GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

An Analysis of Fragmentation Attacks

Jason Anderson

March 15 2001

Introduction

Fragmentation is the term given to the process of breaking down an IP datagram into smaller packets to be transmitted over different types of network media and then reassembling them at the other end. This process is an integral part of the IP protocol and is covered in depth in RFC 791.

This paper will give a brief description of fragmentation, describe some common fragmentation attacks and look at some of the measures used to prevent them. It will also discuss some of the problems fragmentation attacks have on two widely used commercial firewall and IDS packages.

IP Fragmentation

So what is fragmentation and is it always bad?

Well the answer to this question is a definite no. As discussed earlier fragmentation is an integral part of the IP protocol and without it the Internet could not operate, as we know it today.
Fragmentation is necessary in order for traffic, which is being sent across different types of network media to arrive successfully at its intended destination. The reason for this is that different types of network media and protocols have different rules involving the maximum size allowed for datagrams on its network segment. This is known as the maximum transmission unit or MTU.
So in order to transmit a datagram across a network segment which has a MTU smaller than that of the packet to be transmitted fragmentation is required.

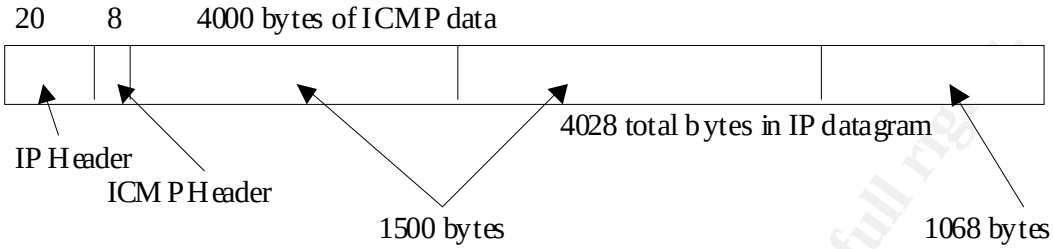
In order for a fragmented packet to be successfully reassembled at the destination each fragment must obey the following rules:

- Must share a common fragment identification number. Also known as fragment Id.
- Each fragment must say what its place or offset is in the original unfragmented packet.
- Each fragment must tell the length of the data carried in the fragment.
- Finally the fragment must know whether more fragments follow this one.

All of this information will be contained in the IP header. The header will be placed in an IP datagram followed by an encapsulated fragment (TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The following diagram shows the breakdown of an IP fragment, which displays the elements as stated above.



Ethernet MTU = 1500

Original 4028 byte fragment broken into 3 fragments of 1500 bytes or less.

Diagram: (TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour P4-8).

The following is the TCP dump output of the same fragmented datagram displaying how the various components above are displayed.

ping.com > myhost.com: icmp: echo request (frag 21223:1480@0+)
ping.com > myhost.com: (frag 21223:1480@1480+)
ping.com > myhost.com: (frag 21223:1048@2960)

notes:

- 21223 is the fragment Id
- 1480 in the first two fragments and 1048 in the last fragment shows the number of data bytes in the current fragment
- The last number of each fragment shows the fragment offset
- The + sign in the first two fragments indicate that more fragments follow

TCP dump: (TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour P4 - 16).

Types of Fragmentation Attacks

There are numerous ways in which attackers have used fragmentation to infiltrate and cause a denial of service to networks, some of these are discussed below.

Ping O' Death Fragmentation Attack

The Ping O' Death fragmentation attack is a denial of service attack, which utilises a ping system utility to create an IP packet, which exceeds the maximum allowable size for an IP datagram of 65535 bytes.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This attack uses many small fragmented ICMP packets which when reassembled at the destination exceed the maximum allowable size for an IP datagram. This can cause the victim host to crash, hang or even reboot.
This attack has however been around for quite sometime and all operating system vendors should have fixes in place to rectify this problem. It is however essential to ensure that you have the latest patches installed for your operating system.

