CYBERARRANGE

# Open source training grounds for attack and response teams

Ivan Kovačević
CyberArrange Security Solutions

# About the speaker

- Graduated at the Faculty of Electrical Engineering and Computing in 2017
- During his PhD studies worked on several cyber security R&D projects; regularly participated in exercise events
- (Co-)Founded the university Spin-off CyberArrange in 2023
- Also worked/works as a Software Engineer and DevOps Engineer

# Why use cyber ranges?

- Allegedly, attacking real systems for training is not desirable
- Learning involves mistakes and requires structure and support
- Trainings and exercises benefit from feedback and after-action reviews
- It should be possible to test alternative scenarios and do experiments

- Cyber ranges provide a safe environment for training
- Their features aim to solve the problems above

# Common cyber range features

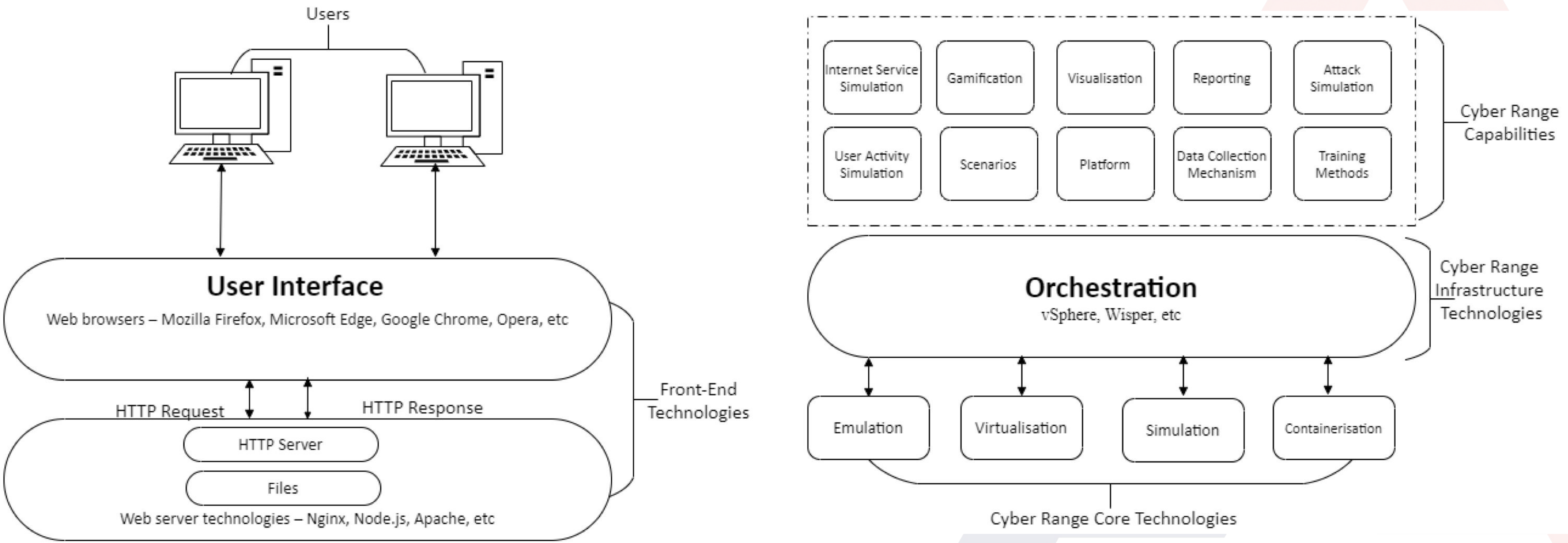


Figure from: Ukwandu, E.; Farah, M.A.B.; Hindy, H.; Brosset, D.; Kavallieros, D.; Atkinson, R.; Tachtatzis, C.; Bures, M.; Andonovic, I.; Bellekens, X. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors 2020, 20, 7148. https://doi.org/10.3390/s20247148

# Why should we care for open-source CRs?

- Many commercial services are available…

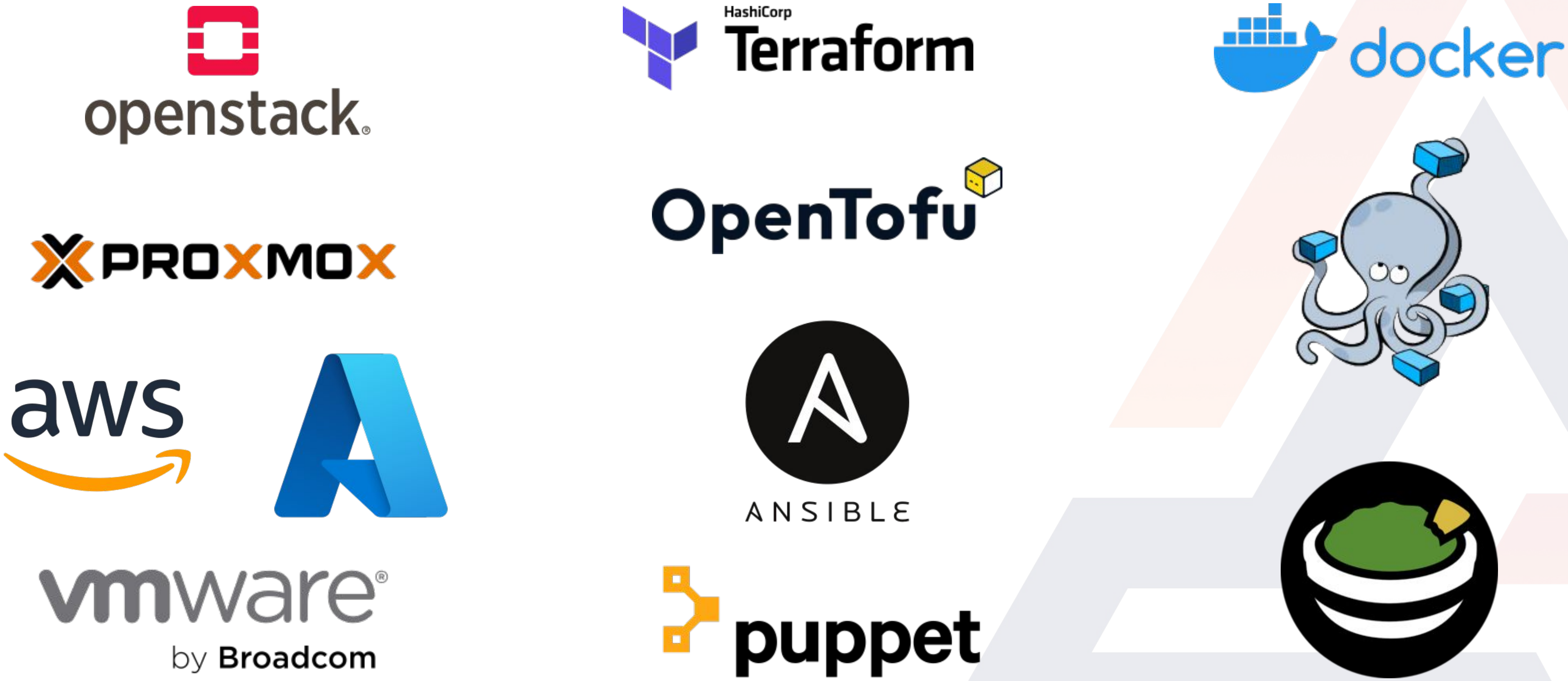
- Flexibility - useful for experiments and internal research
- Creating specific training programmes, e.g. for onboarding
- Lower licensing cost - but demanding maintenance

