NCAE

This is a mostly blue team-oriented event, the CTFs are just if you have some extra time. The scoring is based on how long you keep network services alive. The total you can earn from the services is something like 8000 points vs 2000 for all the CTFs, some of which are pretty hard. Throughout the day, the red team will take down the services if they can.

Preparation

Sandboxes

They offer sandboxes to practice on and it's really important to practice. The sandboxes are not the most fun to use, but the practice that they focus on is pretty much 1-1 for what you do in the competition.

- Packet Man Ping
    - An interactive tutorial with some basic tasks that will be useful in setting up the network.

- Mini Hacks
    - Sandbox tasks the user with setting up a virtual network very similar to the one used during the event.
    - Recommend the most attention be paid to this sandbox

- World of Bills
    - Didn't play around with this much (I really should have, I can't stress the importance of these sandboxes.)
    - Seems to be the tutorial for general system hardening and monitoring

- Capture the Flag
    - CTF sandbox, self-explanatory
    - Only a couple were similar to those during the competition, most were significantly more difficult

Video

There are a bunch of tutorial videos that are related to the competition tasks. I don't necessarily recommend watching every single one, but if you're having trouble with the sandboxes the answers are probably in these videos.

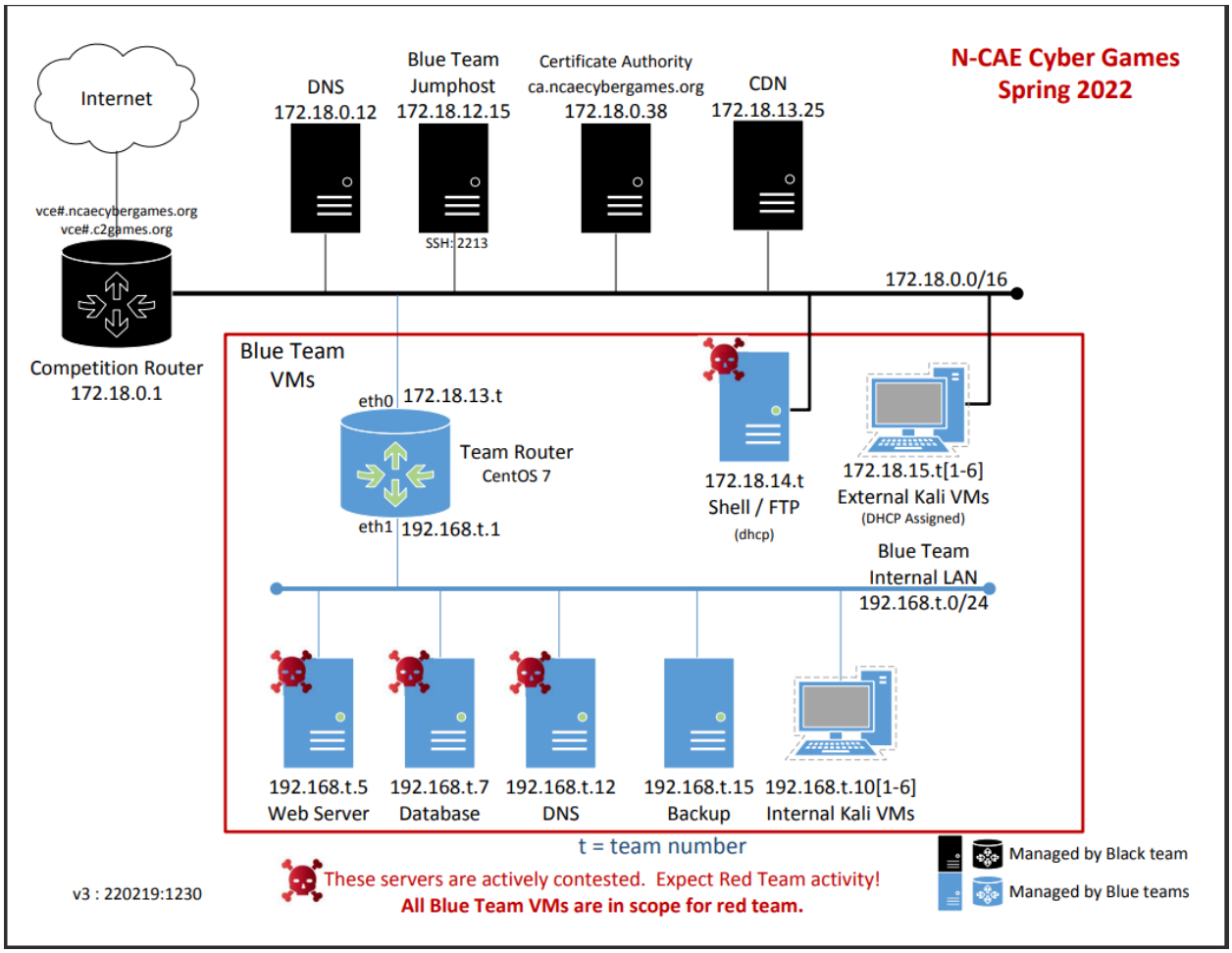
- Intro to Linux Admin
    - A lot of this will be stuff you should already know if you've been coming to meetings.

