IRSEC

PROM 2019

Blue Team Packet 1.0

Our Sponsors

Platinum

Gold

Silver

Bronze

Students,

Prom is finally here! I know you are all very excited to stand on opposite sides of the room on your phones, occasionally glancing towards the dance floor. For the time that you do spend on your phone, we have some fun things set up for you to use. At the end of the night, we will be crowning our prom royalty. How exciting!

However, as some of you know, there are some athletes who are very upset that their choice couple may not win this year's crowns. They will be very disruptive during prom, and it is your job to stop them.

Good luck, and go Wildcat5e!

Shane Oldman, Principal

Schedule

Time	Details
08:00 - 08:15	**Breakfast** ● Golisano 1400 ● Donuts, bagels, and coffee will be provided for participants and sponsors
08:15 - 09:00	**Keynote!** ● Golisano 1400 ● Join us for a talk with a very special guest.
09:15 - 12:00	**Competition Part 1** ● Golisano, Net Lab & Sys Lab ● Round 1
12:00 - 13:00	**Lunch** ● Golisano 1400 ● Pasta, salad, and other food will be provided for participants and sponsors
13:00 - 17:00	**Competition Part 2** ● Golisano, Net Lab & Sys Lab ● Round 2
17:00 - 18:00	**IR Report** ● Golisano, Net Lab & Sys Lab ● Valuable time to gather data and put the finishing touches on your IR report ● Red Team cannot attack you during this time
18:00 - 18:30	**Red Team Debrief** ● Golisano 1400 ● An explanation of why things were on fire, by the Red Team
18:30 - 19:00	**Award Ceremony** ● Golisano 1400 ● Winners and prizes!

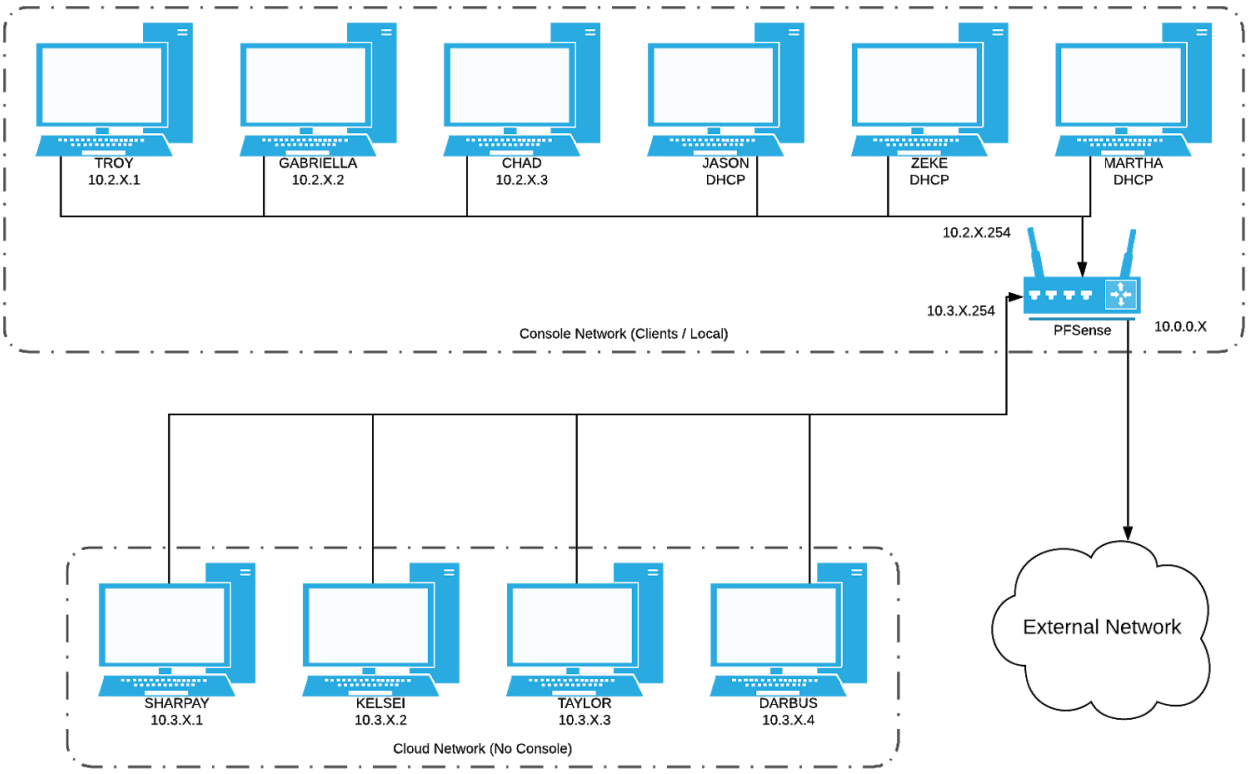
School Policy

Please read and follow all rules while attending the prom, failure to do so could result in expulsion, or worse.

