S.W.O.R.D

A Penetration Testing User Interface For Openwrt Based Dropboxes

By: Bilal Bokhari

Agenda

- Inspirations Behind SWORD
- Design Philosophy
- Development Process
- Key Features
- Demo
- Wrap up

Inspirations behind SWORD

- MiniPwner Project
- Dsploit APP

MiniPwner

"It is a small Wireless 3G router installed with Openwrt and network penetration testing tools."

MiniPwner

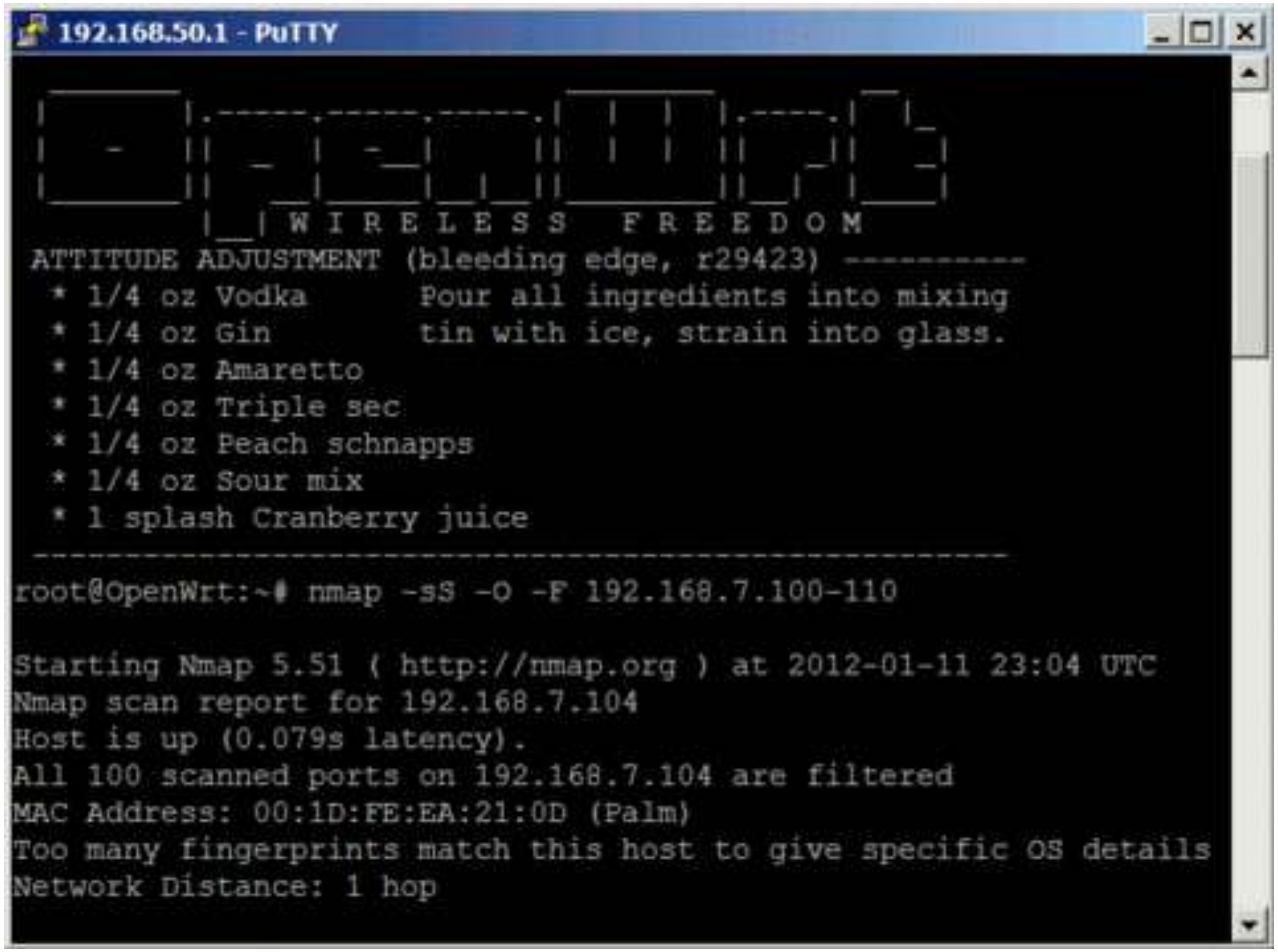
Pros

- On a small 3G router
- Tools
- Wi-Fi Attacks

Cons

- No Interface
- SSH

MiniPwner's Interface



```
  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 ATTITUDE ADJUSTMENT (bleeding edge, r29423) ----------
  * 1/4 oz Vodka      Pour all ingredients into mixing
  * 1/4 oz Gin        tin with ice, strain into glass.
  * 1/4 oz Amaretto
  * 1/4 oz Triple sec
  * 1/4 oz Peach schnapps
  * 1/4 oz Sour mix
  * 1 splash Cranberry juice
 -----------------------------------------------------
root@OpenWrt:~# nmap -sS -O -F 192.168.7.100-110

Starting Nmap 5.51 ( http://nmap.org ) at 2012-01-11 23:04 UTC
Nmap scan report for 192.168.7.104
