Övningar – Nätverksteknik TCP Del2

Ett par instuderingsuppgifter som handlar om Nätverksteknik TCP Del 2.

1. Nämn några så kallade TCP-flaggor (som hittills har diskuterats) och vad de har för syfte:

2. Vad innebär TCP-flaggan **PSH**?

3. Till vilket syfte har flaggorna ECN och CWR ”nyligen” adderats till TCP-standarden?

4. Om en router på vägen mellan två kommunicerande enheter upplever stark stress och väljer att aktivera IP-flaggan ”Congestion Encountered”, vad skall mottagaren av detta göra?

5. Ändras *Window size* någonsin under tiden två parter kommunicerar med varandra?

6. Ändras *Maximum Segment Size* någonsin under tiden två parter kommunicerar med varandra?

TCP Del 2 Laboration

1. Kontrollera om det just nu finns några sessioner som håller på att initieras från den lokala datorn med hjälp av kommando:

   netstat –nao | FIND /i "syn"

   Syns någon? _____

   Skapa medvetet ett felaktigt anslutningsförsök genom att öppna webbläsare och skriva t ex i addressfältet:

   http://13.13.13.13

   Växla (snabbt!) över till kommandoprompt och kör samma netstat-kommando igen (pil upp). Syns någon sessions-öppning? _____

2. Installera programmet *PuTTy* (https://putty.org), detta är en gratis SSH-, Telnet och terminalklient.

   Starta en ny inspelning i Wireshark och ange som filter **tcp.port==23**

   Använd putty och skapa en session med telnet mot adressen **telehack.com** (Detta är en öppen telnet-server.

   Öppna endast session, gör inget mer sedan.

   Kontrollera sedan i Wireshark att vi ser data och hitta det första paketet som gått från dig. (Behåll inspelning igång.)

   Markera paketet och hitta avsändar- och mål-port:

   _____

   Expandera sedan ”Flags”. Är SYN aktiv? _____

   Öppna sedan svaret direkt efter och kontrollera TCP-flaggorna, vilka är aktiva (av de hittills diskuterade) ? _____

   Kontrollera sedan det tredje paket, vilken eller vilka flaggor är aktiva här?

   _____

   Stäng sedan telnet-fönstret så att sessionen avslutas.

Titta i Wireshark, hur sker sessionsnedstängningen, vilka paket/flaggor används?

_____
_____
_____
_____

3. Starta ny Wireshark-inspelning med samma filter som tidigare (**tcp.port==23**).

   Öppna en ny telnet-session mot IP-adress **telehack.com**.
   Växla till Wireshark och hitta det första SYN-paketet. Notera följande och gör en kort förklaring till de värden som syns:

   L2: Ethertype: _____

   L3: Protocol: _____

   L4: Destination Port: _____

   Sequence number: _____

   Om detta sekvensnummer visas som ett väldigt lågt tal, vad beror detta troligen på?

   _____

   Se värdet på ”Window size”. Till vad används denna Window-size från den *andra sidans* perspektiv?

   _____
   _____
   _____
   _____

   Titta på TCP-options längst ned i paketet. Notera följande och gör en kort förklaring till vad de betyder:

   Maximum segment size:
   _____
   _____
   _____
   _____

   Window scale:
   _____
   _____
   _____
   _____

TCP SACK:

4. Undersök vad programvaran **portqry.exe** och **NMAP** används till

5. Vi kommer istället för att använda portqry eller liknande verktyg att använda Powershell-kommandot **Test-NetConnection** som kan användas för att kontrollera TCP-anslutning mot en port åt gången.

   Starta inspelning i Wireshark och sätt ett filter enligt nedan:

   tcp.port==80

   Kör sedan (i Powershell-fönster):

   Test-NetConnection www.sunet.se -Port 80

   Titta sedan i Wireshark efter paket som hör ihop med detta. Vad händer efter att TCP-sessionen har upprättats?

   _____

6. Sätt nytt filter med **tcp.port==23** istället.

   Kör Test-NetConnection som ovan mot www.sunet.se fast mot port TCP/23 istället.

   Notera att det tar tid att utföra kommandot. Titta sedan i Wireshark, vilka paket syns?

   _____