Build Your Own Cybersecurity Lab and Cyber Range

Omar Santos
@santosomar

H4cker
H4CKER.ORG

About // Omar Ωr Santos

https://h4cker.org

@santosomar

https://h4cker.org/discord

/in/santosomar

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of over 20 books and video courses; numerous white papers, articles, and security configuration guidelines and best practices. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar is often presenting at many cybersecurity conferences and he is the co-lead of the DEF CON Red Team Village (redteamvillage.io). He is also the chair of the OASIS Common Security Vulnerability Framework (CSAF) Technical Committee and the co-chair of the Forum of Incident Response and Security Teams (FIRST) PSIRT Open Source Security Working Group.

Omar has been quoted by numerous media outlets, such as TheRegister, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune Magazine, Ars Technica, and more.

Omar's PGP Key: 0x8e19a9d13af27edc

AGENDA

- Creating a virtual networking lab with Virtual Box, VMWare Workstation/Fusion, ESXi, or Proxmox
- Overview of Advanced Deployments
- Using Linux Kernel modules to build a wireless hacking lab without the need of physical adapters
- Building your lab in cloud environments (AWS, Azure, Google Cloud, and Digital Ocean)
- Automating lab deployment with Vagrant and Ansible
- Creating sandboxes for malware analysis
- Introduction to "Cyber Ranges"
- Using Docker to practice your offensive and defensive security skills
- Lab scenarios for ethical hacking certifications such as CEH practical, PenTest+, OSCP, and others

H4cker

H4CKER.ORG

Pre-Requisites

The only pre-requisite for this class is to have some background in computing, virtualization, and networking.

ADDITIONAL NOTES ABOUT THIS TRAINING

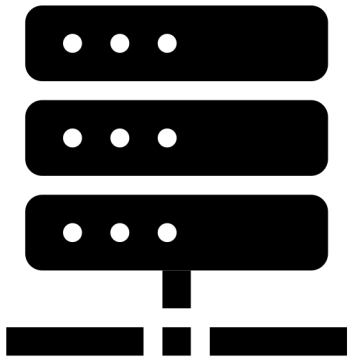
This webinar / live training course is mostly led by demonstrations and Q&A.

You will have the opportunity to ask questions via the Q&A panel. Some of the exercises/demonstrations will take some time to setup in your environment and they must be completed at your own time.

Several of the environments will require dedicated hardware (PC, server, laptops, etc.)

RESOURCES FOR THIS CLASS IN GITHUB

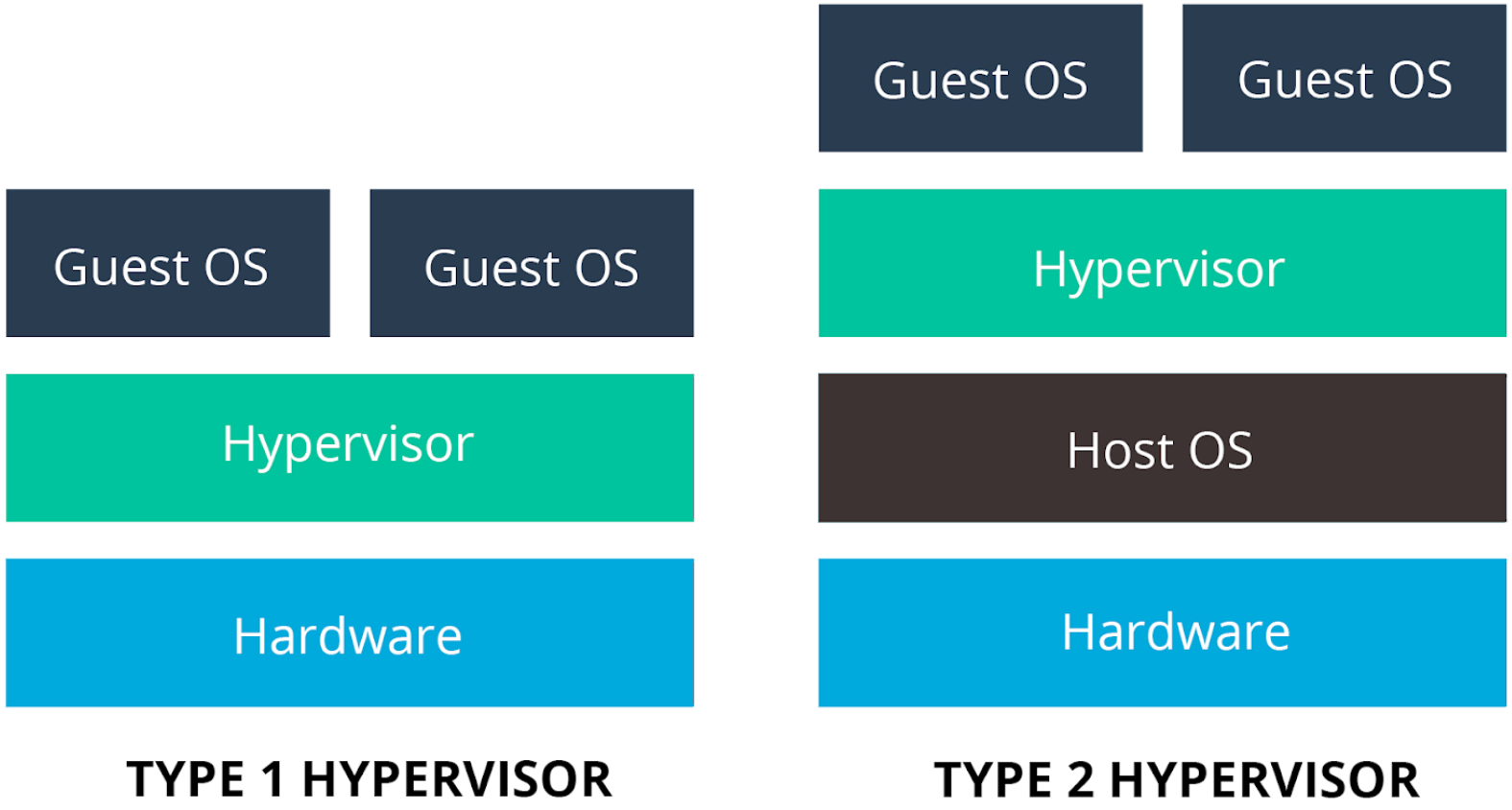
https://h4cker.org/github



CREATING A VIRTUAL NETWORKING LAB WITH VIRTUAL BOX, VMWARE WORKSTATION/FUSION, ESXI, OR PROXMOX

H4cker

H4CKER.ORG


Guest OS
Guest OS
Hypervisor
Hardware
TYPE 1 HYPERVISOR
Guest OS
Guest OS
Hypervisor
Host OS
Hardware
TYPE 2 HYPERVISOR

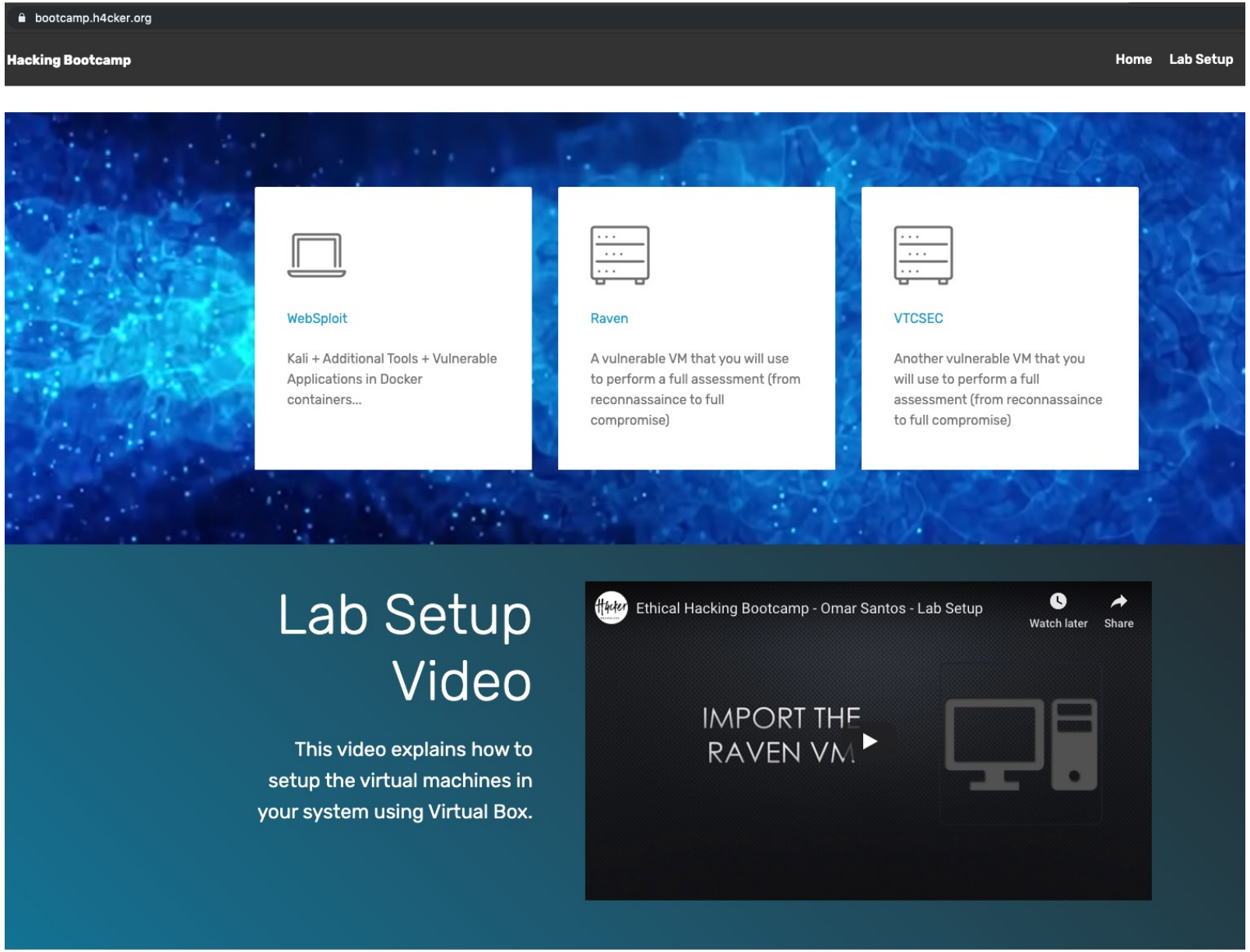
WHAT IS VIRTUAL BOX?

- Free Virtualization Hypervisor Maintained by Oracle.
- Download: https://www.virtualbox.org
- Latest Documentation as a PDF book: http://download.virtualbox.org/virtualbox/UserManual.pdf