Host is up (0.079s latency).
All 100 scanned ports on 192.168.7.104 are filtered
MAC Address: 00:1D:FE:EA:21:0D (Palm)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

“DSploit is a penetration testing suite developed for the Android operating system.”

Dsploit.

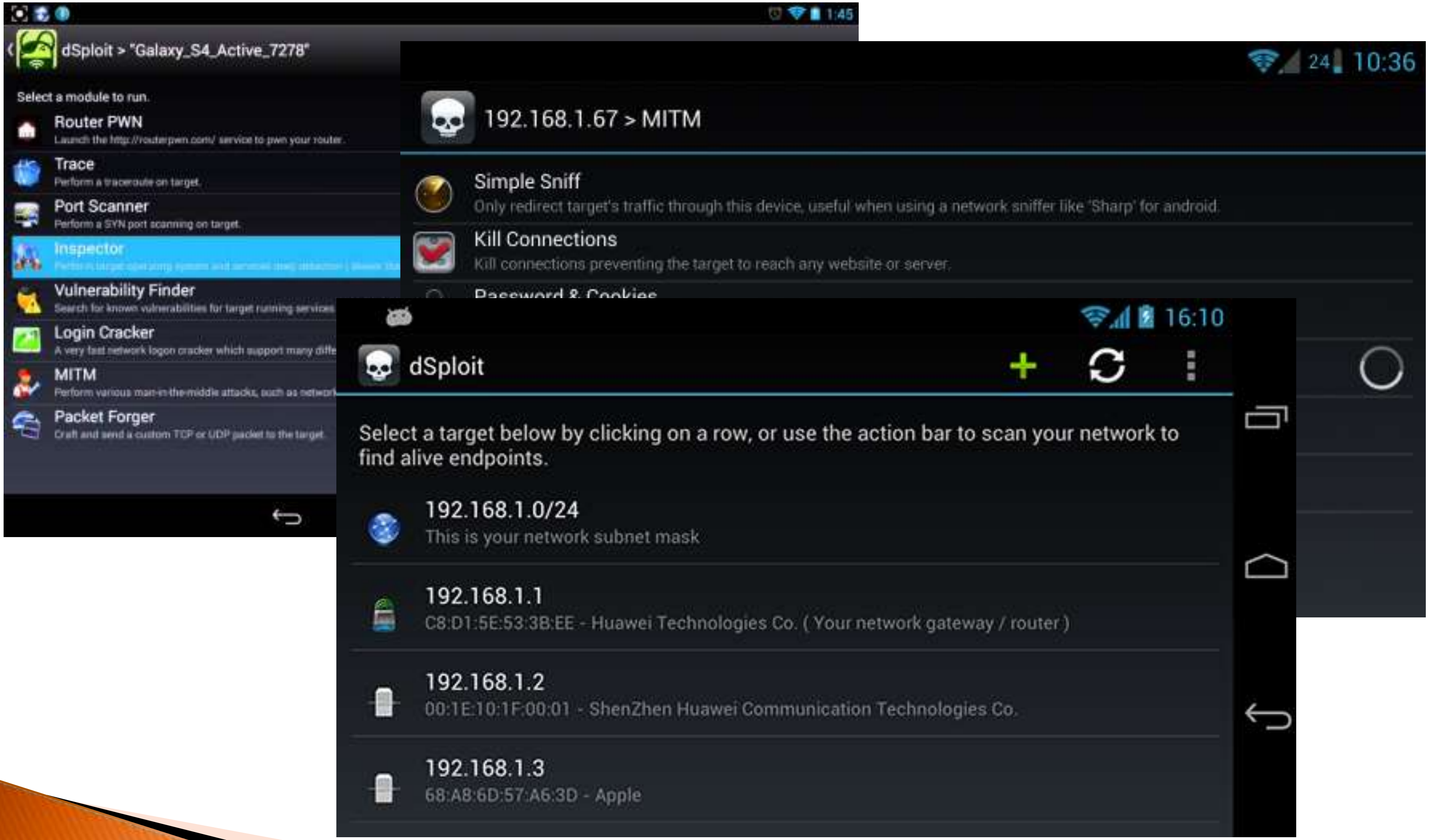
Pros

- User Friendly Interface
- Speed
- Runs on phone

Cons

- Limited Tools
- Can’t launch Wi-Fi Attacks

Dsploit’s Interface



dSploit > "Galaxy_S4_Active_7278"

Select a module to run.

Router PWN
Launch the http://routerpwn.com/ service to pwn your router.

Trace
Perform a traceroute on target.

Port Scanner
Perform a SYN port scanning on target.

Inspector
Perform target operating system and services deep detection (slower tha

Vulnerability Finder
Search for known vulnerabilities for target running services

Login Cracker
A very fast network logon cracker which support many diffe

MITM
Perform various man-in-the-middle attacks, such as network

Packet Forger
Craft and send a custom TCP or UDP packet to the target.

192.168.1.67 > MITM

Simple Sniff
