Linux Learning Centre

Passive Information Gathering

LLC 500 Cybersecurity and Ethical Hacking

www.linuxlearningcentre.co.ke

Website Reconnsaisance

It is the practice of covertly discovering and collecting information about a website.
Site reconnaissance is gaining knowledge by directly observing the site.
Recon in general Will be described as information collection/OSINT/Discovery Etc.

Two Types in general:
Active and passive recon

Website Recon tools

- BlindElephant - https://github.com/lokifer/BlindElephant
- CMS detection and exploitation - https://github.com/Tuhinshubhra/CMSeeK
- CMSmap reconnaissance tool for popular CMS frameworks https://github.com/Dionach/CMSmap
- Gitem (GitHub organization reconnaissance tool) https://github.com/mschwager/gitem
- Recon-ng (web reconnaissance framework) https://github.com/lanmaster53/recon-ng
- Recox https://github.com/samhaxr/recox

Website Recon tools

- VHostScan (virtual host scanner)
  https://github.com/codingo/VHostScan
- Wappalyzer (discovery of technology stack)
  https://github.com/wappalyzer/wappalyzer
- detectem (software enumeration)
  https://github.com/alertot/detectem
- shcheck (test HTTP headers of web applications)
  https://github.com/santoru/shcheck
- Fsociety Hacking Tools Pack
  https://github.com/Manisso/fsociety

Netcraft

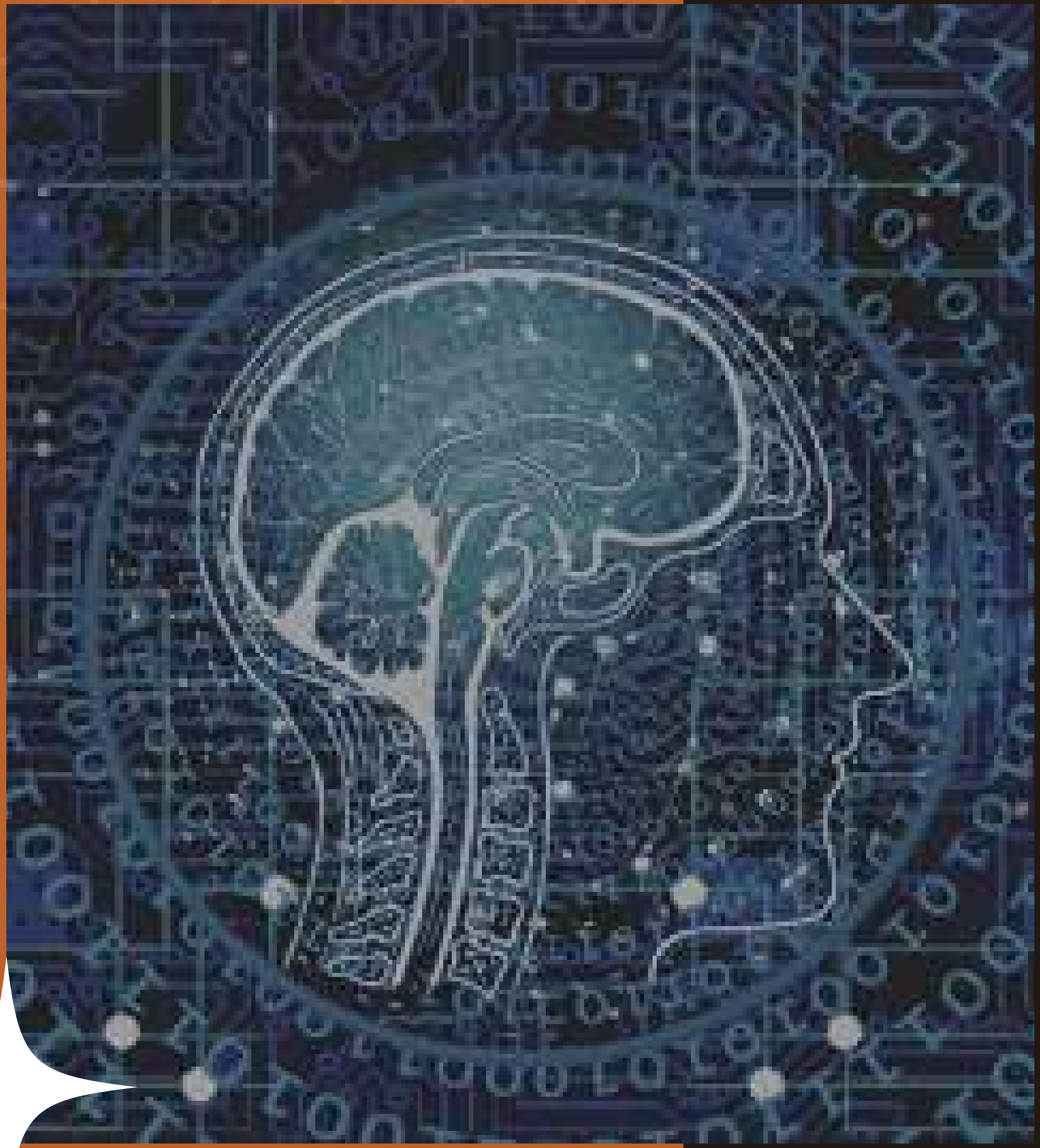
Netcraft is an internet service association that provides detailed data about the web facilitating and the Server with point-by-point data on what is running on the server alongside the IP, Whois data, server-side technologies, and so on. This information ought to be saved in your reports with the goal that you can utilize all the data to find the correct testing methodology and characterize the attack surface, which is the essential piece of a pentest.

