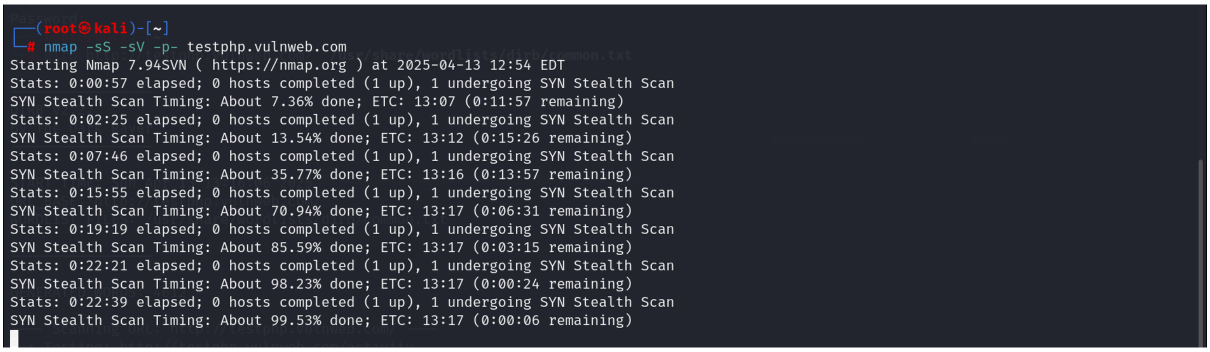
SHADOWFOX CYBER SECURITY INTERNSHIP TASKS

Task Level (Beginner):

1. Open Ports Scan (Nmap)
    - Ran a nmap scan
      #nmap -sS -sV -p- http://testphp.vulnweb.com/



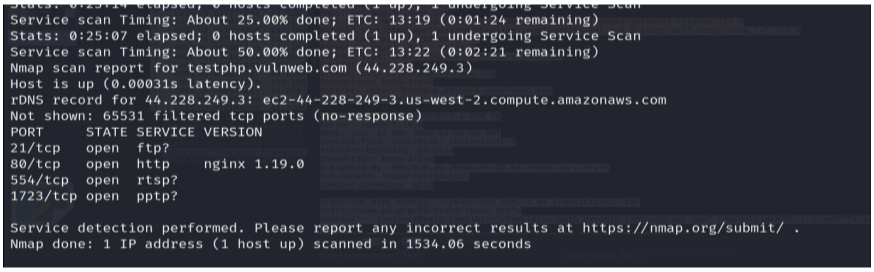
```
┌──(root㉿kali)-[~]
└─# nmap -sS -sV -p- testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-13 12:54 EDT
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.36% done; ETC: 13:07 (0:11:57 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.54% done; ETC: 13:12 (0:15:26 remaining)
Stats: 0:07:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.77% done; ETC: 13:16 (0:13:57 remaining)
Stats: 0:15:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.94% done; ETC: 13:17 (0:06:31 remaining)
Stats: 0:19:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.59% done; ETC: 13:17 (0:03:15 remaining)
Stats: 0:22:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.23% done; ETC: 13:17 (0:00:24 remaining)
Stats: 0:22:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.53% done; ETC: 13:17 (0:00:06 remaining)
```

