DAILY ONLINE ACTIVITIES SUMMARY

Date:	**30-05-2020**	**Name:**	**PRASANNA**
Sem & Sec	**8th,B**	**USN:**	**4AL16CS068**

Online Test Summary

Subject	----------		
Max. Marks	-------	**Score**	--------

Certification Course Summary

Course	**Introduction to ethical hacking**		
Certificate Provider	**Great learner academy**	**Duration**	**6 Hrs**

Coding Challenges

Problem Statement: prob1- ***To print Fibonacci series for given range***

Status: Solved

Uploaded the report in Github	**Yes**
If yes Repository name	**prasanna_p**
Uploaded the report in slack	**Yes**

Online Test Details: (Attach the snapshot and briefly write the report for the same)

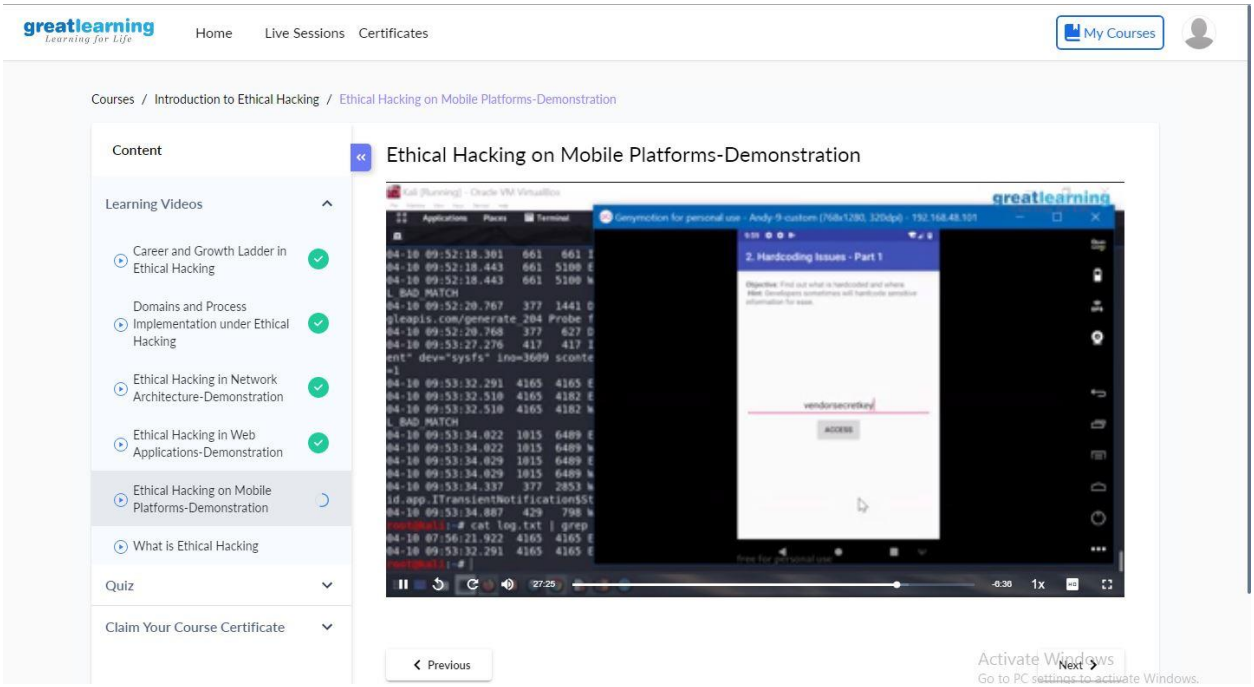
Certification Course Details: (Attach the snapshot and briefly write the report for the same)

Coding Challenges Details: (Attach the snapshot and briefly write the report for the same)

1. Certification Course Details:

Ethical hacking on mobile platform:

Mobile devices are used for our most sensitive transactions, including email, banking, and social media. But they have a unique set of vulnerabilities, which hackers are all too willing to exploit. Security professionals need to know how to close the gaps and protect devices, data, and users from attacks. Join author Malcolm Shore as he explores the two dominant mobile operating systems, Android and iOS, and shows ways to protect devices through analysis and testing. Watch this course to review the basics of mobile OS models, the toolsets you need for testing, and the techniques for detecting and preventing the majority of security flaws.



Hackers use Mobile Devices to hack other systems. Because there are tools supported by mobiles and even EC-Council started their own Mobile Hacking devices called the “Storm”. Now, let me move to the introduction to Mobile Hacking. Mobile hacking is one of the new horizon for hackers. Where data decides per use. Now data is used by the Mobile Devices but where does the data reside? The data moves over network, data can be stored permanently over storage devices, Now the data has to be secure.

Now the hacking when it happens There are few common attacks that also happen over mobile devices. All computer systems are over any other smart platforms. Data exfiltration extracted from Data stream and email, screen capture, copy to the USB keys . Now, this all things come under data exfiltration. Where it may be a link to the organisational data . And your organisation will lose their data the matter will come under confidentiality, integrity, availability of losing the data. And company me lose everything out of it.

Now I will look into the Android OS architecture there will be 4 different layers You will find the application layer, application framework Libraries and the Linux Kernel The application layer is where you are referring into the look and feel of the device Like home, contacts, phone, phone numbers, All browsers, these all things come under the application layer Where user in is interacting with the device Below that you will find the application Framework where lot of frameworks are running like API Which take the request from the user and give it to the kernel Now it is responsible for running all kinds of drivers That means you are come cameras. your Flash Memory. your binders. Keypads. WiFi drivers. audio drivers , power management.

These all things are going to run on top of it So there is a layer call library layer Which is defined according to the application and not according to the mobile device It helps to run the application independently or isolated So if anything will happen to the Slayer the application will crash. Show that how the Android OS layer works. Now let's see how a hacker can enter into this layer structure.

Now imagine a scenario where we are running an application and the application has Manual settings And on this application there is a Trojan behind and it is sitting on the Linux Kernel And

it is by passing your personal data like your camera or microphone Or something else which gives data to the attacker.

So that is where your device is going to be vulnerable and nowadays there is more than one vulnerabilities. Can talk about dos attacks sniffing over the networks or phishing, You can talk about the web application attacks on the normal application attacks Over the network can be possible.

2) Coding Challenges:

1. To display the Fibonacci series for the given range.

Pgrm1:

```
def FibRecursion(n):
   if n <= 1:
      return n
   else:
      return(FibRecursion(n-1) + FibRecursion(n-2))
 nterms = int(input("Enter the terms? "))

if nterms <= 0:
   print("Please enter a positive integer")
else:
   print("Fibonacci sequence:")
   for i in range(nterms):
      print(FibRecursion(i))
```