H4cker
H4CKER.ORG

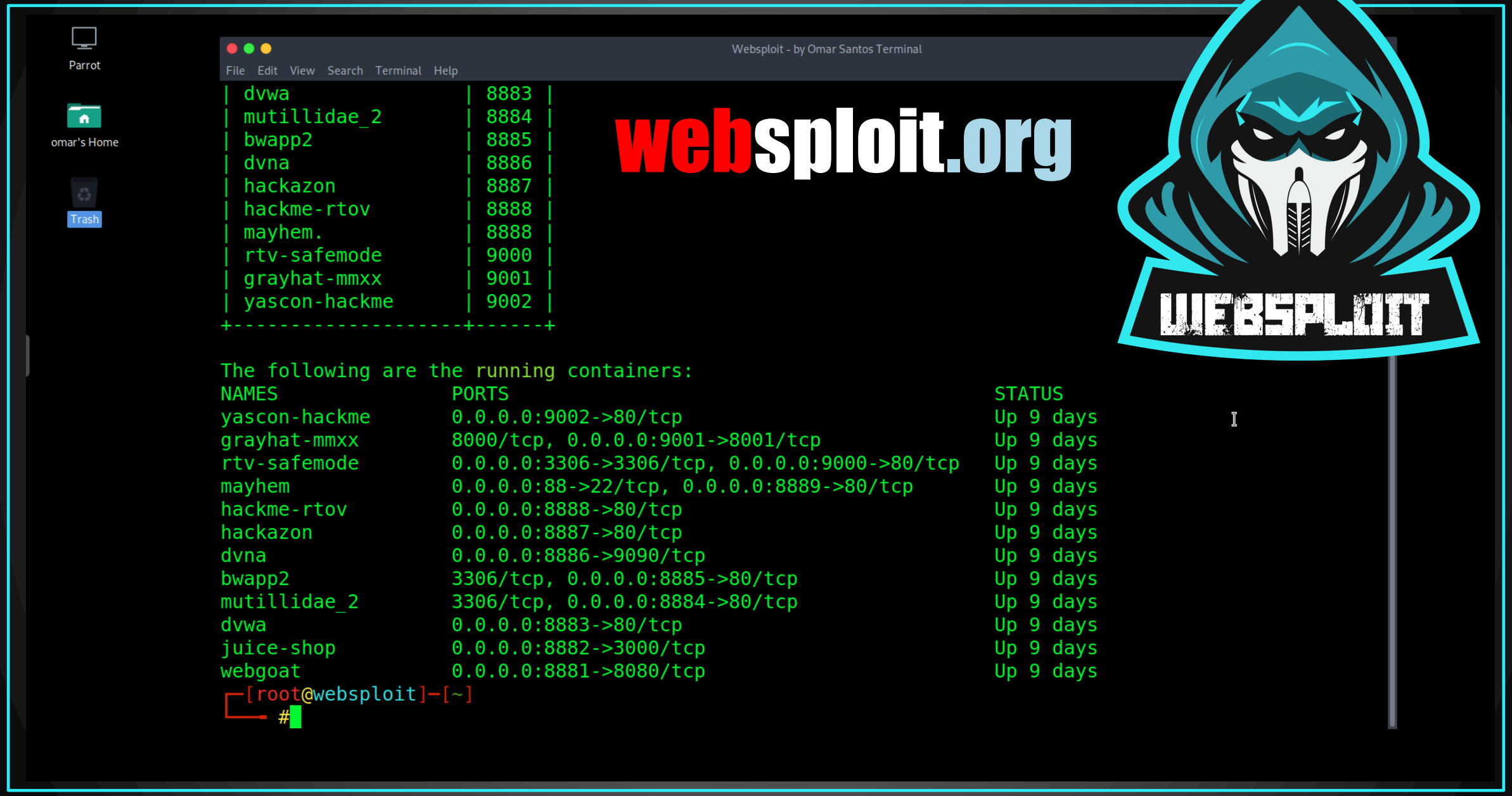
LINUX DISTRIBUTIONS FOR ETHICAL HACKING AND CYBER DEFENSE

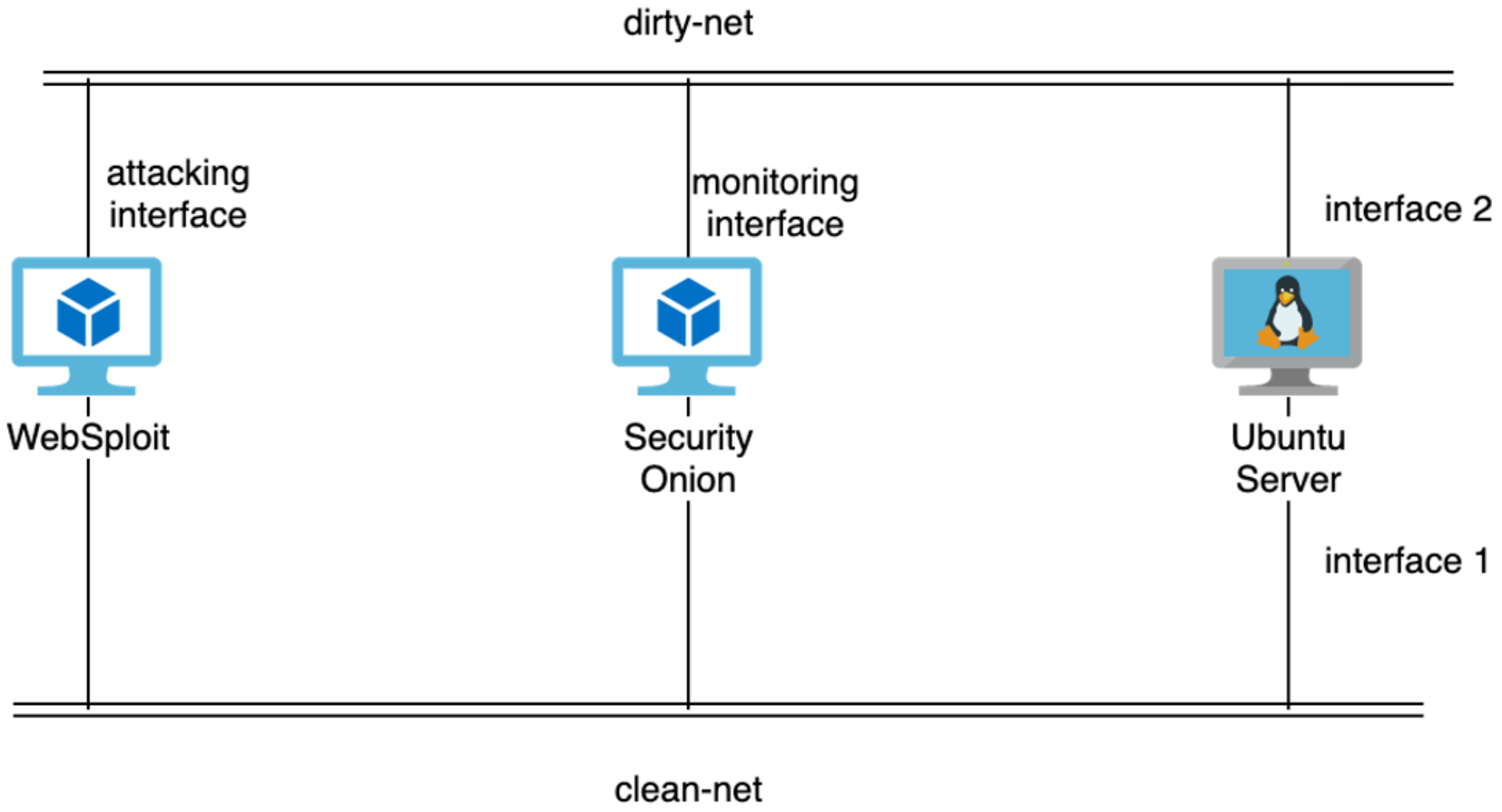
- Kali Linux (offensive and purple teams)
- Parrot OS
- BlackArch Linux
- The PenTesters Framework (PTF)
- PwnMachine by YesWeHack
- Security Onion



EXAMPLE OF A LAB ENVIRONMENT IN VIRTUAL BOX

H4cker
H4CKER.ORG


Parrot
omar's Home
Trash
Websploit - by Omar Santos Terminal
File Edit View Search Terminal Help
dvwa	8883
mutillidae_2	8884
bwapp2	8885
dvna	8886
hackazon	8887
hackme-rtov	8888
mayhem.	8888
rtv-safemode	9000
grayhat-mmxx	9001
yascon-hackme	9002
+---+---+
The following are the running containers:
NAMES PORTS STATUS
yascon-hackme 0.0.0.0:9002->80/tcp Up 9 days
grayhat-mmxx 8000/tcp, 0.0.0.0:9001->8001/tcp Up 9 days
rtv-safemode 0.0.0.0:3306->3306/tcp, 0.0.0.0:9000->80/tcp Up 9 days
mayhem 0.0.0.0:88->22/tcp, 0.0.0.0:8889->80/tcp Up 9 days
hackme-rtov 0.0.0.0:8888->80/tcp Up 9 days
hackazon 0.0.0.0:8887->80/tcp Up 9 days
dvna 0.0.0.0:8886->9090/tcp Up 9 days
bwapp2 3306/tcp, 0.0.0.0:8885->80/tcp Up 9 days
mutillidae_2 3306/tcp, 0.0.0.0:8884->80/tcp Up 9 days
dvwa 0.0.0.0:8883->80/tcp Up 9 days
juice-shop 0.0.0.0:8882->3000/tcp Up 9 days
webgoat 0.0.0.0:8881->8080/tcp Up 9 days
[root@websploit]-[~]
#
websploit.org
WEBSPLOIT



Example Lab Topology with VMs in a Single Node

VIRTUAL BOX DEMO

AND Q&A

H4cker

H4CKER.ORG

VIRTUAL BOX API

VirtualBox Main API which comprises all public COM interfaces and components provided by the VirtualBox server and by the VirtualBox client library.
https://www.virtualbox.org/sdkref/index.html

Personal Desktop

Run multiple operating systems on a single PC or Mac.

Fusion for Mac

Application for running multiple operating systems on Mac

Workstation Player

Simple tool for running a second OS on your Windows or Linux PC, free for personal use

Workstation Pro

Application for running multiple operating systems on Windows and Linux

VMWARE

DEMO OF VMWARE FUSION

H4cker

H4CKER.ORG

PRIVATE NETWORKS?

- Should you expose the VMs to the rest of the network?
- What about NAT configurations?
- What firewalls should I deploy? Can I even deploy firewalls?
- What about IP Tables?
- Can you use jump hosts?

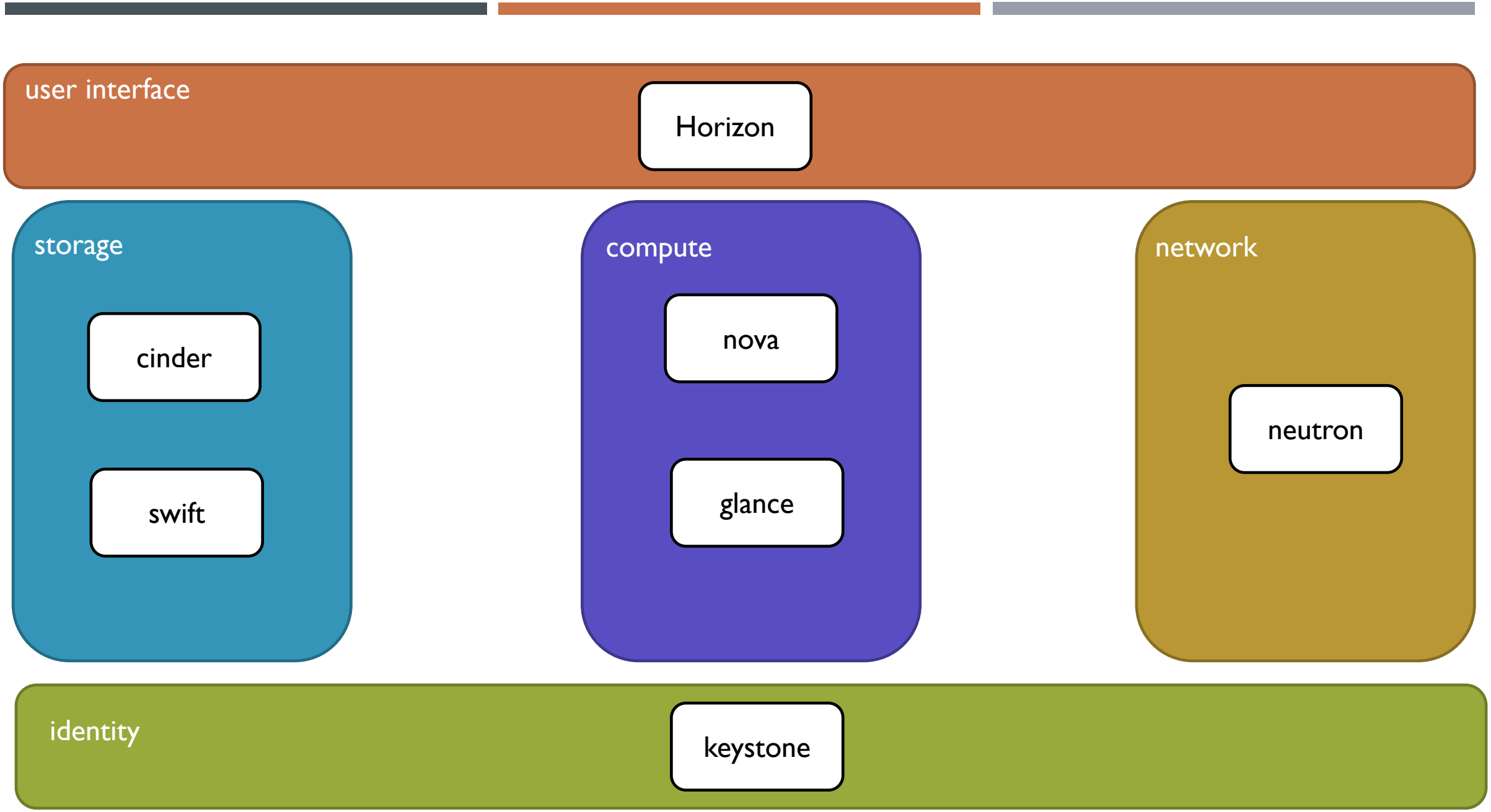
ADVANCED ENVIRONMENTS

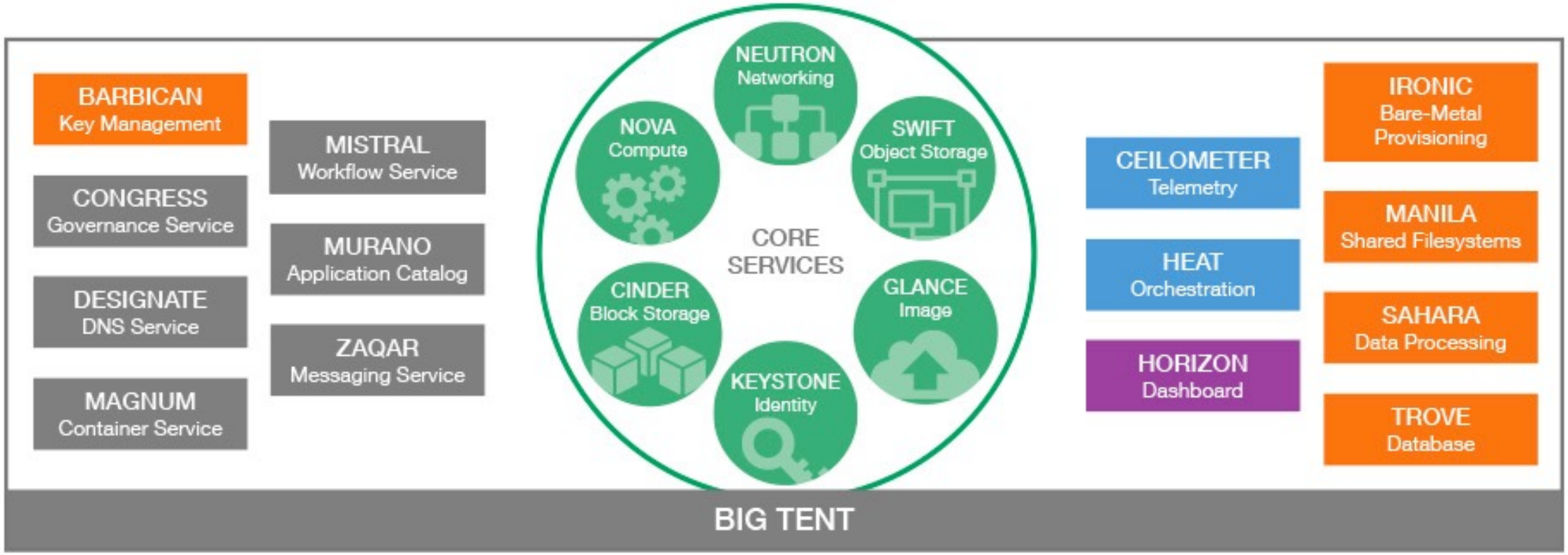
H4cker

H4CKER.ORG

BUILD YOUR OWN CLOUD?

HTTPS://WWW.OPENSTACK.ORG/


user interface
Horizon
storage
cinder
swift
compute
nova
glance
network
neutron
identity
keystone


BARBICAN
Key Management
CONGRESS
Governance Service
DESIGNATE
DNS Service
MAGNUM
Container Service
MISTRAL
Workflow Service
MURANO
Application Catalog
ZAQAR
Messaging Service
NEUTRON
Networking
NOVA
Compute
SWIFT
Object Storage
CORE
SERVICES
CINDER
Block Storage
GLANCE
Image
KEYSTONE
Identity
CEILOMETER
Telemetry
HEAT
Orchestration
HORIZON
Dashboard
IRONIC
Bare-Metal
Provisioning
MANILA
Shared Filesystems
SAHARA
Data Processing
TROVE
Database
BIG TENT

OpenStack Services

An OpenStack deployment contains a number of components providing APIs to access infrastructure resources. This page lists the various services that can be deployed to provide such resources to cloud end users.

https://www.openstack.org/software/project-navigator/openstack-components#openstack-services

Deployment Tools

Tools and packaging recipes to help install and maintain the lifecycle of OpenStack deployments.