Only redirect target's traffic through this device, useful when using a network sniffer like 'Sharp' for android.

Kill Connections
Kill connections preventing the target to reach any website or server.

Password & Cookies

dSploit

Select a target below by clicking on a row, or use the action bar to scan your network to find alive endpoints.

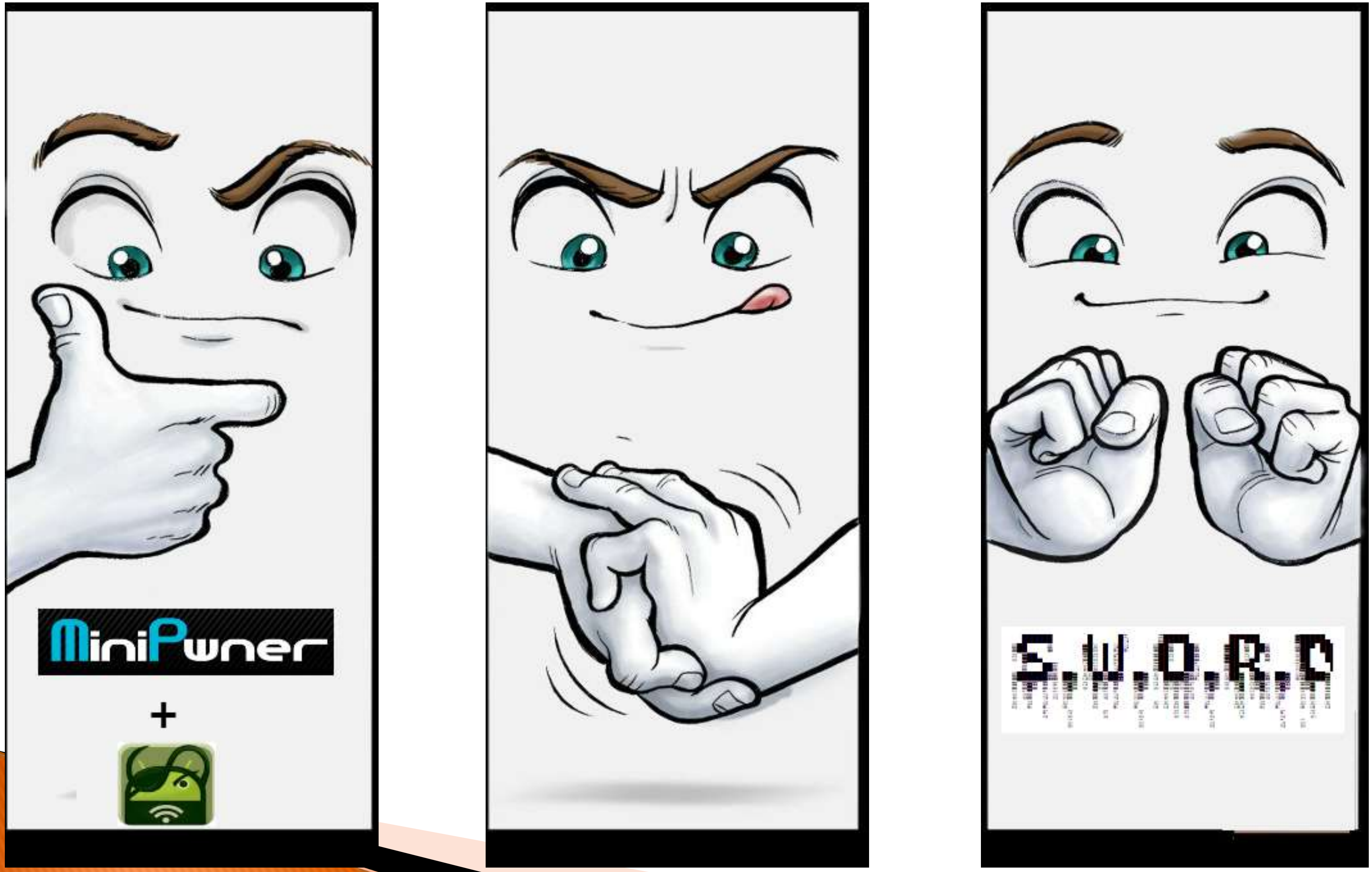
192.168.1.0/24
This is your network subnet mask

192.168.1.1
C8:D1:5E:53:3B:EE - Huawei Technologies Co. (Your network gateway / router)

192.168.1.2
00:1E:10:1F:00:01 - ShenZhen Huawei Communication Technologies Co.

192.168.1.3
68:A8:6D:57:A6:3D - Apple

In a Nutshell



Design Philosophy

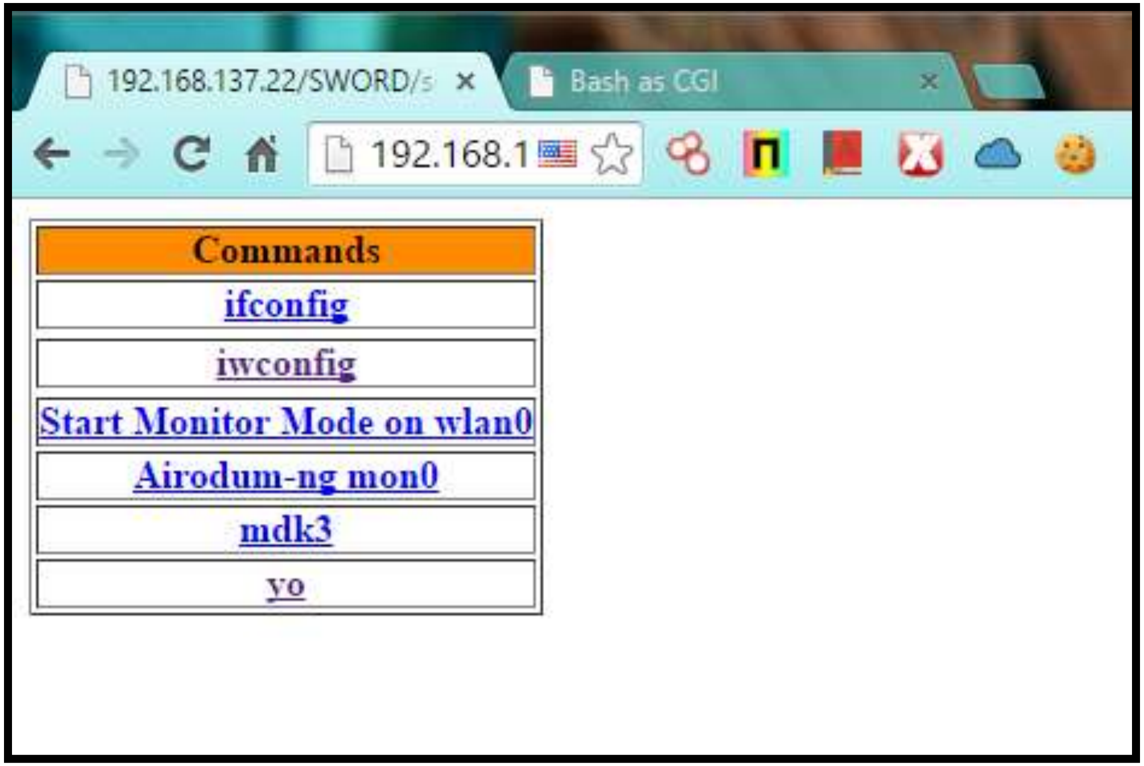
- Easy to use
- Speed
- Practical

Development Process

Hardware Selection

Development Process

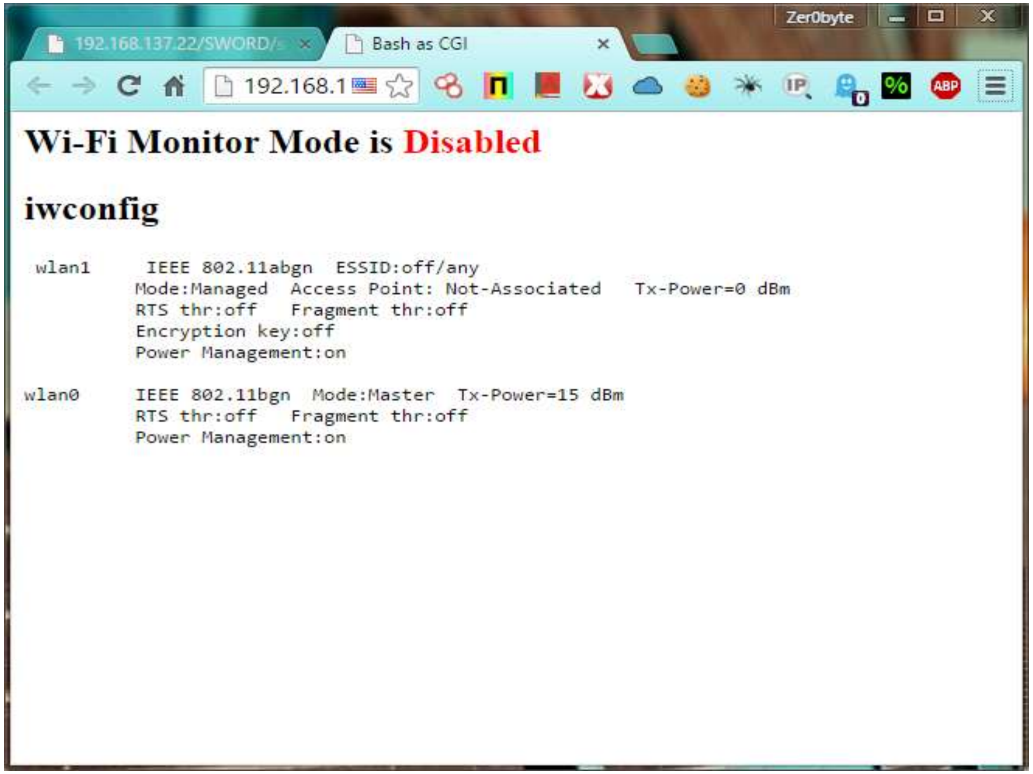
Started with Basics



Commands
ifconfig
iwconfig
Start Monitor Mode on wlan0
Airodum-ng mon0
mdk3
yo

Development Process

Started with Basics



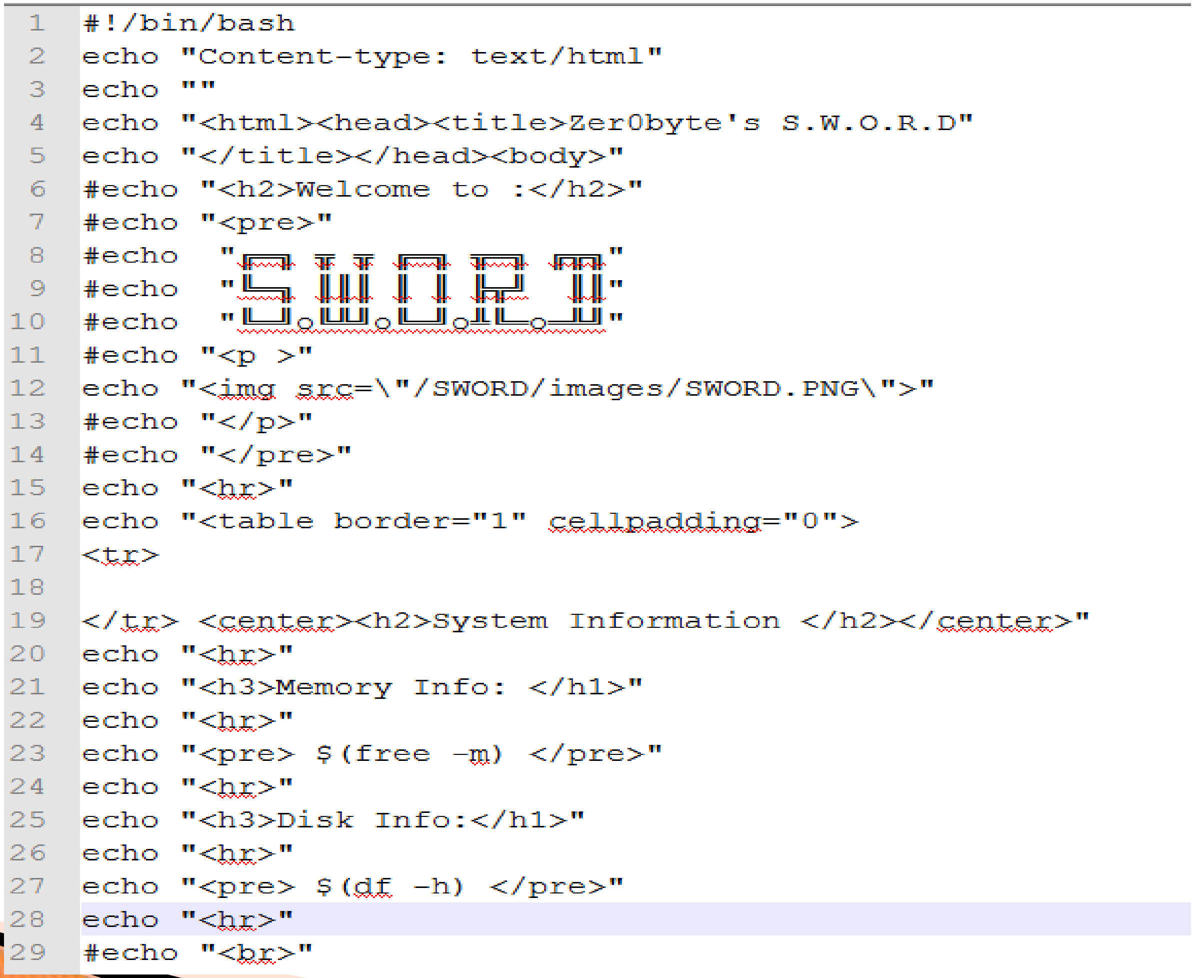
Wi-Fi Monitor Mode is Disabled

iwconfig

