Cyber security lab

Exercise 3:

1. Perform practical approach to implement Footprinting-Gathering target information using Dmitry-Dmagic, UAtester

Aim:

Dmitry ( Deep magic Information Gathering Tool) is a command line utility included in Kali Linux. It is designed to allow a user to collect public information about a target host. It can be used to gather a number of valuable pieces of information,

**Usages of Dmitry Tool :**

1. The who is details of a target host. This will provide information about a registered domain, such as the name, address, and contact information of the person who registered it.
2. The net craft data for a target host. This can include details such as the operating system
3. Dmitry Tool can be used to search **subdomains** of the target.
4. Dmitry Tool can be used to find **open ports** of the target system.
5. Dmitry Tool can be used to perform **TCP scan**.
6. Dmitry Tool can be used with netcraft service to get the target information such as **operating system, web server details, web host details, hosting service details**, etc.
7. Dmitry Tool can be used with whois service to get the target information such as **registered domain**, **name**, **address**, the **contact information** of the person who registered it.
8. Dmitry Tool can be used to get**email addresses** that are associated with the domain of the target.

┌──(root㉿kali)-[/home/kali]

└─# dmitry --version

Deepmagic Information Gathering Tool

"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host

-o Save output to %host.txt or to file specified by -o file

-i Perform a whois lookup on the IP address of a host

-w Perform a whois lookup on the domain name of a host

-n Retrieve Netcraft.com information on a host

-s Perform a search for possible subdomains

-e Perform a search for possible email addresses

-p Perform a TCP port scan on a host

\* -f Perform a TCP port scan on a host showing output reporting filtered ports

\* -b Read in the banner received from the scanned port

\* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )

\*Requires the -p flagged to be passed