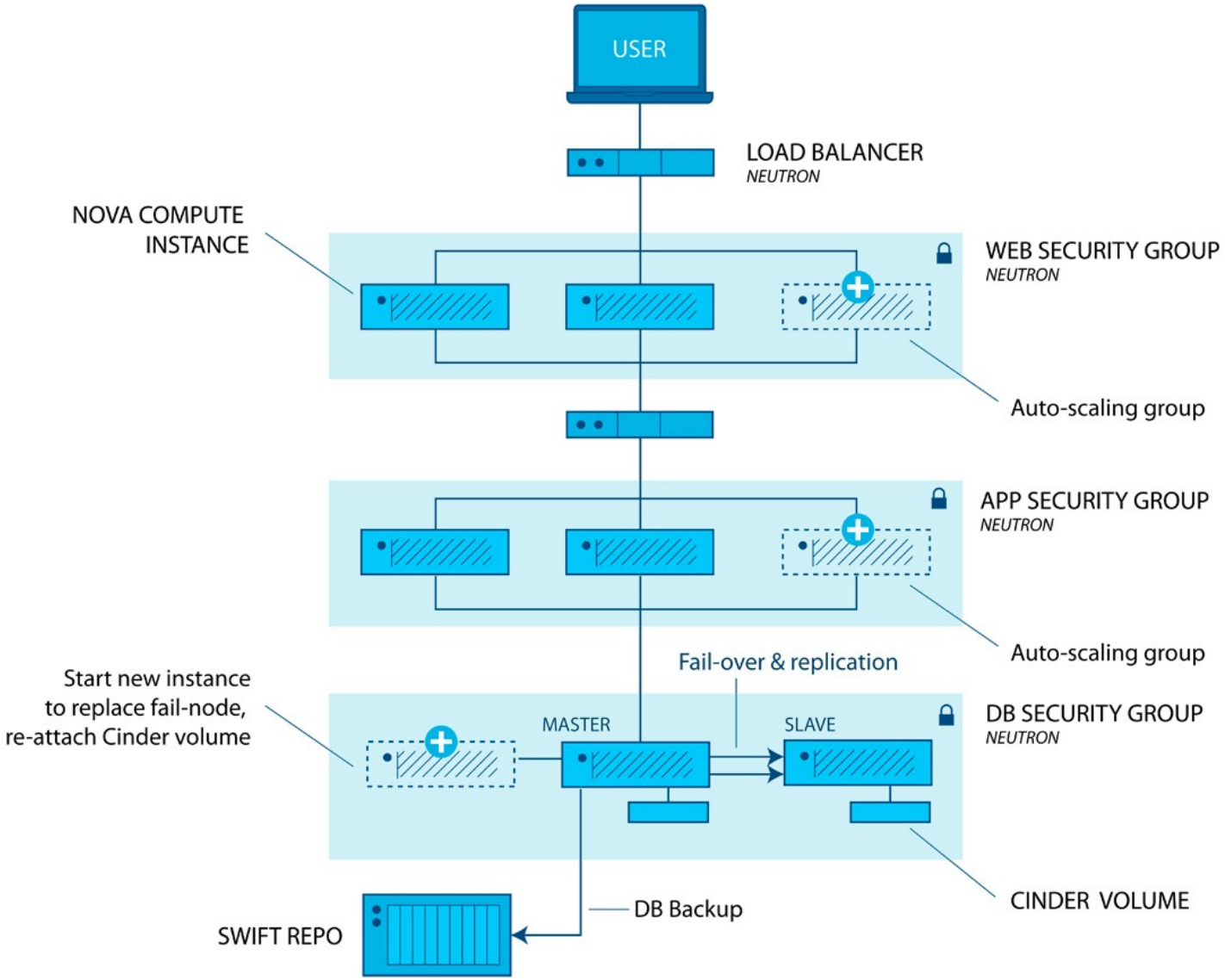
Frameworks for lifecycle management

	**TRIPLEO**	Deploys OpenStack using OpenStack itself
	**OPENSTACK-HELM**	Deploys OpenStack in containers using Helm
	**KOLLA-ANSIBLE**	Deploys OpenStack in containers using Ansible
	**OPENSTACK-ANSIBLE**	Ansible playbooks to deploy OpenStack
	**OPENSTACK-CHARMS**	Deploys OpenStack in containers using Charms and Juju
	BIFROST	Ansible playbooks using ironic
	**OPENSTACK-CHEF**	Chef cookbooks to build, operate and consume OpenStack

Packaging recipes for popular frameworks

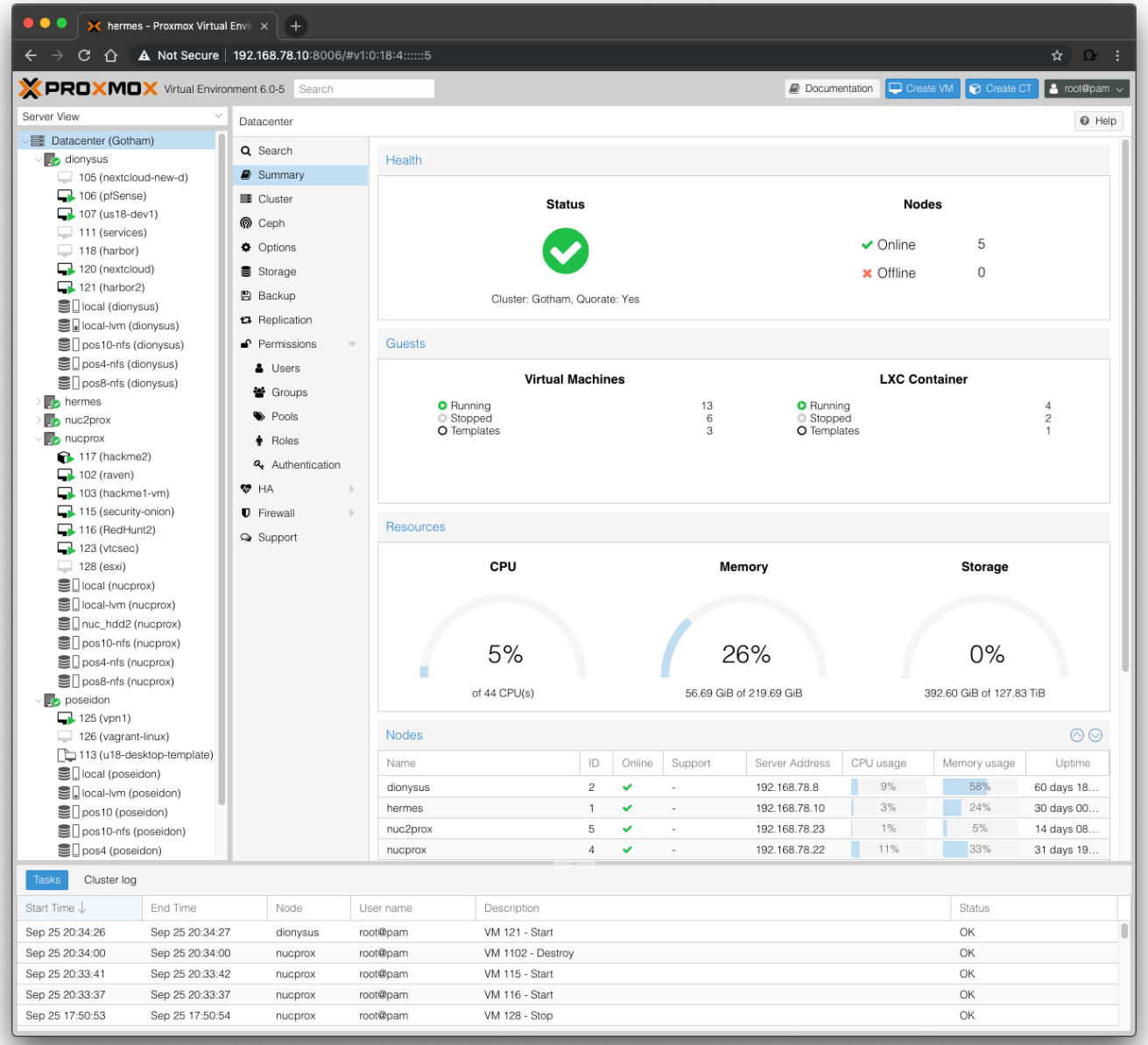
	LOCI	Lightweight OCI containers
	**PUPPET-OPENSTACK**	Puppet modules to deploy OpenStack
	**RPM-PACKAGING**	RPM package specs to deploy OpenStack

https://www.openstack.org/software/project-navigator/deployment-tools


USER
LOAD BALANCER
NEUTRON
NOVA COMPUTE INSTANCE
WEB SECURITY GROUP
NEUTRON
Auto-scaling group
APP SECURITY GROUP
NEUTRON
Auto-scaling group
Fail-over & replication
Start new instance to replace fail-node, re-attach Cinder volume
MASTER
SLAVE
DB SECURITY GROUP
NEUTRON
CINDER VOLUME
DB Backup
SWIFT REPO

PROXMOX

HTTPS://WWW.PROXMOX.COM



PROXMOX

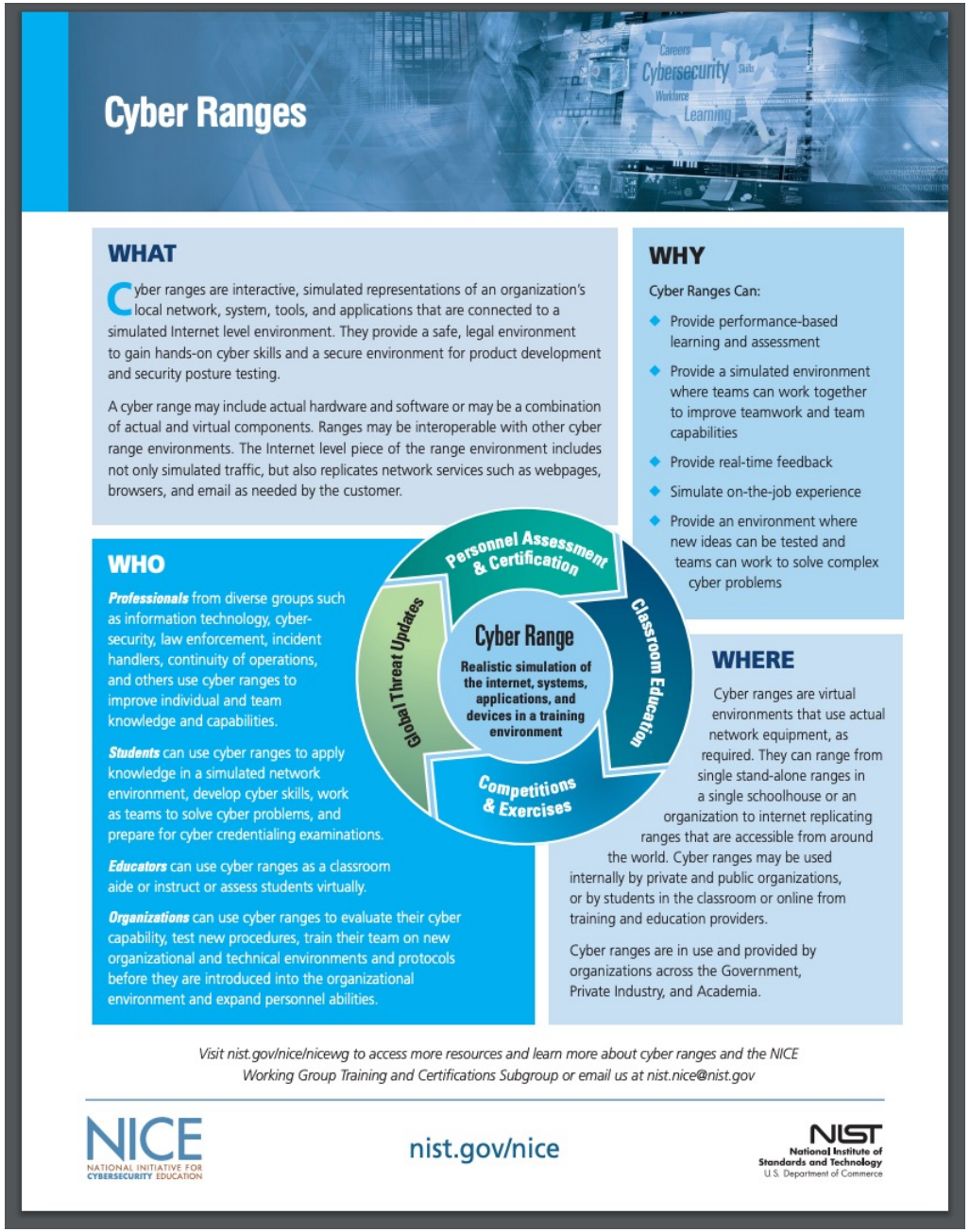
IN-DEPTH DEMO

H4cker

H4CKER.ORG

INTRODUCTION TO CYBER RANGES

WHAT IS A CYBER RANGE?



Cyber Ranges

WHAT

Cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing.

A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.

WHY

Cyber Ranges Can:

- Provide performance-based learning and assessment
- Provide a simulated environment where teams can work together to improve teamwork and team capabilities
- Provide real-time feedback
- Simulate on-the-job experience
- Provide an environment where new ideas can be tested and teams can work to solve complex cyber problems

WHO

Professionals from diverse groups such as information technology, cyber-security, law enforcement, incident handlers, continuity of operations, and others use cyber ranges to improve individual and team knowledge and capabilities.

Students can use cyber ranges to apply knowledge in a simulated network environment, develop cyber skills, work as teams to solve cyber problems, and prepare for cyber credentialing examinations.

Educators can use cyber ranges as a classroom aide or instruct or assess students virtually.

Organizations can use cyber ranges to evaluate their cyber capability, test new procedures, train their team on new organizational and technical environments and protocols before they are introduced into the organizational environment and expand personnel abilities.

WHERE

Cyber ranges are virtual environments that use actual network equipment, as required. They can range from single stand-alone ranges in a single schoolhouse or an organization to internet replicating ranges that are accessible from around the world. Cyber ranges may be used internally by private and public organizations, or by students in the classroom or online from training and education providers.

Cyber ranges are in use and provided by organizations across the Government, Private Industry, and Academia.

