Five Tools

1.NMAP

2.NIKTO

3.METASPLOIT

4.THE HARVESTER

5.DIRB

1.NMAP

Explanation: Nmap, short for Network Mapper is a powerful open-source tool used for network discovery and security auditing. It is basically works on by sending packets to target hosts and analyzing their responses to gather information about the network.we can't imagine hacking without nmap.

i. Port scanning

It scans the ports in a given range

```
┌──(kali㉿kali)-[~]
└─$ nmap -P 1-100 192.168.56.1 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:03 EDT
Failed to resolve "1-100".
Nmap scan report for 192.168.56.1
Host is up (0.0070s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 37.84 seconds
```

ii.OS detection (it scans the operating system of an target)

```
┌──(kali㉿kali)-[~]
└─$ nmap -o 192.168.56.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 05:56 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds

┌──(kali㉿kali)-[~]
└─$ nmap osscan-guess 192.168.56.1 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 05:57 EDT
Failed to resolve "osscan-guess".
Nmap scan report for 192.168.56.1
Host is up (0.0057s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.67 seconds
```

iii.Aggressive Scan

The aggressive scan option combines various scan techniques, including service version detection, OS detection, and script scanning, to provide comprehensive information about the target.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.56.1 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 05:58 EDT
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 05:59 (0:00:16 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 06:00 (0:00:20 remaining)
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 06:00 (0:00:32 remaining)
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 06:01 (0:00:35 remaining)
Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 06:01 (0:00:42 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 06:01 (0:00:47 remaining)
Nmap scan report for 192.168.56.1
Host is up (0.0066s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```

iv. Version Detection

It tries to determine the version of services running on the target ports. Useful for identifying vulnerabilities

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.1 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:06 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0079s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.35 seconds
```

v. Timing and Performance (-T<0-5>):

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 192.168.56.1 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:10 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0054s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 17.74 seconds
```

2.Nikto

Nikto is open source and power tool which is used to identify vulnerabilities in websites.By scanning for a wide range of issues such as dangerous files, misconfigured services, and vulnerable scripts,Nikto helps assess the overall security posture of a website.

i. nikto -h https:hello.com

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nikto -h https:hello.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(kali㉿kali)-[~]
└─$ nikto -h https://hello.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 216.239.32.21, 216.239.36.21, 216.239.34.21, 216.239.38.21, 2001:4860:4802:34::15, 2001:4860:4802:38::15, 2001:4860:4802:32::15, 2001:4860:4802:3
+ Target IP:          216.239.32.21
+ Target Hostname:    hello.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=hello.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-03-12 06:56:51 (GMT-4)
```

ii. nikto -h https://hello.com -ipv4

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nikto -h https://hello.com -ipv4
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 216.239.32.21, 216.239.36.21, 216.239.34.21, 216.239.38.21, 2001:4860:4802:34::15, 2001:4860:4802:38::15, 2001:4860:4802:32::15, 2001:4860:4802:36::15
+ Target IP:          216.239.32.21
+ Target Hostname:    hello.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=hello.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-03-12 07:05:49 (GMT-4)
---------------------------------------------------------------------------
+ Server: Google Frontend
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-cloud-trace-context' found, with contents: e6b0e5d5bfe7a69c8a91647bf52acac9.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-s
sing-content-type-header/
```

iii. nikto -h https://hello.com -output /home/kali/Desktop/result.txt

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nikto -h https://hello.com  -output/home/kali/Desktop/result.txt
Unknown option: output/home/kali/Desktop/result.txt