The Tiny Fragment Attack

This attack uses small fragments to force some of the TCP header information into the next fragment. This may produce a case whereby the TCP flags field is forced into the second fragment and filters that attempt to drop connection requests will be unable to test these flags in the first octet thereby ignoring them in subsequent fragments.
This attack can be used to circumvent user-defined filtering rules. The attacker hopes that a filtering router will examine only the first fragment and allow all other fragments to pass.
This attack can be prevented at the router by enforcing rules, which govern the minimum size of the first fragment. This first fragment should be made large enough to ensure it contains all the necessary header information.

The Teardrop Attack

This is also a denial of service attack that can cause the victim host to hang crash or reboot, as was the Ping O' Death attack.
The teardrop attack utilises the weakness of the IP protocol reassembly process. The teardrop attack is a UDP attack, which uses overlapping offset fields in an attempt to bring down the victim host.
This type of attack has also been around for some time and most operating system vendors have patches available to guard against this sort of malicious activity.

The Overlapping Fragment Attack

Another variation on the teardrop attack that also uses overlapping fragments is the Overlapping Fragment Attack. This attack however is not a denial of service attack but it is used in an attempt to bypass firewalls to gain access to the victim host.
This attack can be used to overwrite part of the TCP header information of the first fragment, which contained data that was allowed to pass through the firewall, with malicious data in subsequent fragments. A common example of this is to overwrite the destination port number to change the type of service i.e. change from port 80 (HTTP) to port 23 (Telnet) which would not be allowed to pass the router in normal circumstances.
Ensuring a minimum fragment offset is specified in the router's IP filtering code can prevent this attack.

The Unnamed Attack

This attack is yet another variation on the teardrop attack that attempts to cause a denial of service to the victim host. This time however the fragments are not overlapping but are created in such a way that there is a gap created in the fragments.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This is done by manipulating the offset values to ensure there are parts of the fragment, which have been skipped. Some operating systems may behave unreliably when this exploit is used upon them.

Some Known Vulnerabilities in Checkpoint Firewall -1 and ISS Real Secure

Fragmentation attacks have been used as a tool by attackers to infiltrate and cause a denial of service to networks for some time now. Many commercially available software packages have experienced vulnerabilities when faced with some of the attacks listed previously. Two well-known packages that have been susceptible to these attacks are Checkpoint Firewall-1 and Internet Security Systems (ISS) RealSecure Intrusion detection system.

Checkpoint Firewall-1 Vulnerabilities

Checkpoint Firewall-1 is one of the more widely used firewall products on the market. By doing a search on the Internet for Checkpoint Firewall-1 vulnerabilities I came across several vulnerabilities which are related to fragmentation. These are detailed below.

IP Fragment-driven Denial of Service Vulnerability

This vulnerability was discovered by Lance Spitzner (lance@spitzner.net) and has been confirmed by Checkpoint. Testing by Checkpoint has confirmed that versions 4.0 and 4.1 of Firewall-1 are affected. Earlier versions of the product were not tested.

This vulnerability exploits the way Firewall-1 handles fragmented packets. Firewall-1 is a Statefull Inspection firewall and for security reasons it reassembles all IP fragments of a datagram prior to inspection against the security policy. This is done in order to guard against attacks such as the Overlapping Fragment attack as discussed in an earlier section of this paper.

In order to identify and audit attacks such as The Ping O' Death Checkpoint added a mechanism to Firewall-1 to log certain events that occur during the fragment reassembly process. This however can cause a possible denial of service to the firewall. As Firewall-1 reassembles the entire packet before sending it on it is possible to send a number of incomplete fragments to the firewall which can never be reassembled. This will cause the logging mechanism to consume all host CPU resources on the Firewall-1 gateway hence rendering the firewall inoperable.

This vulnerability has been addressed in version 4.1 service pack 2 (SP2) and version 4.0 service pack 7 (SP7). The logging mechanism has been modified in these service packs to consume minimal CPU cycles.
As an interim fix however it is possible to disable the console logging by entering the following command on the Firewall-1 module command line:

$FWDIR/bin/fw ctl debug –buf

Further information on this vulnerability can be found at the following site:
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

One-way Connection Enforcement Bypass

Sites allowing protocols employing unidirectional data flow connections (such as FTP and RSH STDERR) are susceptible to this vulnerability.

