



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

Přenosná a přenositelná laboratoř s open source

Praktická výuka na vlastním počítači

Ondřej Caletka | 12. června 2022 | InstallFest 2022

RIPE NCC Learning & Development



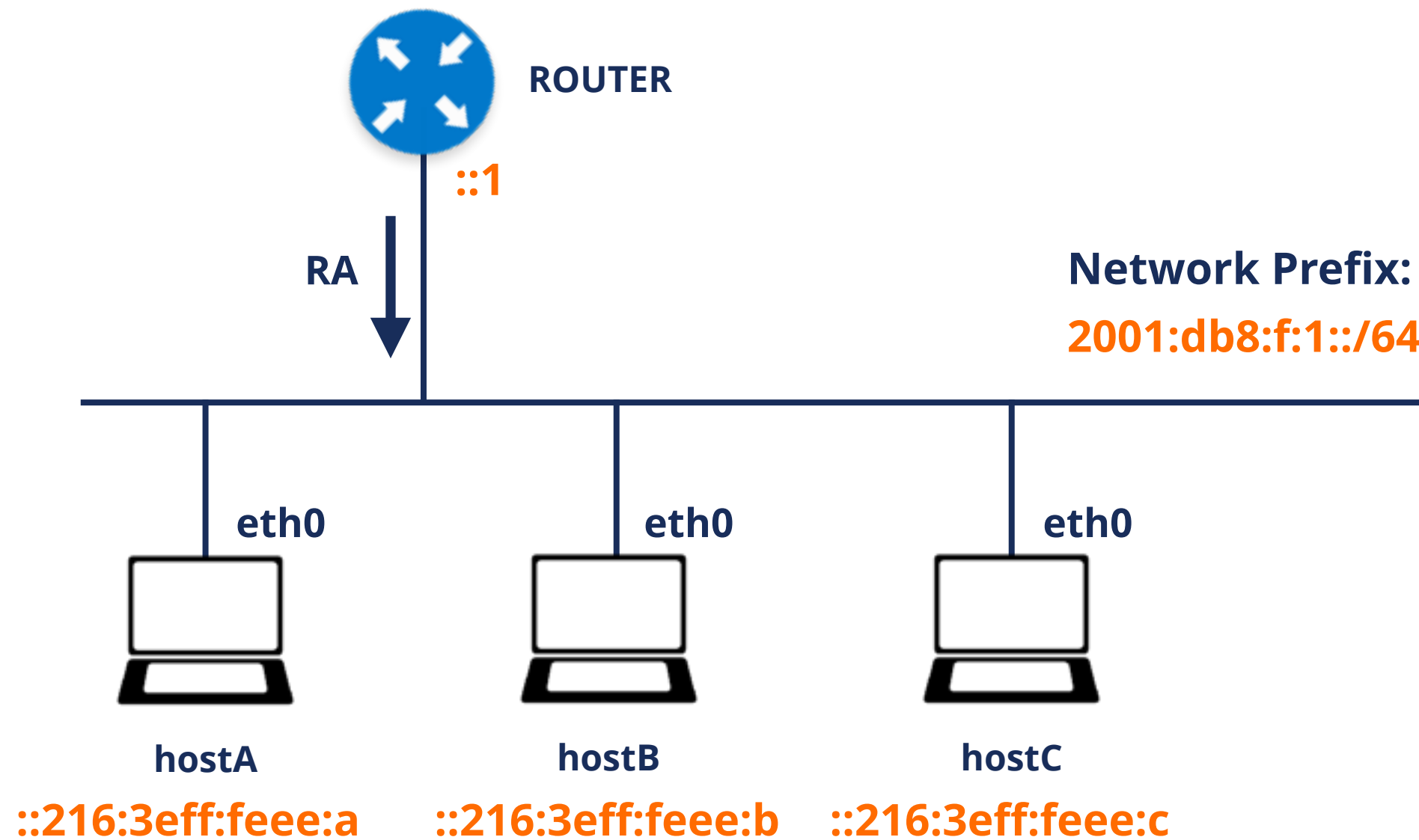
- Dříve RIPE NCC Training Services
- Face-to-face školení pro členy
 - Restartujeme po dvouleté přestávce
- Webináře pro členy
 - Živé on-line lekce na jednu nebo dvě hodiny
- RIPE NCC Academy
 - E-learningové prostředí dostupné všem
- RIPE NCC Certified Professionals
 - Možnost získat digitální certifikát po absolvování online dohledovaného testu



IPv6 Security E-learning Course



- Novinka v portfoliu RIPE NCC Academy
- Příprava pro IPv6 Security Certified Professional exam
- Poprvé včetně praktických úloh ve virtuálním prostředí



