'Capture The Flag' Challenge
(16-17 October 2023)

COMPLETION REPORT

Submitted by:

       Cybersecurity Division
       Government Technology Agency
       Bhutan

1. Introduction

The Cybersecurity Division under the Government Technology (GovTech) Agency conducted CTF 'Capture The Flag' challenge in three colleges: College of Science and Technology, Jigme Namgyel Engineering College and Gyalpozhing College of Information Technology with the grant support offered by the Asia Pacific Telecommunity (APT) under APT Young Professionals and Students program. The Cybersecurity CTF program for college students was organized with the objective to introduce cybersecurity to the college students and develop future talent who can hopefully contribute to the cybersecurity workforce in future. The overall Cybersecurity CTF program consisted of a workshop introducing the basics of cybersecurity followed by a cybersecurity CTF challenge developed by the Cybersecurity Division, where the participants competed in a game-like competition to solve a variety of cybersecurity-related puzzles.

2. Event Details

The Cybersecurity CTF challenge took place from 16 - 17 October 2023, as a part of the National Cybersecurity Week 2023 program. It consisted of a hands-on workshop on introducing the basics of cybersecurity on Day 1 and Capture the Flag competition among the students on Day 2. The objective of the program was to develop the future cybersecurity workforce of Bhutan.

The opening session was graced by Mr. Masanori Kondo, Secretary General, Asia-Pacific Telecommunity (APT), Mrs. Shreya Pradhan, Assistant Project Coordinator, APT and Mr. Yeshi Dorji, Chief of Cybersecurity Division, Govtech Agency.
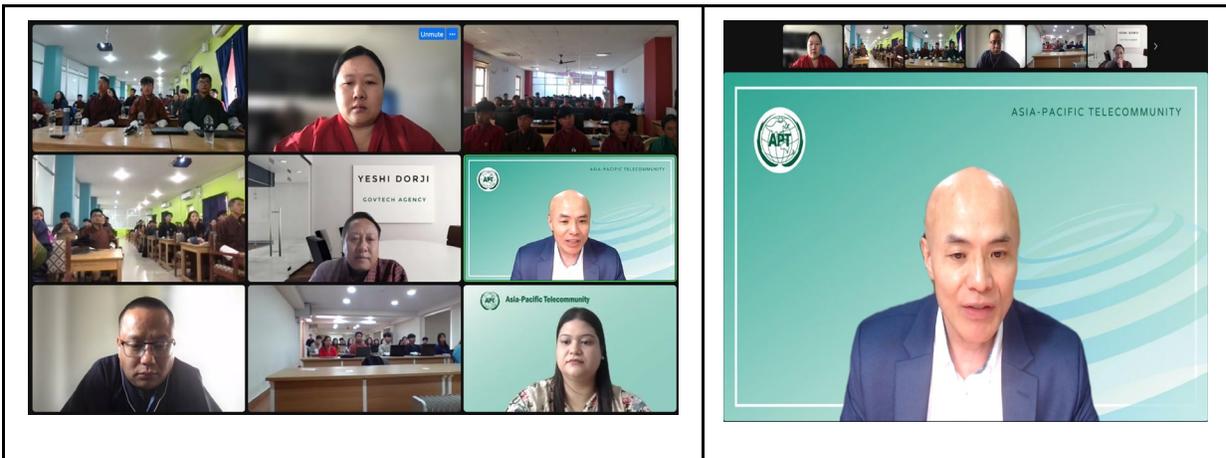

Figure 1: Opening session of the Cybersecurity CTF challenge program

The participants for the cybersecurity CTF program were students from College of Science and Technology (CST), Jigme Namgyel Engineering College (JNEC) and Gyalpozhing College of Information Technology (GCIT). In terms of participation, there were 40 students from CST, of which 5 were 3rd year students and the rest were final year students pursuing Bachelors of

Engineering in Information Technology. In addition, there were 50 students from GCIT studying Bachelor of Information Technology and Computer Science and the rest 48 were diploma students from JNEC studying Diploma in Computer system and Network.

Figure 2: Participants from College of Science and Technology with two resource persons from Cybersecurity Division	*Figure 3: Participants from Jigme Namgyel Engineering College with two resource persons from Cybersecurity Division*	*Figure 4: Participants from Gyalpozhing College of Information Technology*

2.1.   Day 01: Introduction to the basics of cybersecurity and Lab

The topics and the labs covered were:
1. Cyber Ethics & Cybersecurity Principles
2. Attackers and Attacks (Ransomware, Phishing, DDoS)
3. Attacker Motives with case study
   a. Financial Gain
   b. Curiosity
   c. To make a statement or send a message
   d. Steal sensitive and proprietary information
   e. Disrupt business processes
   f. Government espionage and secrets
4. Cyber Attacks
   a. Network attacks(DOS/DDOS, MiTM)
   b. Social Engineering(Phishing, Vishing)
   c. Physical attacks(Tailgating, Shoulder Surfing)
   d. Malware(Ransomware, Bots/Botnets)
5. Security Controls
   a. Anti-Virus
   b. Multi-factor Authentication
   c. Encryption
   d. Password Management
   e. Backups
   f. VPN
   g. IDS/IPS

      h. Firewalls
      i. Cryptography (Practical on Hash and Mailvelope)
6. Threats and Vulnerabilities
7. What is CVE?
8. Network Security
      a. Whois database exercises and Domain name system
      b. IP reputation Exercise
      c. Virustotal Exercise
      d. Packet analysis with Wireshark

The session for day 1 ended with a lab on NMAP scanner and a quick recap on the lessons and labs, where the students were asked to share a summary of topics covered.