- This is a defense only competition. There will be no attacking by any blue team under any circumstance. The Red Team are the only ones who will be performing attacks.
- Attacking White Team infrastructure will result in elimination from the competition.
- Attacking Blue Team infrastructure will result in immediate elimination.
- All devices should be pingable at all times. This means no disabling your NIC.
- You cannot block entire subnets or ranges of IP addresses, but you may block individual IP addresses. Expect severe point deductions if we find out you've been blocking subnets.
- Entering the Red Team room (Air Gap) is prohibited.
- Food is to be eaten in the designated rooms only. No food will be allowed in the labs.
- You are allowed, and encouraged, to use printed aids.
- You are allowed to pre-stage scripts on public sites such as GitHub, so long as the scripts are also public (i.e. you do not need to log in to reach them).
- Do not log into personal accounts on any competition machine; you've been warned.
- Physical host machines are not in scope of attack for Red Team.
- Splunk servers are not in scope of attack for Red Team.
- Red team can be trusted when they are inside of SysLab or NetLab. When communicating with them over the phone or computers you should not assume that they are trusted.
- Have fun!

Network

Everything in this diagram is subject to change :)



Hostname	Services	OS	IP
troy	AD/DNS	Windows Server	10.2.X.1
gabriella	Mail	Fedora	10.2.X.2
chad	MSSQL	Windows Server	10.2.X.3
jason	ICMP	Win 10	DHCP
zeke	ICMP	Win 10	DHCP
martha	ICMP	Solaris 10	DHCP
sharpay	HTTP	Ubuntu	10.3.X.1
kelsi	Voting App	Linux	10.3.X.2
taylor	DNS	CentOS	10.3.X.3
darbus	HTTP	Ubuntu	10.3.X.4
splunk	**Logging**	**Out of Scope**	**10.3.X.5**

Users

When in doubt, use this account.

Name	Pass	Sudo / Admin
principal	Changeme2019!!	Yes
chaperone	Changeme2019!!	Yes
deejay	Changeme2019!!	No
kid_with_sweatpants	Changeme2019!!	No
prom_king	Changeme2019!!	No
prom_queen	Changeme2019!!	No
dbadmin	Changeme2019!!	Yes

Solaris is special.

Name	Pass	Sudo / Admin
princip	Passw0rd-123	?
chap	Passw0rd-123	?
queen	Passw0rd-123	?
king	Passw0rd-123	?
deejay	Passw0rd-123	?
sweats	Passw0rd-123	?

Incident Response (IR)

If your team has noticed incidents caused by the Angry Jocks™, please submit an incident response report. Please include your team number - without it, you won't get any points. See the CCDC IR template in the Resource page for reference.

