ICMP Ping Spoofing and ICMP Redirect Attack

CSE 406: Computer Security

Group 3
2005004: Md Zim Mim Siddiqee Sowdha
2005018: Munzer Mahmood

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology

July 27, 2025

Outline

1. ICMP Fundamentals
2. Ping: How and Why It Works
3. ICMP Ping Spoofing
4. ICMP Redirect Attack
5. Defenses
6. Thank You!

What is ICMP?

- Internet Control Message Protocol (RFC 792)
- Used by routers and hosts for diagnostics and error reporting
- Not for data transfer, but for control messages in IP networks

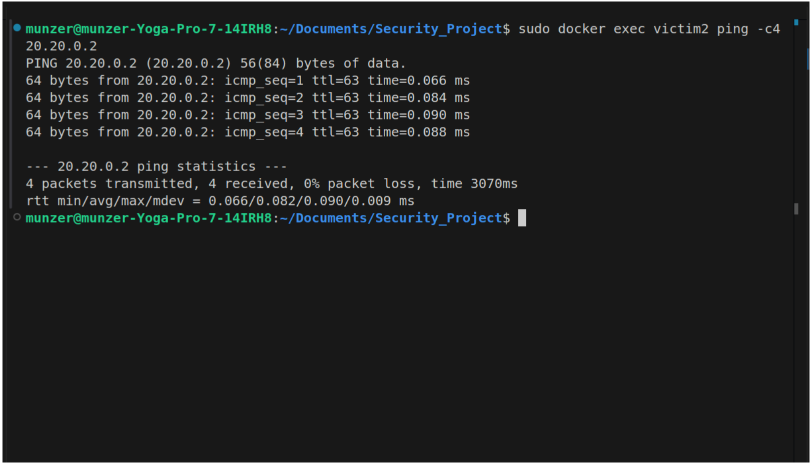
Why ICMP is Used

- Diagnose reachability and latency (Ping)
- Trace routing paths (Traceroute)
- Report network errors (unreachable, TTL expired)
- Route optimization (ICMP Redirect)

What is Ping?

- Sends ICMP Echo Request (Type 8, Code 0)
- Receives ICMP Echo Reply (Type 0, Code 0)
- Measures round-trip time (RTT) and packet loss

Ping Packet Flow



```
munzer@munzer-Yoga-Pro-7-14IRH8:~/Documents/Security_Project$ sudo docker exec victim2 ping -c4
20.20.0.2
PING 20.20.0.2 (20.20.0.2) 56(84) bytes of data.
64 bytes from 20.20.0.2: icmp_seq=1 ttl=63 time=0.066 ms
64 bytes from 20.20.0.2: icmp_seq=2 ttl=63 time=0.084 ms
64 bytes from 20.20.0.2: icmp_seq=3 ttl=63 time=0.090 ms
64 bytes from 20.20.0.2: icmp_seq=4 ttl=63 time=0.088 ms

--- 20.20.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.066/0.082/0.090/0.009 ms
munzer@munzer-Yoga-Pro-7-14IRH8:~/Documents/Security_Project$
```

Normal ICMP Echo Request/Reply Sequence

ICMP Echo Packet Structure

- `Type = 8, Code = 0`: Echo Request
- `Type = 0, Code = 0`: Echo Reply
- Fields: Checksum, Identifier, Sequence Number, Payload

Type (1B) — Code (1B) — Checksum (2B) — Identifier (2B) — Sequence (2B) — Data

What is Ping Spoofing?

- Attacker forges ICMP Echo Replies or Requests
- Impersonates a legitimate host to confuse monitoring
- Goals:
  - Hide presence
  - Disrupt diagnostics
  - Bypass filters

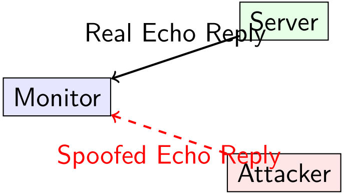
Why Attack Ping?

