Introducing the Smartphone Penetration Testing Framework

Georgia Weidman

CEO, Bulb Security LLC

Abstract: We develop an open source solution to integrate smartphone assessment into the penetration test. While much recent progress has been made in the field of smartphone security such as on device anti-malware solutions, assessing the security posture of networks from a smarttphone, and live environments for application testing, no open source solution for assessing the security posture of smartphone devices in an enterprise was available until this project. The release, developed as a part of the DARPA Cyber Fast Track program and continued with community input includes a wide variety of smartphone specific functionality including information gathering, exploitation, social engineering, and post exploitation that allow penetration testers to perform assessments of these devices.

1. Introduction

As a penetration tester, I am tasked with accessing the security posture of an environment. Surveying workstations, servers, networking devices, physical controls, even the resistance of employees to social engineering attacks, I find where security breaks down and what control and/or sensitive information a malicious attacker can gain by exploiting these vulnerabilities. The field of penetration testing has advanced in recent years, with a best practice standard[1] and a wide variety of both open source and commercial tools to assist penetration testers with each step of the effort. After hiring a skilled penetration tester, an organization can rest reasonably assured of the security posture of their organization.

However, as smartphones infiltrate the workplace, this assurance begins to break down. In today's fast paced business world, everyone from IT to top executives rely on having real time, constant access to communications and company data. It is expected that employees will have access to their company email and files on their smartphone devices. Companies at present have two options, issue company owned smartphones to employees or allow employees to bring their own device to work to be integrated with the network. The pros and cons of both approaches have been discussed in depth elsewhere, but regardless of the choice, the assessing the security posture of the smartphones in the workplace becomes a critical issue. Though in recent months many security tools have been released for smartphones such as app store based antivirus[2], tools to perform network pentests from a smartphone[7], and the MobiSec live testing environment [3] for smartphones, an open source solution for integrating the assessment of smartphones into penetration testing had not been released prior to this project. Such a solution allows security teams and penetration testers to assess the security posture of the smartphones in an environment. As a part of the DARPA cyber fast track program[4], Bulb

Security developed the open source Smartphone Penetration Testing Framework for solve this problem.

2. Goals of the Framework

Rather than create a product that exhaustively tests for every privilege escalation vulnerability on phones, or provides payloads for every useful smartphone functionality, instead for a first release we have chosen a selection of functionality at each phase of a traditional penetration test for implementation. Additionally, the chosen functionality focuses on features that are unique to smartphone platforms. For example, functionality that utilizes the mobile modem is preferred over a traditional TCP/IP remote shell.

The developers hope that the smartphone penetration testing framework will attract community support such as has been seen with other open source penetration testing tools such as the Metasploit Framework[5] and the Social Engineering Toolkit[6]. We hope that practitioners in the field will help shape the framework for what they need working in the field, by requesting new features for subsequent releases. Thus in time the framework will evolve as the threats to and security postures of smartphones likewise evolve.

