Global Information Assurance Certification Paper

Naptha – TCP/IP Stacks in the Spotlight

Introduction

The RAZOR team has unveiled a whole group of DoS (Denial of Service) attacks. The RAZOR team is a group of security experts of the BindView Corporation, a company that offers IT (Information Technology) security solutions across multiple platforms. The attacks exploit TCP (Transmission Control Protocol) stack vulnerabilities, which allow impacting the host system in a variety of ways, ranging from simple slow down to complete shutdown of the system. The vulnerability affects a wide variety of operating systems, like Windows9x, Windows NT (both Microsoft), HP-UX (Hewlett-Packard), Solaris (Sun Microsystems), Linux and FreeBSD (free, open and non-commercial operating systems).

Background

The TCP stack is part of the TCP/IP (Transmission Control Protocol / Internet Protocol) stack, which is implemented in each major operating system and which is the core component of networked systems. As such it is one of the building blocks of network connectivity and the Internet. TCP is an Internet standard, described in RFC 793 (Request For Comment). Two peers communicate with each other via TCP IPC (Inter Process Communication).

Host A Host B

Process 2
Process 1

Port z
Port y
Port x
Port
Port
Port

TCP Stack
TCP Stack

Reliable

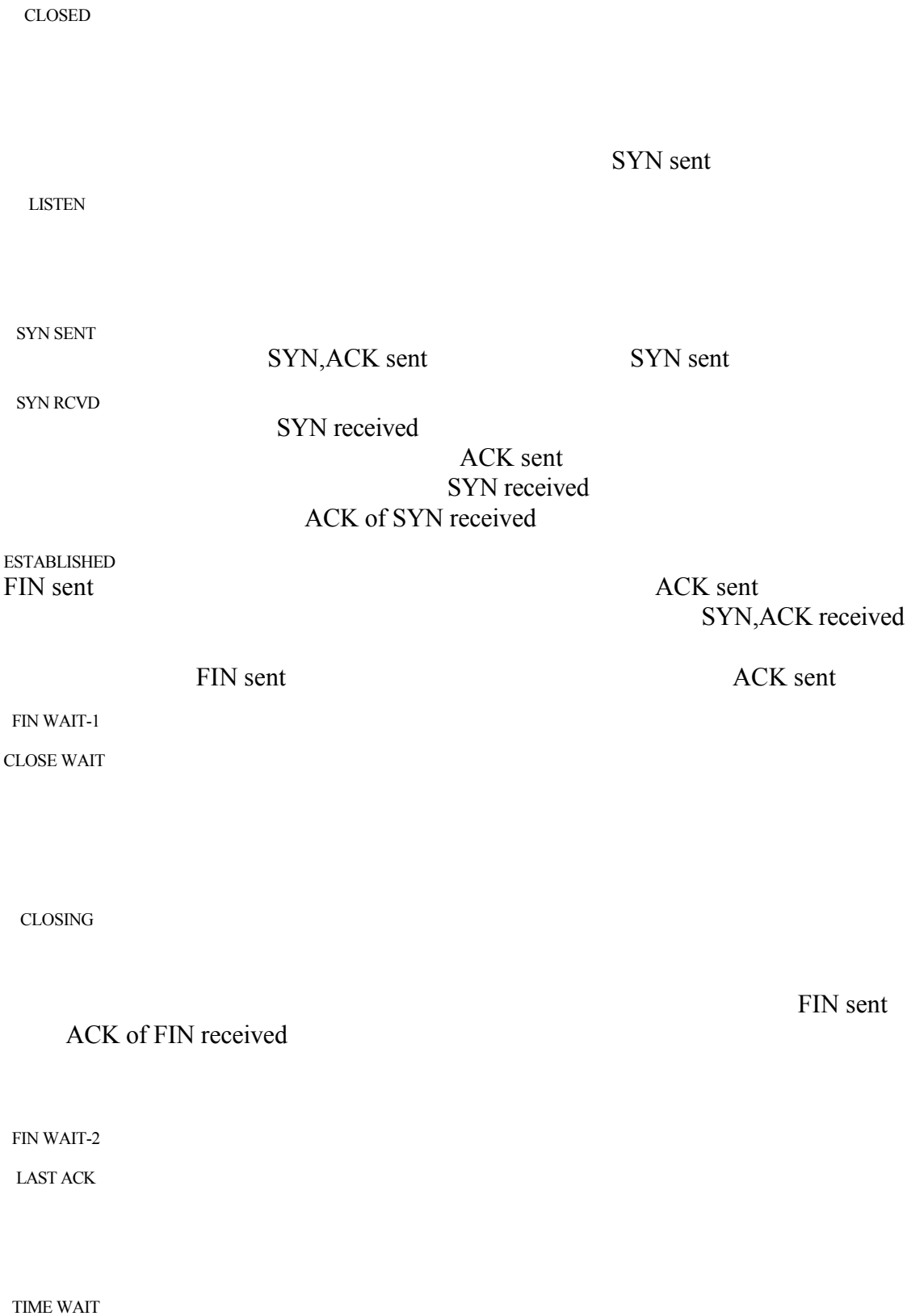
Communication

IP Stack
IP Stack

Unreliable

Communication

The one TCP layer from Host A communicates with the TCP layer from Host B via IPC. The TCP packets are handed down to the IP layer for delivery. IP is a connectionless protocol, whereas TCP is a connection-oriented protocol. The TCP stack fulfills a lot of important tasks in TCP/IP communication. One major function of the TCP layer is to add flow control, reliability and error recovery to the communication, in contrary to its counterpart UDP (User Datagram Protocol), which provides none of the TCP features. Consequently TCP is a much more complex protocol. TCP is a stateful protocol. A stateful protocol is a protocol where a master process, the server, keeps track of a client process, the client. It can be modeled as a finite state machine with eleven states. Below is a simplified state diagram, which shows the eleven states and the various interactions.



FIN received
ACK sent

Every communication process starts with the three-way handshake. The client sends a SYN packet to the server, containing its sequence number of the communication. The server responds with a SYN – ACK back to the client, confirming the client's sequence number and sending its own sequence number. Then the client in return sends another ACK, acknowledging the server's sequence number. Now the connection between client and server is established. When the connection shall be terminated, the server and the client exchange a similar communication dialogue to end the communication and close the connection gracefully. Either client or server sends a FIN request to the other. The other party sends an ACK followed by a FIN. A final ACK terminates the connection gracefully.
Denial of Service Attacks are a serious problem in the networked world. A Denial of Service Attack is aiming at exploiting certain vulnerabilities of a networked computer to make that computer unstable or even crash. The goal of that attack is in the end to interrupt service from that particular machine or network. The nature of the vulnerabilities exploited can be different. It can be a daemon or a service, which has a security issue, running on that machine. Or it can be an operating system component, like the protocol stack or the memory management (for example buffer overflow), which has some sort of flaw. This applies to any operating system and it is therefore very important to always implement the applicable security patches to the system. Off course you should configure your system in a secure way in the first place. And there is a lot of information available what can be done to prevent abuse of networked systems. A server should only be allowed to provide services and data for the purpose it is serving. All other requests shall be denied right away.

