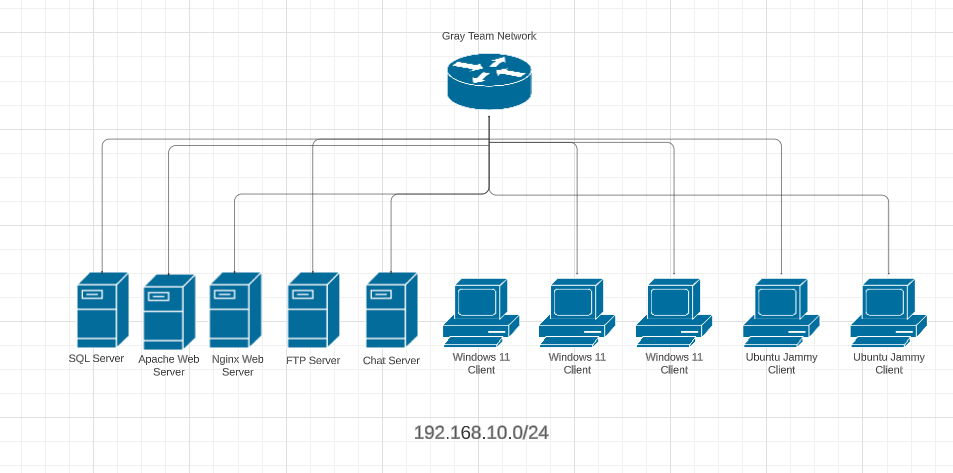


**Theme Description:**Welcome to the Tom & Jerry capture the cheese competition. For this competition the red team will be referred to as “Tom” and the blue team will be referred to as “Jerry.” The goal of the competition is for Tom to not only take down Jerry’s services, but also take his cheese! On most machines there are going to be several of Jerry’s passwords aka “cheese”. Cheese will be indicated by curly braces or dollar signs (i.e. **{this\_is\_cheese}** or **$this\_is\_cheese$**). Tom will obtain points for not only shutting off Jerry’s services, but also collecting his cheese. Jerry on the other hand is in charge of protecting his cheese as well as keeping his services up to earn points (For more information on scoring see the “How scoring works” section). By the end of the competition a winner will be determined based on who has the most points.

Tom = Red

Jerry = Blue

**Topology**

**Boxes**

1. Ubuntu nginx Web Server
2. Ubuntu apache Web Server
3. Ubuntu FTP Server
4. Ubuntu SQL Database Server
5. Ubuntu Chat server
6. Ubuntu Jammy Client
7. Ubuntu Jammy Client
8. Windows 11 Client
9. Windows 11 Client
10. Windows 11 Client

**Credentials**

Local System admin Accounts**:**

Ubuntu**:**  
Username: root

Password: rootroot

Windows:

Username: Administrator

Password: rootroot

MySQL:

root

root

RocketChat:

Number is 1-5

Username: Blue[Number]

Email: Blue[Number]@hotmail.com

password: BlueTeam1!

RocketChat Admin Account

Username: BlueAdmin

Email: BlueAdmin@hotmail.com

password: BlueTeamAdmin1!

Don’t touch accounts:

Ftp admin = gray\_admin

Rocketchat = greyadmin

Sql = greyadmin2

Webservers = grey\_admin

Others: grey\_admin

**Rules**

1. Cannot interfere with the scoring engine
2. Cannot use firewalls
3. No exfiltrating data to work on out of competition hours
4. Blue team must stay to the right side of the room. Red team stays to the left
5. No communication between the Red and Blue team is allowed
6. Bricking machines is not allowed (on purpose, be smart)
7. Breaking the rules will result in some point deduction (as determined by the Gray team)
8. Tools, techniques, or services that render an entire machine’s files/information completely immutable or inaccessible during the competition is prohibited
9. Blue team may not make fake flags
10. Blue team cannot make flags inaccessible (Do not encrypt, lock, or delete flags)
11. Cannot disable SSH
12. Cannot use Fail2ban
13. No configuration changes during prebake time
14. No denial of service attacks
15. Red team cannot take services down, delete blue team tools, or capture flags during prebake time
16. No antivirus
17. Blue cannot attack red
18. Gray team may add more rules during the competition as needed.

**How scoring works:**

* Both teams start with 0 points.
* Services are scored on whether they are running or down. (75 pts per day)
  + For every 3 minutes a service is down red team will earn 1 point
  + For every 3 minutes a service is running blue team will earn 1 point
* Flags give red team extra points proportional to the difficulty of accessing the flag
  + If the flags remain uncaptured by the end of the competition, they are added to blue team score
  + Minus one point for every incorrect submission to the score engine

**Blue Team Specific Information:**

* All client machines will have 5 flags and you are in charge of hiding them anywhere in the system
  + If they get found by Tom, he will get a lot more points