Phase 2: Scanning

- Detecting information useful for break-in
  - Live machines
  - Network topology
  - Firewall configuration
  - Applications and OS types
  - Vulnerabilities

Network Mapping

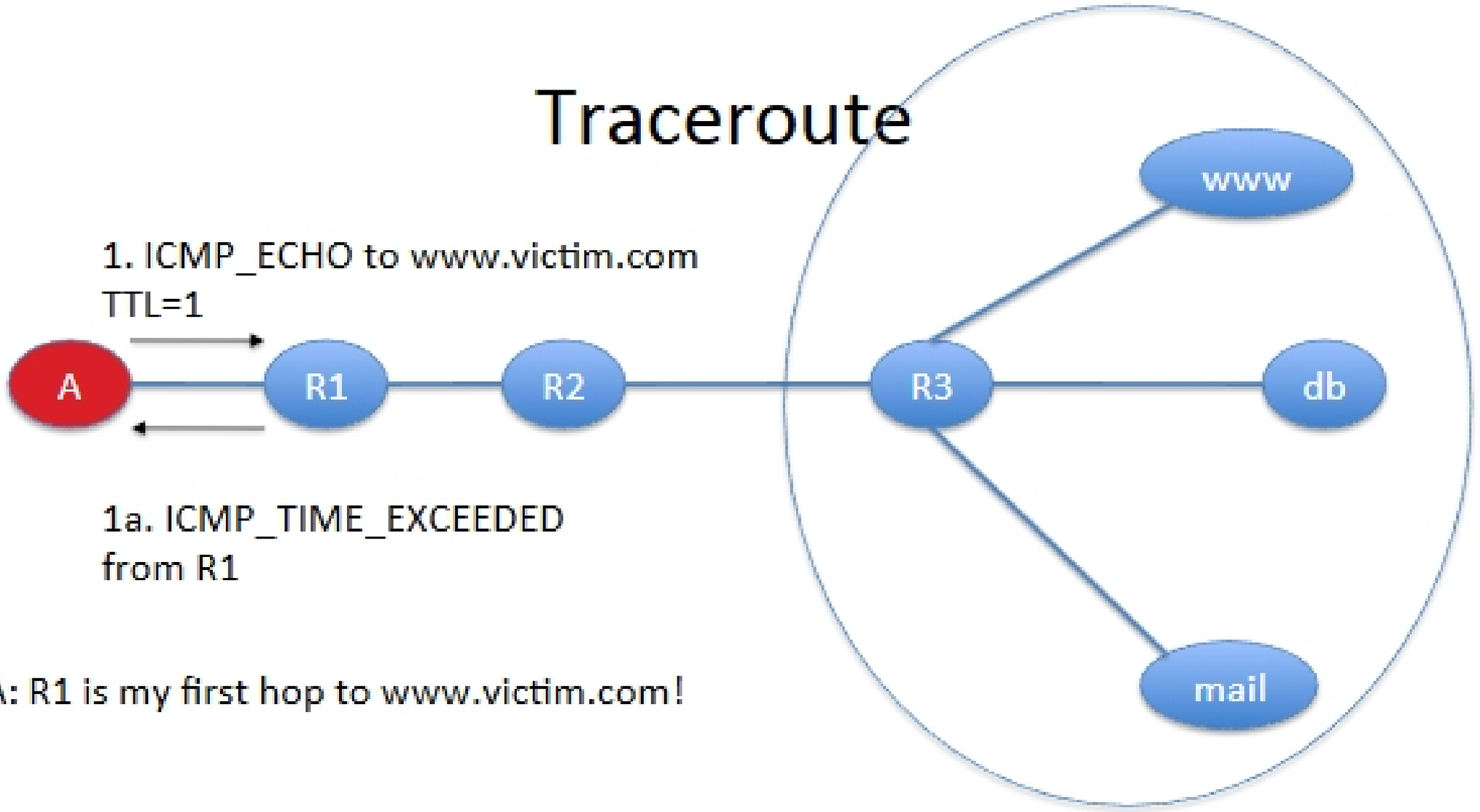
- Finding live hosts
  - Ping sweep
  - TCP SYN sweep
- Map network topology
  - Traceroute
    - Sends out ICMP or UDP packets with increasing TTL
    - Gets back ICMP_TIME_EXCEEDED message from intermediate routers

Traceroute

1. ICMP_ECHO to www.victim.com
TTL=1

1a. ICMP_TIME_EXCEEDED
from R1

A: R1 is my first hop to www.victim.com!



victim.com