W drugim etapie zostaną przygotowane pytania dotyczące wiedzy i umiejętności technicznych z Cyberbezpiczeństwa w ramach 5 zagadnień:

- Systemów Operacyjnych (Linux, Windows),
- Bezpieczeństwa Sieci Komputerowych,
- Kryptografii Stosowanej,
- Bezpiecznego Programowania,
- Bezpieczeństwa Aplikacji WWW.

Bardziej szczegółowa lista została przedstawiona poniżej:

1. **Systemów Operacyjnych (Linux, Windows):**

- Podstawy zarządzania systemem Linux,
- Zarządzanie użytkownikami oraz systemem plików,
- Konfiguracja usług w systemie Linux,
- Kodowanie i dekodowanie danych (różne algorytmy kodowania),
- Analizowanie dzienników zdarzeń,
- Zabezpieczanie systemu (tzw. system hardening),
- Zarządzanie pamięcią oraz procesami,
- Skrypty Bash automatyzujące zarządzanie systemem operacyjnym,
- Audyt bezpieczeństwa systemu operacyjnego.

2. **Bezpieczeństwa Sieci Komputerowych:**

- Podstawy komunikacji sieciowej,
- Skanowanie usług sieciowych,
- Identyfikacja wersji oprogramowania ,
- Kontrola i blokowanie przepływu danych,
- Protokoły internetowe,
- Protokoły poczty,
- Bezpieczna komunikacja oraz przechwytywanie połączeń.

3. **Kryptografii Stosowanej:**

- Funkcje hashujące,
- Szyfrowanie symetryczne,
- Szyfrowanie asymetryczne i podpisy cyfrowe.

4. **Bezpiecznego Programowania:**

- Błędy implementacji (memory leak, przepełnienie bufora, integer overflow, format string attack),
- Zaciemnianie kodu,
- Przechowywanie sekretów,
- Podatności i łaty,
- Backdoory.

5. **Bezpieczeństwa Aplikacji WWW:**

- Bezpieczeństwo aplikacji Web,
- SQL Injection,
- Kontrola dostępu do funkcji i danych,
- Cross Site Scripting (XSS),
- Obsługa danych z niezaufanego źródła,
- Przetwarzanie złożonych danych,
- Błędy konfiguracji aplikacji.