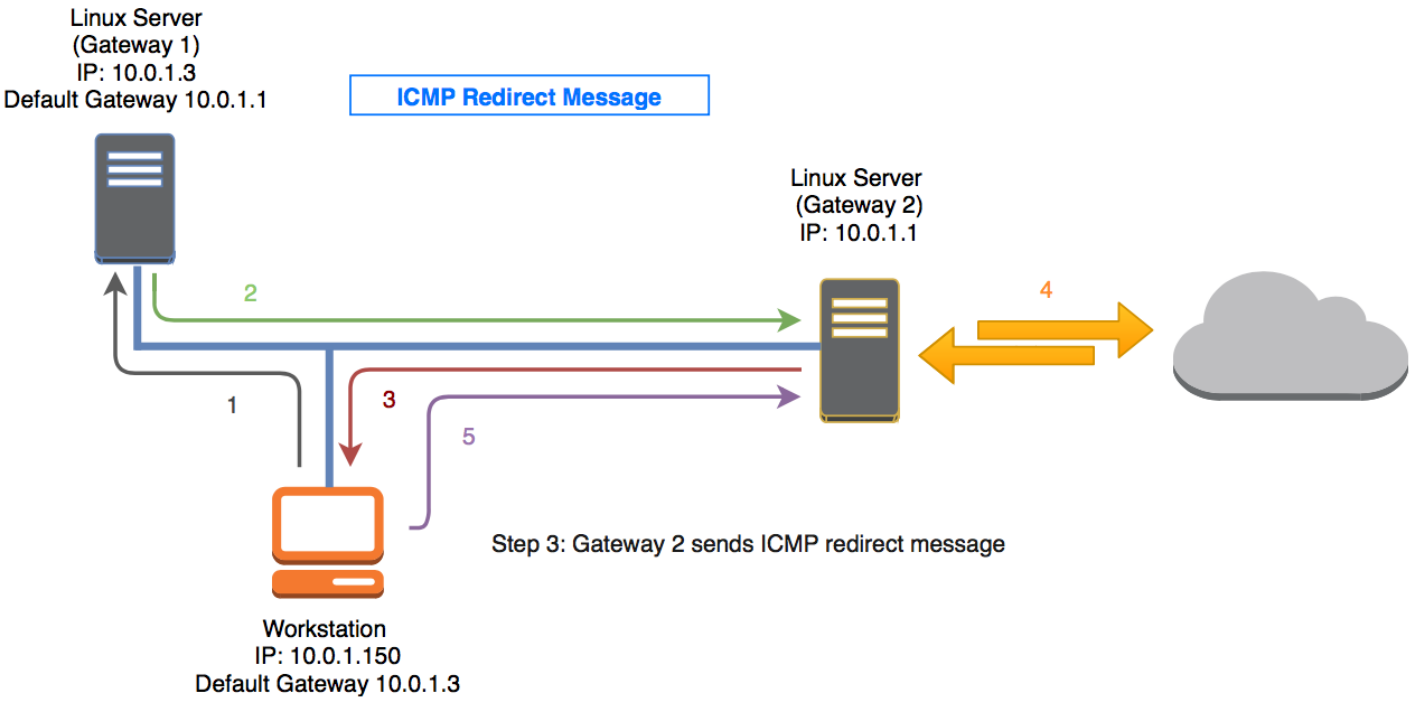

ICMP: The Good, the Bad, and the Ugly

Misconceptions of ICMP

Drew Branch Follow
Jul 19, 2016 · 5 min read

The Internet Control Message Protocol (ICMP) allows Internet hosts to notify each other of errors and allows diagnostics and troubleshooting for system administrators. Because ICMP can also be used by a potential adversary to perform reconnaissance against a target network, and due to historical denial-of-service bugs in broken implementations of ICMP, some network administrators block all ICMP traffic as a network hardening measure. In this blog post, we review the beliefs for why administrators are motivated to block ICMP, the reasons why this is not an effective security measure against any level of targeted attack, and side effects of blocking ICMP that break legitimate network functionality. Finally, we suggest

ways to block only the parts of ICMP that allow network discovery for networks where this is a concern.

Introduction to ICMP

When most people think about the Internet Control Message Protocol (ICMP), two network utilities come to mind — Ping and Traceroute. While Ping and Traceroute are two tools that use ICMP, they are not its only purpose. ICMP is also used by network devices to send error messages, which describe a problem encountered while attempting to deliver a datagram. Network administrators can use these messages to troubleshoot internet connectivity issues. For example, a gateway or destination host will send an ICMP message to the source host if an error or an event that requires warning has surfaced (e.g., destination is unreachable, packet loss, etc). Operating systems' network stacks can read ICMP messages to generate error codes to applications so that they can display an informative error message to the user.

