SAPIENZA
UNIVERSITÀ DI ROMA

Practical Network Defense

Master's degree in Cybersecurity 2020-21

Link-local attacks: lab

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

Lab activity

Main tasks

- Network eavesdropping
- ARP poisoning
  - 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/

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: ex1

Exercise 1: pnd-labs/lab3/ex1

- A lan with a host, a server and a router
- Join the network and eavesdrop the traffic in kathara
- The assignment is to create a virtual interface in the hosting machine and join the internal network A
- This can be done in several ways (using the bridge interface or creating a virtual interface to be joined to the actual bridge)
- Once done sniff the traffic
  - Create some traffic between the host and the server. Can you see the traffic from the hosting machine (the lubuntu box)?

Some hints about virtual interfaces

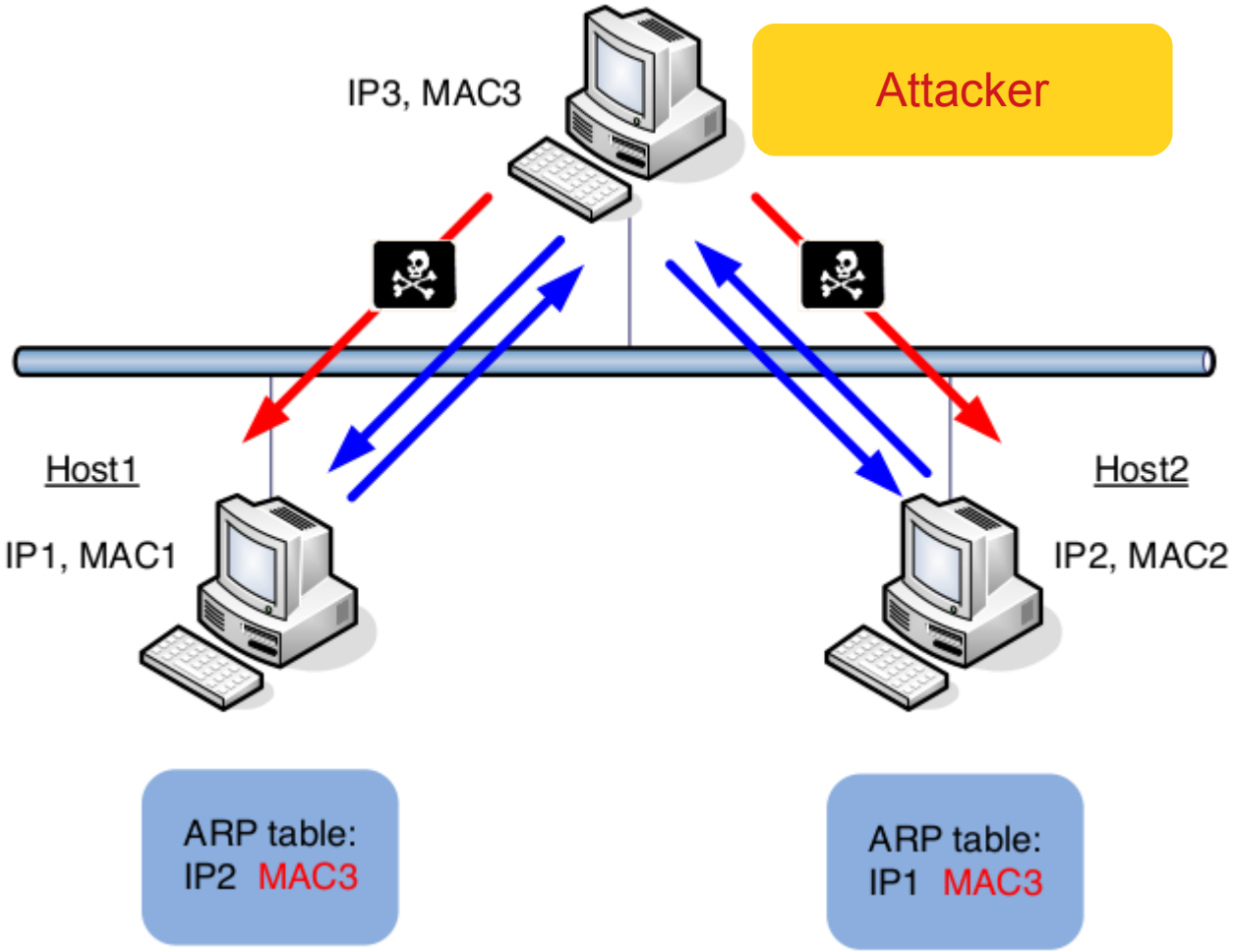
- add (or del) a virtual interface (pair veth0@veth1):
  - `ip link add dev veth0 type veth peer name veth1`
- connect one veth end to the virtual bridge:
  - `ip link set master br0 dev veth1`
- assign an IP address to the other end (not enslaved):
  - `ip addr add x.x.x.x/y dev veth0`
- enable both the ends of the virtual interface
  - `ip link set veth0 up`
  - `ip link set veth1 up`