https://www.netcraft.com/

Shodan.io

Shodan is a search engine that lets the user find specific types of computers connected to the internet using a variety of filters.

Shodan is a search engine for hackers. You know Google, Bing, Yahoo, and DuckDuckGo all crawls front end web pages. Shodan crawls the IPs for devices such as printers, security cameras, Refrigerators, and routers, which are connected to internet.(IOT Devices)



Shodan Dorks

- device in particular area like in a country - ***country:"IN"***
- a particular city - ***city:"Washington"***
- geographical co-ordinates:- ***geo:"47.751076, -120.740135"***
- a particular organization - ***org:"Facebook"***
- You can filter windows RDP password by searching ***"\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00"***
- find default router page with default password:- ***html:"def_wirelesspassword"***
- webcams connected worldwide: ***("webcam 7" OR "webcamXP") http.component:"mootools" -401***
- Printers: ***"Serial Number:" "Built:" "Server: HP HTTP"***
- Epson Printer - ***"SERVER: EPSON_Linux UPnP" "200 OK"***
- Mongo DB Servers: - ***"MongoDB Server Information" port:27017 -authentication***
- Misconfigured Wordpress Sites: ***http.html:"* The wp-config.php creation script uses this file"***
- Reference: - ***https://github.com/jakejarvis/awesome-shodan-queries***

Pastebin

01 Text-sharing “pastebin” sites, such as Pastebin are a popular repository of compromised data

02 perpetrators of computer breaches post the data they have stolen on such sites. Sometimes, sensitive information is unwittingly leaked by a company’s employee.

03 Cool Codes
https://pastebin.com/5mwBqXSH

04 Databases
https://pastebin.com/DiLTsthW

Email harvesting

Email harvesting is an effective way of finding emails, and possibly usernames, belonging to an organization.

These emails are useful in many ways, such as providing us a potential list for client side attacks, revealing the naming convention used in the organization, or mapping out users in the organization.

```
$ theHarvester -d cisco.com -b google >ciscoemails.txt
```

Password Dumps

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches.

This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts

https://haveibeenpwned.com/

https://haveibeenpwned.com/Passwords

OSINT FRAMEWORK

OSINT

OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources.

It can be used to extract data by analyzing various public platforms. These platforms include news, image, social media platforms, etc.

https://osintframework.com/

Maltego

Maltego is a data mining tool that mines a variety of open-source data resources and uses that data to create graphs for analyzing connections.

