LEEDS BECKETT UNIVERSITY

Cybercrime & Security Innovation Centre

Open Source CyBOK Practical Challenges and Learning Resources

Hacktivity
Cyber Security Labs

Dr Z. Cliffe Schreuders

Reader in Cyber Security
Director, Cybercrime & Security Innovation Centre

Challenges

Hands-on hacking challenges are an effective way of engaging learners, **but building challenges is hard work**.

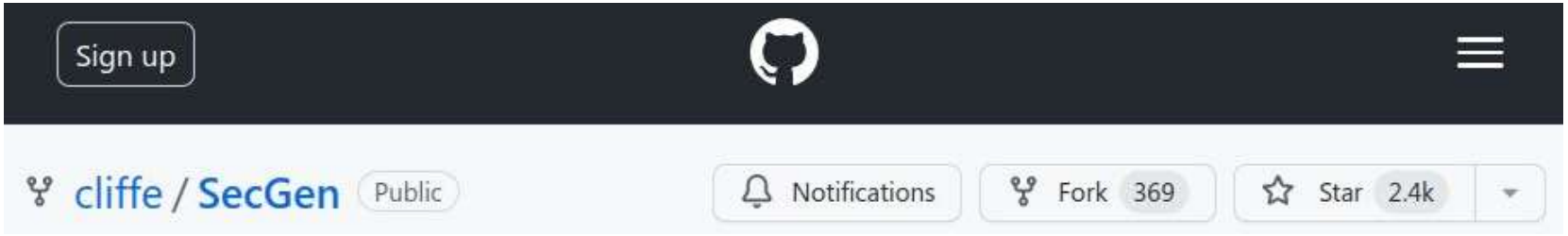
Typically a created CTF challenge is **manually** created for one event and can only be used once.

Solution

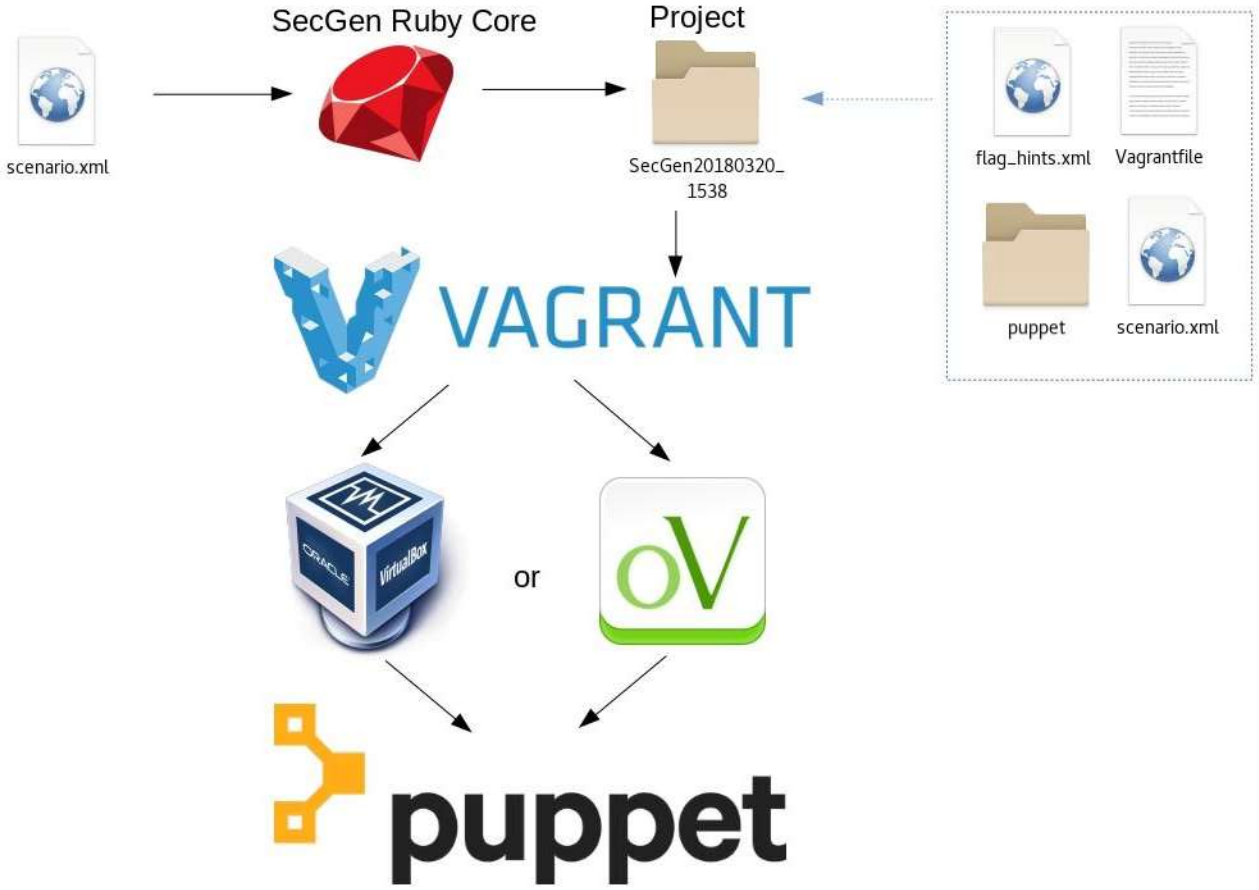
SecGen framework generates randomised VMs, meaningful security challenges, and CTF scenarios.

- Randomisation – **unlike any alternative**
- Code-based approach, with reusable components
- Huge library of content – mapped to CyBOK

open source™



SecGen overview



XML CyBOK Mapping

- Mappings for scenarios (labs/ctfs), videos, and components of challenges

```
<CyBOK KA="AAA" topic="Authorisation">
  <keyword>access control</keyword>
  <keyword>enforcing access control</keyword>
  <keyword>ACCESS CONTROL - DAC (DISCRETIONARY ACCESS CONTROL)</keyword>
  <keyword>Vulnerabilities and attacks on access control misconfigurations</keyword>
</CyBOK>
<CyBOK KA="OSV" topic="Primitives for Isolation and Mediation">
  <keyword>Access controls and operating systems</keyword>
  <keyword>Linux security model</keyword>
  <keyword>Unix File Permissions</keyword>
  <keyword>Filesystems, inodes, and commands</keyword>
  <keyword>umask</keyword>
</CyBOK>
<CyBOK KA="OSV" topic="Role of Operating Systems">
  <keyword>mediation</keyword>
</CyBOK>
```

Huge library of content mapped to CyBOK

- ethical hacking and penetration testing
- web and network security
- systems security
- incident response and investigation
- malware and reverse engineering
- software security and exploit development

CyBOK

Open source content mapped to CyBOK

103 practical cyber security labs mapped to CyBOK

https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Scenarios-Indexed.md

70 lecture videos with CyBOK KAs and Topics

https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Lecture-Videos.md

30 full-length, multi-step CTF scenarios mapped to CyBOK

https://github.com/cliffe/SecGen/blob/master/README-CyBOK-CTF-Scenarios-Indexed.md

Current CyBOK work

- A team of 5 student interns contributing modules to SecGen
- New software vulnerabilities
- New hacking scenarios, including narrative generated by ChatGPT
- New forensics evidence generation and user content

All open source, and mapped to CyBOK!

CyBOK

Hacktivity
Cyber Security Labs

Hosted lab infrastructure, provides access to hacking challenges and learning content, and manages VMs.

Core value of open innovation.

Launching to market 2023.

CYBER + ASAP | Academic Startup Accelerator Programme


Hacktivity
Cyber Security Labs