Lab activity: ex2

Exercise 2: pnd-labs/lab3/ex2

- A lan with a host, a server, a router and the attacker machine.
- In the attacker machine you have to install bettercap and perform a MITM attack. Bettercap does this with the ARP poisoning
  - https://www.cyberpunk.rs/bettercap-usage-examples-overview-custom-setup-caplets
- Set up the links as for ex1, so that the victim machine can be the hosting box (assign it 192.168.100.200)
- Verify the arp poisoning is effective
- Try to use the proxy script included in the folder to alter the image in the server s1
  - kittens → jollypwn

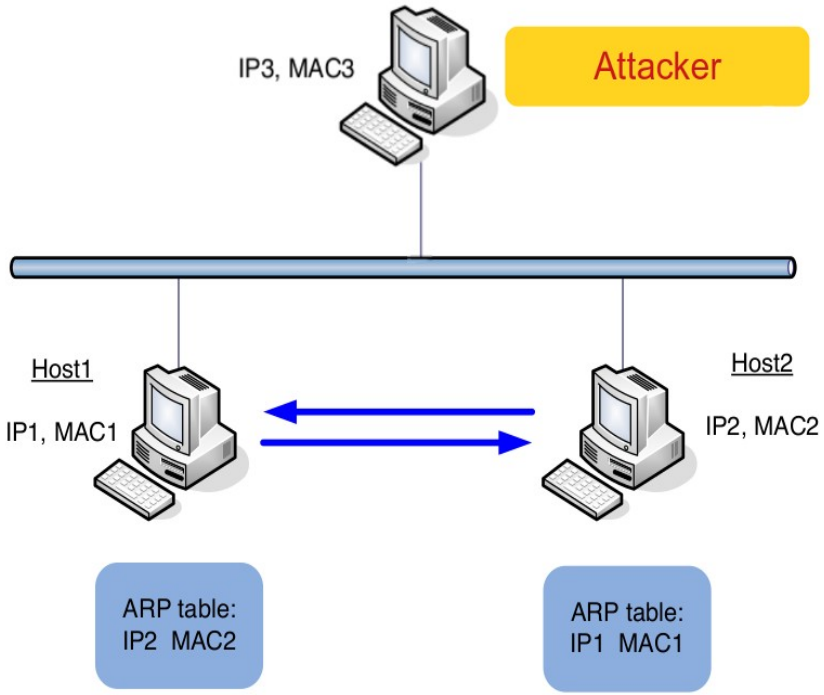
Man-in-the-middle with ARP spoofing



Lab activity: ex3

Exercise 3: pnd-labs/lab3/ex3

- A lan with a host, a server and a router
- Compile the thc toolkit and play with the tools
- If you join the network from the hosting box, you can also monitor the traffic with wireshark



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)