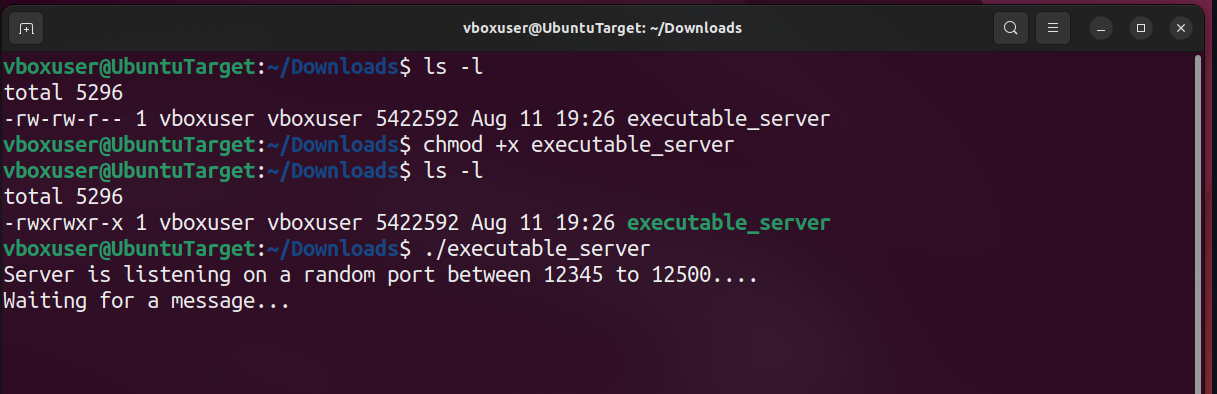
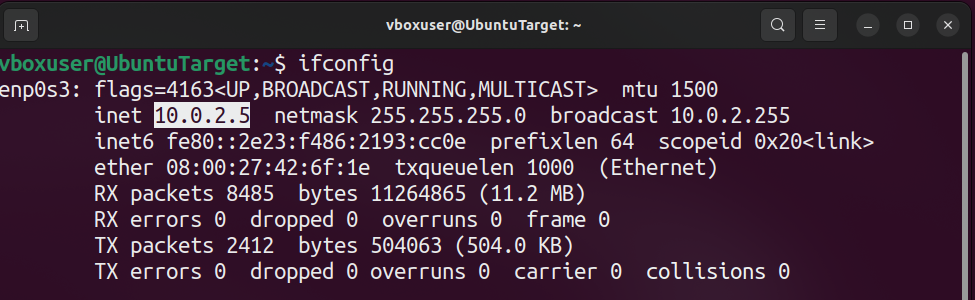
Question 4:  
  
Kali VM: Attacker machine  
Ubuntu VM: Running the target UDP server.

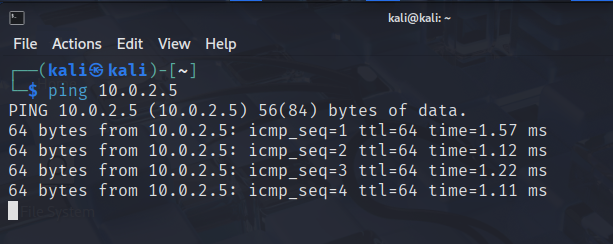
Part 1 Setting up the server on ubuntu.

In the Ubuntu VM, the provided executable\_server file was missing execute permissions.   
$> chmod +x executable\_server.

I added the permissions and started the server.  
Using $>ifconfig, I identified the Ubuntu VM’s IP address to prepare for scanning.  
Ubuntu VM IP address = 10.0.2.5

Part 2 Verifying connectivity

From Kali, I verified that we could reach the Ubuntu with a simple ping.



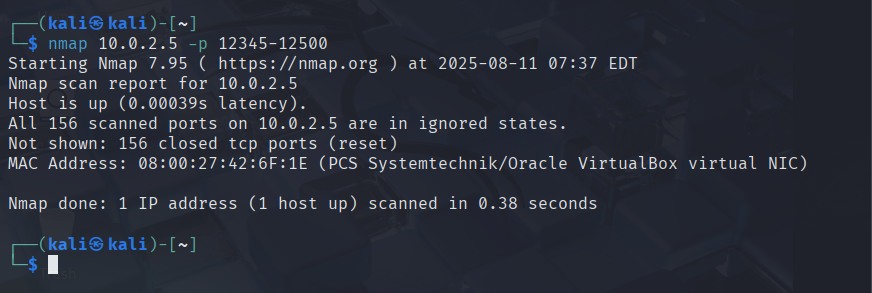
Part 3 Identifying the service.

