TCP Attacks: TCP Sequence Number Prediction and TCP Reset Attacks

by Himanshu Arora on January 20, 2012

Though TCP protocol is a connection oriented and reliable protocol but still there a various loopholes that can be exploited. These loop holes are mostly explained in terms of attacks.

In the previous article on the TCP/IP Attacks series, we explained about ARP Cache Poisoning.

This article explains the following two attacks:

1. TCP sequence prediction attack
2. TCP reset attacks

An overview of TCP

Before getting started with explanations of attacks. Lets develop a basic understanding of how TCP works.

A TCP header looks like the following:
The below explanation explains how a connection is established between two hosts at TCP level. This is known as three way handshake. This handshake is required before any kind of data can be sent in each direction. Once the connection is established, data can flow bi-directionally with each packet containing sequence number of beginning byte of data it contains and acknowledgment of data received.

Suppose there are two hosts (A and B) who want to communicate with each other. Let’s suppose host A starts the communication. Now from TCP point of view, the host A sends a SYN packet to host B.

- A SYN packet is a TCP packet with SYN flag ON.
- Also mentioned in this packet is the Initial sequence number (which is a value generated by the TCP of host A), source port, destination port etc.
- When this packet is received at TCP layer of host B, this host replies with a TCP packet with SYN and ACK flags ON, Initial sequence number and other information.
- When host A receives this packet, it checks some information like the SYN flag, Acknowledgment Number (which should be Host A’s initial sequence number + 1) etc to verify that this is an expected packet from Host B.
- In reply, host A sends a packet with ACK flag ON and Acknowledgment number set to host B’s Initial sequence number + 1.

So we see that sequence numbers play an important role in TCP communication. A sequence number is a number that TCP associates with the starting byte of data in a particular packet. This way the receiving TCP layer knows the starting point of the data packet and can properly process it.
keeps track of data received and acknowledges accordingly. The acknowledgment number is always the next expected sequence number.

**TCP Sequence Prediction Attack**

Suppose Host A and Host B are communicating with each other. Now, lets say an attacker sitting in between is somehow able to monitor the packets between A and B.

Lets see what the attacker does:

- The attacker wants to attack Host A.
- It floods Host B with new requests causing a Denial of service attack to stop Host B from communicating with A.
- Now, the attacker can predict the sequence number of the packet that A is expecting from B.
- Attacker prepares such kind of packet and sends it to Host A.
- Since its a faked packet so host A thinks its coming from B.
- Now, this packet can be a packet terminating the connection or asking host A to run some malicious commands/scripts etc.

So this way a connection can be hijacked by an attacker.

Another way could be the prediction of ISN(initial sequence number).

Lets see an excerpt from RFC-793:

> When new connections are created, an initial sequence number (ISN) generator is employed which selects a new 32 bit ISN. The generator is bound to a (possibly fictitious) 32 bit clock whose low order bit is incremented roughly every 4 microseconds. Thus, the ISN cycles approximately every 4.55 hours. Since we assume that segments will stay in the network no more than the Maximum Segment Lifetime (MSL) and that the MSL is less than 4.55 hours we can reasonably assume that ISN’s will be unique.

BSD TCP/IP stacks diverts away from the above mechanism. BSD TCP/IP stacks increase the sequence number by 128,000 every second and by 64,000 for every new TCP connection. This as you can imagine is more predictable and hence can be easily exploited.

**TCP Reset Attacks**

This attack is fairly simple to understand once the above attack is clear to you. In this attack:

- Once the attacker is able to hijack a TCP session (as told above), this attack can be launched.
- The attacker sends packets with RST Flag ON to both A and B or any one of the host.
- Since both A and B do not know that an attacker has sent these packets so they treat these packets normally.
- Since they are reset packets so connection between A and B is terminated.

So we can see that TCP reset attacks are aimed to terminate a valid TCP connection between two hosts.
Linux provides several powerful administrative tools and utilities which will help you to manage your systems effectively. If you don’t know what these tools are and how to use them, you could be spending lot of time trying to perform even the basic administrative tasks. The focus of this course is to help you understand system administration tools, which will help you to become an effective Linux system administrator.

Get the Linux Sysadmin Course Now!

If you enjoyed this article, you might also like..

1. 50 Linux Sysadmin Tutorials
2. 50 Most Frequently Used Linux Commands (With Examples)
3. Top 25 Best Linux Performance Monitoring and Debugging Tools
4. Mommy, I found it! – 15 Practical Linux Find Command Examples
5. Linux 101 Hacks 2nd Edition eBook Free

Tags: Predictable TCP Initial Sequence Number, TCP Sequence Number Approximation Vulnerability, TCP Sequence Prediction

1 Denis January 20, 2012 at 3:38 am

   excellent tutorial. thank you very much. i was wondering if you could include more tutorials on storage?

