

SCANNING PHASE

PHASE 1: NETWORK RECONNAISSANCE

Main objective: Discover a network topology

Some CLI commands may provide some useful information!

DNS

DNS: Domain Name Server maps IP addresses to hostnames and vice versa

- **DNS Interrogation:** Learn location of web, email, firewall servers
- **nslookup** <@ip or domain> command provides information concerning machines

DNS CONTROL(S)

To Guard Security:

Don't give away information!

- Exclude internal network information in external name servers
- Eliminate **HINFO** records from name servers
- Prevent or restrict zone transfers to authorized machines/users

Restrict access to internal DNS from outside

- Disable inbound connections to TCP port 53: TCP zone transfer, UDP name lookups
- UDP name lookups sent as TCP requests when > 512 bytes
- Log inbound connections to port 53 to track potential attacks

TRACEROUTE

traceroute: Provides list of routers between source and destination

To run:

```
[bash]$ traceroute www.univ-tlse3.fr
```

```
[DOS]: tracert www.univ-tlse3.fr
```

traceroute can be run from multiple locations to learn multiple entry points into network

How traceroute operates:

- Traceroute uses ICMP_TIME_EXCEEDED messages
- Windows: Uses ICMP echo request packet
- UNIX: uses UDP or ICMP with -I option

To Guard Security:

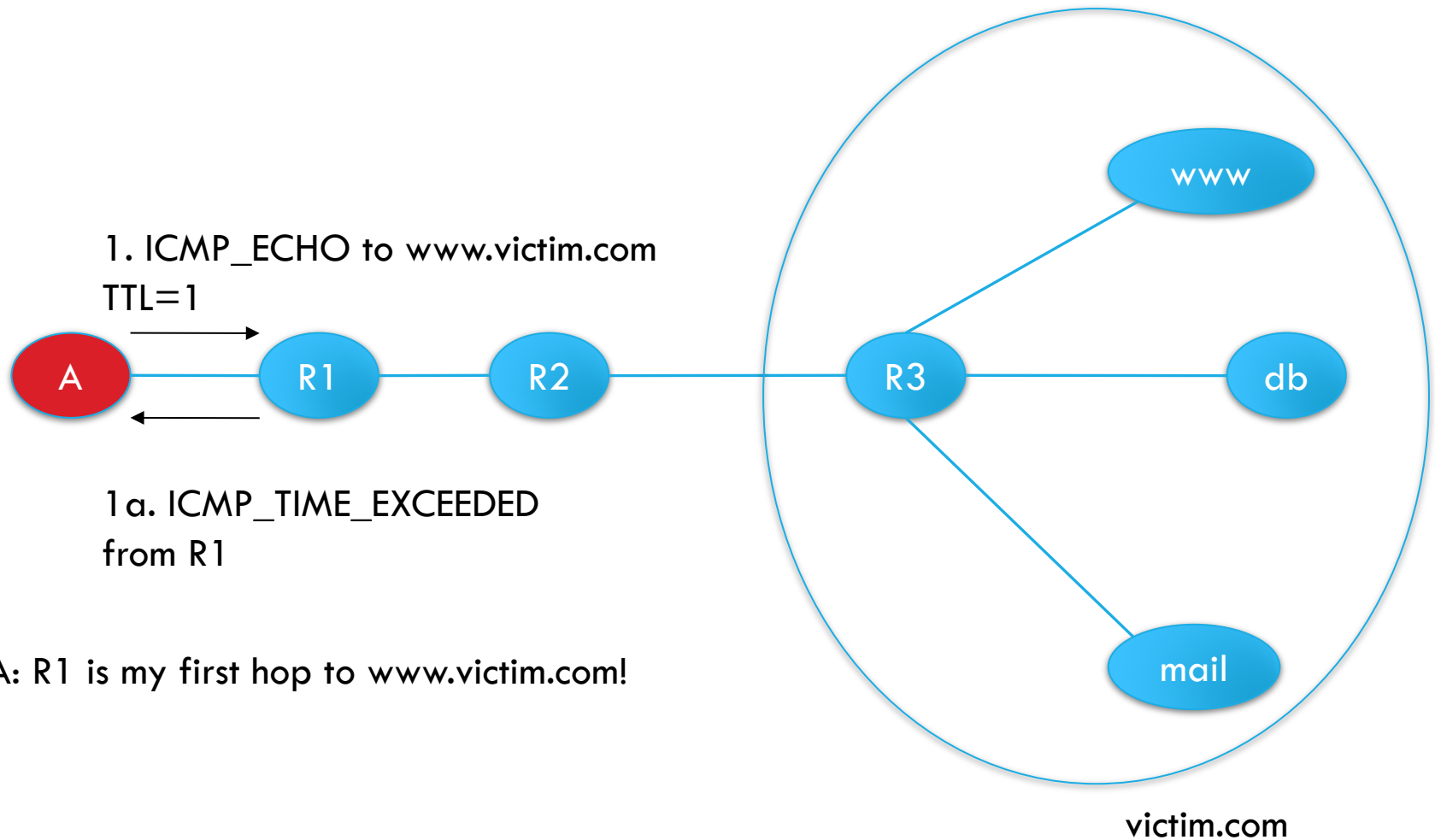
Do not permit pings from outside the network

