

Name – Chaitali Raosaheb Patil

Intern ID - 297

## **Tool Name**

Kismet Bully

## **History**

Kismet Bully is a powerful wireless auditing toolkit integrated with the Kismet Wireless Framework. It includes the original 'Bully' WPS attack tool for wireless security testing.

## **Description**

Kismet Bully is a lightweight tool for WPS vulnerability detection and brute-force PIN attacks. It assesses the security posture of WPS-enabled wireless networks.

## **What Is This Tool About?**

Kismet Bully targets WPS-enabled access points for brute-force attacks.

- Identifies and audits insecure WPS implementations.
- Integrates with Kismet for real-time network analysis.

## **Key Features**

- Real-time WPS-enabled AP detection
- Brute-force WPS PIN attack support
- Session retry/resume
- Multi-chipset compatibility

- Reporting and logging

## Modules

- Kismet Core Engine
- Bully Plugin
- WPS Tracker
- Attack Dashboard
- Report Generator

## Use Cases

- Wireless penetration testing
- Security auditing
- WPS compliance checks
- Red teaming
- Vulnerability assessments

## Kismet bully Commands

```
source=wlan0:name=Foo,channel_hop=false,channel=6  
source=wlan1:name=Wifi6eCard,channel_hop=false,channel=1W6e
```

```
source=wlan0:name=Foo,channels="1,2,3,4,5,6,36HT40+"
```

```
kismet -c 'wlan0:name=Foo,channels="1,2,3,4,5,6,36HT40+"'
```

```
source=wlan0:name=Foo,add_channels="1W5,2W5,6W10"
```

```
kismet -c 'wlan0:name=Foo,add_channels="1W5,2W5,6W10"'
```

# Proof of Concept (PoC) Images

```
File Actions Edit View Help
Required arguments:
  -i, --interface N : Wireless interface in monitor mode (root required) [Auto]
  -b, --bssid macaddr : MAC address of the target access point [Auto]
  -e, --essid string : Extended SSID for the access point [Auto]

Optional arguments:
  -c, --channel N[,N...] : Channel number of AP, or list to hop [b/g] [Auto]
  -l, --lockwait N : Seconds to wait if the AP locks WPS [40]
  -o, --outfile file : Output file for messages [stdout]
  -p, --pin N : Starting pin number (7 or 8 digits) [Auto]
  -s, --source macaddr : Source (hardware) MAC address [Probe]
  -u, --lua : Lua script file
  -v, --verbosity N : Verbosity level 1-4, 1 is quietest [3]
  -w, --workdir path : Location of pin/session files [~/bully/]
  -5, --5ghz : Hop on 5GHz a/n default channel list [No]
  -B, --bruteforce : Bruteforce the WPS pin checksum digit [No]
  -F, --force : Force continue in spite of warnings [No]
  -S, --sequential : Sequential pins (do not randomize) [No]
  -T, --test : Test mode (do not inject any packets) [No]

Advanced arguments:
  -d, --pixiewps : Attempt to use pixiewps [No]
  -a, --acktime N : Deprecated/ignored [Auto]
  -r, --retries N : Resend packets N times when not acked [2]
  -m, --m13time N : Deprecated/ignored [Auto]
  -t, --timeout N : Deprecated/ignored [Auto]
  -1, --pin1delay M,N : Delay M seconds every Nth nack at M5 [0,1]
  -2, --pin2delay M,N : Delay M seconds every Nth nack at M7 [5,1]
  -A, --noacks : Disable ACK check for sent packets [No]
  -C, --nocheck : Skip CRC/FCS validation (performance) [No]
  -D, --detectlock : Detect WPS lockouts unreported by AP [No]
  -E, --eapfail : EAP Failure terminate every exchange [No]
  -L, --lockignore : Ignore WPS locks reported by the AP [No]
  -M, --m5m7nack : M5/M7 timeouts treated as WSC_NACK's [No]
  -N, --nofcs : Packets don't contain the FCS field [Auto]
  -P, --probe : Use probe request for nonbeaconing AP [No]
  -Q, --wpsinfo : Use probe request to gather WPS info [No]
  -R, --radiotap : Assume radiotap headers are present [Auto]
  -W, --windows7 : Masquerade as a Windows 7 registrar [No]
  -Z, --suppress : Suppress packet throttling algorithm [No]
  -V, --version : Print version info and exit
  -h, --help : Display this help information

No monitor mode interface specified
(aryan@kali)-[~]
```

Kismet Sort View Windows

Start Server... S

Server Console... c

Connect... c

Disconnect D

Add Source... A

Config Channel... L

Plugins >>

Preferences >>

Quit Q

Ch	Pkts	Size	
4	125	0B	kali
5	53	0B	Elapsed
6	35	849B	00:01.21
6	46	294B	Networks
6	30	0B	40
2	60	0B	Packets
1	89	11K	1065
			Pkt/Sec
			8
			Filtered
			0

