20CYS114 - Cyber Security Essentials

Lab 7 – Open-Source Intelligence (OSINT)

For each of the following steps complete the task and include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and to answer each question in your report.

Lab Environment:

This lab Demonstrate how to gather information about public domains.

Task 1: OSINT

Read and understand about OSINT. Write about OSINT in your own language.

Task 2: WHOIS

Go to https://www.whois.com/ and search for any website. See what all information you are getting about that domain.

Task 4: shodan and ipinfo

Go to https://www.shodan.io/ and search for some website. See what all information you are getting from there. Select one IP from the result and search it on https://ipinfo.io/ website.

Task 3: Google Hacking

Read about google hacking and make a note on it. Use below commands after changing the website name and searched text 'report'. You can choose any website and text of your own.

Operator	Searches	Example
`site`	A specific site.	`site:comptia.org report` to search CompTIA's website only for results including the text "report".
`link`	For pages that link to the specified page.	`link:comptia.org report` to search for any pages that link to CompTIA's website and have the text "report" anywhere on the page.
`filetype`	For specific file types.	`filetype:pdf report` to search for PDFs including the text "report".
`intitle`	For page titles.	`intitle:Certification report` to search for any pages whose titles include the text "Certification" and have the text "report" anywhere on the page.
`inurl`	For URLs.	`inurl:Certification report` to search for any pages whose URLs include the text "Certification" and have the text "report" anywhere on the page.
`inanchor`	For anchor text.	`inanchor:Certification report` to search for any pages whose anchor text includes the text "Certification" and have the text "report" anywhere on the page.

Task 4: Go through below website, search for any URL and document your finding.

Best Search Engines For Security Professionals And Pen Testers

Shodan — shodan.io
Censys — censys.io
Hunter — hunter.io
GreyNoise — viz.greynoise.io
ZoomEye — zoomeye.org
WiGLE — wigle.net
PublicWWW — publicwww.com
Pulsedive — pulsedive.com
Intelligence X — intelx.io
Reposify — reposify.com