- Block ICMP and UDP at network edge (firewall or router)
- **Note:** Blocking only ICMP or UDP may allow access, since both may be used

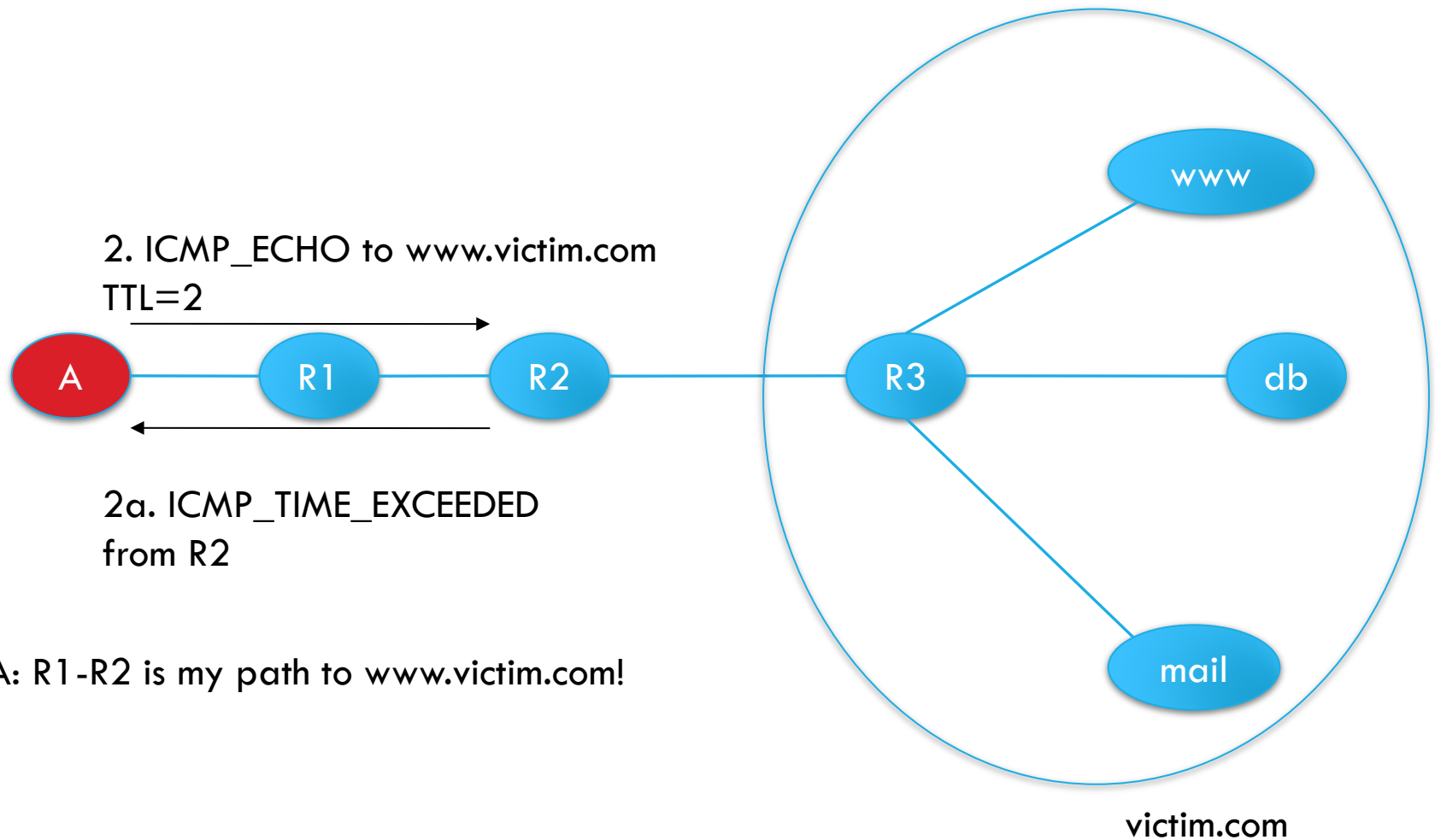
Detect attacks

- Use IDS systems to detect traceroute requests
- **www.snort.org**: a free IDS program that detects these