3. Components of the Framework

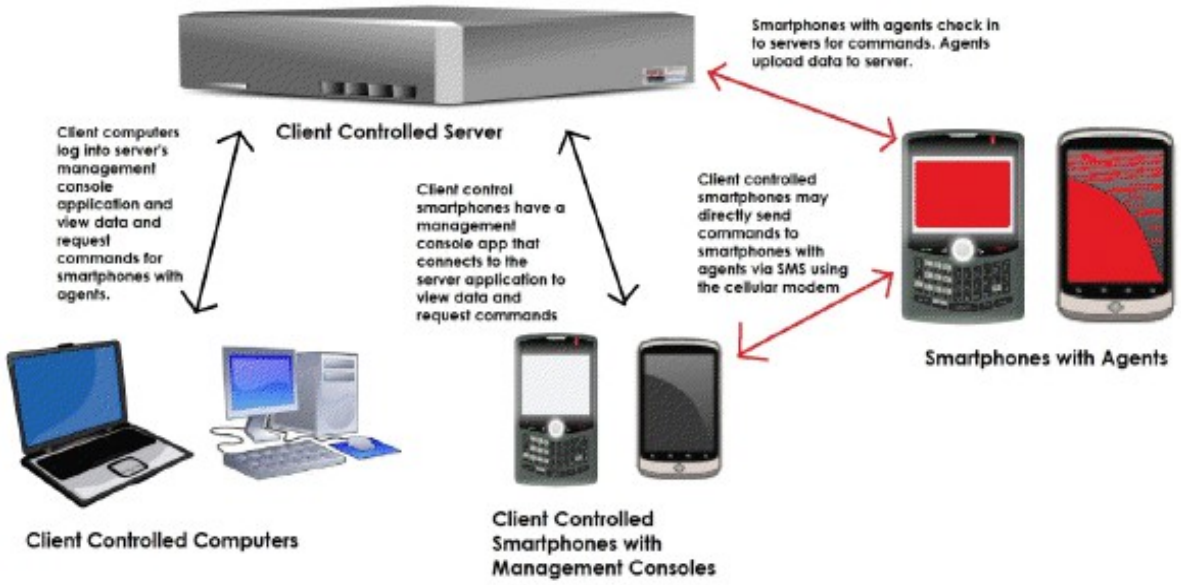

Figure 1: Smartphone Penetration Testing Framework Architecture

The framework consists of a management console, web based management graphical user interface, management app, and platform specific payloads or agents. The management console, GUI, and app are used to launch new remote attacks, create social engineering attacks, gathering information about smartphones, or interact with deployed agents. The management console, GUI, and app can interact with smartphones via the mobile modem or via TCP/IP. In particular agents receive commands through SMS and HTTP. Mobile modem based attacks and commands can be sent through an attached smartphone with the management app installed or through a mobile modem attached to the computer with the management console installed. TCP/IP based attacks and commands are sent through a web server. The management console is a command line interface that allows the user to interact with agents, launch new attacks, view gathered information, etc. without in depth technical knowledge of the commands or exploits, through a series of menus. The graphical user interface component is a web based front end for users who prefer to interact with a GUI rather than the command line version. The functionality is identical to the command line management console. The associated app is smartphone based and allows users to complete these same functionalities directly from a smartphone that attaches to the management console. Additionally, the mobile modem in the smartphone with the app installed can be leveraged by the framework to launch mobile modem based attacks or commands to an agent.

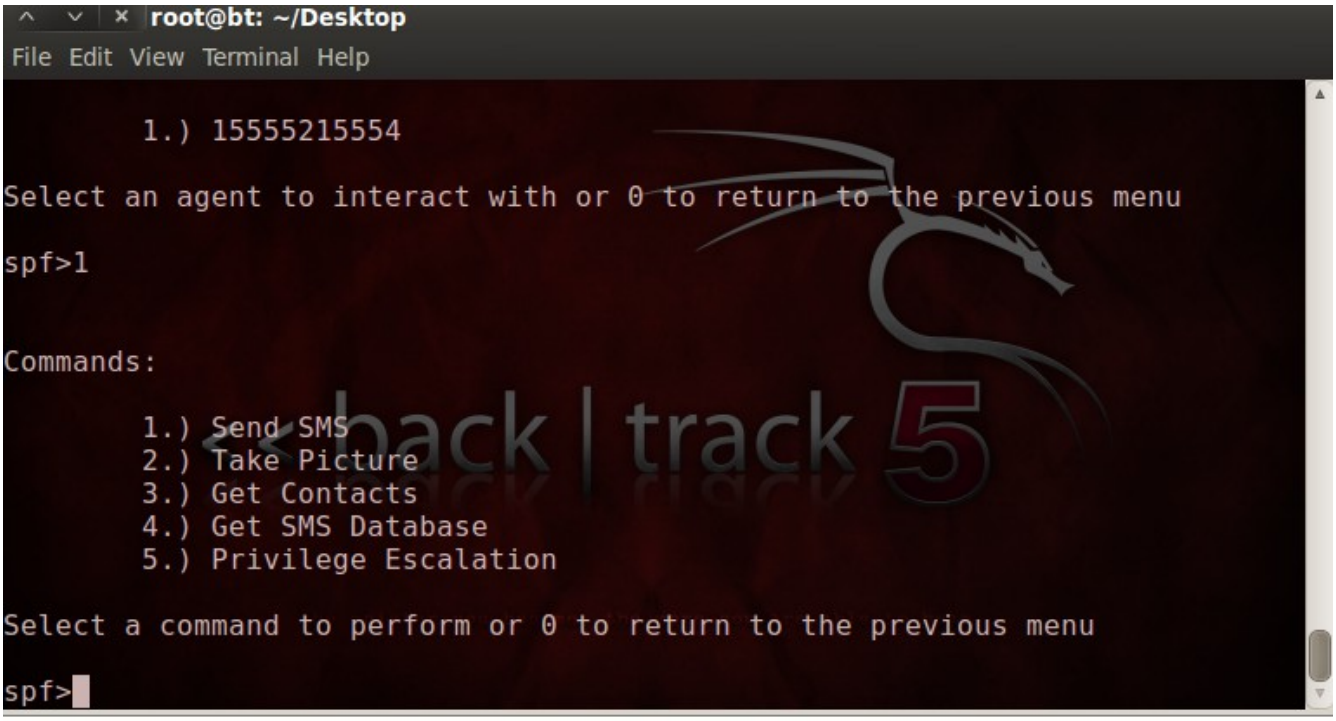

Figure 2: Management Console

The agents are deployed on smartphone platforms and respond to commands via SMS and HTTP to transparently perform a variety of functionality including information gathering, remote control, and privilege escalation payloads. The agents are designed in a modular fashion, such that additionally functionality can be easily added in future releases. Agents are deployed on victim phones by a successful remote, client side, or social engineering attack launched from the management console, GUI, or app. The agents transparently await instructions via SMS or HTTP.