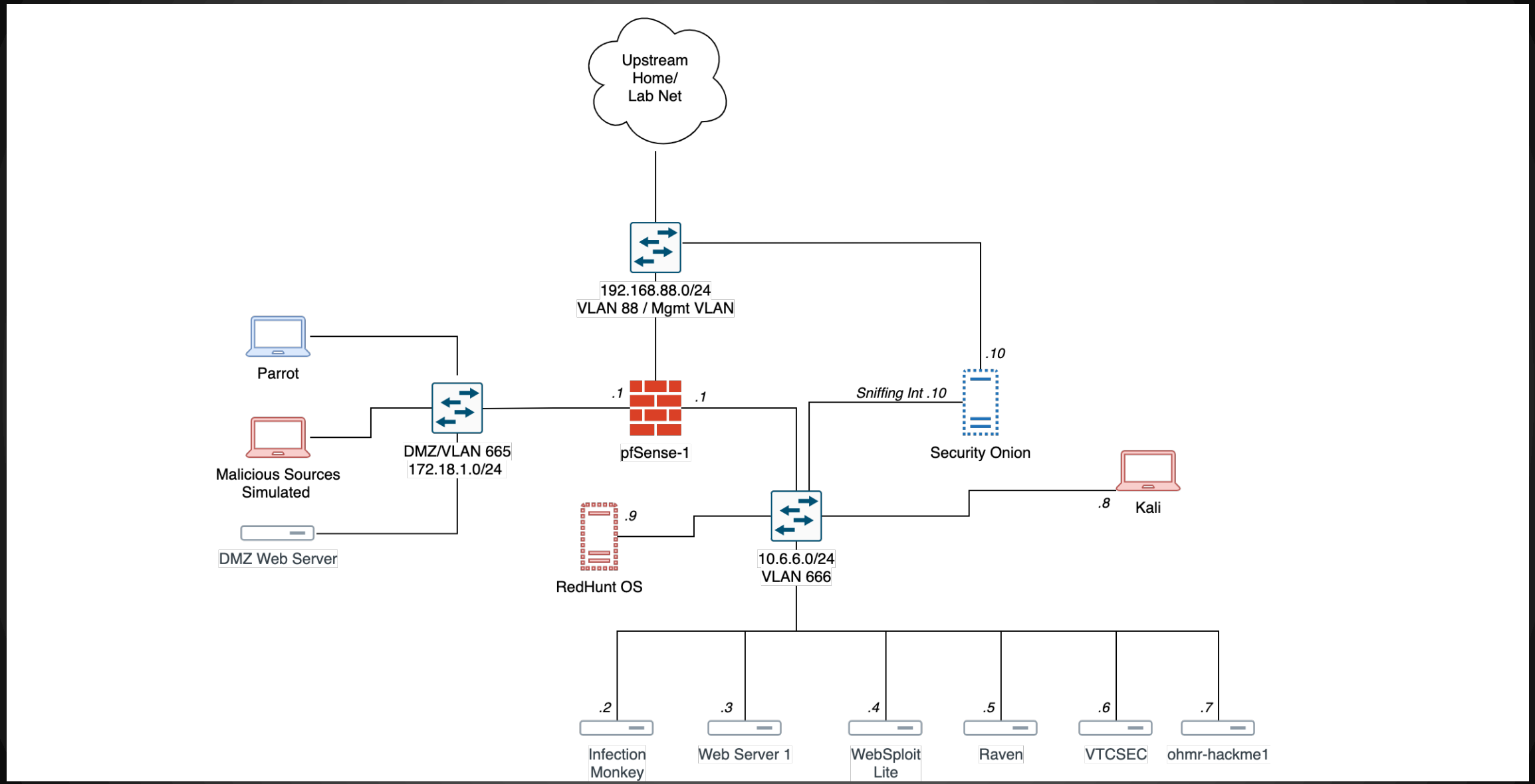
Visit nist.gov/nice/nicewg to access more resources and learn more about cyber ranges and the NICE Working Group Training and Certifications Subgroup or email us at nist.nice@nist.gov

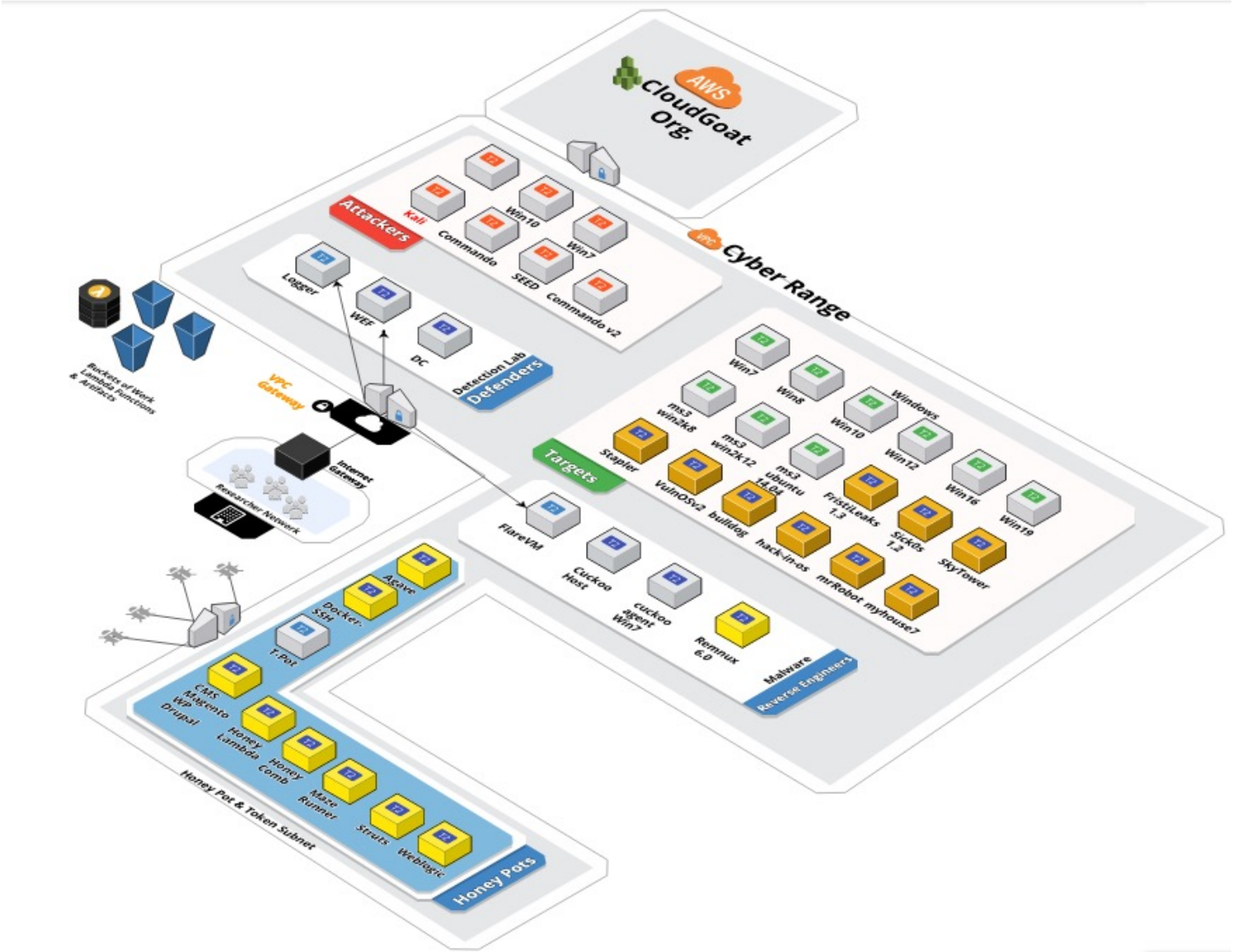
NICE National Initiative for Cybersecurity Education

nist.gov/nice

NIST National Institute of Standards and Technology U.S. Department of Commerce

https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf


Upstream
Home/
Lab Net
192.168.88.0/24
VLAN 88 / Mgmt VLAN
.10
Sniffing Int .10
Parrot
.1
.1
DMZ/VLAN 665
172.18.1.0/24
pfSense-1
Security Onion
Malicious Sources
Simulated
.8
Kali
.9
DMZ Web Server
RedHunt OS
10.6.6.0/24
VLAN 666
.2
.3
.4
.5
.6
.7
Infection
Monkey
Web Server 1
WebSploit
Lite
Raven
VTCSEC
ohmr-hackme1



https://github.com/The-Art-of-Hacking/h4cker/tree/master/build_your_own_lab

BREAK

WHAT ABOUT ADDITIONAL HARDWARE LIKE WIRELESS ADAPTERS?

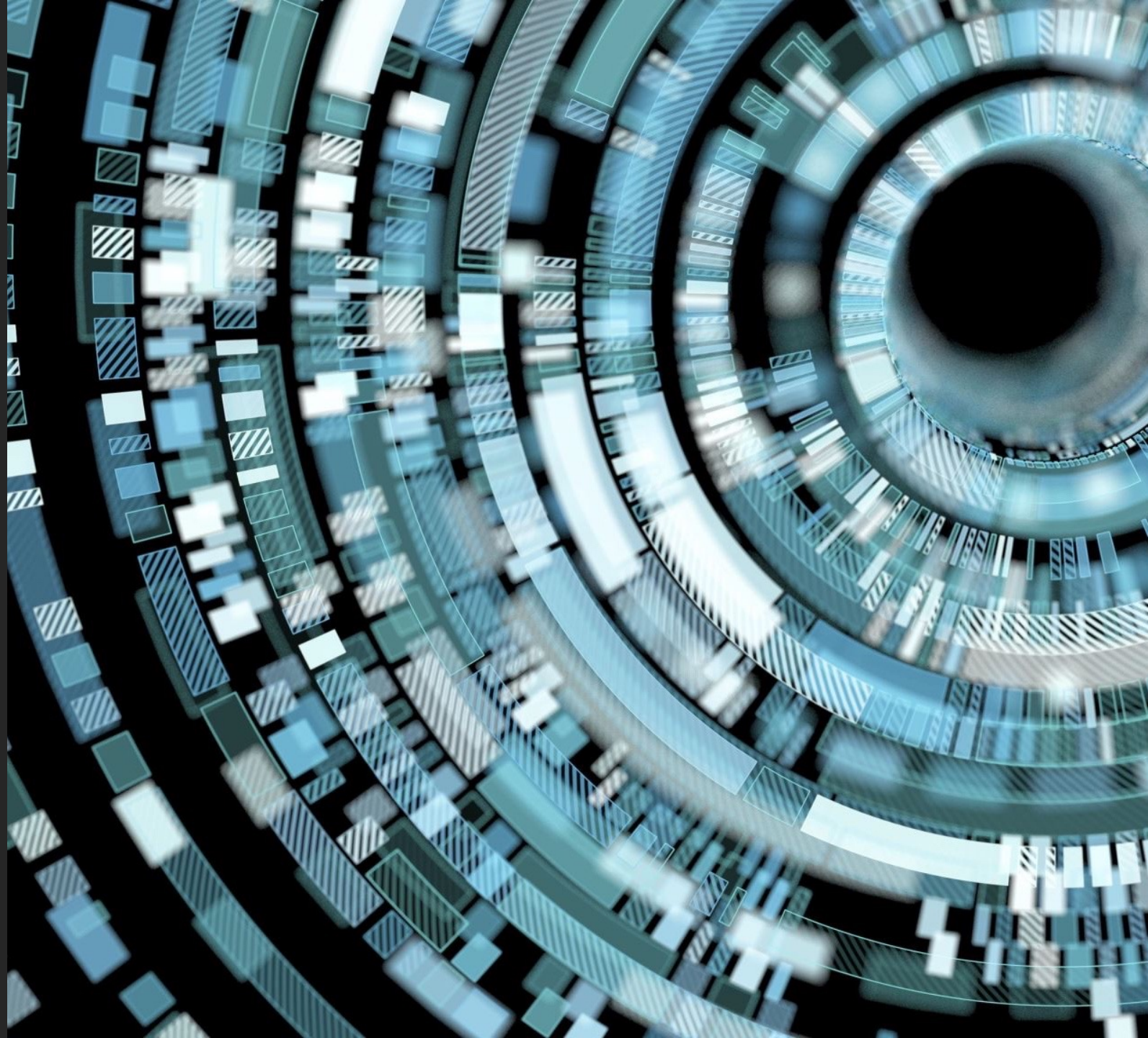
https://github.com/The-Art-of-Hacking/h4cker/tree/master/wireless_resources

USING LINUX KERNEL MODULES TO BUILD A WIRELESS HACKING LAB WITHOUT THE NEED OF PHYSICAL ADAPTERS

Linux

DEMO

WIRELESS VIRTUAL ADAPTERS

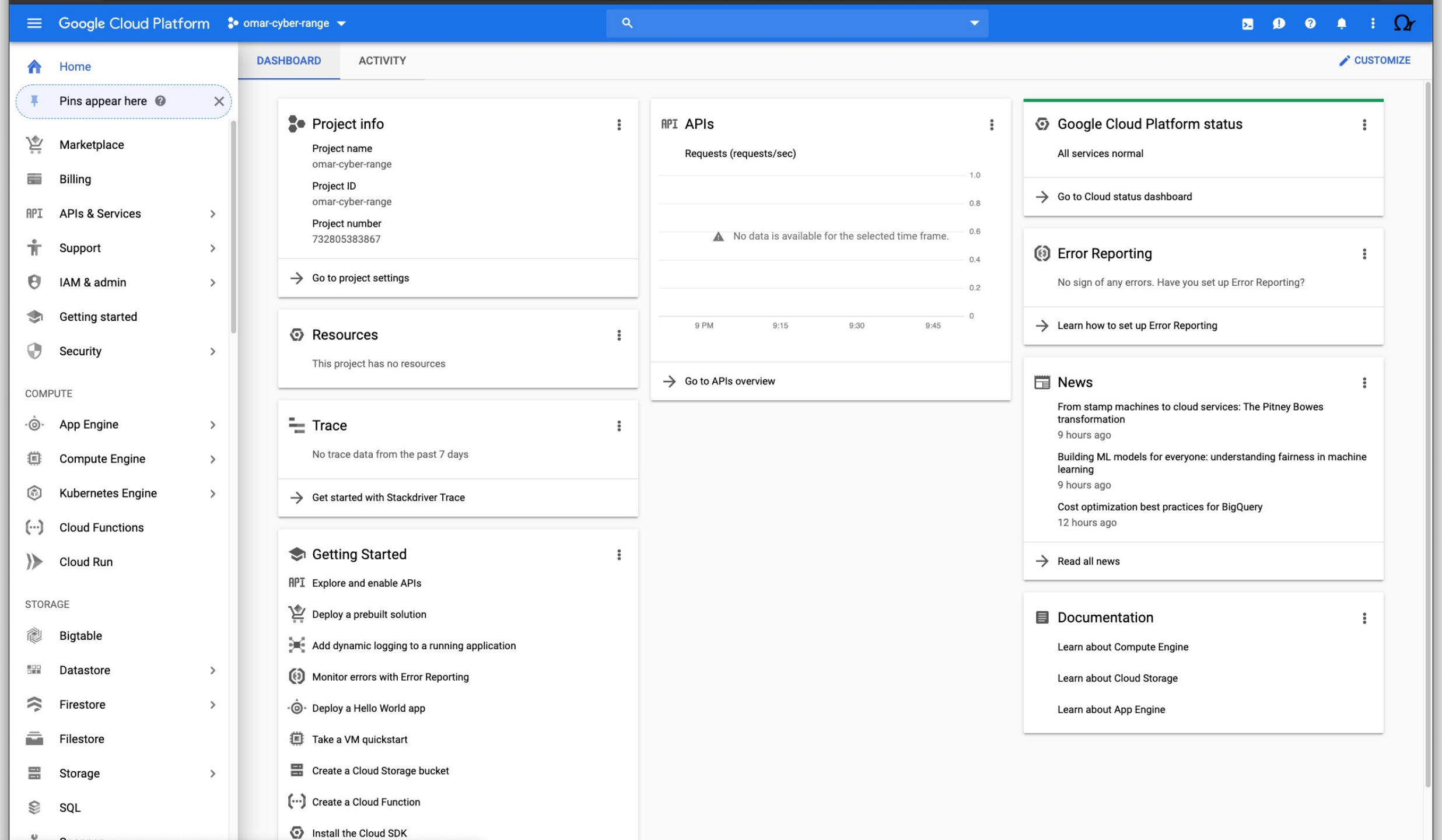


https://learning.oreilly.com/videos/wireless-networks-iot/9780134854632

BUILDING YOUR LAB IN CLOUD ENVIRONMENTS (AWS, AZURE, GOOGLE CLOUD, AND DIGITAL OCEAN)

IMPORTANT

- Having your cyber environment in the cloud costs $$$$!!
- VM Disk Size Matters!!!
- Amount of virtual CPUs Matter!!!!
- Amount of traffic (transfer rates) matter!!!
- Amount of available memory matters!!!
- Check the pricing of each cloud provider in detail!


