



**SCANNING PHASE**



# PHASE 1: NETWORK RECONNAISSANCE

**Main objective:** Learn network topology

# DNS

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

- **DNS Interrogation:** Learn location of web, email, firewall servers

# 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:

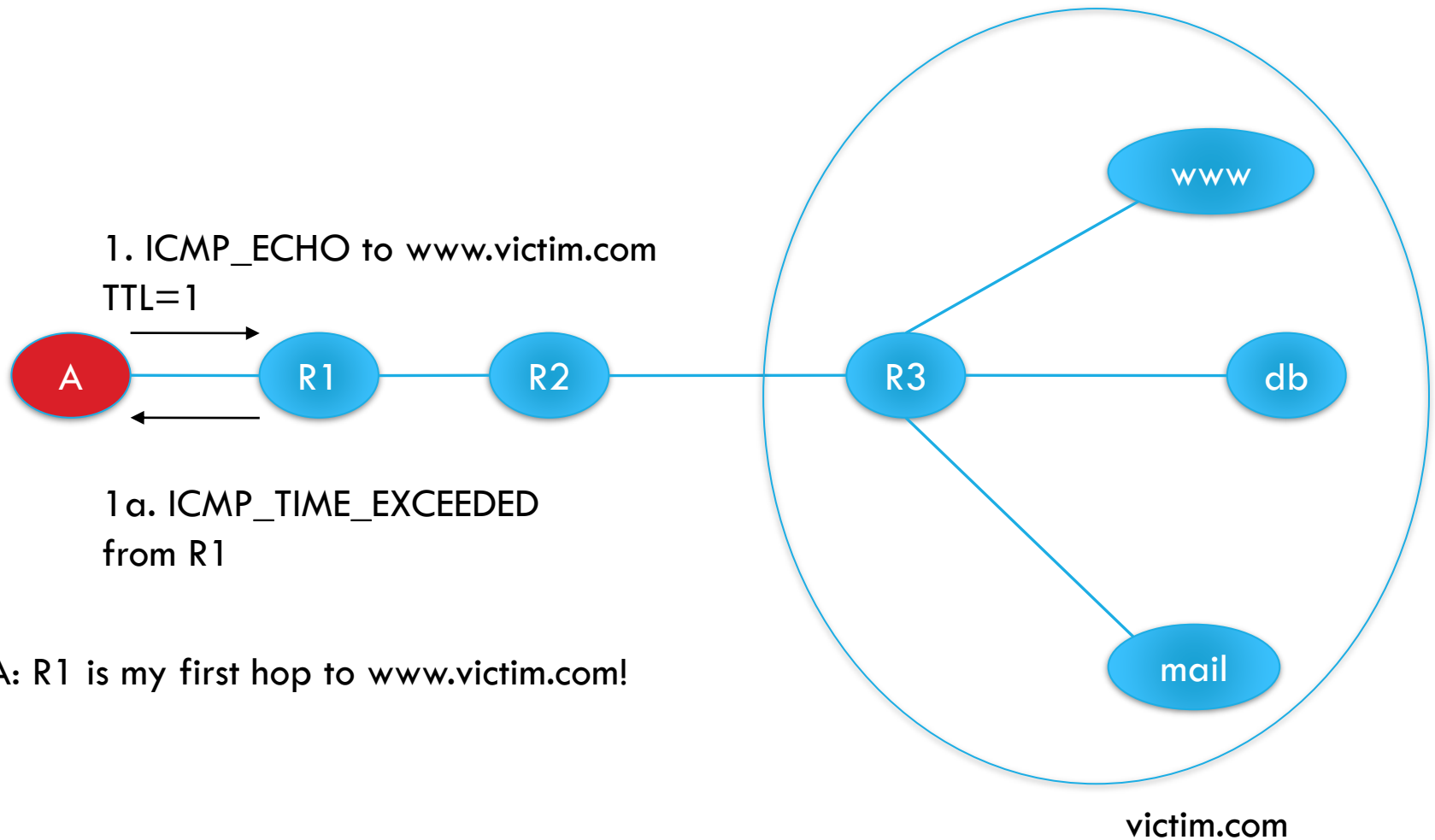
Do not permit pings from outside the network