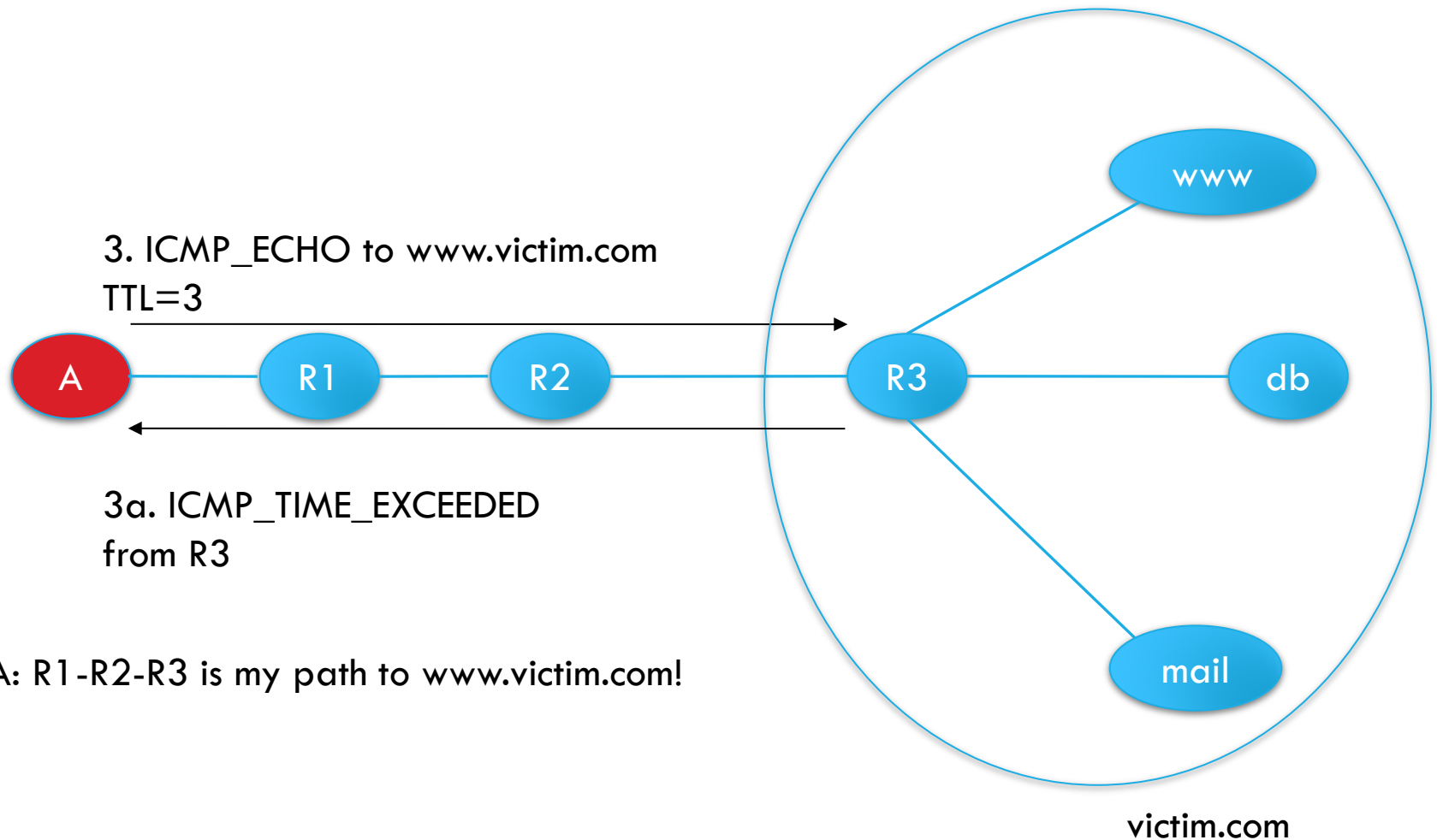
TRACEROUTE



TRACEROUTE

