Assignment No: 5

Title: Network Scanning Using Nikto: A Practical Approach to perform network discovery and scanning Using Nikto.

Name: Shubhankar jakate
PRN : 22310371
Roll No = 382019

Theory

Nikto

- Nikto is an **open-source web server scanner** that performs comprehensive tests against web servers for vulnerabilities.
- It can detect:
  - Outdated server software.
  - Potentially dangerous files and scripts.
  - Misconfigured HTTP headers (like missing X-Frame-Options, CSP, etc.).
  - Default files and directories.
- It supports both HTTP and HTTPS scanning.

Nmap (for discovery)

- Nmap is used to perform **network discovery** (finding live hosts and open ports).
- By combining Nmap with Nikto, we can first discover active hosts (with web servers) and then scan them for vulnerabilities.

Working Principle:

1. **Nmap** identifies IPs with port `80/443` open.
2. **Nikto** scans those IPs for vulnerabilities, headers, outdated versions, and misconfigurations.

Procedure

Step 1: Update System and Install Nikto

```
sudo apt update
sudo apt install nikto -y
```

Step 2: Verify Nikto Installation

```
nikto -Help
```

Step 3: Scan a Website

```
nikto -h linuxhint.com
```

Step 4: Scan an HTTPS Website

```
nikto -h pbs.org -ssl
```

Step 5: Check Your Network Interfaces

```
sudo ifconfig
```

Step 6: Use Nmap for Discovery

```
sudo nmap -p 80 192.168.0.0/24 -oG linuxhint.txt
```

Implementation :

(base) e-102@e-102-21:~$ sudo apt update
Hit:1 https://packages.microsoft.com/repos/code stable InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:5 https://ppa.launchpadcontent.net/deadsnakes/ppa/ubuntu noble InRelease
Hit:6 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
167 packages can be upgraded. Run 'apt list --upgradable' to see them.

(base) e-102@e-102-21:~$ sudo apt install nikto
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.1.5-3.1).
The following packages were automatically installed and are no longer required:
  libllvm17t64 nvidia-firmware-535-535.183.01 python3-netifaces
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 167 not upgraded.

(base) e-102@e-102-21:~$ nikto -help
Unknown option: help

```
    -config+            Use this config file
    -Display+           Turn on/off display outputs
    -dbcheck            check database and other key files for syntax errors
    -Format+            save file (-o) format
    -Help               Extended help information
    -host+              target host
    -id+                Host authentication to use, format is id:pass or id:pass:realm
```

```
    -list-plugins      List all available plugins
    -output+           Write output to this file
    -nossl             Disables using SSL
    -no404             Disables 404 checks
    -Plugins+          List of plugins to run (default: ALL)
    -port+             Port to use (default 80)
    -root+             Prepend root value to all requests, format is /directory
    -ssl               Force ssl mode on port
    -Tuning+           Scan tuning
    -timeout+          Timeout for requests (default 10 seconds)
    -update            Update databases and plugins from CIRT.net
    -Version           Print plugin and database versions
    -vhost+            Virtual host (for Host header)
               + requires a value

      Note: This is the short help output. Use -H for full help text.
```

```
(base) e-102@e-102-21:~$ nikto -h linuxhint.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.67.135.17
+ Target Hostname:    linuxhint.com
+ Target Port:        80
+ Start Time:         2025-08-26 13:39:04 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ Retrieved via header: HTTP/1.1 forward.http.proxy:3128
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'report-to' found, with contents: {"group":"cf-
nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=cS4sjJF2BY7
WxAL0CXzx%2FbZrh511zW9kcsmzo5MKG3d%2F5iRFyu4v6sx560cOJ6wyAkkjzCHgdmBJktw
GNXouDyjmvb0AYa61MfkcSDI%3D"}]}
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'cf-ray' found, with contents: 9751d84d89433f79-BOM
+ Uncommon header 'nel' found, with contents: {"report_to":"cf-
nel","success_fraction":0.0,"max_age":604800}
+ Root page / redirects to: https://linuxhint.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'proxy-status' found, with contents: Cloudflare-Proxy;error=http_request_error
+ 6544 items checked: 24 error(s) and 8 item(s) reported on remote host
+ End Time:           2025-08-26 13:40:39 (GMT5.5) (95 seconds)
```

```
(base) e-102@e-102-21:~$ nikto -h pbs.org -ssl
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          54.225.198.196
+ Target Hostname:    pbs.org
```

```
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /CN=wnet.video-staging.pbs.org
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer:  /C=US/O=Let's Encrypt/CN=E5
+ Start Time:         2025-08-26 13:44:22 (GMT5.5)
---------------------------------------------------------------------------
+ Server: openresty
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-12-151.ec2.internal
+ Uncommon header 'x-kids-map' found, with contents: nousername
+ Root page / redirects to: https://www.pbs.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-cache-fs-status' found, with contents: HIT
+ Hostname 'pbs.org' does not match certificate's CN 'wnet.video-staging.pbs.org'
```

(base) e-102@e-102-21:~$ sudo ifconfig

```
[sudo] password for e-102:
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 24:6a:0e:77:fa:f9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3623  bytes 382799 (382.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3623  bytes 382799 (382.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.25.6.7  netmask 255.255.224.0  broadcast 10.25.31.255
        inet6 fe80::5d34:aa91:bee9:50e8  prefixlen 64  scopeid 0x20<link>
        ether c0:bf:be:b8:d8:c2  txqueuelen 1000  (Ethernet)
        RX packets 358504  bytes 245245020 (245.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41959  bytes 9728226 (9.7 MB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0
```

(base) e-102@e-102-21:~$ sudo nmap -p 80 192.168.0.0/24 -oG linuxhint.txt

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-26 14:07 IST
Nmap scan report for 192.168.0.0
```

Host is up (0.0036s latency).

PORT   STATE SERVICE
80/tcp open http

Nmap scan report for 192.168.0.1
Host is up (0.0060s latency).

PORT   STATE SERVICE
80/tcp open http

Nmap scan report for 192.168.0.2
Host is up (0.0060s latency).

PORT   STATE SERVICE
80/tcp open http

Nmap scan report for 192.168.0.3

Host is up (0.0060s latency).

PORT   STATE SERVICE
80/tcp open http

Nmap scan report for 192.168.0.4
Host is up (0.0060s latency).

Nmap scan report for 192.168.0.255
Host is up (0.0037s latency).

PORT   STATE SERVICE
80/tcp open http

Nmap done: 256 IP addresses (256 hosts up) scanned in 36.94 seconds