4th Phase of Hacking methodologies

Vulnerability Analysis/Identification

Vulnerability Analysis is the fourth phase of the ethical hacking methodology, where the attacker (or ethical hacker) identifies and evaluates security weaknesses in a target system, application, or network. The goal is to find flaws that could be exploited to gain unauthorized access or perform malicious activities.

- It comes after the **Scanning** phase.
- It involves analyzing data collected from reconnaissance and scanning.
- Tools like **Nessus, OpenVAS, Nikto**, or manual methods are used.
- Vulnerabilities may include:
    - Unpatched software
    - Misconfigured systems
    - Weak passwords
    - Open ports/services
    - Web application flaws (e.g., SQL Injection, XSS)

Some Command Line Scanners are as follows:

1) **Nikto**
   Nikto is an open-source web server scanner that performs comprehensive tests against web servers for:
    - Dangerous files and scripts
    - Outdated software versions
    - Insecure configurations (e.g., directory listing enabled)
    - Potentially harmful CGI scripts
    - Server configuration issues

What You Might Discover

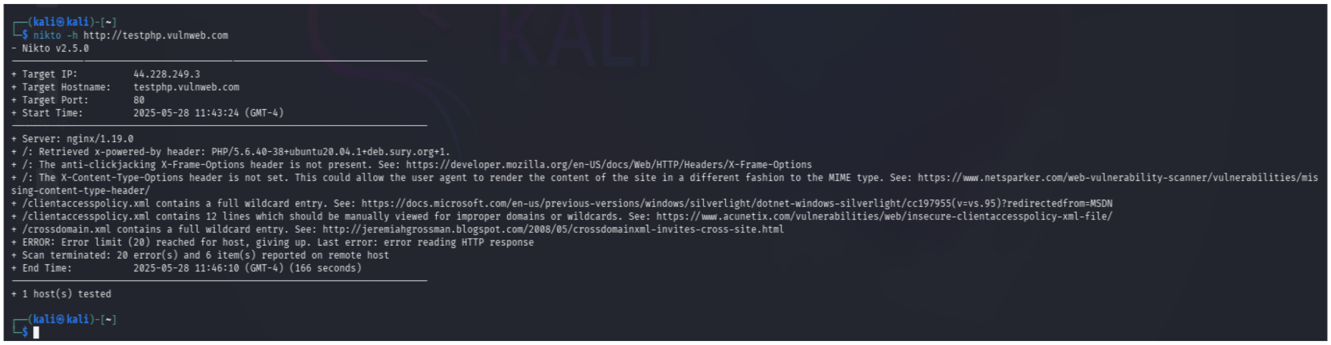
- Apache version and possible vulnerabilities
- Exposed admin interfaces

- Unsecured directories
- Default files (e.g., /phpinfo.php)
- Insecure cookies

How to Run Nikto in Kali Linux

Nikto is pre-installed in Kali Linux. To run a basic scan:

In this example we did basic scan with the help of nikto on target name example.com



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://testphp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-05-28 11:43:24 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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-scanner/vulnerabilities/mis
sing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-05-28 11:46:10 (GMT-4) (166 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

2) Dirsearch

Dirsearch is a fast and powerful **command-line brute-force directory and file scanner** written in Python. It works by trying different directory and file names (from a wordlist) on the target web server to see which ones exist.