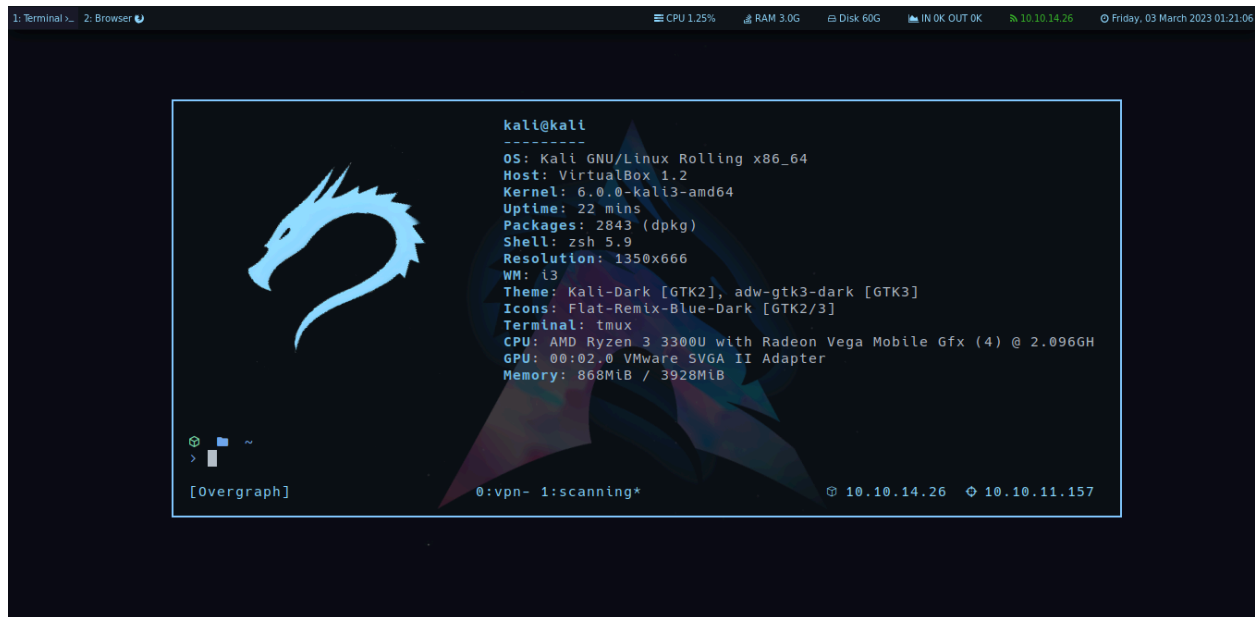
No GPS data (GPS not connected) Pwr: AC

25

0

encryption yes, channel 10, 54.00 mbit  
INFO: Detected new probe network "<Any>", BSSID 28:6A:BA:47:8A:35, encryption no, channel 0, 54.00 mbit  
INFO: Detected new probe network "Fuck off leech", BSSID CC:9E:00:1A:E1:79, encryption no, channel 0, 54.00 mbit

wlan0  
Hop



```
[vps-admin@srv515631:~$ diff -c 1.txt 2.txt
*** 1.txt      2024-07-30 04:59:41.015519052 +0000
--- 2.txt      2024-08-06 10:36:44.771006073 +0000
*****
*** 1,6 ****
    HOSTINGER
!  hostinger
    HSTNGR
    hstngr
!  HSTR
    hstr
--- 1,6 ----
    HOSTINGER
!  hostingers
    HSTNGR
    hstngr
!  HSTRS
    hstr
```

```
vps-admin@srv515631:~$ ping 8.8.8.8 | tee -a test_network.txt
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=0.919 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=0.974 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=0.934 ms
^Cvps-admin@srv515631:~$ cat test_network.txt
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=0.919 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=0.974 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=0.934 ms
```

## 15-Liner Summary

1. Wireless audit tool
2. WPS vulnerability targeting
3. Real-time scanning
4. Kismet integration
5. Multi-chipset support
6. Attack automation
7. Retry/resume sessions
8. Passive mode
9. Linux compatible
10. CLI-based
11. Logs reports
12. Portable
13. Red team utility
14. Recon friendly

15. Open-source

## **Best Use Time**

- During wireless audits
- Red team exercises
- Penetration testing
- Physical assessments
- War-driving

## **When to Use in Investigation**

- Pre-engagement Wi-Fi recon
- Insecure AP identification
- Brute-force test scenarios
- Wireless security documentation

## **Best Users & Skills**

Best Users:

- Wireless Pentester
- Red Teamer- Security Auditor

Skills:

- Linux command line
- Wireless protocol knowledge
- Kismet experience

- Understanding WPS attacks

## **Flaws & Suggestions**

- High WPS lockout delays
- Chipset dependencies
- No GUI module
- Limited reporting
- Hidden SSID detection weak

## **Good About the Tool**

- Quick auditing
- CLI portable
- Kismet integration
- WPS test efficiency
- Strong log output