NAME:- SANI ASHIRU YAHAYA
STUDENT ID:- IDEAS/24/7780
EMAIL:- Ashirusani92@gmail.com

Week 1: Reconnaissance, Information Gathering, and Scanning Assignments

INT302: Kali Linux Tools and System Security – Lab 1: Reconnaissance (Information Gathering)

Lab Overview

This lab will guide you through essential reconnaissance techniques to gather preliminary information about a target system or domain during penetration testing. You'll learn to identify IP addresses, retrieve domain registration details, and perform DNS lookups using popular Linux tools such as ping, whois, and nslookup. This hands-on experience will help you gather data that is crucial for vulnerability assessment and further penetration testing.

Step 1: Get the IP Address of a Domain Using ping

The ping command helps you verify the reachability of a domain and returns its IP address.
Instructions:

1. **Open your Terminal in Kali Linux.**
2. **Run the ping command followed by the domain name you want to investigate.**

Command Syntax:

```
ping <domain>
```

Exercise 1:
Use the ping command to find the IP addresses of the following domains

•facebook.com
•twitter.com
•amazon.com

Answers:
1.facebook.com: __**102.132.101.35**
2.twitter.com: __**104.244.42.1**
3.amazon.com:__**52.94.236.248**

Step 2: Retrieve Domain Registration Details Using whois

The whois command fetches domain registration details such as registrar, creation date, and expiration date.
Instructions:
1.
In the terminal, use the whois command followed by the domain name.
Command Syntax:

```
whois <domain>
```

Exercise 2:
Run the whois command for the following domains:
- github.com

- linkedin.com
- apple.com

Answers

1. What is the registration expiration date for github.com? _____**2007-10-09T18:20:50Z**

2.Who is the registrar for linkedin.com? ____ **Network Solutions, LLC**

3.What country is the registrant of apple.com from? ____ **US**

Step 3: **Perform a DNS Lookup Using nslookup**

The nslookup command queries DNS servers to retrieve DNS records and IP addresses.
Instructions:

1. Run the nslookup command followed by the domain name.
Command Syntax:

```
nslookup <domain>
```

Exercise 3:

Use nslookup to look up DNS information for the following domains:

- bbc.co.uk
- netflix.com

Answer :

1.What is the IP address for bbc.co.uk? ___**192.168.229.2#53**

2.What are the name servers (NS) for netflix.com? ____**_netflix.com**

INT302: Kali Linux Tools and System Security – Lab 2: Website Enumeration and Information Gathering

Lab Overview
This lab focuses on website enumeration and information gathering techniques that are essential in the reconnaissance phase of penetration testing. You will learn to detect web technologies used by a target website and perform aggressive scanning to gather detailed information. We will utilize the whatweb tool, a powerful utility designed for identifying web technologies.

Lab Objectives

By the end of this lab, you will:

1. Detect web technologies used by a website or server using the whatweb command.
2.Perform aggressive scanning on a target IP address or URL to extract detailed information about its web technologies.

Tools Used

- Kali Linux: A Linux distribution tailored for penetration testing.
- Terminal: The command-line interface to execute commands.

Prerequisites

- Basic knowledge of Kali Linux and command-line operations.
- Internet access to perform scans on live web servers.
- whatweb installed in your Kali Linux environment (it usually comes pre-installed).

Step 1: Detect Web Technologies Using whatweb
The whatweb command allows you to identify the technologies used by a web application, including the server type, programming languages, and content management systems.
Instructions:
1. Open your Terminal in Kali Linux.
2.Use the whatweb command followed by the target IP address or URL.
Command Syntax:

```
whatweb <IP address or URL>
```

Expected Output: The output will display various technologies detected on the specified web server, including web server software, programming languages, frameworks, and more.
Exercise 1:
Run the whatweb command to detect technologies for the following targets:

- example.com
- stackoverflow.com
- github.com

Record Your Findings:

1. **example.com:** ______ttp://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[ECAcc (nyd/D147)], IP[93.184.215.14], Title[Example Domain]

2. **stackoverflow.com**____http://stockoverflow.com [404 Not Found] IP[185.83.219.2], UncommonHeaders[x-content-type-options]

