Global Information Assurance Certification Paper

James Farrell

IP Fragmentation Attacks on Checkpoint Firewalls

Introduction

Since the explosive growth of the Internet, corporations have met the demand and brought their business to the World Wide Web. As of January 2001, it is estimated that there are close to 110,000,000 hosts available on the Internet. However, corporations are not the only ones that have contributed to the growth of the Internet. The presence of the e-businesses has also led to the growth of consumers on the Internet. With more and more business being conducted on the web, it is no surprise that hackers and hacker organizations have also seen a population boom. The types of attacks have also grown; both in number and complexity. All of this translates into a strong need for technically capable security administrators who keep companies' assets secure and the link to the electronic commerce center open for business. Security administrators know that the most secure network is the one with no connection to the outside world. However, it is impossible to be completely secure and open for business on the web. Therefore, security administrators have had to deal with the never-ending game of trying to stay ahead of hackers. In addition to combating hacks aimed at stealing or destroying information, the security administrators must also defend against attacks designed to render a network or host unusable through a Denial of Service (DOS) attack. A DOS attack can consist of any of the following methods to deny service:

* Utilize bandwidth – A network based attack where the attacker generates traffic that leads to company's Internet connection being fully utilized so that no other traffic can be carried through connection

* Utilize system CPU – A host based attack where the attacker generates an attack that leads to CPU becoming overpowered

* Utilize available ports – A host based attack where the attacker generates an attack that sends numerous connections to host until all available ports are used

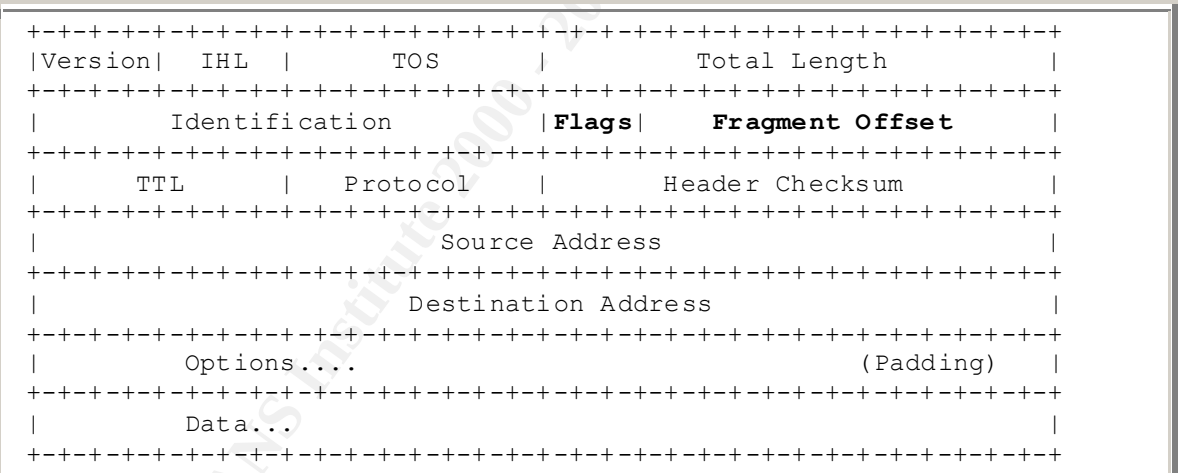
* Utilize system memory – A host based attack where the attacker generates an attack that consumes all of host's memory

A DOS attack is generally nothing more than a nuisance in that it renders a system unusable. At times, DOS attacks are used to mask more dangerous attacks. As a result of the threats of doing business on the Internet, security administrators use firewalls as a means to protect against attacks. However, at times, security administrators find that even firewalls are no match for the latest hack. On May 27, 2000, Lance Spitzner found a vulnerability of the Checkpoint Firewall-1 software. Spitzner was researching the way in which Checkpoint handles IP fragmentation when he discovered that the popular

firewall was susceptible to a DOS if numerous improperly fragmented packets were sent to or through the firewall.

What is IP Fragmentation?

During IP communications, packets are exchanged between two hosts. During the exchange of information, these packets may have to travel great distances and over a wide variety of transmission types. Different transmission media may have different constraints on the flow of information. These constraints can lead to fragmentation of IP packets. For example, when using Ethernet, the maximum transmission unit (MTU) is 1500 bytes, whereas as a 4M Token Ring environment has a default MTU of 4464 bytes. Consider the following situation: host A and host B are at the same company site. They are separated by a router, with host A being on Token Ring and host B being on an Ethernet segment. If host A is trying to communicate with host B, host A will send the packet out with 4464 bytes of data. Before the packet can be placed on the Ethernet wire, the router must fragment the packet into smaller packets that comply with Ethernet's smaller MTU. Once the router has fragmented the packet, it sends the fragments out to host B as individual IP packets. Once host B has received the fragments, host B then reassembles them.