# Our investigation

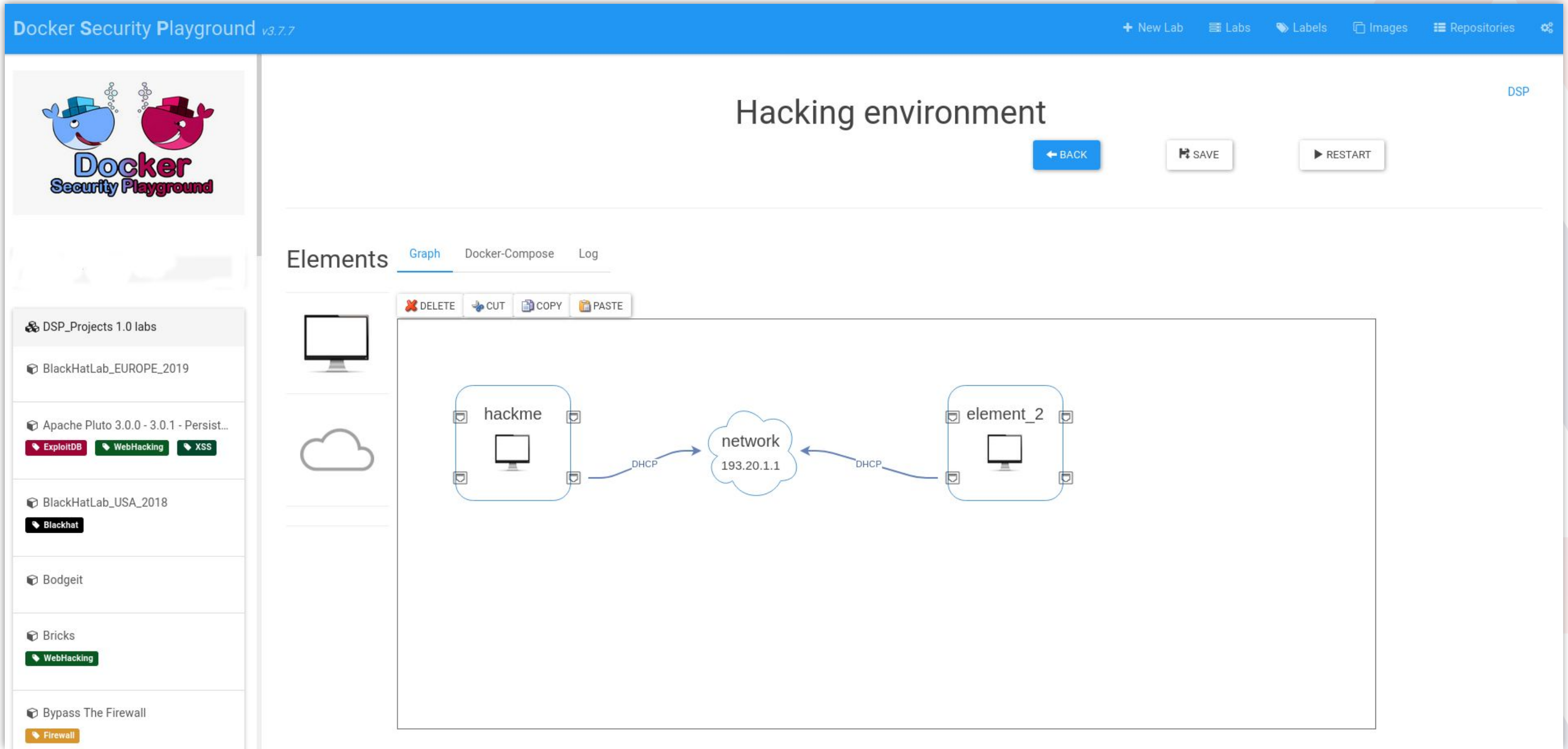
- We investigated ~20 open-source CR technologies for deployment in CyberArrange
- Some representative examples:

| **Small scale trainings<br>(e.g. on workstations)** | **Medium-scale trainings** | **Large-scale trainings** |
|---|---|---|
| Docker Security Playground | Ludus | Open Cyber Range |
| AWS Cyber Range | KYPO Cyber Range Platform | DeterLab |
| ... | ... | ... |