3. **Github.com:**______http://github.com [301 Moved Permanently] Country[UNITED STATES][US], IP[140.82.121.3], RedirectLocation[https://github.com/]
https://github.com/ [200 OK] Content-Language[en-US], Cookies[_gh_sess,_octo,logged_in], Country[UNITED STATES][US], HTML5, HTTPServer[GitHub.com], HttpOnly[_gh_sess,logged_in], IP[140.82.121.3], Open-Graph-Protocol[object][1401488693436528], OpenSearch[/opensearch.xml], Script[application/javascript,application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubdomains; preload], Title[GitHub · Build and ship software on a single, collaborative platform · GitHub], UncommonHeaders[x-content-type-options,referrer-policy,content-security-policy,x-github-request-id], X-Frame-Options[deny], X-XSS-Protection[0]

Step 2: Perform Aggressive Scanning Using whatweb

The --aggression option allows for more thorough scanning by enabling additional checks, which can reveal more information about the target.

Instructions:

1. In the terminal, run the whatweb command with the --aggression option.
Command Syntax:

```
whatweb --aggression 3 -v <IP address or URL>
```

Exercise 2: Perform an aggressive scan on the following targets:

- google.com
- facebook.com

Record Your Findings:

1. google.com: _________WhatWeb report for http://google.com

```
Status    : 301 Moved Permanently
Title     : 301 Moved
IP        : 142.250.185.14
Country   : UNITED STATES, US

Summary   : HTTPServer[gws], RedirectLocation[http://www.google.com/],
UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

Detected Plugins:
[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
    identify the operating system from the server header.

    String       : gws (from server string)

[ RedirectLocation ]
    HTTP Server string location. used with http-status 301 and
    302

    String       : http://www.google.com/ (from location)

[ UncommonHeaders ]
    Uncommon HTTP server headers. The blacklist includes all
    the standard headers and many non standard but common ones.
    Interesting but fairly common headers should have their own
    plugins, eg. x-powered-by, server and x-aspnet-version.
    Info about headers can be found at www.http-stats.com

    String       : content-security-policy-report-only (from headers)

[ X-Frame-Options ]
    This plugin retrieves the X-Frame-Options value from the
    HTTP header. - More Info:
    http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
    aspx

    String       : SAMEORIGIN

[ X-XSS-Protection ]
    This plugin retrieves the X-XSS-Protection value from the
    HTTP header. - More Info:
    http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
    aspx

    String       : 0

HTTP Headers:
    HTTP/1.1 301 Moved Permanently
    Location: http://www.google.com/
    Content-Type: text/html; charset=UTF-8
    Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-HCTztaK3AKAuEh5w1ogu_A'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
    Date: Sat, 02 Nov 2024 23:58:33 GMT
    Expires: Mon, 02 Dec 2024 23:58:33 GMT
    Cache-Control: public, max-age=2592000
    Server: gws
    Content-Length: 219
    X-XSS-Protection: 0
    X-Frame-Options: SAMEORIGIN
    Connection: close

WhatWeb report for http://www.google.com/
Status    : 200 OK
Title     : Google
IP        : 216.58.223.196
Country   : UNITED STATES, US

Summary   : Cookies[AEC,NID], HTML5, HTTPServer[gws], HttpOnly[AEC,NID], Script,
UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

Detected Plugins:
[ Cookies ]
    Display the names of cookies in the HTTP headers. The
    values are not returned to save on space.

    String       : AEC
    String       : NID

[ HTML5 ]
    HTML version 5, detected by the doctype declaration


[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
    identify the operating system from the server header.

    String       : gws (from server string)

[ HttpOnly ]
    If the HttpOnly flag is included in the HTTP set-cookie
    response header and the browser supports it then the cookie
    cannot be accessed through client side script - More Info:
    http://en.wikipedia.org/wiki/HTTP_cookie

    String       : AEC,NID

[ Script ]
    This plugin detects instances of script HTML elements and
    returns the script language/type.


[ UncommonHeaders ]
    Uncommon HTTP server headers. The blacklist includes all
    the standard headers and many non standard but common ones.
    Interesting but fairly common headers should have their own
    plugins, eg. x-powered-by, server and x-aspnet-version.
    Info about headers can be found at www.http-stats.com
```

```
	String       : content-security-policy-report-only (from headers)

[ X-Frame-Options ]
	This plugin retrieves the X-Frame-Options value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : SAMEORIGIN

[ X-XSS-Protection ]
	This plugin retrieves the X-XSS-Protection value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : 0

HTTP Headers:
	HTTP/1.1 200 OK
	Date: Sat, 02 Nov 2024 23:58:35 GMT
	Expires: -1
	Cache-Control: private, max-age=0
	Content-Type: text/html; charset=ISO-8859-1
	Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-6cBJdDhoyHSxRePpo8YncA'
'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
	P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
	Content-Encoding: gzip
	Server: gws
	Content-Length: 9014
	X-XSS-Protection: 0
	X-Frame-Options: SAMEORIGIN
	Set-Cookie: AEC=AVYB7crdLDysy4VeVgViNo-AfuLkyXiLk1ddqblDVTT8IdDjl50UKUBgvg; expires=Thu,
01-May-2025 23:58:35 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
	Set-Cookie:
NID=518=dCzovrXqYdJkUh_-ALAJF67rg4ZCcvKdYpyNRnNV0KQnSaj-1n_Kj8BCcv2VYaO06Qtpp3A-R9X41lBaIlg2BPao
VT2hKVSlzAGbVxabPwasFxqOzupZ9Xc83BZro0DyOh2ZDweD3qNk1k4NZAgUHruqlecFmdmeJMcz_grUueyrUhkAHHW
hYQSi8_v900wvhnbd; expires=Sun, 04-May-2025 23:58:35 GMT; path=/; domain=.google.com; HttpOnly
	Connection: close
```