```
 wlan1      IEEE 802.11abgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

wlan0     IEEE 802.11bgn  Mode:Master  Tx-Power=15 dBm
          RTS thr:off   Fragment thr:off
          Power Management:on
```

Development Process

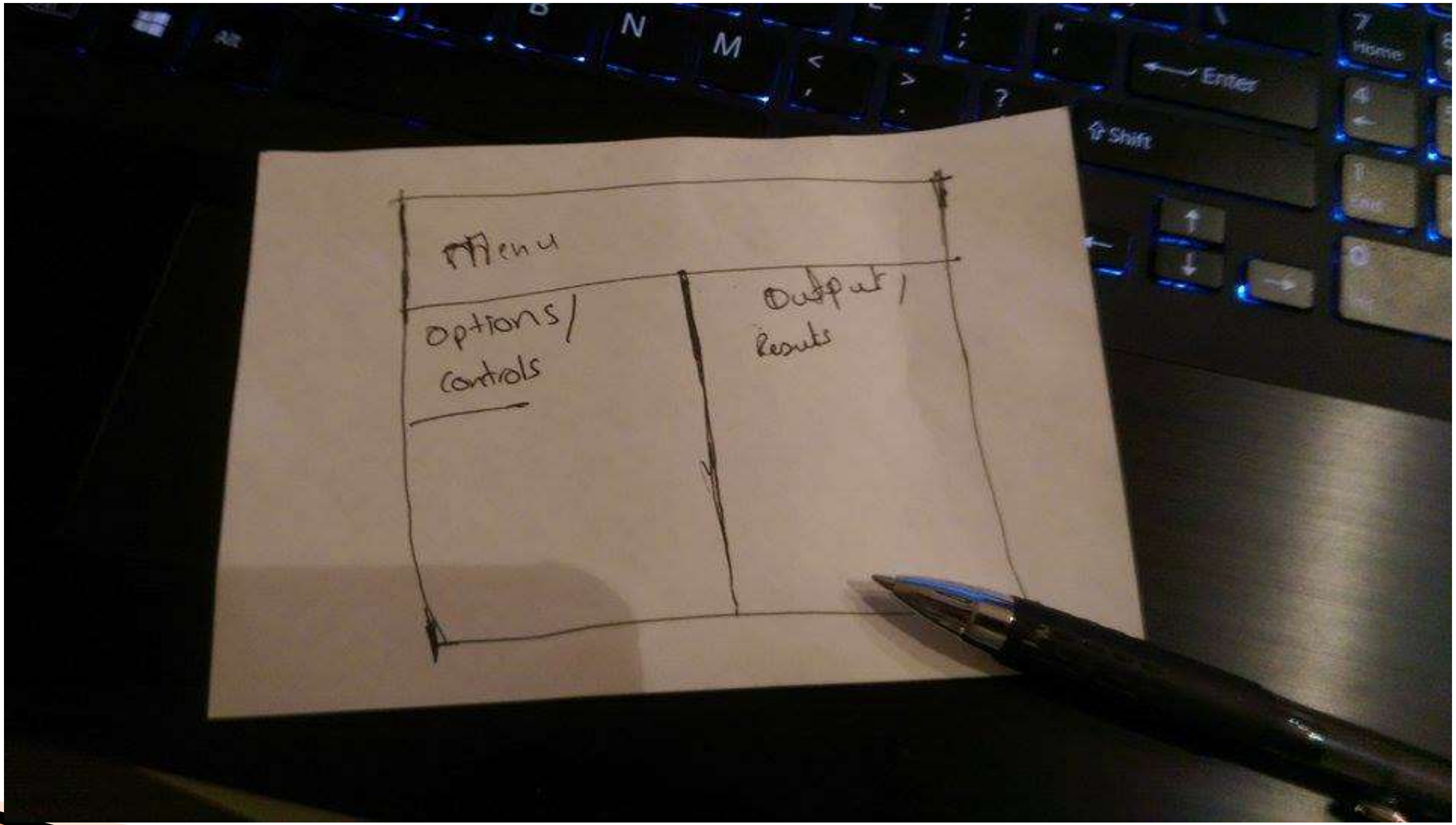
Scripts



