Pocket mein Rocket

By: Anant Shrivastava
&
Ankur Bhargava

THE FOLLOWING **PREVIEW** HAS BEEN APPROVED FOR

ALL AUDIENCES

BY THE MOTION PICTURE ASSOCIATION OF AMERICA

THE FILM ADVERTISED HAS BEEN RATED

For information on film ratings,
go to www.filmratings.com

Star Cast


Sony Ericsson
Target @ 192.168.1.109
About
Nmap scans
IP: 192.168.1.109
Mac: 00:16:76:3A:F3:FB
Name:
4 Ports
1 Vulnerabilities
Actions
Port Discovery
Detect devices on your network
Establish connection to remote service
Establish connection to protocol
Replace Img
Demonstrate packet manipulation by showing different images
Sniffer
Discover unsecure cookies/urls/passwords on network
MITM
Test Man-In-The-Middle filters
Pentest ClientSide
Test for client-side vulnerabilities
XPERIA
Network Discovery
Discover
Options
Unknown
192.168.1.110
00:21:6a:5b:5b:d0
Unknown
192.168.1.108
04:46:65:ed:f8:f2
Unknown
192.168.1.107
00:16:76:3b:2b:8d
Unknown
192.168.1.106
00:80:48:68:71:cc
Unknown
192.168.1.109
00:16:76:3a:f3:fb
Unknown
IP: 192.168.1.115/24 (wlan0)
SSID: ruby arena
MODE: WiFi
SAMSUNG
ARP-Spoofing
Generic mode
RUNNING AND SPOOFING

Supported by

- Network Discovery
- zAnti by Zimperium
- Droidsheep
- Shark / Reader
- And many more