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

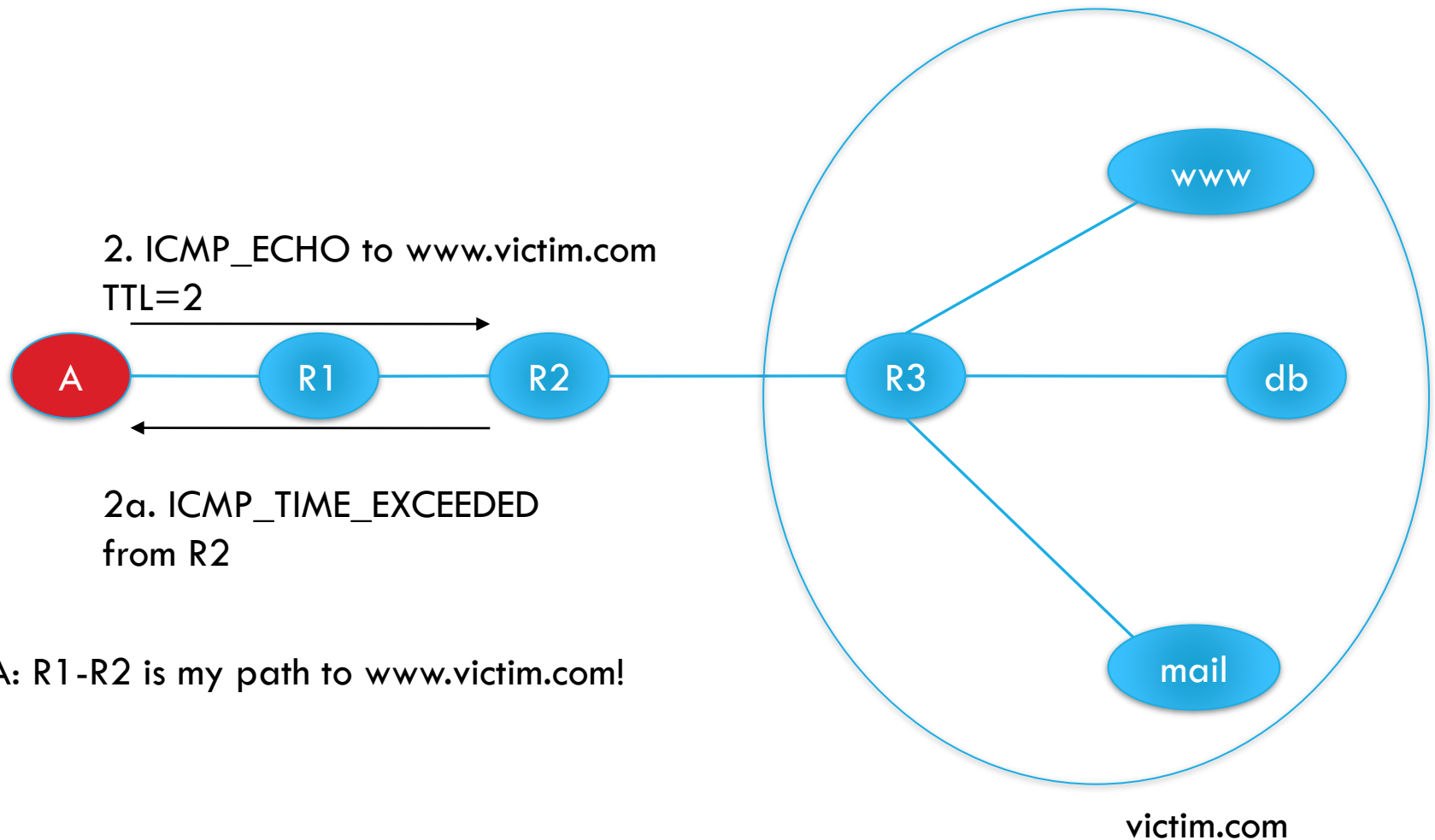
Detect attacks

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