Figure 3: SPF GUI

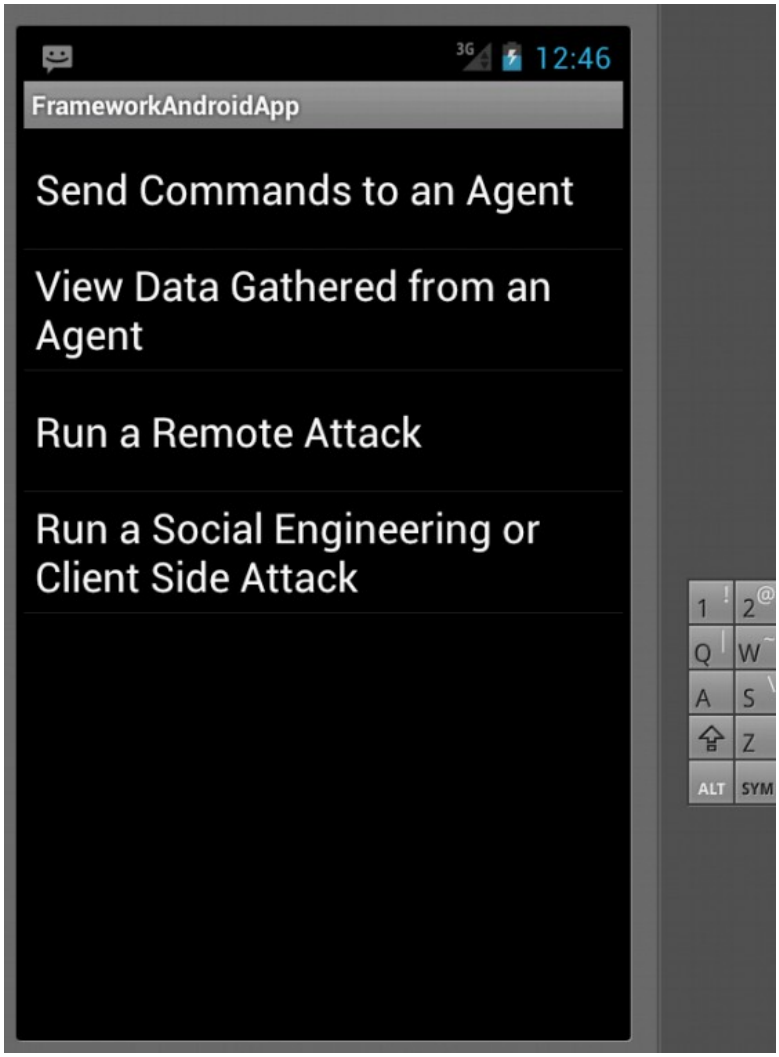

Figure 4: SPF App

4. Framework Functionality

The Smartphone Penetration Testing Framework includes a selection of functionality spanning the phases of a penetration test. Given a set of phone numbers, the framework performs information gathering by searching public records and databases for information. Additionally, if the smartphone can be discovered on the local network, a port scan will be performed. The framework searches for a subset of known vulnerabilities such as the default SSH password for jailbroken iPhone devices. The framework provides a selection of remote, client side, and social engineering based exploitation attacks. For example, the framework sends a text message to a potential victim disguised as typical advertisements that come from vendors with a link included. When users click on the link they are directed to a framework controlled web server that launches a client side attack against the smartphone browser.

Once an agent is installed on a victim smartphone, framework users have a variety of payload options to choose from. Users may request information about the smartphone that is returned via HTTP or SMS as desired. Users may also check for privilege escalation vulnerabilities. At this time the agent gains a root shell on the smartphone and then returns that the smartphone is vulnerable. In further releases additional root level functionality may be included to further leverage privilege escalation. Users may also remotely control the victim smartphone, calling functionality such as sending a text message or taking a picture.

5. Conclusions

We believe SPF provides security teams and penetration testers a strong starting point for an open source community driven tool for integrating smartphone platforms into the penetration test. Though the framework has ample room to grow and implement additional functionality, in this initial release it is fully functional targeting smartphone platforms via both TCP/IP (HTTP) and the mobile modem (SMS), and is controllable via a command line console, a graphical user interface, and a smartphone based app. Bulb Security would like to thank Pieter “Mudge” Zatko and the DARPA Cyber Fast Track team for allowing us to devote our time to this project.

6. Bibliography

[1] Penetration Testing Execution Standard http://www.pentest-standard.org

[2] Google Android Bouncer http://googlemobile.blogspot.com/2012/02/android-and-security.html

[3] Mobisec Live Environment http://blog.secureideas.net/2011/11/mobisec-live-environment-darpa-project.html

[4] DARPA Cyber Fast Track Program http://cft.usma.edu/

[5]Metasploit Framework http://www.metasploit.com

[6]Social Engineering Toolkit http://secmanic.com

[7]Zanti Android Based Security Testing Platform http://cyberarms.wordpress.com/2012/06/28/zanti-fast-simple-android-based-security-testing-platform/