DAILY ONLINE ACTIVITIES SUMMARY

Date:	**31-05-2020**	**Name:**	**PRASANNA**
Sem & Sec	**8th,B**	**USN:**	**4AL16CS068**

Online Test Summary

Subject	**IOT**		
Max. Marks	**20**	**Score**	**20**

Certification Course Summary

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

Coding Challenges

Problem Statement: prob1- ***To print pyramid patterns***

Status: Solved

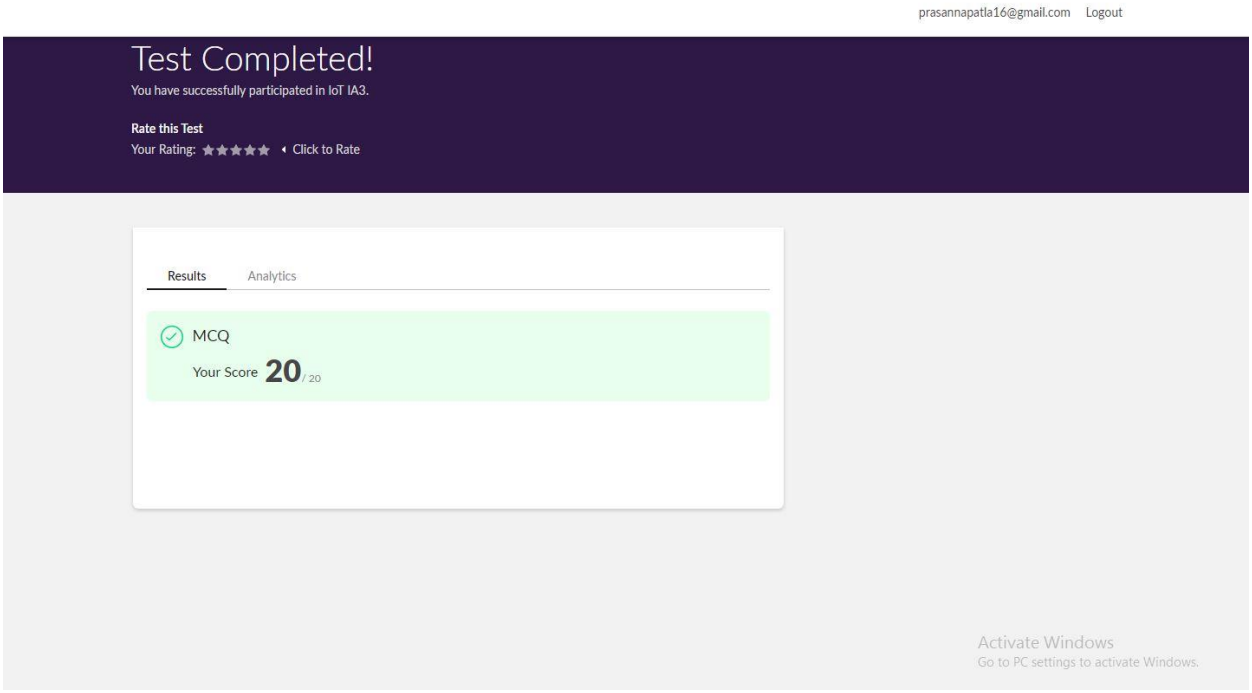
Uploaded the report in Github	**Yes**
If yes Repository name	**prasanna_p**
Uploaded the report in slack	**Yes**

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. Online test details:

