

DAILY ONLINE ACTIVITIES SUMMARY

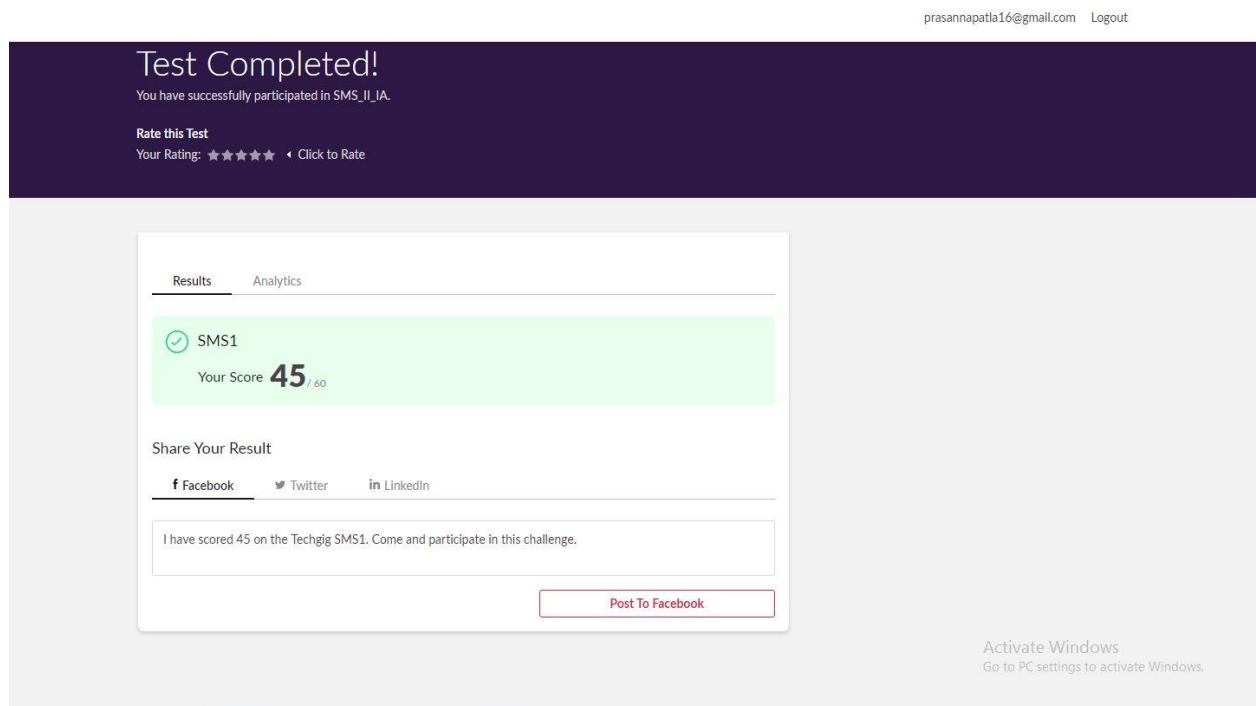
Date:	21-05-2020	Name:	PRASANNA
Sem & Sec	8 th ,B	USN:	4AL16CS068
Online Test Summary			
Subject	SMS		
Max. Marks	60	Score	45
Certification Course Summary			
Course	Introduction to ethical hacking		
Certificate Provider	Great learner academy	Duration	6 Hrs
Coding Challenges			
Problem Statement: prob1- Given an array ,rotate the array to the right by k steps , where k is non-negative			
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:

The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. In networking, devices on the same network communicate with each other using packets. If you send a video, login a website, sending chat messages sending email, all the data is send as packets.













 Home Live Sessions

My Courses 

 Introduction to Ethical Hacking Course In Progress

CONTENT ASSESSMENTS

Learning Videos

 Career and Growth Ladder in Ethical Hacking	18m	
 Domains and Process Implementation under Ethical Hacking	54m	
 Ethical Hacking in Network Architecture-Demonstration	48m	
 Ethical Hacking in Web Applications-Demonstration	50m	
 Ethical Hacking on Mobile Platforms-Demonstration	34m	
 What is Ethical Hacking	50m	

TCP 3-Way Handshake Process

This could also be seen as a way of how TCP connection is established. Before getting into the details, let us look at some basics. TCP stands for **Transmission Control Protocol** which indicates that it does something to control the transmission of the data in a reliable way.

The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model). The Application layer is a top pile of stack of TCP/IP model from where network referenced application like web browser on the client side establish connection with the server.