2. facebook.com: _________WhatWeb report for http://facebook.com

```
Status    : 301 Moved Permanently
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>

Summary   : HTTPServer[proxygen-bolt], RedirectLocation[https://facebook.com/]

Detected Plugins:
[ HTTPServer ]
	HTTP server header string. This plugin also attempts to
	identify the operating system from the server header.
```

```
        String       : proxygen-bolt (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://facebook.com/ (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Location: https://facebook.com/
        Content-Type: text/plain
        Server: proxygen-bolt
        Date: Sun, 03 Nov 2024 00:03:25 GMT
        Connection: close
        Content-Length: 0

WhatWeb report for https://facebook.com/
Status    : 301 Moved Permanently
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>

Summary   : RedirectLocation[https://www.facebook.com/], Strict-Transport-Security[max-age=15552000; preload],
UncommonHeaders[x-fb-debug,x-fb-connection-quality,alt-svc]

Detected Plugins:
[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://www.facebook.com/ (from location)

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=15552000; preload

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Location: https://www.facebook.com/
        Strict-Transport-Security: max-age=15552000; preload
        Content-Type: text/html; charset="utf-8"
        X-FB-Debug:
7BkJ3lXkjfR4jL9Eky0aavkcC857urWcpwpuMNO85tWv4HpzmrbrNtM9PcXqedaQlRlZC6zH8LbuARFqcYuobQ==
        Date: Sun, 03 Nov 2024 00:03:27 GMT
```

```
	X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=37, rtx=0, c=10, mss=1392, tbw=2522, tp=-1, tpl=-1, uplat=118,
ullat=0
	Alt-Svc: h3=":443"; ma=86400
	Connection: close
	Content-Length: 0

WhatWeb report for https://www.facebook.com/
Status    : 302 Found
Title     : <None>
IP        : 157.240.212.35
Country   : UNITED STATES, US

Summary   : RedirectLocation[https://web.facebook.com/?_rdc=1&_rdr], Strict-Transport-Security[max-age=15552000;
preload],
UncommonHeaders[reporting-endpoints,report-to,cross-origin-opener-policy,x-fb-zr-redirect,x-fb-debug,x-fb-connection-qu
ality,alt-svc]

Detected Plugins:
[ RedirectLocation ]
	HTTP Server string location. used with http-status 301 and
	302

	String       : https://web.facebook.com/?_rdc=1&_rdr (from location)

[ Strict-Transport-Security ]
	Strict-Transport-Security is an HTTP header that restricts
	a web browser from accessing a website without the security
	of the HTTPS protocol.

	String       : max-age=15552000; preload

[ UncommonHeaders ]
	Uncommon HTTP server headers. The blacklist includes all
	the standard headers and many non standard but common ones.
	Interesting but fairly common headers should have their own
	plugins, eg. x-powered-by, server and x-aspnet-version.
	Info about headers can be found at www.http-stats.com

	String       :
reporting-endpoints,report-to,cross-origin-opener-policy,x-fb-zr-redirect,x-fb-debug,x-fb-connection-quality,alt-svc (from
headers)

HTTP Headers:
	HTTP/1.1 302 Found
	Location: https://web.facebook.com/?_rdc=1&_rdr
	reporting-endpoints: coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0"
	report-to:
{"max_age":2592000,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"co
op_report","include_subdomains":true}
	cross-origin-opener-policy: unsafe-none
	x-fb-zr-redirect: 02|1730678609|
	Strict-Transport-Security: max-age=15552000; preload
	Content-Type: text/html; charset="utf-8"
	X-FB-Debug:
+yt3jMeeQXkgnwotlFoPZpbdsy5E9rw8u7ZCivWIZ2/prnLcbbnRUuDsW/g1wxAHEbu8ISh+Er/vC6xAyLVhYg==
	Date: Sun, 03 Nov 2024 00:03:29 GMT
	X-FB-Connection-Quality: MODERATE; q=0.3, rtt=175, rtx=0, c=10, mss=1392, tbw=2520, tp=-1, tpl=-1, uplat=52,
ullat=0
```

```
    Alt-Svc: h3=":443"; ma=86400
    Connection: close
    Content-Length: 0

WhatWeb report for https://web.facebook.com/?_rdc=1&_rdr
Status    : 200 OK
Title     : <None>
IP        : 57.144.120.141
Country   : FRANCE, FR

