Practical Network Defense

Master's degree in Cybersecurity 2020-21

Link-local attacks: ICMP redirect lab

Angelo Spognardi

spognardi@di.uniroma1.it

Dipartimento di Informatica

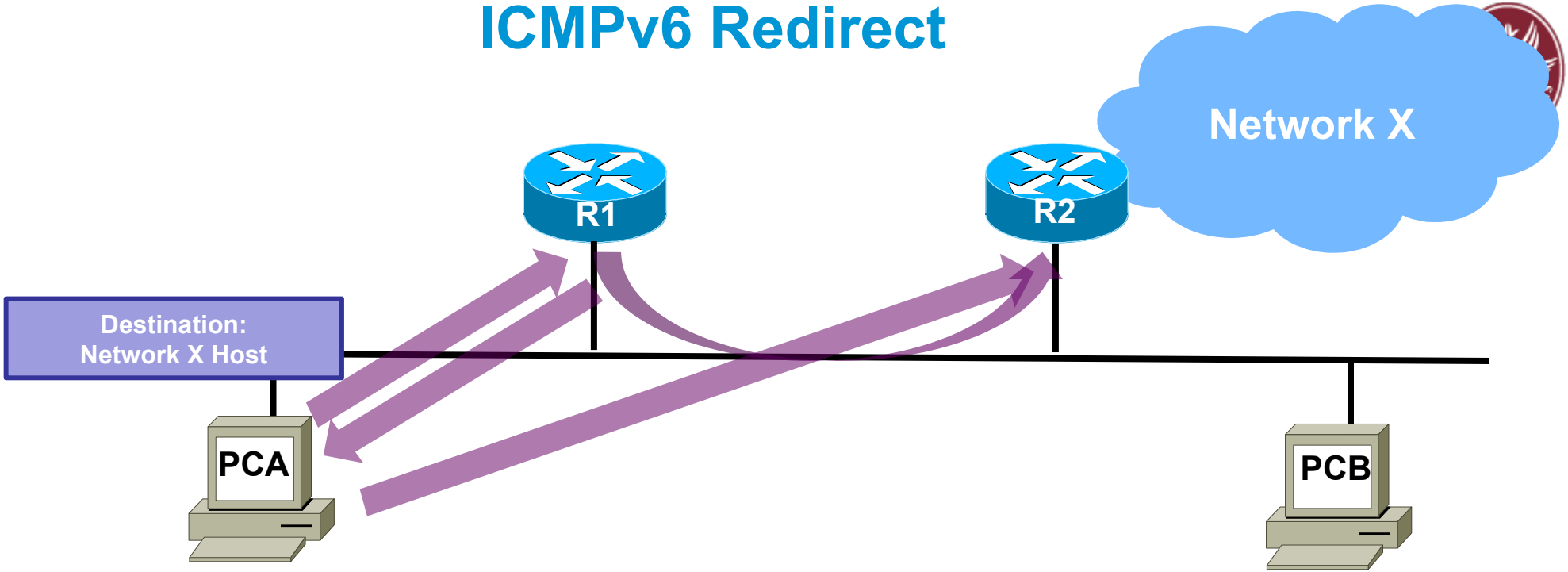
Sapienza Università di Roma

Lab activity

Main tasks

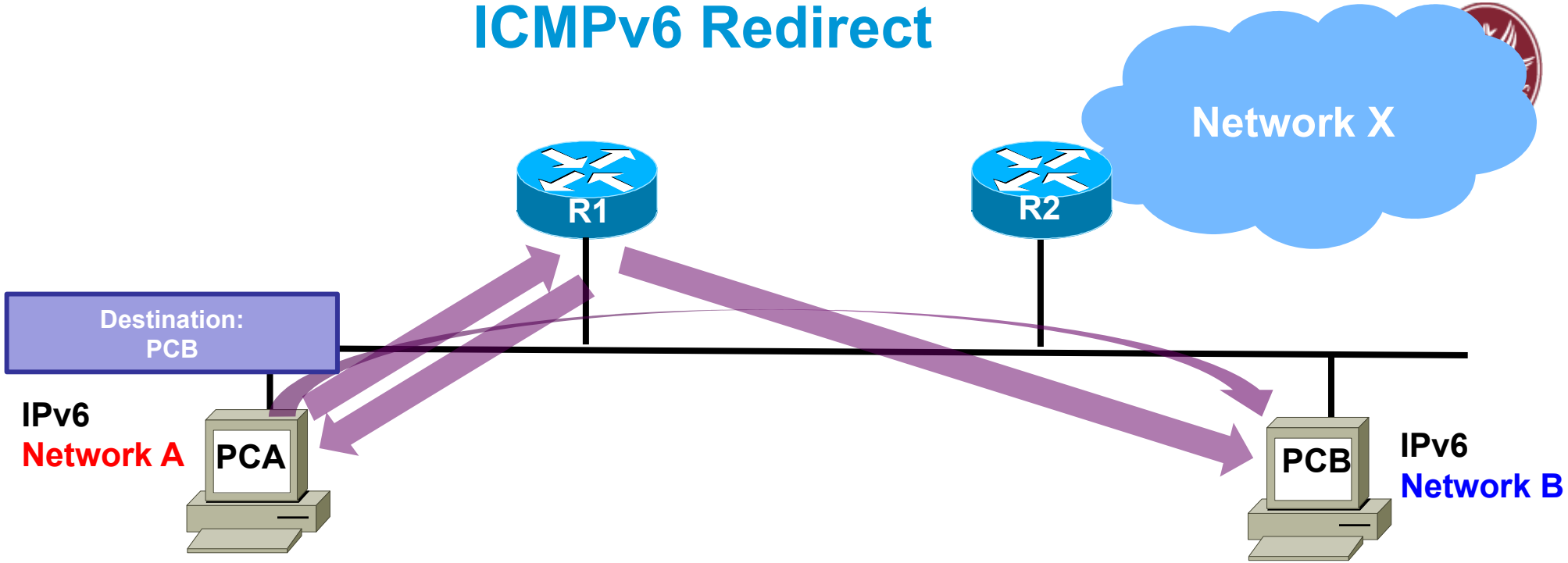
- Network eavesdropping
- ICMP redirect attack
  - MITM
- Reference links:
  - https://developers.redhat.com/blog/2018/10/22/introduction-to-linux-interfaces-for-virtual-networking/
  - https://www.fir3net.com/Networking/Terms-and-Concepts/virtual-networking-devices-tun-tap-and-veth-pairs-explained.html
  - https://www.ettercap-project.org/
  - https://pentestmag.com/ettercap-tutorial-for-windows/

ICMPv6 Redirect



- Similar functionality as ICMPv4.
- Like IPv4, a router informs an originating host of the IP address of a router that is on the local link and is closer to the destination.

ICMPv6 Redirect



- Similar functionality as ICMPv4.
- Like IPv4, a router informs an originating host of the IP address of a router that is on the local link and is closer to the destination.
- Unlike IPv4, a router informs an originating host that the destination host (on a different prefix/network) is on the same link as itself.

To do the activities

- We will use Kathará (formerly known as netkit)
  - A container-based framework for experimenting computer networking: http://www.kathara.org/
- A virtual machine is made ready for you
  - https://drive.google.com/file/d/1W6JQzWVyH5_LKLD20R6XH1ugPDP5LWP5/view?usp=sharing
- For not-Cybersecurity students, please have a look at the Network Infrastructure Lab material
  - http://stud.netgroup.uniroma2.it/~marcos/network_infrastructures/current/cyber/
    - Instructions are for netkit, we will use kathara