```
#!/bin/bash
echo "Content-type: text/html"
echo ""
echo "<html><head><title>Zer0byte's S.W.O.R.D"
echo "</title></head><body>"
#echo "<h2>Welcome to :</h2>"
#echo "<pre>"
#echo  "╔═╗ ╦ ╦ ╔═╗ ╦═╗ ╔╦╗"
#echo  "╚═╗ ║║║ ║ ║ ╠╦╝  ║║"
#echo  "╚═╝o╚╩╝o╚═╝o╩╚═o═╩╝"
#echo "<p >"
echo "<img src=\"/SWORD/images/SWORD.PNG\">"
#echo "</p>"
#echo "</pre>"
echo "<hr>"
echo "<table border="1" cellpadding="0">
<tr>

</tr> <center><h2>System Information </h2></center>"
echo "<hr>"
echo "<h3>Memory Info: </h1>"
echo "<hr>"
echo "<pre> $(free -m) </pre>"
echo "<hr>"
echo "<h3>Disk Info:</h1>"
echo "<hr>"
echo "<pre> $(df -h) </pre>"
echo "<hr>"
#echo "<br>"
```

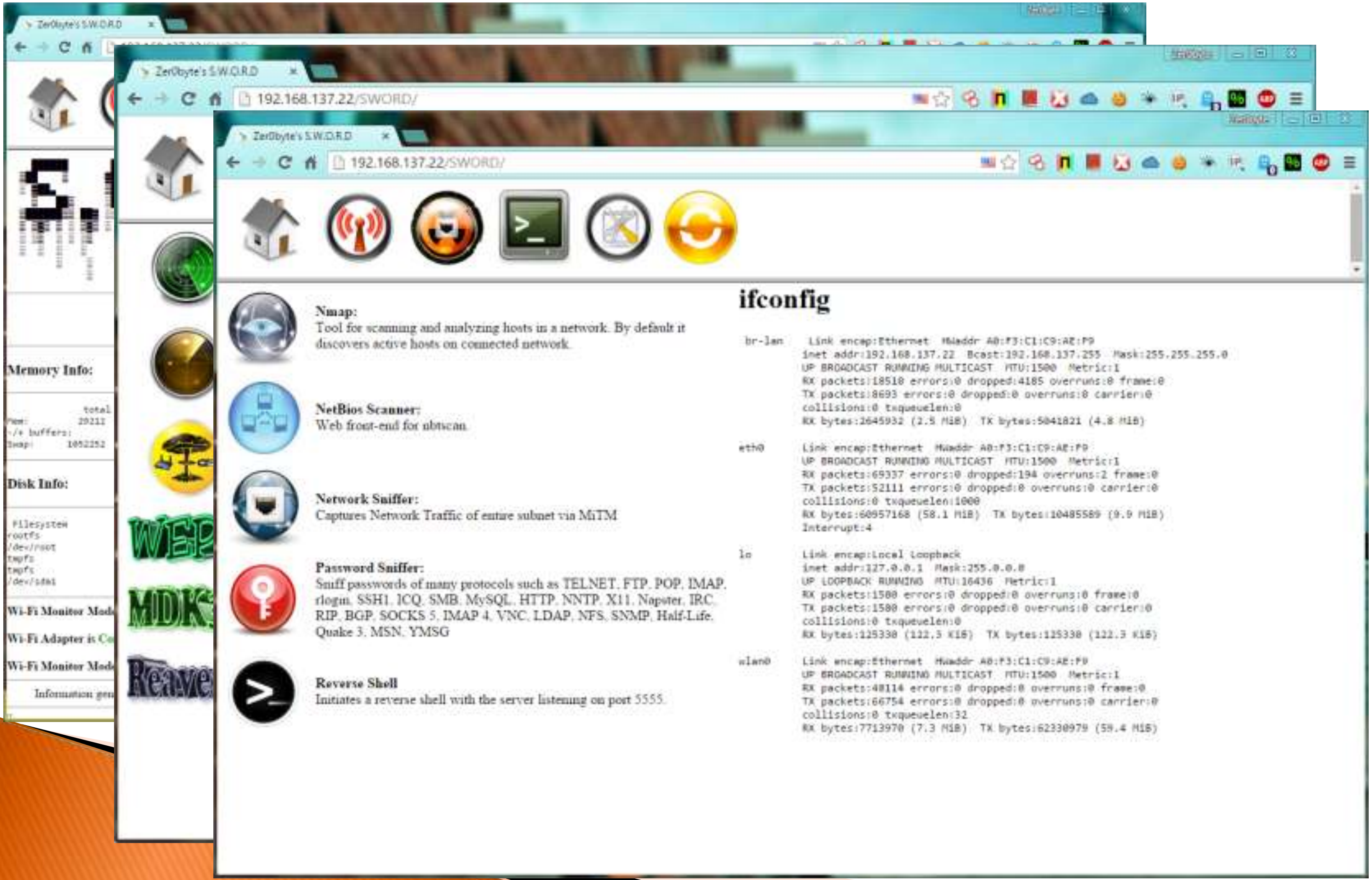
Development Process

Adding HTML Frames



Development Process

Final Look ☺



Nmap:
Tool for scanning and analyzing hosts in a network. By default it discovers active hosts on connected network.

NetBios Scanner:
Web front-end for nbtscan.

Network Sniffer:
Captures Network Traffic of entire subnet via MiTM

Password Sniffer:
Sniff passwords of many protocols such as TELNET, FTP, POP, IMAP, rlogin, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, Napster, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, Half-Life, Quake 3, MSN, YMSG

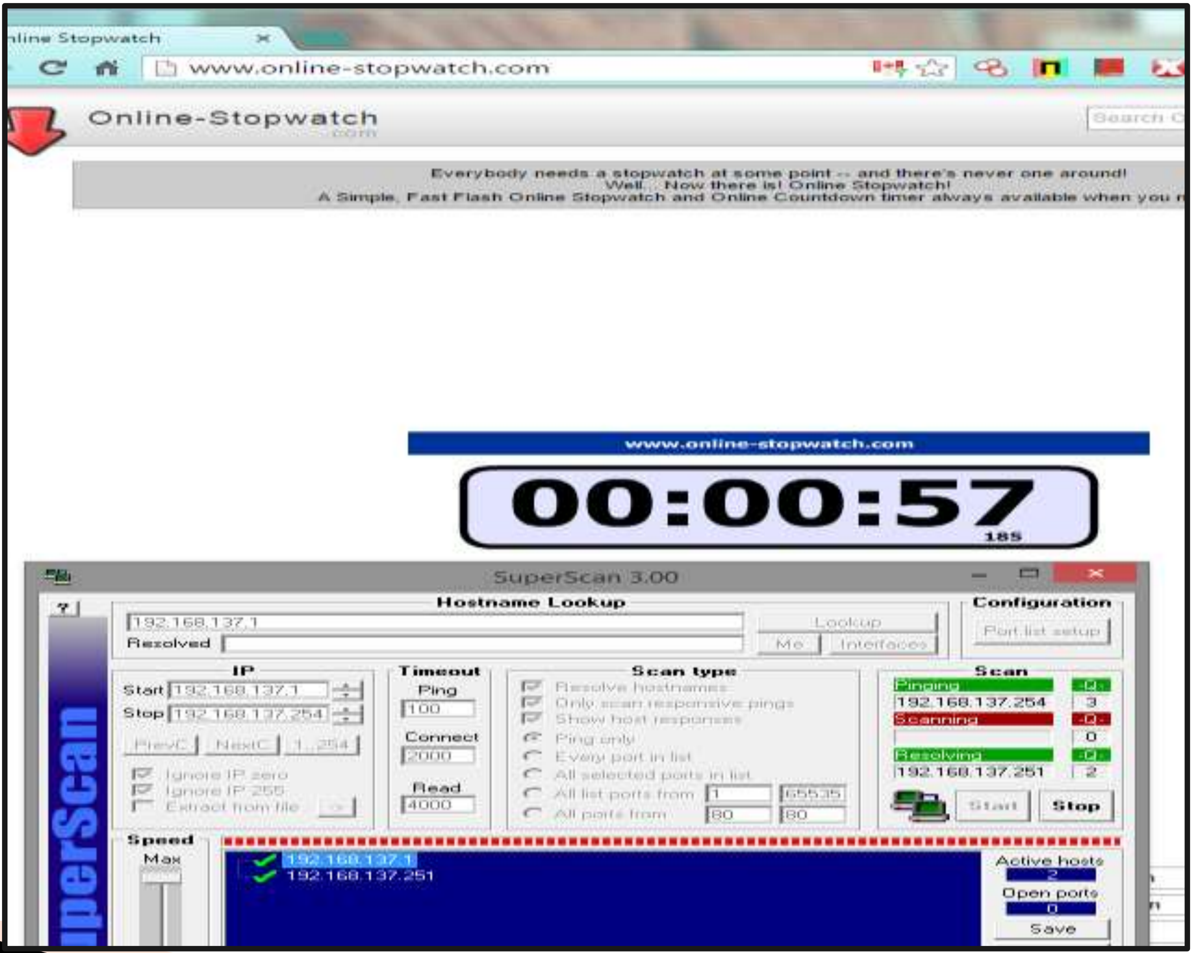
Reverse Shell
Initiates a reverse shell with the server listening on port 5555.

ifconfig

