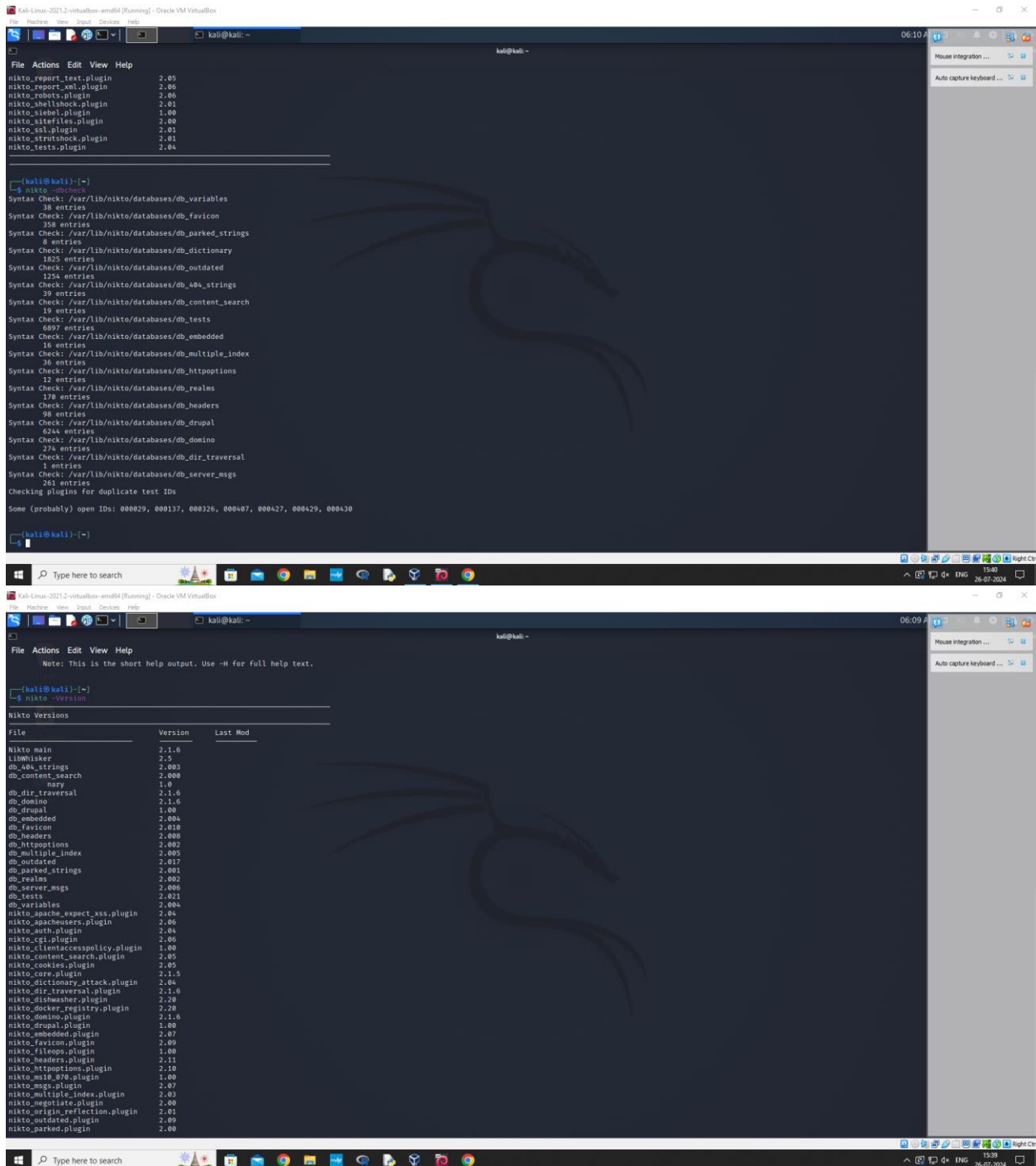


# Cyber Security and Digital Forensics

## Practical 2 – Vulnerability scanning using Nikto in Kali Linux



The image displays two screenshots of a Kali Linux terminal window, showing the execution of the Nikto vulnerability scanner.