Summary   : Cookies[fr,sb], HTML5, HttpOnly[fr,sb], Meta-Refresh-Redirect[/?_rdc=1&_rdr&_fb_noscript=1],
PasswordField[pass], Script[application/ld+json,text/javascript], Strict-Transport-Security[max-age=15552000; preload],
UncommonHeaders[reporting-endpoints,report-to,content-security-policy,document-policy,permissions-policy,cross-origin-r
esource-policy,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc],
X-Frame-Options[DENY], X-XSS-Protection[0]

Detected Plugins:
[ Cookies ]
    Display the names of cookies in the HTTP headers. The
    values are not returned to save on space.

    String       : fr
    String       : sb

[ HTML5 ]
    HTML version 5, detected by the doctype declaration


[ HttpOnly ]
    If the HttpOnly flag is included in the HTTP set-cookie
    response header and the browser supports it then the cookie
    cannot be accessed through client side script - More Info:
    http://en.wikipedia.org/wiki/HTTP_cookie

    String       : fr,sb

[ Meta-Refresh-Redirect ]
    Meta refresh tag is a deprecated URL element that can be
    used to optionally wait x seconds before reloading the
    current page or loading a new page. More info:
    https://secure.wikimedia.org/wikipedia/en/wiki/Meta_refresh

    String       : /?_rdc=1&_rdr&_fb_noscript=1

[ PasswordField ]
    find password fields

    String       : pass (from field name)

[ Script ]
    This plugin detects instances of script HTML elements and
    returns the script language/type.

    String       : application/ld+json,text/javascript

[ Strict-Transport-Security ]
    Strict-Transport-Security is an HTTP header that restricts
    a web browser from accessing a website without the security
```

```
	of the HTTPS protocol.

	String       : max-age=15552000; preload

[ UncommonHeaders ]
	Uncommon HTTP server headers. The blacklist includes all
	the standard headers and many non standard but common ones.
	Interesting but fairly common headers should have their own
	plugins, eg. x-powered-by, server and x-aspnet-version.
	Info about headers can be found at www.http-stats.com

	String       :
reporting-endpoints,report-to,content-security-policy,document-policy,permissions-policy,cross-origin-resource-policy,cross
-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

[ X-Frame-Options ]
	This plugin retrieves the X-Frame-Options value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : DENY

[ X-XSS-Protection ]
	This plugin retrieves the X-XSS-Protection value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : 0

HTTP Headers:
	HTTP/1.1 200 OK
	Vary: Accept-Encoding
	Content-Encoding: gzip
	Set-Cookie: fr=0cBpNRVw5mdPs3IIB..BnJr3U..AAA.0.0.BnJr3U.AWWWUei4lMU; expires=Sat, 01-Feb-2025
00:03:32 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
	Set-Cookie: sb=1L0mZ7NVFf2mmo1-_GxH7QKA; expires=Mon, 08-Dec-2025 00:03:32 GMT; Max-Age=34560000;
path=/; domain=.facebook.com; secure; httponly
	reporting-endpoints: coop_report="https://web.facebook.com/browser_reporting/coop/?minimize=0",
default="https://web.facebook.com/ajax/browser_error_reports/?device_level=unknown&brsid=7432836953324171737",
permissions_policy="https://web.facebook.com/ajax/browser_error_reports/"
	report-to:
{"max_age":2592000,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"co
op_report","include_subdomains":true},
{"max_age":259200,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&
brsid=7432836953324171737"}]},
{"max_age":21600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/"}],"group":"permissions_p
olicy"}
	content-security-policy: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net
'unsafe-eval';script-src 'report-sample' *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data:
'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data:
*.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net
*.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:*
blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com
wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com