Flags: Also used for fragmentation and reassembly. The first bit is the reserved bit and is always set to 0. The second bit is the Don't Fragment (DF) bit, which suppresses fragmentation. The third bit is called the More Fragments (MF) bit, and is used to indicate the last fragment of a packet so that the receiver knows that the packet can be reassembled.

Fragment Offset: Indicates the position of this fragment in the original packet. In the first packet of a fragment stream, the offset will be 0; in subsequent fragments, this field will indicate the offset in increments of 8 bytes.

FIGURE 1 – Fragmentation bits in an IP packet header

In figure 1 above, a standard IP packet is shown with the fragmentation sections displayed in bold print. The "flags" section make up three bits of an IP packet. The first of the three bits is a reserved bit and is always set to zero regardless of whether or not the packet is a result of fragmentation. The second bit is the Don't Fragment bit and is used to keep a packet from being fragmented. If a packet cannot be forwarded without fragmentation and this bit is set, then the gateway will discard the packet and send an ICMP destination unreachable, fragmentation blocked error message back to the sender. The third bit is the More Fragments bit. If this bit is set to one, more fragments will follow this packet. If this bit is set to zero, then the final fragment has been sent. The fragment offset field made up of 13 bits that carry the offset number. The destination host uses this number to determine the offset from the first fragmented packet. This field enables the destination host to be able to assemble the fragments in the correct order.

How is IP Fragmentation Used to Attack Firewall-1?

To understand how the IP fragmentation attack affects Checkpoint's Firewall-1 implementation, one must first understand how stateful inspection occurs on Firewall-1. The stateful inspection table is used by Firewall-1 to maintain the state of established connections going through the firewall. It also enables Firewall-1 to analyze packets to see if they are being received in the proper sequence. In the case of IP fragments, the Checkpoint firewall itself attempts to reassemble all fragments prior to forwarding them on to the final destination. This behavior was described in Lance Spitzner's document "Understanding the Firewall-1 State Table." In his writings, Spitzner describes a test scenario he performed where he sends all fragments of an original IP packet through the firewall. The firewall accepted the packets, logged the traffic in its event logs, and passed the packets on to the final destination host. Spitzner then sent a single fragment of an IP packet. Not only was the packet not accepted, it was neither logged in the firewall events log, nor passed on to the destination host. Based on his findings, Spitzner concluded that the firewall does not inspect fragments until all fragments have been received and the firewall has been successful in reassembling the original packet. Once the packet has been reassembled, the firewall would compare the packet to its state table, and then the rule base (if necessary) to decide whether or not to accept the packet.

This implementation of handling IP fragments makes Firewall-1 vulnerable to a Denial of Service attack. If incomplete fragments are continuously sent to the firewall, the firewall will wait for the remaining fragments to be received before handling the connection. A feature that Checkpoint added to their Firewall-1 software introduced this vulnerability. The excerpt below from the Checkpoint website describes why the feature was implemented:

> "To identify and audit attacks such as Ping of Death, Checkpoint added a mechanism to Firewall-1 – outside of its standard logging capability – to log certain events that occur during the Firewall-1 virtual assembly process. This

> fragmentation logging takes place on the gateway itself and not on the management station."

If enough incomplete fragment packets are sent to the firewall, system resources become fully consumed by the fragmentation logging process, and the firewall is unable to process any other connections. In this situation, either the system is locked up until the incomplete fragments cease and the firewall timeouts expire for these packets, or in some extreme cases, the system may crash. Since all of this occurs prior to comparison with the rule base, the rule base cannot be used to protect the firewall. Even a firewall with a rule base that drops all IP traffic is susceptible to this attack. Furthermore, since the packets are not sent to the rule base for inspection, the attack does not show up in the firewall log. In addition, the firewall is vulnerable to this attack whether the packets are sent to the firewall itself or to hosts that reside behind the firewall. Unlike many other Denial of Service attacks, this vulnerability does not require that the attacker have a large amount of bandwidth at his disposal, nor does it require accomplices to make the attack successful.

Based on Spitzner's findings, Bugtraq assigned the tracking number 1312 to this vulnerability. According to the Security Focus website, Checkpoint Firewall versions 4.0 and 4.1 are vulnerable to this attack. The vulnerability does not appear to be dependent upon Checkpoint running on any certain platform, although certain operating systems may be able to handle the illegal fragments prior to Checkpoint utilizing all of the available processor time. The exploit used to test this vulnerability was the jolt2 Denial of Service tool commonly used to attack Windows systems. This tool was used to send a stream of extremely large IP fragments to or through the firewall, which led to the logging mechanism consuming all CPU resources.

