

Northeast RRC Meeting Recap

Jake Mihevc
jmihevc@mvcc.edu



Virtual Platforms
and Exercise
Design for Cyber
Competitions

DIY Virtualization in EDU: Types

VM Repos

- ▶ Initial Higher than Average Technical Skill & Capital Requirements Create High Barriers of Entry for Users
- ▶ Loss of Control Leads to High Variance in User Experience

VMs + Public Cloud

- ▶ Complex & Varying Interfaces Create a Barrier to Entry for Users
- ▶ Public Cloud is a Costly Utility and Poorly Fits into Cost Structures Outside of Pay-to-Play

VMs + Private Cloud

- ▶ Complex Interfaces Create a Barrier of Entry for Users
- ▶ Manual Management & Mass VM Storage Costly
- ▶ Big Upfront Cost for Cloud Infrastructure

VMs + Private Cloud + BYO* Platform

- ▶ Biggest Upfront Cost Initially & Higher Staffing Requirements*
 - ▶ Buy == Admins & Support Staff
 - ▶ Build ++ Developers & DevOps Engineers & Time

Scale: Three Examples

- ▶ Local
- ▶ National
- ▶ Regional

Local

- ▶ Facebook CTF (open source)
- ▶ Amazon MicroCTF

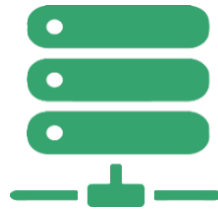


NICE Challenge PROJECT



Platform

- We run & host the hardware, no upfront investment required
- Powerful & highly accessible web interface, no installs required
- Enables specialized content development, deployment, & analysis



Environments

- Full scale context rich environments inspired by NICE Cybersecurity Workforce Framework Categories
- Fictional organizations & employees
- Virtualized networks, servers, & employee desktops



Challenges

- Competency based assessments focused on real world problems & context
- Maps to NICE Cybersecurity Workforce Framework Tasks/KSAs & CAE KUs
- Designed to capture useful data for actionable metrics & analytics

Regional



Proxmox Virtual Environment

PROXMOX Virtual Environment 4.3-1/e7cdc165 Search You are logged in as 'root@pam' Help Create VM Create CT Logout

Server View

- 1715071 (Team7-kali1-internal)
- 1715081 (Team8-kali1-internal)
- 1715091 (Team9-kali1-internal)
- 1715101 (Team10-kali1-internal)
- 1791001 (Team0-router)
- 1791002 (Team0-fri-httpd)
- 1791011 (Team1-router)**
- 1791012 (Team1-fri-httpd)
- 1791021 (Team2-router)
- 1791022 (Team2-fri-httpd)
- 1791031 (Team3-router)
- 1791032 (Team3-fri-httpd)
- 1791041 (Team4-router)
- 1791042 (Team4-fri-httpd)
- 1791051 (Team5-router)
- 1791052 (Team5-fri-httpd)
- 1791061 (Team6-router)
- 1791062 (Team6-fri-httpd)
- 1791071 (Team7-router)
- 1791072 (Team7-fri-httpd)
- 1791081 (Team8-router)
- 1791082 (Team8-fri-httpd)
- 1791091 (Team9-router)
- 1791092 (Team9-fri-httpd)
- 1791101 (Team10-router)

Virtual Machine 1791011 ('Team1-router') on node 'proxmox2' Start Shutdown Reset Remove Migrate

Summary Console Hardware Options Task History Monitor Backup Snapshots Firewall Permissions

