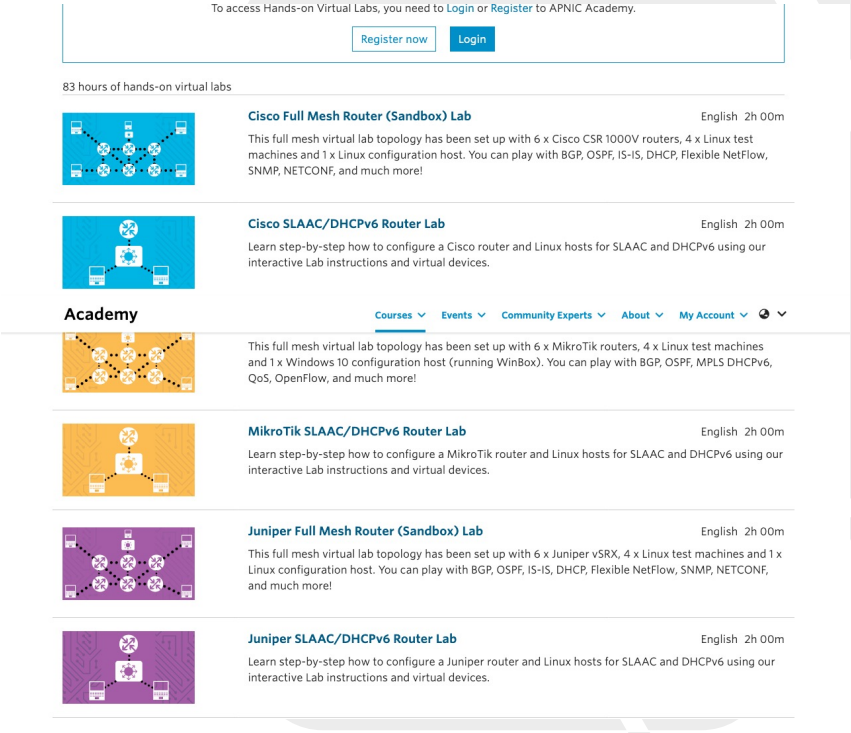
Practical Cyber Security Workshop

PACNOG 30, Suva



https://academy.apnic.net/en/virtual-labs

Register for Virtual Labs

Day1

Time	
9:00 – 1030	Over view / Intro / Recap
11– 1230	Devices Hardening
130 – 330	Pentesting Lab 1
1600 - 1700	Pentesting Lab 2

* Pentesting Lab (Academy)

Day 2

Time	
9:00 – 1030	Practical Packet Analysis
11– 1230	Practical Packet Analysis – 2
130 – 330	Practical Packet Analysis – 3
1600 - 1700	Honeypots

* Practical Packet Analysis Lab (Academy)

Day 3

Time	
9:00 – 1030	Security Monitoring – part 1
11– 1230	Security Monitoring – part 2
130 – 330	Security Monitoring – part 3
1600 - 1700	Memory Forensics – part 1

- New Academy Lab
  - Wazuh for security monitoring
  - Volatility for memory forensics (malware memory dump)
- Plan B: Virtual Box

Day 4

Time	
9:00 – 1030	Memory Forensics – part 2
11– 1230	CSIRT & Incident Response
130 – 330	Threat Sharing & Table Top Exercise
1600 - 1700	Wrap Up / Discussion

What to Expect

1. Learn various aspects of security and security monitoring (network, os, prevention, detection, resilience)
2. Proactive and reactive
3. Related issues to the core topics
4. Lots of discussion & sharing
5. Practical labs – visualize the concepts & ideas
6. Lessons learned from real case studies
7. Some ideas of how to improve security or ask for more security resources ($$)
8. Post-workshop discussion & sharing and friendship. Starting a security community / special interest group

Self-Introduction