# These CRs rely on IaC and cloud technologies…



# Docker Security Playground (1)



DSP_Projects 1.0 labs

BlackHatLab_EUROPE_2019

Apache Pluto 3.0.0 - 3.0.1 - Persist...
ExploitDB WebHacking XSS

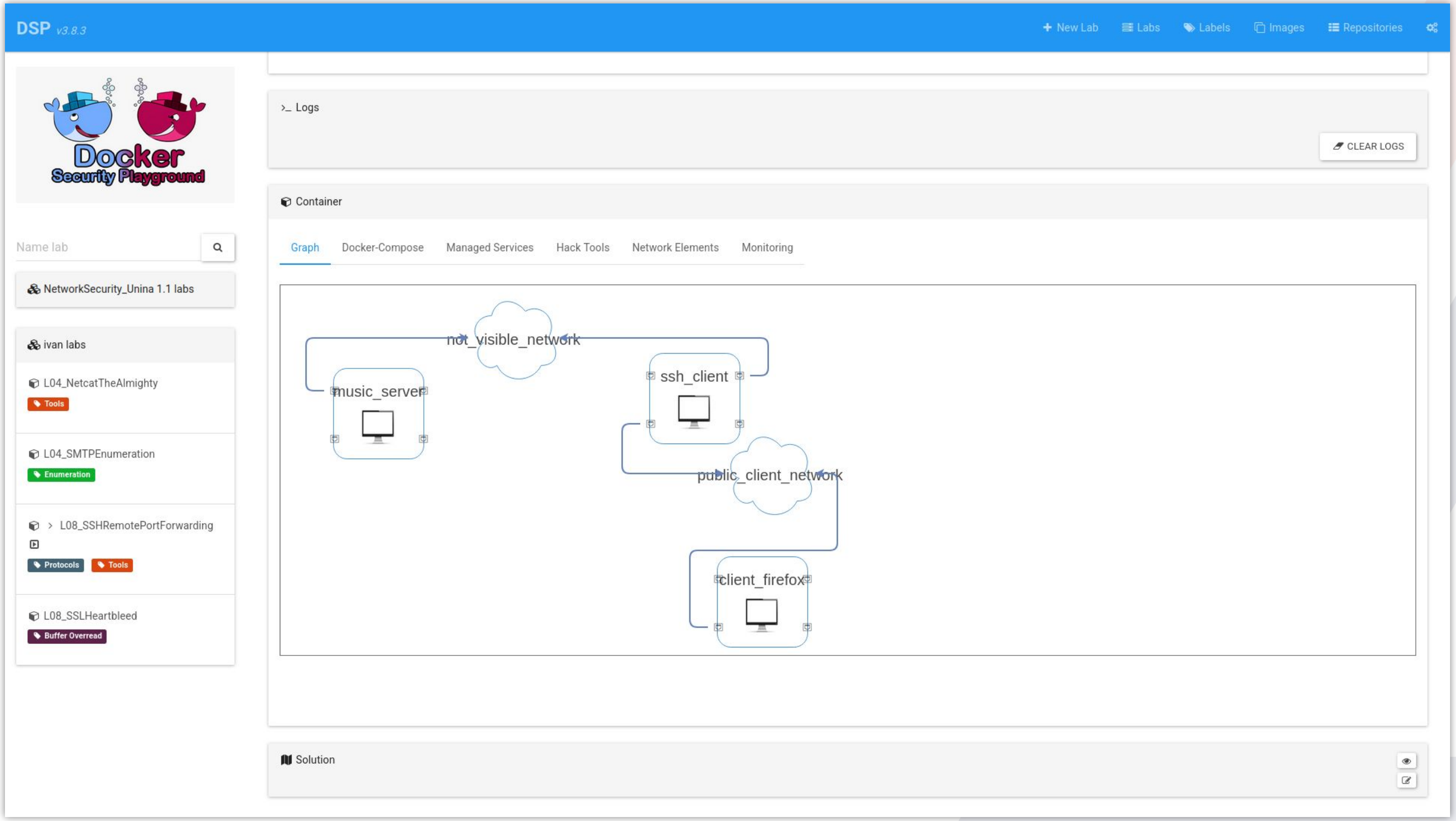
BlackHatLab_USA_2018
Blackhat

Bodgeit

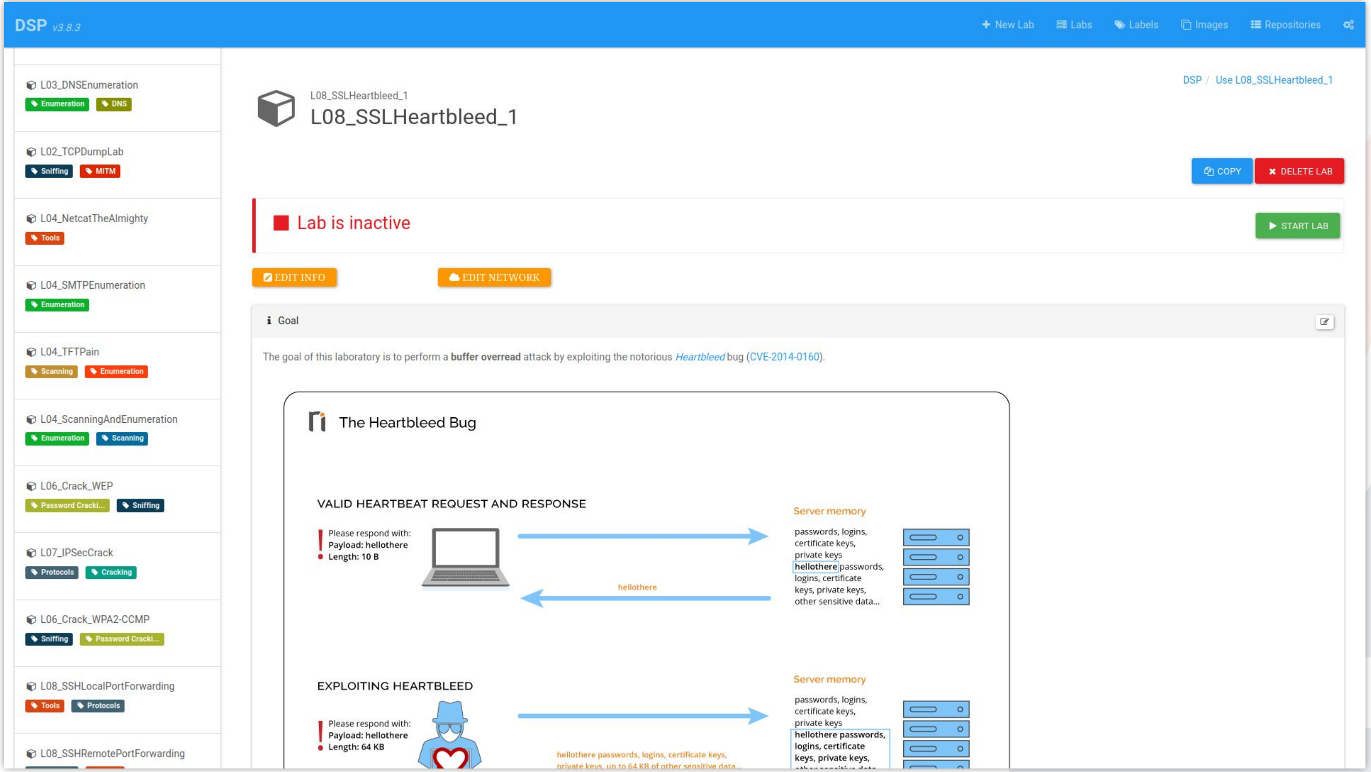
Bricks
WebHacking

Bypass The Firewall
Firewall

# Docker Security Playground (2)



# Docker Security Playground (3)



DSP v3.8.3

- L03_DNSEnumeration — Enumeration, DNS
- L02_TCPDumpLab — Sniffing, MITM
- L04_NetcatTheAlmighty — Tools
- L04_SMTPEnumeration — Enumeration
- L04_TFTPain — Scanning, Enumeration
- L04_ScanningAndEnumeration — Enumeration, Scanning
- L06_Crack_WEP — Password Cracki..., Sniffing
- L07_IPSecCrack — Protocols, Cracking
- L06_Crack_WPA2-CCMP — Sniffing, Password Cracki...
- L08_SSHLocalPortForwarding — Tools, Protocols
- L08_SSHRemotePortForwarding

