**Performance Assessment: Hacking Mobile Devices**

In this Performance Assessment, you will perform the tasks you have been taught in the Guided Practices (iLabs content from EC-Council).  You may use the book, and any notes you have. You may look at your prior labs. You may not give or receive help from other students. You may ask your instructor for assistance, but it is likely to cost points.

How does this practical lab apply in the real world?

**Android**

Is your financial data safe? Think about the last time you used your phone for banking or purchased something on the Internet. About 80% of all Android users were impacted by recent vulnerabilities that allowed attackers to gain access to your phone. The total amount of user accounts that were impacted is estimated to reach over 900 million individuals. Apple experienced something similar to the Android attack however the attack on the Android platform was more severe. The hacker could erase the phone, access personal account details, and turn on your camera without your knowledge or consent.

**Apple**

Breaking News: Sept 2021Apple Advised that an Israeli spyware firm created a method to take control of almost any apple phone, tablet, computer, watch.  Warning clicking is not required for this exploit and most users will never know their phone has been compromised, once again without their consent just like android all things mobile are available to the hacker.

Resources Needed

This lab assessment covers Modules 17 and 18 from your EC-council lab content. Thus, all resources you will need will be from your labs, your text, and any research that you might have.

* ParrotOS (only)
* Android OS
* msfvenom
* meterpreter
* apache2

Level of Difficulty

Advanced

*Important*

***Please note the following guidance****: This Assessment should be performed in the VCastle POD using the Parrot Linux virtual machine.*

*All screenshots should reflect your own work and should have the date, time and user information (name, student ID) clearly displayed*

*All takeaways/inferences you can make about your target based on the reconnaissance should be clearly expressed (full sentences without excessive use of bullet points) and should be in your own words and result from you doing the work.*

Instructions

***Tasks:***

1. Using any of the tools available on the ParrotOS virtual machine, perform attack on the Android phone using msfvenom to create a payload. Provide screenshot of payload creation on ParrotOS
2. Create a web server on Parrot OS apache2 to deliver the msfvenom exploit document this screenshot once completed.
3. Provide a screenshot of the Android OS while the msfvenom exploit is installed
4. Provide a screenshot of the Android system once it has been compromised, explain the tools that are available using Metasploit.
5. Explain in a narrative the overall process of how you used the resources and tools to gain access to the Android Phone as well as how to prevent future attacks on the Android phone platform.