Lab Activities

IPv6 Security E-Learning Course

What can you do with the IPv6 Security labs?

Applying theory in practice

Reproduce an attack

Implement a solution and **verify** if it is actually working

Lab Activities

Lab Activity 0 - Installing and Troubleshooting the Labs

Lab Activity 1 - Generating IPv6 packets using Scapy

Lab Activity 2 - IPv6 Network Scanning

Lab Activity 3 - NDP Neighbor Cache Poisoning

Lab Activity 4 - Verifying if a security solution is working: RA-Guard

Lab Activity 5 - IPv6 Network Scanning using MLD

Lab Activity 6 - Configuring IPv6 packet filtering on hosts

Lab Activities

Lab Activity 0 - Installing and Troubleshooting the Labs

Lab Activity 1 - Generating IPv6 packets using Scapy

Lab Activity 2 - IPv6 Network Scanning

Lab Activity 3 - NDP Neighbor Cache Poisoning

Lab Activity 4 - Verifying if a security solution is working: RA-Guard

Lab Activity 5 - IPv6 Network Scanning using MLD

Lab Activity 6 - Configuring IPv6 packet filtering on hosts

SANDBOX INC.

Lab activity: Is Sandbox Inc. under attack?

You follow these 6 steps:

1. Look at the details of the detected NS message
2. Create your tailor-made NS message
3. Check the effect of the NS message
4. Look at the details of the detected NA message
5. Create your tailor-made NA message
6. Check the effect of the NA message

1. Academy Instructions

Step 2.1

From host C, start the interactive shell using the scapy command

```
root@hostC:~# scapy
```

Step 2.2

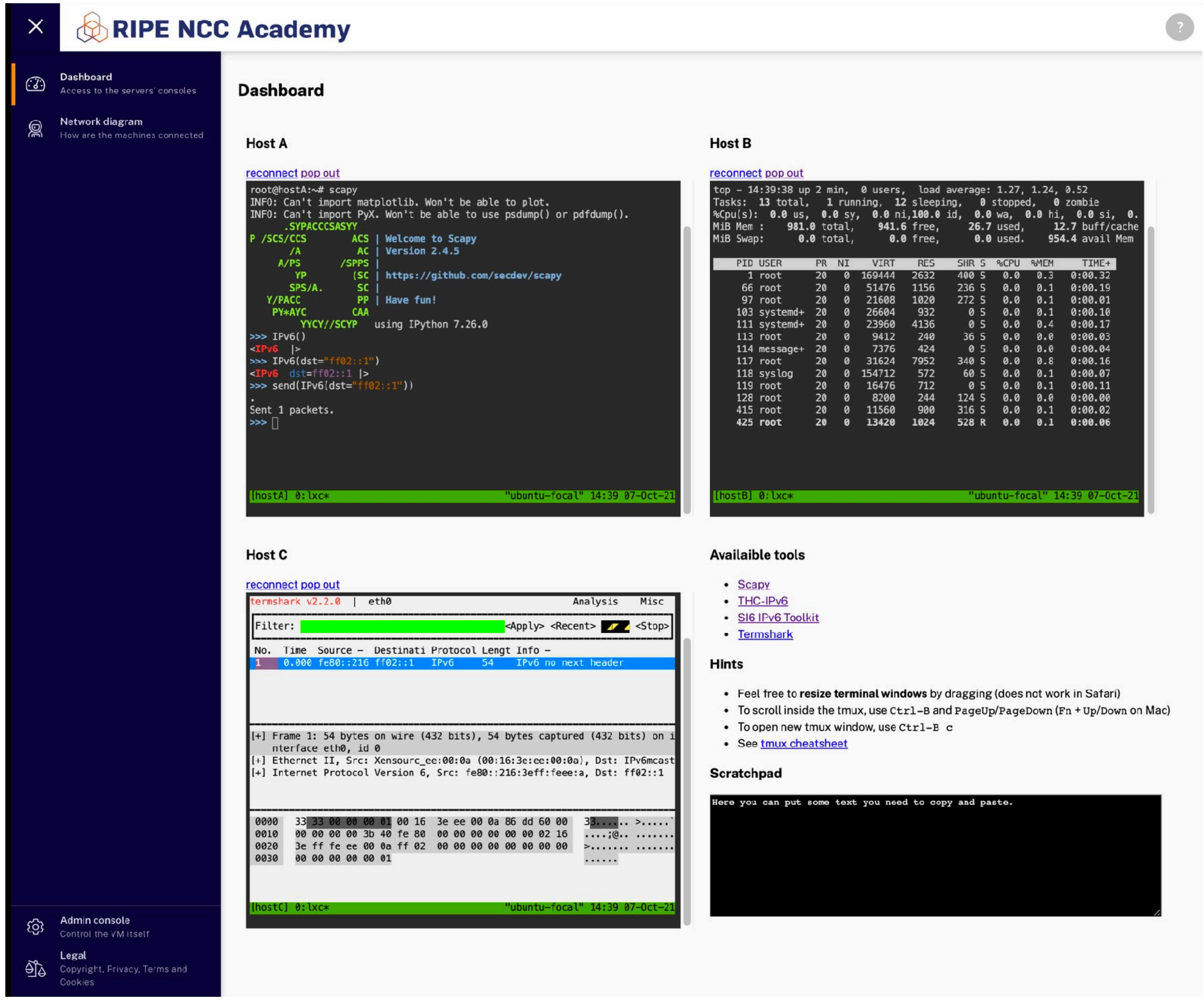
Now you can create your tailor-made message:

```
>>> a = IPv6(src="2001:db8:f:1:216:3eff:feee:b",
dst="2001:db8:f:1:216:3eff:feee:a")
>>> b = ICMPv6ND_NS(tgt="2001:db8:f:1:216:3eff:feee:a")
>>> c = ICMPv6NDOptSrcLLAddr(lladdr="00:16:3e:ee:00:0c")

>>> pkt = a / b / c
```

