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

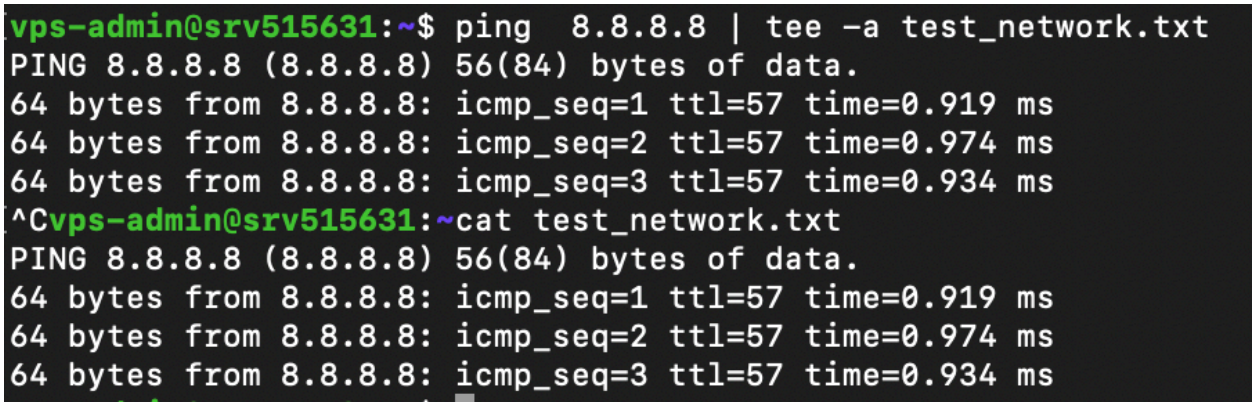
- Wireless penetration testing
- Security auditing
- WPS compliance checks
- Red teaming
- Vulnerability assessments

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


```
[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
```



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