DSP / Use L08_SSLHeartbleed_1

L08_SSLHeartbleed_1

## L08_SSLHeartbleed_1

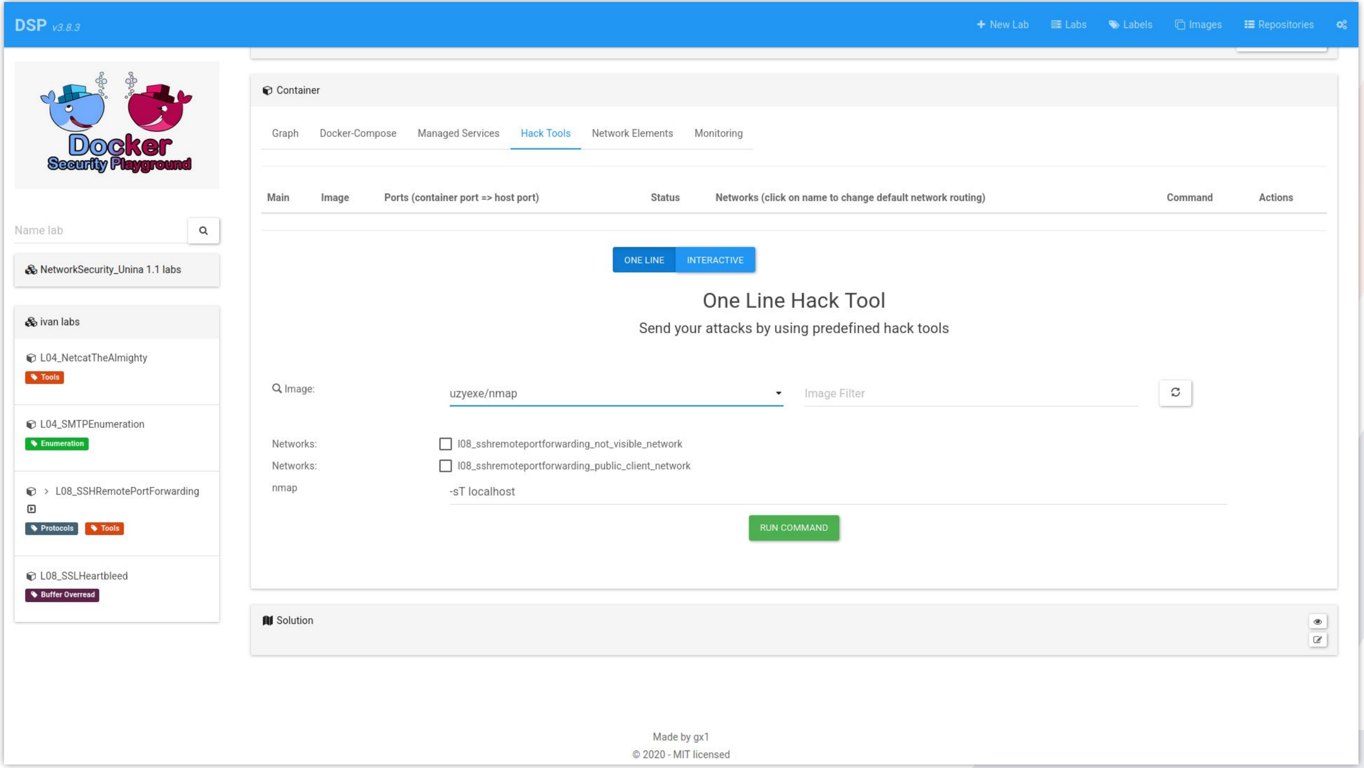
🟥 Lab is inactive

ℹ Goal

The goal of this laboratory is to perform a **buffer overread** attack by exploiting the notorious *Heartbleed* bug (CVE-2014-0160).

The Heartbleed Bug
VALID HEARTBEAT REQUEST AND RESPONSE
Please respond with:
Payload: hellothere
Length: 10 B
hellothere
Server memory
passwords, logins, certificate keys, private keys
hellothere passwords, logins, certificate keys, private keys, other sensitive data...
EXPLOITING HEARTBLEED
Please respond with:
Payload: hellothere
Length: 64 KB
hellothere passwords, logins, certificate keys, private keys, up to 64 KB of other sensitive data...
Server memory
passwords, logins, certificate keys, private keys
hellothere passwords, logins, certificate keys, private keys,

# Docker Security Playground (4)



DSP v3.8.3

Name lab

NetworkSecurity_Unina 1.1 labs

ivan labs

- L04_NetcatTheAlmighty — Tools
- L04_SMTPEnumeration — Enumeration
- L08_SSHRemotePortForwarding — Protocols, Tools
- L08_SSLHeartbleed — Buffer Overread

Container

| Main | Image | Ports (container port => host port) | Status | Networks (click on name to change default network routing) | Command | Actions |
|---|---|---|---|---|---|---|