2.2. Day 02: Capture the Flag

The day 2 started with officials from the cybersecurity division under GovTech agency doing a quick recap of Day 1 and briefing of the CTF challenge for the day. The Capture Flag Challenge included seven categories that were: General, Threat Intel, Basic Linux Command, PCAP, Cryptography, Recon, and Log Analysis.
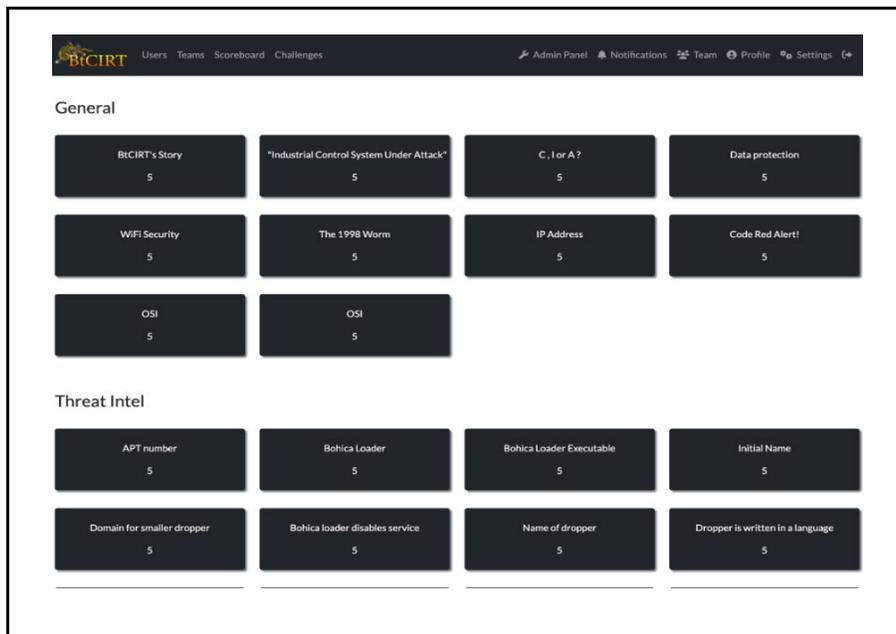
Figure 5: Challenge dashboard prepared by Cybersecurity Team.

The teams were formed in the following manner:
- 8 groups consisting of 5 members each for CST,
- 12 groups consisting of 4 members for JNEC, and
- 10 groups consisting of 5 members each for GCIT

All teams were asked to login and join their respective team in the CTF platform. The platform contained the Registrations page, Login page, Challenges (Problems to solve) and the Live

Scoreboard to trace the progress of each team. Every team was very competitive, and the winning teams were; Blue Pill from CST, Group 3 from GCIT and Hello world from JNEC.

Figure 6: CTF challenge in the action in the three colleges.

Prizes were provided to top positions and certificates were distributed beforehand to each participant prior to the closing ceremony to efficiently manage the time.

Figure 7: Simple certificate designed by BtCIRT, Cybersecurity Division
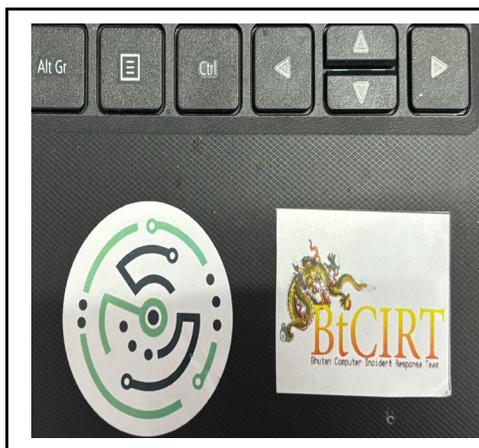
Figure 8: Stickers   *Figure 9: Pamphlets*

Winner from CST: Group 'Blue Pill'	*Winner from GCIT: Group 3*	*Winner from JNEC: Group 'Hello world'*

Figure 10: Photograph with the winners

3. Feedback from Colleges

The following are feedback received from the colleges:

a. Colleges have basic cybersecurity courses in their curriculum, hence advanced knowledge and tools could be introduced next time.

b. Create a cybersecurity community in the colleges to take up cybersecurity awareness within the college students and staff members.

c. Conduct workshops so that it does not overlap with the preparation of student's semester exams.

4. Conclusion

The Cybersecurity Division of the GovTech Agency successfully conducted a Capture the Flag (CTF) challenge from October 16-17, 2023, at three colleges in Bhutan: College of Science and Technology, Jigme Namgyel Engineering College, and Gyalpozhing College of Information Technology. The program was made possible by a grant from the Asia Pacific Telecommunity (APT) under the APT Young Professionals and Students program.

The challenge began with an introduction to cybersecurity concepts, followed by a competition in which participants solved a variety of cybersecurity-related puzzles. Winning teams were declared at the end of the competition. Following the conclusion of the program, the Cybersecurity Division is hopeful that the CTF challenge has managed to spark interest in the participants to pursue future cybersecurity studies and contribute to the vital cybersecurity workforce of the future.