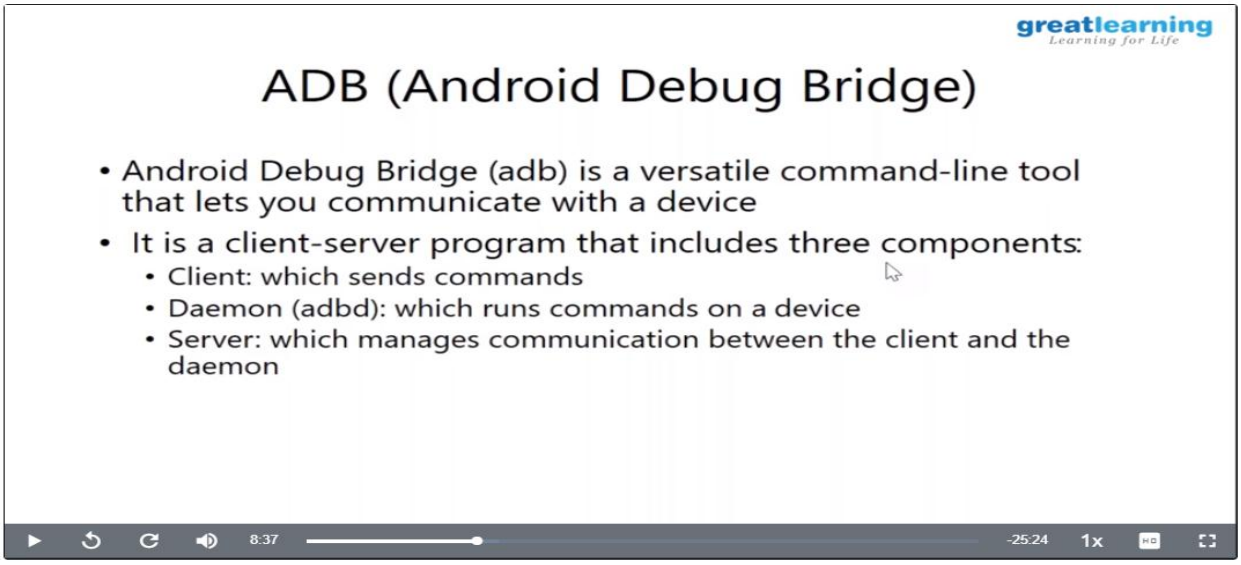
DAILY ASSESSMENT FORMAT

Date:	19 June 2020	**Name:**	Safiya Banu
Course:	Introduction to Ethical Hacking	**USN:**	4AL16EC061
Topic:	• Ethical hacking on mobile platforms - Demonstration • Ethical hacking in network architecture - Demonstration	**Semester & Section:**	8th sem "B"section
Github Repository:	Safiya-Courses		

Ethical Hacking on Mobile Platforms-Demonstration



Imagine an attack surface that is spread across your organization and in the hands of every user. It moves regularly from place to place, stores highly sensitive and critical data, and sports numerous and different wireless technologies all ripe for attack. Unfortunately, such a surface already exists today: mobile devices. These devices constitute the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

SEC575 Now Covers Android 10 and iOS 13

SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills to understand

the security strengths and weaknesses of Apple iOS and Android devices. Mobile devices are no longer a convenience technology - they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores across the world. Users rely on mobile devices more today than ever before -- we know it, and the bad guys do too. The SEC575 course examines the full gamut of these devices.

Learn How to Pen Test the Biggest Attack Surface in Your Entire Organization

With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and manipulate apps to circumvent client-side security techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS, and you'll bypass lock screen to exploit lost or stolen devices.

Take a Deep Dive into Evaluating Mobile Apps and Operating Systems and Their Associated Infrastructures

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review ways to effectively communicate threats to key stakeholders. You'll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks for in-house applications.

To be an EC Council Certified Ethical Hacker, you have to be thorough with the EC Council course materials. You should not only master the theoretical aspect of it but also the step by step implementation of all the processes.

Here’s a webinar video hosted 21st of November 2017 by Mr. Joe Davis, Business Manager, Americas and presented by Mr.Syama Prasad a Certified Ethical Instructor by EC Council.

Mr. Syama gives you a feel of working on iLabs. The access to this is provided along with the Training

and Certification course provided by GreyCampus.

In the video Mr. Syama covers:

- Collecting information from target websites (eg. session id, platform, technologies, organization details like email, phone number and fax) using firebug & web data extractor which demonstrate steps of Reconnaissance.
- UDP & TCP packet crafting techniques using hping3.
- Gaining windows 8 machine access using Metasploit exploitation toolkit.
- Maintaining access to system using spytech spyagent.