

Ex. No. 2	Passive Reconnaissance (OSINT)
Date of Exercise	28/08/23

Aim:

To gather information about targeted computers and networks without actively engaging with the systems.

Description:

dnstwist is a domain name permutation engine for detecting typosquatting, phishing and corporate espionage. dnstwist takes in your domain name as a seed, generates a list of potential phishing domains and then checks to see if they are registered.

DNS fuzzing is an automated workflow that aims to uncover potentially malicious domains that target your organization. This tool generates a comprehensive list of permutations based on a provided domain name, and subsequently verifies whether any of these permutations are in use.

```
$ dnstwist --dictionary dictionaries/english.dict domain.name
```

```
$ dnstwist --tld dictionaries/common_tlds.dict domain.name
```

```
$ dnstwist --fuzzers homoglyph,hyphenation domain.name
```

TheHarvester is a command-line tool included in Kali Linux that acts as a wrapper for a variety of search engines and is used to find email accounts, subdomain names, virtual hosts, open ports / banners, and employee names related to a domain from different public sources (such as search engines and PGP key servers).

usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s]

[--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t]

[-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME] [-b SOURCE]

Output:

DnsTwist

```
(root@kali)-[~]
# dnstwist google.com

{20230509}

permutations: 100.00% of 3612 | found: 258 | eta: 0m 00s | speed: 8 qps

*original      google.com      142.250.205.238 2404:6800:4007:818::200e NS:ns1.go
ogle.com MX:smtp.google.com
addition       googlek.com     !ServFail !ServFail NS:!ServFail
addition       googlem.com     107.161.23.204 NS:ns1.dnsowl.com
addition       googlew.com     107.161.23.204 NS:ns1.dnsowl.com
addition       googlez.com     13.248.169.48 NS:ns3.afternic.com MX:
addition       googlee.com     142.250.196.164 2404:6800:4007:82c::2004 NS:ns1.go
ogle.com MX:
addition       googlei.com     162.210.196.166 NS:ns1.quokkadns.com
addition       google4.com     185.53.177.54 NS:ns1.parkingcrew.net MX:mail.b.ema
```

```
root@kali: ~
File Edit View Search Terminal Help
replacement googl3.com NS:ns24.domaincontrol.com MX:mailstore1.secureserv
er.net
replacement googl4.com -
replacement googls.com NS:ns1.googledomains.com
replacement googlw.com NS:dns1.name-services.com MX:mx.googlw.com.cust.a.
hostedemail.com
replacement googlz.com -
replacement googpe.com NS:ns1.googledomains.com
replacement gopgle.com NS:ns1.googledomains.com
subdomain g.oogole.com 104.21.19.57 2606:4700:3032::ac43:b945
subdomain goo.gle.com 13.248.169.48 NS:ns5.afternic.com MX:
subdomain go.oogole.com -
subdomain goog.le.com -
transposition oogle.com 142.250.182.36 2404:6800:4007:823::2004 NS:ns1.goo
gle.com MX:
transposition googel.com 142.250.195.132 2404:6800:4007:825::2004 NS:ns1.go
ogle.com MX:
transposition gogole.com 142.250.196.4 2404:6800:4007:82a::2004 NS:ns1.goog
le.com MX:
transposition goolge.com 142.250.77.100 2404:6800:4007:812::2004 NS:ns1.goo
gle.com MX:
various googlecom.com 142.250.205.228 2404:6800:4007:82d::2004 NS:ns1.go
ogle.com MX:
vowel-swan gangle.com 107.180.51.12 NS:ns25.domaincontrol.com MX:mail.ea
```

The Harvester:

```
(root@kali)~# theHarvester -d tesla.com -l 300 -b google

*****
*                                     *
* [theHarvester]                   *
* [theHarvester]                   *
* theHarvester 4.0.3                *
* Coded by Christian Martorella     *
* Edge-Security Research            *
* cmartorella@edge-security.com     *
*                                     *
*****

You have chosen to open:
[*] Target: tesla.com
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
    Searching 300 results.
[*] Searching Google.
```

```
[*] No IPs found.

[*] Emails found: 3
customersupport@tesla.com
resolutions@tesla.com
vulnerabilityreporting@tesla.com

[*] Hosts found: 7
digitalassets-secure.tesla.com:151.101.130.92, 151.101.2.92, 151.101.66.92, 1
51.101.194.92
ir.tesla.com:104.120.58.166
static-assets.tesla.com:104.120.58.166
www.tesla.com:104.120.58.166
x22ir.tesla.com
x22www.tesla.com

(root@kali)~# theHarvester -d carminesnyc.com -l 300 -b google
```

```
[*] Target: carminesnyc.com
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
    Searching 300 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 5
```

```
aesparza@carminesnyc.com  
dj@carminesnyc.com  
j.smith@carminesnyc.com  
john@carminesnyc.com  
x22john@carminesnyc.com  
  
[*] Hosts found: 3  
  
www.carminesnyc.com:104.26.0.99, 104.26.1.99, 172.67.74.42  
x22www.carminesnyc.com:67.227.199.194
```

Result:

Using Harvester and Dnstwist we have successfully found information of the targeted systems.