- The graphs allow you to easily make connections between information such as name, email organizational structure, domains, documents, etc

Reference
https://wondersmithrae.medium.com/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc

DNS Enumeration

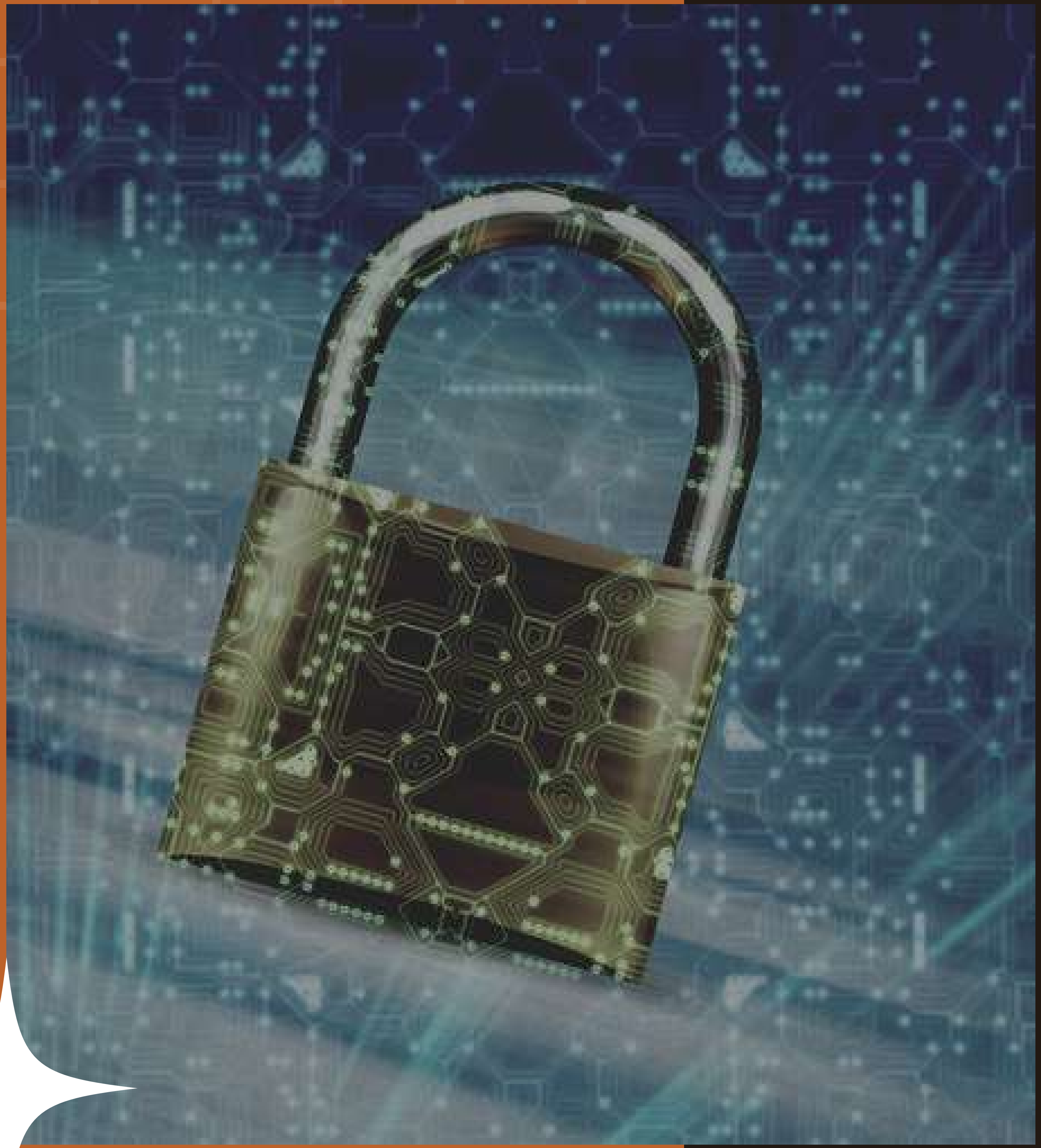
DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

https://www.nslookup.io/

```
dnsrecon -d www.cisco.com
dig cisco.com -t ns +short
host cisco.com
```

OSINT TOOLS

- https://github.com/ThoughtfulDev/EagleEye
- https://github.com/DataSploit/datasploit
- https://github.com/threat9/routersploit
- https://github.com/tweepy/tweepy
- https://nmap.org/zenmap/



CYBER SEC CONFERENCES

https://media.defcon.org/
https://www.blackhat.com/html/archives.html
https://conference.africahackon.com/

https://twitter.com/cyberspeaklc?lang=en
https://twitter.com/shehacks_ke

Mathematics | 2023

www.linuxlearningcentre.co.ke

INFORMATION GATHERING

Presentation by **Linux Learning Centre Ltd**

LLC 500 Cybersecurity and Ethical Hacking