ENDSEM - CS 212

19003043
Page No. TSATWIK
Date

PART-1

(1) The different flags used in TCP header are:
- SYN - Synchronize flag that initiates
- ACK - Acknowledgement flag that acknowledges
- FIN - Final; this is used to terminate/end the TCP connection
- Some other flags include push, reset, etc.

(2) ICMP is a network layer protocol that is used for ping & trace route. ICMP is used in the TCP/IP architectured networks.

(3) Yes a machine can have a single DNS name with multiple IP addresses. We have seen a example of this in one of the labs, www.google.com has multiple IP addresses with same DNS. This is done to incorporate the benefits of each of this servers & also overcome the problem of servers being offline & also decreases the load on networks.

(4) When we ping a particular website, our computer sends out the specified number of requests/packets (ICMP packets). Our machine will calculate the time taken for it to go to the destination & come back to our machine (server).

This time is the RTT value & if after a certain time out, we considers the packet is lost/servers is offline.

(5) HTTP status codes

200 - OK (indicates that there are no problems)

304 - NOT MODIFIED (indicates, that the data is not modified since the last time downloaded)

401 - UNAUTHORIZED (indicates, that there is a username & password for retriving data)

~~403~~ 403 - FORBIDDEN (indicates, that our request cannot be processed)

(6) Wireshark uses sequence numbers & acknowledgment numbers to detect delayed duplicates, packets are uniquely identify the packet, hence if we transmit them, wireshark can detect them as retransmissions that have the same destination IP address & the sequence, acknowledgment numbers

(7) (a) ping [-c] 5 <url> is the command option to specify the number of requests to be sent.
In the example, it sets the count to be 5

(b) ping [-i] 5 <url> is the command option to set the interval b/w each packets
In the example, it sets the interval to be 5 seconds

(8) When a machine accesses a website, first it uses DNS protocol to retrive the IP address of amazon's servers, so it sends a UDP packet for this
~~Then our machine will send a GET request message using HTTP, to~~ to the server.
Then the machine will send ARP broadcasts to check if the servers is in LAN. Then the machine will send TCP packets using the 3-way handshaking, i.e TCP SYN is sent from our machine, then TCP SYN & ACK is recieved, then ACK is sent from our machine. (HTTP)
Once the connection is established, it used ~~HTTP~~ GET request & responses to send bigger files with each other.
It may use TCP packet again in case of any functionality of webpage is used

(9) ~~In non secured websites, the username & password of non se entered by the users are sent along with the packet.~~

Along with TCP, TLS packets are also sent which are more secure.

Hence this is the ~~use~~ sequence of messages

Page No.
Date

(4) For non-secure websites, like the one we encountered in lab, our machine will send a request & get a 401 unauthorized message back.

Then when we type the username & password and press enter, these values are appended and sent along with the packet in a new field called authorization.

Though the data is encrypted, we can easily decode it by using online tools, because the encryption key is not secure.

At this point if somebody captures our packets using wireshark & then they can easily decode it to find out the username & password.

In this way anyone can get the username & password in non secured websites.

(10) Here we have 2 machines 1 & 2. LAN network

Computer-1 & ~~Computer~~ wants to send to Computer-2.

Using DNS, (1) knows the IP address of (2) as 192.168.0.55.

As we know that in LAN network, there are no routers/gateways, hence communication can happen only by node-node. For this we need the MAC addresses of both the machines, as MAC - ~~is~~ in data link layer.

Hence ARP is required to find the MAC address of computer (2), & this is done as follows.

comp (1) sends a broadcast ARP request by indicating the IP address, then comp (2) will send a unicast ARP response to comp (1) by indicating its MAC address.

Hence, now both of them will communicate