RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Virtual IPv6 Security Lab Environment

Hands-on Learning

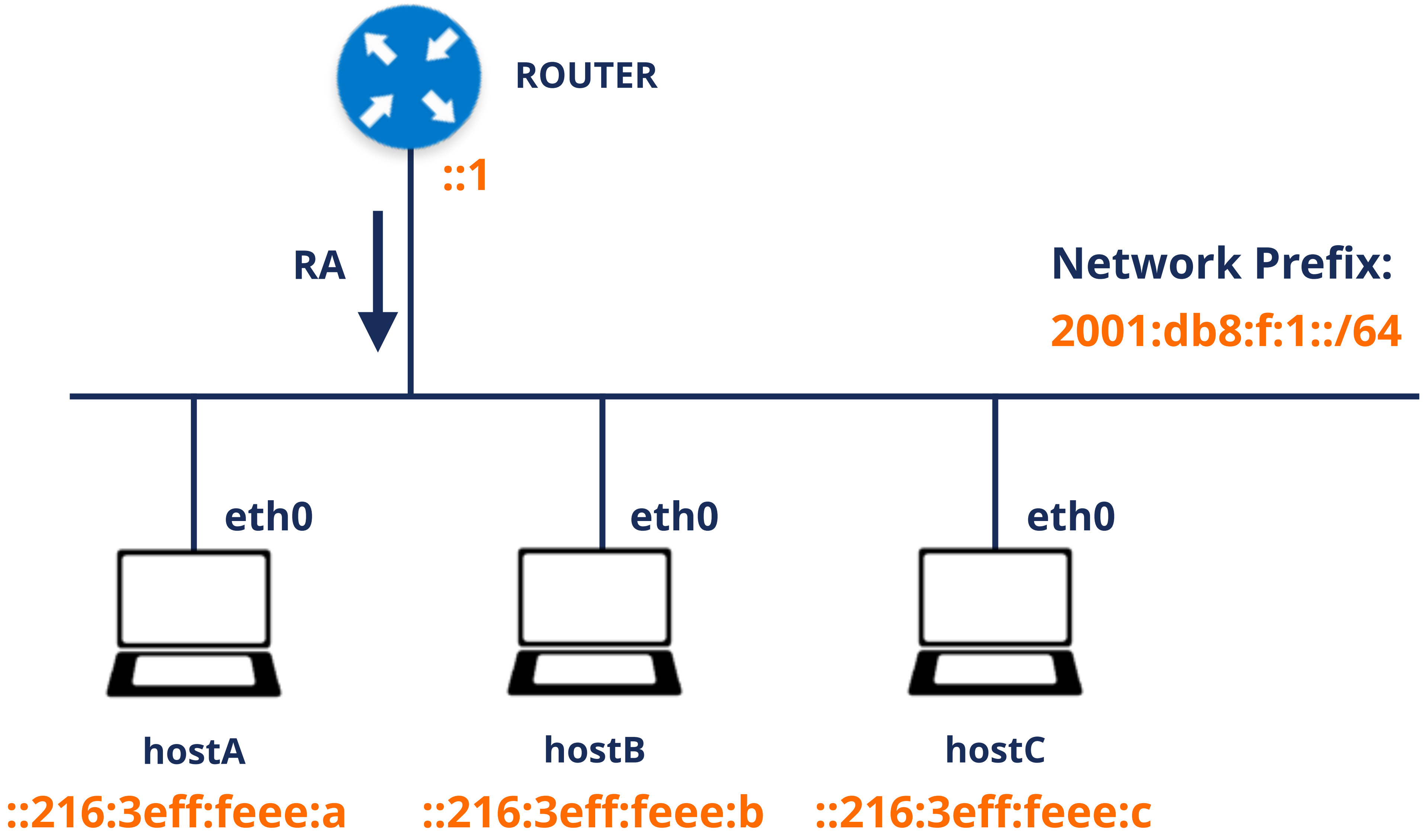
Ondřej Caletka | 25 November 2021 | RIPE 83

RIPE NCC Learning & Development

- Former Training Services of RIPE NCC
- Face-to-face trainings for LIRs
  - Temporary suspended due to COVID-19
- Webinars for LIRs
  - Live interactive sessions lasting one or two hours
- RIPE NCC Academy
  - E-learning platform accessible to everyone
- RIPE NCC Certified Professionals
  - Prove your skills and receive a digital badge

IPv6 Security E-learning Course

- The newest addition to IPv6 Security trainings and webinars
- Preparation for IPv6 Security Certified Professional exam
- First time with hands-on labs



Delivering Lab Environment

- Should be universally scalable
- Should not cost us too much money
- Should allow enough time to play with it
- Should be easy to use
- We decided to **deliver a Virtual Machine image**