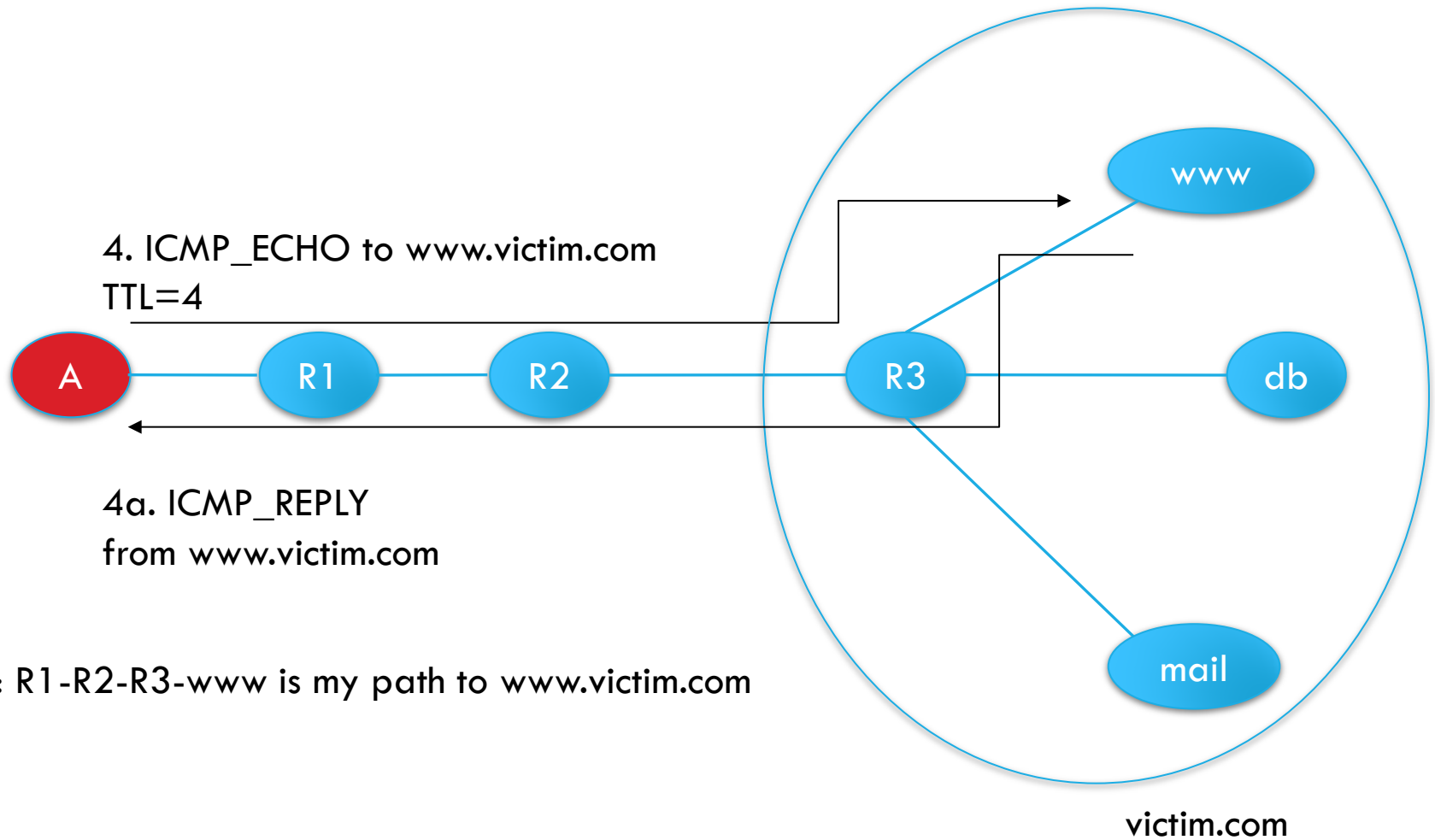


TRACEROUTE