```
 br-lan    Link encap:Ethernet  HWaddr A0:F3:C1:C9:AE:F9
          inet addr:192.168.137.22  Bcast:192.168.137.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18510 errors:0 dropped:4185 overruns:0 frame:0
          TX packets:8693 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2645932 (2.5 MiB)  TX bytes:5041821 (4.8 MiB)

eth0      Link encap:Ethernet  HWaddr A0:F3:C1:C9:AE:F9
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:69337 errors:0 dropped:194 overruns:2 frame:0
          TX packets:52111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60957168 (58.1 MiB)  TX bytes:10485589 (9.9 MiB)
          Interrupt:4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1580 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1580 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:125330 (122.3 KiB)  TX bytes:125330 (122.3 KiB)

wlan0     Link encap:Ethernet  HWaddr A0:F3:C1:C9:AE:F9
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66754 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:32
          RX bytes:7713970 (7.3 MiB)  TX bytes:62330979 (59.4 MiB)
```

Key Features

Device Boots under 1 minute.



Everybody needs a stopwatch at some point -- and there's never one around!
Well.. Now there is! Online Stopwatch!
A Simple, Fast Flash Online Stopwatch and Online Countdown timer always available when you n

00:00:57
185

Hostname Lookup
192.168.137.1
Resolved

Configuration

IP
Start 192.168.137.1
Stop 192.168.137.254
☑ Ignore IP zero
☑ Ignore IP 255
□ Extract from file

Timeout
Ping 100
Connect 2000
Read 4000

Scan type
☑ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
● Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
○ All ports from 80 80

Scan
Pinging -Q-
192.168.137.254 3
Scanning -Q-
0
Resolving -Q-
192.168.137.251 2

Speed
Max

✓ 192.168.137.1
✓ 192.168.137.251

Active hosts
2
Open ports
0

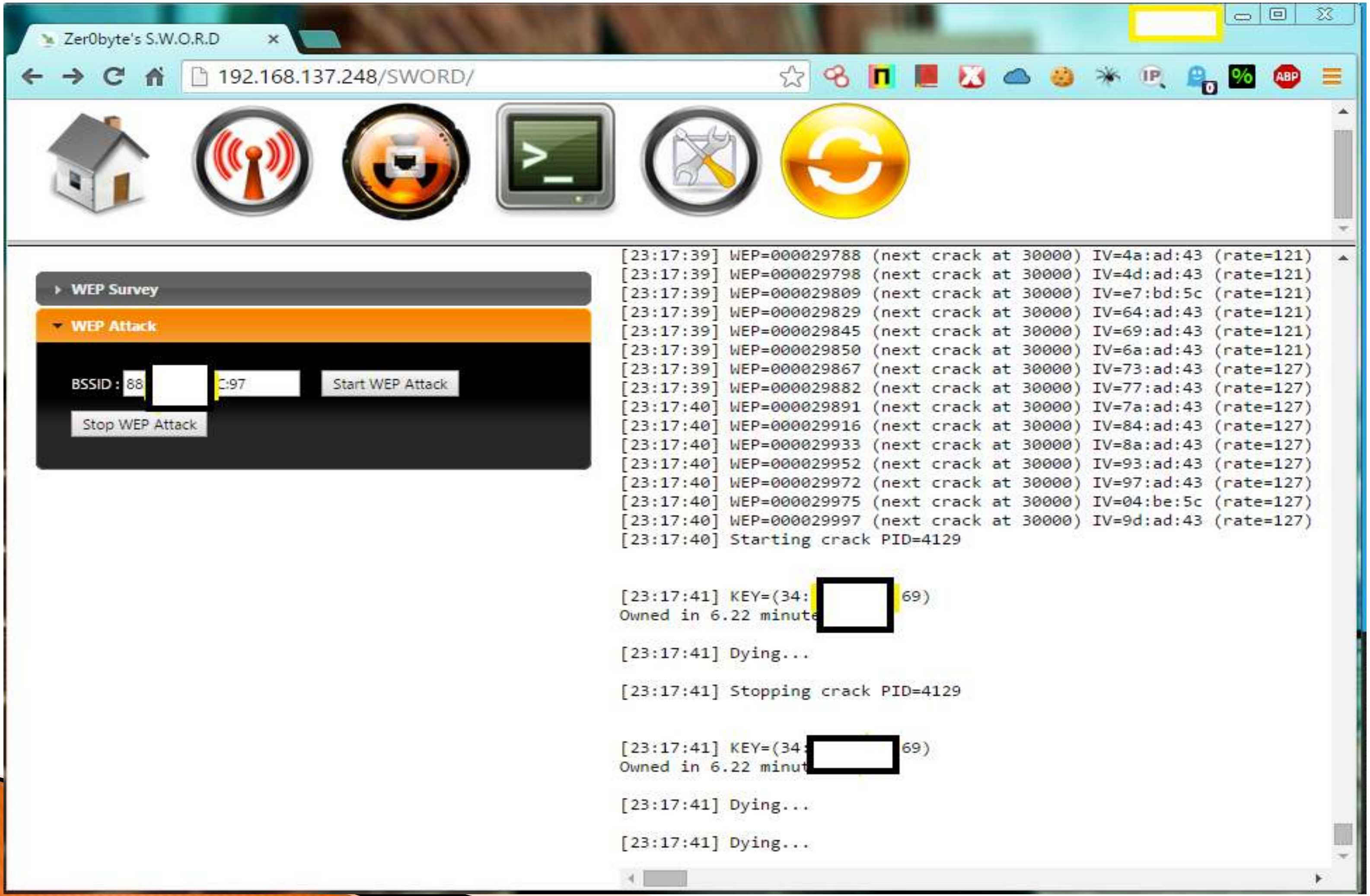
Key Features

Cross Platform Access

- Tablets
- Smart Phones
- Laptop

Key Features

WEP Cracking Made Easy ☺



BSSID : 88[redacted]C:97

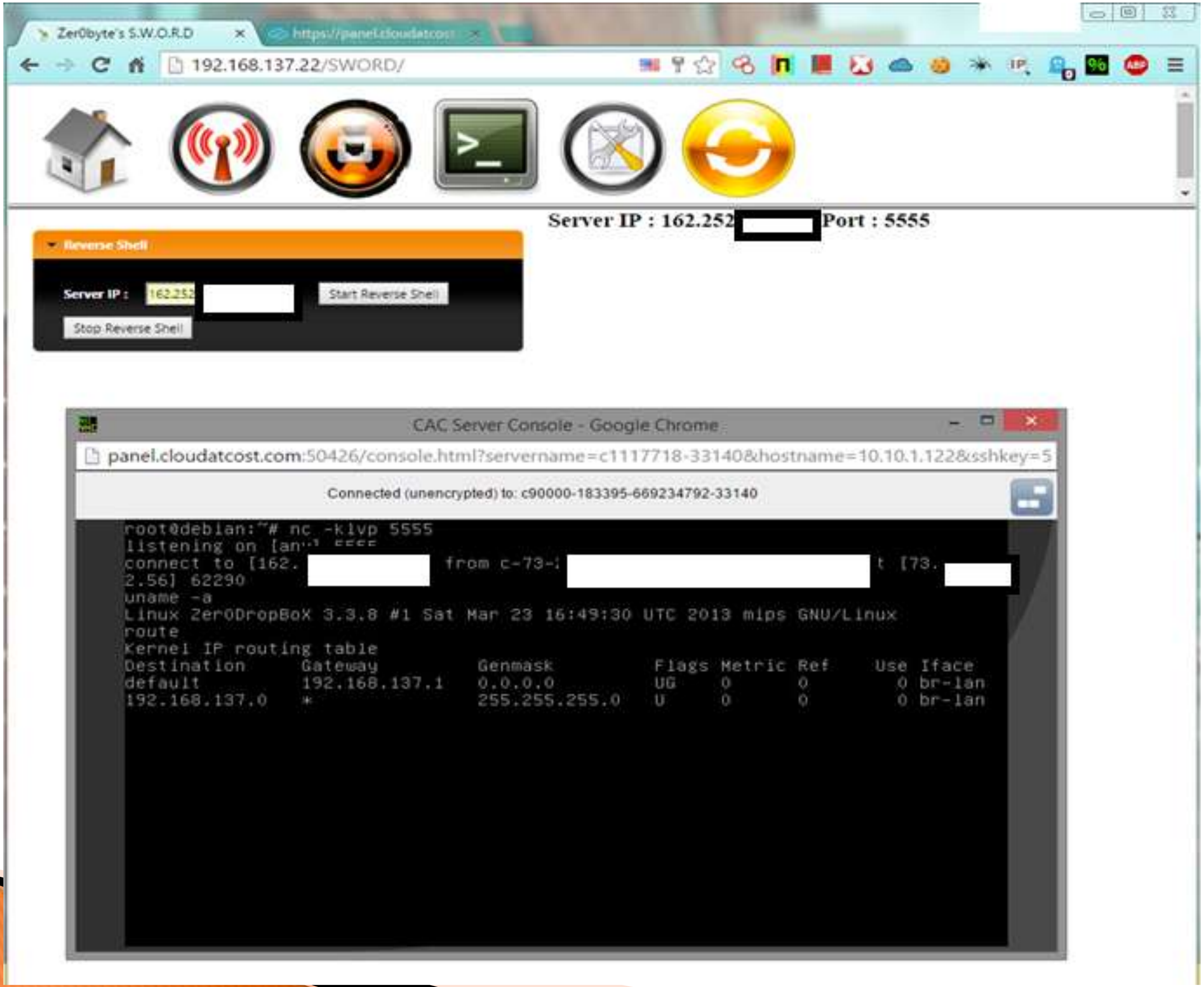
```
[23:17:39] WEP=000029788 (next crack at 30000) IV=4a:ad:43 (rate=121)
[23:17:39] WEP=000029798 (next crack at 30000) IV=4d:ad:43 (rate=121)
[23:17:39] WEP=000029809 (next crack at 30000) IV=e7:bd:5c (rate=121)
[23:17:39] WEP=000029829 (next crack at 30000) IV=64:ad:43 (rate=121)
[23:17:39] WEP=000029845 (next crack at 30000) IV=69:ad:43 (rate=121)
[23:17:39] WEP=000029850 (next crack at 30000) IV=6a:ad:43 (rate=121)
[23:17:39] WEP=000029867 (next crack at 30000) IV=73:ad:43 (rate=127)
[23:17:39] WEP=000029882 (next crack at 30000) IV=77:ad:43 (rate=127)
[23:17:40] WEP=000029891 (next crack at 30000) IV=7a:ad:43 (rate=127)
[23:17:40] WEP=000029916 (next crack at 30000) IV=84:ad:43 (rate=127)
[23:17:40] WEP=000029933 (next crack at 30000) IV=8a:ad:43 (rate=127)
[23:17:40] WEP=000029952 (next crack at 30000) IV=93:ad:43 (rate=127)
[23:17:40] WEP=000029972 (next crack at 30000) IV=97:ad:43 (rate=127)
[23:17:40] WEP=000029975 (next crack at 30000) IV=04:be:5c (rate=127)
[23:17:40] WEP=000029997 (next crack at 30000) IV=9d:ad:43 (rate=127)
[23:17:40] Starting crack PID=4129


[23:17:41] KEY=(34:[redacted]69)
Owned in 6.22 minute

[23:17:41] Dying...