https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src
*.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net
```

```
connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com
*.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/
https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src
*.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com
https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net
https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com
https://googleads.g.doubleclick.net https://www.google.com https://td.doubleclick.net *.google.com
*.doubleclick.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;
	document-policy: force-load-at-top
	permissions-policy: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self),
camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(),
ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self),
compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self),
gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(),
microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(),
publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(),
private-state-token-redemption=(), usb=(), unload=(self), window-management=(),
xr-spatial-tracking=(self);report-to="permissions_policy"
	cross-origin-resource-policy: same-origin
	cross-origin-opener-policy: unsafe-none
	Pragma: no-cache
	Cache-Control: private, no-cache, no-store, must-revalidate
	Expires: Sat, 01 Jan 2000 00:00:00 GMT
	X-Content-Type-Options: nosniff
	X-XSS-Protection: 0
	X-Frame-Options: DENY
	Strict-Transport-Security: max-age=15552000; preload
	Content-Type: text/html; charset="utf-8"
	X-FB-Debug:
G+qr5W9iRRN9JsUOwXHnBzmMFmdEHbVDd59gyNTn/uFMAp9ACXLA1ft8jb6RD3DTg8499Hh0ONlBKDnJLhLdcQ==
	Date: Sun, 03 Nov 2024 00:03:32 GMT
	X-FB-Connection-Quality: MODERATE; q=0.3, rtt=168, rtx=0, c=10, mss=1392, tbw=2520, tp=-1, tpl=-1, uplat=151,
ullat=0
	Alt-Svc: h3=":443"; ma=86400
	Transfer-Encoding: chunked
	Connection: close

WhatWeb report for https://web.facebook.com/?_rdc=1&_rdr&_fb_noscript=1
Status    : 200 OK
Title     : <None>
IP        : 57.144.120.141
Country   : FRANCE, FR

Summary   : Cookies[fr,noscript,sb], HTML5, HttpOnly[fr,sb], PasswordField[pass],
Script[application/ld+json,text/javascript], Strict-Transport-Security[max-age=15552000; preload],
UncommonHeaders[reporting-endpoints,report-to,content-security-policy,document-policy,permissions-policy,cross-origin-r
esource-policy,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc],
X-Frame-Options[DENY], X-XSS-Protection[0]

Detected Plugins:
[ Cookies ]
	Display the names of cookies in the HTTP headers. The
	values are not returned to save on space.

	String       : fr
	String       : noscript
	String       : sb
```

```
[ HTML5 ]
	HTML version 5, detected by the doctype declaration


[ HttpOnly ]
	If the HttpOnly flag is included in the HTTP set-cookie
	response header and the browser supports it then the cookie
	cannot be accessed through client side script - More Info:
	http://en.wikipedia.org/wiki/HTTP_cookie

	String       : fr,sb

[ PasswordField ]
	find password fields

	String       : pass (from field name)

[ Script ]
	This plugin detects instances of script HTML elements and
	returns the script language/type.

	String       : application/ld+json,text/javascript

[ Strict-Transport-Security ]
	Strict-Transport-Security is an HTTP header that restricts
	a web browser from accessing a website without the security
	of the HTTPS protocol.

	String       : max-age=15552000; preload

[ UncommonHeaders ]
	Uncommon HTTP server headers. The blacklist includes all
	the standard headers and many non standard but common ones.
	Interesting but fairly common headers should have their own
	plugins, eg. x-powered-by, server and x-aspnet-version.
	Info about headers can be found at www.http-stats.com

	String       :
reporting-endpoints,report-to,content-security-policy,document-policy,permissions-policy,cross-origin-resource-policy,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