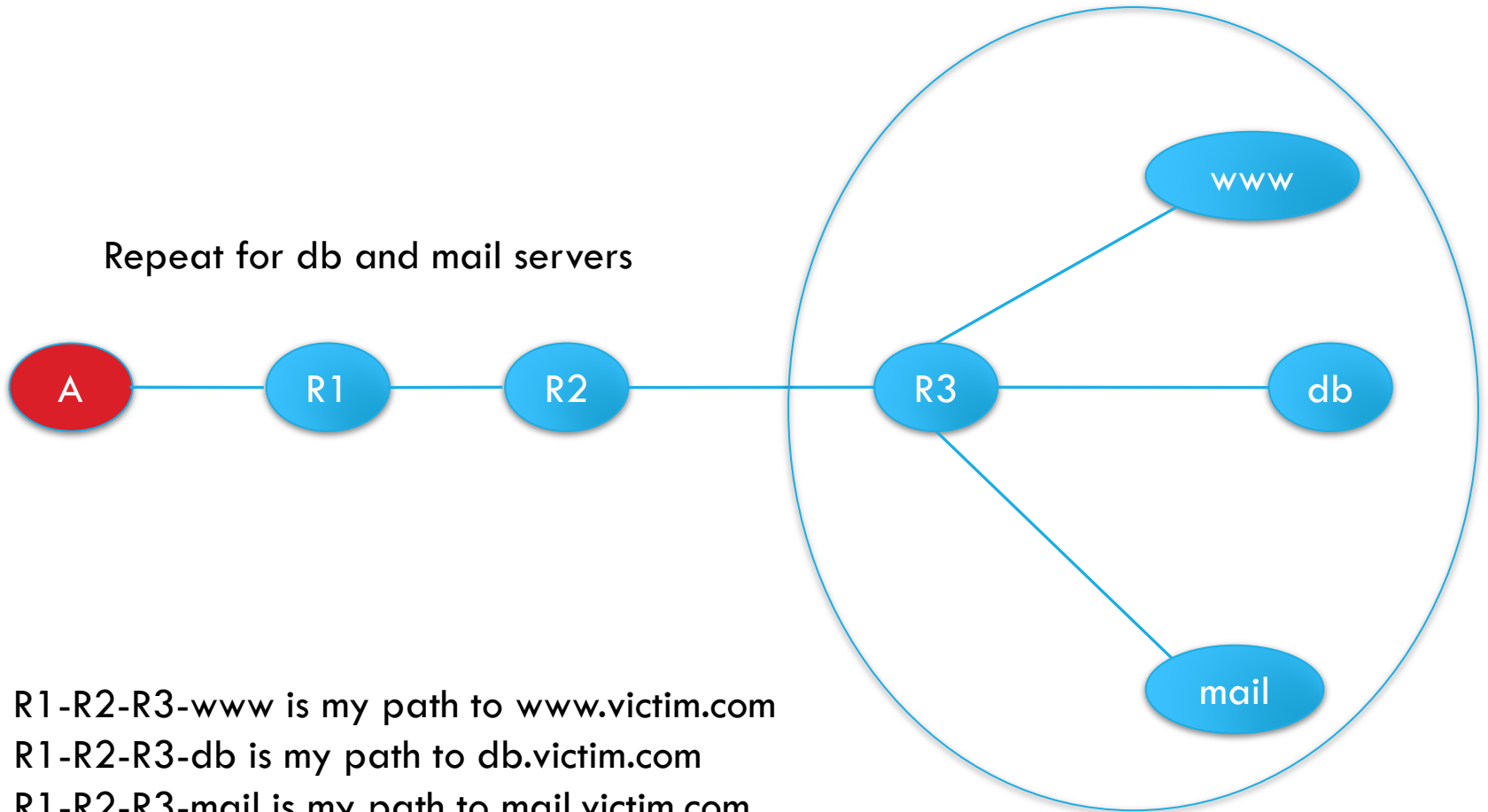
A: R1-R2-R3 is my path to www.victim.com!