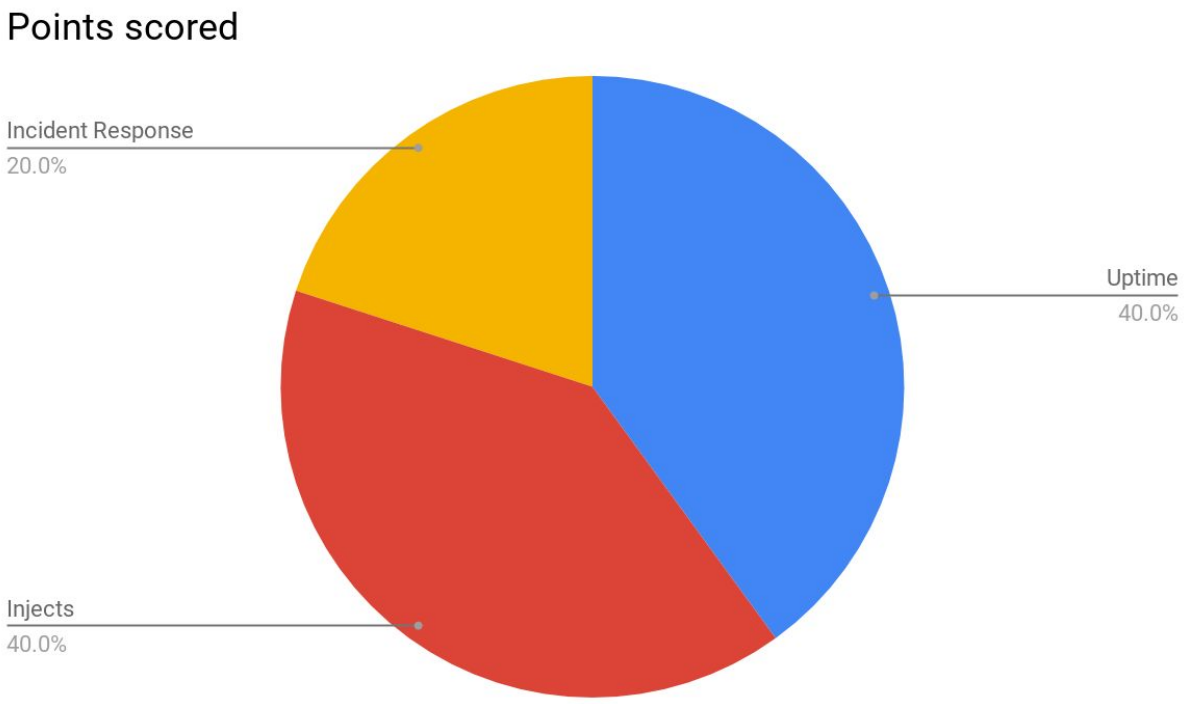
Incident reports must contain a description of what occurred, how the Red Team was able to get in, a discussion of what was affected, and a remediation plan. The more complete and accurate your report is, the better it will be scored, but there will be partial credit awarded if the report meets enough criteria. Submitting an incident report without all of the relevant data is better than not submitting a report at all, but if the report is missing too much information it will not receive any credit. Screenshots may be submitted for evidence of the incident but are not required.

Below are items you should strongly consider including to receive maximum credit for your reports:

- Attacker IP address(es)
- Timelines of activity
- Level of access obtained by the attacker
- IP addresses and/or hostnames of affected machines
- How the attacker gained access
- Description of attacker activity (ie passwords cracked, files affected, services affected, data lost or defaced, etc.)
- Steps to remediate the incident

For your convenience, we have set up a Splunk server on your network to consolidate logs.

Scoring



Uptime - 40%

Making sure everyone has a great prom experience is our top priority. If services aren't working as expected, our guests won't be able to perform important functions during the event. How will prom royalty be decided?! Just because a service is listening on a port does not mean it is functioning as expected. Check the scoring engine OFTEN!

Injects - 40%

Our principal is already very uptight about the event. Keeping him (and other teachers/administrators) pleased throughout the event is imperative. These tasks will be graded by the chaperones (white team) during the event. If your team is unable to finish a task, you MUST make the task-giver aware of this.

Incident Response - 20%

Those evil jocks ruin everything! Let's make sure we have some evidence of what they did when it's all over. Submit reports as you find things, using the template below or similar.

Student Credit

Your team has saved up quite an impressive amount of credit for the student store during the school year; a total of **1350 CATBUX** We have some fun activities and options for you to spend that during prom!

White Glove Service - 100 CATBUX
One member of a team of your choice gets to wear a pair of stylish, elbow-high white gloves for 5 minutes.

Hit the Dancefloor - 300 CATBUX
Two members of a team of your choice gets to dance to a song of your choosing, for up to 3 minutes.

Revert to Snapshot - 500 CATBUX
Lose access to a machine? Worry not! Reset the machine to its original competition state.

Superintendent Visit - 500 CATBUX
Get help from a sponsor of your choice.

Parent Phone Call - 500 CATBUX
Extend the due date of an inject of your choice by up to an hour. This may not extend past the end of the competition.

Tryouts - 750 CATBUX
Get help from a Red Team member of your choice. They can walk you through a process verbally, but may NOT put hands on keyboard.

Resources

CCDC's IR Template
https://tinyurl.com/y98ftv4n

Week 3 - Advanced Networking
https://tinyurl.com/y45axubl

Week 4 - Advanced Linux
https://tinyurl.com/y24muwda

Week 5 - Advanced Windows
https://tinyurl.com/y5h8mtgg

Week 8 - Blue Linux
https://tinyurl.com/y4u9w53u

Week 9 - Blue Windows
https://tinyurl.com/y54akrjs

Week 10 - Red Linux
https://tinyurl.com/y2vrkfzx

Week 11 - Red Windows
https://tinyurl.com/y2etqszs