-sS: TCP SYN scan

-sV: Service version detection

-p-: Scan all 65535 ports

- Result



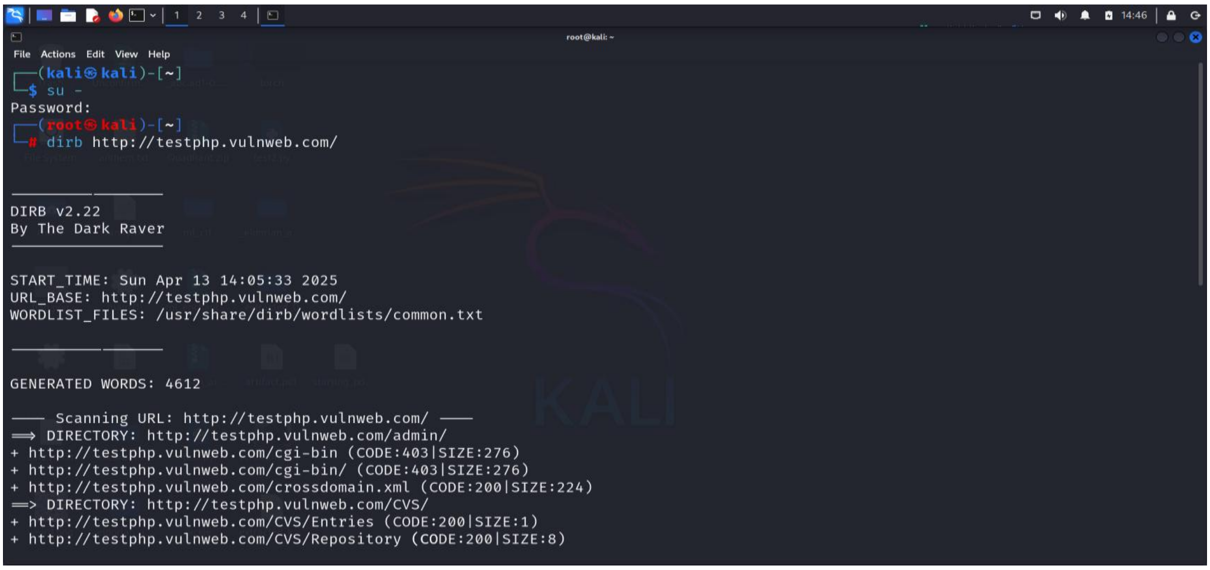
```
Stats: 0:23:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 13:19 (0:01:24 remaining)
Stats: 0:25:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 13:22 (0:02:21 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.00031s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp?
80/tcp   open  http    nginx 1.19.0
554/tcp  open  rtsp?
1723/tcp open  pptp?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1534.06 seconds
```

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
554/tcp	open	rtsp
1723/tcp	open	pptp

2.Brute Force Directories

- **Target**: `http://testphp.vulnweb.com/`
- Used Dirb v2.22



```
┌──(kali㉿kali)-[~]
└─$ su -
Password:
┌──(root㉿kali)-[~]
└─# dirb http://testphp.vulnweb.com/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Apr 13 14:05:33 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
```

- generated words: 4612
- **Scan Duration**: ~27 minutes

- Discovered Directories (7) are:
  http://testphp.vulnweb.com/admin/

  http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)