2 Reynold February 4, 2012 at 10:27 am
Thanks for the info .. it would be great if you could add some practical ways to carry out this attack and the countermeasures that can be applied to protect the system from these kind of attack..

3 mike March 19, 2012 at 2:17 pm

Please add some demos!

4 ananthan July 27, 2012 at 9:00 am

This article lacks solution 😞
will setting time-stamps prevent this attack??

5 annenarg December 11, 2012 at 8:54 am

Time-stamps would not prevent this attack, because the attacker can estimate it, too.
- **COURSE**
  - [Linux Sysadmin CentOS 6 Course](#) - Master the Tools, Configure it Right, and be Lazy

- **EBOOKS**
  - [Free Linux 101 Hacks 2nd Edition eBook](#) - Practical Examples to Build a Strong Foundation in Linux
  - [Bash 101 Hacks eBook](#) - Take Control of Your Bash Command Line and Shell Scripting
  - [Sed and Awk 101 Hacks eBook](#) - Enhance Your UNIX / Linux Life with Sed and Awk
  - [Vim 101 Hacks eBook](#) - Practical Examples for Becoming Fast and Productive in Vim Editor
  - [Nagios Core 3 eBook](#) - Monitor Everything, Be Proactive, and Sleep Well

- **POPULAR POSTS**
  - [12 Amazing and Essential Linux Books To Enrich Your Brain and Library](#)
  - [50 UNIX / Linux Sysadmin Tutorials](#)
  - [50 Most Frequently Used UNIX / Linux Commands (With Examples)](#)
  - [How To Be Productive and Get Things Done Using GTD](#)
  - [30 Things To Do When you are Bored and have a Computer](#)
  - [Linux Directory Structure (File System Structure) Explained with Examples](#)
Linux Crontab: 15 Awesome Cron Job Examples
Get a Grip on the Grep! – 15 Practical Grep Command Examples
Unix LS Command: 15 Practical Examples
15 Examples To Master Linux Command Line History
Top 10 Open Source Bug Tracking System
Vi and Vim Macro Tutorial: How To Record and Play
Mommy, I found it! -- 15 Practical Linux Find Command Examples
15 Awesome Gmail Tips and Tricks
15 Awesome Google Search Tips and Tricks
RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams
Can You Top This? 15 Practical Linux Top Command Examples
Top 5 Best System Monitoring Tools
Top 5 Best Linux OS Distributions
How To Monitor Remote Linux Host using Nagios 3.0
Awk Introduction Tutorial – 7 Awk Print Examples
How to Backup Linux? 15 rsync Command Examples
The Ultimate Wget Download Guide With 15 Awesome Examples
Top 5 Best Linux Text Editors
Packet Analyzer: 15 TCPDUMP Command Examples
The Ultimate Bash Array Tutorial with 15 Examples
3 Steps to Perform SSH Login Without Password Using ssh-keygen & ssh-copy-id
Unix Sed Tutorial: Advanced Sed Substitution Examples
UNIX / Linux: 10 Netstat Command Examples
The Ultimate Guide for Creating Strong Passwords
6 Steps to Secure Your Home Wireless Network
Turbocharge PuTTY with 12 Powerful Add-Ons

- CATEGORIES
  - Linux Tutorials
  - Vim Editor
  - Sed Scripting
  - Awk Scripting
  - Bash Shell Scripting
  - Nagios Monitoring
  - OpenSSH
  - IPTables Firewall
  - Apache Web Server
  - MySQL Database
  - Perl Programming
  - Google Tutorials
  - Ubuntu Tutorials
  - PostgreSQL DB
  - Hello World Examples
  - C Programming
  - C++ Programming
  - DELL Server Tutorials
  - Oracle Database
  - VMware Tutorials
About The Geek Stuff

My name is Ramesh Natarajan. I will be posting instruction guides, how-to, troubleshooting tips and tricks on Linux, database, hardware, security and web. My focus is to write articles that will either teach you or help you resolve a problem. Read more about Ramesh Natarajan and the blog.

Support Us

Support this blog by purchasing one of my ebooks.

- Bash 101 Hacks eBook
- Sed and Awk 101 Hacks eBook
- Vim 101 Hacks eBook
- Nagios Core 3 eBook

Contact Us

Email Me: Use this Contact Form to get in touch me with your comments, questions or suggestions about this site. You can also simply drop me a line to say hello!.

- Follow us on Google+
- Follow us on Twitter
- Become a fan on Facebook

Copyright © 2008–2014 Ramesh Natarajan. All rights reserved | Terms of Service