- Firewalls often allow ICMP for network checks
- Monitoring tools trust ICMP replies implicitly
- Spoofing can mislead logs and intrusion detection

Ping Spoofing Objectives

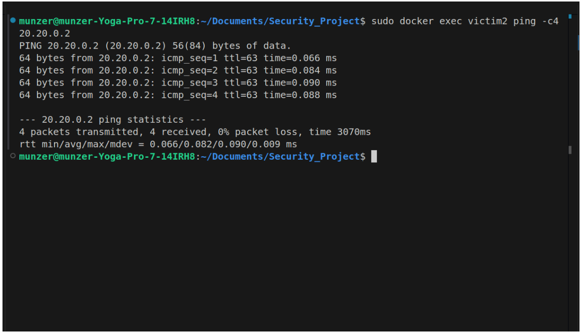
- Hide malicious traffic by impersonation
- Evade intrusion detection systems
- Pollute network logs
- Bypass IP-based access controls

Ping Spoofing Attack Steps



1. Attacker crafts ICMP packet with victim's IP as source
2. Sends forged Echo Reply to the monitoring host
3. Monitoring host accepts reply as genuine
4. Real Echo Reply from server may arrive separately

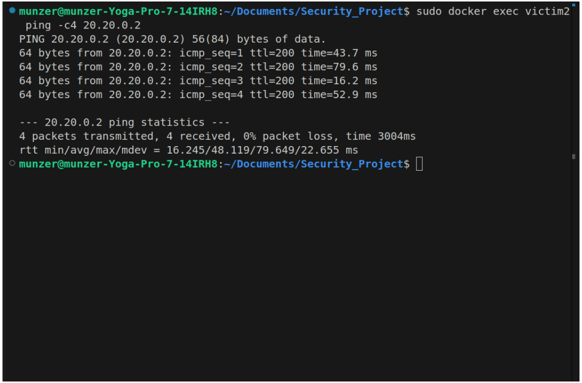
Spoofed vs. Normal Echo Replies



```
munzer@munzer-Yoga-Pro-7-14IRH8:~/Documents/Security_Project$ sudo docker exec victim2 ping -c4
20.20.0.2
PING 20.20.0.2 (20.20.0.2) 56(84) bytes of data.
64 bytes from 20.20.0.2: icmp_seq=1 ttl=63 time=0.066 ms
64 bytes from 20.20.0.2: icmp_seq=2 ttl=63 time=0.084 ms
64 bytes from 20.20.0.2: icmp_seq=3 ttl=63 time=0.090 ms
64 bytes from 20.20.0.2: icmp_seq=4 ttl=63 time=0.088 ms

--- 20.20.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.066/0.082/0.090/0.009 ms
munzer@munzer-Yoga-Pro-7-14IRH8:~/Documents/Security_Project$
```

Normal Echo Reply



```
munzer@munzer-Yoga-Pro-7-14IRH8:~/Documents/Security_Project$ sudo docker exec victim2
 ping -c4 20.20.0.2
PING 20.20.0.2 (20.20.0.2) 56(84) bytes of data.
64 bytes from 20.20.0.2: icmp_seq=1 ttl=200 time=43.7 ms
64 bytes from 20.20.0.2: icmp_seq=2 ttl=200 time=79.6 ms
64 bytes from 20.20.0.2: icmp_seq=3 ttl=200 time=16.2 ms
64 bytes from 20.20.0.2: icmp_seq=4 ttl=200 time=52.9 ms

--- 20.20.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 16.245/48.119/79.649/22.655 ms
munzer@munzer-Yoga-Pro-7-14IRH8:~/Documents/Security_Project$
```

Forged Echo Reply from Attacker

Detecting and Mitigating Spoofing

- Enable reverse path filtering (`rp_filter`)
- Rate-limit ICMP traffic
- Validate source MAC–IP mappings
- Use IPsec for authenticated diagnostics

What is an ICMP Redirect Attack?

- ICMP Redirect suggests a better next-hop router
- Attacker sends spoofed Redirect to reroute traffic
- Enables interception or denial-of-service

Why Attack Redirects?