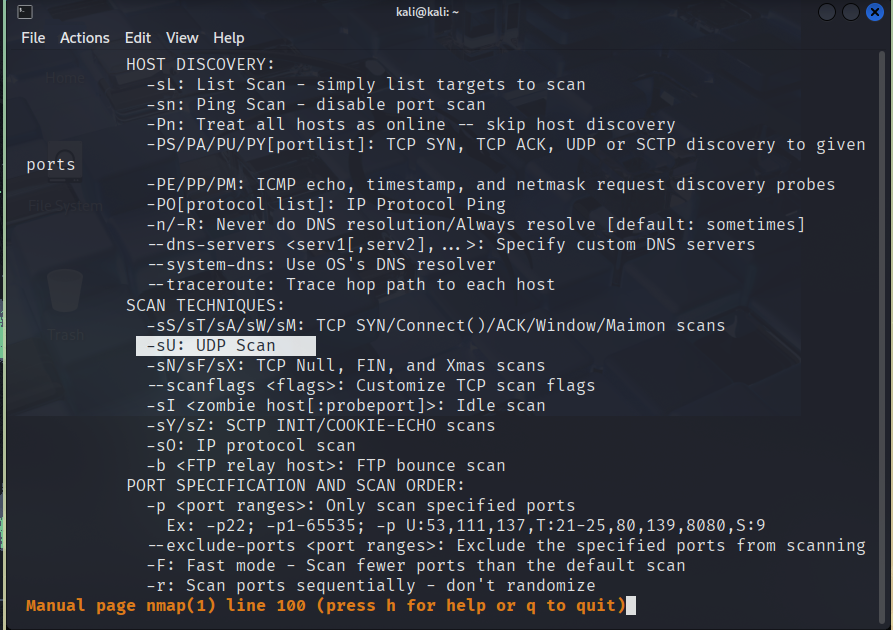
We were told that:

* The service runs **UDP** ports in this range **12345 – 12500**
* Uses a weak hash **MD5** to generate the codes.

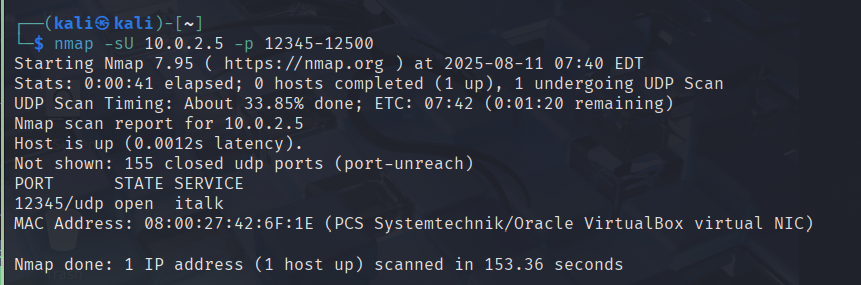
Running a TCP SYN scan (which is the default) over this range found nothing.

$> nmap 10.0.2.5 -p 12345-12500



Reviewing the nmap man pages, I found the UDP scan flag –sU  
Re-scanning revealed that UDP port 12345 was open

$> nmap –sU 10.0.2.5 -p 12345-12500

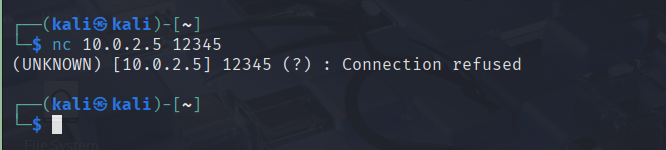


1. The open port is 12345

Part 4 connecting to the service.

