Practical Network Defense
Master's degree in Cybersecurity 2024-25

IPv6 addressing lab

Angelo Spognardi

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

Lab activity

Main tasks

- Properly configure the topology provided in the lab packages

- Manual configuration
  - Via ip and via interfaces file

- Automatic configuration
  - Via SLAAC
  - Via SLAAC + stateless DHCP

Reference links

- Linux ipv6 configuration: ipv6 sysctl

    – https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt

- Routing Advertisement deaemon: radvd

    – https://manpages.debian.org/testing/radvd/radvd.conf.5.en.html

    – https://www.linuxtopia.org/online_books/network_administration_guides/Linux+IPv6-HOWTO/hints-daemons-radvd.html

- dibbler DHCPv6 server/client

    – https://github.com/tomaszmrugalski/dibbler/raw/master/doc/dibbler-user.pdf

- dnsmasq network Swiss-knife:

    – https://thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html#index

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/12w2wwdFo7jmokVxDWlUdpVWDgf4g8sRe/view

- For not-Cybersecurity students, please have a look at the Kathará official manuals

  - https://github.com/KatharaFramework/Kathara-Labs/tree/main/tutorials

The kathara VM

- It <u>should</u> work in both Virtualbox and VMware

- It <u>should</u> 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**: the first lstart attempt can (...will...) fail

Lab activity: ex1

Exercise 1: pnd-labs/lab2/ex1

- Manually configure pc1, pc2, pc3 and pc4 in order to be in two different subnetworks and r1 to be the default gateway for all of the hosts

  - See the README file for the addresses to assign

  - Configure pc1 and pc4 using the `interfaces` file

  - Configure pc2 using the `ip` command

  - Configure pc3 using the `ifconfig` command

- The DNS server can be the server used by the host machine

  - This should be used also in the `r1`

- The default gateway must be the r1 host

  - Remember: its link-local address

- Verify connectivity within the network with ping

  - See the difference when pinging a link-local address and a GUA

Lab activity: ex2

Exercise 2: pnd-labs/lab2/ex2

- Configure the four PC in order to receive their networking configuration using SLAAC
  - Hint: this is the default!
- See the README file for the different settings
  - Start with the interface file, then set the `sysctl` parameters accordingly to the specifications
  - You can refer to https://docs.kernel.org/networking/ip-sysctl.html
  - **IMPORTANT**: in Katharà to make modifications with `sysctl` you need to start the lab in **priviledged mode** (→ you can use the `lstart.sh` script in the directory)
- Capture the router advertisements/solicitation sent in the network
  - The `radvd` has to be started manually, so that you can launch `tcpdump` before
- Verify connectivity within the network with ping

Understanding addr_gen_mode parameter

- Defines how link-local and autoconf addresses are generated.

    - 0: generate address based on EUI64 (default)

    - 1: do no generate a link-local address, use EUI64 for addresses generated from autoconf

    - 2: generate stable privacy addresses, using the secret from stable_secret (RFC7217, see stable_secret parameter)

        - This allows for a balance between privacy and stability

    - 3: generate stable privacy addresses, using a random secret if unset

Understanding use_tempaddr parameter

- Preference for Privacy Extensions (RFC3041).

    - <= 0 : disable Privacy Extensions

    - == 1 : enable Privacy Extensions, but prefer publicaddresses over temporary addresses.

    - > 1 : enable Privacy Extensions and prefer temporary addresses over public addresses.

- See also:

    - temp_valid_lft - INTEGER

        - valid lifetime (in sec) for temporary addresses (default: 604800, 7 days)

    - temp_prefered_lft - INTEGER

        - preferred lifetime (in sec) for temporary addresses (default: 86400, 1 day)

Lab activity: ex3

Exercise 3: pnd-labs/lab2/ex3

- Configure the router and the PC

  - Router has to correctly advertise prefix, route and stateless directive (namely, via sysctl, dnsmasq)

  - Pcs have to receive their networking configuration using SLAAC and stateless DHCP

- See the README file for the different settings

- Capture the router advertisements/solicitation sent in the network

  - You should start the `dnsmasq` in foreground (-d option), so that you can launch `tcpdump` before

- Verify connectivity within the network with ping

Dnsmasq

- Very comfortable with dual stack hosts

- It handles both IPv4 and IPv6

- With DHCP it is very useful:
  - You can use DHCPv4 to get IPv4 configuration AND to send your hostname
  - You can use DHCPv6 to get IPv6 configuration
  - If the dnsmasq is also the DNS it knows ALL the hostnames in a quite automated way

That's all for today

- **Questions?**

- See you next lecture!!