Name: Akil Hosang

ID: 816003000

Assignment # 3

Course Code and Name:

INFO 2604 – Information System Security

Year: 2

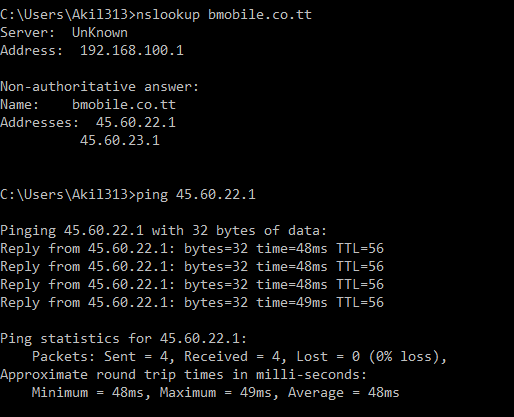
Semester 2

Method 1

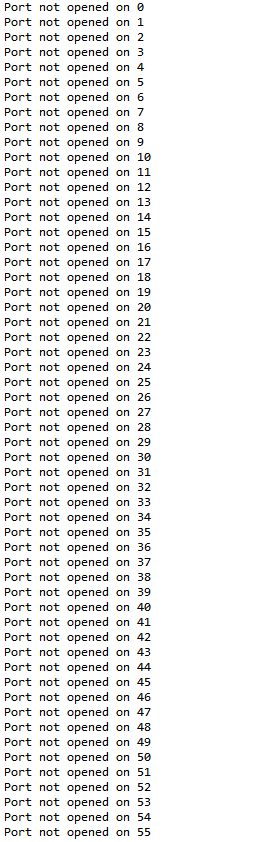
First, **nslookup** was used to obtain the address of the site bmobile.co.tt

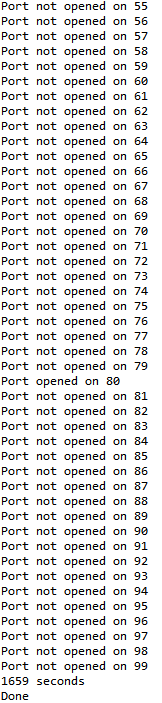
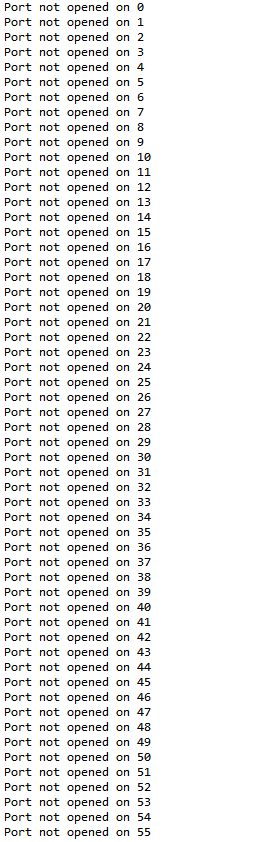
The site name a dn addresses were returned.

Then the server address was pinged to see if it would return a response. When the server responded we could confirm it is online.



Then, the first 100 ports of the ip address of   
bmobile.co.tt was scanned.

After 1659 seconds, as shown on the line above the  
last, only port 80 was found to be open.



,

NMAP Method

On the other hand, this process was replicated using nmap. Upon calling nmap on the site bmobile.co.tt, the 2 IP addresses were returned, one being scanned and the other wasn’t.

The IP address that was scanned was then checked for open ports and found open ports at ports 25, 53, 80, 81, 82, 83, 85, 88, 89 and 90.



On comparison of the two methods, nmap was observed to be more efficient, effective and informational.

Where in the first method provided the same IP addresses as the nmap method but the information provided by one command of the nmap method was way more than the information provided by the single command in method one.

Over the course of the both methods the same information was returned in terms of IP addresses but when it came to the ports, method one only showed the ports that were opened whereas the nmap method provided the number of unfiltered ports, the open ports, the protocol on the port and the service all within 2-5 seconds where as method one took 1659 seconds to find the open ports only in the range of 0 to 100.

In conclusion, the nmap method is observed to be superior to the first method.