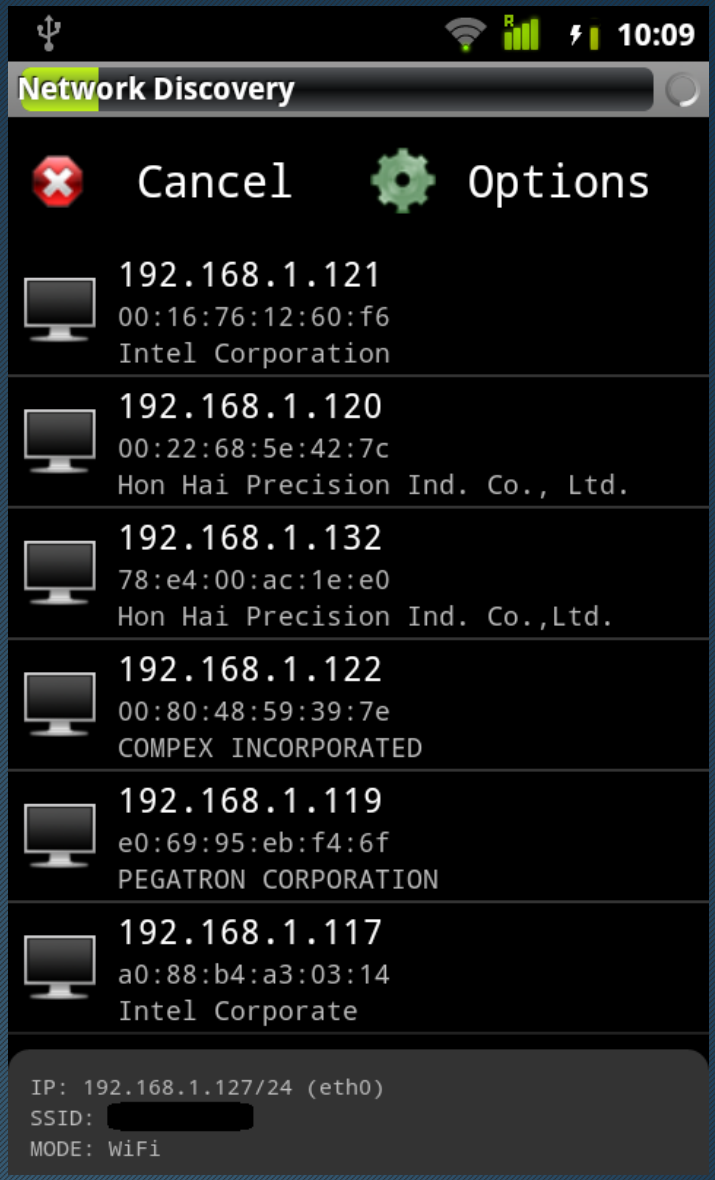
Console Support

- Terminal Client
- Skipfish
- Blind Elephant

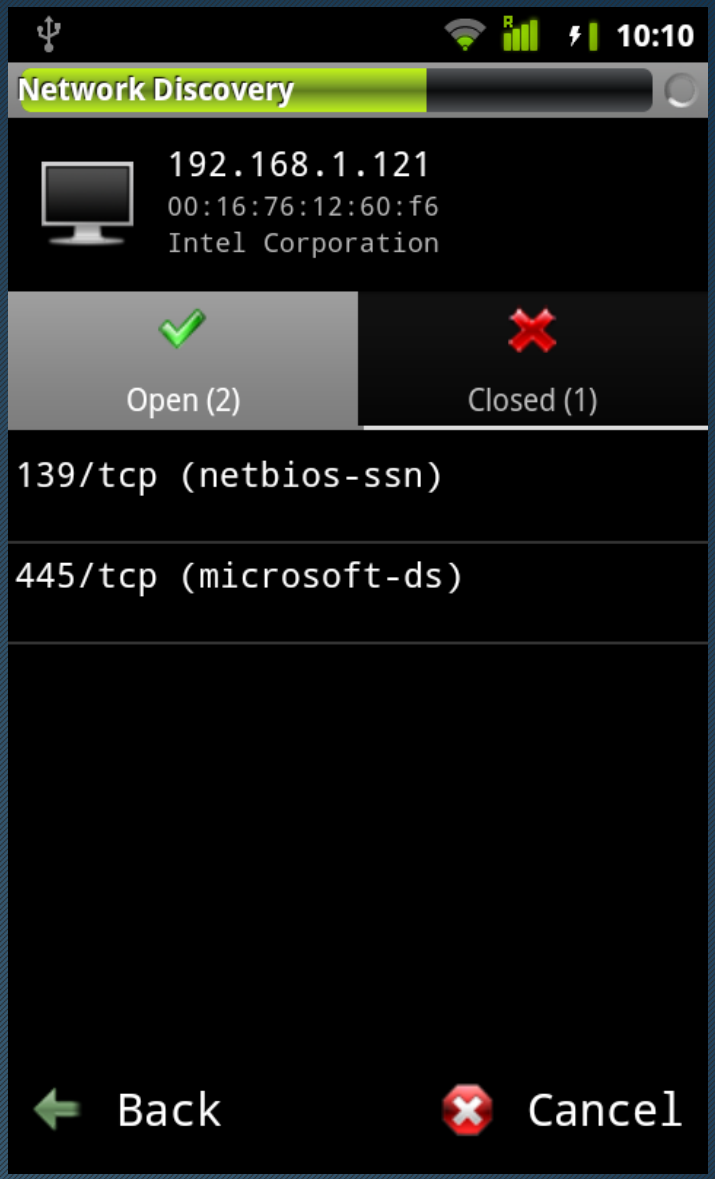
Dubbed in

- Python
- Perl
- PHP
- Bash

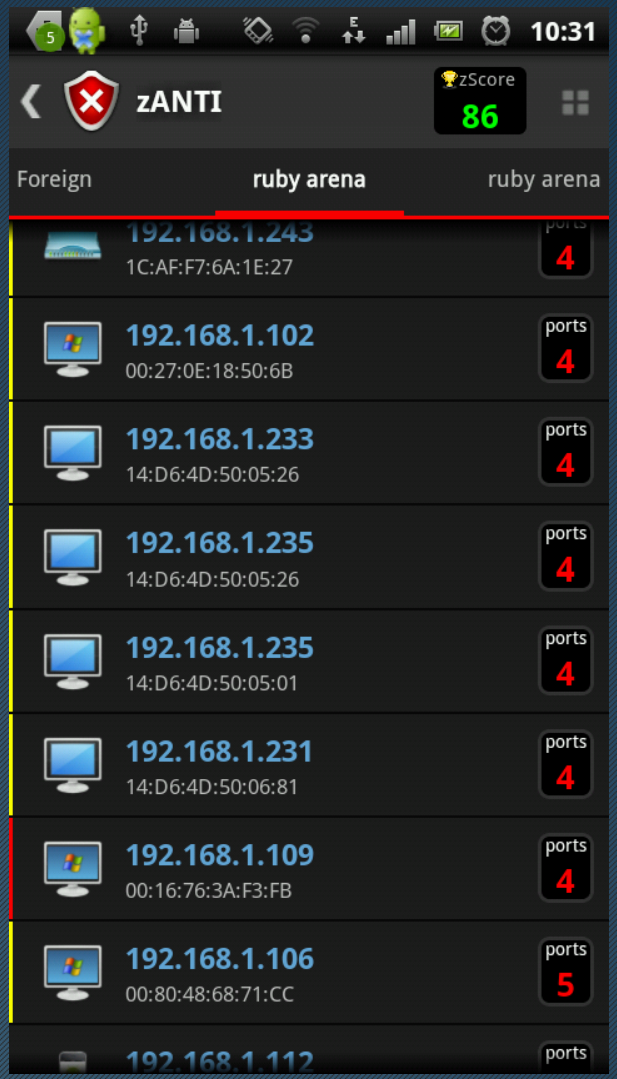
Network Discovery



Network Discovery



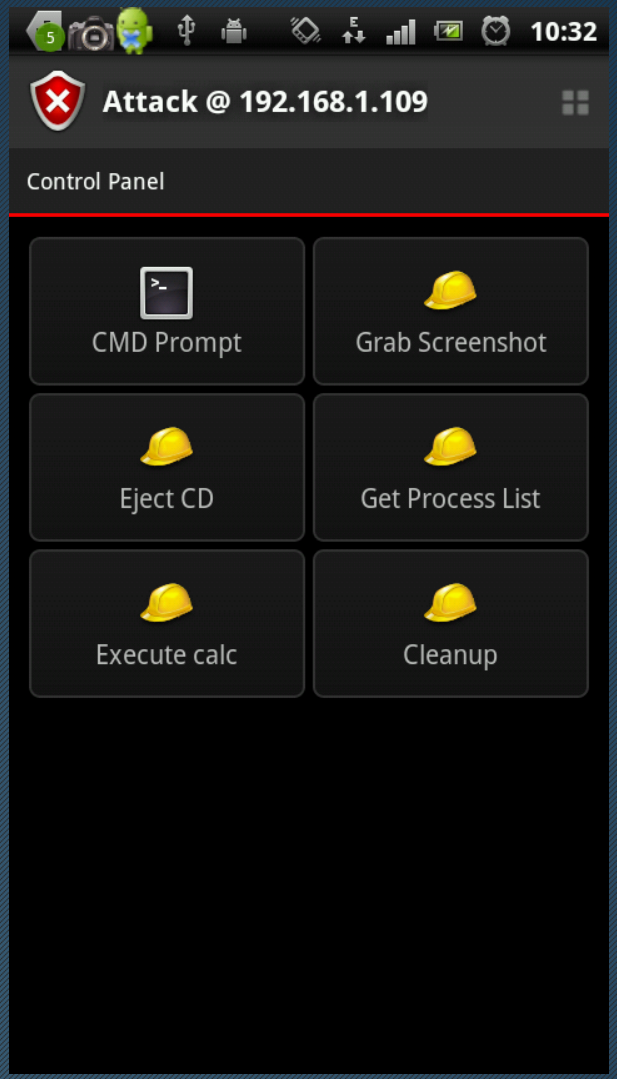
zAnti


10:31
zANTI
zScore
86
Foreign
ruby arena
ruby arena
192.168.1.243
1C:AF:F7:6A:1E:27
4
192.168.1.102
00:27:0E:18:50:6B
ports
4
192.168.1.233
14:D6:4D:50:05:26
ports
4
192.168.1.235
14:D6:4D:50:05:26
ports
4
192.168.1.235
14:D6:4D:50:05:01
ports
4
192.168.1.231
14:D6:4D:50:06:81
ports
4
192.168.1.109
00:16:76:3A:F3:FB
ports
4
192.168.1.106
00:80:48:68:71:CC
ports
5
192.168.1.112
ports

zAnti


10:32
Attack @ 192.168.1.109
Control Panel
CMD Prompt
Grab Screenshot
Attacking 192.168.1.109
3%
3/100

