**DAILY ASSESSMENT FORMAT(DAY 5)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **21-June-2020** | **Name:** | **Bhuvanesh M** | |
| **Course:** | **Introduction to Ethical Hacking** | **USN:** | **4AL16EC015** | |
| **Topic:** | **Ethical hacking on mobile platforms - Demonstration** | **Semester & Section:** | **8th sem & ‘A’ section** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **Image of session** | | | |
| **Mobile Hacking Tools and Techniques**  GreyCampus brings forth yet another Webinar on one of the most trending topics of 2017, “Amazing Mobile Hacking Tools and Techniques”. We try and demonstrate the most popular attacks which can victimize even the best of the Computer Geeks. These attack techniques are not to be practised without any supervision.  GreyCampus gives you full access to the iLabs provided by EC-council to learn and practise various attacks as an Ethical Hacker. There are various modules and tools present in the iLabs which makes it a mandatory possession for every Ethical Hacking aspirant.  Below is the recorded version of the Webinar that was held on 15th of December 2017. ****TRANSCRIPT:**** Penetration testing is a first thing what I am going to discuss and then we'll go to introduction for mobile hacking then I'll give you some of the technique how the Android operating system works. And then will move to iOS architecture and then I will show you multiple hacking techniques and I am going to the demonstrate that thing over EC Council ilabs at the end I will take your query send feedback. Mobile phones are allowed under the “BYOD” policy, which stands for “Bring Your Own Devices”. This makes the vulnerable to leak their data and hackers are looking for such kinds of vulnerabilities or threats or mobile devices.  **Mobile Hacking can be divided into two categories:**   1. Hacking the Mobile Devices which the companies do. 2. Using the Mobile Devices for hacking.   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.  The next thing will be data tampering,  modification using another app Kind of trojans  or viruses worms  or rat programs. Now these things come under data tampering. Let me give you a small example  let us talk about the Trojan  suppose the Trojan has been wrapped with the  gaming program And people tend to play the games over mobile devices  now this may lead to some kind of internal operations On maybe Android or iOS device So you don't get to know that your device is sending multiple information like Videos of screenshots And these all things are moving over to the attackers phone over a small piece of code called Back door. There will be another kind of attack that you  where the data loss happens maybe loss of device. Your device has been changed to a break maybe on  probe access. This is kind of jailbreaking or rooting the device Or maybe there is the vulnerability over an application So this all things may lead to data loss. At the end of the day the  Malware is doing everything. Virus applications and mobile  modifications.  The moving to the next  slide we will see the architecture of the Android OS.It is a very popular operating system and it is an open source and a lot of applications are running on it This is supported by multiple vendors for multiple types of operations and applications He talked about business, banking and finance You can even talk about retail or you can talk about anything That is coming over this application it is also emerging with the new updates Like iot and all. ****ANDROID OS ARCHITECTURE**** 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. | | | |