    - Most helpful will be the videos on managing permissions, exploring sudoers and removing users, and (if you mess up some “scoring users”) passwords and shadow hashes.

- Intro to Networking
    - Most of these could use a quick watch, but they are also pretty basic
    - The three most relevant videos are the three that deal with static configuration. You will definitely need to know all three of these forwards and backward during competition. The red team loves to mess with the config files.

- Routing and services
    - This is the most important section.
    - Videos that go over the Mini Hack sandbox will be very helpful during practice.
    - SSH videos can hel limit red team intrusions into your network.
    - The DNS videos are very important. The way they score DNS is kind of finicky, and these videos go over everything you need to know to set them up the way they want.

Event



This is the topology for NCAE Spring 2022. The main purpose is to get the services on the blue machines up and running, then keep them up and running. The red team will try and actively bring down the services on the systems marked with skulls but will use the kali VMs as vectors to attack your systems if you let them. I'll list the number of services scored from memory so it may not be entirely accurate.

- External Kali VMs
    - Allow access to the internet
    - No scored services
    - After initial setup most helpful for doing CTFs
- Shell/FTP
    - 4 scored services
    - Requires very little configuration at first, but the red team will definitely mess with it at some point. Back up all the important files. Locally at first then the backup server once you can

- Router
    - Self-explanatory, a router is necessary to connect interior services to the scoring server
    - 1 scored service I believe, but all the interior scored services depend on it.
- Web Server
    - 3 scored services
    - Worth a lot, essentially getting an apache web server online and attaching the database to it
- Database
    - 1 scored service for sure and 1 of the web services is dependent on it
- DNS
    - 3 scored services
    - Very annoying, make sure to watch the videos on it
- Backup
    - This is off-limits to the red team, get it online and store backups of important files like config files
    - You will not be given access to it, you have to “break-in”
    - IIRC is a CentOS server and you can use grub to alter the root password to gain access
- Internal Kali VMs
    - Useful to SSH into internal network devices

Tips

- They will give you access to a webpage the night before that has a lot of specific information on scoring and whatnot, make sure you read it. Pay special attention to the way they are scoring services.
- The FIRST thing you do is get the shell/FTP server hardened. The red team absolutely will try to screw you as soon as possible by messing with it. They dropped a “reverse shell” on us within minutes of the event starting. It reversed all input. If that happens, I used i- hs/nib/ to get something I could use.
- The FTP server has users that are necessary for scoring, DON’T REMOVE THEM. It’s a giant pain to get them back online. They will be listed in the scoring part of that webpage I mentioned.
- Now a red team can’t get to your internal services without having the router up, but you can’t start scoring points either. I recommend hardening your systems a bit, starting your services, and then configuring the router. You service likely won’t be up for a bit after you start anyway.
- Back up your config files before you mess with them. It can be easier to start from scratch than to hunt for the error in whatever you messed up.
- Get into that backup server as soon as possible so that you can safely back up the config files once you get them the way you want them. The red team will absolutely mess with your config files on contested machines.

- The web server services are worth a bunch of points, so try to get that up as soon as possible.
- Have some people monitoring the logs to keep an eye on the red team.
- They will assign a black team member to you. If you need help, make sure to ask them. They won't flat out tell you what to do, but they'll put you on the right track. Our guy Steven was the real MVP.