



Fall 2024

<http://score.cnyhackathon.org/>

Black Team

- Responsible for managing infrastructure
- and assisting blue teams during the competition
 - Each Blue team will have an assigned Black team member in your team room
 - Reach out to your Black team member if there's something you need
 - Catch us in #blackteam-open
 - Summon us to your team channel - @blackteam
 - blackteam has accounts on Linux VMs
 - Usernames: blackteam & blackteam-r
 - Abusing these accounts will be out of scope for red team

Competition Environment

- Everyone should have a lab workstation
 - Use your lab workstation to access the competition platform
 - Competition VMs:
 - <http://vce.cnyhackathon.org/>
 - Kali (Internal & External)
 - Infrastructure Server VMs
 - Gravwell Instance
 - Your team's Discord channel has a pinned message with a URL containing any additional credentials

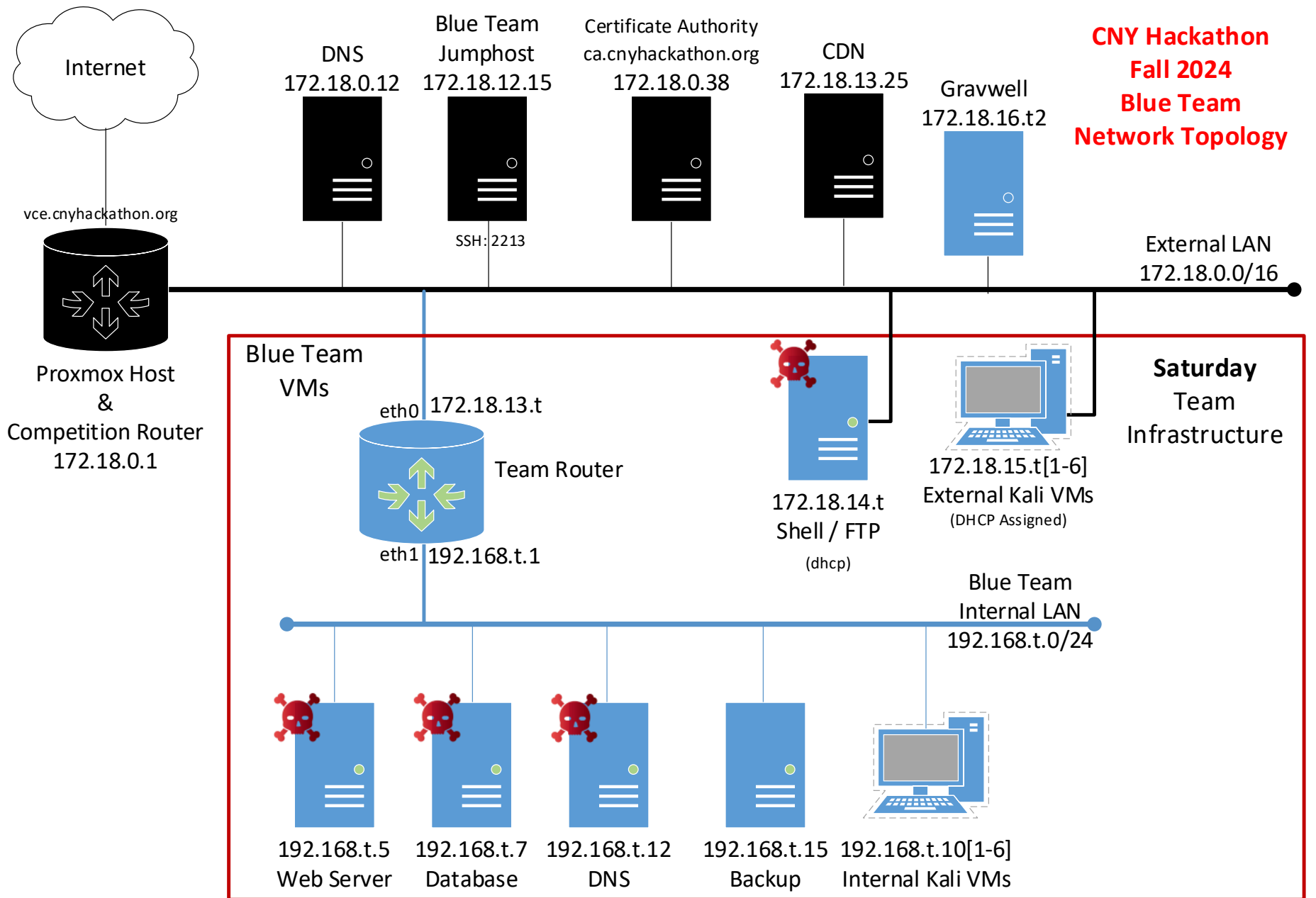
Challenge Groups

- Total points available: 15,000
 - Infrastructure - 12,000 points
 - Capture the Flag & injects - 3,000 points

Infrastructure Competition

- Each team will be given a small network to secure and defend
- Profile your system and search for configuration errors and weaknesses
- The red team will be doing this as well
 - They have the advantage
- Their goal is to infiltrate and disrupt services

**CNY Hackathon
Fall 2024
Blue Team
Network Topology**



t = team number



These VMs are already compromised!

All Blue Team VMs are in scope for red team.



Managed by Black team

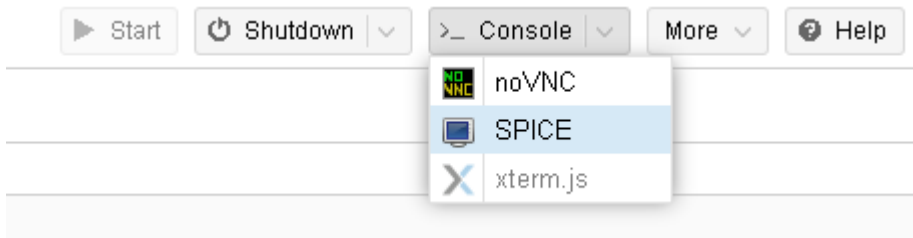
Managed by Blue teams

Kali VMs

- Running updated kali rolling
 - With some performance tweaks
- Three external and three internal
 - External Kali address are DHCP assigned
 - You will need to assign internal: 192.168.t.10[1-6]
 - Let us know if you need more VMs
- Only the first two have 3gb RAM
