Network Security Assignment 1

CSCI 6708

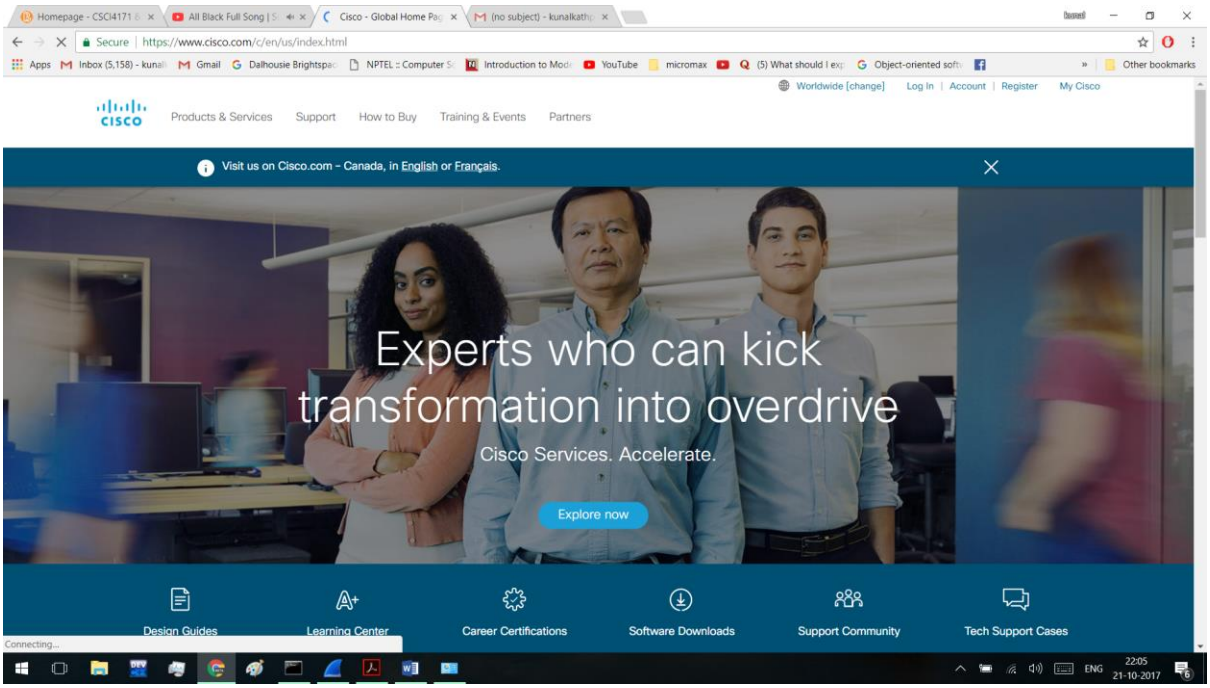
Kunal Kathpal B00765934

Question 1

a.

- Wire shark is a open source computer network traffic monitor
- It is used to analyse and sniff packets
- Usable on multiple platforms
- Wire shark is roburst
- It's free of cost