Google Cloud Platform
omar-cyber-range
Home
Pins appear here
Marketplace
Billing
APIs & Services
Support
IAM & admin
Getting started
Security
COMPUTE
App Engine
Compute Engine
Kubernetes Engine
Cloud Functions
Cloud Run
STORAGE
Bigtable
Datastore
Firestore
Filestore
Storage
SQL
DASHBOARD
ACTIVITY
CUSTOMIZE
Project info
Project name
omar-cyber-range
Project ID
omar-cyber-range
Project number
732805383867
Go to project settings
Resources
This project has no resources
Trace
No trace data from the past 7 days
Get started with Stackdriver Trace
Getting Started
Explore and enable APIs
Deploy a prebuilt solution
Add dynamic logging to a running application
Monitor errors with Error Reporting
Deploy a Hello World app
Take a VM quickstart
Create a Cloud Storage bucket
Create a Cloud Function
Install the Cloud SDK
APIs
Requests (requests/sec)
No data is available for the selected time frame.
1.0
0.8
0.6
0.4
0.2
0
9 PM
9:15
9:30
9:45
Go to APIs overview
Google Cloud Platform status
All services normal
Go to Cloud status dashboard
Error Reporting
No sign of any errors. Have you set up Error Reporting?
Learn how to set up Error Reporting
News
From stamp machines to cloud services: The Pitney Bowes transformation
9 hours ago
Building ML models for everyone: understanding fairness in machine learning
9 hours ago
Cost optimization best practices for BigQuery
12 hours ago
Read all news
Documentation
Learn about Compute Engine
Learn about Cloud Storage
Learn about App Engine

console.cloud.google.com/compute/instances?project=omar-cyber-range&instancessize=50&duration=PT1H

Google Cloud Platform | omar-cyber-range

Compute Engine

VM instances | CREATE INSTANCE | IMPORT VM | REFRESH | START | STOP | RESET | DELETE | HIDE INFO PANEL | LEARN

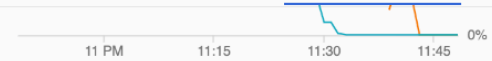
- VM instances
- Instance groups
- Instance templates
- Sole-tenant nodes
- Disks
- Snapshots
- Images
- TPUs
- Committed use discounts
- Metadata
- Health checks
- Zones
- Network endpoint groups
- Operations
- Security scans
- Marketplace

Filter VM instances | Columns

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
attack-box	us-east1-c			10.142.0.4 (nic0)	[redacted]	SSH
instance-1	us-east1-c			10.142.0.2 (nic0)		SSH
instance-2	us-east1-c			10.142.0.3 (nic0)		SSH

3 instances selected

PERMISSIONS | LABELS | MONITORING



CPU (attack-box):
CPU (instance-1):
CPU (instance-2):

Network Bytes

Bytes/sec | Sep 25, 2019 10:55 PM

3 | by project, instance name (sum) | 1 min interval (rate)

Incoming (attack-box):
Incoming (instance-1):
Incoming (instance-2):
Outgoing (attack-box):
Outgoing (instance-1):
Outgoing (instance-2):

Network Packets

(omar-cyber-range)

```
santosomar@cloudshell:~ (omar-cyber-range)$ gcloud compute --project=omar-cyber-range instances list
NAME        ZONE        MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP     STATUS
attack-box  us-east1-c  n1-standard-1               10.142.0.4   [redacted]      RUNNING
instance-1  us-east1-c  n1-standard-1               10.142.0.2                   RUNNING
instance-2  us-east1-c  n1-standard-1               10.142.0.3                   RUNNING
santosomar@cloudshell:~ (omar-cyber-range)$
```

console.cloud.google.com/compute/instances?project=omar-cyber-range&orgonly=true&supportedpurview=organizationId&instancessize=50

Google Cloud Platform | omar-cyber-range

Compute Engine

VM instances | CREATE INSTANCE | IMPORT VM | REFRESH | START | STOP | RESET | DELETE | HIDE INFO

- VM instances
- Instance groups
- Instance templates
- Sole-tenant nodes
- Disks
- Snapshots
- Images
- TPUs
- Committed use discounts
- Metadata
- Health checks
- Zones
- Marketplace

Filter VM instances | Columns

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
attack-box	us-east1-c			10.142.0.4 (nic0)	[redacted]	SSH
gke-omar-k8s-cluster-default-pool-e7abab1c-6shv	us-east4-c		gke-omar-k8s-cluster-default-pool-e7abab1c-grp, aedb8e98ae01611e982b442010a96002	10.150.0.2 (nic0)		SSH
gke-omar-k8s-cluster-default-pool-e7abab1c-qmcq	us-east4-c		gke-omar-k8s-cluster-default-pool-e7abab1c-grp, aedb8e98ae01611e982b442010a96002	10.150.0.3 (nic0)		SSH
gke-omar-k8s-cluster-default-pool-e7abab1c-ss77	us-east4-c		gke-omar-k8s-cluster-default-pool-e7abab1c-grp, aedb8e98ae01611e982b442010a96002	10.150.0.4 (nic0)		SSH
instance-1	us-east1-c			10.142.0.2 (nic0)		SSH

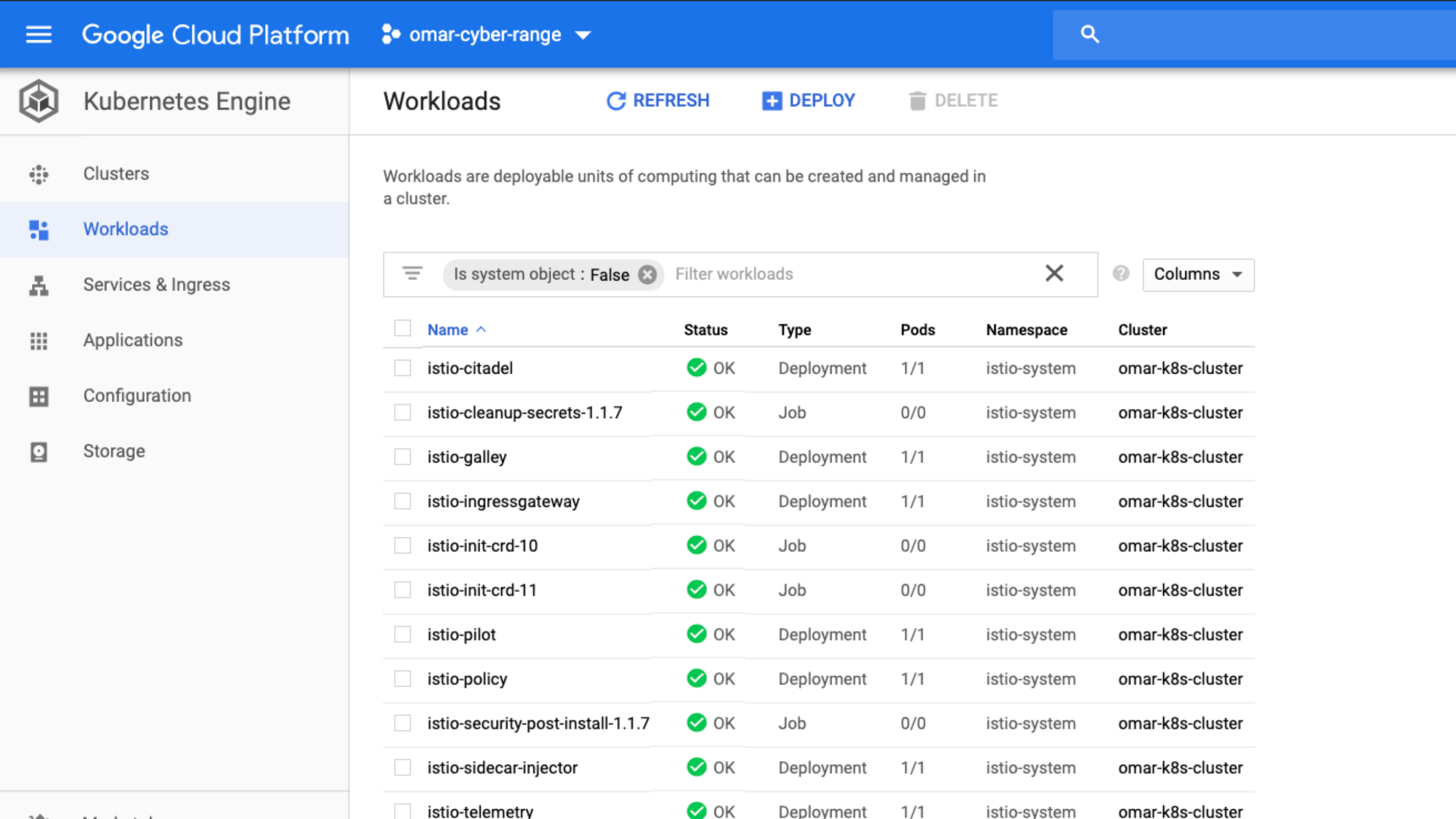
Select an instance

PERMISSIONS | LABELS | MONI

Please select at least one resource.

(omar-cyber-range) (omar-cyber-range)

```
santosomar@cloudshell:~ (omar-cyber-range)$ gcloud compute --project=omar-cyber-range instances list
NAME                                          ZONE        MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP    STATUS
attack-box                                    us-east1-c  n1-standard-1               10.142.0.4   [redacted]     RUNNING
instance-1                                    us-east1-c  n1-standard-1               10.142.0.2                  RUNNING
gke-omar-k8s-cluster-default-pool-e7abab1c-6shv  us-east4-c  n1-standard-1               10.150.0.2                  RUNNING
gke-omar-k8s-cluster-default-pool-e7abab1c-qmcq  us-east4-c  n1-standard-1               10.150.0.3                  RUNNING
gke-omar-k8s-cluster-default-pool-e7abab1c-ss77  us-east4-c  n1-standard-1               10.150.0.4                  RUNNING
santosomar@cloudshell:~ (omar-cyber-range)$
```


Google Cloud Platform
omar-cyber-range
Kubernetes Engine
Clusters
Workloads
Services & Ingress
Applications
Configuration
Storage
Workloads
REFRESH
DEPLOY
DELETE
Workloads are deployable units of computing that can be created and managed in a cluster.
Is system object : False
Filter workloads
Columns
Name
Status
Type
Pods
Namespace
Cluster
istio-citadel OK Deployment 1/1 istio-system omar-k8s-cluster
istio-cleanup-secrets-1.1.7 OK Job 0/0 istio-system omar-k8s-cluster
istio-galley OK Deployment 1/1 istio-system omar-k8s-cluster
istio-ingressgateway OK Deployment 1/1 istio-system omar-k8s-cluster
istio-init-crd-10 OK Job 0/0 istio-system omar-k8s-cluster
istio-init-crd-11 OK Job 0/0 istio-system omar-k8s-cluster
istio-pilot OK Deployment 1/1 istio-system omar-k8s-cluster
istio-policy OK Deployment 1/1 istio-system omar-k8s-cluster
istio-security-post-install-1.1.7 OK Job 0/0 istio-system omar-k8s-cluster
istio-sidecar-injector OK Deployment 1/1 istio-system omar-k8s-cluster
istio-telemetry OK Deployment 1/1 istio-system omar-k8s-cluster

Google Cloud Platform omar-cyber-range

Kubernetes Engine

- Clusters
- Workloads
- Services & Ingress
- Applications
- Configuration
- Storage
- Marketplace

Kubernetes clusters

CREATE CLUSTER DEPLOY REFRESH DELETE

A Kubernetes cluster is a managed group of VM instances for running containerized applications. Learn more

Filter by label or name

Name	Location	Cluster size	Total cores	Total memory	Notifications	Labels	
omar-k8s-cluster	us-east4-c	3	3 vCPUs	11.25 GB			Connect

(omar-cyber-range)

```
santosomar@cloudshell:~ (omar-cyber-range)$ gcloud compute --project=omar-cyber-range instances list
NAME                                          ZONE        MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP    STATUS
attack-box                                    us-east1-c  n1-standard-1               10.142.0.4   [redacted]     RUNNING
instance-1                                    us-east1-c  n1-standard-1               10.142.0.2                  RUNNING
gke-omar-k8s-cluster-default-pool-e7abab1c-6shv  us-east4-c  n1-standard-1               10.150.0.2                  RUNNING
gke-omar-k8s-cluster-default-pool-e7abab1c-qmcq  us-east4-c  n1-standard-1               10.150.0.3                  RUNNING
gke-omar-k8s-cluster-default-pool-e7abab1c-ss77  us-east4-c  n1-standard-1               10.150.0.4                  RUNNING
santosomar@cloudshell:~ (omar-cyber-range)$
```

H4cker

H4CKER.ORG

GOOGLE CLOUD DEMO

Google Cloud

https://www.kali.org/news/kali-linux-in-the-digitalocean-cloud/

DEMO

H4cker
H4CKER.ORG

BREAK

WHERE TO GET VULNERABLE APPLICATIONS AND VIRTUAL MACHINES?