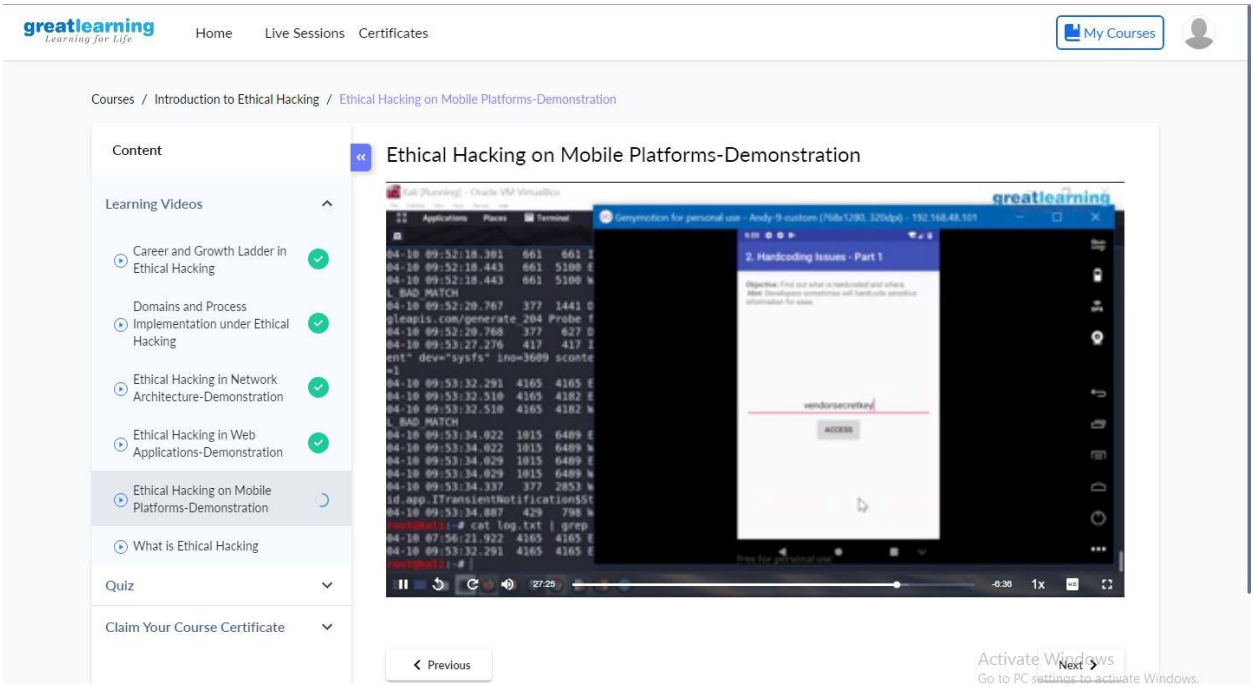


2. Certification Course Details:

Ethical hacking on mobile platform:

In a similar way iOS is also an architecture which is famous over the Apple platform Set also comes with multiple layers like the Android Operating System Architecture. Here the upper layer has the application Here the users will be interacting with the mobile directly. Here the Coco attach layer helps to create the look and feel. Or you can say it is a user interface kit. Below that is the media layer where you can find all the audios and videos. And the core service layer which take cares of the entire iOS architecture With the kernel based module This is a fully secured layer or the hardware layer which takes

care of the entire Operating system. This also connects with the core OS layer + Linux kernel.



So this is the lab environment which will be getting access to during your classroom training or CEH training. It's not only the mobile hacking tools you'll get 18 different tools to practice hacking. So let me quickly move to one of the last which is mobile hacking. Some connecting to one of the Android devices here and let me quickly put the IP addresses. So I'm just connecting this device to the network. I am giving the IP address to the simulator Over one of the Ethernet ports.

Now I will log in to the Kali Linux to create an exploit. This will be an APK backdoor vacancy Android operating system runs all the APK applications.

So I am going to create an exploit using a metasploit payload that is the MSF console. Now this will give me a remote access over Android on a particular mobile device. No the back door has been created successfully you can see it is on the desktop. Now I am quickly going to create a directory to share this backdoor to the Android device.

Now I am going to the web server where I will create the link and I will share this link to the social engineering methods Maybe I will spam it or send it over an email or make use of all the social Engineering. Now I'm going to install the application and I'm changing the settings so that I can install it over the web browser. I am changing the contacts as of now. so that anybody can access who is connecting over the web browser. and I am going to share this folder. I am pretty much time you are so I will just start the Apache server. and I will just copy the back door from the desktop.

Now I will move to MSFconsole to enable the handler so that whoever connect to this Android device can be handled by my Kali Linux machine. I am going for the river session and I am going to use reverse TCP here and I am going to keep the IP address of my Kali Linux machine so whoever is connecting to the system will connect to my Kali Linux machine. And now I'm going to create the exploit.

So now it is connected Now I am sending it to the Android device the Android device is a victim to me Here I will make the device run this back door As of now I am accessing things over the web browser normally it happens over spam How sending the links and making the user to click on it, there are multiple methods to do so. let me install the back door.

So once it is done on the device you can see the Kali Linux is got the response And I'm going to start the session. Now I got the access of the Android device. I can see the Android devices on my hand now now I can run the webcam or chat or list or check.I can also check whether it is a rooted device or not. I can also check their contacts or call logs anything.

I can also check the system information to cell information I can also execute Any commands I can download or upload anything. You can see here on the top I have multiple command which I can run . Speaking frankly the device is yours and you could do whatever you want. Hey this is the demonstration I have showed you that how an Android device is vulnerable to the back door.

2) Coding Challenges:

1. To display the pyramid patern.

Pgrm1:

```
rows = int(input("Enter the number of rows "))

for num in range(rows):

    for i in range(num):

        print(num, end=" ")

    print(" ")
```