One Line Hack Tool

Send your attacks by using predefined hack tools

Image: uzyexe/nmap

Image Filter

Networks: □ l08_sshremoteportforwarding_not_visible_network

Networks: □ l08_sshremoteportforwarding_public_client_network

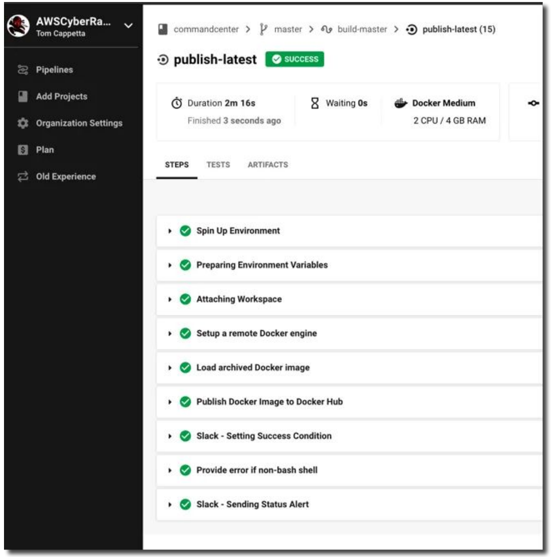
nmap -sT localhost

Solution

Made by gx1

© 2020 - MIT licensed

# AWS Cyber Range



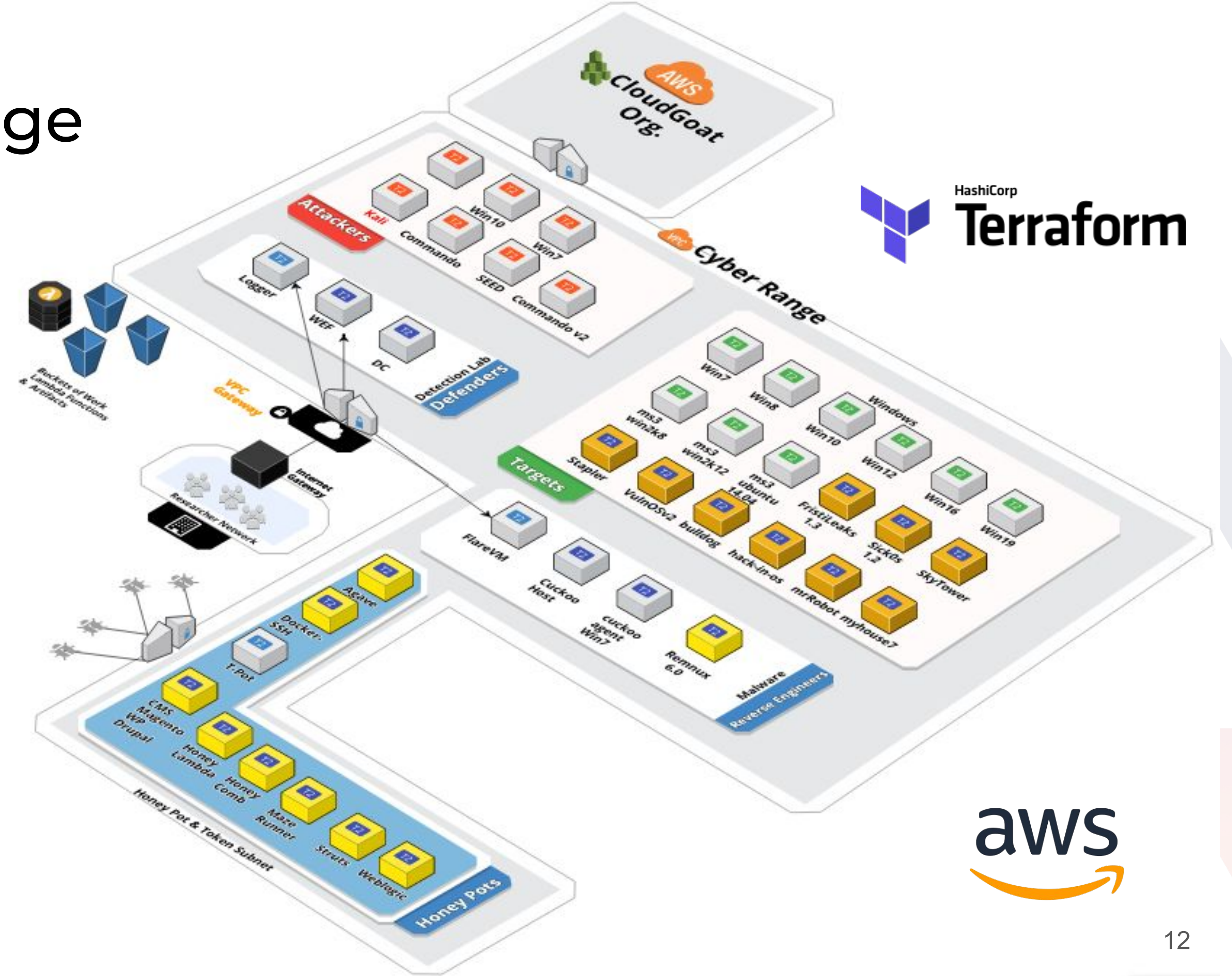
publish-latest SUCCESS

Duration 2m 16s
Finished 3 seconds ago

Waiting 0s

Docker Medium
2 CPU / 4 GB RAM

- Spin Up Environment
- Preparing Environment Variables
- Attaching Workspace
- Setup a remote Docker engine
- Load archived Docker image
- Publish Docker Image to Docker Hub
- Slack - Setting Success Condition
- Provide error if non-bash shell
- Slack - Sending Status Alert



HashiCorp Terraform

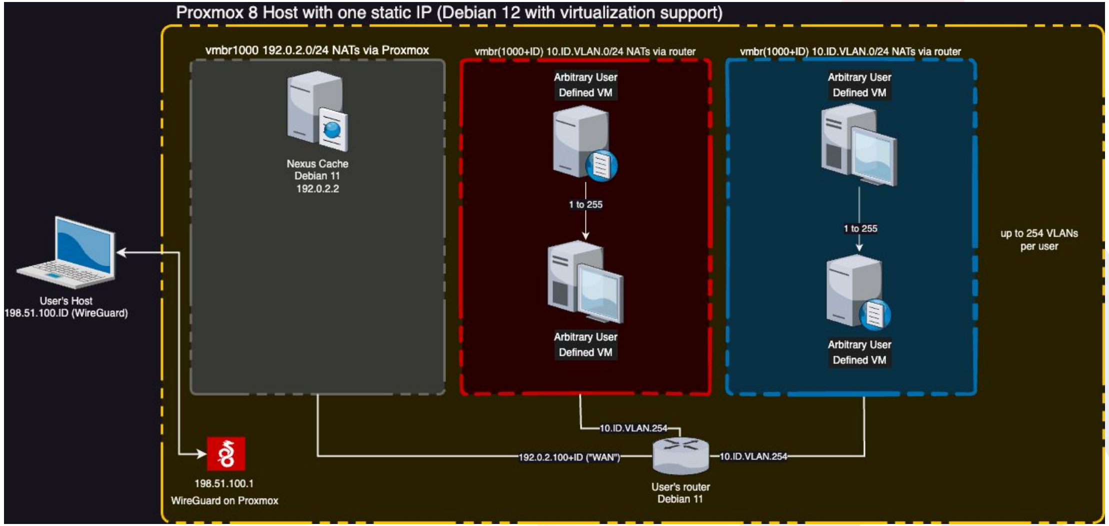
docker

aws

# Ludus (1)

```
user@ludus:~$ ludus templates list
+------------------------------------+--------+
|              TEMPLATE              | BUILT  |
+------------------------------------+--------+
| debian-11-x64-server-template      | FALSE  |
| debian-12-x64-server-template      | FALSE  |
| kali-x64-desktop-template          | FALSE  |
| win11-22h2-x64-enterprise-template | FALSE  |
| win2022-server-x64-template        | FALSE  |
+------------------------------------+--------+
```

```
user@ludus:~$ ludus range deploy
[INFO]  range deploy started
```

