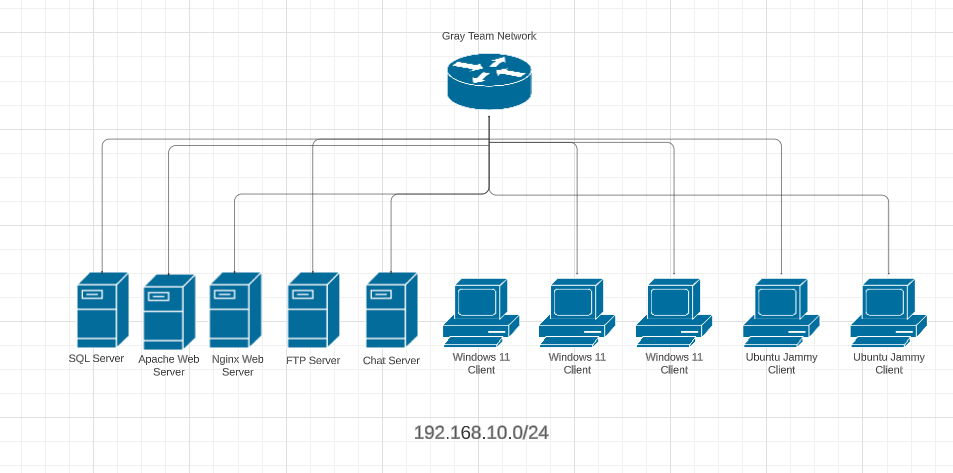


**Theme Description:**Welcome to the Tom & Jerry capture the cheese competition. For this competition the red team will be referred to as “Tom” and the blue team will be referred to as “Jerry.” The goal of the competition is for Tom to not only take down Jerry’s services, but also take his cheese! On 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 accounts (ubuntu & windows)(low privilege):

Username: mousecostume

Password: catinside

Rocket Chat:

Number is 1-5

Username: Red[Number]

Email: Red[Number]@hotmail.com

password: RedTeam1!

Admin Account

Username: RedAdmin

Email: RedAdmin@hotmail.com

password: RedTeamAdmin1!

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. Bricking machines is not allowed (on purpose, be smart)
5. Breaking the rules will result in some point deduction (as determined by the Gray team)
6. Tools, techniques, or services that render an entire machine’s files/information completely immutable or inaccessible during the competition is prohibited
7. Blue team may not make fake flags.
8. Cannot disable SSH or lock the blue team out of boxes completely
9. Cannot use Fail2ban
10. Cannot make flags inaccessible (Do not encrypt, lock, or delete flags)
11. No configuration changes during prebake time (only addings tools, can’t uninstall, remove blue team tools, add users, change passwords)
12. No timed tasks during pre bake
13. No denial of service attacks
14. Red team cannot take services down, delete blue team tools, or capture flags during prebake time
15. No antivirus
16. Blue cannot attack red
17. No deleting services as a whole (ie. no making it so that services can't be rebuilt)
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
  + Access Code to submit flags in the scoring engine: TomTheCat

**Red Team Specific Information:**

* HINT: Most machines will have flags in either services or the file system (Do recon before taking down services)
* If you think of anything you want to try that might not specifically be in the rules (for example physical attacks), just ask us if you can do it.
* Flags exist within services…if you stop the services you may lose the ability to gain points from flags. Consider doing recon on flags first before shutting services down!
* Security Groups
  + Create a security group in openstack
  + Total of four rules
    - Every rule is “other protocol”
    - Two rules for 192.168.10.0/24 (one ingress and one egress)
    - Two rules for 192.168.20.0/24 (one ingress and one egress)
    - Every IP protocol set o “-1”
    - Remote set to CIDR
  + Make sure to apply the Security Groups before the competition starts