CS 332: Ethical Hacking
Study Guide for Mid-term Exam

1 The Labs

Android Repackaging Attack Lab. What's the key idea of the repackaging attack?

Android Repackaging Attack Lab. What's an APK file? Where can you get Android APK files?

Android Repackaging Attack Lab. In this lab, we didn't choose a popular app like Facebook or Instagram, instead, we used a app specifically developed for this lab, called RepackagingLab.apk. What problems we might face if we want to perform this attack in real life and we choose Facebook as the target app?

Android Repackaging Attack Lab. What's a broadcast receiver? In the task which we delete the victim's contact records, explain why would the contact records be deleted when the victim attempts to set the system time on the Android device.

Android Repackaging Attack Lab. In the task of tracking victim's location, we used a mock location app. Why such an app is needed? In real life attacks on an Android phone, do we still need such an app? Why?

Android Repackaging Attack Lab. In the task of tracking victim's location, why do we need to tell the Android phone the ip address of www.repackagingattacklab.com?

Android Rooting Attack Lab. Why or when rooting is needed?

Android Rooting Attack Lab. Typically there are two approaches to get the root permission of an Android device, modifying Android from inside and modifying Android from outside. Which approach did we take in this lab? Why is this approach more realistic for us?

Android Rooting Attack Lab. Most Android devices has two operating systems installed, the regular OS and the recovery OS. In real life, what is this recovery OS normally used for?

Android Rooting Attack Lab. On a typical Android device, the recovery OS doesn't give users a shell prompt, why? Would this be a problem for us to perform this attack, let's say, specifically, task 1? And how was this problem solved in this lab?

Android Rooting Attack Lab. What is an OTA package used for? The lab manual says two files: update-binary and update-script, are both needed for updating the Android OS, but we actually only used the update-binary, and didn't do anything with the update-script, why?

Android Rooting Attack Lab. In task 1, we created a malicious program called dummy.sh, how

did we make this program run automatically during the Android booting process?

Android Rooting Attack Lab. In task 2, we renamed the original app_process to app_process_original. Can we just delete this file, instead of renaming it? Why?

Android Rooting Attack Lab. In task 2, if successful, a file called /system/dummy2 is created; explain the technique behind this file creation, like how this file is created.

Android Rooting Attack Lab. In task 3, explaining what happens when you run the client program mysu.

Environment Variables Lab. What are environment variables? Please provide an example.

Environment Variables Lab. What are set-uid programs, how to determine if one program is a set-uid program or not? Give an example about which well known program in a Linux system should be a set-uid program?

Environment Variables Lab. Explain why calling system() within a set-uid program is quite dangerous.

2 The Slides

1. What's the difference between virus and worms?

2. What's the difference between DoS attack and DDos attack?

3. What's the purpose of keyloggers?

4. In the Android repackaging attack lab, the malicious program we created to track the victim's location, is it a virus, a worm, or a trojan program, or is it a spyware?

5. In the Android rooting attack lab, the malicious daemon program we created to get the root shell, is it a virus, a worm, or a trojan program?

6. What's nmap used for?

7. From attackers' perspective, when is port scanning needed?

8. Commonly used port numbers: like 80 is for which service, 443 is for which service, 22 is for which service, 25 is for which service?

9. Each IPv4 address includes two components, what are they?

10. Given the subnet mask, how to determine if two ip addresses are belonging to the same network or not.