The Harvester

The Harvester is used for e-mail harvesting across several search engines. If an organization doesn't have a public employee directory, this can be a quick way to gather email addresses for phishing or searching for passwords in recent database dumps.

For example:

theharvester -d microsoft.com -b google -l 5

The domain is specified by -d and the data source with -b (Google). Search results can be limited with the -l option.

Recon-ng

Recon-ng is a Metasploit-style reconnaissance framework which can harvest emails and also check data dumps for passwords:

modules search

modules load recon/contacts-credentials/hibp\_breach

[recon-ng][default][hibp\_breach] > options list

options set source info@microsoft.com

Similar to Metasploit, you can select specific data dumps and set the source email to search.

haveibeenpwnd >>> for data leaked