TRACEROUTE



TRACEROUTE

Repeat for db and mail servers



A: R1-R2-R3-www is my path to www.victim.com

R1-R2-R3-db is my path to db.victim.com

R1-R2-R3-mail is my path to mail.victim.com

➔ Victim network is a star with R3 at the center

victim.com

RECONNAISSANCE: WHOIS

Whois provides information on:

Registrar: Sponsoring company

Organizational/Point of contact: Contact information

Whois databases include:

<https://www.afnic.fr/fr/produits-et-services/services/whois/>

<https://www.ripe.net>

Guard Security by:

Posting fictitious name in whois database

Keep contact information, contact registration in registry up-to-date

PHASE 2: SCANNING & ENUMERATION

Scanning

Host Scanning: Which IP addresses are valid?

Network Scanning: How is the network routing system organized?

Port Scanning: Which services are running on which ports?

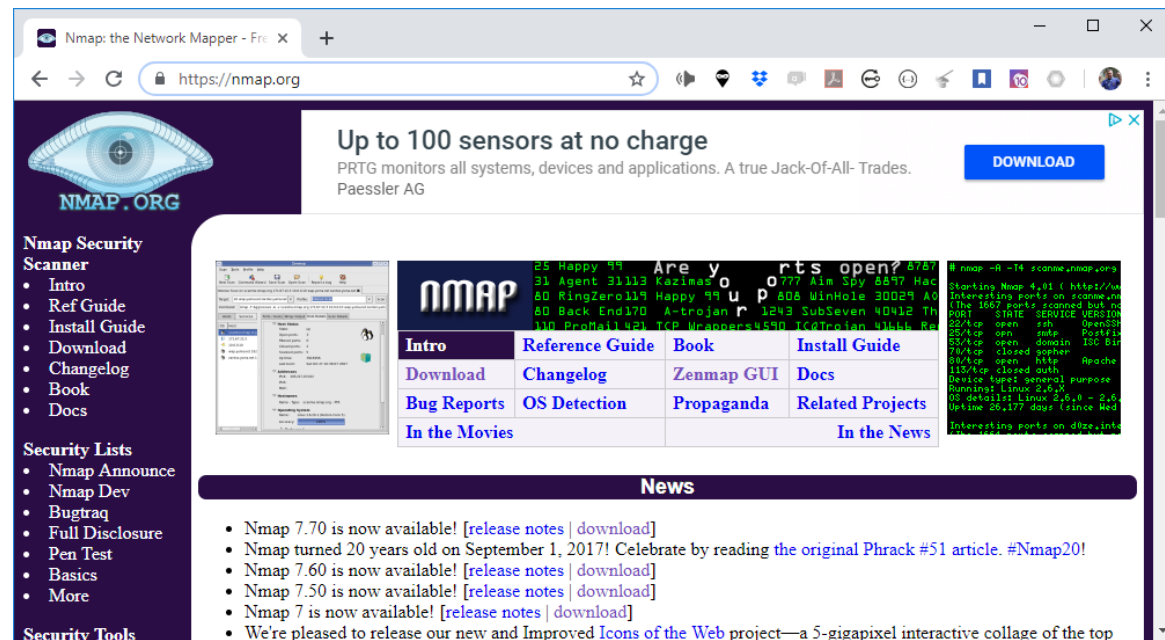
Enumeration

Fingerprinting: Which software versions are running on different sockets?