This vulnerability made it possible to bypass Firewall -1's normal directionality check by using specially fragmented TCP connection requests or by closing and reopening one-way TCP connections in conjunction with certain complex multi -connection protocols.

This vulnerability has been addressed in version 4.1 service pack 2 (SP2) and version 4.0 service pack 7 (SP7). These service packs feature tighter control of directionality checks which will prevent malicious back -channel communication.

Further information on this vulnerability can be found at the following sites:
http://www.checkpoint.com/techsupport/alerts/one_way.html
http://neworder.box.sk/showme.php3?id=2622

Internet Security Systems (ISS) RealSecure Intrusion Detection System Vulnerability

ISS RealSecure is one of the more widely used Intrusion Detection System products on the market. By doing a search on the Internet for RealSecure vulnerabilities I came across the following vulnerability which are relates to fragmentation. A description of this vulnerability is detailed below.

RealSecure RSKill Denial of Service Vulnerability

This vulnerability was discovered by the Modulo Security Labs Team and has been confirmed by ISS. This vulnerability affects version 3.2 of RealSecure.

This vulnerability uses IP fragmentation to cause a denial of service to the RealSecure engine causing it to crash.
A failure in the treatment of fragmented packets with the SYN flag set causes the immediate failure in the RealSecure engine, disabling the intrusion detection.
On the Solaris version of RealSecure the engine service file ('network_engine') is disabled, causing a core dump memory file creation. The event is immediately reported through the RealSecure console.
On the NT version, the engine ('network_engine.exe') has a different bug. The service after crashing, restarts immediately, generating a Windows NT Application Log event. A large and continuous stream of these fragmented packets (SYN Flood) take the processor load up to 100% thus rendering the RealSecure engine inoperable and unable to detect any other attacks.

In order to rectify this vulnerability you will need to apply the 3.2.2 patch, available from Internet Security Systems Customer Support (support@iss.net).
Further information on this vulnerability can be found at the following sites:
http://xforce.iss.net/static/5133.php
http://www.securityfocus.com/archive/1/77548

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Conclusion

As you can see fragmentation is a necessary part of the IP protocol but it has also been used extensively by attackers to circumvent and bring down firewalls and intrusion detection systems.
Although most of the attacks described in this paper have been around for some time they still can cause problems if your systems are not updated to the latest versions of patches and service packs.

References

TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour.

Northcutt Stephen. Network Intrusion Detection – An Analyst's Handbook, 1999, New Riders Publishing.

Ptacek, Thomas. Newsham, Timothy. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection". January 1998. URL: http://secinf.nrt/info/ids/idspaper/idspaper.html

Unknown. "RFC791 Internet Protocol DARPA Internet Program Specification" September 1981. URL: http://www.rfc-editor.org/rfc/rfc791.txt

Merkow, Mark. "E-Commerce Security Technologies – Part One". 02 December 1999. URL: http://ecommerce.internet.com/outlook/article/0,1467,7761_253601_2,00.html

Spitzner, Lance. "Understanding the FW-1 State Table". 29 November 2000. URL: http://www.enteract.com/~lspitz/fwtable.html

Fucs, de Miranda. "RealSecure Vulnerable to a DoS (Fragmented SYN)". 30 August 2000. URL: http://neworder.box.sk/showme.php3?id=2627

Unknown. "RealSecure RSKill Denial of Service". August 2000. URL: http://xforce.iss.net/static/5133.php

Unknown. "IP Fragment-driven Denial of Service Vulnerability". 31 January 2001. URL: http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

Unknown. "Potential Security Issues in VPN-1/FireWall-1". 31 January 2001. URL: http://www.checkpoint.com/techsupport/alerts/list_vun.html

Unknown. "Common Vulnerabilities and Exposures". 22 January 2001. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0804

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.