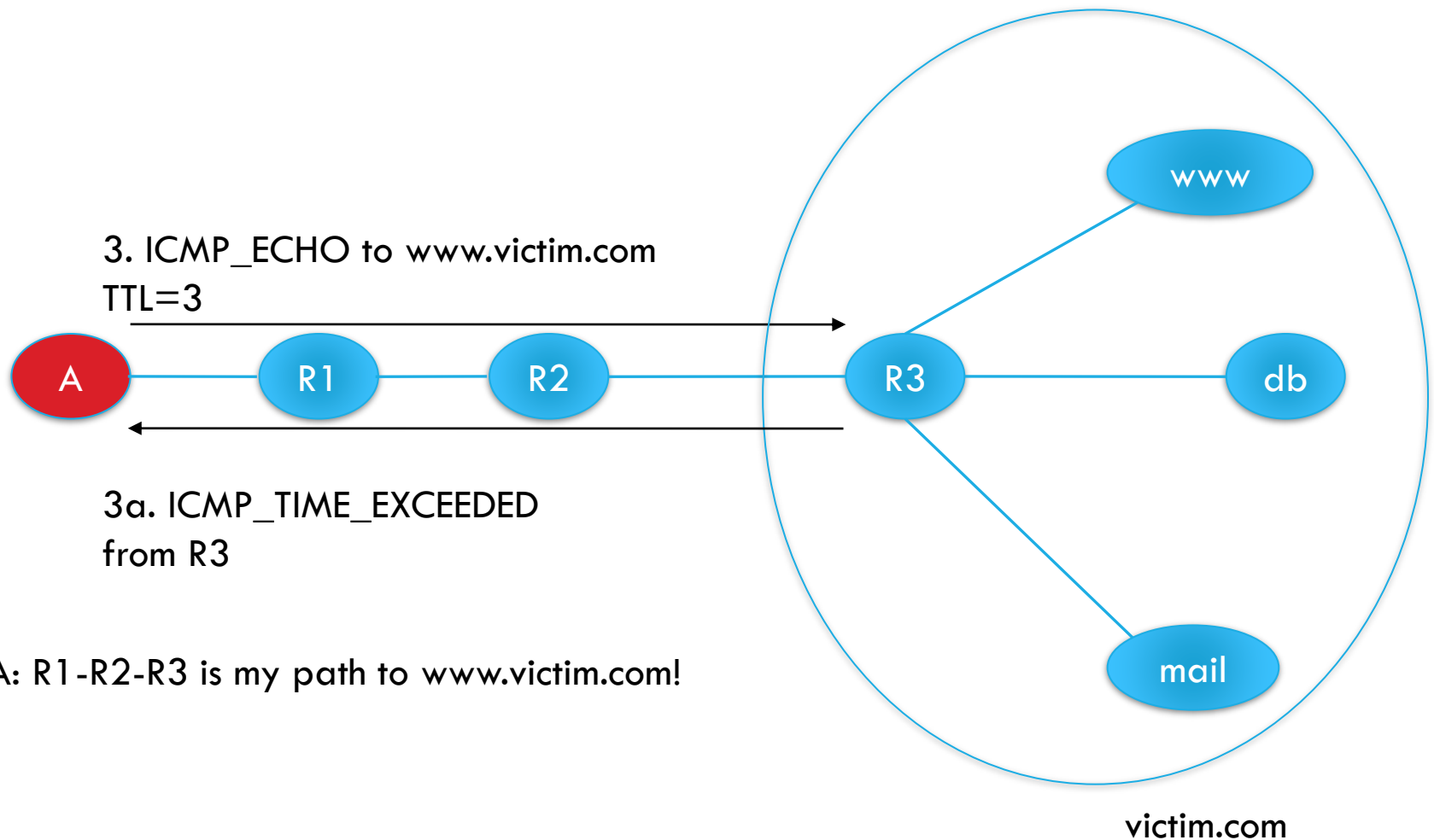
# TRACEROUTE



# TRACEROUTE

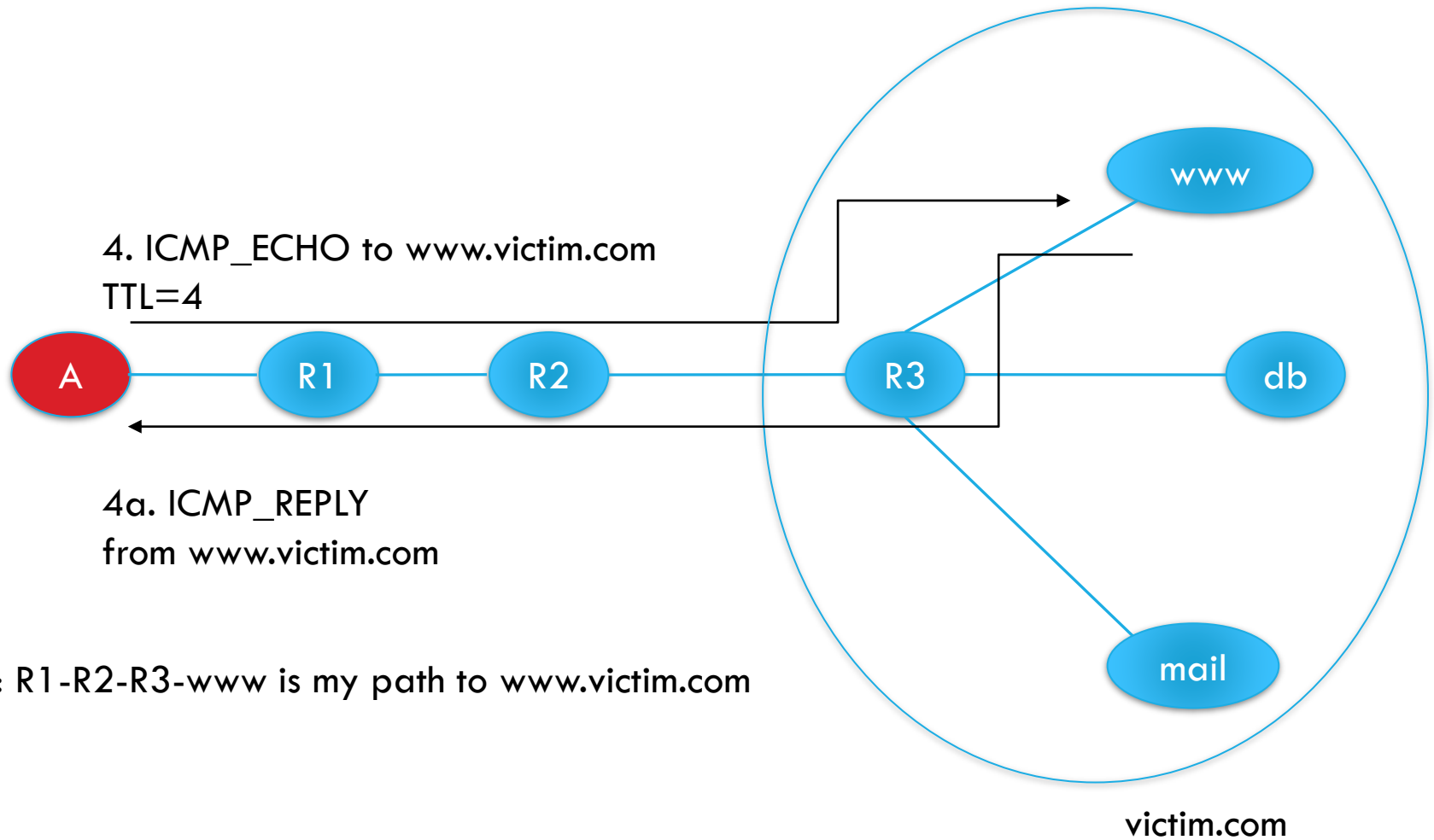


# TRACEROUTE



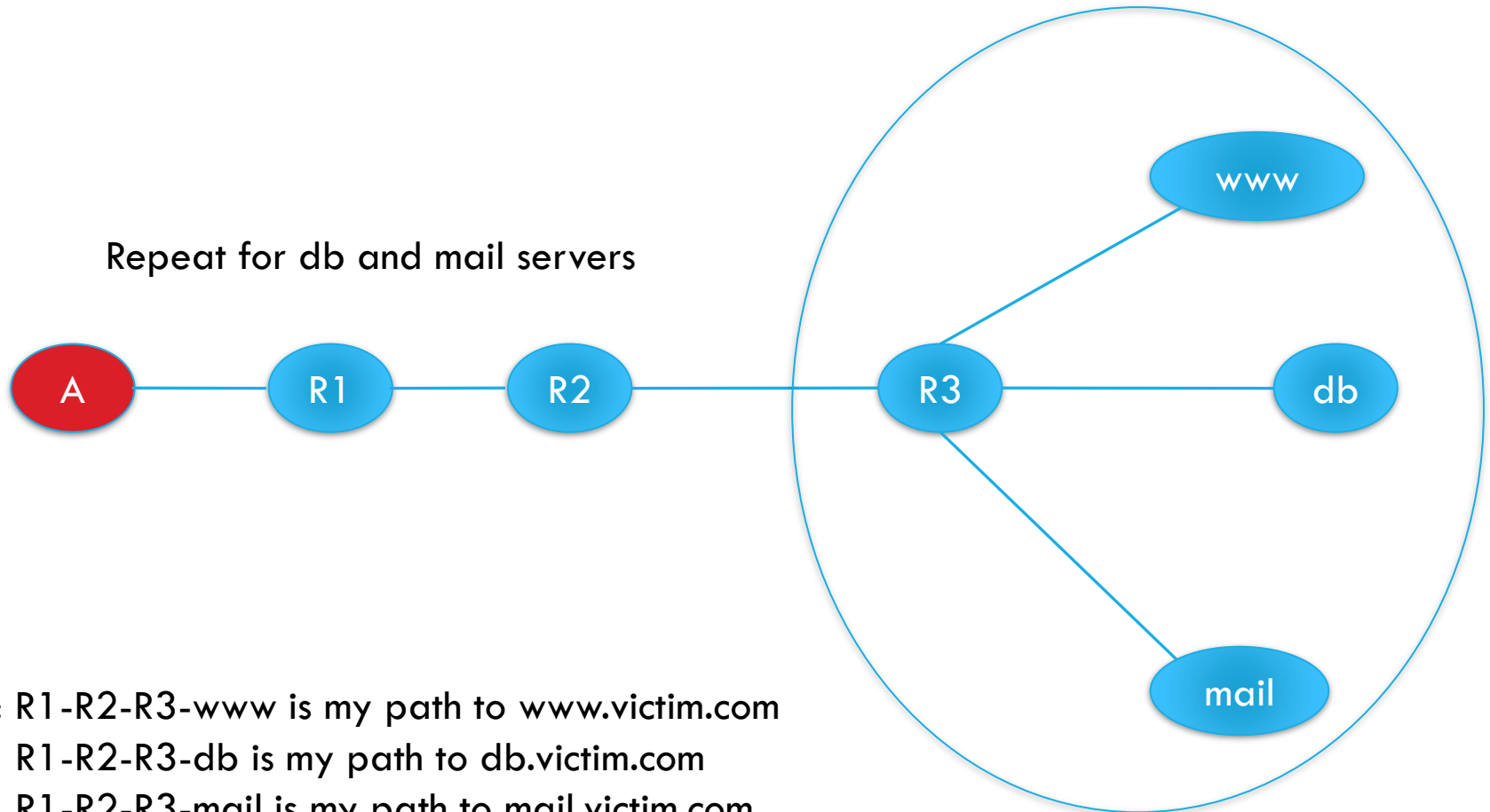


# TRACEROUTE



# 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/>**

**<http://whois.ripe.net>**

**Guard Security by:**

Posting fictitious name in whois database

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

# ASSIGNMENT

Find all information you can retrieve from **univ-toulouse.fr** domain  
(IP addresses, mail servers, DNS, .... Names, phone numbers, ...)