b. First, we will connect to a website i.e. cisco.com

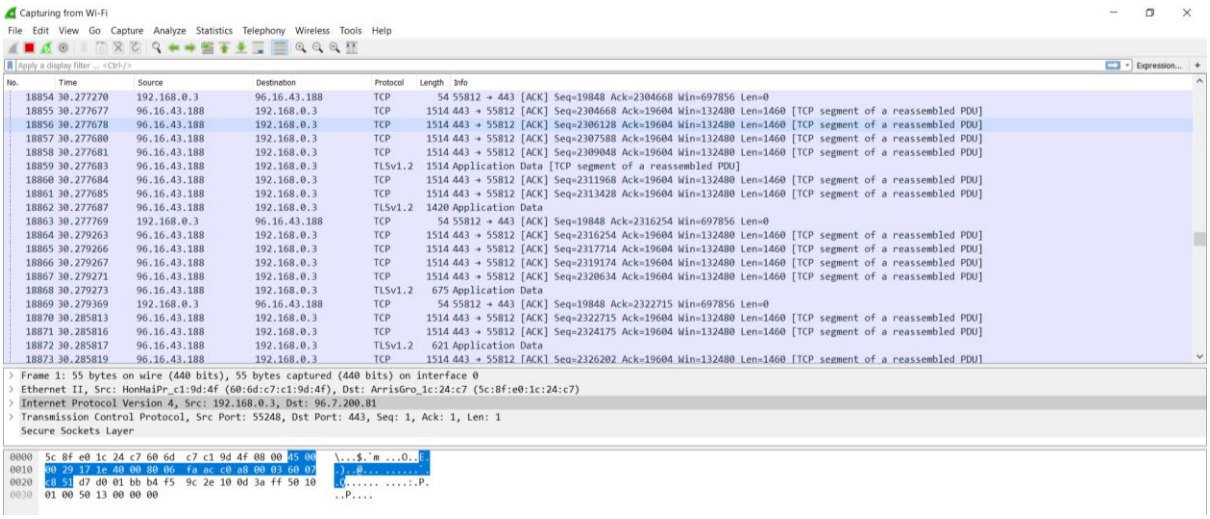


Then we will open CMD and ping cisco.com using the ping command.

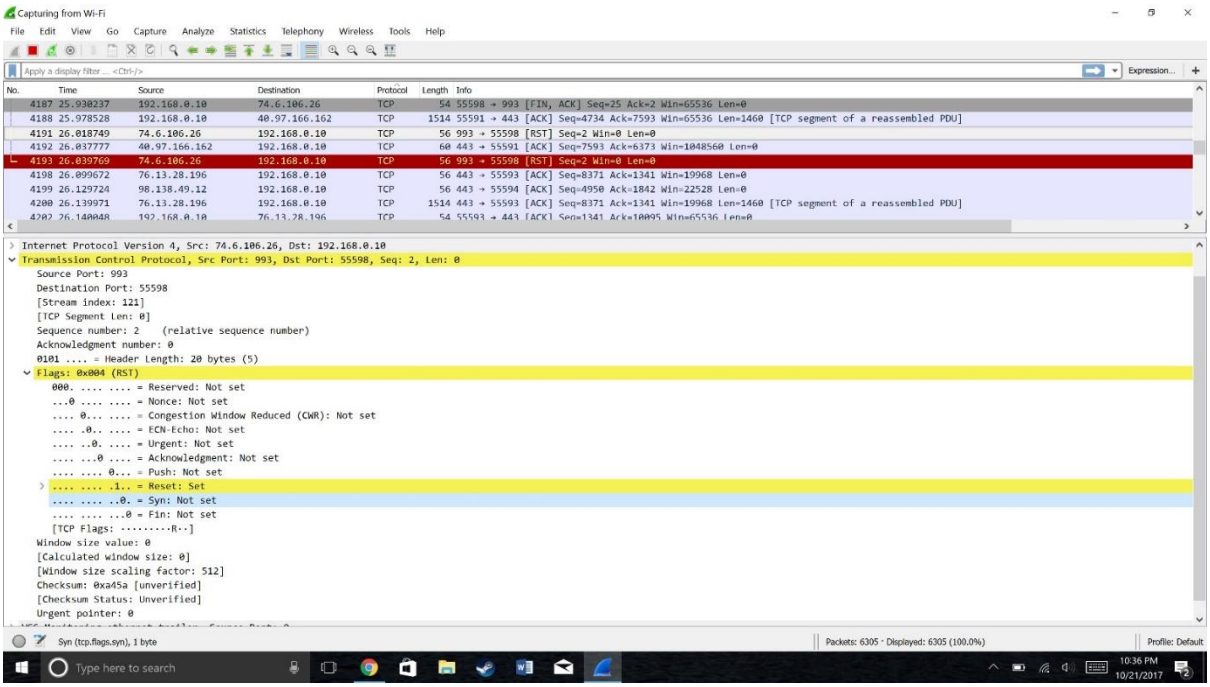
```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\kunal>ping cisco.com

Pinging cisco.com [72.163.4.161] with 32 bytes of data:
Reply from 72.163.4.161: bytes=32 time=81ms TTL=240
Reply from 72.163.4.161: bytes=32 time=81ms TTL=240
Reply from 72.163.4.161: bytes=32 time=102ms TTL=240
Reply from 72.163.4.161: bytes=32 time=193ms TTL=240

Ping statistics for 72.163.4.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 81ms, Maximum = 193ms, Average = 114ms

C:\Users\kunal>
```