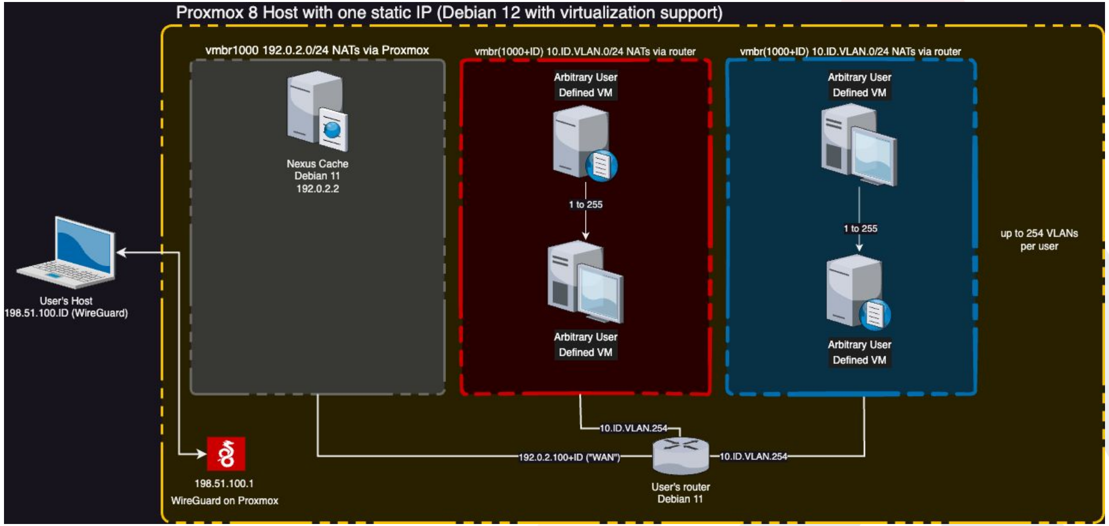


Proxmox 8 Host with one static IP (Debian 12 with virtualization support)
vmbr1000 192.0.2.0/24 NATs via Proxmox
vmbr(1000+ID) 10.ID.VLAN.0/24 NATs via router
vmbr(1000+ID) 10.ID.VLAN.0/24 NATs via router
Nexus Cache
Debian 11
192.0.2.2
Arbitrary User Defined VM
1 to 255
Arbitrary User Defined VM
Arbitrary User Defined VM
1 to 255
Arbitrary User Defined VM
up to 254 VLANs per user
User's Host
198.51.100.ID (WireGuard)
10.ID.VLAN.254
192.0.2.100+ID ("WAN")
10.ID.VLAN.254
198.51.100.1
WireGuard on Proxmox
User's router
Debian 11

```
user@ludus:~$ ludus range status
+---------+---------------+------------------+---------------+-------------------+-----------------+
| USER ID | RANGE NETWORK | LAST DEPLOYMENT  | NUMBER OF VMS | DEPLOYMENT STATUS | TESTING ENABLED |
+---------+---------------+------------------+---------------+-------------------+-----------------+
|   JD    |  10.2.0.0/16  | 2023-12-31 18:42 |       4       |      SUCCESS      |      FALSE      |
+---------+---------------+------------------+---------------+-------------------+-----------------+
+------------+------------------------------------+-------+-------------+
| PROXMOX ID |              VM NAME               | POWER |  IP         |
+------------+------------------------------------+-------+-------------+
|     107    | JD-router-debian11-x64             |  On   | 10.2.10.254 |
|     109    | JD-ad-dc-win2019-server-x64        |  On   | 10.2.10.11  |
|     113    | JD-ad-win11-22h2-enterprise-x64-1  |  On   | 10.2.10.21  |
|     114    | JD-kali                            |  On   | 10.2.99.1   |
+------------+------------------------------------+-------+-------------+
```

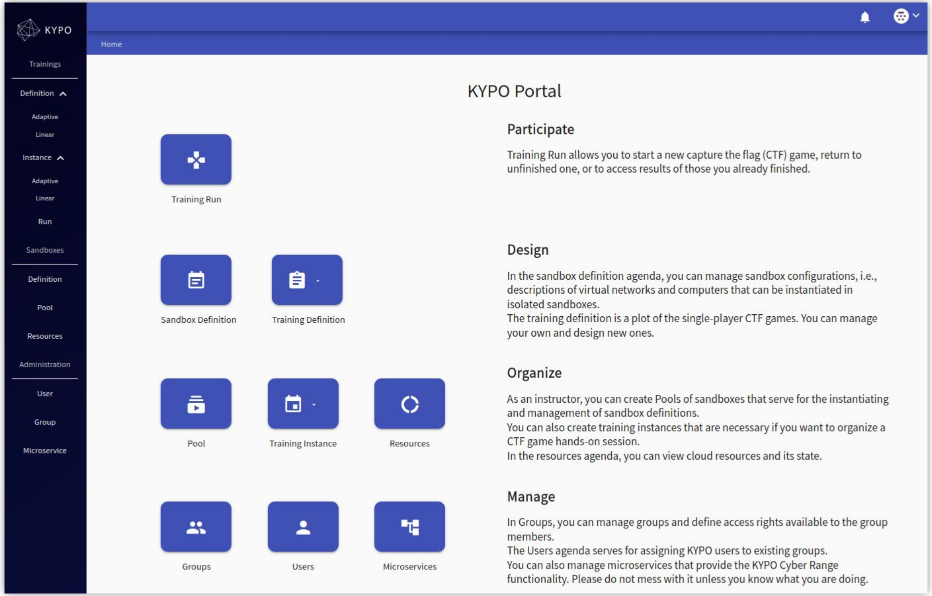
# Ludus (2)

```
ludus:
  - vm_name: "{{ range_id }}-DC01"
    hostname: "DC01"
    template: win2022-server-x64-template
    vlan: 10
    ip_last_octet: 10
    ram_gb: 4
    ram_min_gb: 1
    cpus: 2
    windows:
      sysprep: true
    domain:
      fqdn: ludus.domain
      role: primary-dc
    roles:
      - synzack.ludus_sccm.install_adcs
      - synzack.ludus_sccm.disable_firewall

  - vm_name: "{{ range_id }}-Workstation"
    hostname: "Workstation"
    template: win11-22h2-x64-enterprise-template
    vlan: 10
    ip_last_octet: 11
    ram_gb: 4
    ram_min_gb: 1
    cpus: 4
```


Proxmox 8 Host with one static IP (Debian 12 with virtualization support)
vmbr1000 192.0.2.0/24 NATs via Proxmox
vmbr(1000+ID) 10.ID.VLAN.0/24 NATs via router
vmbr(1000+ID) 10.ID.VLAN.0/24 NATs via router
Nexus Cache
Debian 11
192.0.2.2
Arbitrary User Defined VM
1 to 255
Arbitrary User Defined VM
Arbitrary User Defined VM
1 to 255
Arbitrary User Defined VM
up to 254 VLANs per user
User's Host
198.51.100.ID (WireGuard)
198.51.100.1
WireGuard on Proxmox
10.ID.VLAN.254
192.0.2.100+ID ("WAN")
10.ID.VLAN.254
User's router
Debian 11

*Example from:
https://github.com/Synzack/ludus_sccm

# KYPO Cyber Range Platform (1)



## KYPO Portal

### Participate

Training Run allows you to start a new capture the flag (CTF) game, return to unfinished one, or to access results of those you already finished.

### Design

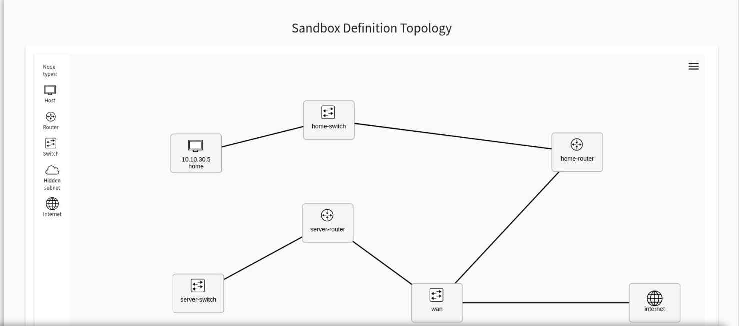
In the sandbox definition agenda, you can manage sandbox configurations, i.e., descriptions of virtual networks and computers that can be instantiated in isolated sandboxes.
The training definition is a plot of the single-player CTF games. You can manage your own and design new ones.

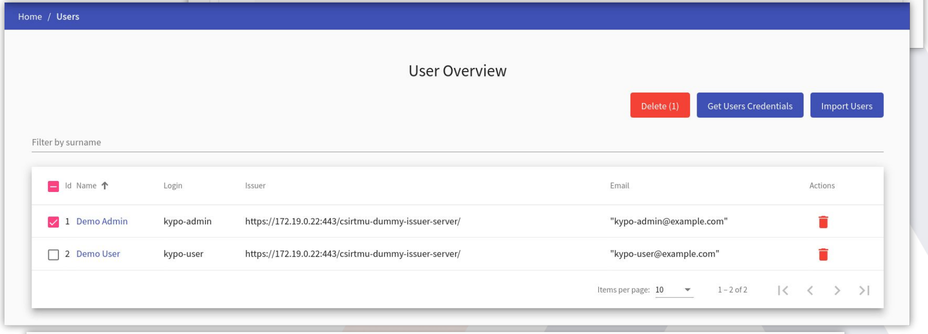
### Organize

As an instructor, you can create Pools of sandboxes that serve for the instantiating and management of sandbox definitions.
You can also create training instances that are necessary if you want to organize a CTF game hands-on session.
In the resources agenda, you can view cloud resources and its state.