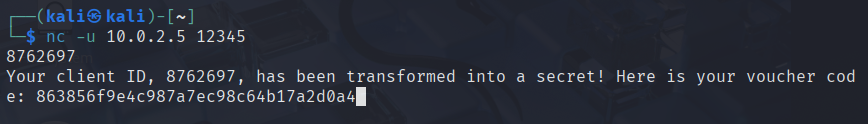
I attempted to connect with netcat using

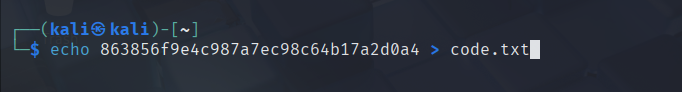
$> nc 10.0.2.5 12345

This hung because netcat defaults to TCP, after a quick google I found that i can switch modes using the –u flag.  
$> nc –u 10.0.2.5 12345



The cursor is hanging there as if waiting for input.   
So this is where I entered my UOW ID: 8762697

I copy and paste this and save this into code.txt on my kali for future use.

$> echo 863856f9e4c987a7ec98c64b17a2d0a4 > code.txt 

1. My gift voucher code: 863856f9e4c987a7ec98c64b17a2d0a4

Part 5 Generating the password wordlist using Crunch

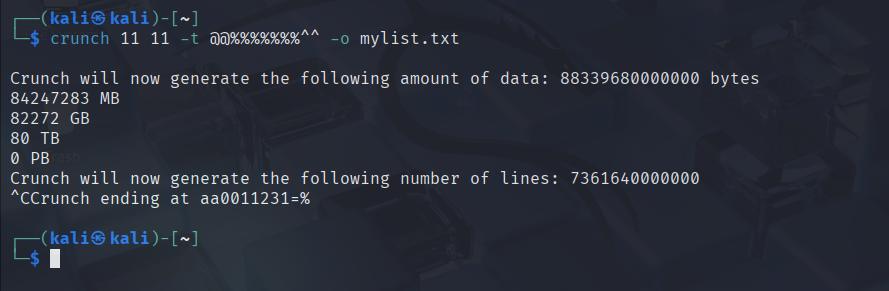
From the assignment outline we were told that the password format was:  
A | UOW ID | B  
where A = any two lowercase characters,  
B = two special characters  
and UOW ID is my university number.

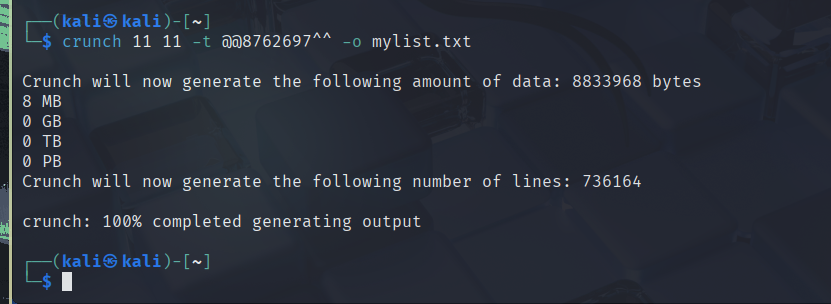
In Crunch:  
@ = a wildcard for lower case letters

^ = a wildcard for special character

% = a wildcard for a number

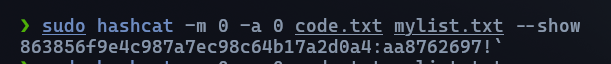
Initially, I mistakenly tried a pattern with numeric guessing which resulting in this gigantic wordlist of 80+ TB.

$> crunch 11 11 –t @@%%%%%%%^^ -o mylist.txt   
Then I remembered that we don't have to play the guessing game for the digits.. Its my personal UOW ID. So i tried it again with that specific number.

$> crunch 11 11 –t @@8762697^^ -o mylist.txt  
This produced a manageable file size.

Part 6 Cracking the MD5 Hash.  
Now all thats left to do is to run hashcat on MD5 mode on the hash with my generated wordlist.  
I ran into some hardware problems, memory issues likely due to VM environment. I ran this on my linux host machine instead.

$> hashcat –m 0 –a 0 code.txt mylist.txt

I forgot to screenshot the initial cracking process. Since hashcat saves cracked hashes in the potfile, I used –show   


The full password was: aa8762697!` which means:

C)  
A = aa

B = !`