The message is composed of the Basic IPv6 header (a), the ICMPv6 NS message (b) and a Source Link Layer Address Option (c) that is included in the NS message. Remember that you can see details using the **show()** function (pkt.show()), to check whether everything is OK.

2. Lab environment


RIPE NCC Academy
Dashboard
Access to the servers' 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: Xensourc_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.
```

Questions to check your understanding

Your boss is very concerned and nervously asks what the **first** action should be right now.

○ Keep looking at the IDS logs

○ Disconnect the attacking host from the network

○ Elevate the warning level of the IDS for that kind of messages

○ That all your colleagues learn about the problem

SUBMIT

Lab activities alignment with exam questions

1.3.1 Choose the correct tool to assess IPv6 security threats and mitigation techniques

3.1.4 Identify the IPv6 security threats related to NDP

3.2.2 Choose a suitable and available security measure for IPv6 security issues related with NDP

An initiative by the RIPE NCC, the Regional Internet Registry for Europe, Middle East and Central Asia

Certifying Skills for the Future

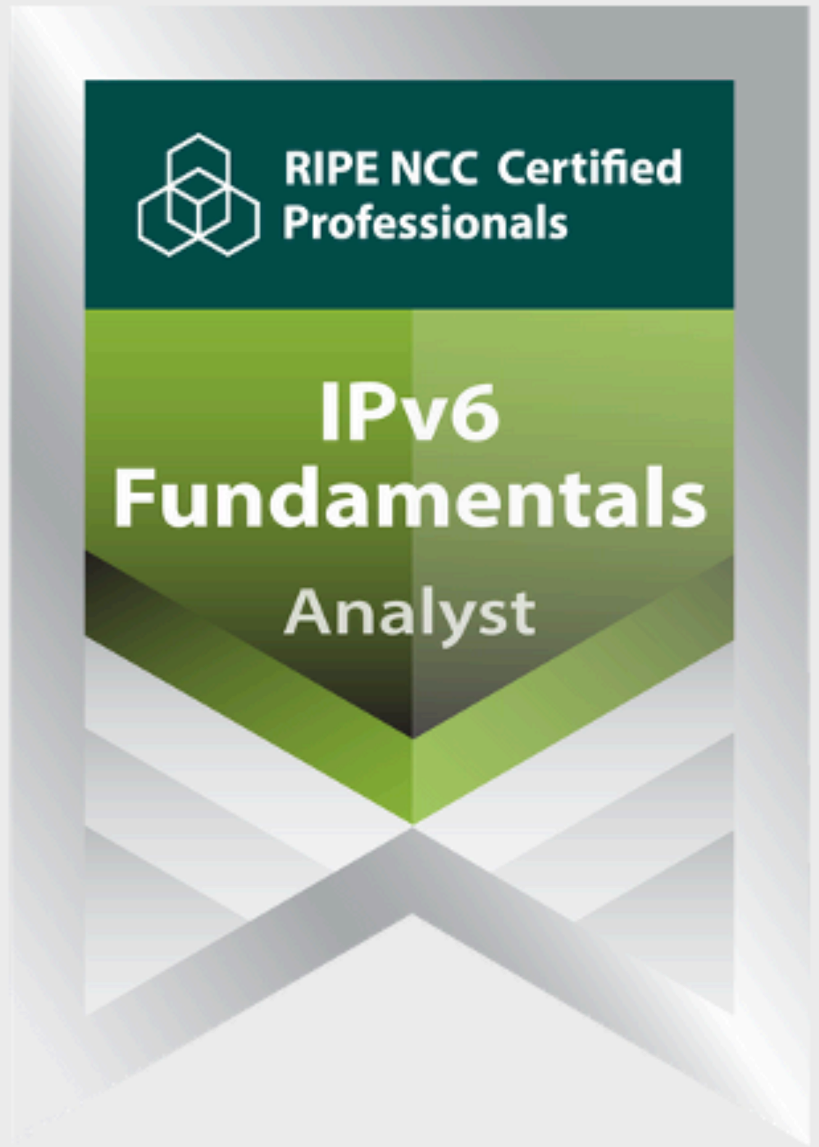
RIPE NCC
Certified
Professionals

Our Learning Paths

IP Address Management

→

IPv6 Technology



→

Network Security

→

Why certify with the RIPE NCC

01

Knowledge and skills based on best practices

02

Over 20 years of experience in technical capacity building

03

Vendor-neutral, independent certification

04

Content developed based on market requirements with experts in the field

05

The authority on the technical infrastructure of the Internet

We build our certifications drawing on the input of the RIPE community and our in-house experts.

RIPE NCC CERTIFIED PROFESSIONALS

Training Support Offered

Live webinars on multiple topics

Detailed downloadable exam guide for each certification

Open e-learning courses on the RIPE NCC Academy

In-person training courses for RIPE NCC members

A team of over 15 trainers and experts in the field deliver our trainings.

Certification Process

- Schedule an exam online
- Study using the e-learning course in the RIPE NCC Academy or join a webinar
- Take the exam online under the supervision of a 'live' proctor