You can use any tool you want 😊

# 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

# PORT SCANNING

## Set source port and address

- To allow packets to pass through the firewall
- To hide your source address

## Use TCP fingerprinting to find out OS type

- TCP standard does not specify how to handle invalid packets
- Implementations differ a lot

# 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

# FIREWALK: DETERMINING FIREWALL RULES

Find out firewall rules for new connections

We don't care about target machine, just about packet types that can get through the firewall

- Find out distance to firewall using traceroute
- Ping arbitrary destination setting  $TTL = \text{distance} + 1$
- If you receive ICMP\_TIME\_EXCEEDED message, the ping went through



# DEFENSES AGAINST FIREWALKING

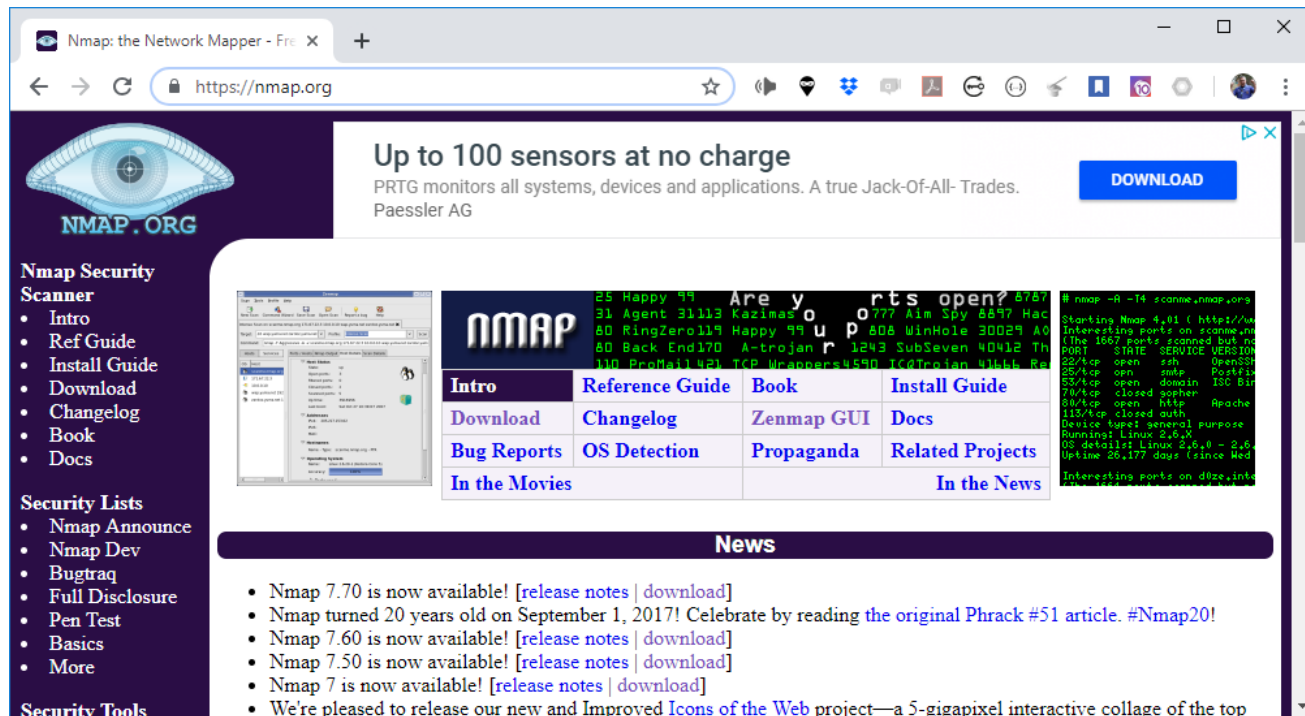
Filter out outgoing ICMP traffic

Use firewall proxies

- This defense works because a proxy recreates each packet including the TTL field
- The destination host would have to be set up to ignore messages that are not allowed

# 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". A banner at the top right says "Up to 100 sensors at no charge" with a "DOWNLOAD" button. The main content area features a grid of links: "Intro", "Reference Guide", "Book", "Install Guide", "Download", "Changelog", "Zenmap GUI", "Docs", "Bug Reports", "OS Detection", "Propaganda", "Related Projects", "In the Movies", and "In the News". On the left, there are sections for "Nmap Security Scanner" (with links to Intro, Ref Guide, Install Guide, Download, Changelog, Book, Docs) and "Security Lists" (with links to Nmap Announce, Nmap Dev, Bugtraq, Full Disclosure, Pen Test, Basics, More). At the bottom, a "News" section lists several updates, including Nmap 7.70, 7.60, 7.50, and 7, along with a link to "Icons of the Web".