What It Helps You Discover

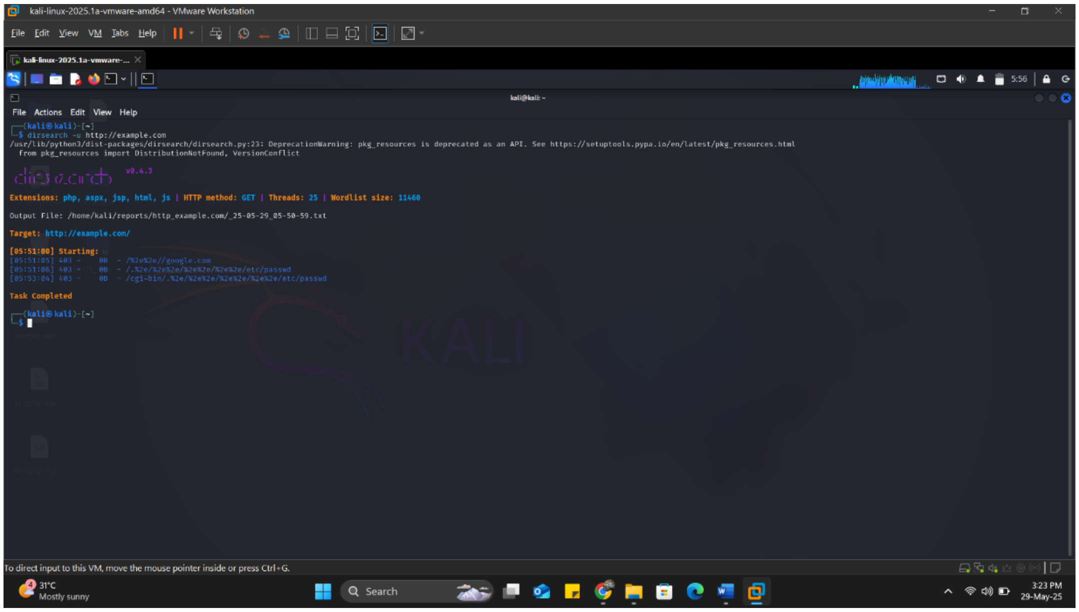
- Hidden admin panels (e.g., /admin/)
- Unlinked login pages (e.g., /login.php)
- Backup files (e.g., backup.zip)
- Development directories (e.g., /dev/, /test/)
- Misconfigured or forgotten paths

How to Run Dirsearch in Kali Linux

To scan a Ip or url you need to install the diesearch in kali for that type a following command:

Sudo apt install dirsearch

In this example we did basic scan with the help of dirsearch on target name example.com

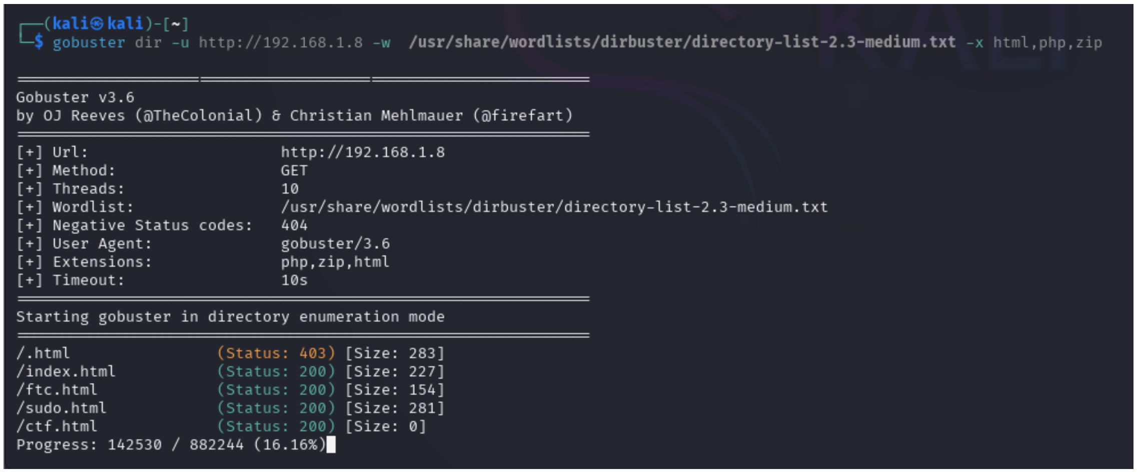

kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1a-vmware-...
5:56
kali@kali: ~
File Actions Edit View Help
31°C
Mostly sunny
Search
3:23 PM
29-May-25

```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://example.com
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

                              v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/reports/http_example.com/_25-05-29_05-50-59.txt

Target: http://example.com/

[05:51:00] Starting:
[05:51:05] 403 -    0B  - /%2e%2e//google.com
[05:51:06] 403 -    0B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[05:53:04] 403 -    0B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd

Task Completed

┌──(kali㉿kali)-[~]
└─$ 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3) Gobuster

Gobuster is use for brute forcing the directories of specific targeted Ip Address.



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.8 -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.8
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,zip,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 283]
/index.html           (Status: 200) [Size: 227]
/ftc.html             (Status: 200) [Size: 154]
/sudo.html            (Status: 200) [Size: 281]
/ctf.html             (Status: 200) [Size: 0]
Progress: 142530 / 882244 (16.16%)
```

In this above imagine we targeted 192.168.1.8 this ip we brute force directories of this system using gobuster.

Command: gobuster dir -u http://192.168.1.8 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip

Nessus explaination remaning in this pdf because it cant run in this system after I will add nessus explaination in it