Dear Participants,

We hope the amount of knowledge and concepts you gained from our recent, intensive bootcamp sessions has enlightened you. The journey thus far has been nothing short of remarkable, and now, it's your chance to apply that newfound expertise! We're thrilled to extend an invitation to you for the upcoming Cyber Security Hackathon hosted by CBC SIT.

Here are the key details you need to know:

Hackathon Details:

Prizes: We have some exciting prizes up for grabs:

1st Place: Rs. 3000
2nd Place: Rs. 2000
3rd Place: Rs. 1000

Team Size: You can participate as an **individual or form a team of 2**. Feel free to collaborate and bring your collective skills to the table.

Submission Format:

1) Use image files provided as mail attachments to solve the questions.
2) Prepare a Word file with a screenshot (use screen capture tools like Snipping Tool for Windows) of all questions from the problem statement.
3) "Save As" word file to PDF for easy evaluation purposes.
4) Prepare a PowerPoint presentation (not more than 5 slides) to showcase the method used to solve given questions.
5) All documents are to be zipped together into a single zip file, named as the name of a first-team member.
6) Upload this zip file to the Google form link attached below:

https://forms.gle/w11sXEj5vhTBJVGJ8

Hackathon Window: The hackathon will be open from **17 September 8 am, Sunday to 18 September 8 am, Monday 2023**. You have a full 24 hours to work your magic and come up with innovative solutions.

Results Announcement: Mark your calendars for September 20 as we'll be unveiling the hackathon results on that day.

Please Note:
To ensure fair competition and engagement, eligibility for the hackathon will be granted exclusively to students who attended both days of the workshop.

We have attached the Hackathon Rules, evaluation pattern, and Problem Statements to this email. Please make sure to review them carefully before you begin. If there are multiple students with the same marks, we will schedule a Google Meet for an interview as a tie-breaker.

17.09.2023 20-02:01:26pm

We encourage you to collaborate with your fellow participants, think outside the box, and have a great time while working on your projects. If you have any questions or need assistance during the hackathon, don't hesitate to reach out to us.

We wish you the best of luck, and may the most innovative and creative solutions win!

Let's make this hackathon a memorable and rewarding experience. Happy hacking!

Note:

1) Check Google form to understand the pattern of solution submission.
2) Read the instructions carefully. Contact the CBC team in case of queries before the start of the hackathon.
3) Solutions, like copy-pasted from websites, peers, or other participants or generated using ChatGPT or similar tools, will be considered plagiarism and participants will be disqualified from the hackathon.
4) All rights are reserved by the CBC committee and a panel of judges.
5) The decision of the judges and committee will be considered final.
6) Considering the process followed at SIT for cash prize distribution, a few documents of the winners will be required after the result declaration.
7) Prizes will be deposited to the account of the winner (in the case of a team, cash prizes will be deposited in only one participant's bank account).

127.0.0.1-2023.09.20-02:01:26pm

Warm regards,
CBC SIT Organizing Team

Cyber Security Hackathon Evaluation details:

1) Each correct answer for the Quiz in Google Form – 2 marks each.
2) PowerPoint presentation to explain the provided solution (maximum 10 slides) – For tiebreaker only.

In case of a tie between participants after evaluation of the provided solution – An interview using a point presentation submitted in point 3.

Cyber Security Hackathon Quiz

Solve the below questions using the Autopsy tool and note down all answers. Click the screenshot of every question one by one and paste it into a Word file for submission. During submission, enter your answers to fill in the blanks in Google form. Attack your zip file containing a PDF document of the screenshot of answers, and a presentation prepared as per the evaluation format mentioned above.

Before we begin the lab, make sure you download the attached images to use with Autopsy. If you want to confirm that you had no corruption, these are the MD5 values of the files:

- MD5 (device1_laptop.e01) = dc176d653c5613e305e831525e874090
- MD5 (device2_mediacard.e01) = c8343d3976eec2985e7580a2b6321591

We will now begin the analysis of the hard drive that was found in the dognappers car. At this point in the scenario, we haven't searched the house yet and therefore will not have access to the media card device. So, make sure you do not add that yet.

1. Launch Autopsy
2. Choose "Create New Case"
3. Make a case with the following information:
    1. Case Name: case1
    2. Base Directory: c:\ (or where ever you'd like to store the case)
    3. Skip case number and examiner
4. Add device1_laptop.e01 image as data source.
   ***** NOTE: Do NOT add device2_mediacard.e01 yet *****
5. Deselect ALL ingest modules.
   - As a reminder, this is not what you'd typically do. But, we are doing it this way for the course.
6. Finish Adding Image.
7. Open the "Data Sources" part of the left-hand tree
    1. **Question**: How many volumes does the disk image have?
    2. **Question**: What is the name of the unallocated space file in vol1?
    3. **Question**: Right-click on vol7 and choose "File System Details". What file system is in vol7?
8. In Windows, open "C:\case1" in a file explorer and observe its contents.
    1. **Question**: What is the database called?
    2. **Question**: Roughly how big is the database (in megabytes)?