  Options:
      -ask+               Whether to ask about submitting updates
                              yes   Ask about each (default)
                              no    Don't ask, don't send
                              auto  Don't ask, just send
      -check6             Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
      -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
      -config+            Use this config file
      -Display+           Turn on/off display outputs:
                              1     Show redirects
                              2     Show cookies received
                              3     Show all 200/OK responses
                              4     Show URLs which require authentication
                              D     Debug output
                              E     Display all HTTP errors
                              P     Print progress to STDOUT
                              S     Scrub output of IPs and hostnames
                              V     Verbose output
      -dbcheck            Check database and other key files for syntax errors
      -evasion+           Encoding technique:
                              1     Random URI encoding (non-UTF8)
                              2     Directory self-reference (/./)
                              3     Premature URL ending
                              4     Prepend long random string
                              5     Fake parameter
                              6     TAB as request spacer
                              7     Change the case of the URL
                              8     Use Windows directory separator (\)
                              A     Use a carriage return (0x0d) as a request spacer
                              B     Use binary value 0x0b as a request spacer
       -followredirects   Follow 3xx redirects to new location
       -Format+           Save file (-o) format:
                              csv   Comma-separated-value
                              json  JSON Format
                              htm   HTML Format
                              nbe   Nessus NBE format
                              sql   Generic SQL (see docs for schema)
                              txt   Plain text
                              xml   XML Format
                              (if not specified the format will be taken from the file extension passed to -output)
      -Help               This help information
      -host+              Target host/URL
      -id+                Host authentication to use, format is id:pass or id:pass:realm
      -ipv4                  IPv4 Only
      -ipv6                  IPv6 Only
      -key+               Client certificate key file
      -list-plugins       List all available plugins, perform no testing
      -maxtime+           Maximum testing time per host (e.g., 1h, 60m, 3600s)
```

iv.sudo proxychains nikto -h https://hello.com

```
┌──(kali㉿kali)-[~]
└─$ sudo proxychains -h https://hello.com
[sudo] password for kali:
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
proxychains: can't load process '-h'. (hint: it's probably a typo): No such file or directory

┌──(kali㉿kali)-[~]
└─$ sudo proxychains nikto  -h https://hello.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
- Nikto v2.5.0
---------------------------------------------------------------------------
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  timeout
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  timeout
---------------------------------------------------------------------------
+ 0 host(s) tested
```

3.Metasploit

Explanation: Metasploit is a powerful framework used for penetration testing, vulnerability assessment, and security research.

i.sudo su

Explanation: In Metasploit, the `sudo su` command is typically used to elevate privileges within the Metasploit Framework. This command allows you to run Metasploit with superuser privileges.

```
kali [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
1  2  3  4

File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts
```

ii.msfconsole

Explanation: In Metasploit, the `msfconsole` command is used to launch the Metasploit Framework console, which is the primary interface for interacting with the various modules, exploits, payloads, and other features of Metasploit

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

 ____________________________________
/ it looks like you're trying to run a \
\ module                               /
 ------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit windows/misc/hta_server

Matching Modules
================

   #  Name                            Disclosure Date  Rank    Check  Description
   -  ----                            ---------------  ----    -----  -----------
   0  exploit/windows/misc/hta_server  2016-10-06       manual  No     HTA Web Server


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/misc/hta_server

[*] Using exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

iii.show options

Explanation: In Metasploit, the `show options` command serves as a fundamental tool for configuring modules before launching attacks or performing security assessments.

```
msf6 exploit(windows/misc/hta_server) > show options

Module options (exploit/windows/misc/hta_server):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Powershell x86


