘nc’ should use UDP rather than TCP, as the port identified is a UDP port.
* ‘10.0.2.15’ the ip address of the Ubuntu VM.
* ‘12441’ is the port number identified from the nmap scanning in part (a).

Summary of the whole command, it sends the string "770029" (without a newline character) as a UDP message to the IP address 10.0.2.15 on port 12441.

As seen from the terminal output, a hashed gift voucher code is generated.

1. Performing **brute force attack** crack the MD5 hash to find the matched combination of the two-alphabet character from A and the two-symbol character from B that the server used to combined with the ClientID to generate the gift voucher code.

While crunch is a tool used to generate wordlists based on user-defined patterns. Crunch is powerful, but can be very slow and resource-intensive when generating large wordlists, particularly if the pattern space is very large like generating all the possible combinations of A, ClientID, and B. Therefore, using brute force technique is more suitable.

* Import
  + ‘*import itertools’*, it provides functions that create iterators for efficient looping. These functions can be used to generate permutations, combinations, and other iterators for various tasks. It is used to generate all possible combinations of two characters from a given set (like lowercase letters or symbols).
  + ‘*import hashlib’*, it provides a common interface to many secure hash and message digest algorithms. It is used to generate an MD5 hash by encoding a string (composed of different parts like a client ID, and combinations of characters) and then passing it to the md5() function to get the corresponding hash value.
  + ‘*import string’*, it provides a collection of string constants, like string.ascii\_lowercase, which is a string containing all lowercase letters.
* Generating combinations for A and B
  + ‘*itertools.product(string.ascii\_lowercase, repeat=2)*’, generates all the possible combinations of the set of two lowercase alphabet characters for A.
  + Similarly, a list of 32 symbols is specified to generates all the possible combination of the two set of two symbols for B.
* Known details
  + ClientID is known which is the student number and is used as part of the input to the MD5 hash function
  + Voucher code is obtained earlier in part (b), which is the MD5 hash that the script is trying to match through performing brute force.
* Brute force matching
  + The script iterates over each combination of ‘A’ and ‘B’.
  + ‘*input\_string = a + ClientID + b’*, this constructs the string to be hashed, by concatenating a possible A, the ClientID, and a possible B.
  + ‘*md5Hash = hashlib.md5(input\_string.encode()).hexdigest()*’, this generates the MD5 hash of the constructed string.
  + ‘*md5Hash == voucherCode*’, script checks if the generated MD5 hash matches the known voucher code.
  + If a match is found, the script prints the summary which consist of ClientID, the generated voucher code, and the successful combination of A and B. The loop then breaks, stopping further attempts.
* Output
  + If the script finds the correct A and B, it prints out the details and stops.
  + If no match is found after all possible combinations have been tried, the script outputs "No match found."

As seen from the terminal output, the matched combinations of A and B is found.

A close up of numbers

Description automatically generated

The source code, bruteforce.py.

A computer screen shot of a computer code

Description automatically generated

A computer screen shot of a program code

Description automatically generated