Rapport för Laboration 3

31/03/16

Fredrik Larsson, 9306278111

Institutionen för data- och
systemvetenskap,
Stockholms universitet

Datorsystem DA
Vårterminen 2016

DA

Innehållsförteckning

Inledning

Laborationen går ut på att ge kunskap inom området nätverk. Genom att gå igenom baskunskaper samt visa hur paket de paket, som kommandona i uppgifterna använder, ser ut erhålls en klarare bild över hur information skickas samt tas emot över internet.

Förberedelsefrågorna ger en bas förståelse för hur information skickas på internet. Uppgift 2 ger en klar bild för hur informationen som skickas ser ut i applikationslagret samt hur paketen ser ut. Uppgift 3 ger kunskap hur domännamn översätts till IP adresser.

Verktyg

I den här labben har verktygen Wireshark samt PuTTY använts.

Wireshark är en s.k. packet sniffer vilken sparar de packet som skickas samt tas emot på en given interface, vilka sedan kan gås igenom av användaren. PuTTY är en telnet(& SSH) klient som används för att ansluta samt be om data från en webbserver.

Förberedelsefrågor

1.1.1 Which layers are included in the TCP/IP model?
Application, transport, internet, link

1.1.2 What are the advantages and disadvantages of using a layer model?
Fördelar; Gör kommunikation mellan olika typer av applikationer samt datortyper enkelt. Det gör det även enkelt att ändra i ett av lagerna utan att påverka de andra lagerna.

Nackdelar; Overhead, då lagrade modeller inte ser skillnad på kommunikation mellan två enheter direkt över ett nätverk eller två enheter med tusen andra enheter. En annan nackdel är att de övre lagerna inte kan påverka de under även om detta skulle vara välgörande.

1.2.1 What is the purpose of using ports?
Portar skiljer på anslutningar mellan olika processer och tjänster på samma enhet.

1.2.2 In total there are 65536 ports and one usually divide them into three area. What are these areas called and which port range belong to which area?
Well-known ports/system ports 1-1023
Registered ports 1024-49151
Dynamic/Private ports 49152-65535

1.2.3 What is the default port for HTTP?
Port 80

1.2.4 Which is the standard port for SMTP?
Port 25

1.3.1 What is the purpose of the HTTP protocol?
Att möjliggöra kommunikation mellan en webserver och en klient.

1.3.2 What response code is received from a web server if everything has gone well?
200 OK

1.3.3 What response code is obtained if the web server cannot find resource that is in demand?
404 Not found

1.3.4 Which two response codes, you can get if you do not have rights to a requested resource?
401 Unauthorized, 403 Forbidden

1.3.5 What are the different request can be done using HTTP?
OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT, PATCH

1.4.1 What is the purpose of the SMTP protocol?
Att transportera e-mail över internet.

1.4.2 How the command appears to indicate the sender's address to SMTP?
"MAIL", användning: "MAIL from:<avsändarens address>"

1.4.3 How the command appears to enter the destination address under SMTP?
"RCPT", användning: "RCPT to:<mottagarens address>"

1.4.4 How the command appears to indicate the actual text of an e-mail to SMTP?
"DATA", användning: "DATA" följt av en data stream

1.4.5 Which command asks an AMTP server on which extensions it supports?
Klienten börjar med att sända EHLO och om server inte svara faller tillbaka till HELO

1.4.6 An e-mail message consists of two parts: Header and body. Which two fields must always be in the header?
From, Date

1.5.1 What is the purpose of DNS?
Att kunna använda adresser som är mänskligt läsbara för datorkommunikation, som sedan översätts till IP adresser via DNS servrar.

1.5.2 What type of DNS resource record should you ask for if you want to know the IPv4 address for a domain?
Type A

1.5.3 What type of DNS record should you ask for if you want to know the IPv6 address for a domain?
Type AAAA

1.6.1 How can you define a filter in Wireshark to only see the traffic that contains the HTTP?

Börja med att endast fånga traffiken på port 80, tillämpa sedan ett display filter för paket innehållande HTTP

1.6.2 How to follow a specific TCP stream in Wireshark?

Högerklicka på ett paket och välj ”ström typ” under ”follow”. Alternativt hitta ”stream index” under transport protokollet och sätt “tcp.stream eq X” som displayfilter.

Laborationsuppgifter

Uppgift 2.1

Metodbeskrivning

En fråga ställs till servern da.dsv.su.se via putty sedan kontrolleras svarsmeddelandet, vilket innehåller information såsom responskod, respons header(som innehålls t.ex. innehållstyp) samt svars data.

Resultat

Ask for the resource /art.txt

2.1.1 How did your conversation with the Web server look like?

Jag ställde en fråga till servern(GET /art.txt HTTP/1.0), servern svarade med statuskod samt den resurs som efterfrågades(/art.txt)

2.1.2 What response code you got?

200 OK

2.1.3 What are response codes?

Standard svar till klientens begäran

2.1.4 What type of content is in the response from the web server?

Vanlig text, text/plain

Ask for resource /layers.html

2.3.1 How did your conversation with the Web server look like?

Jag ställde en fråga till servern(GET /layers.html HTTP/1.0), servern svarade med statuskod samt den resurs som efterfrågades(/layers.html)

2.3.2 What response code you got?

200 OK

2.3.3 What are response codes?

Standard svar till klientens begäran

2.3.4 What type of content is in the response from the web server?
Html text, text/html

Ask for resource /grades.txt

2.4.1 How did your conversation with the Web server look like?
Jag ställde en fråga till servern(GET /grades.txt HTTP/1.0), servern svarade med statuskod samt den resurs som efterfrågades(/grades.txt)

2.4.2 What response code you got?
200 OK

2.4.3 What are response codes?
Standard svar till klientens begäran

2.4.4 What type of content is in the response from the web server?
Vanlig text som råkar vara HTML, text/plain

Uppgift 2.2

Metodbeskrivning

En fråga ställs till server da.dsv.su.se medan wireshark sparar paketen för inspektion. Paketet i fråga kontrolleras därefter.

Resultat

2.5.1 What are the IP addresses of both sender & receiver?
Sändare: 10.100.16.211
Mottagare: 130.237.177.253

2.5.2 Between which ports the packet was sent?
Sändare: 65059
Mottagare: 80

2.5.3 Which transport protocol used?
TCP

2.5.4 How large is the package in bytes?
56 bytes

2.5.5 Between which MAC addresses the packet was send?
Sändare: 40:e2:30:cf:d8:47
Mottagare: 00:09:0f:09:00:18

Uppgift 3

Metodbeskrivning

DNS cachen på den klient som används töms, i detta fall windows genom ”ipconfig /flushdns”. En DNS lookup utav adressen da.dsv.su.se genomförs medan wireshark sparar paketen, sedan hittas ”standard query response” paketet vilket sedan gås igenom för information.

Resultat

3.1.1 Which transport protocol was used by DNS?

UDP

3.1.2 Between which ports packet were sent?

Sändare: 53

Mottagare: 49775