Global Information Assurance Certification Paper

The truth about ICMP

Lindsay van Eden

Introduction:

ICMP: Internet Control Message Protocol.

"Jeah sure, add a rule to the firewall. It's only ICMP"
-Famous last words perhaps?

It never ceases to amaze me that there are so many individuals who seem to be under the impression that ICMP is a completely harmless protocol.
That PING and ICMP are one of the same and the definitive test as to whether a host is alive.

I must admit that I too used to believe it was a pretty harmless protocol. I knew that it carried a payload but had no idea as to the depth of information one could obtain from it. Things like, what services are running on the hosts, how those hosts are organized and what operating systems are they running.

Scary stuff I know, but with this paper I hope to create an awareness of the true dangers of ICMP.

What does ICMP do?

ICMP normally contain control messages and is a vital part of IP.
Although not designed to be 100% reliable, ICMP is how we receive information about routing difficulties, simple exchanges such as echo transactions and errors in datagram processing.

Does everyone know what ping does?
Ping uses timed IP/ICMP ECHO_REQUEST and ECHO_REPLY packets to probe the "distance" to the target machine. Now I'm pretty sure that no one has ever seen a PING that looks like this:

Pinging 196.30.30.1 with 32 bytes of data:

Sorry, your default gateway appears to be switched off: Request timed out,
Sorry, your default gateway appears to be switched off: Request timed out,
Sorry, your default gateway appears to be switched off: Request timed out,

Ping statistics for 196.30.30.1
Packets: Sent = 4, Received = 0, Lost = 100 (100% loss),
Approximate round trip times in milli-seconds:

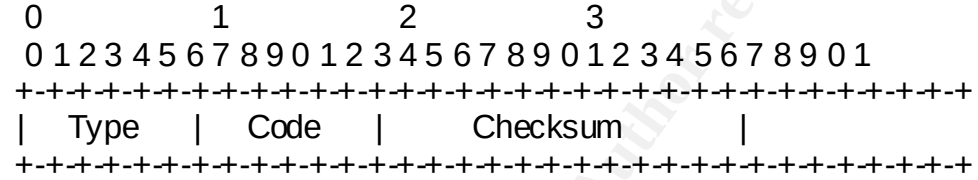
Minimum = 0ms, Maximum = 0ms, Average = 0ms

So where are these so called ICMP messages I've been talking about?.

Well, ICMP messages are sent for a number of different reasons such as/including errors and information.

ICMP is catagorised into 'types' and 'codes'. Each ICMP 'type' has a specific function, and the 'codes' within a given type offer a degree of specification or granularity to this 'type'.

An ICMP header is 8-bytes (64-bits) long. It may contain more data depending upon the exact operation being performed.



For example, Type 11 - Time Exceeded
Type 11 Code 0 - Time to live exceeded in transit
Type 11 Code 1 - Fragment reassembly time exceeded

Type	Code	Description
0		Echo Reply
3		Destination Unreachable
3	0	Net Unreachable
3	1	Host Unreachable
3	2	Protocol unreachable
3	3	Port Unreachable
3	4	Fragmentation needed and DF set
3	5	Source route failed
4		Source Quench
5		Redirect
5	0	Redirect datagrams for the network
5	1	Redirect datagrams for the host
5	2	Redirect datagrams for the type of service and network
5	3	Redirect datagrams for the type of service and host
8		Echo Request
11		Time Exceeded
11	0	Time to live exceeded in transit
11	1	Fragment reassemble time exceeded.
12		Parameter Problem
13		Timestamp
14		Timestamp Reply

15		Information Request
16		Information Reply

In practice, while running a tcpdump or snoop (these are both UNIX based network packet sniffers) one may receive a Type 3 Code 3 message. From this one can ascertain that the IP module cannot deliver the datagram as the indicated protocol or process is not active. (Type 3 Code 3 = Destination port unreachable, normally associated with UDP sockets not listening)

ICMP does have advantages.

An ICMP type that should not be filtered is type 3 code 4 (Fragmentation needed and DF set). Let's say one has a particular host connected to an Ethernet segment which wanted to communicate to another host separated by a serial link. The default Ethernet MTU (Maximum Transmit Unit) is 1500bytes while the serial is 576bytes. The packets would have to be segmented due their size but the 'Do not Fragment' flag is set. (too large for the serial MTU) .One would never know that the packets are to big to transmit if it weren't for the icmp packet

So ICMP serves it's purpose of providing feedback about problems in communication.

How does ICMP become a problem?

Take a look at your current organization. How many times have you seen users logging calls and complaining that the network is down just because they are unable to PING.
A happy user is a user that can PING so companies often allow icmp to traverse their network and firewall.
"My application is not working as I cannot ping the firewall" - hmm, that sounds familiar.

This is when the system breaks down. Network administrators and such tend to turn a blind eye due to the pressure from users. You know they're going to complain to mangement who in turn will instruct it to be allowed. This is when it becomes vital that the risks are communicated to management as it could one day be the downfall of your network!!

How is ICMP exploited?

Firstly, there is no such thing as an ICMP port. Would be hackers use ICMP messages to obtain information about one's network and to even redirect traffic.

