TCP: How are the seq / ack numbers generated?

Asked 15 years, 9 months ago Modified 3 months ago

Viewed 33k times

20

I am currently working on a program which sniffs TCP packets being sent and received to and from a particular address. What I am trying to accomplish is replying with custom tailored packets to certain received packets. I've already got the parsing done. I can already generated valid Ethernet, IP, and--for the most part--TCP packets.

The only thing that I cannot figure out is how the seq / ack numbers are determined.

While this may be irrelevant to the problem, the program is written in C++ using WinPCap. I am asking for any tips, articles, or other resources that may help me.

c++ network-programming tcp winpcap

Share

Improve this question

Follow

edited May 4, 2012 at 18:47

Wooble

89.7k • 12 • 110 • 132

asked Mar 28, 2009 at 14:54

xian

4,683 • 5 • 35 • 38

The best place for standards-related information is usually the original RFC (Request for comments), in this case, RFC 2018. In general Wikipedia is also a good place to look. Failing that, you're almost guaranteed to get results here.
– Adam Liss Mar 28, 2009 at 15:03

8 Answers

Sorted by: Highest score (default)

29

When a TCP connection is established, each side generates a random number as its initial sequence number. It is a strongly random number: there are security problems if anybody on the internet can guess the sequence number, as they can easily forge packets to inject into the TCP stream.

Thereafter, for every byte transmitted the sequence number will increment by 1. The ACK field is the sequence number from the other side, sent back to acknowledge reception.

RFC 793, the original TCP protocol specification, can be of great help.

Share Improve this answer

Follow

edited Oct 7, 2021 at 7:34

Community Bot

1 • 1

answered Mar 28, 2009 at 15:02

DGentry

16.3k • 8 • 53 • 66

6 Isn't the ack field *not* the seq# from the other side, but seq# + received length (as in the zainee khan answer below)
– Ben Schwehn Aug 11, 2014 at 10:02

8

I have the same job to do. Firstly the initial seq# will be generated randomly(0-4294967297). Then the receiver will count the length of the data it received and send the ACK of `seq# + length = x` to the sender. The sequence will then be x and the sender will send the data. Similarly the receiver will count the length `x + length = y` and send the ACK as `y` and so on... Its how the the seq/ack is generated...

If you want to show it practically try to sniff a packet in Wireshark and follow the TCP stream and see the scenario...

Share Improve this answer

Follow

edited Dec 18, 2012 at 3:18

Jonathan Leffler

752k • 145 • 946 • 1.3k

answered Jul 8, 2010 at 10:49

zainee khan

81 • 1 • 1

1 Improve the clarity of your answer. – JSuar Dec 18, 2012 at 3:10

you can also capture packets from the terminal like this : sudo tcpdump -i eth0 – z atef Oct 2, 2016 at 4:03

6

If I understand you correctly - you're trying to mount a TCP SEQ prediction attack. If that's the case, you'll want to study the specifics of your target OS's Initial Sequence Number generator.

There were widely publicized vulnerabilties in pretty much all the major OS's wrt their ISN generators being predictable. I haven't followed the fallout closely, but my understanding is that most vendors released patches to randomize their ISN increments.

Share Improve this answer

Follow

answered Mar 28, 2009 at 16:16

Mark Brackett

85.6k ● 17 ● 111 ● 155

3

Seems that the rest of the answers explained pretty much all about where to find detailed and official information about ACK's, namely TCP RFC

Here's a more practical and "easy understood" page that I found when I was doing similar implementations that may also help TCP Analysis - Section 2: Sequence & Acknowledgement Numbers

Share Improve this answer

Follow

edited Oct 7, 2021 at 5:59

Community Bot

1 ● 1

answered Mar 28, 2009 at 15:07

Milan

15.8k ● 20 ● 59 ● 65

1

RFC 793 section 3.3 covers sequence numbers. Last time I wrote code at that level, I think we just kept a one-up counter for sequence numbers that persisted.

Share Improve this answer

Follow

answered Mar 28, 2009 at 15:00

John Ellinwood

14.5k ● 7 ● 40 ● 49

1

These values reference the expected offsets of the start of the payload for the packet relative to the initial sequence number for the connection.

Reference

> Sequence number (32 bits) – has a dual role If the SYN flag is set, then this is the initial sequence number. The sequence number of the actual first data byte will then be this sequence number plus 1. If the SYN flag is not set, then this is the sequence number of the first data byte

> Acknowledgement number (32 bits) – if the ACK flag is set then the value of this field is the next expected byte that the receiver is expecting.

Share Improve this answer

Follow

answered Mar 28, 2009 at 15:00

tvanfosson

532k ● 102 ● 699 ● 798

1

Numbers are randomly generated from both sides, then increased by number of octets (bytes) sent.

Share Improve this answer

Follow

edited Sep 4 at 23:06

Błażej Michalik

5,035 ● 44 ● 61

answered Mar 28, 2009 at 15:01

Kazimieras Aliulis

1,551 ● 3 ● 13 ● 25

0

The sequence numbers increment after a connection is established. The initial sequence number on a new connection is ideally chosen at random but a lot of OS's have some semi-random algorithm. The RFC's are the best place to find out more TCP RFC.

Share Improve this answer

Follow

answered Mar 28, 2009 at 14:59

sipsorcery

30.7k ● 25 ● 106 ● 158