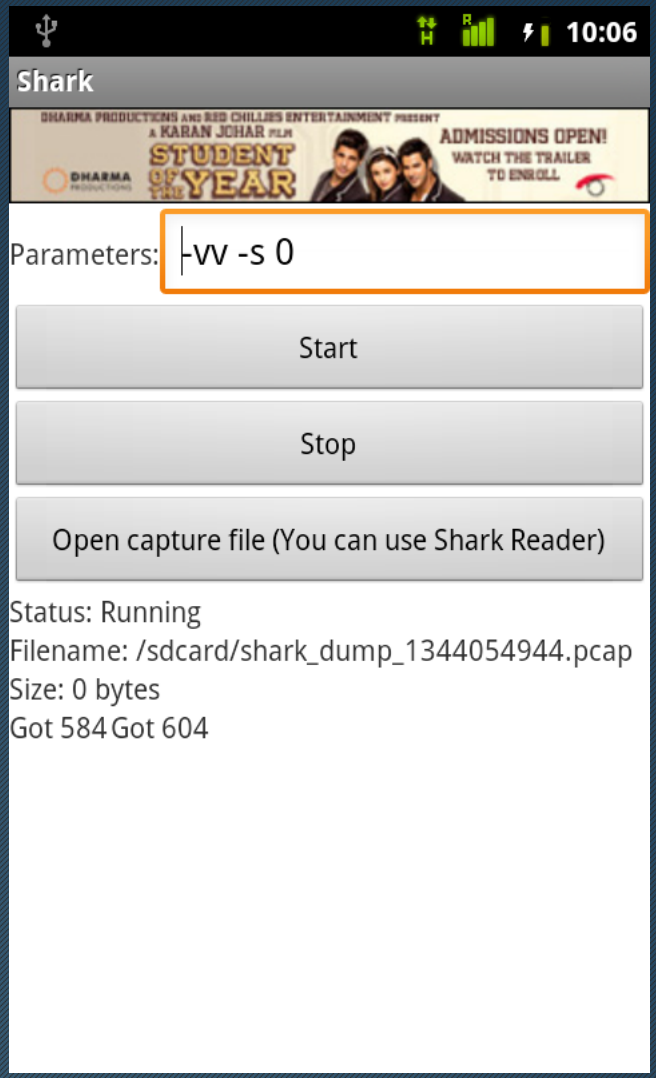
zAnti


10:32
Attack @ 192.168.1.109
Control Panel
CMD Prompt
Grab Screenshot
Eject CD
Get Process List
Execute calc
Cleanup

DroidSheep


10:01
Connected to
Spoofing IP: 192.168.1.254
http://www.google.de
IP=192.168.1.109 http://www.google.de@...
[http://www.facebook....
IP=192.168.1.107 [http://w...
Ankit Goyal [http://www.facebook.c...
IP=172.16.1.106 Ankit Goyal [http://www....
http://api.longurl.org
IP=192.168.1.132 ID: 1295603431
http://rover.ebay.in
IP=192.168.1.132 ID: 1631414886
http://search.twitter.com
IP=192.168.1.132 ID: -1813905711
http://www.espncricinfo.com
IP=192.168.1.110 ID: 1842627365
http://www.google.com
IP=192.168.1.116 ID: -1700429508
http://www.google.co.in
IP=192.168.1.116 ID: 1683548255
ARP-Spoofing
Generic mode
SPOOFING ONLY
Start

