Zac Crane

14151501

17DEC2014

Cyber Security

Kali linux utilizing Metasploit to attack an Android Smartphone

1. What tool is and does

Kali linux is a penetration security distribution of linux. It is a compilation of tools and packages that allows a user to quickly and easily test the strength of a network. It achieves this in many different ways. It is offered with 12 different metapackages from the homepage for kali ("Kali Linux | Rebirth of BackTrack, the Penetration Testing Distribution."). These vary in common options for the distribution to include a base package that will only include what is needed for the operating system to work all the way to a package that includes all the tool kits for kali. Some of these kits include software to help the user achieve different things. There is a kit for software defined radio, a default kit, GPU powered tools, wireless tools, web tools, forensics options, password cracking, a top ten package, and an RFID option ("Kali Linux | Rebirth of BackTrack, the Penetration Testing Distribution."). All of these various metapackages creates a very powerful distribution of linux that is free for anyone to use. Kali linux includes too many tools to list, but they range from sniffing and spoofing, password attacks, to exploitation tools, with many others available. All in all, Kali linux does one thing, it gives power to the people to test their security against attackers.

Metasploit is a software package that is compatible with Kali linux and is a very popular choice for penetration testing. Metasploit is a community of 200,000 users and contributors that have come together to create a penetration testing software in order to help users better prepare their defenses ("Penetration Testing Software, Pen Testing Security | Metasploit"). The goal of the software is to help users find weak points in their defense before a malicious user can exploit it against them. Metasploit allows users to efficiently conduct penetration testing on their network to discover weaknesses in their defenses.

The goal of these two tools is to use them in unison with each other. The following gives an outline of how to use it:

1. The first step is to install kali onto a USB key in order to use it on a computer.
2. The step after that is to add the metasploit package onto the machine.
3. Launch a network scanner and identify the targeted smartphone
4. Acquire the IP address of the smart phone as well as the attackers port and IP address
5. “Build” a fake application using metasploits Android Application package File
6. Launch the attack, plugging in the IP and port for the attacker and the destination (phones IP)
7. Wait to see if the user accepts the applications permission to run
8. Enjoy access to the phone

The exploit uses a reverse tcp connection, which means the attacker sends something and expects a connection back. This is why metasploit takes in the attackers IP and port, it allows the smartphone to create a connection to the attacking machine

1. Why tool is a risk, or

Metasploit and Kali linux do not pose a risk to the user, but instead attempt to reduce the risk of a computer on the user’s network from being attacked. The example here is that a user’s smartphone is not safe or immune to attacks from computers. The smartphone in this case is like a lone tuna fish out swimming in the sea, and the kali linux machine is a shark, its sole purpose is to find the tuna and attempt to eat it.

1. What benefit it has to improve security

The largest benefit that this tool provides is to help raise awareness of smartphone users. The basis for this attack is a user installing an application to their phone that is created by metasploit. This fake application actually pulls permission from the user when they hit accept to install the application. This will help to alert people to double check application permissions to ensure that they are not installing a rogue application. While there is no patch for human stupidity, there is at least some hope of being able to prevent more episodes of fake applications from giving a malicious user full access to the phone and its content.

The other benefits this has to improve security is to show people that a smartphone is really an advanced mobile computer and that it is not safe. People have a tendency to think that since it is a smart phone it is not vulnerable to any attack. This is not true, smart phones act very similar to a computer, especially when they are hooked up to a network like many people do (who wants to use data?). As mentioned, this exploit is only one of many different exploits that smart phones in specific are prone to. The important part of this exploit is to raise awareness to users that applications should be verified and created by trusted sources before being installed.

1. How to mitigate risk of tool if there is one

Risk mitigation for this exploit is accomplished by education. As mentioned earlier, there is no patch for human stupidity, but there is a lot to be gained by educating people in proper security protocols for a smart phone. The simplest way to prevent this attack is to verify that the creator can be trusted, and to not give an application total access to your phone. What business would a video game application have that would require access to the phones camera and microphone? Physical access to the phone is always important too. The owner of a phone should not leave it laying around for others to access. This can be mitigated by having a lock screen password or pattern set, but there are tools to exploit weaknesses in those too. The best mitigation for this risk is a combination of the above, keep your phone on your persons with a proper password and screen applications that are going to be put on the phone. There was no mention of antivirus or antimalware because these programs do not usually pick up application exploits.

Works Cited

1. "Kali Linux | Rebirth of BackTrack, the Penetration Testing Distribution." *Kali Linux*. Web. 17 Dec. 2014. <http://www.kali.org/>.
2. "Penetration Testing Software, Pen Testing Security | Metasploit." *Metasploit*. Web. 17 Dec. 2014. <http://www.metasploit.com/>.