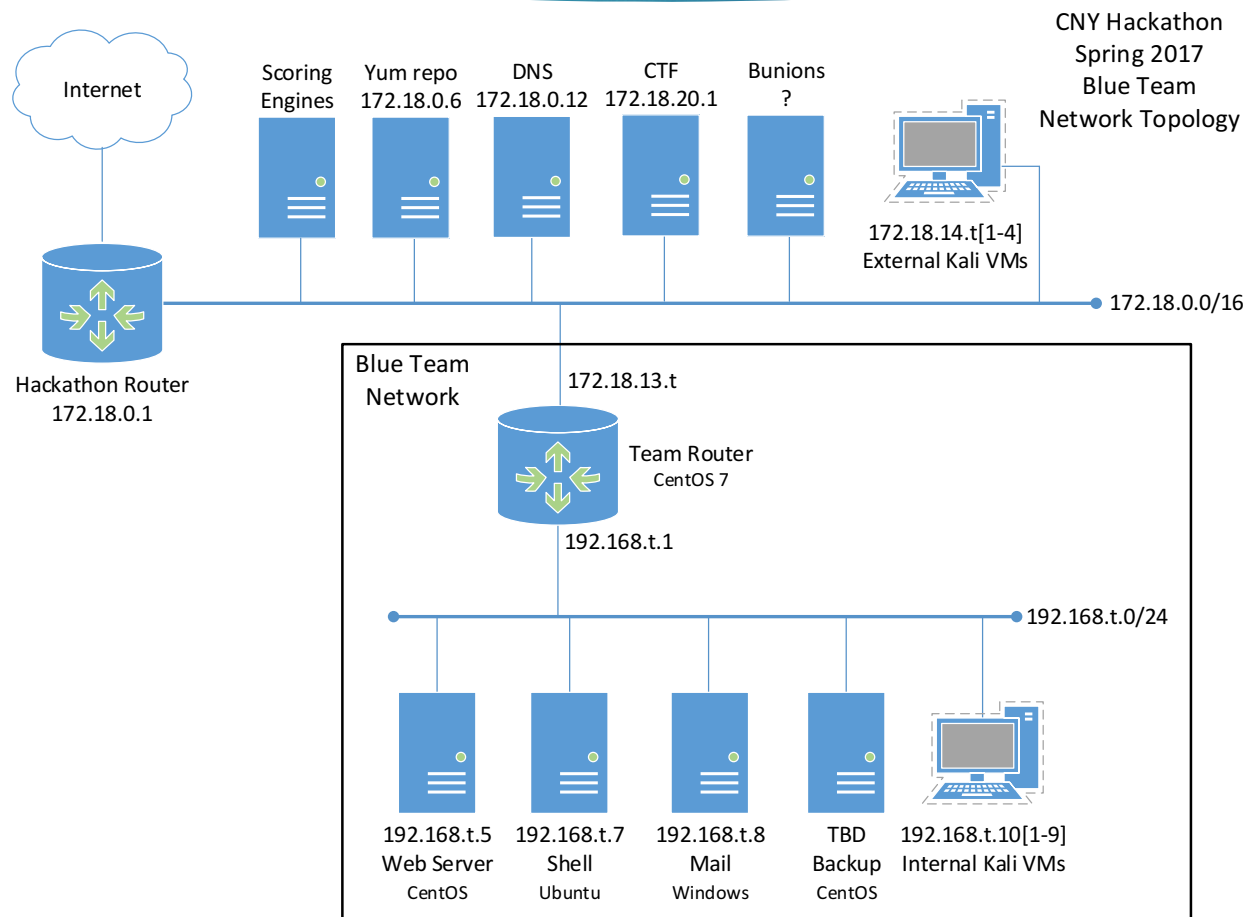
Connected (encrypted) to: QEMU (Team1-router)

```
(root@team1-router /)# ls
bin boot dev etc home lib lib64 media mnt opt proc root run shin srv sys usr var
(root@team1-router /)# passwd
bash: passwd: command not found
(root@team1-router /)# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
(root@team1-router /)#
```

Tasks Cluster log

Start Time ↓	End Time	Node	User name	Description	Status
Nov 01 22:21:58		proxmox2	root@pam	VM/CT 1791011 - Console	









































Proxmox Virtual Environment



t = team number

Proxmox Virtual Environment

Team External Routers (team_router_external)

Host	Status	Services	Actions
t10_router_external	DOWN	10 CRITICAL	   
<u>t1_router_external</u>	UP	1 OK	   
		9 CRITICAL	
t2_router_external	DOWN	10 CRITICAL	   
t3_router_external	DOWN	10 CRITICAL	   
t4_router_external	DOWN	10 CRITICAL	   
t5_router_external	UP	1 OK	   
		9 CRITICAL	
t6_router_external	DOWN	10 CRITICAL	   
t7_router_external	DOWN	10 CRITICAL	   
t8_router_external	UP	1 OK	   
		9 CRITICAL	
t9_router_external	UP	2 OK	   
		8 CRITICAL	

Proxmox Virtual Environment

proxmox2 (Uptime: 34 days 11:58:05)

CPU usage 10.59% of 32 CPU(s)

Load average 3.16,3.25,3.05

RAM usage 30.76% (38.72 GiB of 125.87 GiB)

HD space(root) 6.01% (5.67 GiB of 94.37 GiB)

IO delay 0.08%

KSM sharing 0 B

SWAP usage 0.00% (0 B of 8.00 GiB)

CPU(s)

32 x Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (2 Sockets)

Kernel Version

Linux 4.4.19-1-pve #1 SMP Wed Sep 14 14:33:50 CEST 2016

PVE Manager Version

pve-manager/4.3-1/e7cdc165

Broader Regional Implementation?

- ▶ Regional Collaboration
- ▶ Online
- ▶ Preparation for CCDC
- ▶ Satisfy Competition Criteria for Candidate Schools

Credits

- ▶ NE Region CAEs
- ▶ James Ashley NICE Challenge
- ▶ Nick Merante CNY Hackathon
(Nmerante@mvcc.edu)
- ▶ Dr. Ronny Bull CNY Hackathon
(rlbull@utica.edu)