[ X-Frame-Options ]
	This plugin retrieves the X-Frame-Options value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : DENY

[ X-XSS-Protection ]
	This plugin retrieves the X-XSS-Protection value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : 0

HTTP Headers:
        HTTP/1.1 200 OK
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Set-Cookie: fr=0nSrluJIEyX3bTICy..BnJr3Y..AAA.0.0.BnJr3Y.AWUBPUFV6bs; expires=Sat, 01-Feb-2025 00:03:36
GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
        Set-Cookie: noscript=1; path=/; domain=.facebook.com; secure
        Set-Cookie: sb=2L0mZ6128AeymotO9Nb1sIa2; expires=Mon, 08-Dec-2025 00:03:36 GMT; Max-Age=34560000;
path=/; domain=.facebook.com; secure; httponly
        reporting-endpoints: coop_report="https://web.facebook.com/browser_reporting/coop/?minimize=0",
default="https://web.facebook.com/ajax/browser_error_reports/?device_level=unknown&brsid=7432836970697682830",
permissions_policy="https://web.facebook.com/ajax/browser_error_reports/"
        report-to:
{"max_age":2592000,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"co
op_report","include_subdomains":true},
{"max_age":259200,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&
brsid=7432836970697682830"}]},
{"max_age":21600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/"}],"group":"permissions_p
olicy"}
        content-security-policy: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net
'unsafe-eval';script-src 'report-sample' *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data:
'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data:
*.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net
*.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:*
blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com
wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com
https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src
*.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net
connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com
*.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/
https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src
*.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com
https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net
https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com
https://googleads.g.doubleclick.net https://www.google.com https://td.doubleclick.net *.google.com
*.doubleclick.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;
        document-policy: force-load-at-top
        permissions-policy: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self),
camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(),
ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self),
compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self),
gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(),
microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(),
publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(),
private-state-token-redemption=(), usb=(), unload=(self), window-management=(),
xr-spatial-tracking=(self);report-to="permissions_policy"
        cross-origin-resource-policy: same-origin
        cross-origin-opener-policy: unsafe-none
        Pragma: no-cache
        Cache-Control: private, no-cache, no-store, must-revalidate
        Expires: Sat, 01 Jan 2000 00:00:00 GMT
        X-Content-Type-Options: nosniff
        X-XSS-Protection: 0
        X-Frame-Options: DENY
        Strict-Transport-Security: max-age=15552000; preload
        Content-Type: text/html; charset="utf-8"
        X-FB-Debug:
HirswwGkC4LehbYDJ/Nu1sGJv5knKcz4bvTfIfB+qgbsIb4/vu8aCD9lS8iTwdXq+LlX8DLrcP8nvMLS5spgvg==
        Date: Sun, 03 Nov 2024 00:03:36 GMT
        X-FB-Connection-Quality: MODERATE; q=0.3, rtt=180, rtx=0, c=10, mss=1392, tbw=2520, tp=-1, tpl=-1, uplat=192,
ullat=0
        Alt-Svc: h3=":443"; ma=86400
        Transfer-Encoding: chunked
        Connection: close
```