[23:17:41] Stopping crack PID=4129


[23:17:41] KEY=(34[redacted]69)
Owned in 6.22 minut

[23:17:41] Dying...

[23:17:41] Dying...
```

DEMO:

- Wifi Nuke
- WEP cracker
- MDK3
- Reaver

- Reverse shell
- Nmap
- Nbtscan
- Password Sniffer
- Network Sniffer

Reverse Shell Connection: VPS



Server IP : 162.252[redacted]Port : 5555

Server IP : 162.252[redacted]

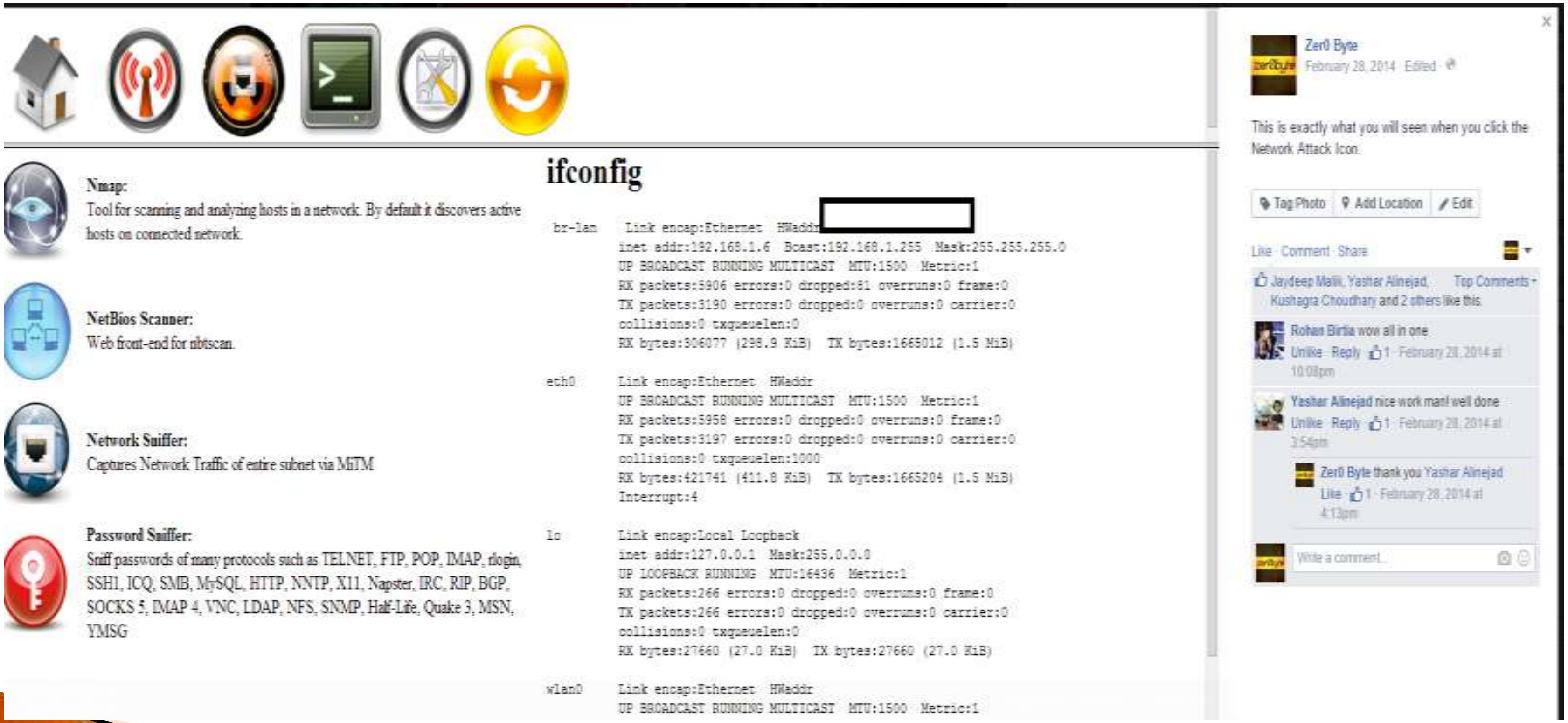
panel.cloudatcost.com:50426/console.html?servername=c1117718-33140&hostname=10.10.1.122&sshkey=5

Connected (unencrypted) to: c90000-183395-669234792-33140

```
root@debian:~# nc -klvp 5555
listening on [any] 5555
connect to [162.[redacted] from c-73-[redacted]t [73.[redacted]
2.56] 62290
uname -a
Linux Zer0DropBoX 3.3.8 #1 Sat Mar 23 16:49:30 UTC 2013 mips GNU/Linux
route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.137.1   0.0.0.0         UG    0      0        0 br-lan
192.168.137.0   *               255.255.255.0   U     0      0        0 br-lan
```

Wrap Up

Positive Community Feedback



Nmap:
Tool for scanning and analyzing hosts in a network. By default it discovers active hosts on connected network.

NetBios Scanner:
Web front-end for nbtscan.

Network Sniffer:
Captures Network Traffic of entire subnet via MiTM

Password Sniffer:
Sniff passwords of many protocols such as TELNET, FTP, POP, IMAP, rlogin, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, Napster, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, Half-Life, Quake 3, MSN, YMSG

ifconfig

```
 br-lan    Link encap:Ethernet  HWaddr [redacted]
           inet addr:192.168.1.6  Bcast:192.168.1.255  Mask:255.255.255.0
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:5906 errors:0 dropped:81 overruns:0 frame:0
           TX packets:3190 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:306077 (298.9 KiB)  TX bytes:1665012 (1.5 MiB)

eth0       Link encap:Ethernet  HWaddr
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:5958 errors:0 dropped:0 overruns:0 frame:0
           TX packets:3197 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:421741 (411.8 KiB)  TX bytes:1665204 (1.5 MiB)
           Interrupt:4

lo         Link encap:Local Loopback
           inet addr:127.0.0.1  Mask:255.0.0.0
           UP LOOPBACK RUNNING  MTU:16436  Metric:1
           RX packets:266 errors:0 dropped:0 overruns:0 frame:0
           TX packets:266 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:27660 (27.0 KiB)  TX bytes:27660 (27.0 KiB)

wlan0      Link encap:Ethernet  HWaddr
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Zer0 Byte
February 28, 2014 · Edited ·

This is exactly what you will seen when you click the Network Attack Icon.

Jaydeep Malik, Yashar Alinejad, Kushagra Choudhary and 2 others like this.

Rohan Birla wow all in one
Unlike · Reply · 1 · February 28, 2014 at 10:08pm

Yashar Alinejad nice work man! well done
Unlike · Reply · 1 · February 28, 2014 at 3:54pm

Zer0 Byte thank you Yashar Alinejad
Like · 1 · February 28, 2014 at 4:13pm

Wrap Up

- Room For Improvement.
- Need To try SWORD on different Hardware.

Questions ?

Thank You