View the full module info with the info, or info -d command.
```

iv.set lhost

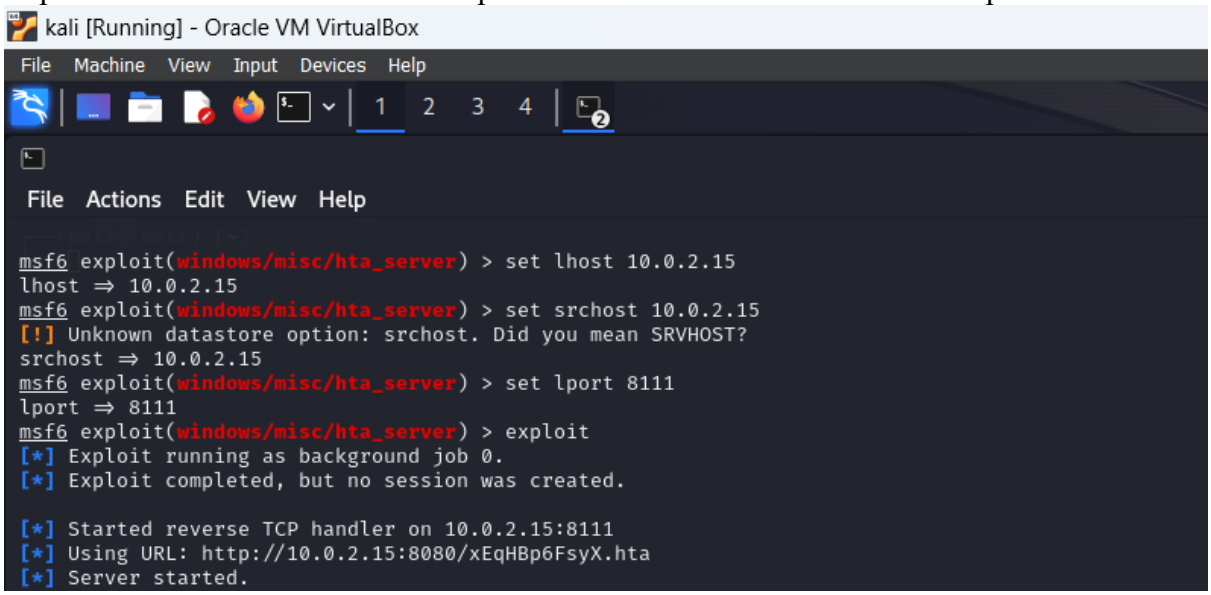
Explanation: This command sets the local host IP address for the payload to connect back to. When you exploit a vulnerability on a remote system and gain access to it, the exploited system needs to establish a connection back to your machine to receive further instructions or to provide you with a shell.

set srvhost

Explanation: This command sets the IP address of the host that will be used when setting up a server to deliver exploits or payloads.

set port

Explanation: This command sets the port number to use for the listener or exploit module.

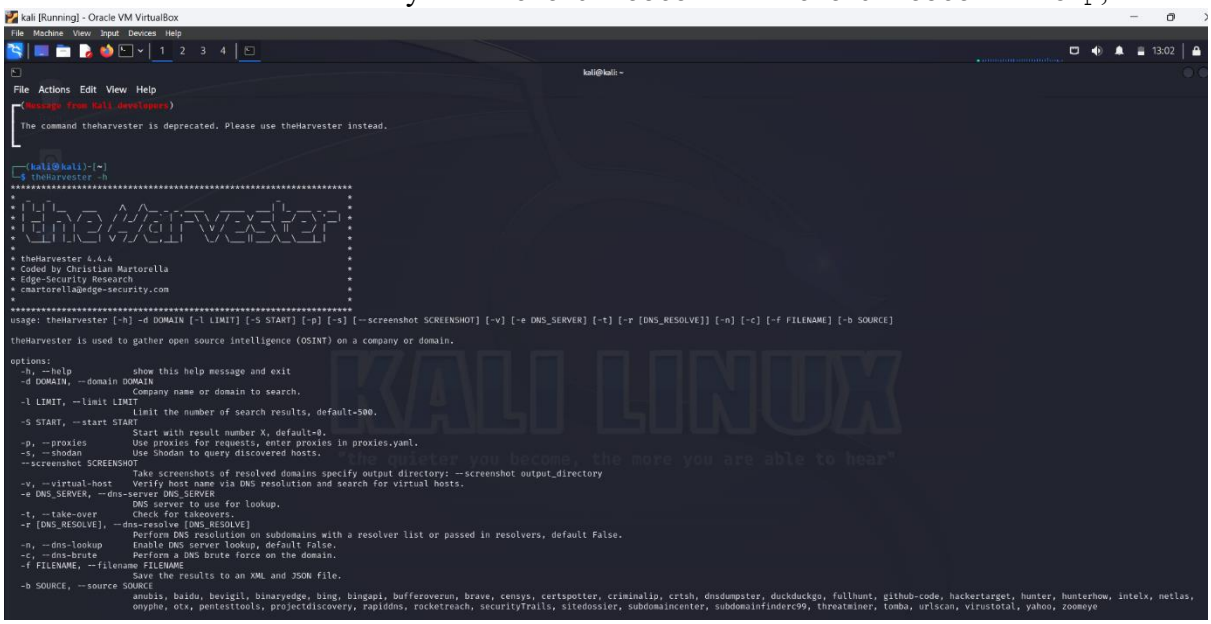


4.theharvester

Explanation:A harvester is typically a tool used to gather information about individuals,organizations,but in market there are many harvesters are there.

i.theHarvester -h

Explanation: In theHarvester, the `-h` option is used to display the help menu or usage information for the tool. When you run `theHarvester -h` or `theHarvester --help`,



ii.theharvester -d kali.org -b duckduckgo

Explanation: you're instructing theHarvester tool to search for information related to the domain "kali.org" using the DuckDuckGo search engine as one of the data sources.

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d kali.org -b duckduckgo
*******************************************************************
*  _  _                                                           *
* | |_| |__   __    ^  /\__ _ _ ___   _____   __| |_ __ _ __     *
* | __|  _ \ / _ \  / /_/ / _` |'__\ \ / / _ \ / __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: kali.org


[*] Searching Duckduckgo.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 14
---------------------
2Fdocs.kali.org
2Ftools.kali.org
arm.kali.org
autopkgtest.kali.org
bugs.kali.org
discord.kali.org
docs.kali.org
forums.kali.org
http.kali.org
nethunter.kali.org
old.kali.org
pkg.kali.org
status.kali.org
tools.kali.org
```