Checkpoint's Response to the Vulnerability

Shortly after the vulnerability was announced, Checkpoint offered the following statement:

> "Checkpoint is in the process of building new kernel binaries that will modify the mechanism by which fragment events are written to the host system console, as well as providing configurable options as to how often to log. In addition and independent of the console message writing, with the new binaries FireWall-1 administrators will be able use the Checkpoint log file method for reporting fragmentation events. These binaries will be released shortly in Service Pack 2 of FireWall-1 version 4.1, for 4.1 users, and as a Service Pack 6 Hot Fix for FireWall-1 version 4.0 users. A follow up response will be made to this forum when this software is available.
>
> As an interim workaround, customers can disable the console logging, thereby mitigating this issue by using the following command line on their FireWall-1 module(s):

$FWDIR/bin/fw ctl debug -buf

This takes effect immediately. This command can be added to the $FWDIR/bin/fw/fwstart command in order to be enabled when the firewall software is restarted. It should be noted that although this command will disable fragmentation console output messages, standard log messages (e.g., Long, Short, control messages, etc.) will continue to operate in their traditional way."

Checkpoint later release service packs for both Firewall-1 version 4.0 and Firewall-1 version 4.1 that addressed the vulnerability.

Other Ways to Defend

Obviously, this vulnerability shows that even security-minded companies can be vulnerable to hackers through Denial of Service attacks. We can also deduce from this that they can also be susceptible to more malicious attacks as well. So what is a security administrator to do to keep the corporate LAN secure? These administrators should be using a multi-layered approach to security. This vulnerability shows that one cannot assume a firewall by itself will keep a LAN secure from the evils on the Internet.

Security administrators should strive to keep their operating systems and software patched to the most recent certified release. In the situation with the IP fragmentation attack, many operating systems had already released patches that protected against jolt2 and similar attacks.

Another way in which security administrators can protect themselves would be to utilize an intrusion detection sensor. The sensors, like the operating systems must be updated on a regular basis. Intrusion detection developers routinely release updates to the signature files that the sensors use to detect an attack. Once the sensor has detected an attack, the administrator would be alerted. At that point, the administrator could choose to block packets from the perpetrator at the Internet gateway prior to the packets making it to the firewall. The administrator can choose to report the incident to the ISP's abuse desk for investigation.

Conclusion

In conclusion, the above arguments have shown how Checkpoint Fireweall-1 is vulnerable to the IP fragmentation attack. While this paper only addresses this vulnerability with regard to Checkpoint, other firewall implementations are vulnerable as well. Likewise, the IP fragment attack is not the only vulnerability Checkpoint has had to deal with. What this shows is that no one is safe from the constant pressure applied by hackers and their ever-evolving attacks. Security companies such as Checkpoint make great strides to help arm companies with a formidable arsenal to fend off attackers.

However, security administrators must have a multifaceted approach to security. It is unreasonable to think that in today's age of the hacker that a single line of defense will prove to be enough to keep a corporate network secure. In addition, security vendors must continue to stay abreast of new attacks and vulnerabilities. When the vendors learn of new attacks, timely updates and patches must be released to address the new concerns. If one looks at the historical growth of the Internet and correlates that with the projections for its future growth, one could only assume that hackers and their exploits will continue to grow as well. Security administrators must stay ready for battle.

References:

1. Spitzner, Lance. "Understanding the FW-1 State Table." November 2000. URL: http://www.enteract.com/~lspitz/fwtable.html

2. IT World.com. "Firewall-1 Vulnerable to Denial-of-service Attacks." June 2000. URL: http://www2.itworld.com/cma/ett_content_article/0,2849,1_1065,00.html

3. Internet Rack Monitor. "IP Fragmentation." June 1992. URL: http://irm.fnal.gov/software/locsys/syscode/ipsoftware/IPFragmentation.html

4. Sankar, Jaya. "Final Exam Solution." Date Not Available. URL: http://www.mscs.mu.edu/~ssitamra/MSCS209/final/02.htm

5. Kessler, Gary C. "An Overview of TCP/IP Protocols and the Internet." April 1999. URL: http://www.hill.com/library/publications/tcpip.shtml

6. SANS Institute. "Jolt2: DoS that Is Not Just for Windows Anymore." August 2000. URL: http://www.sans.org/infosecFAQ/malicious/jolt2.htm

7. Check Point Support. "IP Fragment-driven Denial of Service Vulnerability." Date Not Available. URL: http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html