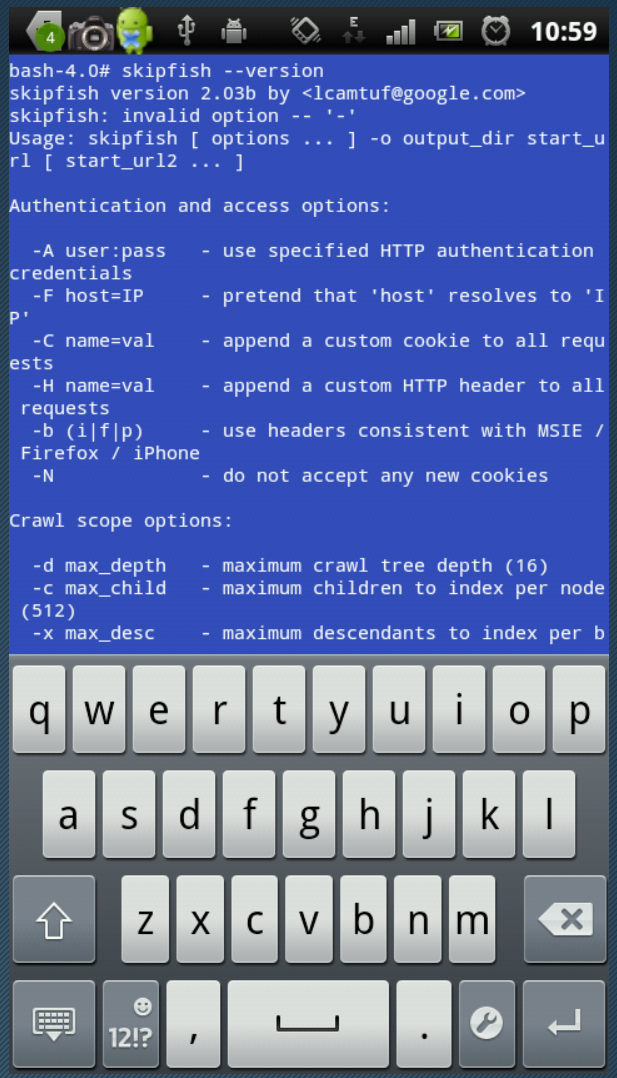
Shark


10:06
Shark
DHARMA PRODUCTIONS AND RED CHILLIES ENTERTAINMENT PRESENT
A KARAN JOHAR FILM
STUDENT OF THE YEAR
DHARMA PRODUCTIONS
ADMISSIONS OPEN!
WATCH THE TRAILER
TO ENROLL
Parameters: -vv -s 0
Start
Stop
Open capture file (You can use Shark Reader)
Status: Running
Filename: /sdcard/shark_dump_1344054944.pcap
Size: 0 bytes
Got 584 Got 604

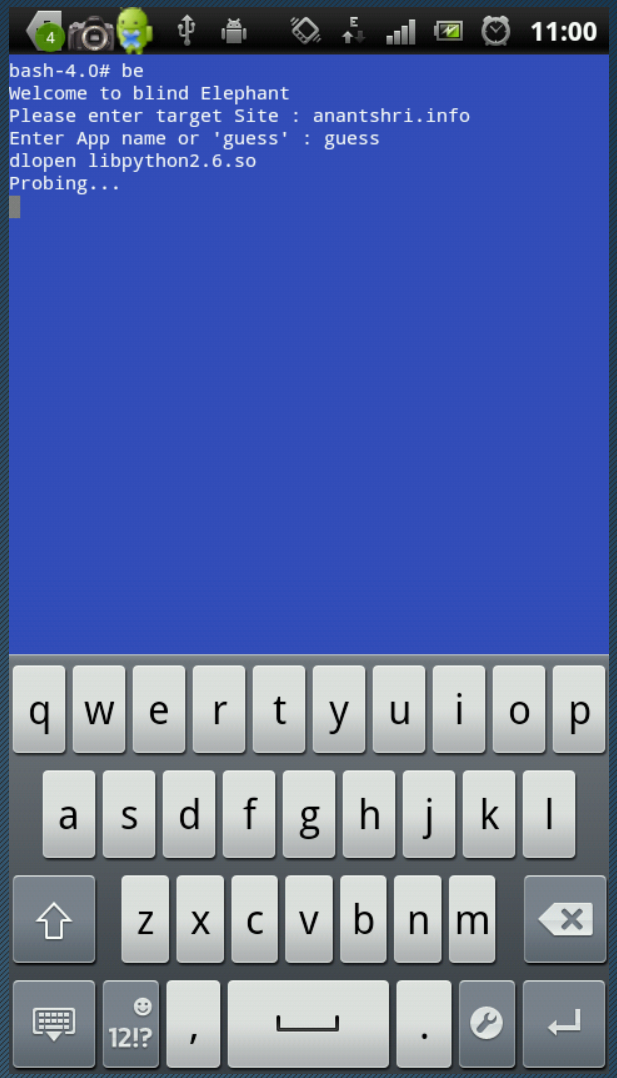
Terminal


62
10:16
$ export PATH=/data/local/bin:$PATH
$ ls
efs
config
sdcard
acct
mnt
vendor
d
etc
init
dbdata
cache
recovery.rc
default.prop
system
init.herring.rc
sbin
voodoo
recovery
sys
lpm.rc
ueventd.rc
usr
proc
init.rc
data
res
fota.rc
ueventd.herring.rc
lib
ueventd.goldfish.rc
init.goldfish.rc
tmp
dev
bin
$