**Top Screenshot:** The terminal shows the output of the `nikto -h` command, displaying a list of available plugins and their versions. The output is as follows:

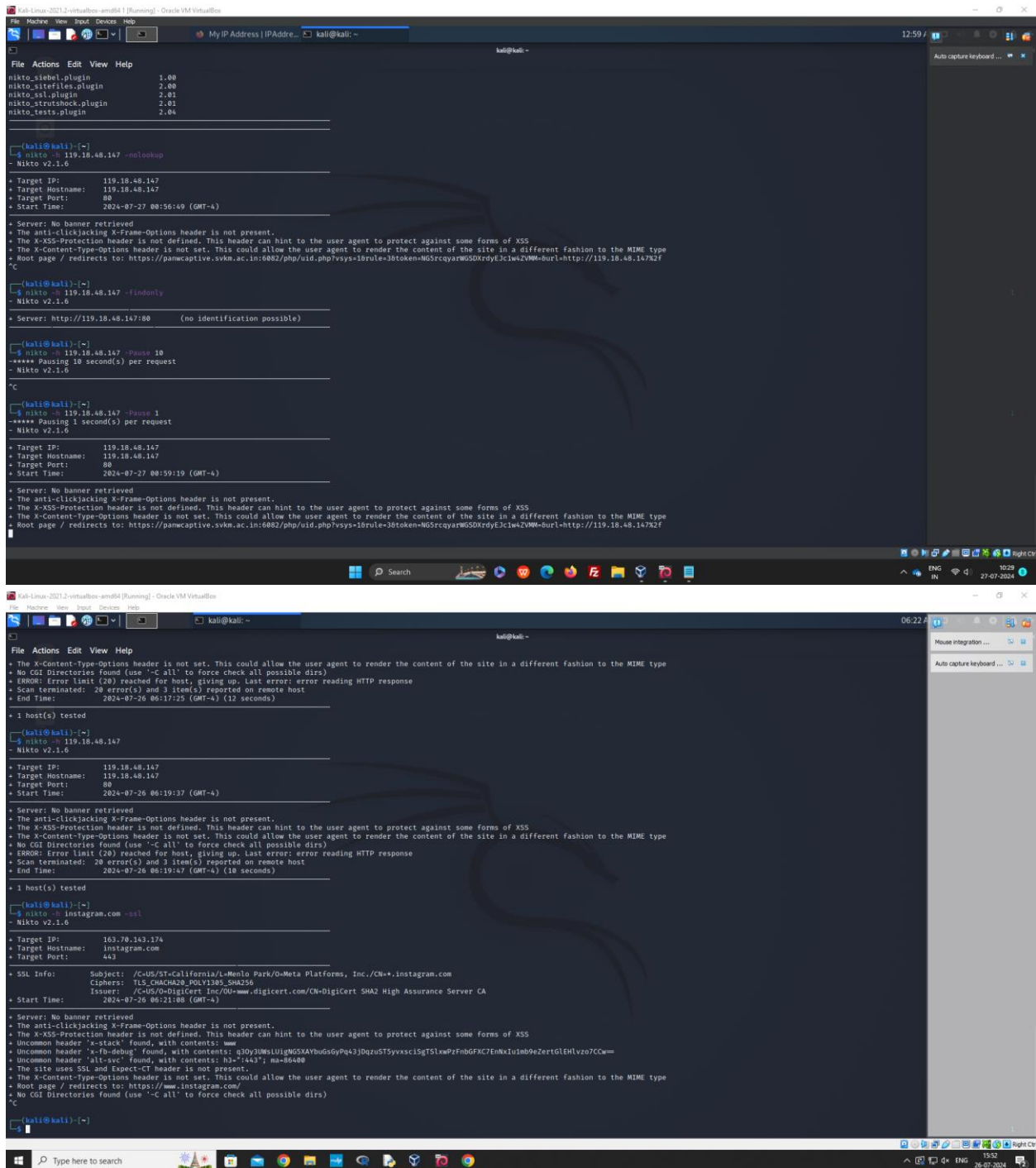
```
File Actions Edit View Help
nikto_report_test.plugin 2.05
nikto_report_xml.plugin 2.06
nikto_robots.plugin 2.06
nikto_shellshock.plugin 2.01
nikto_siebel.plugin 1.00
nikto_siteriles.plugin 2.00
nikto_ssl.plugin 2.01
nikto_struts2.plugin 2.01
nikto_tests.plugin 2.04
```

