VULNERABILITY ANALYSIS USING NIKTO

Aim :

To do Vulnerability analysis using Nikto.

Procedure :

• Open the Kali Linux.

• Open the Root Terminal and TYPE nikto –H

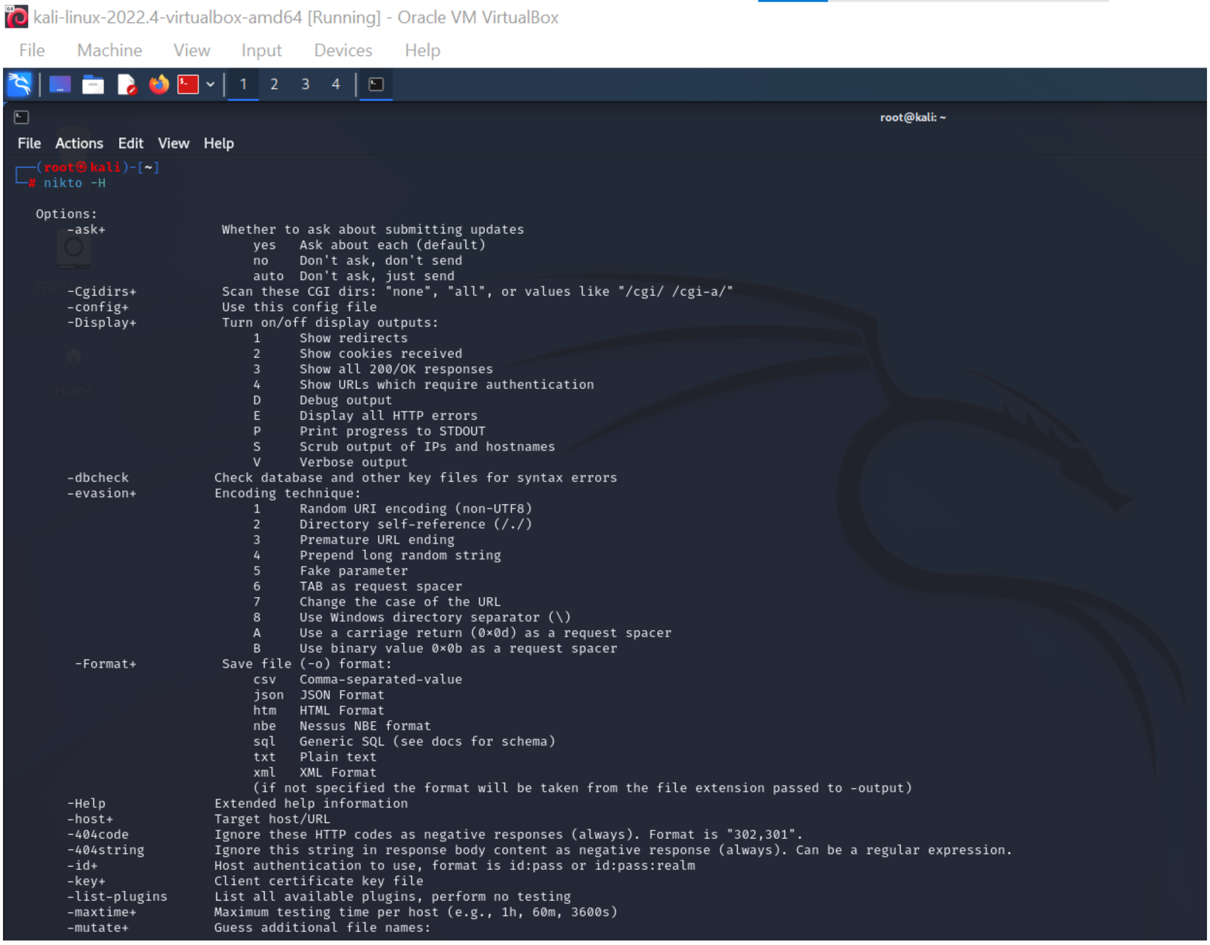
• TYPE nikto -h www.zoho.com -Tuning x COMMAMD

• Nikto starts web scanning with all turning options enabled.

