RULE LIST FOR CTF Event

Web Based:

- Participants need to use their own device to access CTF.
- Participants need to find at least of **8 Vulnerabilities** to qualify for runner-up.
- For web-based CTF Participants needs to provide write-up for found vulnerability to qualify .
- Any Participants found cheating during CTF will be disqualified from event.
- Web-based CTF consists vulnerabilities from Beginner to Advanced Level (Starting from Admin Panel to RCE execution on server.)

Network Based:

- Participants Needs to connect to the IP Provided by CT University.
- There will be 5 Machine in the Network starting from Beginner to Advanced Level (Windows' & Linux Based)
- To qualify for network based CTF Participants needs to provide the captured **flag** with the name of machine & captured hash.
- Any Participants found cheating during CTF will be disqualified from event.

PCAP File Analysis:

- This event comprises of finding the credentials from .pcap file provided by CT University.
- Participants need to open and analysis .PCAP only in Wire shark.
- To get qualify for the runner-up, Participants needs to provide the found credential in a prescribed manner.

Hacking Game For CTF:

1. Web-Based CTF(Juice-Book hosted in-house)
2. Network Based CTF (7 Machine)
3. PCAP File Analysis. (9 files)