Jak doručit virtuální laboratoř



- Která škáluje i na stovky účastníků
- Bez velkých nákladů z naší strany
- Bez omezení doby používání
- Která je snadno spustitelná
- Nakonec jsme se rozhodli distribuovat **obraz virtuálního serveru**



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

Problémy s virtuálními stroji



- Každá platforma poskytuje jiný způsob virtualizace
 - Jediné společné řešení je **Oracle VM VirtualBox**, dostupný na Windows, macOS i Linuxu
 - Suboptimální proti nativní virtualizaci jako Hyper-V nebo KVM
- Každý používá jiné rozlišení displeje a rozložení klávesnice
 - Proto používáme *headless* VM s přístupem pomocí webového prohlížeče
- Spuštění virtuálního stroje z obrazu je složité
 - Používáme **Vagrant** pro sestavení, snadné stažení a spuštění obrazu

Spuštění prostředí



- Nainstalujte VirtualBox
- Nainstalujte Vagrant
- Napište do terminálu:
vagrant init ripencc/ipv6seclab
vagrant up
- Otevřte prohlížeč na
<http://localhost:8080/>

The screenshot shows the RIPE NCC Academy dashboard at localhost:8080. The dashboard is divided into several sections:

- Host A:** A terminal window showing the Scapy installation process. The output includes:

```
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 psdup() or pdfdump().
.SYPAACCSASY
P /SCS/CCS AC 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!
  PYWYC CAA
  YYCV/SCVP using Python 3.7.6.0
>>> TPv6()
<TPv6 |>
>>> TPv6(dst='ff02::1')
<TPv6 dst=ff02::1 |>
>>> send(IPv6dst='ff02::1')
.
Sent 1 packets.
>>> []
```
- Host B:** A terminal window showing the output of the 'top' command, displaying system statistics and a list of running processes.
- Host C:** A terminal window showing the output of the 'tcpdump' command, displaying network traffic details.
- Available tools:** A list of tools available for use, including Scapy, THC-IPV6, SIB IPv6 Toolkit, and Tormshark.
- Hints:** A list of hints for using the environment, including instructions on how to resize terminal windows and scroll inside the tmux.
- Scratchpad:** A text area for taking notes.

Jak to funguje



- Založeno na Ubuntu 20.04 LTS
- Tři kontejnery spuštěné pomocí **LXD**
- Zpřístupnění konzolí pomocí **ttyd** a **tmux**
- Statická webová stránka a WebSocket proxy pomocí **NGINX**
- Všechno nainstalováno pomocí **Ansible**
- **Veřejný vývoj** na GitHubu RIPE NCC

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

Jak dostat terminál do prohlížeče



- Na výběr z: Gotty (Go), WeTTY (node.js), ttyd (C)
- Chová se jako HTTP server s podporou WebSocket
- Poskytuje aplikaci **Xterm.js**
- Pro *každý* WebSocket je spuštěn uživatelem určený příkaz

```
localhost:7681
1[|||||] 32.9% 5[|||||] 19.2%
2[|||||] 4.0% 6[|||||] 2.6%
3[|||||] 24.0% 7[|||||] 18.7%
4[|||||] 2.7% 8[|||||] 2.0%
Mem[|||||] 5.71G/8.00G Tasks: 434, 1757 thr, 0 kthr; 2 running
Swp[|||||] 15.10G/6.00G Load average: 1.87 2.88 3.08
Uptime: 10 days, 06:07:02

PID USER PRI NI VIRT RES S CPU%MEM% TIME+ Command
0 root 32 0 0 0 0 ? 0.0 0.0 0:00.00 kernel_task
1 root 8 0 0 0 0 ? 0.0 0.0 0:00.00 launchd
70 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 syslogd
71 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 UserEventAgent
75 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 uninstalld
76 root 50 0 0 0 0 ? 0.0 0.0 0:00.00 fseventsd
77 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 mediaremoted
80 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 systemstats
82 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 configd
85 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 powerd
89 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 remoted
91 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 logd
97 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 watchdogd
101 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 mds
105 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 kernelmanagerd
106 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 diskarbitrationd
113 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 thermalmonitord
114 root 17 0 0 0 0 ? 0.0 0.0 0:00.00 contextstored

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice F9Kill F10Quit

+ vagrant-netlab-IPv6-security git:(main) ttyd http
[2021/10/14 15:28:25:8945] N: ttyd 1.6.3 (libwebsockets 4.3.0-v4.3.0)
[2021/10/14 15:28:25:8957] N: tty configuration: 411981: 0 Καθαρός Δ... Support
[2021/10/14 15:28:25:8957] N: start command: http 019: Ref. 780001... Support
[2021/10/14 15:28:25:8957] N: close signal: SIGHUP (1) ourartie... noreply@labs.ripe.net
[2021/10/14 15:28:25:8957] N: terminal type: xterm-256color
[2021/10/14 15:28:26:0342] N: /usr/local/Cellar/libwebsockets/4.3.0/lib/libwebsocke
ts-evlib_uv.dylib Frantisek Holop
[2021/10/14 15:28:26:0342] N: LWS: 4.3.0-v4.3.0, NET CLI SRV H1 H2 WS ConMon IPV6-off
[2021/10/14 15:28:26:0346] N: elops_init_pt_uv: Using foreign event loop...
[2021/10/14 15:28:26:0346] N: ++ [wsil0|pipe] (1)
[2021/10/14 15:28:26:0347] N: ++ [vhl0|default|7681] (1)
[2021/10/14 15:28:26:0442] N: [null wsi]: lws_socket_bind: source ads 0.0.0.0
[2021/10/14 15:28:26:0443] N: ++ [wsil1|listen|default|7681] (2)
[2021/10/14 15:28:26:0443] N: Listening on port: 7681
[2021/10/14 15:28:44:4740] N: ++ [wsisrvl0|adopted] (1)
[2021/10/14 15:28:44:4747] N: HTTP / - 127.0.0.1
[2021/10/14 15:28:44:6064] N: HTTP /token - 127.0.0.1
[2021/10/14 15:28:44:8348] N: ++ [wsisrvl1|adopted] (2)
[2021/10/14 15:28:44:8357] N: WS /ws - 127.0.0.1, clients: 1
[2021/10/14 15:28:44:8516] N: started process, pid: 1743
[2021/10/14 15:28:49:6120] N: -- [wsisrvl0|adopted] (1) 5.137s
```