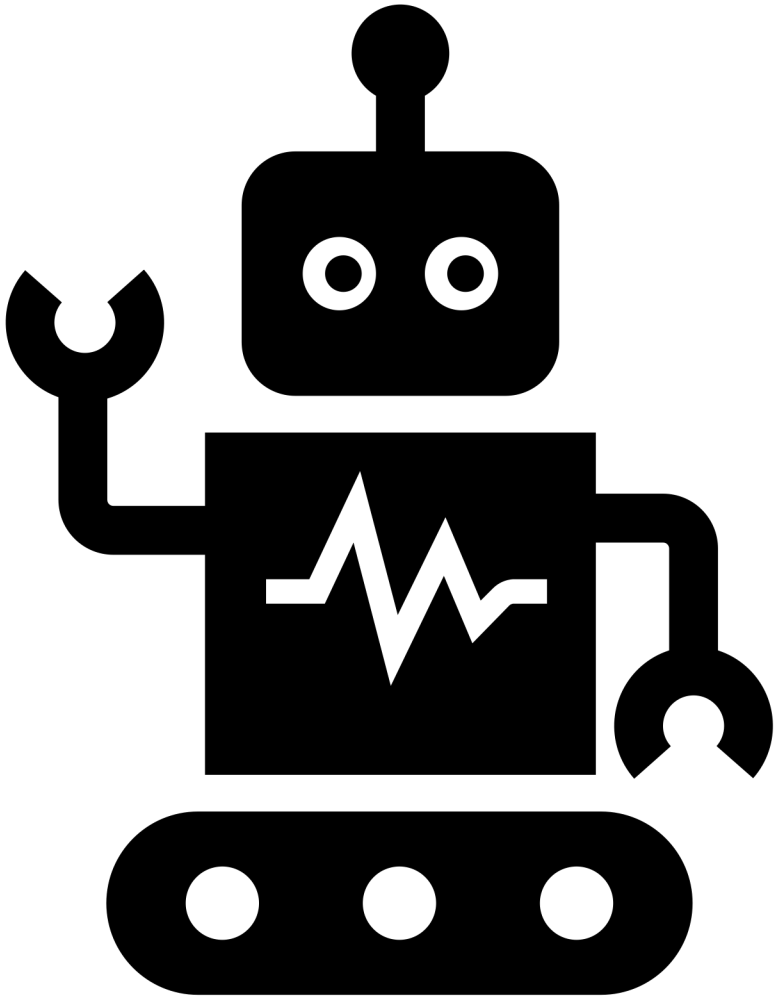
h4cker.org/github

DEMO

Vulnerables…

H4cker

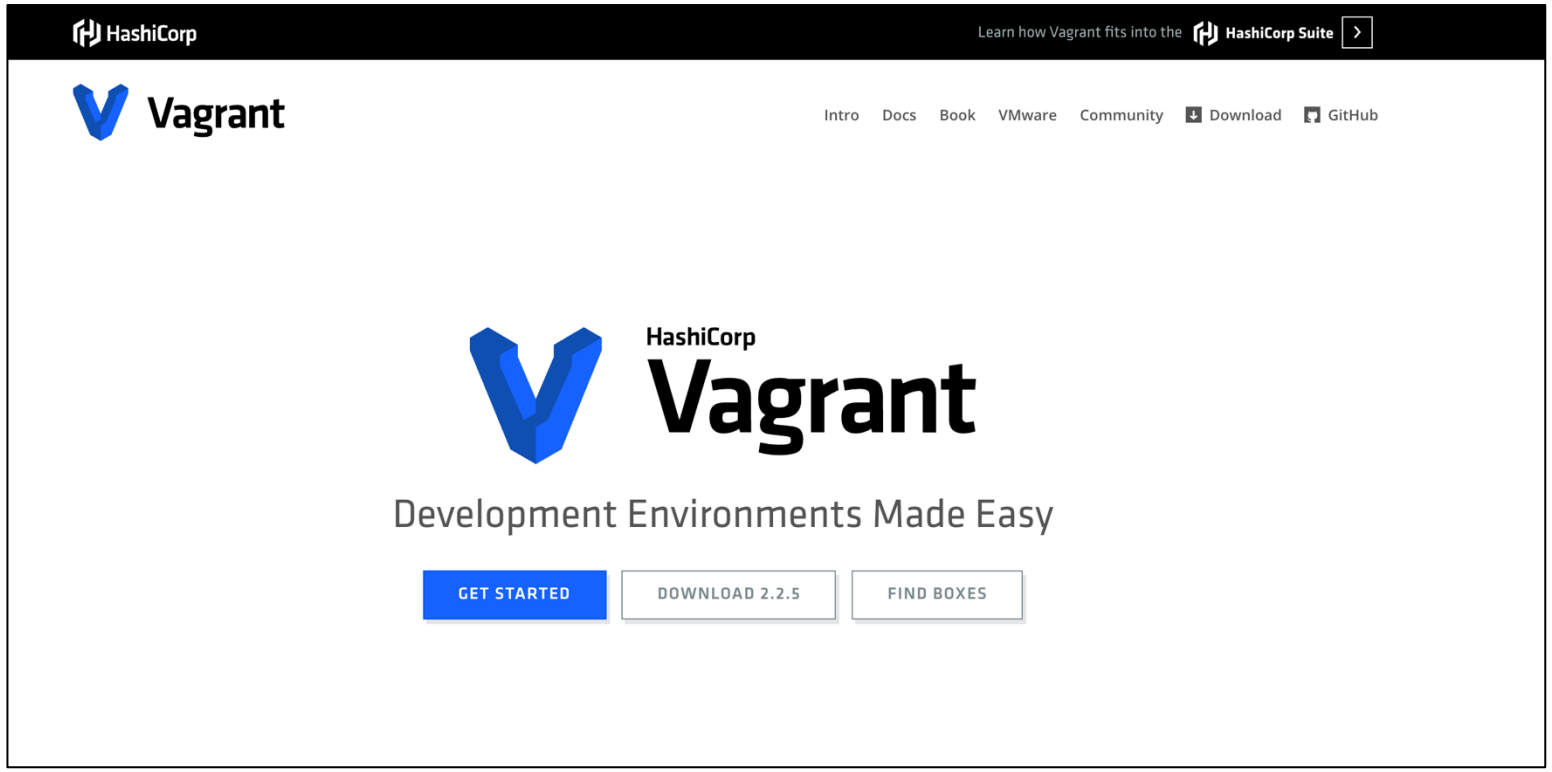
H4CKER.ORG



AUTOMATING LAB DEPLOYMENT WITH VAGRANT AND ANSIBLE

H4cker

H4CKER.ORG



https://www.vagrantup.com/

WHAT IS VAGRANT?

H4CKER.ORG

INTRODUCTION TO VAGRANT

- Vagrant is very simple on the surface, but is actually incredibly complex under the hood.
- It allows you to quickly and effortlessly create virtual environments (known as Vagrant boxes) and customize them.
- Vagrant easily integrates with multiple providers, such as VirtualBox, VMware, and Docker.
- These providers actually power the virtual environments, but Vagrant provides a customizable API to that virtual machine.
- Vagrant features can be split into a few key areas—Vagrantfile, boxes, networking, provisioning, and plugins.

THE ”VAGRANT FILE” (Vagrantfile)

- A Vagrantfile is a configuration file that uses the Ruby programming language syntax.
- It is easy to understand and can be quickly tested by making a change and then running the vagrant up command to see whether the expected results happen.
- A Vagrantfile can easily be shared and added into version control.
- It's lightweight and contains everything needed for another user to replicate your virtual environment/application.

NETWORKING

- Vagrant supports three main types of networking when creating virtual environments: public networks, private networks, and port-forwarding.
- The simplest networking option is port-forwarding, which allows you to access a specific port through the guest operating system into the Vagrant machine.

FIND VAGRANT BOXES

https://app.vagrantup.com/boxes/search

DEMO OF VAGRANT

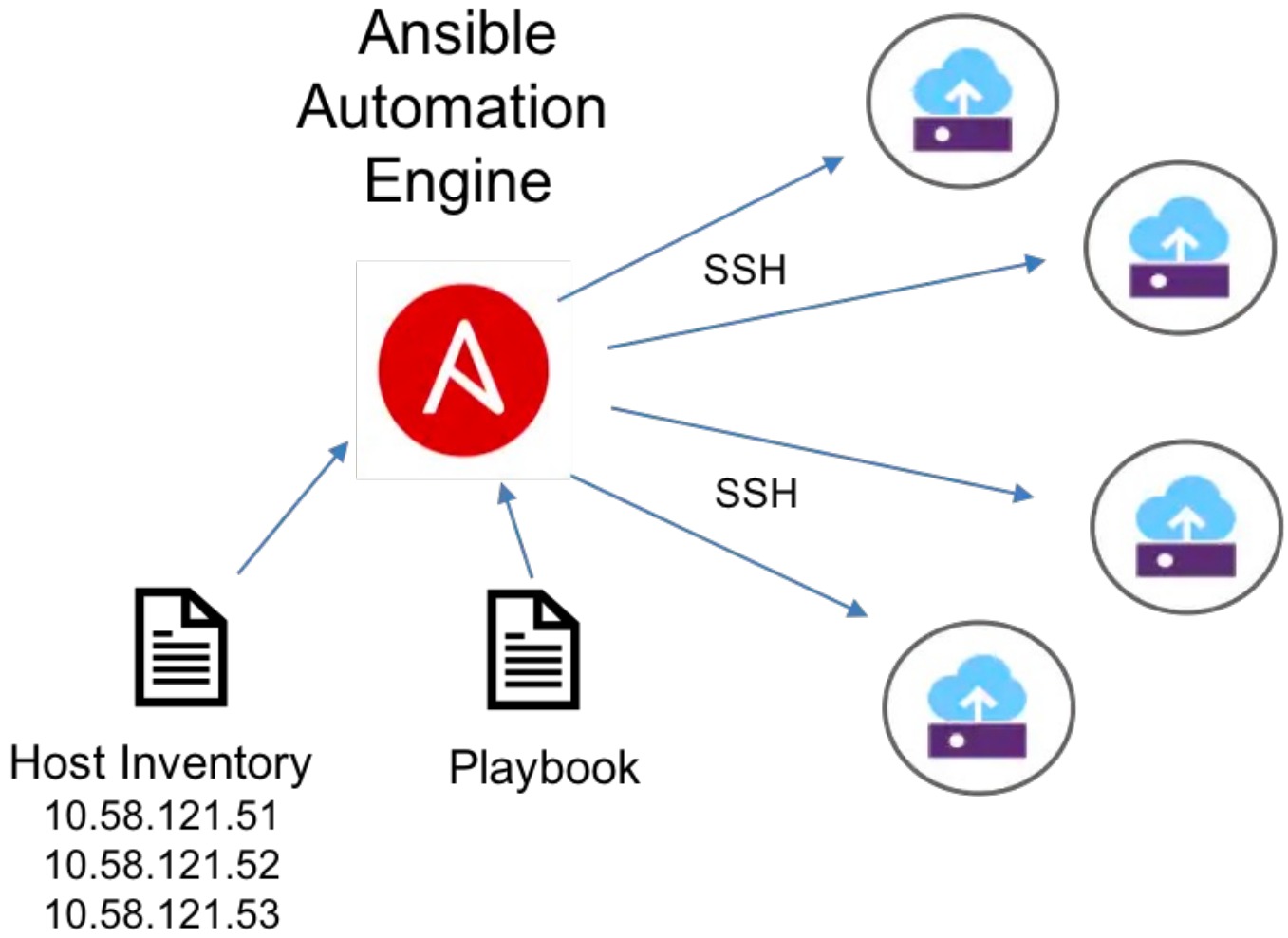
AUTOMATING VIRTUAL MACHINES

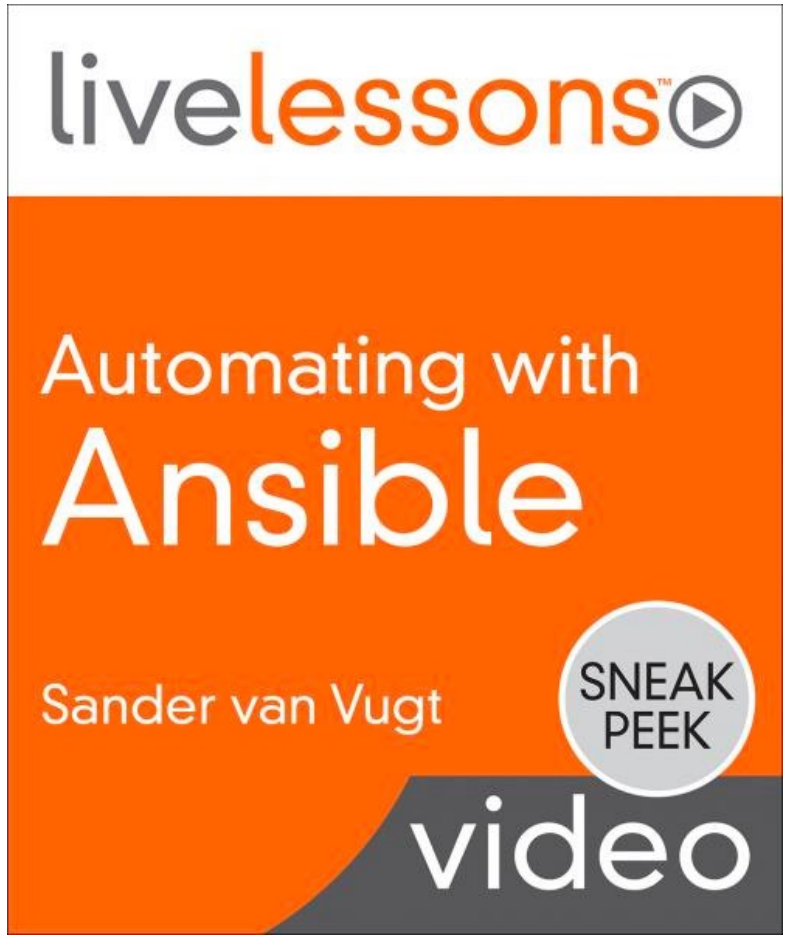
INTENSE ANSIBLE INTRODUCTION

INVENTORIES

- In Ansible, nothing happens without an inventory.
- Even ad hoc actions performed on the localhost require an inventory, though that inventory may just consist of the localhost.
- The inventory is the most basic building block of Ansible architecture.
- When executing ansible or ansible-playbook, an inventory must be referenced.
- Inventories are either files or directories that exist on the same system that runs ansible or ansible-playbook.
- The location of the inventory can be referenced at runtime with the --inventory-file (-i) argument, or by defining the path in an Ansible config file.