iii.theharvester -d gatesit.ac.in -b duckduckgo

Explanation: It aims to gather information about the domain "gatesit.ac.in" using the DuckDuckGo search engine..

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d gatesid.ac.in -b duckduckgo
*******************************************************************
*  _  _                                                           *
* | |_| |__   ___    ^  /\__ _ _ ___   ____   ___| |_ ___ _ __   *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \ __| __/ _ \ '_| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: gatesid.ac.in

[*] Searching Duckduckgo.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

iv.theHarvester -d gatesit.ac.in -b google,duckduckgo,pgp,bing

Explanation:Each search engine might uncover different kinds of information, giving a broader picture. Just like looking through different windows to see different views, using multiple search engines can reveal more about the target.

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d gatesid.ac.in -b google,duckduckgo,pgp,bing
*******************************************************************
*  _  _                                                           *
* | |_| |__   ___    ^  /\__ _ _ ___   ____   ___| |_ ___ _ __   *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \ __| __/ _ \ '_| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[!] Invalid source.
```

5.Dirb

Explanation: Dirb is an online directory scanner that searches web servers for hidden files, directories, and pages. It is a free and open-source utility included in the Kali Linux distribution, a popular operating system for penetration testing and ethical hacking.

i. Basic directory scan: dirb http://10.10.242.256

Explanation: `dirb` is a tool commonly used in penetration testing for web applications. It's essentially a web content scanner that helps identify web servers and their corresponding directories and files that may not be easily discoverable.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.242.136

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 14 13:12:48 2024
URL_BASE: http://10.10.242.136/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.242.136/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Thu Mar 14 13:12:48 2024
DOWNLOADED: 0 - FOUND: 0
```

ii. dirb http://10.10.242.236 -w /usr/share/dirb/wordlists/directory-list-2.0.txt

Explanation: The purpose of this command is to systematically search for directories and files on the web server by trying common directory and file names listed in the wordlist.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.242.136 -w /usr/share/dirb/wordlists/directory-list-2.0.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 14 13:14:26 2024
URL_BASE: http://10.10.242.136/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.242.136/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Thu Mar 14 13:14:26 2024
DOWNLOADED: 0 - FOUND: 0
```

iii. dirb http://10.10.242.236 -w usr/share/dirb/wordlists/directory-list-2.0.txt -X .php

Explanation: This tells dirb where to find a big list of possible hidden things on websites. It's like giving the detective a big list of secret hiding spots to check.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.242.136 -w /usr/share/dirb/wordlists/directory-list-2.0.txt -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 14 13:15:01 2024
URL_BASE: http://10.10.242.136/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

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

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.242.136/ ---
```

iv. dirb http://10.10.242.236 -w /usr/share/dirb/wordlists/directory-list-2.0.txt -a "pickle-rick"

Explanation: It's handy for conducting web reconnaissance, especially in penetration testing, to uncover hidden areas or vulnerabilities on a website, while also targeting something specific like pickle-rick.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.242.136 -w /usr/share/dirb/wordlists/directory-list-2.0.txt -a "pickle-rick"

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 14 13:15:53 2024
URL_BASE: http://10.10.242.136/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
USER_AGENT: pickle-rick
OPTION: Not Stopping on warning messages

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

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.242.136/ ---

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Thu Mar 14 13:15:53 2024
DOWNLOADED: 0 - FOUND: 0
```