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).

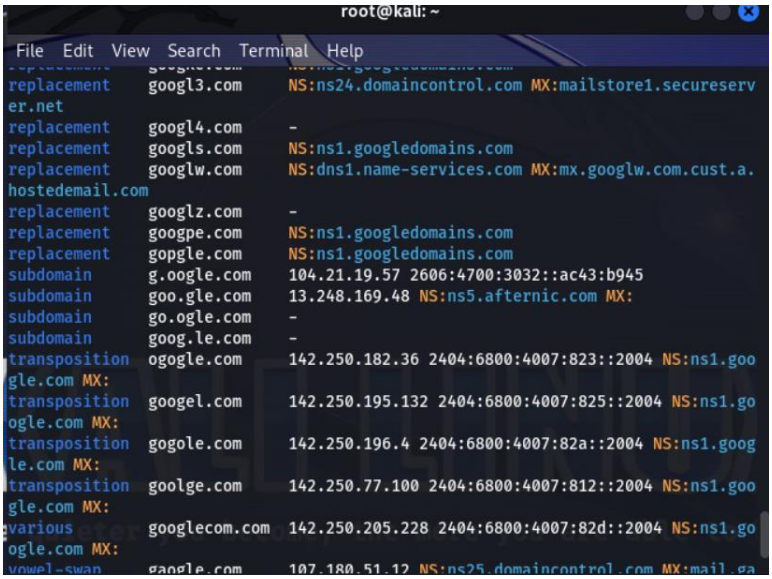
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s]

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

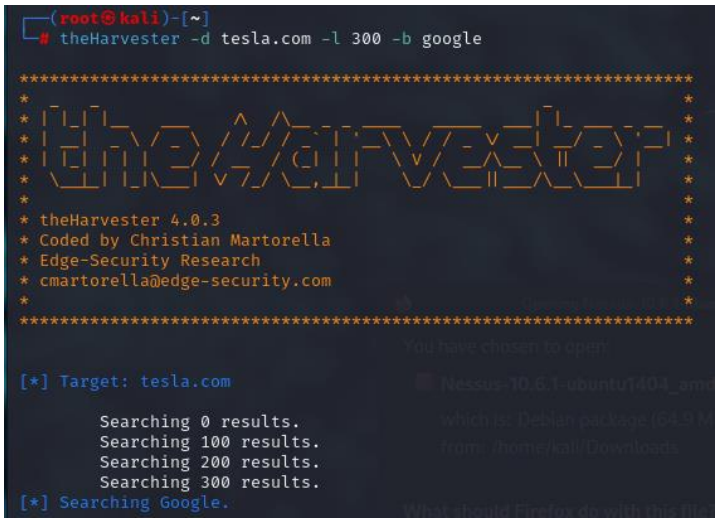
[-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME] [-b SOURCE]

Output:

DnsTwist



The Harvester:



Result:

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