Chakra - Round 1 - Technical Challenge

Some general notes:

- You have 24 hours from sending this email to complete the challenge.
- DO NOT share this with others (regardless of whether they are attending the interviews or NOT)
- Reply here ASAP if you did not get the PCAP file (one each) that you need for the exercise
- Email ASAP if you have any issues with the links or if there is an error in questions
    - Outside of issues with questions, we won't be able to provide additional help or hints
- When you are done, reply to this email with your source code files and answers to the questions in a Word document/PDF. For Tasks 1 and Task 4 it is mandatory that you perform a screen recording of you providing a demo of you completing the task. This video should be shared along with the responses.
- If you get help from others, we will find that out in the subsequent rounds and will be immediately disqualified. So be genuine in doing these tasks yourself
- Here is the breakdown of the points. For each task you will get points based on how much you have completed (for example, if you did 50% of the task, you will get 50% of the points). Choose which tasks wisely based on your strengths:
    - Task 1 - 35 points
    - Task 2 - 15 points
    - Task 3 - 30 points
    - Task 4 - 35 points

TASK 1: Android Development

Develop an Android application with the following features. It is totally up to you to pick the platform to do the development (Flutter / Native Android / other).

Required Features

1. The app should connect to a REST API endpoint running locally on your laptop (consider the endpoint a simulated backend). REST API calls from the app can be simple GET calls that fetch a hard coded list of items (e.g., list of books).
2. The app should have the following buttons and upon pressing each of the buttons, it should perform the following:
   "Camera" -> clicking it should request the user for Camera permissions
   "Mic" -> clicking it should request the user for Mic permissions
3. The app should list the names of all the (other) apps installed on the phone.

NOTE: For all this task, you need to do a screen record of you running the code and providing a demo of the project working. This video should be shared along with the source code files.

TASK 2: Log Analysis with Grep

Prerequisite (required):

- For this exercise, you will need a system where the command *grep* can be run
- This can either be done directly with a *Nix OS OR through utilities such as Cygwin on Windows that will let you run Linux commands
    - Alternatively, on Windows, you can enable the Linux subsystem and enable one of the Linux OSs

Background

- In the world of Incident Response, oftentimes, you will need to work with large logs and you need to be able to analyze those logs quickly without having to load them in another tool
- Linux offers a variety of tools that support log analysis, chief of them being grep

- Type *man grep* on any Linux terminal and you will find all the options that can be used with the command. There is also a lot of open-source help available such as this one
- For this exercise, you will need to download the dataset from here. This is an OpenSSH server's log files meaning all SSH activity for that server will be logged here (e.g., successful login of a user over SSH)

Tasks

1. Threat actors try to break in by attempting to use common usernames and passwords. In this log, there were attempts to guess usernames. You can see this denoted by the entry "Failed password for invalid user….". Find the count of such attempts with grep
2. Assume your threat intelligence team told you that a threat actor targeted you exactly at Dec 10 11:00:00 (line 1524 in the log). Print 10 lines before and after this line with grep
3. There were several failed login attempts for the account "root". Use grep to list all the IPs from which failure occurred. Note the output should be a deduplicated list along with a count of their occurrences. For example, it should look like this, where the number of attempts from each IP is listed to the right.

   1.1.1.13 2

   8.8.8.8 8

   8.8.4.4 1

4. Sometimes the rhost field captures the full hostname instead of the IP address. For example, see the below line.

Dec 10 07:07:38 LabSZ sshd[24206]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=ec2-52-80-34-196.cn-north-1.compute.amazonaws.com.cn

Write a grep statement that filters based on Regex to look for instances where rhost contained a hostname as opposed to an IP. The output should only be a list of hostnames (don't want the full line). For example, the output should list something like this:

ec2-52-80-34-196.cn-north-1.compute.amazonaws.com.cn

5.36.59.76.dynamic-dsl-ip.omantel.net.om

5. For entries such as the following with “Bye Bye”, we want a deduplicated list of all the port numbers in the previous line along with their count of occurrence. Hint: you may need to pipe the output of one grep into another grep.

Dec 10 11:00:58 LabSZ sshd[25289]: Failed password for root from 183.62.140.253 port 50953 ssh2

Dec 10 11:00:58 LabSZ sshd[25289]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]

Output should look something like:

<port number a line before Bye Bye> <count of occurrences>

50953 23

50951 12

50943 9

NOTE: For all the questions in this section, you need to provide the exact commands that you used share it in a text document / Word file, and respond back

Task 3: PCAP analysis

Prerequisite (optional): Setup a Sandbox

- For this challenge, it is safer to do it in a sandbox environment considering you will be working with real malware
- There are multiple tutorials on how to set this up online
- Use Virtual Box (link) and download and install an OS of your choice and then install WireShark. If you have not already, you need to turn on Virtualization on that hardware level (you can Google how to turn on Virtualization for your laptop/desktop)
- Make sure to turn off the virtual network adapter to ensure the VM does not have connectivity to your host machine/internet

Background

- Download and install Wireshark (link here)
- Understand the basics of Wireshark and how to filter with the tool. There are tons of tutorials online, so pick what fits you. You can find the official documentation here
- Download the PCAP file attached to this email.

Tasks

1. Somewhere in the PCAP, there is a ZIP file that is downloaded
    - What is the name of the ZIP file?
    - Extract the ZIP file - what are the contents of the ZIP file?
    - Examine the contents of the extracted file: On a high level what does the file do? (e.g., does it download another subsequent malware?)
2. There is something fishy about the IP address 72.5.43.29. Based on the traffic to that IP, what is the suspicious activity?
3. Based on the activity from the previous question, can you deduce the variant of the malware infection that we are dealing with? Provide details on how you deduced the malware variant.

NOTE: For all the questions in this section, you may type your answers in a text document / Word file and respond back.

Task 4: Vulnerability Scan and Exploiting

The goal is to Install and use NMAP and Nessus tools to perform operating system fingerprinting and vulnerability analysis. Once you have identified the target environment, use Metasploit to take advantage of the identified vulnerabilities and gain access to the systems.

Requirements:

1. You need a device (host machine) to be able install and run Virtual Machines
2. Setup the Metasploitable virtual machine (link) on your host machine
3. Setup another VM your - any system where you can run NMAP (link) and Nessus (link)
    a. Using NMAP and Nessus, scan the Metasploitable VM to gain familiarity with how these tools operate and how to interpret their output
4. Install Metasploit - for this either reuse the VM in step #3 or setup a new VM
5. Tip: there is a lot of tutorials online for this exercise on Youtube and other online places

Task:

1. Using NMAP or Nessus, find the exact operating system version of the Metasploitable VM
2. Using NMAP or Nessus, how many vulnerabilities can you identify on the Metasploitable VM? List them.
3. Use Metasploit to exploit at least one of the identified vulnerabilities on the target system.

NOTE: For all the questions in this section, you need to do a screen record of you completing each of the tasks. This video should be shared along with the source code files.