### Manage

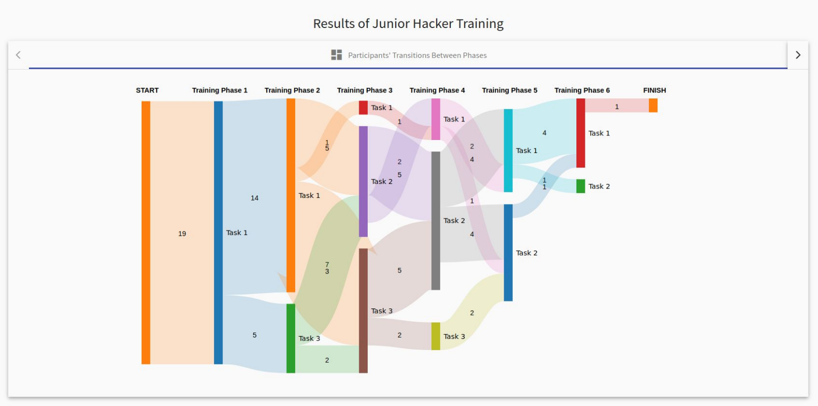
In Groups, you can manage groups and define access rights available to the group members.
The Users agenda serves for assigning KYPO users to existing groups.
You can also manage microservices that provide the KYPO Cyber Range functionality. Please do not mess with it unless you know what you are doing.


Sandbox Definition Topology



User Overview

| | Id | Name | Login | Issuer | Email | Actions |
|---|---|---|---|---|---|---|
| ☑ | 1 | Demo Admin | kypo-admin | https://172.19.0.22:443/csirtmu-dummy-issuer-server/ | "kypo-admin@example.com" | 🗑 |
| □ | 2 | Demo User | kypo-user | https://172.19.0.22:443/csirtmu-dummy-issuer-server/ | "kypo-user@example.com" | 🗑 |


Results of Junior Hacker Training

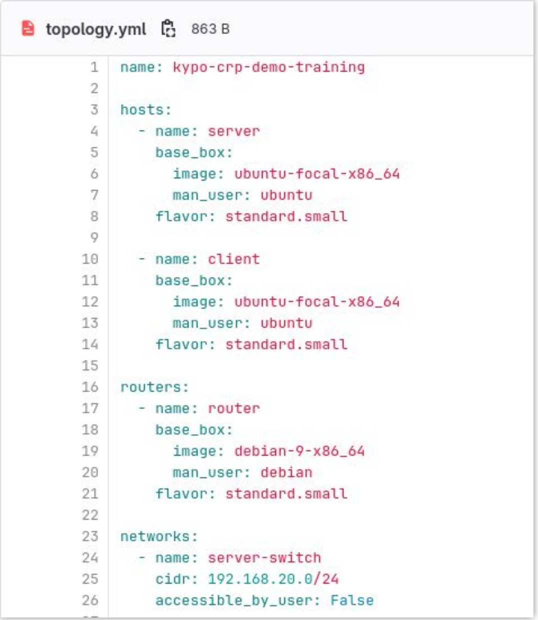
HashiCorp Terraform

OpenTofu

ANSIBLE

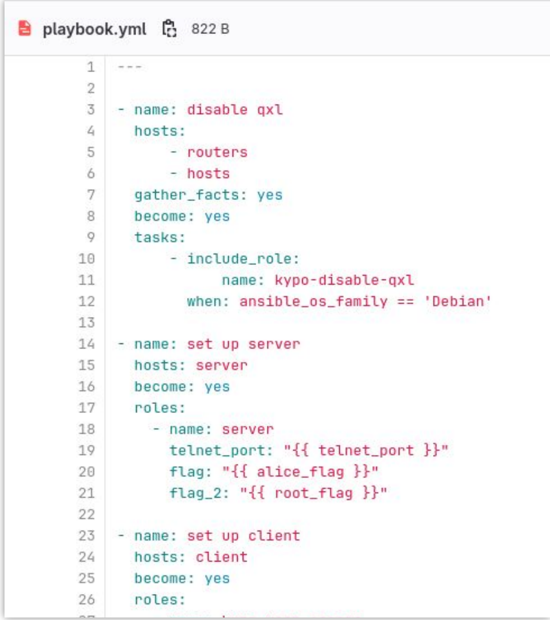
# KYPO Cyber Range Platform (2)

git



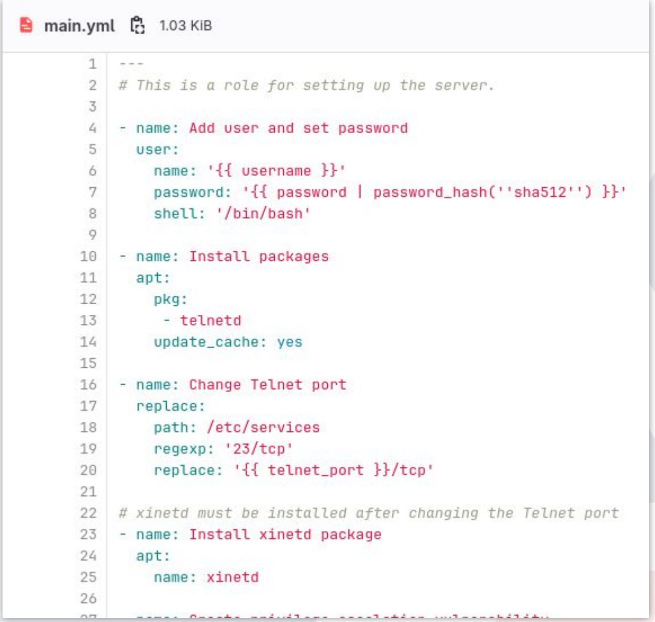
topology.yml 863 B

```yaml
name: kypo-crp-demo-training

hosts:
  - name: server
    base_box:
      image: ubuntu-focal-x86_64
      man_user: ubuntu
    flavor: standard.small

  - name: client
    base_box:
      image: ubuntu-focal-x86_64
      man_user: ubuntu
    flavor: standard.small

routers:
  - name: router
    base_box:
      image: debian-9-x86_64
      man_user: debian
    flavor: standard.small

networks:
  - name: server-switch
    cidr: 192.168.20.0/24
    accessible_by_user: False
```



playbook.yml 822 B

```yaml
---

- name: disable qxl
  hosts:
      - routers
      - hosts
  gather_facts: yes
  become: yes
  tasks:
      - include_role:
            name: kypo-disable-qxl
        when: ansible_os_family == 'Debian'

- name: set up server
  hosts: server
  become: yes
  roles:
    - name: server
      telnet_port: "{{ telnet_port }}"
      flag: "{{ alice_flag }}"
      flag_2: "{{ root_flag }}"

- name: set up client
  hosts: client
  become: yes
  roles:
```