Historically there were 255 requests/responses that comprised ICMP. Many are deprecated or reserved for various reasons; ten types of ICMP messages relevant to modern networks are shown in Table 1. Within each message type, there are several codes to identify a specific condition or request.

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation needed and DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect datagram for the Network
	1	Redirect datagram for the host

	2	Redirect datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem	0	Pointer indicates error
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

Table 1. Relevant ICMP messages [1].

Blocking ICMP Traffic for Security

Network administrators often opt to disable ICMP on network devices to evade network mapping applications used by adversaries (e.g., Nmap and Nessus scans). Unwarranted actions such as network discovery attacks, covert communication channels, and network traffic redirection could all be executed with ICMP enabled, which include but are not limited to:

- Ping sweep — A type of attack that uses ICMP echo request messages to enumerate live hosts on a network.
- Ping flood — Utilized to launch a denial of service attack (DoS), where the attacker sends ICMP requests in a rapid succession without waiting for the targeted system to respond. Ping floods aim to consume both incoming and outgoing bandwidth as well as utilize CPU resources to degrade the system's performance.

- ICMP tunneling — A method used to establish a covert communication channel between remote systems, most times between a client and a proxy. All communications are sent via ICMP requests and replies. ICMP tunneling could be used to bypass firewall rules.

- Forged ICMP redirects — Network traffic could be fraudulently redirected to an attacker via a forged ICMP redirect message. The attacker would send a ICMP redirect message, which informs a host of a direct path to a destination, to the victim that contains the IP addresses of the attacker's system. This allows an attacker to compromise network traffic via a man-in-the-middle attack or cause a DoS.

Due to all of the possible attacks involving ICMP, and the fact that TCP/IP "mostly" works even when ICMP traffic is blocked, network administrators sometimes block ICMP traffic on their firewalls as a "quick fix" security measure.

Impacts of Blocking ICMP

By disabling the ICMP protocol, diagnostics, reliability, and network performance may suffer as a result (see page 4–4 of [2]). Important mechanisms are disabled when the ICMP protocol is restricted.

- Path MTU discovery (PMTUD) — Used to determine the maximum transmission unit size on network devices that connects the source and destination to avoid IP fragmentation[3]. ICMP type 3, code 4, and max packet size are returned when a packet exceeds the MTU size of a network device on the connected path. If these ICMP messages are blocked, the destination system continuously requests undelivered packets and the source system continues to resend them infinitely but to no avail, since they are too large to pass through the complete path from the source to the destination. This behavior most likely will cause a hang and is called an ICMP black hole[4].

- Time to live (TTL) — Defines the lifespan of a data packet while traveling from source to destination. The lifespan of a packet is set by a timestamp or a hop counter to ensure the datagram does not propagate through the Internet indefinitely. A

network device with ICMP blocked will not receive type 11, time exceeded, code 0, time exceeded in transit error message — notifying the source host to increase the lifespan of the data to successfully reach the destination, if the datagram fails to reach the destination[5].

- ICMP redirect — Utilized by a router to inform a host of a direct path from the host (source) to destination. This reduces the amount of hops data has to travel through to reach the destination. With ICMP disabled, the host will not be aware of the most optimal route to the destination — causing the host to send data through excessive network devices, consuming unnecessary resources which leads to the reduction of network performance.

Better Ways to Prevent ICMP Abuse

Disabling the full ICMP protocol may not be a good approach in securing network devices. Instead disabling a subset of ICMP types provide fine-grained control over which types of ICMP messages network devices could request, receive, and respond to.

On Linux, iptables [5] provides users an avenue to achieve fine-grained control over ICMP. For example, to allow echo reply enter the follow shell command within a terminal:

```
sudo iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

or

```
sudo iptables -A OUTPUT -p icmp --icmp-type 0 -j ACCEPT
```

The example above will allow all outgoing echo replies where:

```
-A OUTPUT is the target chain
```

```
-p icmp is the protocol

--icmp-type 0 is the messages type (echo reply)

-j ACCEPT is the action to be carried out.
```

When evaluating which message types a network device should be permitted to send and receive, device type and purpose should be taken into consideration. Completely blocking the whole ICMP may not be the best solution when attempting to implement supplementary layers of protection against network attacks. An assessment of each network device should be carried out to determine which types of messages should be disabled to provide additional security or remain enabled to maintain a high level of network performance.

Drew Branch is a Security Analyst at Independent Security Evaluators.

Twitters: @ISESecurity

Networking Internet Programming Linux Security