Information Gathering

- Information Gathering is the process of Gathering Important information about the Target of Assessment .

- This is a Pre-Attack

- This is also called as reconnaissance/foot printing/information Gathering

WEBSITES TO GATHER PASSIVE INFORMATION

www.who.is
www.netcraft.com
www.technicalinfo.net
www.dnsstuff.com
www.centralops.com
www.robtex.com

Passive reconnaissance

Passive reconnaissance:
In Passive IG we do not directly engage with the target Instead we use search engine, social media, Job sites and search other websites to gather info about target
Passive reconnaissance is used to gather publicly available information (network, organization, email id, mobile no , contact details And DNS info)

Passive reconnaissance techniques:

1. Who is
2. NSLookup (windows)/(Linux)
3. Netcraft
4. Maltego tool

NSLOOKUP It is a command line tool used to query DNS to obtain IP Address of the target

Usage

To find A record nslookup <domain name>
e.g. nslookup google.com

To check ns record
nslookup-type=ns <domain name> → nslookup-type=ns example.com

To check the MX record
nslookup-type=mx<domain name> → nslookup-type=mx example.com

To check all available DNS records
Nslookup-type=any example.com

To check domain name from IP Address
nslookup <Target Domain name>

knockpy

Subdomain Enumeration

Knockpy is a python tool used to enumerate subdomains of target machine
1.sudo apt-get install python-dnspython
2.git clone https://github.com/guelfoweb/knock
3.cd knock
4.cd knockpy
5.sudo python setup.py install Usage: python knockpy.py example.com / knockpy example.com

Google Hacking Database

- What A hacker can do with Google Hacking?
- Pages containing network or vulnerability data
- Pages containing logon portals
- Sensitive Directories
- Files Containing Passwords
- Error Messages that containing sensitive information
- Advisories and server vulnerabilities

Examples

- http://www.balpom.ru/obmen-opytom/03_huawei_e392_pod_clearos_6/wvdial.conf
- http://elcto.com/.env
- http://www.freezy.cz/blog/id30/wvdia
- http://www.meridianinvest.com/_wp/wp-content/uploads/wpsc/

Google Hacking

Search Operators using Google:

- Google uses advanced search engine operators to gather information
- Site: Narrow search to a particular domain or subdomain site:Microsoft.com
- Link: List all the pages that has link to specified webpage link:www.microsoft.com
- info: Give information about the webpage Info:www.microsoft.com
- Related: It will list the webpages that are similar to the specified webpage. Related:www.google.com

Google Hacking

filetype: Find documents of the specified type

- Antivirus filetype:ppt

Intitle: Restricts the results to documents containing that word in the title

- intitle:google search

Inurl: Restricts the results to documents containing that word in the title

- inurl:google search

allintitle: Restricts results to those with all of the query words in the title.

- allintitle:google search

allinurl: Restricts results to those with all of the query words in the title.

- allinurl:google search
- allintext: All query words must appear the in text of the page

Email harvesting

- Email harvesting is the process of obtaining lists of email addresses using various methods for use in bulk email or other purposes usually grouped as spam.
- The effective way of finding emails and usernames belonging to the organisation.

• Manual : By using google.com , bing.com, yandex.com, yahoo.com etc…

• Automated : Theharvester

- -d: domain to search or company name. -b: data source (google, Bing, LinkedIn etc). -f: save the file into html or xml file. -l: limit the number of results to work with.
- theharvester -d Microsoft.com -l 500 -b google

Maltego

- Maltego is a data mining tool built in kali Linux.
- It is used to gather information about an individual or network
- It has the capability to gather significant amount of information about a target in a single sweep
- It displays the data in GUI format