INT302: Kali Linux Tools and System Security – Lab 3: Subdomain Hunting

Lab Overview

In this lab, you will learn how to identify subdomains associated with a target domain using various tools. Subdomain hunting is a crucial part of reconnaissance in penetration testing, as it helps identify additional attack surfaces that may not be immediately visible. We will utilize sublist3r for subdomain enumeration, dirb for directory discovery, and theHarvester for gathering information from public sources.

Tools Used

- **Kali Linux:** A Linux distribution tailored for penetration testing**.**
- **sublist3r:** A tool designed for subdomain enumeration.
- **dirb:** A web content scanner for discovering hidden directories.
- **theHarvester:** A tool for gathering emails and subdomains from public sources.

Lab Steps

Step 1: Subdomain Enumeration Using sublist3r

sublist3r is an effective tool for finding subdomains of a target domain.

Instructions:

1. Open your Terminal in Kali Linux.
2. Use the sublist3r command followed by the target domain.
3.

Command Syntax:

```
sublist3r -d <target domain>
```

Exercise 1: Run the sublist3r command for the following domains:

- github.com
- google.com

Record Find:

1.Subdomains for github.com: ___

```
[-] Enumerating subdomains now for github.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 95
www.github.com
atom-installer.github.com
branch.github.com
brandguide.github.com
camo.github.com
central.github.com
cla.github.com
classroom.github.com
cloud.github.com
f.cloud.github.com
codespaces.github.com
codespaces-dev.github.com
codespaces-ppe.github.com
communication.github.com
www.communication.github.com
m.communication.github.com
res.communication.github.com
t.communication.github.com
community.github.com
docs.github.com
docs-front-door.github.com
dodgeball.github.com
edu.github.com
education.github.com
emails.github.com
enterprise.github.com
support.enterprise.github.com
www.support.enterprise.github.com
examregistration.github.com
examregistration-api.github.com
examregistration-uat.github.com
examregistration-uat-api.github.com
fast.github.com
garage.github.com
gist.github.com
graphql.github.com
www.graphql.github.com
graphql-stage.github.com
www.graphql-stage.github.com
help.github.com
helpnext.github.com
hq.github.com
vpn-ca.iad.github.com
id.github.com
import.github.com
import2.github.com
importer2.github.com
jira.github.com
www.jira.github.com
```

```
jobs.github.com
lab.github.com
lab-sandbox.github.com
learn.github.com
mac-installer.github.com
maintainers.github.com
www.maintainers.github.com
octostatus-production.github.com
offer.github.com
partnerportal.github.com
www.partnerportal.github.com
pkg.github.com
porter.github.com
porter2.github.com
proxima-review-lab.github.com
raw.github.com
registry.github.com
render.github.com
render-lab.github.com
www.render-lab.github.com
review-lab.github.com
octocaptcha.review-lab.github.com
rs.github.com
schrauger.github.com
api.security.github.com
www.api.security.github.com
skyline.github.com
www.skyline.github.com
slack.github.com
smtp.github.com
www.smtp.github.com
staging-lab.github.com
api.stars.github.com
www.api.stars.github.com
status.github.com
stg.github.com
styleguide.github.com
ws.support.github.com
www.ws.support.github.com
talks.github.com
visualstudio.github.com
www.visualstudio.github.com
vscode-auth.github.com
workspaces.github.com
workspaces-dev.github.com
workspaces-ppe.github.com
```