Jak neztratit relaci



- GNU Screen, nebo tmux
- Umožňuje vícenásobné připojení ke stejné relaci
- Sdílení terminálů je složitá úloha
- Komplikované ovládání vestavěného scrollbacku
- Verze novější než tmux 2.3 ~~zkracují~~ *optimalizují* dlouhé výpisy
- Workaround: rollback na tmux 2.3

```
ocaletka — _zsh_tmux_plugin_run a — tmux — tmux a — 86x27
1[|||||] 32.7% 5[|||||] 22.7%
2[|] 3.3% 6[|] 2.6%
3[|||||] 35.3% 7[|||||] 19.9%
4[|] 3.3% 8[|] 2.0%
Mem[|||||] 5.90G/8.00G Tasks: 460, 1813 thr, 0 kt
Swp[|||||] 5.25G/6.00G Load average: 2.66 3.49 3.
Uptime: 10 days, 06:19:09

PID USER PRI NI VIRT RES S CPU%MEM% TIME+
0 root 32 0 0 0 ? 0.0 0.0 0:00.00
1 root 17 0 0 0 ? 0.0 0.0 0:00.00
70 root 17 0 0 0 ? 0.0 0.0 0:00.00
71 root 17 0 0 0 ? 0.0 0.0 0:00.00
75 root 17 0 0 0 ? 0.0 0.0 0:00.00
76 root 50 0 0 0 ? 0.0 0.0 0:00.00
77 root 17 0 0 0 ? 0.0 0.0 0:00.00
80 root 17 0 0 0 ? 0.0 0.0 0:00.00
82 root 17 0 0 0 ? 0.0 0.0 0:00.00
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -

[0] 0:htop* "macicek" 15:42:04 2021-10-14
```

ICMPv6 přesměrování a Linux



- Pracovalo bez problémů až do Linuxu 4.17
- Linuxu 4.18 a novější ICMPv6 přesměrování ignoruje
 - Bez ohledu na `sysctl net.ipv6.conf.all.accept_redirects = 1`
 - Vždy reprodukovatelné v Ubuntu
 - Nejspíš kvůli IPv6 spravované pomocí `systemd-networkd` (or `dhcpcd`)
 - Přesměrování fungují správně s autokonfigurací v jádře
 - Nepodařilo se mi reprodukovat v self-testu jádra (`icmp_redirect.sh`)
- Beztak doporučujeme přesměrování zablokovat ;)
 - Ale úloha vyžaduje, aby napřed fungovalo
 - Workaround pomocí vynucení autokonfigurace v jádře

Další kroky



- Získat zpětnou vazbu
- Řešit kompatibilitu s Apple silicon
 - nepodporován VirtualBoxem
 - emulace amd64 je problematická
- Přidat do prostředí více realistické routery
 - Pro kurz BGP Security
 - Některé routery jsou dnes k dispozici jako kontejnery (*containerlab.dev*)
 - Nejisté licenční podmínky

<https://academy.ripe.net>





Questions



Ondrej.Caletka@ripe.net
<https://ondrej.caletka.cz>