c. The figure below shoes packets being received from 96.16.43.188

The IP Address of my PC is 192.168.0.10 and the figure shows packets been received from cisco.com whose IP address is 72.163.4.161.



TCP



Source code is 993

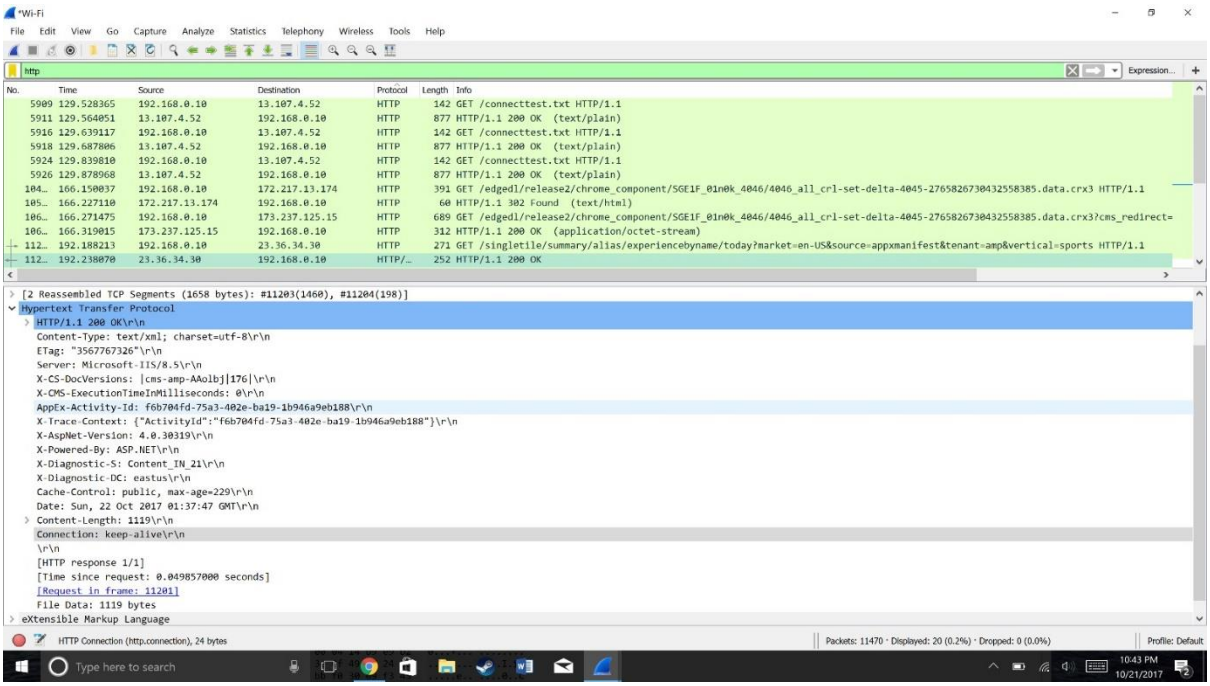
Destination port is 55598

Sequence number is 2

I observed Reset flag is SET and SYN flag NOTSET

Checksum status is verified

HTTP

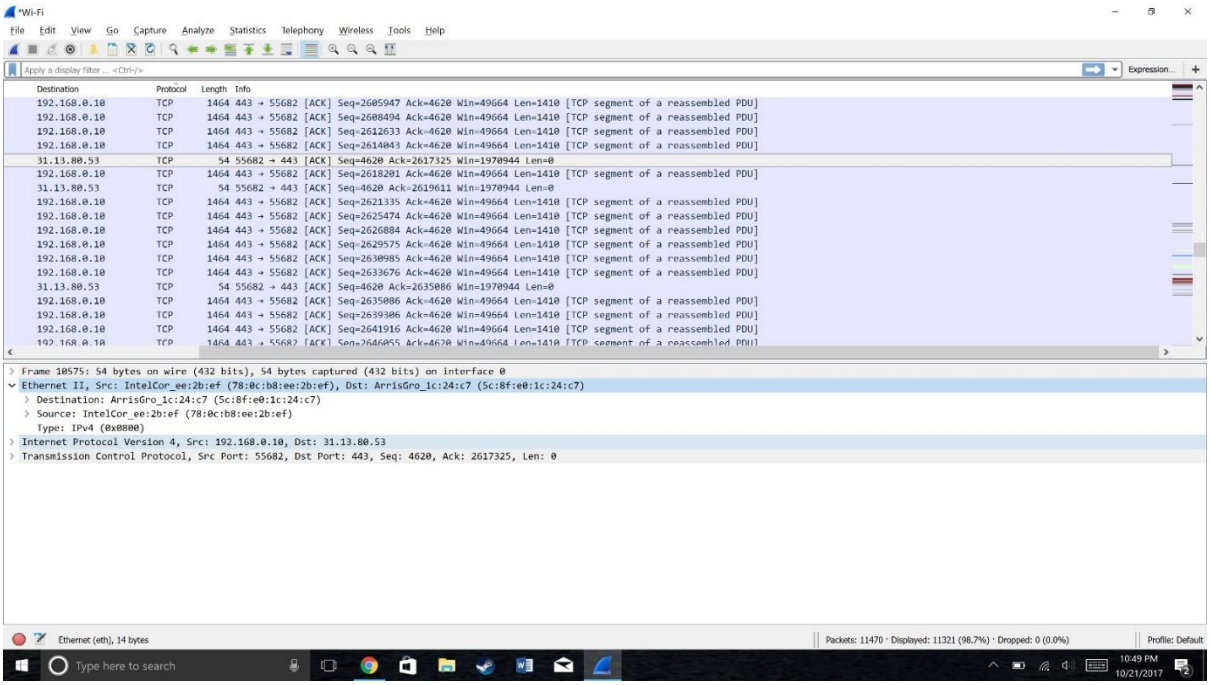


Content- type : test/xml

Charset is utf-8\r\n

Cache control is public and the length of the of content is 1119

DATA LINK LAYER



Moving to the Ethernet layer , we can see that it is pretty simple. It contains a destination address and a source address. The data link layer is relatively simple in that it is only concerned with getting a frame to the next adjacent node on the physical medium

d.

- First, I logged on to cisco.com
- Then I pinged cisco.com using CMD
- Then I monitored traffic on wireshark for 13 minutes
- I observed various different types of protocols such as tcp, ip, http, https, dns, arp etc..