Below the plugin list, the terminal shows the output of the `nikto -c /var/lib/nikto/databases/db_variables` command, displaying a list of syntax checks and their results:

```
nikto -c /var/lib/nikto/databases/db_variables
Syntax Check: /var/lib/nikto/databases/db_variables
38 entries
Syntax Check: /var/lib/nikto/databases/db_favicon
358 entries
Syntax Check: /var/lib/nikto/databases/db_parked_strings
8 entries
Syntax Check: /var/lib/nikto/databases/db_dictionary
1825 entries
Syntax Check: /var/lib/nikto/databases/db_outdated
1254 entries
Syntax Check: /var/lib/nikto/databases/db_404_strings
39 entries
Syntax Check: /var/lib/nikto/databases/db_content_search
19 entries
Syntax Check: /var/lib/nikto/databases/db_tests
4897 entries
Syntax Check: /var/lib/nikto/databases/db_embedded
10 entries
Syntax Check: /var/lib/nikto/databases/db_multiple_index
36 entries
Syntax Check: /var/lib/nikto/databases/db_httpoptions
12 entries
Syntax Check: /var/lib/nikto/databases/db_realms
278 entries
Syntax Check: /var/lib/nikto/databases/db_headers
98 entries
Syntax Check: /var/lib/nikto/databases/db_drupal
6244 entries
Syntax Check: /var/lib/nikto/databases/db_domino
274 entries
Syntax Check: /var/lib/nikto/databases/db_dir_traversal
1 entries
Syntax Check: /var/lib/nikto/databases/db_server_msgs
261 entries
Checking plugins for duplicate test IDs
Some (probably) open IDs: 000029, 000137, 000326, 000407, 000427, 000429, 000430
```