Nmap: the Network Mapper - Free & Open Source

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 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**

**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/>

# SCAN TYPES

TCP connect scan: Performs 3-way handshake

TCP SYN: SYN → ← SYN/ACK

TCP FIN: FIN → ← RST (UNIX)

TCP XmasTree scan: FIN/URG/PUSH → ← RST

TCP Null: no flags → ← RST

TCP ACK: ACK → Is firewall stateful?

TCP Windows: Identify system via window size reporting

TCP RCP: Identify RCP ports, program names and version numbers

UDP Scan: If inactive ← ICMP port unreachable

# SCANNER - CONTROLS

## To Guard Security:

### Detect attack

- Detect ping sweeps and incoming ICMP traffic for port scans via IDS/IPS
- Identify attacker and possible time of attack

### Prevent attacks

- Filter all incoming sessions from ports except those that are expressly permitted
- Filter traffic from attack source IP addresses
- Filter all ICMP traffic or
  - Filter ICMP TIMESTAMP and ADDRESS MASK packet requests
- Minimal: Allow ECHO\_REPLY, HOST\_UNREACHABLE, TIME\_EXCEEDED into demilitarized zone (DMZ)

# ENUMERATION → FINGERPRINTING: IDENTIFYING THE SYSTEM SOFTWARE

**Active Stack Fingerprinting:** Send messages to determine versions of system software

Stack Fingerprinting: Identify host OS.

**Banner Grabbing:** Identify applications (including version if possible)

Identify host OS version: FIN probe, Bogus Flag probe, Initial Sequence Number sampling, Don't fragment bit monitoring, TCP initial window size, ACK value, ICMP message reactions, etc.

**Passive Stack Fingerprinting:** Monitors network traffic to determine OS type/version

TTL: What is initial Time To Live value?

Window Size: What is the default window size?

DF: Is the Don't Fragment flag set?

# 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 TOOLS

Port scanners and Enumeration Tools include:

**Nmap or other network Mapper:** TCP/UDP, decoy or bogus scans supported to complicate IDS detection

Scanners & Probes

**Unix scanners:** Samba: Smbclient,

**Wireless tools:** NetStumbler, AiroPeek,

**Netcat or nc:** TCP & UDP port scanning, verbose options

**NetScan:** whois, ping sweeps, NetBIOS name table scans, SNMP walks, etc.



# 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

# ASSIGNMENT

- Create a local network
- Plug some computers (yours and RPi for instance)
- Scan your network and try to find vulnerabilities!