- Claim your verifiable digital badge and share it online

Certify Your Team

Skill Competence Across the Organisation

We can support your capacity building efforts to ensure skill competence across your organisation. RIPE NCC's Certified Professionals programme can leverage training as part of your project, by ensuring that the people involved develop practical skills and reach a high standard of competence.

Institutional Partnerships

As member of RIPE NCC, you have access to our Certified Professionals program through exam vouchers. We also offer additional exam vouchers in bundles for larger programs and for non-members through our institutional partnerships.

IPv6 Security Expert

An IPv6 Security Expert is capable of designing a high-level strategy to protect an IPv6 network against common threats. A holder of this badge has demonstrated the ability to identify and analyse common IPv6 security threats and their impact, and create a plan to counter them. An IPv6 Security Expert has shown their ability to assess the security of an IPv6 network, and to make use of the latest information about IPv6 network vulnerabilities and mitigation techniques.

This exam certifies the ability to:

- Design a high-level IPv6 security strategy to protect your IPv6 network against new attack vectors and most common threats
- Design filtering rules for IPv6 packets
- Choose security options for IPv6 routing protocols
- Choose the correct type of tool to assess IPv6 security threats and mitigation techniques

Recommended knowledge

- IPv4 and IPv6 networking knowledge
- Proficiency with details of IPv6 and associated protocols like ICMPv6, NDP, MLD and DHCPv6
- Familiarity with IP traffic filtering concepts
- General knowledge about existing routing protocols, and more specifically about BGP
- Experience with security assessment tools

Exam Format

- Multiple-choice
- Multiple answers
- Matching
- Drag and drop and ordering questions
- Fill in the blank questions

Exam Duration

60 minutes

Passing Grade

Candidates must score a minimum of 70% in the exam.

Contact us

Ivy Agbo

Exams Coordinator

exams@ripe.net

Marc Wullings

Partnerships Lead

Certified Professionals

mwullings@ripe.net

RIPE NCC Academy

academy@ripe.net

Together, let's shape the future of the Internet

A RIPE NCC INITIATIVE