Take an ICMP redirect message. What if the ICMP packet was generated by a host "acting" as a router. The router could than be tricked into using a false

route. The attacker could than direct the traffic straight to their host where they could have an application waiting to receive and interpret the contents. Contents which they, under normal circumstances would and often should not have access to.

There are lots of potential denial of service (DoS) threats available through ICMP). One of them being an ICMP bomb. An ICMP bomb often includes forged messages such as EOF (end of file), dead socket, redirect, information etc. They may also be used in a denial of service attack. This could be when a host is sent a route that loses it's connectivity or is sent an ICMP Network Unreachable packet The host thinks that it can no longer access a particular network.

ICMP Sweeps are yet another form of attack. It's a way of querying multiple hosts using ICMP ECHO. However, with today's firewalls and routers, one can block this type of traffic. To get around it, one could use a more advanced ICMP scanning technique. Try making use of the non-ECHO ICMP protocols (types that are not protocols - ALL ICMP is IP protocol 1). These include support to request timestamp and netmask information. Many firewall and packet filter designers forget to block all ICMP traffic and only filter ECHO traffic. In this case, making non-ECHO requests is still a valid form of host identification.

There are a number of programs that use ICMP as a basis for obtaining information.
Nmap and Snort are perfect examples.

In short, I've listed an explanation of each message and where applicable, a possible attack.

Type	Code	Possible attack
0		The infamous Smurf - ICMP echo requests to a network broadcast with a spoofed source address of the victim. Hense the victim obtains serveral (potentailly thousands) replies...tying up the victims network resources: * Don't forget type 0 is the REPLY
3		According the gateway's routing tables, the destination network is unreachable: I'd watch out for the typical Denial of service attack.
3	0	Route configuration problem or incorrectly specified IP address.
3	1	It means that the router one hop before the destination host

		could not ARP the host.
3	2	This means that the receiver of the packet does not have anything that recognizes the specified IP protocol of the packet. This is something hardly every seen in practice. Either there's a configuration problem or a possible attack.
3	3	The server tells the client that nobody is listening at the port the client attempted to contact. Normally UDP – Unix traceroute makes use of this.
3	4	In practice one should not be see this being dropped. There could be a misconfigured your firewall.
3	5	This is an obvious attack against your Win9x and Solaris hosts. The would be hacker can DoS you by redirecting your default router. A neighboring hacker can also do a man-in-the-middle attack by directing you through his/her router.
4		Congestion. Somebody could flood your network with these packets in an attempt of tricking your hosts to slow transmitting data. For those of you getting ideas, this is not as easy as it seems as there are specific ICMP header fields required to "Legitimise" the packet to the destination.
5		Another man in the middle attack or mismanaged routes.
5	0	Redirect datagrams for the network
5	1	Redirect datagrams for the host
5	2	Redirect datagrams for the type of service and network
5	3	Redirect datagrams for the type of service and host
8		Ping. Echo Request.
11		This is when the packet never reaches its target destination because it's times out. Such as the gateway processing the datagram finds the Time to live exceeded.
11	0	The frame passed through sufficient gateway devices that the TTL (time to live) field which is set on transmition (often to 255) was decremented to 0. Each gateway decrements this field by one before forwarding it

		Basically, the router dropped the packet either because of a routing loop or maybe because of an access-list.
11	1	The host dropped the packet because it didn't receive all the fragments.
12		Something unusual is going on, and probably indicates an attack. The gateway finds an error in the header parameters. The pointer identifies the octet of the original datagram's header where the error was detected.
13		Timestamp: The host can request the "time" from another host. The timestamp is 32 bits of milliseconds since midnight UT. The originate timestamp is the time the sender last touched the message before sending it. The receive timestamp is the time the echoer first touched it on receipt. The Transmit timestamp is the time the echoer last touched the message on sending it. (?huh?)
14		Timestamp Reply
15		Information Request
16		Information Reply

Conclusion:

ICMP is a great hacking tool as it's versatile, mostly overlooked and let's not forget, commonly misunderstood. Engineers, administrators, security officers etc. need to be aware of the dangers.

The amount of information carried within the message can be used by attackers to exploit known vulnerabilities.

How are you going to explain to the board of directors that your network's been compromised because icmp was allowed through??

References:

Graham, Robert "Firewall, FAQ: Firewall Forensics (What am I seeing?)" Copyright 1998-2000 http://secinf.net/info/fw/firewall-seen.html

Arkin, Ofir "ICMP Usage in Scanning" July 2000 http://secinf.net/info/misc/ICMP_Scanning/ICMP_Scanning.html

The Black2 Team: Ajay Kumar Gummmadi; Eric Daniel; Faisal Karim; Ikram Ahmed Khan; Ralph Akram Gholmieh; Raul Gonzalez Barron; Rehan Ayyub Sheikh "'Advanced Networking Security" CPSC689 - Summer '96 http://secinf.net/info/unix/report.html

Postel, J "Internet Control Message Protocal Darpa Internet Program Protocol Specification" - RFC 792 September 1981 http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc792.html

Bontoft, Andy "Checkpoint Firewall-1 Rulebases*" April 2001 Dimension Data Security.