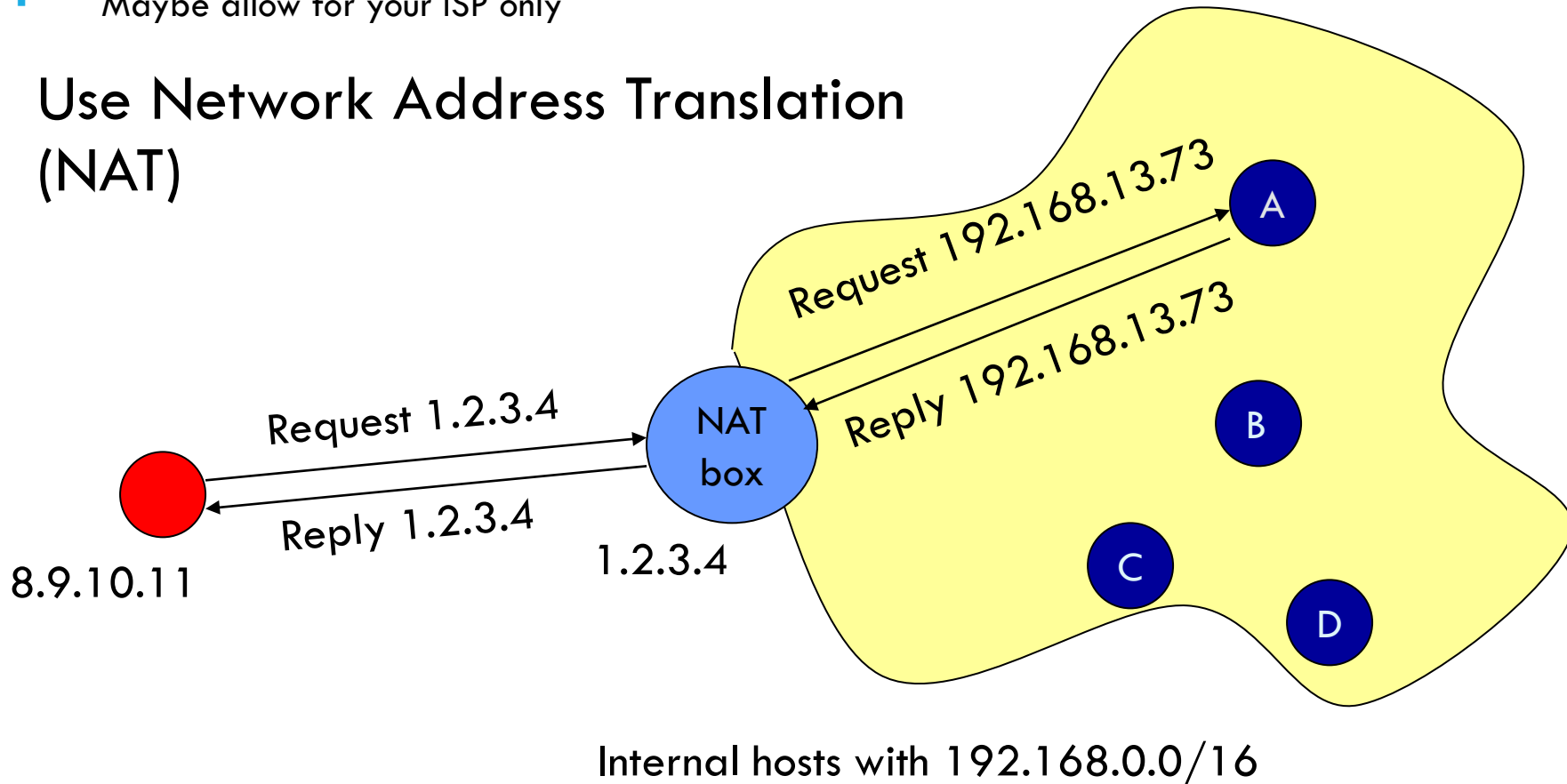


# DEFENSE AGAINST NETWORK MAPPING AND SCANNING

Filter out outgoing ICMP traffic

- Maybe allow for your ISP only

Use Network Address Translation (NAT)



# HOW NAT WORKS

For internal hosts to go out

- B sends traffic to [www.google.com](http://www.google.com)
- NAT modifies the IP header of this traffic
  - Source IP: B → NAT
  - Source port: B's chosen port Y → random port X
- NAT remembers that whatever comes for it on port X should go to B on port Y
- Google replies, NAT modifies the IP header
  - Destination IP: NAT → B
  - Destination port: X → Y

# HOW NAT WORKS

For public services offered by internal hosts

- You advertise your web server A at NAT's address (1.2.3.4 and port 80)
- NAT remembers that whatever comes for it on port 80 should go to A on port 80
- External clients send traffic to 1.2.3.4:80
- NAT modifies the IP header of this traffic
  - Destination IP: NAT → A
  - Destination port: NAT's port 80 → A's service port 80
- A replies, NAT modifies the IP header
  - Source IP: A → NAT
  - Source port: 80 → 80

# HOW NAT WORKS

What if you have another Web server C

- You advertise your web server A at NAT's address (1.2.3.4 and port 55) – not a standard Web server port so clients must know to talk to a diff. port
- NAT remembers that whatever comes for it on port 55 should go to C on port 80
- External clients send traffic to 1.2.3.4:55
- NAT modifies the IP header of this traffic
  - Destination IP: NAT → C
  - Destination port: NAT's port 55 → C's service port 80
- C replies, NAT modifies the IP header
  - Source IP: C → NAT, source port: 80 → 55