**Bottom Screenshot:** The terminal shows the output of the `nikto -v` command, displaying the Nikto version information. The output is as follows:

```
File Actions Edit View Help
Note: This is the short help output. Use -H for full help text.
nikto -v
Nikto Versions
File Version Last Mod
Nikto main 2.1.6
LibWhisker 2.5
db_404_strings 2.003
db_content_search 2.000
db_dir_traversal 1.0
db_domino 2.1.6
db_drupal 1.00
db_embedded 2.004
db_favicon 2.010
db_headers 2.005
db_httpoptions 2.002
db_multiple_index 2.005
db_outdated 2.017
db_parked_strings 2.001
db_realms 2.002
db_server_msgs 2.005
db_tests 2.021
db_variables 2.004
nikto_apache_expect_xss.plugin 2.04
nikto_apacheusers.plugin 2.05
nikto_auth.plugin 2.04
nikto_cgi.plugin 2.00
nikto_clientaccesspolicy.plugin 1.00
nikto_content_search.plugin 2.05
nikto_cookies.plugin 2.05
nikto_core.plugin 2.1.5
nikto_dictionary_attack.plugin 2.04
nikto_dir_traversal.plugin 2.1.6
nikto_dishwasher.plugin 2.20
nikto_docker_registry.plugin 2.20
nikto_domino.plugin 2.1.6
nikto_drupal.plugin 1.00
nikto_embedded.plugin 2.07
nikto_favicon.plugin 2.00
nikto_fileops.plugin 1.00
nikto_headers.plugin 2.11
nikto_httpoptions.plugin 2.10
nikto_ms10_070.plugin 1.00
nikto_msgs.plugin 2.07
nikto_multiple_index.plugin 2.03
nikto_negotiate.plugin 2.00
nikto_origin_reflection.plugin 2.01
nikto_outdated.plugin 2.09
nikto_parked.plugin 2.00
```



```
File Machine View Input Devices Help
My IP Address | IP Address | kali@kali: ~
kali@kali: ~
File Actions Edit View Help
nikto_siebel.plugin 1.00
nikto_sitefiles.plugin 2.00
nikto_ssl.plugin 2.01
nikto_strutshock.plugin 2.01
nikto_tests.plugin 2.04

[kali@kali]~$
[kali@kali]~$ nikto -h 119.18.48.147 -nolookup
- Nikto v2.1.6

+ Target IP: 119.18.48.147
+ Target Hostname: 119.18.48.147
+ Target Port: 80
+ Start Time: 2024-07-27 00:56:49 (GMT-4)

+ Server: No banner retrieved
+ 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://pamcaprive.svkm.ac.in:6082/php/uid.php?sys=10rule=30token=NGScrqarWGS0XrdyEJclw4ZVMw-burl-http://119.18.48.147x2f
°C

[kali@kali]~$
[kali@kali]~$ nikto -h 119.18.48.147 -findonly
- Nikto v2.1.6

+ Server: http://119.18.48.147:80 (no identification possible)

[kali@kali]~$
[kali@kali]~$ nikto -h 119.18.48.147 -Pause 10
-***** Pausing 10 second(s) per request
- Nikto v2.1.6
°C

[kali@kali]~$
[kali@kali]~$ nikto -h 119.18.48.147 -Pause 1
-***** Pausing 1 second(s) per request
- Nikto v2.1.6

+ Target IP: 119.18.48.147
+ Target Hostname: 119.18.48.147
+ Target Port: 80
+ Start Time: 2024-07-27 00:59:19 (GMT-4)

+ Server: No banner retrieved
+ 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://pamcaprive.svkm.ac.in:6082/php/uid.php?sys=10rule=30token=NGScrqarWGS0XrdyEJclw4ZVMw-burl-http://119.18.48.147x2f
°C

File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR! Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-07-26 06:17:25 (GMT-4) (12 seconds)

+ 1 host(s) tested

[kali@kali]~$
[kali@kali]~$ nikto -h 119.18.48.147
- Nikto v2.1.6

+ Target IP: 119.18.48.147
+ Target Hostname: 119.18.48.147
+ Target Port: 80
+ Start Time: 2024-07-26 06:19:37 (GMT-4)

+ Server: No banner retrieved
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR! Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-07-26 06:19:47 (GMT-4) (10 seconds)

+ 1 host(s) tested

[kali@kali]~$
[kali@kali]~$ nikto -h instagram.com -ssl
- Nikto v2.1.6

+ Target IP: 163.70.143.174
+ Target Hostname: instagram.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=Menlo Park/O=Meta Platforms, Inc./CN=*.instagram.com
Cipher: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
+ Start Time: 2024-07-26 06:21:08 (GMT-4)

+ Server: No banner retrieved
+ 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
+ Uncommon header 'x-stack' found, with contents: www
+ Uncommon header 'x-fb-debug' found, with contents: 630yJUmLlUgNGSxAYvBdGpPq4jDzuzST3yvxsc1SgTslwzFmBGFxc/EnXlUmb9eZertGELHlvz7CCw=
+ Uncommon header 'alt-svc' found, with contents: h3='143'; ma=86400
+ The site uses SSL and Expect-CT header is not present.
+ 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.instagram.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
°C

[kali@kali]~$
```