King’s Cache Casino

Gray Team Packet

Team Alpha:
Amour Narcisse Thompson, Brennan Kane, Daniel Railic, Ethan Wolman, Gavin Monick, Gina O'Shaughnessy, Jacob Robertson, Krzysztof Grochal, Roberto Reade, Ryan Clancy

Table of Contents

Background:

At the lavish King’s Cache Casino, the infamous hacker group, The Red Team, has issued a bold challenge, threatening to breach the casino's legendary encrypted vault and steal its digital treasures. The casino’s elite cybersecurity team, The Blue Team, is tasked with defending the vault, knowing that if the attackers succeed, it could ruin the casino’s reputation forever. The race is on in this high-stakes cyber battle to see whether The Red Team can crack the vault or if The Blue Team can outsmart them and protect the casino's secrets.

Executive Summary:

In this casino-themed cybersecurity competition, two Blue Teams are tasked with defending their respective systems, while a Red Team is focused on attacking and exploiting vulnerabilities. The competition follows a Capture the Flag scoring format, where points are awarded based on successfully identifying and exploiting weaknesses or preventing attacks. The competition simulates a high-stakes casino environment where participants must defend critical infrastructure and sensitive information against ongoing attacks.

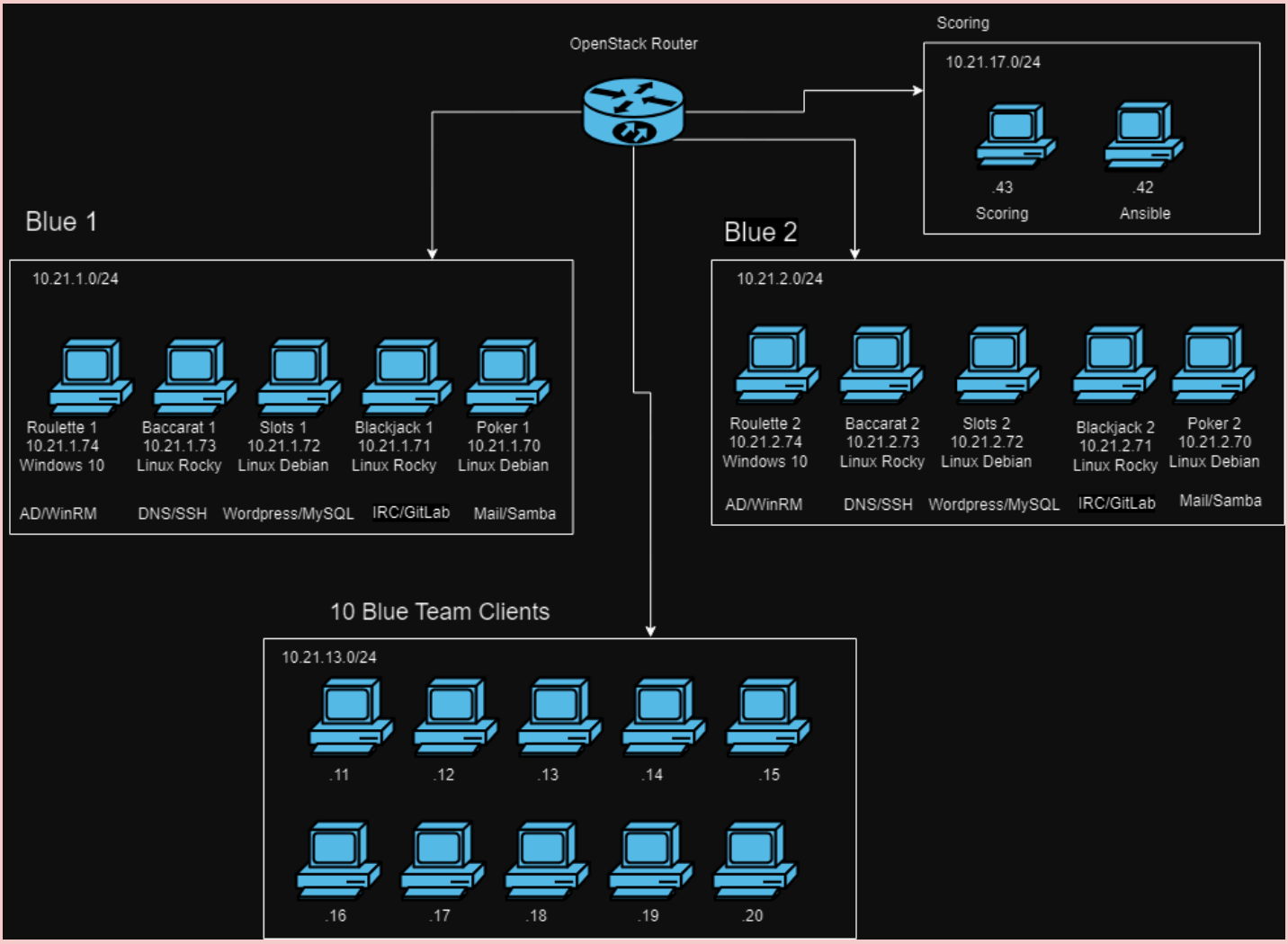
Blue Team:

The Blue Team will be split into two groups, each given access to an image of the same virtual machines. The Blue Team is responsible for defending and securing systems against attacks. The overall goal of the Blue Team is to prevent the impact of attacks launched by the Red Team.