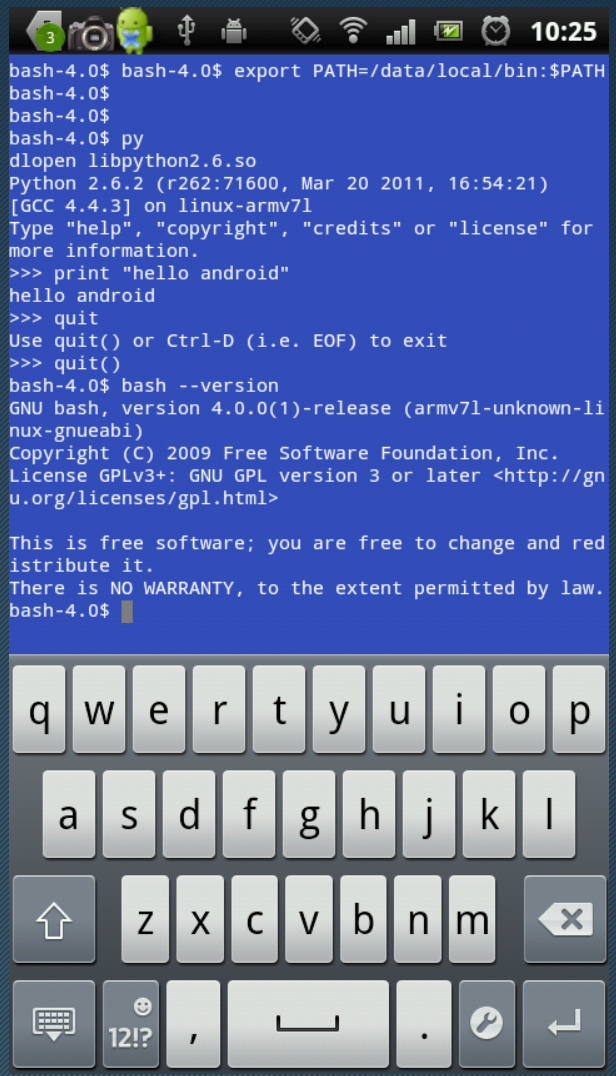
Skipfish


10:59
bash-4.0# skipfish --version
skipfish version 2.03b by <lcamtuf@google.com>
skipfish: invalid option -- '-'
Usage: skipfish [options ...] -o output_dir start_u
rl [start_url2 ...]
Authentication and access options:
-A user:pass - use specified HTTP authentication
credentials
-F host=IP - pretend that 'host' resolves to 'I
P'
-C name=val - append a custom cookie to all requ
ests
-H name=val - append a custom HTTP header to all
requests
-b (i|f|p) - use headers consistent with MSIE /
Firefox / iPhone
-N - do not accept any new cookies
Crawl scope options:
-d max_depth - maximum crawl tree depth (16)
-c max_child - maximum children to index per node
(512)
-x max_desc - maximum descendants to index per b

Blind Elephant



Shells


10:25
bash-4.0$ bash-4.0$ export PATH=/data/local/bin:$PATH
bash-4.0$
bash-4.0$
bash-4.0$ py
dlopen libpython2.6.so
Python 2.6.2 (r262:71600, Mar 20 2011, 16:54:21)
[GCC 4.4.3] on linux-armv7l
Type "help", "copyright", "credits" or "license" for
more information.
>>> print "hello android"
hello android
>>> quit
Use quit() or Ctrl-D (i.e. EOF) to exit
>>> quit()
bash-4.0$ bash --version
GNU bash, version 4.0.0(1)-release (armv7l-unknown-li
nux-gnueabi)
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gn
u.org/licenses/gpl.html>
This is free software; you are free to change and red
istribute it.
There is NO WARRANTY, to the extent permitted by law.
bash-4.0$
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
12!?
,
.

Get your Own Rocket ????

- When are you getting your own Rocket?????

Collection available as Droidcat @ your nearest playstore
http://bit.ly/w25pHq

Directed and produced by
- Anant : http://anantshri.info
- Ankur : http://hakers.info