Image: Markus Meier, FSFE, CC-BY-SA 4.0

Virtual Machine Challenges

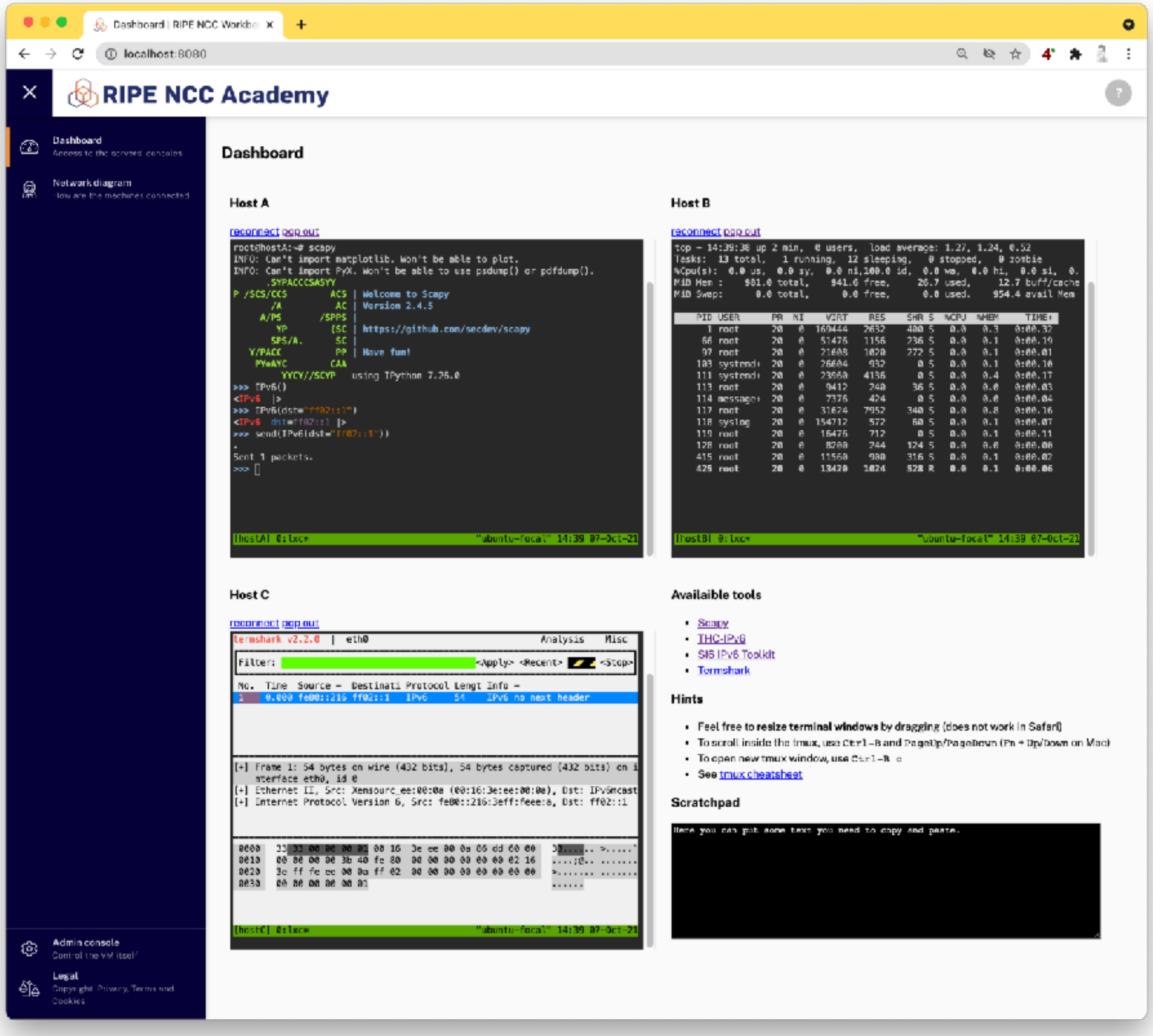
- Different virtualisation technology on each platform
  - The only *common* solution is **Oracle VM VirtualBox**, available on Windows, macOS or Linux
  - Still suboptimal compared to native solutions like Hyper-V or KVM
- No common keyboard layout or screen resolution
  - Therefore, we deliver the VM **headless** with everything accessible over a web interface
- Deploying a VM image is hard
  - We try to make it easier by using **Vagrant**

Running The Labs

- Install VirtualBox
- Install Vagrant
- Open terminal and type:

```
vagrant init ripencc/ipv6seclab
vagrant up
```

- Open web browser on `http://localhost:8080/`



Dashboard | RIPE NCC Workbe
localhost:8080
RIPE NCC Academy
Dashboard
Access to the served consoles
Network diagram
How are the machines connected
Admin console
Control the VM itself
Legal
Copyright, Privacy, Terms and Cookies