Denial of Service Attacks come in two different flavors. The original use of this attack was that a single system attacked another system. Later came a more sophisticated version of the DoS attack, the so-called DDoS (Distributed Denial of Service) attack. In this variant of the DoS attack the Victim (the attacked system) gets attacked by several machines, so-called Agents, from different locations. A Handler, a machine that the Attacker compromised first and setup to launch the attack, usually manages the Agents.

It is difficult to protect against DoS attacks. It is really important to setup and configure systems in the first place to make DoS attacks as difficult to execute as possible. This includes configuring your network and servers properly. In the following paragraph I will point out a few measures that can be taken to help protect against DoS attacks.

First measure that can be taken is to prevent IP address spoofing. Egress filtering can do this. It allows you to set up the network so that only valid IP addresses exit your network. With this measure you can prevent your network from being an active part of a DoS attack. Another important step is to not allow IP Directed Broadcast. IP Directed Broadcast allows to send a request to a broadcast address on a different subnet across the network. The Smurf attack for example uses this "feature". If a packet that uses a

broadcast address is routed across the Internet, only the last router can actually detect the broadcast address and filter it out. So it is important to configure the WAN router properly, using the correct features and access lists.

Description

The Naptha attack exploits weaknesses or flaws in TCP stack implementations. Apparently certain conditions apply when the TCP state machine is in a state other then SYN RECVD, including ESTABLISHED and FIN-WAIT 1, that allows a remote system to tight up or even exhaust certain system resources. This leads to system instability, service degradation or even interruption of service on the targeted host.

A very similar DoS attack is the SYN flood attack, which exploits a weakness of the way certain TCP stacks handle a large number of connection requests (SYN packets) in the SYN RECVD state. The way the attack is exercised is an attacker sends a lot of SYN's without ever sending any ACK's which leads to an accumulation of resources on the targeted host and finally to resource exhaustion. Naptha can be regarded as a serious network security threat. BindView released a new update to its "bv-Control for Internet Security" product, which allows testing for the vulnerability.

So far Microsoft and Compaq released patches for their Windows and Digital Unix operating systems. Sun Microsystems stated that connections between two Sun Solaris machines are not vulnerable to the way the attack is performed. However Sun and others are still investigating the issue as of this writing.

References

1. http://archives.neohapsis.com/archives/cc/2000-q4/0003.html
2. http://razor.bindview.com/index.shtml
3. http://www.bindview.com/news/display.cfm?Area=10&Release=/2000/1130.txt
4. http://www.cis.ohio-state.edu/htbin/rfc/rfc793.html
5. http://www.sans.org/dosstep/index.htm
6. http://www.cert.org/advisories/CA-2000-21.html
7. TCP/IP Tutorial and Technical Overview, Sixth Edition, Prentice Hall
8. Managing Bandwidth, Deploying QOS in Enterprise Networks, Prentice Hall