  http://testphp.vulnweb.com/CVS/

  http://testphp.vulnweb.com/images/

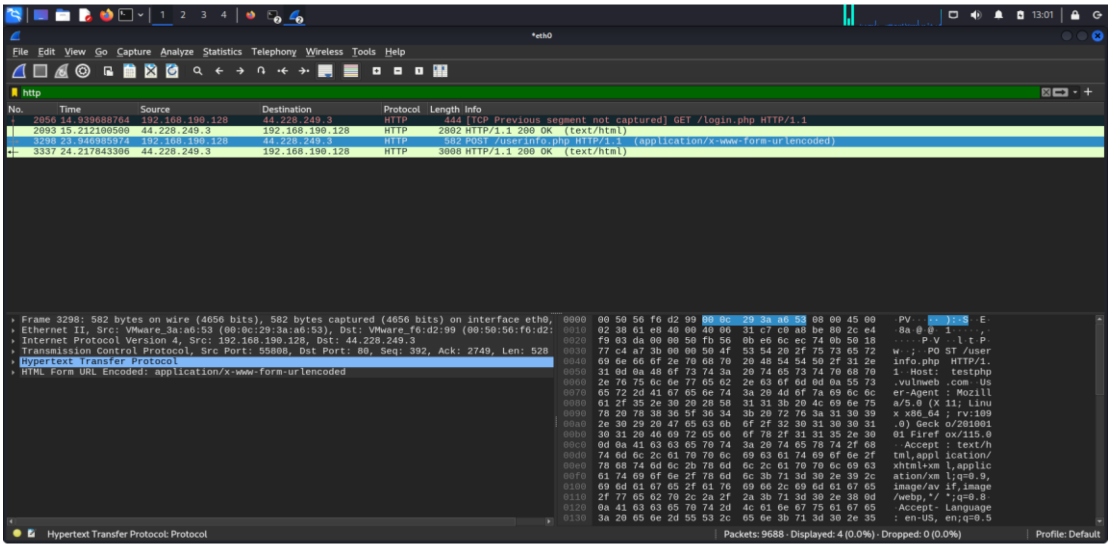
  http://testphp.vulnweb.com/pictures/

  http://testphp.vulnweb.com/secured/

  http://testphp.vulnweb.com/vendor/

3.Login Credentials through Wireshark

- Opened wireshark - #wireshark
- Selected the active network interface
- Started capturing packets and filtered http packets after logging using credentials Username= test and Password=test in http://testphp.vulnweb.com/ .



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
13:01

```
No.   Time            Source            Destination       Protocol  Length Info
2056 14.939688764  192.168.190.128   44.228.249.3      HTTP       444 [TCP Previous segment not captured] GET /login.php HTTP/1.1
2093 15.212100500  44.228.249.3      192.168.190.128   HTTP      2802 HTTP/1.1 200 OK  (text/html)
3298 23.946985974  192.168.190.128   44.228.249.3      HTTP       582 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
3337 24.217843306  44.228.249.3      192.168.190.128   HTTP      3008 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 3298: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface eth0,
▸ Ethernet II, Src: VMware_3a:a6:53 (00:0c:29:3a:a6:53), Dst: VMware_f6:d2:99 (00:50:56:f6:d2:
▸ Internet Protocol Version 4, Src: 192.168.190.128, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 55808, Dst Port: 80, Seq: 392, Ack: 2749, Len: 528
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

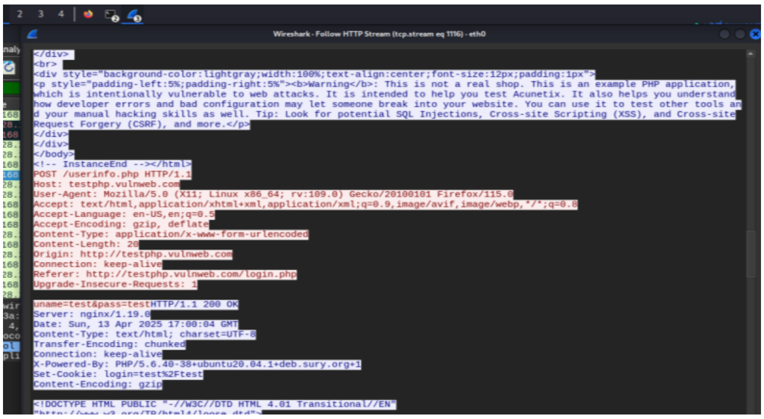
```
0000  00 50 56 f6 d2 99 00 0c  29 3a a6 53 08 00 45 00   ·PV··· ·· ):·S··E·
0010  02 38 61 e8 40 00 40 06  31 c7 c0 a8 be 80 2c e4   ·8a·@·@· 1·····,·
0020  f9 03 da 00 00 50 fb 56  0b e6 6c ec 74 0b 50 18   ·····P·V ··l·t·P·
0030  77 c4 a7 3b 00 00 50 4f  53 54 20 2f 75 73 65 72   w··;··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 30 39   x x86_64 ; rv:109
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 31 35 2e 30   01 Firef ox/115.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  69 6d 61 67 65 2f 61 76  69 66 2c 69 6d 61 67 65   image/av if,image
0110  2f 77 65 62 70 2c 2a 2f  2a 3b 71 3d 30 2e 38 0d   /webp,*/ *;q=0.8·
0120  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0130  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
```

Hypertext Transfer Protocol: Protocol

Packets: 9688 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

- Found a POST request to /userinfo.php.
- Then , Right-click on the packet → Follow → HTTP Stream.



Wireshark · Follow HTTP Stream (tcp.stream eq 1116) · eth0

```
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real shop. This is an example PHP application,
which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand
how developer errors and bad configuration may let someone break into your website. You can use it to test other tools an
d your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site
Request Forgery (CSRF), and more.</p>
</div>
</div>
</body>
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 13 Apr 2025 17:00:04 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

- Therefore, found the credentials by inspecting the packet.