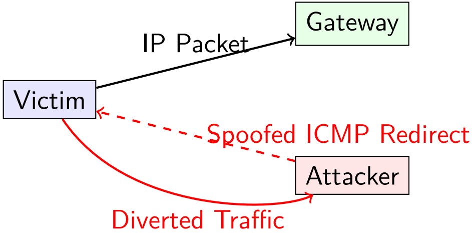
- Routers silently optimize paths using ICMP Redirect
- Hosts trust redirects by default
- Malicious redirects bypass network policies
- Attackers gain visibility into traffic

Redirect Attack Objectives

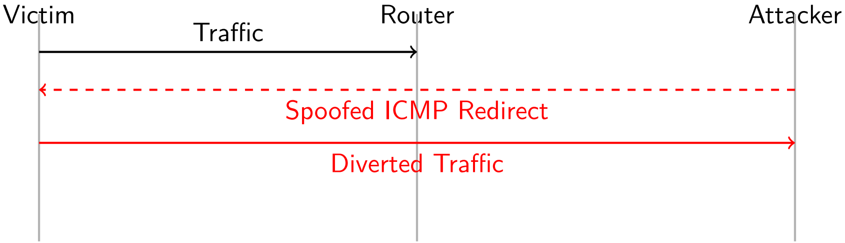
- Divert traffic through attacker-controlled host
- Steal or modify data in transit
- Create covert exfiltration channels
- Launch MITM or DoS attacks

Redirect Attack Steps

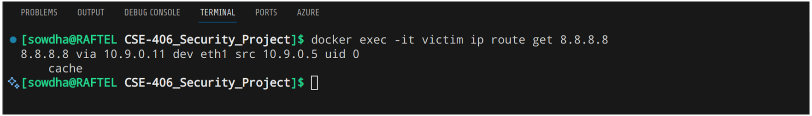
1. Victim sends packet to default gateway
2. Attacker observes and crafts ICMP Redirect (Type 5)
3. Sends spoofed Redirect pointing to attacker IP
4. Victim updates routing table and forwards to attacker



Timing Diagram

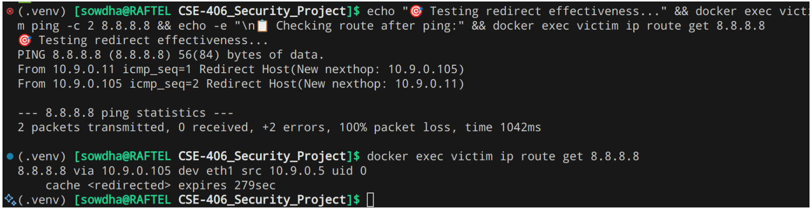


Attacker and Victim Terminals



```
● [sowdha@RAFTEL CSE-406_Security_Project]$ docker exec -it victim ip route get 8.8.8.8
  8.8.8.8 via 10.9.0.11 dev eth1 src 10.9.0.5 uid 0
      cache
  [sowdha@RAFTEL CSE-406_Security_Project]$ 
```

Attacker Terminal



```
⊗ (.venv) [sowdha@RAFTEL CSE-406_Security_Project]$ echo "🎯 Testing redirect effectiveness..." && docker exec victi
  m ping -c 2 8.8.8.8 && echo -e "\n📋 Checking route after ping:" && docker exec victim ip route get 8.8.8.8
  🎯 Testing redirect effectiveness...
  PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
  From 10.9.0.11 icmp_seq=1 Redirect Host(New nexthop: 10.9.0.105)
  From 10.9.0.105 icmp_seq=2 Redirect Host(New nexthop: 10.9.0.11)

  --- 8.8.8.8 ping statistics ---
  2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1042ms

● (.venv) [sowdha@RAFTEL CSE-406_Security_Project]$ docker exec victim ip route get 8.8.8.8
  8.8.8.8 via 10.9.0.105 dev eth1 src 10.9.0.5 uid 0
      cache <redirected> expires 279sec
  (.venv) [sowdha@RAFTEL CSE-406_Security_Project]$ 
```

Victim Terminal

Detecting and Mitigating Redirects

- Disable redirect acceptance on hosts:

  ```
  sysctl -w net.ipv4.conf.all.accept_redirects=0
  ```

- Monitor unexpected routing table changes
- Use static or authenticated routing protocols
- Deploy IDS signatures for anomalous ICMP Redirects

Defense against ICMP Attacks

- Disable ICMP redirects on hosts:
  ```
  sysctl -w net.ipv4.conf.all.accept_redirects=0
  ```
- Enable rp_filter on all interfaces
- Rate-limit and inspect ICMP/ARP traffic
- Deploy IPsec for control-plane messages

Thank You!