 - Let us know if you run into resource issues.

Kali Virtual Console

- Use the SPICE viewer instead of VNC
 - Dual monitor and clipboard support
 - Much more responsive
 - Requires a viewer client application
 - Download from <http://www2.cnyhackathon.org/spice.html>






















Infrastructure VMs

- Competition Start
 - We will release all competition VMs at once
 - IP addresses need to be assigned to all VMs on your internal LAN
 - Some configuration work may be necessary to bring your services fully online
 - External Kali VMs and the shell server will be DHCP assigned
 - Scoring will start at 9am Saturday
 - Scoring schedule: 9am to 12pm then 1:30pm to 4:30pm
 - We'll break for lunch & career fair from noon to 1:30pm

Infrastructure Scoring

- You will only receive points if your services are online and functioning properly
- The scoring engine can be found at
 - <https://score.cnyhackathon.org/>
- The red team will be attempting to disrupt services and rob you of points
- Full score details will be published in the scoring engine: <http://score.cnyhackathon.org/>

Scoring

 Router ICMP	HTTP	
Team0		
Team1		
Team2		
Team3		
Team4		
Team5		
Team6		
Team7		
Team8		

<https://score.cnyhackathon.org/>

Scope

- It is very important to stay within scope!
- Blue Team:
 - Defense only (except CTF challenges, where appropriate)
 - May not access other team's resources
 - Including their VMs and Discord channels
 - May not interfere with or access Black Team infrastructure
 - May not attack back at Red Team
- Red Team:
 - May not use blackteam or blackteam-r shell accounts
 - May not access blue team jumphost
 - May not abuse any scoring accounts
 - May not access Blue team Discord channels

Lockdown

- Access to the infrastructure and VMs will be locked Friday at 10pm.
- Get some rest, you'll need it!

<http://score.cnyhackathon.org/>