- *Active fingerprinting:* Send specific messages & observe replies
- *Passive fingerprinting:* Observe patterns in IP packets
- *Stealth scanning:* Slow scanning stays under intrusion detection radar screen

AN ANSWER ... NMAP (& ZENMAP)

Remember that ... **it's illegal to use this in France (except on your own network)**



The screenshot shows the Nmap.org website in a web browser. The browser's address bar displays "https://nmap.org". The website has a dark purple header with the Nmap logo (an eye) and the text "NMAP.ORG". Below the header, there is a section titled "Up to 100 sensors at no charge" with a "DOWNLOAD" button. The main content area features a grid of links for "Intro", "Reference Guide", "Book", "Install Guide", "Download", "Changelog", "Zenmap GUI", "Docs", "Bug Reports", "OS Detection", "Propaganda", and "Related Projects". There is also a "News" section with several announcements about Nmap versions 7.70, 7.60, 7.50, and 7.0. The left sidebar contains links for "Nmap Security Scanner" and "Security Lists".

Nmap: the Network Mapper - Fre x +

https://nmap.org

Up to 100 sensors at no charge
PRTG monitors all systems, devices and applications. A true Jack-Of-All- Trades.
Paessler AG

DOWNLOAD

NMAP.ORG

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

Intro Reference Guide Book Install Guide

Download Changelog Zenmap GUI Docs

Bug Reports OS Detection Propaganda Related Projects

In the Movies In the News

News

- Nmap 7.70 is now available! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.60 is now available! [release notes | download]
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top

<https://www.cyberciti.biz/security/nmap-command-examples-tutorials/>

HOST DISCOVERY

One of very first steps in network reconnaissance mission to reduce a (sometimes huge) set of IP ranges into a list of active or interesting hosts

- administrator uses an ICMP ping to locate hosts on internal network
- external penetration uses a diverse set of “probes” in an attempt to evade firewall restrictions
 - Aka “ping” scan, but goes beyond `ICMP echo request` packets

PORT SCANNING

Goal of port scanning: find out which ports are open, closed, or filtered

- e.g., find out if a remote host is providing a service that is vulnerable to buffer overflow attack
- port scanning may involve all 65,535 ports or only the ports that are well-known to provide services vulnerable to security-related exploits

PORT SCANNING

A port is **open** on a machine if there is a running (server) process on the machine and the port is assigned to this process

- if a port on a remote host is open for incoming connection requests and you send it a SYN packet, the remote host will respond back with a SYN+ACK packet

A port is **filtered** if packets passing through that port are subject to filtering rules of a firewall

- if a port is filtered with something like an iptables based packet filter and you send it a SYN packet or an ICMP ping packet, you may not get back anything at all

If a port on a remote host is **closed** and you send it a SYN packet, the remote host will respond back with a RST packet

NMAP

nmap is more than just a port scanner

- listing open ports on a network
- trying to construct an inventory of all services running in a network
- trying to detect as to which operating system is running on each machine

NMAP

nmap comes with a large number of options for carrying out different security scans of a network such as:

- -sT: carries out a TCP connect() scan
- -sU: sends a dataless UDP header to every port (state of the port is inferred from the ICMP response packet [if there is such a response at all])
- -sP: “ping scanning” to determine which machines are up in a network
- -sV: “version detection”

DEFENSE AGAINST PORT SCANNING

- Close all unused ports
- Remove all unnecessary services
- Filter out all unnecessary traffic
- Find openings before the attackers do
- Use smart filtering, based on client's IP

VULNERABILITY SCANNING

The attacker knows OS and applications installed on live hosts

- He can now find for each combination
 - Vulnerability exploits
 - Common configuration errors
 - Default configuration

Vulnerability scanning tool uses a database of known vulnerabilities to generate packets

Vulnerability scanning is also used for sysadmin

DEFENSE AGAINST VULNERABILITY SCANNING

- Close your ports and keep systems patched
- Find your vulnerabilities before the attackers do

ENUMERATION CONTROLS

To Guard Security:

Evaluate computer from the inside

- Enumeration tools help the administrator to determine available services and evaluate vulnerabilities

Evaluate computer from the outside

- Scan to find unnecessary services from outside FW
 - Can use **nmap** to scan your own machine or network

Disable all unnecessary services

- UNIX: comment out unnecessary services in /etc/init.d
- WINDOWS: Disable services via Control Panel/Services

AT THE END OF SCANNING PHASE

- Attacker has a list of “live” IP addresses
- Open ports and applications at live machines
- Some information about OS type and version of live machines
- Some information about application versions at open ports
- Information about network topology
- Information about firewall configuration