2.Subdomains for google.com___________

```
[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 97
www.google.com
accounts.google.com
freezone.accounts.google.com
adwords.google.com
qa.adz.google.com
answers.google.com
apps-secure-data-connector.google.com
audioads.google.com
checkout.google.com
mtv-da-1.ad.corp.google.com
ads-compare.eem.corp.google.com
da.ext.corp.google.com
m.guts.corp.google.com
m.gutsdev.corp.google.com
login.corp.google.com
mtv-da.corp.google.com
mygeist.corp.google.com
mygeist2010.corp.google.com
proxyconfig.corp.google.com
reseed.corp.google.com
twdsalesgsa.twd.corp.google.com
uberproxy.corp.google.com
uberproxy-nocert.corp.google.com
uberproxy-san.corp.google.com
ext.google.com
cag.ext.google.com
cod.ext.google.com
da.ext.google.com
eggroll.ext.google.com
fra-da.ext.google.com
glass.ext.google.com
glass-eur.ext.google.com
glass-mtv.ext.google.com
glass-twd.ext.google.com
hot-da.ext.google.com
hyd-da.ext.google.com
ice.ext.google.com
meeting.ext.google.com
mtv-da.ext.google.com
soaproxyprod01.ext.google.com
soaproxytest01.ext.google.com
spdy-proxy.ext.google.com
spdy-proxy-debug.ext.google.com
twd-da.ext.google.com
```

flexpack.google.com
www.flexpack.google.com
accounts.flexpack.google.com
gaiastaging.flexpack.google.com
mail.flexpack.google.com
plus.flexpack.google.com
search.flexpack.google.com
freezone.google.com
www.freezone.google.com
accounts.freezone.google.com
gaiastaging.freezone.google.com
mail.freezone.google.com
news.freezone.google.com
plus.freezone.google.com
search.freezone.google.com
gmail.google.com
hosted-id.google.com
jmt0.google.com
aspmx.l.google.com
alt1.aspmx.l.google.com
alt2.aspmx.l.google.com
alt3.aspmx.l.google.com
alt4.aspmx.l.google.com
gmail-smtp-in.l.google.com
alt1.gmail-smtp-in.l.google.com
alt2.gmail-smtp-in.l.google.com
alt3.gmail-smtp-in.l.google.com
alt4.gmail-smtp-in.l.google.com
gmr-smtp-in.l.google.com
alt1.gmr-smtp-in.l.google.com
alt2.gmr-smtp-in.l.google.com
alt3.gmr-smtp-in.l.google.com
alt4.gmr-smtp-in.l.google.com
vp.video.l.google.com
m.google.com
freezone.m.google.com
mail.google.com
freezone.mail.google.com
misc.google.com
misc-sni.google.com
mtalk.google.com
mx.google.com
ics.prod.google.com
sandbox.google.com
cert-test.sandbox.google.com
ecc-test.sandbox.google.com
services.google.com
talk.google.com
upload.google.com
dg.video.google.com
upload.video.google.com
wifi.google.com

onex.wifi.google.com

Step 2: Directory Discovery Using dirb

dirb is a powerful tool for discovering hidden directories and files on web servers.

Instructions:

1. In the terminal, run the dirb command followed by the target URL.

Command Syntax:

```
dirb <target URL>
```

Exercise 2:

Perform a directory discovery scan on the following targets:

- http://example.com
- http://example.org

Record Find:

Directories for example.com:_______

```
START_TIME: Tue Nov  5 00:09:12 2024
URL_BASE: https://example.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://example.com/ ----
+ https://example.com/index.html (CODE:200|SIZE:1256)

-----------------
END_TIME: Tue Nov  5 00:46:34 2024
DOWNLOADED: 4612 - FOUND: 1
```

Directories for example.org:___

```
START_TIME: Tue Nov  5 00:58:01 2024
URL_BASE: https://example.org/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://example.org/ ----
+ https://example.org/index.html (CODE:200|SIZE:1256)

-----------------
END_TIME: Tue Nov  5 01:16:48 2024
DOWNLOADED: 4612 - FOUND: 1
```

Step 3: Information Gathering Using theHarvester

theHarvester is a tool for gathering emails, subdomains, and other relevant information from search engines.

Instructions:

1. In the terminal, run the theHarvester command followed by the target domain.

Command Syntax:

```
theharvester -d <target domain> -b google
```

Exercise 3: Use theHarvester to gather information on the following domain:

- example.com

Record Finded:

- **Emails and Information Gathered:**

- **[*] No IPs found.**
-
- **[*] No emails found.**
-
- **[*] No hosts found.**