Dashboard

Host A

reconnect pop out

```
root@hostA:~# scapy
INFO: Can't import matplotlib. Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
         .SYPACCCSASYY
P /SCS/CCS        ACS | Welcome to Scapy
      /A          AC  | Version 2.4.5
    A/PS       /SPPS  |
       YP         (SC | https://github.com/secdev/scapy
      SPS/A.      SC  |
   Y/PACC         PP  | Have fun!
    PY*AYC       CAA
          YYCY//SCYP   using IPython 7.26.0
>>> IPv6()
<IPv6  |>
>>> IPv6(dst="ff02::1")
<IPv6  dst=ff02::1 |>
>>> send(IPv6(dst="ff02::1"))
.
Sent 1 packets.
>>> 
[hostA] 0:lxc*                              "ubuntu-focal" 14:39 07-Oct-21
```

Host B

reconnect pop out

```
top - 14:39:38 up 2 min,  0 users,  load average: 1.27, 1.24, 0.52
Tasks:  13 total,   1 running,  12 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.
MiB Mem :    981.0 total,    941.6 free,     26.7 used,     12.7 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.    954.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+
      1 root      20   0  169444   2632    400 S   0.0   0.3   0:00.32
     66 root      20   0   51476   1156    236 S   0.0   0.1   0:00.19
     97 root      20   0   21608   1020    272 S   0.0   0.1   0:00.01
    103 systemd+  20   0   26604    932      0 S   0.0   0.1   0:00.10
    111 systemd+  20   0   23960   4136      0 S   0.0   0.4   0:00.17
    113 root      20   0    9412    240     36 S   0.0   0.0   0:00.03
    114 message+  20   0    7376    424      0 S   0.0   0.0   0:00.04
    117 root      20   0   31624   7952    340 S   0.0   0.8   0:00.16
    118 syslog    20   0  154712    572     60 S   0.0   0.1   0:00.07
    119 root      20   0   16476    712      0 S   0.0   0.1   0:00.11
    128 root      20   0    8200    244    124 S   0.0   0.0   0:00.00
    415 root      20   0   11560    900    316 S   0.0   0.1   0:00.02
    425 root      20   0   13420   1024    528 R   0.0   0.1   0:00.06

[hostB] 0:lxc*                              "ubuntu-focal" 14:39 07-Oct-21
```

Host C

reconnect pop out

```
termshark v2.2.0  |  eth0                                    Analysis   Misc
 Filter:                                  <Apply> <Recent>      <Stop>
 No.  Time  Source -  Destinati Protocol Lengt Info -
 1    0.000 fe80::216 ff02::1   IPv6     54    IPv6 no next header

[+] Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on i
    nterface eth0, id 0
[+] Ethernet II, Src: Xensource_ee:00:0a (00:16:3e:ee:00:0a), Dst: IPv6mcast
[+] Internet Protocol Version 6, Src: fe80::216:3eff:feee:a, Dst: ff02::1

 0000   33 33 00 00 00 01 00 16  3e ee 00 0a 86 dd 60 00   33...... >.....`
 0010   00 00 00 00 3b 40 fe 80  00 00 00 00 00 00 02 16   ....;@.. ........
 0020   3e ff fe ee 00 0a ff 02  00 00 00 00 00 00 00 00   >....... ........
 0030   00 00 00 00 00 01                                  ......
[hostC] 0:lxc*                              "ubuntu-focal" 14:39 07-Oct-21
```

Availaible tools

- Scapy
- THC-IPv6
- SI6 IPv6 Toolkit
- Termshark

Hints

- Feel free to **resize terminal windows by dragging** (does not work in Safari)
- To scroll inside the tmux, use `Ctrl-B` and `PageUp/PageDown` (Fn + Up/Down on Mac)
- To open new tmux window, use `Ctrl-B c`
- See tmux cheatsheet

Scratchpad

```
Here you can put some text you need to copy and paste.
```

Under The Hood

- Based on Ubuntu 20.04 LTS
- Three containers managed by **LXD**
- Consoles accessible from web browser using **ttyd** and **tmux**
- Static website and WebSocket proxy by **NGINX**
- Everything deployed using **Ansible**
- **Public development** in RIPE NCC's GitHub repository

`https://github.com/RIPE-NCC/ipv6-security-lab/`

ICMPv6 Redirects vs. Linux

- Worked as expected until Linux 4.17
- From Linux 4.18 on, incoming redirects are ignored
  - Regardless of sysctl `net.ipv6.conf.all.accept_redirects = 1`
  - Always reproducible with Ubuntu
    - Probably related to IPv6 being set up by `systemd-networkd` (or `dhcpcd`)
  - Redirects work as expected with kernel-level autoconfiguration
  - Hard to reproduce in kernel self-test (`icmp_redirect.sh`)
- After all, we do recommend disallowing redirects ;)
  - But for the lab environment, we need them working
  - Workaround by reverting to kernel-level autoconfiguration

Further Steps

- Collect feedback from the users
- Expand the lab to use a more real networking gear
  - Some routers are now available as containers
  - Uncertain licence conditions

Try out our new IPv6 security e-learning course!

https://academy.ripe.net

Questions?

Ondrej.Caletka@ripe.net
@ripencc