• TYPE nikto -h www.certifiedhacker.com -Cgidirs all

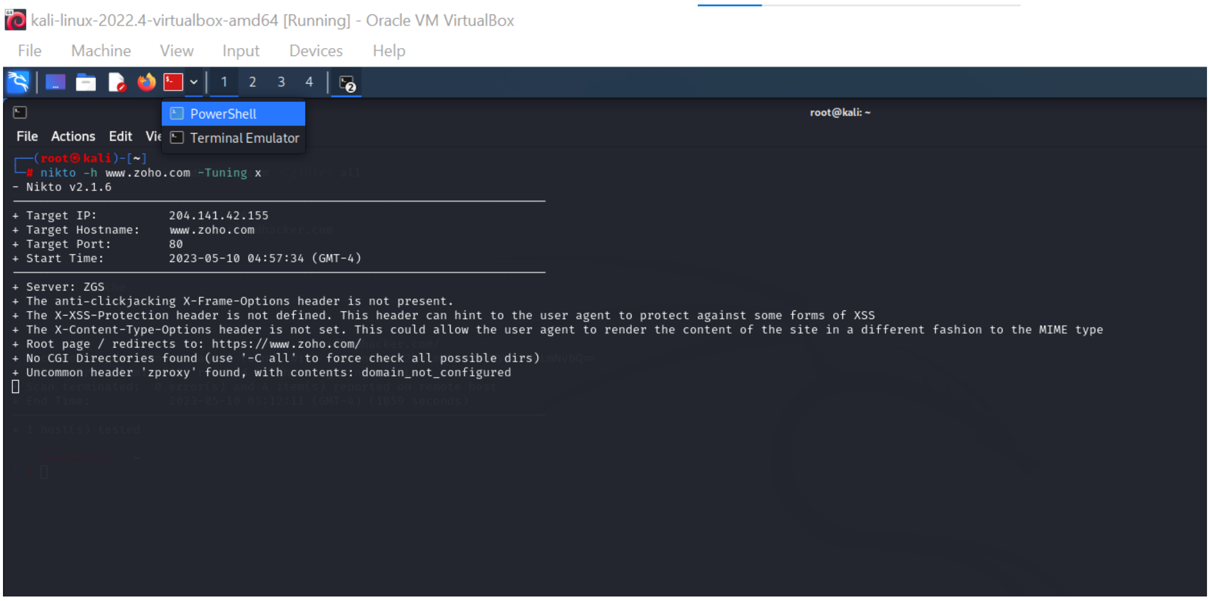
• Nikto will scan web server as it looks vulnerable CGI directories. It scans webserver and list of directories.

Output :


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: ~
File Actions Edit View Help

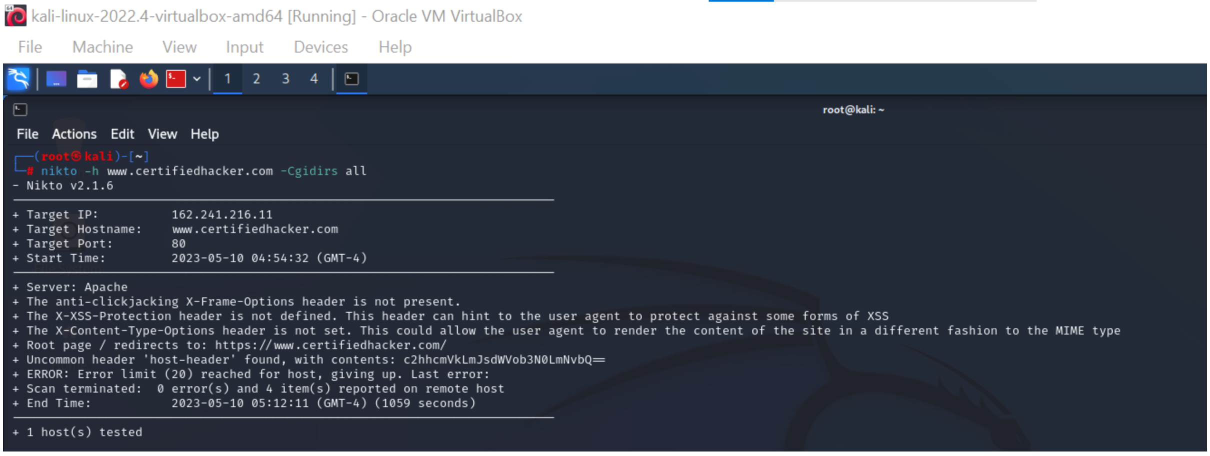
```
┌──(root㉿kali)-[~]
└─# nikto -H

   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
       -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 (0×0d) as a request spacer
                               B     Use binary value 0×0b as a request spacer
        -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              Extended help information
       -host+             Target host/URL
       -404code           Ignore these HTTP codes as negative responses (always). Format is "302,301".
       -404string         Ignore this string in response body content as negative response (always). Can be a regular expression.
       -id+               Host authentication to use, format is id:pass or id:pass:realm
       -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)
       -mutate+           Guess additional file names:
```



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
PowerShell
Terminal Emulator
root@kali: ~
File Actions Edit Vie

```
┌──(root㉿kali)-[~]
└─# nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          204.141.42.155
+ Target Hostname:    www.zoho.com
+ Target Port:        80
+ Start Time:         2023-05-10 04:57:34 (GMT-4)
---------------------------------------------------------------------------
+ Server: ZGS
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Root page / redirects to: https://www.zoho.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'zproxy' found, with contents: domain_not_configured
```



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2023-05-10 04:54:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Root page / redirects to: https://www.certifiedhacker.com/
+ Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  0 error(s) and 4 item(s) reported on remote host
+ End Time:           2023-05-10 05:12:11 (GMT-4) (1059 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Result :

Hence the Vulnerability Analysis using Nikto is Executed Successfully.