DEMO


Ansible
Automation
Engine
SSH
SSH
Host Inventory
10.58.121.51
10.58.121.52
10.58.121.53
Playbook



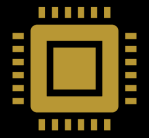
VIDEO COURSE FREE WITH YOUR O'REILLY SUBSCRIPTION

https://learning.oreilly.com/videos/automating-with-ansible/9780135308806

BREAK

CREATING SANDBOXES FOR MALWARE ANALYSIS

WE ALL MAKE MISTAKES…



DO NOT use your work computer!

DO NOT use your personal computer that you use on a daily basis!

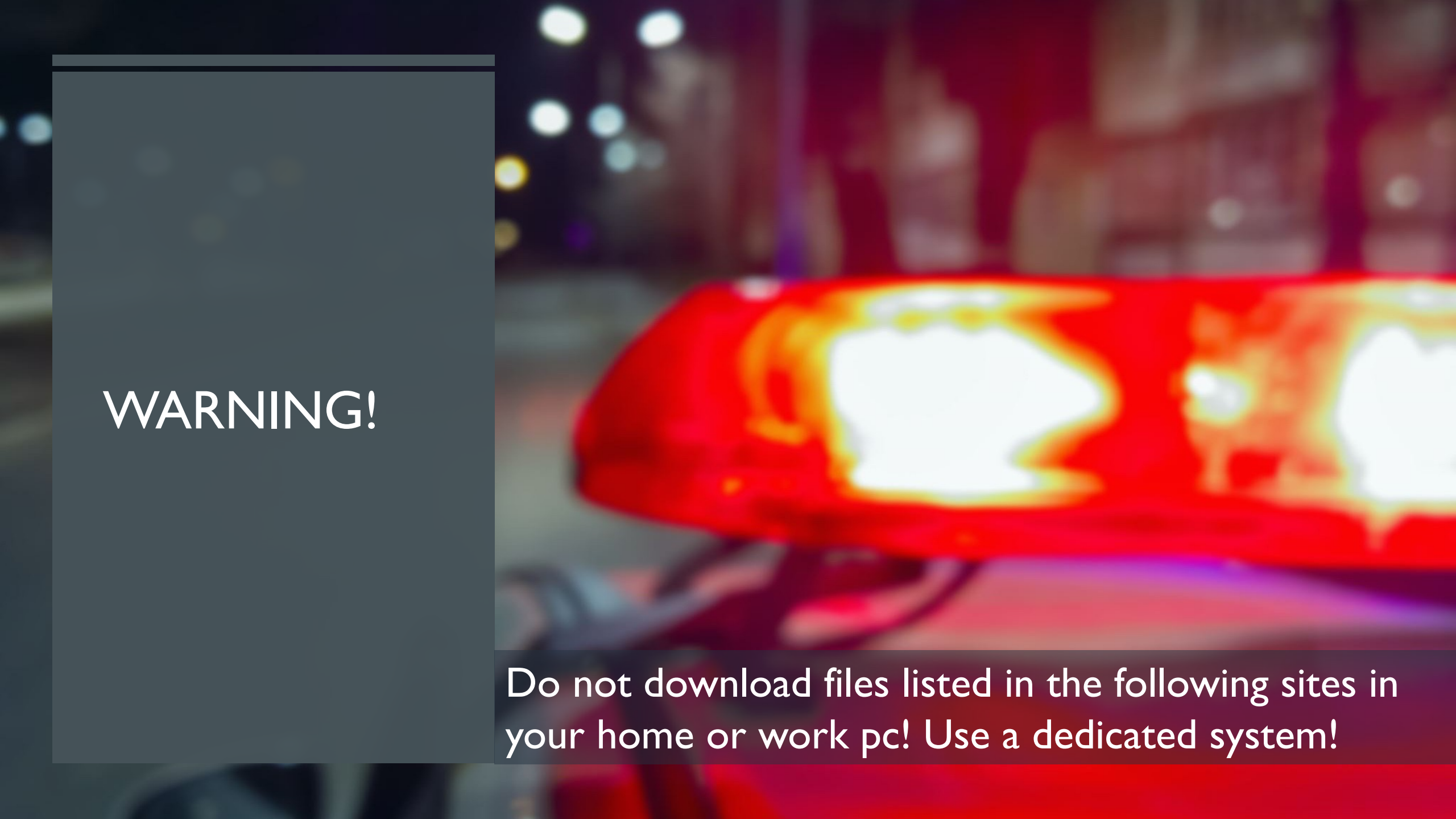
USE a malware analysis dedicated system (yes, even the hypervisor)!

MODERN MALWARE ANTI-ANALYSIS

- Malware detects whether it runs within a virtualized environment…
- Malware detects whether it runs within a sandbox environment…
- Malware check for sandbox by looking for mouse movements
- Malware can check for active windows
- Malware can check for size of hard disk
- Malware check whether foreground color changes
- Malware checks whether clipboard contents are empty

ONLINE MALWARE ANALYSIS

- https://www.virustotal.com
- https://sandbox.anlyz.io
- https://app.any.run
- https://valkyrie.comodo.com
- https://www.hybrid-analysis.com
- https://analyze.intezer.com
- https://www.talosintelligence.com/talos_file_reputation



WARNING!

Do not download files listed in the following sites in your home or work pc! Use a dedicated system!

theZoo aka Malware DB

A repository of LIVE malwares for your own joy and pleasure

View the Project on GitHub
ytisf/theZoo

Download ZIP File | Download TAR Ball | View On GitHub

theZoo - A Live Malware Repository

theZoo is a project created to make the possibility of malware analysis open and available to the public. Since we have found out that almost all versions of malware are very hard to come by in a way which will allow analysis, we have decided to gather all of them for you in an accessible and safe way. theZoo was born by Yuval tisf Nativ and is now maintained by Shahak Shalev.

theZoo is open and welcoming visitors!

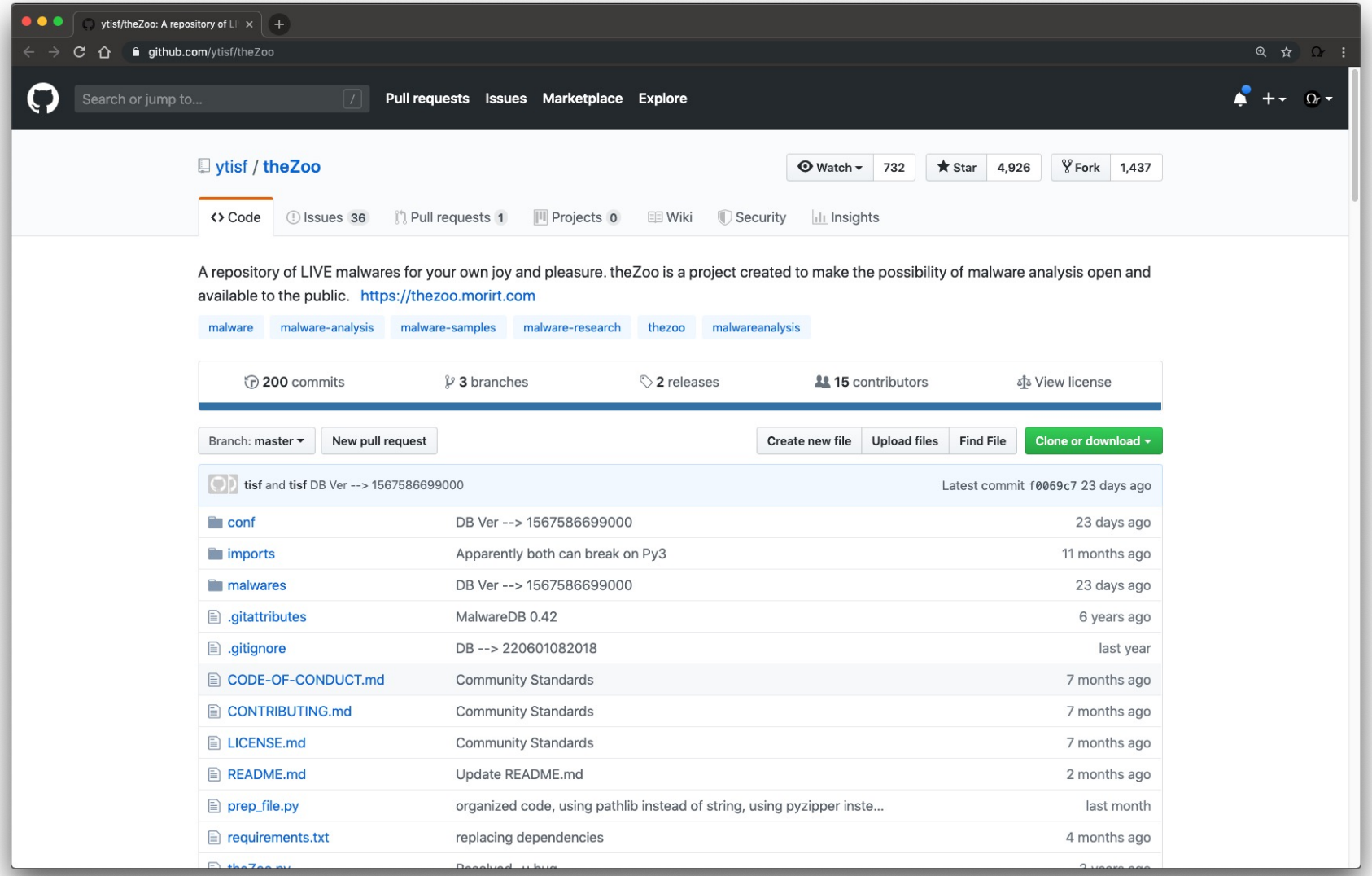
If you are about to interact with our community please make sure to read our `CODE-OF-CONDUCT.md` prior to doing so. If you plan to contribute, first - thank you. However, do make sure to follow the standards on `CONTRIBUTING.md`.

Disclaimer

theZoo's purpose is to allow the study of malware and enable people who are interested in malware analysis (or maybe even as a part of their job) to have access to live malware, analyse the ways they operate, and maybe even enable advanced and savvy people to block specific malware within their own environment.

Please remember that these are live and dangerous malware! They come encrypted and locked for a reason! Do NOT run them unless you are absolutely sure of what you are doing! They are to be used only for educational purposes (and we mean that!) !!!

https://thezoo.morirt.com/


ytisf/theZoo: A repository of LI
github.com/ytisf/theZoo
Search or jump to...
Pull requests
Issues
Marketplace
Explore
ytisf / theZoo
Watch 732
Star 4,926
Fork 1,437
Code
Issues 36
Pull requests 1
Projects 0
Wiki
Security
Insights
A repository of LIVE malwares for your own joy and pleasure. theZoo is a project created to make the possibility of malware analysis open and available to the public. https://thezoo.morirt.com
malware
malware-analysis
malware-samples
malware-research
thezoo
malwareanalysis
200 commits
3 branches
2 releases
15 contributors
View license
Branch: master
New pull request
Create new file
Upload files
Find File
Clone or download
tisf and tisf DB Ver --> 1567586699000
Latest commit f0069c7 23 days ago
conf DB Ver --> 1567586699000 23 days ago
imports Apparently both can break on Py3 11 months ago
malwares DB Ver --> 1567586699000 23 days ago
.gitattributes MalwareDB 0.42 6 years ago
.gitignore DB --> 220601082018 last year
CODE-OF-CONDUCT.md Community Standards 7 months ago
CONTRIBUTING.md Community Standards 7 months ago
LICENSE.md Community Standards 7 months ago
README.md Update README.md 2 months ago
prep_file.py organized code, using pathlib instead of string, using pyzipper inste... last month
requirements.txt replacing dependencies 4 months ago

VirusShare.com

virusshare.com

Account: Login

VirusShare.com - Because Sharing is Caring

Home - About - Hashes - Research - Support the Project

Please login to search and download.

System currently contains 34,073,865 samples.

Please note that this site is constantly under construction and might be broken.

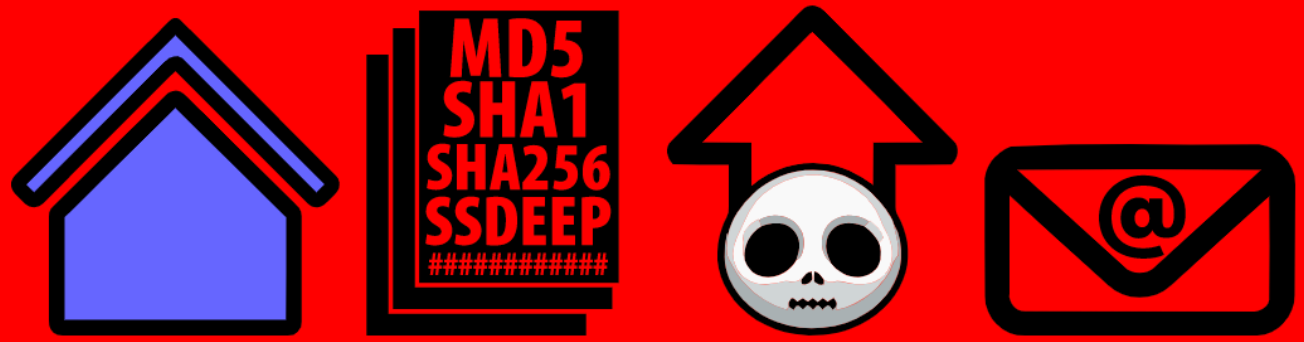
Latest sample added to the system:

MD5	e706e43b0bd55839b739516068a28731
SHA1	8df975bac400eab2c248a442fac3143b58126834
SHA256	0710ce9405b1d10b143083dae172a6e0396abf8b46cca4fc182305883cfa8065
SSDeep	196608:qBi9rTxnblV9O7qP+z/MRX19XQ0rHa/7lSrTkYPLOoI087vjzLm:q4lnj9O768/MJHXQeHaTlSMYPLZI0Uv6
Size	6,641,455 bytes
File Type	Zip archive data, at least v2.0 to extract
Detections	Avira = SPR/ANDR.Secapk.FAB.Gen CAT-QuickHeal = Android.SecApk.B (PUP) Cyren = AndroidOS/Secapk.B.gen!Eldorado ESET-NOD32 = a variant of Android/Secapk.F potentially unsafe Ikarus = AdWare.AndroidOS.Secapk K7GW = Adware (0052d5ee1) Sophos = Generic PUA IN (PUA) SymantecMobileInsight = AppRisk:Generisk
ExIF Data	FileSize = 6.3 MB FileType = ZIP FileTypeExtension = zip MIMEType = application/zip ZipBitFlag = 0x0008 ZipCRC = 0x1b78ce80 ZipCompressedSize = 37025 ZipCompression = Deflated ZipFileName = META-INF/MANIFEST.MF ZipModifyDate = 2016:01:07 07:40:04 ZipRequiredVersion = 20 ZipUncompressedSize = 112345
VirusTotal Report submitted 2019-09-13 08:57:06 UTC	
VirusShare info last updated 2019-09-27 07:45:00 UTC	

Virusign - Home

virusign.com

ViruSign



EXACT NUMBER OF DETECTIONS
(Except ClamAV)

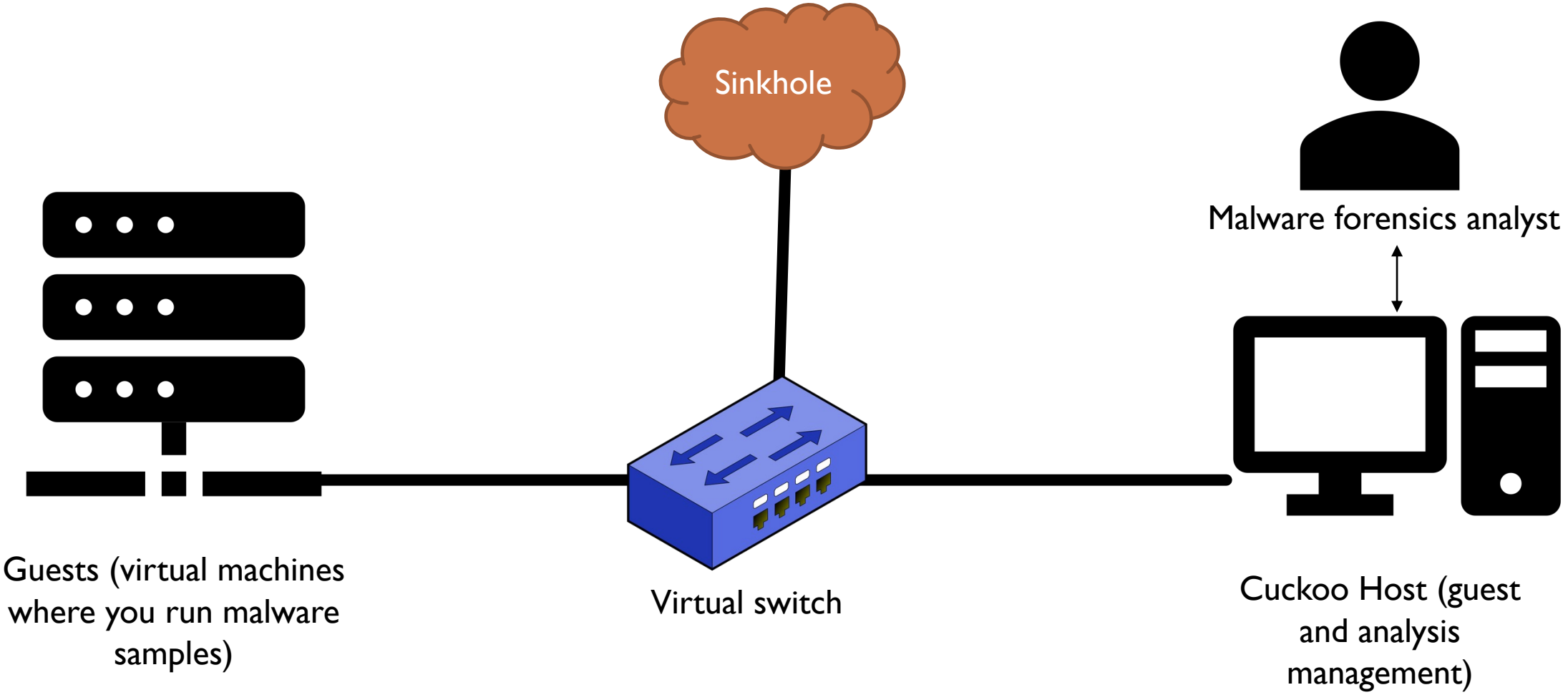
4 3 2 1 0

<< < 1 2 3 4 5 6 7 8 9 10 > >>

Search

7zip	Date	Size	CRC32 / MD5 SHA1 / SHA256		AV1		AV2		AV3		AV4		AV5	
Download	2019-09-26	1.7MB	2d418b68 1bea911ed87d6b901b39e85ae8eb7e1f 0235423d8e5a503b0d996e85f6ded38d8923de6e bb668c06fd68a3b41db12cc862909f63661afa79022ea78f1b85c9e95f43146e	More Info	No	2019-09-26	Yes	2019-09-26	Yes	2019-09-26	Yes	2019-09-26	Yes	2019-09-26
Download	2019-09-24	140.5KB	2347a849 ebb00cdd113fd1f2335425de5066c02f de5e1f6d29b92bc801872032631311ea2573756c 44bc4363ec41247d13997acf8cf8eceb23502d491b86b72402afb1a04d90c6b9	More Info	No	2019-09-26	Yes	2019-09-25	Yes	2019-09-24	Yes	2019-09-24	Yes	2019-09-24
Download	2019-09-24	1.3MB	57f266ed 458da8ac0ac693f654c5c3316781301f b5c618fd438cccacd0d57af82f15ba7241c46fc0 0fe869f90aa27324319c8e014973fa8695899bfef816cf981b064befc8dcac76	More Info	No	2019-09-25	Yes	2019-09-25	Yes	2019-09-24	Yes	2019-09-24	Yes	2019-09-24
Download	2019-09-23	1.1MB	b9f6dc7d 4b77d54d7c3aa88ec43ed09f872ff00f b861160959e43696684fdc78bdfeb4a7c7cd814c 9167de316e876b04c6660ba3a60e4e2956593b030a657b158c71140d6563e204	More Info	No	2019-09-23	Yes	2019-09-25	Yes	2019-09-23	Yes	2019-09-23	Yes	2019-09-23
Download	2019-09-21	2.1MB	2429812c 427f13ee968dde84656e02ac446c4f62 e428e672472aa1537cef50636f315e59fb7572e1 4709592e7bf5f8082d72781a8a656944b726bf753319f1128d973ea7ca781dc1	More Info	No	2019-09-26	Yes	2019-09-21	Yes	2019-09-21	Yes	2019-09-21	Yes	2019-09-21
Download		1.4KB	d9905b8e de6901a34021d5085a94d7db88c022dc	More										


Cuckoo Sandbox - Automated
cuckoosandbox.org
cuckoo
Automated Malware Analysis
Home
Downloads
Partners
Docs
Blog
About Cuckoo
Discussion
What is Cuckoo?
Cuckoo Sandbox is the leading open source automated malware analysis system.
cuckoo
You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.
Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization.
In these evolving times, detecting and removing malware artifacts is not enough: it's vitally important to understand how they operate in order to understand the context, the motivations, and the goals of a breach.
Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under Windows, macOS, Linux, and Android.
Download Cuckoo Sandbox 2.0.7
Contribute to Cuckoo
More downloads
READ NOW:
Cuckoo Sandbox 2.0.7
Posted on June 19, 2019
Read this blogpost!
DISCUSSION
Join the discussion on one of our community networks:
IRC
#cuckoosandbox
cuckoosandbox



https://cuckoo.sh/docs/introduction/index.html

AWESOME TUTORIAL

https://www.youtube.com/watch?v=V4z2tLRCuIY

H4cker

H4CKER.ORG

REVERSE ENGINEERING TOOLS : HEX EDITORS

- 010 Editor
- Hex Workshop
- HexFiend
- Hiew
- HxD

REVERSE ENGINEERING TOOLS : DISASSEMBLERS

- Ghidra
- Binary Ninja
- Capstone
- fREedom
- Hopper
- IDA Pro
- JEB
- objdump
- Radare

REVERSE ENGINEERING TOOLS : DYNAMIC ANALYSIS

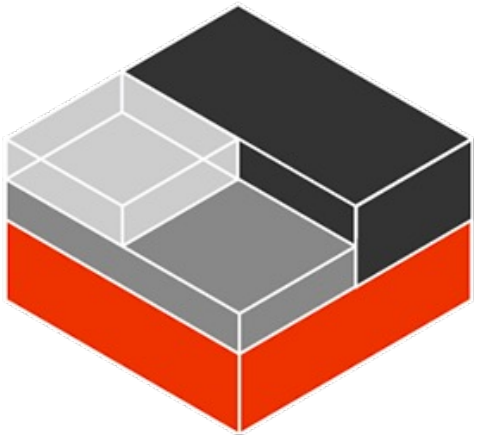
- Autoruns
- Process Monitor
- Process Explorer
- Process Hacker
- Noriben - Portable, Simple, Malware Analysis Sandbox
- API Monitor
- INetSim: Internet Services Simulation Suite
- FakeNet
- Volatility Framework
- Stardust
- LiME: Linux Memory Extractor

REVERSE ENGINEERING TOOLS : DEOBFUSCATION

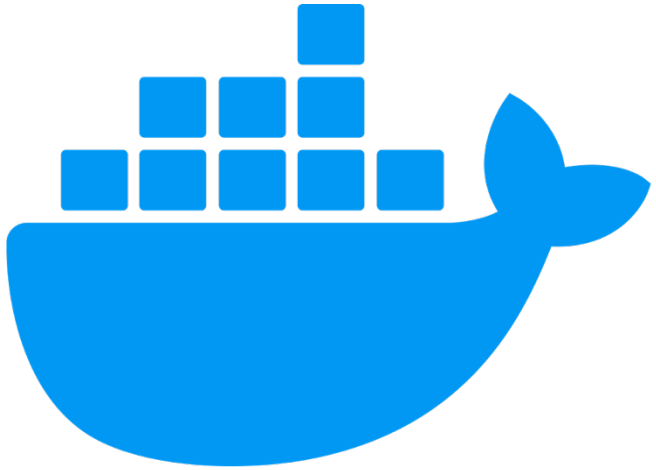
- Balbuzard
- de4dot
- ex_pe_xor
- iheartxor
- FLOSS
- NoMoreXOR
- PackerAttacker
- unpacker
- unxor
- VirtualDeobfuscator
- XORBruteForcer
- XORSearch & XORStrings
- xortool

REVERSE ENGINEERING TUTORIALS

- ARM Assembly Basics
- Binary Auditing Course
- Corelan Training
- Dr. Fu's Malware Analysis
- Legend of Random
- Lenas Reversing for Newbies
- Modern Binary Exploitation
- Offensive and Defensive Android Reversing
- Offensive Security
- Open Security Training
- REcon Training
- Reverse Engineering Malware 101
- RPISEC Malware Course
- TiGa's Video Tutorials
- Malware Traffic Analysis

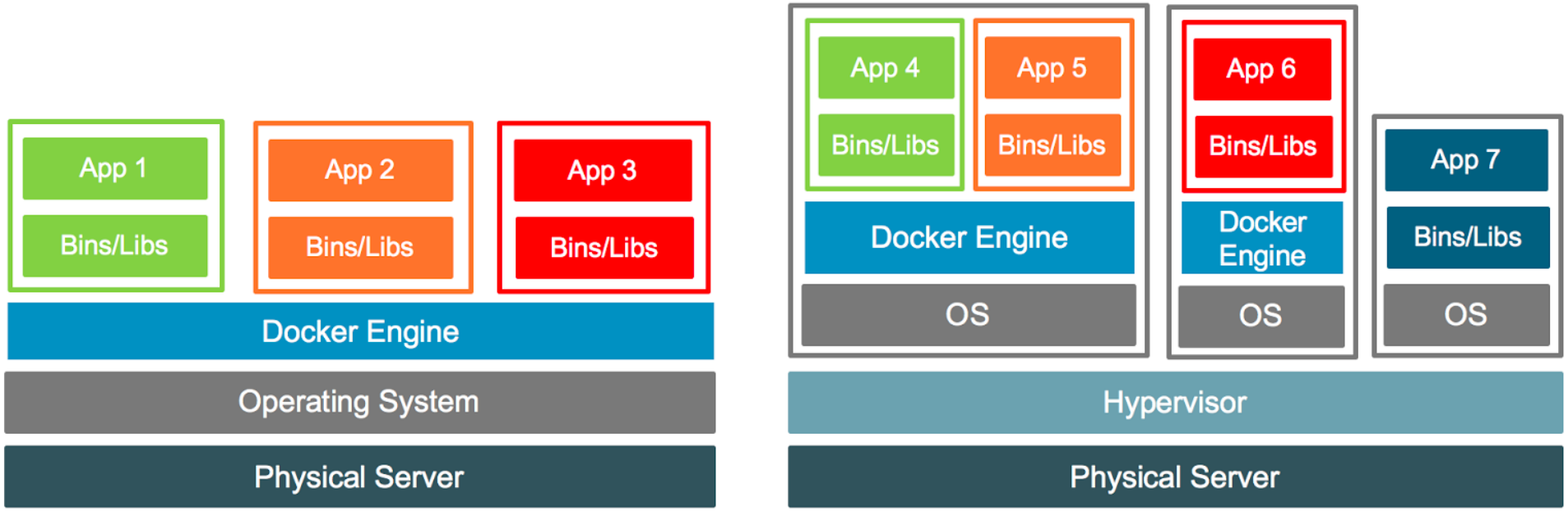


LXC



docker

USING CONTAINERS TO PRACTICE YOUR OFFENSIVE AND DEFENSIVE SECURITY SKILLS



VMS VS CONTAINERS

Linux Containers

liblxc

namespaces

cgroups

SELinux/AppArmor

Linux kernel

Docker 1.10 and later

runC

runC

runC

containerd-shim

containerd-shim

containerd-shim

containerd

Docker Engine

namespaces

cgroups

SELinux/AppArmor

Linux kernel

DEMO

https://hub.docker.com/u/santosomar

LAB SCENARIOS FOR CYBER SECURITY CERTIFICATIONS

WHITEBOARD SCENARIOS

VulnHub OSCP Practice VMs

- https://www.vulnhub.com/?q=oscp&sort=date-asc

Q&A

H4cker

H4CKER.ORG

THANK YOU!

H4cker

H4CKER.ORG