---

1. Keep the same case open that you created in the last section. Let's look at the data in the tree.
    1. Question: By extension, how many databases are there?
    2. Question: What is the size of the largest database?
    3. Question: Are there any databases by MIME type yet?
    4. Question: What are the names of the files between 200MB and 1GB in size?

127.0.0.1-2023.09.20-02:01:26pm

We are now going to begin analyzing the laptop. We are starting off the case with some clues. Most notably, we have pictures that were sent with the ransom emails to Basis Technology

1. Keep same case open from previous lab, or reopen the case ("case1").
2. Right click on device1_laptop.e01 image in tree and choose “Run Ingest Modules”
3. Disable all modules except the following (we will pre-load some for the next lap):
    1. Hash Lookup
    2. File Type Identification
    3. Extension Mismatch Detector
    4. Embedded File Extractor
    5. Exif Parser (Picture Analyzer)
    6. Email Parser
    7. Central Repository
4. Configure the Hash Lookup module with two hash sets:
    1. Import the NSRL File (NSRLComplete.txt-md5.idx) that you previously downloaded in Section 1.
        1. You may need to unzip the file you downloaded.
        2. You can use the default values (i.e. Type: Known).
    2. Create a New Hash Set:
        1. Destination: Local
        2. Name: Ransom Case
        3. Hash Set Path: [Any folder on your computer]
        4. Type: Notable
    3. Use "Add Hashes to Hash Set" button to copy and paste the following MD5 value into the "Ransom Case" hash set. This is the hash of the ransom note.
    07c94320f4e41291f855d450f68c8c5b
5. Start the Ingest Modules.
6. Observe:
    1. Use Ingest Inbox as an indicator when ‘Known Bad’ hash hits are found.
    2. Use “Go To Result” to go to tree area of hash hits.
    3. View the hash hit.
    4. **Question**: Let ingest get at least 15% through the drive. How many total hits are found under the “Hashset Hits” results after running the Hash Lookup Ingest Module?
    5. **Question**: What are the filenames of the hash hits?
    6. One of the hits is in a folder named “Pictures”. Right click on the file to “View” there.
    7. **Question**: How many total ".jpg" files are in the folder “Pictures” where the notable hash hit was found?
    8. While reviewing the images in that folder, it is noticed that “IMG_20191024_155744.jpg” shows health violations by bringing the dog into a restaurant. We want to tag this as Notable:
        1. Right click on it
        2. Select “Add File Tag” and choose “Notable Item”

127.0.0.1-2023.09.20-02:01:26pm

Run ingest with only “Recent Activity” enabled.

1. **Question**: How many Web Bookmarks were found?
2. **Question**: What URL is a suspicious bookmark given the dognapping?
3. **Question**: What day are the cookies associated with the domain “youtube.com” from?
4. **Question**: What is the Value associated with the Name “identification” under Web Form Autofill?
5. **Question**: Under Web History, what day were the following Google Searches performed?
    1. “how to treat a dog bite”
    2. “how to make a ransom note”
6. **Question**: How many non-VM USB devices were attached to the system?
    1. NOTE: April 21, 2020: Some Linux systems are not getting a correct answer for this with Autopsy 4.14 because RegRipper cannot run. This problem was fixed in 4.15.
    2. We are hearing about some Windows systems where the UI does not show the device IDs (but they are saved into the case database). You can then re-open the case and see the results. We are investigating why this happens.
7. **Question**: How many file(s) is/are currently in the Recycle Bin?
    1. What was likely the original name of the file(s)?
8. **Question**: Under Accounts, what is the username associated with the Twitter account found on the device?

We will now run ingest and prepopulate with keywords that we already know about the case.

1. Run ingest with “Keyword Search” enabled.
    1. Create a keyword list with the following words:
        1. Exact Match Keywords:
            1. renzik
    2. Configure to update every 1 minute (so that you don’t have to wait too long - change it back after).
2. Start Ingest.
3. After it runs for a few percent of the files, you should see some hits. They honestly aren’t that exciting, but they are good enough for this lab. There are more relevant ones if you let it run until 15% or so.
4. **Question**: There are references to a document with renzik. What is the name of the file?
5. **Question**: How many hits are there for “Renzik” in NTUSER.DAT?
6. Don’t forget to change your keyword search periodic timer back to 5 minutes.

127.0.0.1-2023.09.20 02:01:26pm

At this point in the scenario, the police have searched the house and, with the help of Siri the electronic sniffing K9, found a media card. We will add that to our case and find some correlations.

1. Add device2_mediacard.e01 as a new data source (NOTE: We already added the device1_laptop.e01 data source to the Central Repository during the Hash Lookup Lab)
2. Right click on device2_mediacard.e01 and run Ingest Modules, with the following enabled:
    1. Hash Lookup
    2. Exif Parser
    3. Central Repository
3. **Question**: Was an Interesting Item created because a file on the media card was previously marked as notable?
4. **Question**: The picture on the laptop had a created date of 2019-11-01. What is the created date (in YYYY-MM-DD format) on the media card?
5. **Question**: How many total .jpg files are in the same folder as the Notable file?
6. **Question**: Look at the Other Occurrences tab for that file to see if it showed up anywhere else in this case with a different name. If it was, what is the other name?

127.0.0.1-2023.09.20 02:01:26pm