**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18-06-2020** | **Name:** | **Kiran N** |
| **Course:** | **Introduction to Ethical Hacking** | **USN:** | **4al16ec031** |
| **Topic:** | **1.Ethicalhackinginnetworkarchitectureand on mobile platforms** | **Semester & Section:** | **8th and A** |
| **Github Repository:** | **Kiran-course** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| 1.Ethicalhackingonmobileplatforms Mobiledevicesareusedforourmostsensitivetransactions,includingemail,banking,andsocialmedia.Buttheyhaveauniquesetof vulnerabilities,whichhackersarealltoowillingtoexploit.Securityprofessionalsneedtoknowhowtoclosethegapsandprotect devices,data,andusersfromattacks.JoinauthorMalcolmShoreasheexploresthetwodominantmobileoperatingsystems,Android andiOS,andshowswaystoprotectdevicesthroughanalysisandtesting.WatchthiscoursetoreviewthebasicsofmobileOSmodels, thetoolsetsyouneedfortesting,andthetechniquesfordetectingandpreventingthemajorityofsecurityflaws.  MobileDeviceSecurityandEthicalHackingisdesignedtogiveyoutheskillstounderstandthesecuritystrengthsandweaknessesofAppleiOSandAndroiddevices.Mobiledevicesarenolongeraconveniencetechnologytheyareanessentialtoolcarriedorwornbyusersworldwide,oftendisplacingconventionalcomputersforeverydayenterprisedataneeds.Youcanseethistrendincorporations,hospitals,banks,schools,andretailstoresacrosstheworld.Usersrelyonmobiledevicesmoretodaythaneverbeforeweknowit,andthebadguysdotoo.courseexaminesthefullgamutoftheseyouwillbeabletoevaluatethesecurityweaknessesofbuilt-inandthirdpartyapplications.You'lllearnhowtobypassplatformencryptionandmanipulateappstocircumventclientsidesecuritytechniques.You'llleverageautomatedandmanualmobileapplicationanalysistoolstoidentifydeficienciesinmobileappnetworktraffic,filesystemstorage,andinterpcommunicationchannels.You'llsafelyworkwithmobilemalwaresamplestounderstandthedataexposureandaccessthreatsaffectingAndroidandiOS,andyou'llbypasslockscreentoexploitlostorstolen devices  **Ethical Hacking – Footprinting**  Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both passive and active. Reviewing a company’s website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.  Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.  During this phase, a hacker can collect the following information −  •Domain name  •IP Addresses  •Namespaces  •Employee information  •Phone numbers  •E-mails  • Job Information  In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet.  Domain Name Information  You can use  <http://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry,name server, owner's contact information, etc.  **Quick Fix**  It's always recommended to keep your domain name profile a private one which  should hide the above-mentioned information from potential hackers.  Finding IP Address You can use ping command at your prompt. This command is available on Windows  as well as on Linux OS. Following is the example to find out the IP address of  tutorialspoint.com $ping tutorialspoint.com  It will produce the following result − PING tutorialspoint.com (66.135.33.172) 56(84) bytes of data.  64 bytes from 66.135.33.172: icmp\_seq = 1 ttl = 64 time = 0.028 ms  64 bytes from 66.135.33.172: icmp\_seq = 2 ttl = 64 time = 0.021 ms  64 bytes from 66.135.33.172: icmp\_seq = 3 ttl = 64 time = 0.021 ms  64 bytes from 66.135.33.172: icmp\_seq = 4 ttl = 64 time = 0.021 ms |