Day 22

Exploitation Analyst

Hacking ICMP Protocol:

ICMP Tunneling (e.g., bypass firewall):

What is ICMP Tunneling?

ICMP tunneling is a covert method of transporting data using ICMP (Internet Control Message Protocol) packets—typically used for network diagnostics (like ping). Attackers exploit ICMP to bypass firewall restrictions or exfiltrate data, since many firewalls allow ICMP Echo/Reply by default. It encapsulates TCP traffic (e.g., SSH) inside ICMP packets, making it difficult to detect.

Countermeasures by attack types:

Attack Type	**Countermeasure**
Ping Flood (hping3 -1 --flood)	Use rate-limiting (e.g., iptables or firewalld) to restrict ICMP echo requests per IP
Smurf Attack	Block directed broadcast on routers (e.g., no ip directed-broadcast on Cisco)
ICMP Tunneling (covert channel)	Block or monitor ICMP outbound, especially to unknown IPs
ICMP Redirect Attack	Disable ICMP redirects on OS and router (net.ipv4.conf.all.accept_redirects = 0)
Host Discovery (ICMP ping scan)	Drop ICMP echo-request on external interfaces; use firewall rules
Covert Shell (icmpsh)	Deep Packet Inspection + Egress filtering + ICMP type/code inspection

--The End--