<https://github.com/lanmaster53/recon-ng>

**🧨 1. Google BreachAlarm – *(Deprecated)***

**❓ What was BreachAlarm?**

**BreachAlarm** was an online service (similar to “Have I Been Pwned?”) that:

* Monitored stolen email addresses in **data breaches**
* Sent alerts if your email showed up in leaked databases
* Helped companies **detect exposed employee emails**

**🪦 Why is it deprecated?**

* The service has **shut down**
* Its role has been taken over by more robust platforms like:
  + [HaveIBeenPwned](https://haveibeenpwned.com/)
  + [Firefox Monitor](https://monitor.firefox.com/)
  + [Dehashed.com](https://www.dehashed.com/) *(for advanced users)*

🧠 **Why it mattered?**  
Knowing if your info was breached helps you:

* Change passwords
* Monitor accounts
* Warn employees or customers early

**🧠 2. Recon-ng – *OSINT Framework (Like Metasploit but for Recon)***

**🔧 What is Recon-ng?**

**Recon-ng** is a **powerful open-source reconnaissance tool** used by ethical hackers for gathering information from public sources (OSINT).

Think of it like:

💻 “Kali Linux for Recon”  
🧩 Modules = like plugins (for scanning domains, emails, IPs)

**⚙️ Features**

| **Feature** | **Description** |
| --- | --- |
| 🔍 Domain Recon | Find subdomains, WHOIS info, records |
| 📧 Email Harvesting | Discover public emails using APIs |
| 📡 IP Recon | Get geolocation, reverse DNS, etc. |
| 🌐 Web APIs | Connect to services like Shodan, HaveIBeenPwned, VirusTotal |
| 📊 Reporting | Exports data in CSV, JSON, HTML formats |

**🧪 How to Use It (Simple Steps)**

1. **Launch Recon-ng**

recon-ng

1. **Create a workspace**

workspaces create your\_project\_name

1. **Add domain target**

add domains example.com

1. **Use a module (e.g. search subdomains)**

modules load recon/domains-hosts/bing\_domain\_web

1. **Set the source**

options set SOURCE example.com

1. **Run the module**

run

1. **View results**

show hosts

**📌 Popular Modules to Explore**

| **Module Path** | **Purpose** |
| --- | --- |
| recon/domains-hosts/google\_site\_web | Find subdomains |
| recon/hosts-hosts/resolve | IP resolution |
| recon/hosts-ports/shodan\_hostname | Port + service info via Shodan |
| recon/contacts-credentials/hibp\_breach | Check if emails are pwned |

**🤯 Why is it Important?**

Recon-ng helps you:

* Save time (automates multiple tools)
* Get deep data from APIs
* Organize findings neatly
* Perform **stealthy passive recon** (no alerting targets)

**✅ Summary**

| **Tool** | **Status** | **Use Case** |
| --- | --- | --- |
| **BreachAlarm** | ❌ Deprecated | Warn about breached emails |
| **Recon-ng** | ✅ Active | Full-featured OSINT recon framework |