From the application layer,the information is transferred to the transport layer where our topic comes into picture. The two important protocols of this layer are – TCP, **UDP(User Datagram**

Protocol) out of which TCP is prevalent(since it provides reliability for the connection established). However you can find application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.

The Protocol Data Unit(PDU) of the transport layer is called segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), then receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received.

The screenshot shows the Great Learning website interface. At the top, there's a navigation bar with the Great Learning logo, 'Home', 'Live Sessions', a 'My Courses' button, and a user profile icon. Below this, a breadcrumb trail reads 'Courses / Introduction to Ethical Hacking / Ethical Hacking in Network Architecture-Demonstration'. The main content area is split into two columns. The left column, titled 'Content', contains a 'Learning Videos' section with a list of videos: 'Career and Growth Ladder in Ethical Hacking' (checked), 'Domains and Process Implementation under Ethical Hacking' (checked), 'Ethical Hacking in Network Architecture-Demonstration' (selected), 'Ethical Hacking in Web Applications-Demonstration', 'Ethical Hacking on Mobile Platforms-Demonstration', and 'What is Ethical Hacking'. Below the videos are sections for 'Quiz' and 'Claim Your Course Certificate'. The right column displays the selected video, 'Ethical Hacking in Network Architecture-Demonstration'. The video player shows a presentation slide with the following text: 'Computer 1 - Microsoft in Seattle', 'TCP/SMTP', 'HTTP/HTTPS', 'Data Packets - Label (Sender, Rec, Type of Data Packets)', 'Proxy Server (Masking and Filtering)', 'Router Switch (Routing and Shortest Path)', and 'Proxy Server (Masking and Filtering)'. Below the slide, it says 'Computer 2 - Google in India' and 'TCP/SMTP'. At the bottom of the video player, there's a status bar showing 'Ln 10, Col 37', '100%', 'Windows (CRLF)', and 'UTF-8'. A 'Previous' button is located at the bottom left of the video player, and an 'Activate Windows' watermark is visible at the bottom right.

Netdiscover :

The netdiscover is a tool which is used to gather all the important information about the network. It gathers information about the connected clients and the router. As for the connected clients, we'll be able to know their IP, MAC address and the operating system, as well as the ports that they have open in their devices. As for the router, it will help us to know the manufacturer of the

router. Then we'll be able to look for vulnerabilities that we can use against the clients or against the router if we are trying to hack them.

The **netdiscover** is a quicker and simplest program to use, but it doesn't show very detailed information about the target clients. It'll only show us their IP address, their MAC address, and sometimes the hardware manufacturer. We're going to use it by typing netdiscover, then we are going to use -r, and then we are going to specify the range, which can be any range we want. Looking at the IP (which is 10.0.2.1) tells us which network we are in. We want to discover all the clients that are in this network, so we're going to try and see if there is a device in 10.0.2.1.

Stealth Scan :

Stealth Scan - Computer Definition. Mechanism to perform reconnaissance on a network while remaining undetected. Uses SYN scan, FIN scan, or other techniques to prevent logging of a scan. See Also: Synchronize Packet (SYN); Synchronize Packet Flood (SYN Flood). Internet Security Systems.

To use Metasploit to perform a TCP stealth scan, you will need to have a remote system that is running accessible network services over TCP. In the examples provided, an instance of Metasploitable2 is used to perform this task ■

3) Coding Challenges:

Given an array, rotate the array to the right by k steps, where k is non-negative.

Example 1:

Input1: [1, 2, 3, 4, 5, 6, 7] and k = 3

Output1: [5, 6, 7, 1, 2, 3, 4]

Explanation:

rotate 1 steps to the right: [7, 1, 2, 3, 4, 5, 6]

rotate 2 steps to the right: [6, 7, 1, 2, 3, 4, 5]
rotate 3 steps to the right: [5, 6, 7, 1, 2, 3, 4]

Example 2:

Input2: [-1, -100, 3, 99] and k = 2

Output2: [3, 99, -1, -100]

Explanation:

rotate 1 steps to the right: [99, -1, -100, 3]

rotate 2 steps to the right: [3, 99, -1, -100]

Program :

```
def right_rotate(l,n):  
    result=[]  
    for i in range(len(l)-n,len(l)):  
        result.append(l[i])  
    for j in range(0,len(l)-n):  
        result.append(l[j])  
    return result  
k=int(input('enter a step to right rotate:'))  
l=[1,2,3,4,5,6]  
print(right_rotate(l,k))
```