Red Team:

Red Team will attack both of Blue Team’s machines, which are the same but in different machines. During the competition, Red Team should aim to simulate an offensive attack on the various systems and networks which can be done through exploitation, privilege escalation, data exfiltration, and lateral movements throughout the network. The Red Team's overall goal is to challenge both the Blue Team's defenses by exploiting vulnerabilities, gaining access, and potentially stealing "flags" while avoiding detection and containment.

Topology:


OpenStack Router
Scoring
10.21.17.0/24
.43
Scoring
.42
Ansible
Blue 1
10.21.1.0/24
Roulette 1
10.21.1.74
Windows 10
AD/WinRM
Baccarat 1
10.21.1.73
Linux Rocky
DNS/SSH
Slots 1
10.21.1.72
Linux Debian
Wordpress/MySQL
Blackjack 1
10.21.1.71
Linux Rocky
IRC/GitLab
Poker 1
10.21.1.70
Linux Debian
Mail/Samba
Blue 2
10.21.2.0/24
Roulette 2
10.21.2.74
Windows 10
AD/WinRM
Baccarat 2
10.21.2.73
Linux Rocky
DNS/SSH
Slots 2
10.21.2.72
Linux Debian
Wordpress/MySQL
Blackjack 2
10.21.2.71
Linux Rocky
IRC/GitLab
Poker 2
10.21.2.70
Linux Debian
Mail/Samba
10 Blue Team Clients
10.21.13.0/24
.11
.12
.13
.14
.15
.16
.17
.18
.19
.20

Boxes:

Debian Boxes	Rocky Boxes	Windows Boxes
1. Mail	1. IRC	1. AD
Samba	GitLab	WinRM
2. Wordpress	2. DNS	
MySQL	SSH	

Credentials:

Name	User	Password
Mysql Users	root myuser	4dvantagePlayer$ myuser
Wordpress User	person	password
Linux Login	casino_user casino_admin	casino_user casino_admin
Scoring Login	Team 1 or Team 2	Changeme123!
Windows	Administrator	password1234%
Services	user	password1234%

Blue and Red Team cannot touch: pitboss, ansible, & gray
Red Team cannot touch: any Blue Team workstation

Rules:

1. Do not interfere with scoring.
2. The Blue Teams cannot attack the Red Team.
3. Teams are required to keep all services and applications operational while defending against attacks. Disabling or shutting down any app or service to prevent red team access is not allowed.
4. Physically tampering with any devices is strictly off-limits. No USBs or repos may be used during the competition.
5. Blue Team cannot download packages unless Gray Team allows it.
6. Red Team cannot permanently render a box unusable or service unfixable.
7. Only tools pre-approved by Gray Team may be used during the competition.
8. Do not modify network settings.
9. Any competitors on the Red Team and both Blue Teams may not attempt and/or perform any attacks or build additional defense outside of in-class competition time. Additionally, neither team may try to gain private information about the competition outside of in-class time.
10. No misconduct toward other teams or teammates, including acts of sabotage, harassment, or disruptive behavior, will be tolerated.
11. One warning will be given for violating the rules. After the first warning, you will be asked to leave the competition.
12. Red Team cannot change Blue Team passwords
13. Gray Team reserves the right to change, add, or remove these rules at any time during the competition.

Scoring:

- Overall, there will be 1 flag per scored box, totaling 5 flags.

Red Team:

1. Each flag captured from a service is worth between 10 and 50 points per 30 seconds.
2. Flags captured will be tallied after each day of competition.
3. Each service will be checked every 30 seconds, and Red Team will be awarded points if the service is offline.
4. Points for service downtime will be announced at the end of the competition.
5. They must find CTF prompts for the Red Team. Each flag is statically assigned and worth 200-800 points based on how long it takes to find and how hard it is to achieve.

Blue Teams:

1. Each service will be checked every 30 seconds and be awarded points if the service is online and accessible by the scoring engine.
2. Points will be tallied at the end of the competition.
3. Flags cannot be moved, and a defense has been pre-built around them.

Win Conditions:

- The Red Team wins if they have more points than both Blue Teams combined.
- If Red Team doesn’t win the Blue Team with the most points will be the winner