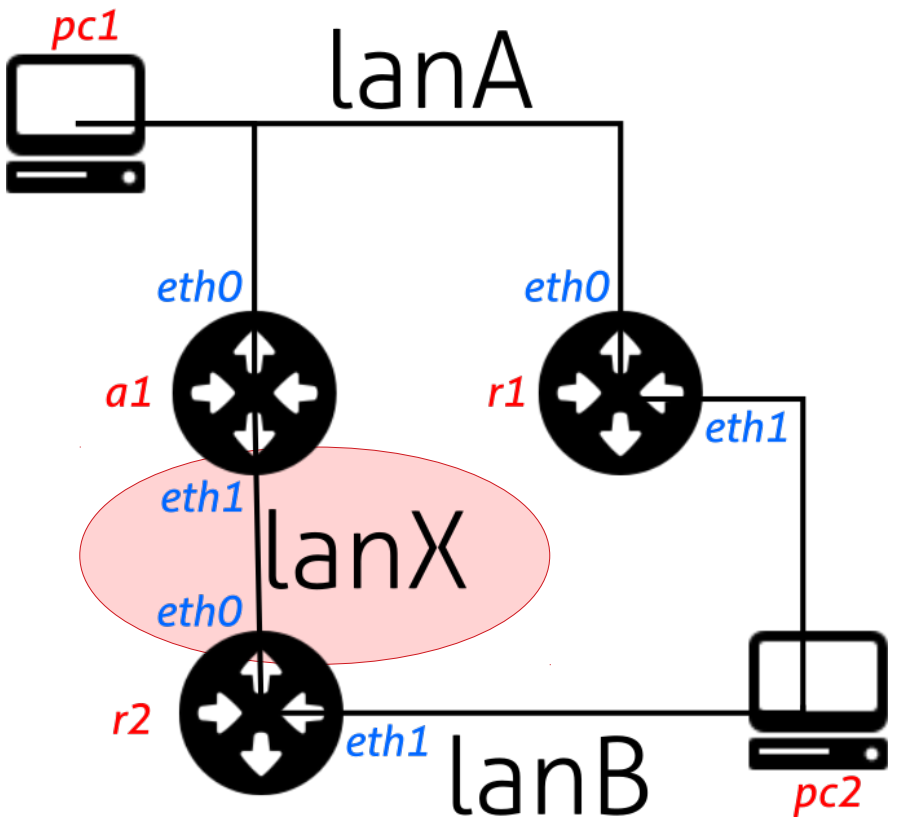
The kathara VM

- It should work in both Virtualbox and VMware
- It should work in Linux, Windows and MacOS
- There are some alias (shortcuts) prepared for you
  - Check with **`alias`**
- All the exercises can be found in the git repository:
  - https://github.com/vitome/pnd-labs.git
- You can move in the directory and run lstart
  - **NOTE**: launch docker first or the first lstart attempt can (...will...) fail

Lab activity: ex4

Exercise 1: pnd-labs/lab3/ex4

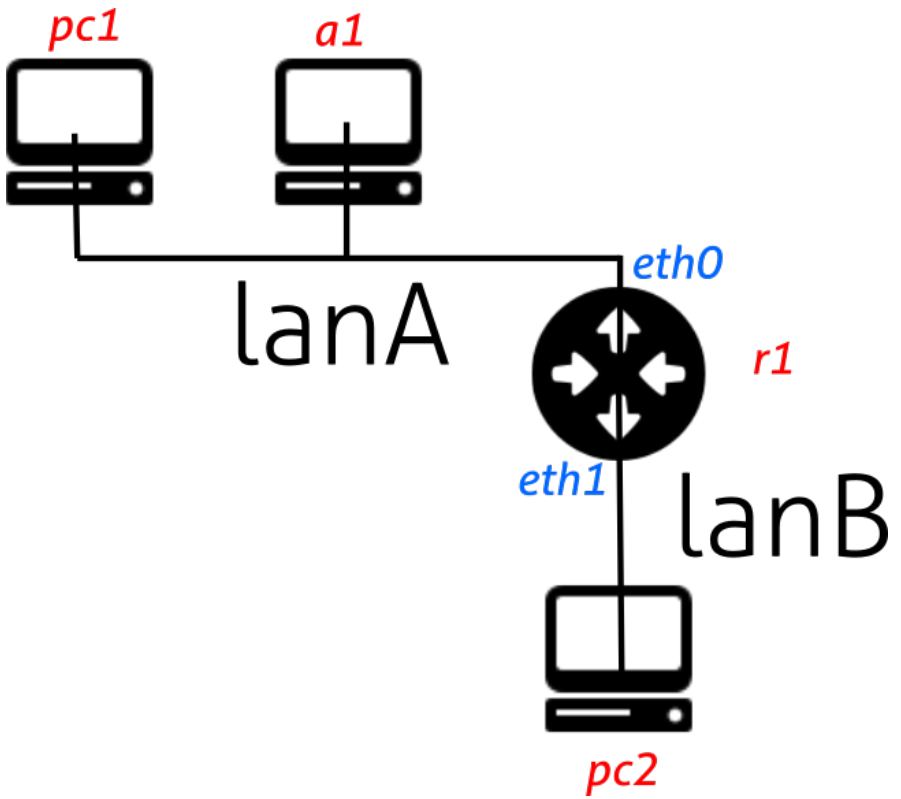
- PC1 reaches PC2 via r1
- The assignment is to use ICMP redirect to hijack the traffic from pc1 and capture the traffic in **lanX**
- Observe the type of packet exchange of a1
- The tool to be used is **`redir6`**



Lab activity: ex5

Exercise 2: pnd-labs/lab3/ex5

- PC1 reaches PC2 via r1
- The assignment is to use ICMP redirect to convince pc1 that a1 is a best hop for pc2
- Observe the type of packet exchange of a1 using wireshark
- The tool to be used is **`redir6`**



Lesson learned: reject redirects!

- If you check the default parameters:
  - /proc/sys/net/ipv4/conf/all/accept_redirects
    - TRUE (host)
    - FALSE (router)
  - /proc/sys/net/ipv4/conf/all/secure_redirects
    - TRUE
  - /proc/sys/net/ipv4/conf/all/shared_media
    - TRUE
  - /proc/sys/net/ipv6/conf/all/accept_redirects
    - Functional default: enabled if local forwarding is disabled
    - disabled if local forwarding is enabled.
- Then: accept_redirects and alike → FALSE
- Try the patch on the labs and see the effects

That's all for today

- **Questions?**
- References:
- IPv6 security references: https://www.ripe.net/support/training/material/ipv6-security/ipv6security-references.pdf
  - http://www.tcpipguide.com/free/t_InternetProtocolVersion6IPv6IPNextGenerationIPng.htm
  - https://www.6diss.org/e-learning/
  - http://www.cabrillo.edu/~rgraziani/ipv6-presentations.html
  - Book chapter 11 (even if quite obsoleted)