main.yml 1.03 KiB

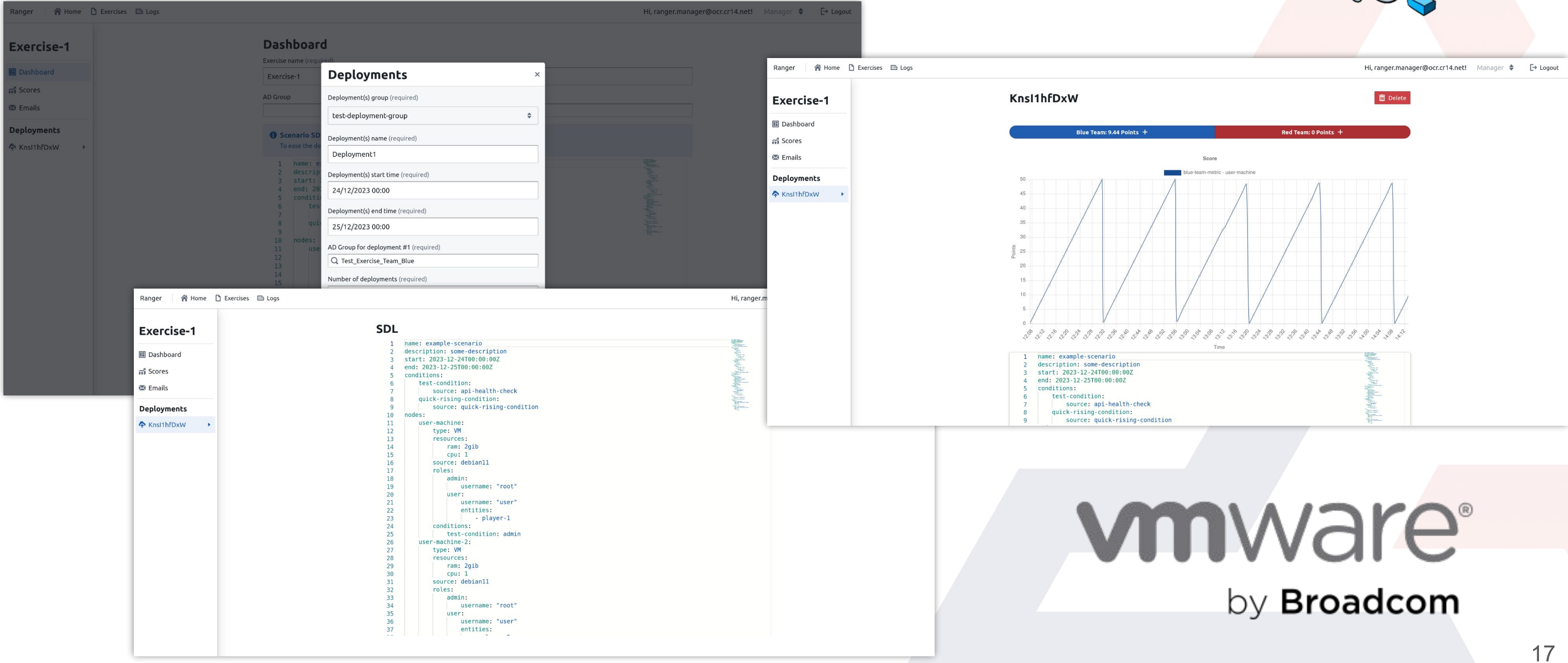
```yaml
---
# This is a role for setting up the server.

- name: Add user and set password
  user:
    name: '{{ username }}'
    password: '{{ password | password_hash(''sha512'') }}'
    shell: '/bin/bash'

- name: Install packages
  apt:
    pkg:
      - telnetd
    update_cache: yes

- name: Change Telnet port
  replace:
    path: /etc/services
    regexp: '23/tcp'
    replace: '{{ telnet_port }}/tcp'

# xinetd must be installed after changing the Telnet port
- name: Install xinetd package
  apt:
    name: xinetd

- name: Create privilege escalation vulnerability
```

HashiCorp Terraform

OpenTofu

ANSIBLE

# Open Cyber Range



Ranger | Home | Exercises | Logs | Hi, ranger.manager@ocr.cr14.net! | Manager | Logout

**Exercise-1**

- Dashboard
- Scores
- Emails

**Deployments**

- Knsl1hfDxW

## Dashboard

Exercise name (required)

Exercise-1

AD Group

Scenario SD

To ease the de

```
name: e
descrip
start: 
end: 20
conditi
    tes

    qui

nodes:
    use
```

### Deployments

×

Deployment(s) group (required)

test-deployment-group

Deployment(s) name (required)

Deployment1

Deployment(s) start time (required)

24/12/2023 00:00

Deployment(s) end time (required)

25/12/2023 00:00

AD Group for deployment #1 (required)

Test_Exercise_Team_Blue

Number of deployments (required)

Ranger | Home | Exercises | Logs | Hi, ranger.m

**Exercise-1**

- Dashboard
- Scores
- Emails

**Deployments**

- Knsl1hfDxW

## SDL

```
name: example-scenario
description: some-description
start: 2023-12-24T00:00:00Z
end: 2023-12-25T00:00:00Z
conditions:
    test-condition:
        source: api-health-check
    quick-rising-condition:
        source: quick-rising-condition
nodes:
    user-machine:
        type: VM
        resources:
            ram: 2gib
            cpu: 1
        source: debian11
        roles:
            admin:
                username: "root"
            user:
                username: "user"
                entities:
                    - player-1
        conditions:
            test-condition: admin
    user-machine-2:
        type: VM
        resources:
            ram: 2gib
            cpu: 1
        source: debian11
        roles:
            admin:
                username: "root"
            user:
                username: "user"
                entities:
```

Ranger | Home | Exercises | Logs | Hi, ranger.manager@ocr.cr14.net! | Manager | Logout

**Exercise-1**

- Dashboard
- Scores
- Emails

**Deployments**

- Knsl1hfDxW

## Knsl1hfDxW

Delete

Blue Team: 9.44 Points + | Red Team: 0 Points +

```
name: example-scenario
description: some-description
start: 2023-12-24T00:00:00Z
end: 2023-12-25T00:00:00Z
conditions:
    test-condition:
        source: api-health-check
    quick-rising-condition:
        source: quick-rising-condition
```

# DETER/DeterLab

- Based on university simulator Emulab
- Runs over hundreds of physical machines
- Used for large–scale experiments and team exercises
- Global and federated usage
- Deter Agents Simulating Humans (DASH) toolkit

# Demo…

- KYPO CRP
- Docker Security Playground

# Conclusions

- Small scale CRs (e.g. DSP, AWS CR) make sense for smaller teams
- Bigger CRs require a larger infrastructure and specialized operators
- Features such as user and attack simulation are available only with larger CRs and come with a significant overhead
- Team exercise support varies a lot, many CRs primarily focus on individuals
- Creating new trainings is challenging and time-consuming

# Q&A

Contact: ivan.kovacevic@cyberarrange.com

Alternatively, feel free to send a message on LinkedIn