Question 2:

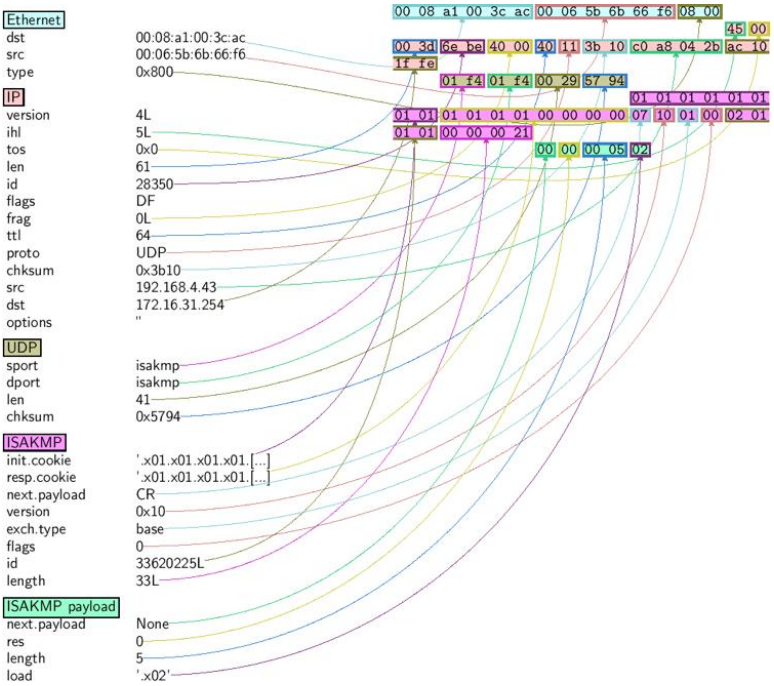


Figure 1: http://sectools.org/tool/scapy/screenshot/0/

Scapy is a very simple tool and it's written in python language.

Scapy is used for manipulating the packets. Here are some hidden features of this powerful tool.

- Capture packets of wide range of protocols
- Forges and decodes packets of wide range of protocols and send them over wire.
- It's known for managing the classical tasks like Tracerouting (similar to tracert in windows), Unit testing, attacks, probing.

Scapy is a open source tool that's compatible with any type of operating system and it's very light to use as it doesn't use a lot of ram. The network security specialist like this tool because they can modify the software to their own need and they can mould the code according to their requirements.

All hackers use terminal to attack because it's more powerful and vast as compared to GUI. Scapy can be directly operated from the python terminal that's what make it too handy for hackers. Scapy is used for manipulating the packets and packets. Suppose the packets are going from client server to the merchant server and the packets contain the financial credentials of the transaction. Scapy is powerful enough to alter those packets and the hacker/middleman will change the account credentials to his credentials to gain economically.

Question 3:

DDOS attack, (distributed denial of service attack). In DDOS there are multiple computer/bots over the vast geographical area. They all request from the same server (victim) and the server can't handle soo many requests of these number of clients as a result either it replies late or the company shuts it down for a while. The attackers aims to shutdown the system of the server because it effects the company clients emotionally and financially.

The one of the Successful attack of 2016 was Rio Olympics attack.

Technique used in attacking and the victim.

LizardStresser (an organization responsible for previous Olympics attack) deployed DDoS campaign using the lesser known Ip protocol i.e GRE (Generic Routing Protocol)

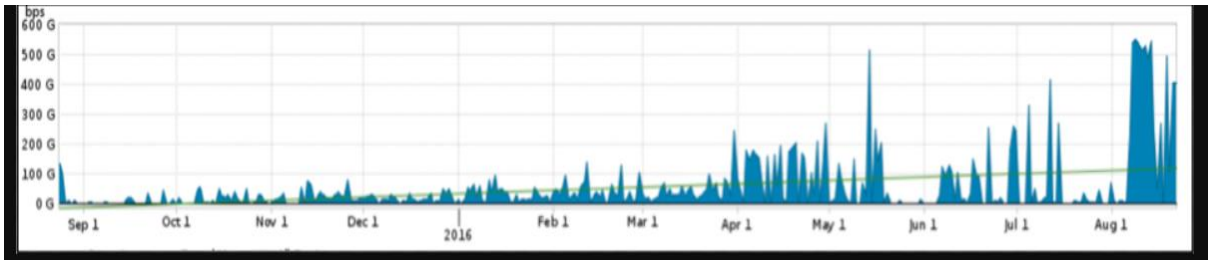


Figure 2: https://blog.apnic.net/wp-content/uploads/2016/09/DDoS_Olympics.png

Who is faced the attack??

