**Red Team vs Blue Team**

1. The link below is to a video that discusses the differences between red teams and blue teams.

[Red Team vs. Blue Team | How to Get Started in IT](https://www.youtube.com/watch?v=M9eOJ3abcJs)

As you watch it, pay close attention to the different terms used, what roles these teams play, and what value they add to an infosec environment.

2. Answer the following questions regarding red Teams and Blue Teams

What is a Red Team?

* The attacking team would serve as an ongoing threat to our system so that we can identify any weaknesses.

What is a Blue Team?

* The team that works as system defenders spend their days patching, upgrading, and looking for vulnerabilities.

List some ways that Blue Teams make their environment more secure.

* The Blue team secures their environment by examining configuration, updating firewall rules, and implementing IDs and IPS, which are intrusion detection systems. They also install malware endpoint protection on all workstations.

List the major activities that Red Teams perform.

* Assessments of vulnerabilities, vulnerability scans, and penetration testing are some of the main tasks carried out by the red team. They behave similarly to a PT (advanced persistent threat), breaking into systems and sticking around undetected.

What is the difference between a vulnerability assessment and a penetration test?

* A vulnerability assessment will just report on the vulnerabilities it finds; in contrast, a penetration test will determine whether any attack was available to the tester and will include that information in the report.

At this point in your journey, do you see yourself as more of a Red Team person or a blue team person? Why?

* Preferable on the blue team because it is pleasurable to defend the system, to look for vulnerabilities, patching, and upgrading.