According to the Abor network all the public facing websites that were affiliated with the 2016 RIO Olympics were targeted by sustained, sophisticated DDOS attacks that reached upto 540 Gbps according to Abor Networks. According to the network security companies the attacks started before the Olympics games had begun, but the attacks increased significantly during the games. It was the largest and the longest duration sustained attact Abor has ever sustained 500gb + DDoS.

Techniques used to supress and stop the attack.

I companies knew something will happen because the traffic on google was increasing before the starting of the Rio Olympics. In the initial phase the attack the defenders tried to use (Netflow, sFlow, cFlow, IPFIX) for classifying and tracing the attacks, but the attack was mitigated using Intelligent DDoS mitigation System (IDMS). IDMS is responsible and capable of cleaning attack traffic from layer 3 and layer 4 and layer 7.

Question 4

4 (a)

s	**r11**	**S**	**D**	**51111**	**20**	**DATA**

(b)

r14	**r21**	**S**	**D**	**51111**	**20**	**DATA**

(c)

r22	**r34**	**S**	**D**	**51111**	**20**	**DATA**

(d)

r31	**d**	**S**	**D**	**51111**	**20**	**DATA**

(e)

r11	**S**	**D**	**S**	**20**	**51111**	**DATA**

(f)

r21	r14	D	S	20	51111	DATA

(g)

r34	r22	D	S	20	51111	DATA

(h)

r14	r21	S	D	51112	22	DATA

(i)

r22	r34	S	D	51112	22	DATA

(j)

r31	d	S	D	51112	22	DATA

(k)

r11	s	D	S	22	51112	DATA

(l)

r21	r14	D	S	22	51112	DATA

Question 5:

Scenario	Intrusion(s)	Security Goal(s) violated	Justification
Bob crashes Alice's computer system by sending a flood of packets	Interruption	Availability	This is a classic case of a DoS attack and hence falls under the category of Interruption. Alice's computer is unavailable for her use and hence the security goal violated is Availability.
Alice copies Bob's assignment by eavesdropping on traffic from his machine.	Interception	Confidentiality	In this scenario alice copies bob assignment but as she is unaware of the things she can't modify the assignment. Bob is the owner of the assignment only he can see the assignemnt no one else.
Bob copies Alice's assignment by accessing her hard drive.	Interception, Invasion	Access Control	In this scenario bob is stealing the assignment by accesing her hard disk. Only alice should have the access to the had disk as its her personal stuff.

Alice changes the amount on Bob's cheque when it is being transmitted.	Modification	Integrity	Alice modifies the amount on Bob's cheque when it was transmitting that clearly means that she gained the advantage of the transmission.
Bob sends a property deed to the Registrar in the name of Alice by Forging Alice's signature.	Modification/ Interception	Authentication, Certification	The documents given to the registrar are not authentic as the Bobs forged alice signature.
Alice spoof's Bob's IP address to Gain access to his office server.	Interception	Access control, Authentication	Alice spoofs bob and enter into his server "she is not the appropriate persont to do this". She tried to gain access of the system.
Bob installs malware on Alice's Computer.	Fabrication	Integrity, Confidentiality	Bob installed a malware on Alice computer which indicates that he either wants to alter the information or to gain remote access of her computer.
Bob obtains Alice's credit card Information online and has the credit card company replace it with another card bearing a different account Number.	Fabrication	Authentication/ Integrity	This clearly indicates that bob did this all because he wants to gain financial benefits from her.
Alice has a fake third party Authenticate her server as legitimate.	Fabrication/ Interception	Certification / Integrity	The certification goals is violated as alice has a third party to authenticate her server.