

COMPUTER NETWORKS

LAB 9

NAME - KAPAROTU VENKATA SURYA THARANI
USN - 22BTRAD018
BRANCH - AIDE

Ques - Demonstrate the security aspects of all possible protocols using Wireshark.

FTP

Entered login credentials are visible in Wireshark

```
C:\Users\kvsth>ftp
ftp> o ftp.dlptest.com
Connected to ftp.dlptest.com.
220 Welcome to the DLP Test FTP Server
200 Always in UTF8 mode.
User (ftp.dlptest.com:(none)): dlpuser
331 Please specify the password.
Password:
230 Login successful.
ftp> bye
221 Goodbye.

C:\Users\kvsth>|
```

```
Wireshark · Follow TCP Stream (tcp.stream eq 2) · Wi-Fi

220 Welcome to the DLP Test FTP Server
OPTS UTF8 ON
200 Always in UTF8 mode.
USER dlpuser
331 Please specify the password.
PASS rNrKYTX9g7z3RgJRmxWuGHbeu
230 Login successful.
QUIT
221 Goodbye.
```

As we can see the login details are written in ftp protocol therefore it is not a secured protocol.

Telnet: Telnet clock

```
Connected to TELEHACK port 89

It is 8:52 am on Sunday, July 2, 2023 in Mountain View, California, USA.
There are 183 local users. There are 26647 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
?          a2          advent      basic       bf          c8
cal        calc        cat         ching       clear       clock
date       ddate       delta      diff        dir         echo
eliza      exit        factor     fnord       gif         head
ipaddr     joke       liff       login       md5         minesweeper
more       morse      netstat    newuser     notes       octopus
phoon     pig        ping       pong        primes      privacy
rand       rfc        rig        roll        rot13       run
sleep     starwars   traceroute typespeed   units       usenet
uupath    uupath     uuplot     when        zc          zork

Press control-C to interrupt any command.
More commands become available after login.
.clock█
```

```

Connected to TELEHACK port 89

It is 8:55 am on Sunday, July 2, 2023 in Mountain View, California, USA.
There are 102 local users. There are 26647 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
2048      ac      aquarium  bf      cal      calc
cat       ching   clock     cowsay  date     ddate
delta     diff      echo      exit    factor   figlet
file      fnord     geoip     head    help     ipaddr
joke      liff      login     mac      minesweeper more
morse     netstat   newuser   notes   octopus  pig
ping      pong     primes   privacy qr       rain
rand      rig      rot13    run     sleep    starwars
sudoku    tail     traceroute units   usenet   users
uumap     uupath   uuplot   weather zc       zork

Press control-C to interrupt any command.
More commands become available after login.
.login
username? xyz
?User not available - "xyz"
.login
username? hi
Password: ****
?Password not correct
Password: ^C

```

```

Password: ^C

```

```
?Password not correct
Password: q*u*i*t
*
?Password not correct
Password: .^C
.lloogigni
n
username? hihi


Password: i*d*o*nt*kn*o***w*

?Password not correct
Password:
```

Since we can see the password and login details written therefore it is not a secured protocol.

Http:

Login unsuccessfully



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

go

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

Getting the username and password using Wireshark.

```
Wireshark · Follow TCP Stream (tcp.stream eq 27) · Wi-Fi

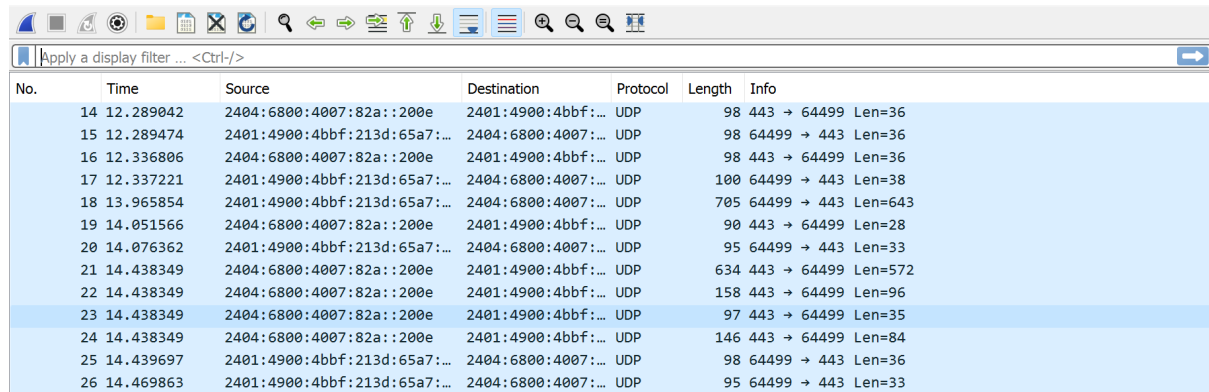
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 29
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=hey_112&pass=olla_12345HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sun, 02 Jul 2023 16:11:05 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
Location: login.php

e
```

Since anyone can see the password and details therefore http is not secured.

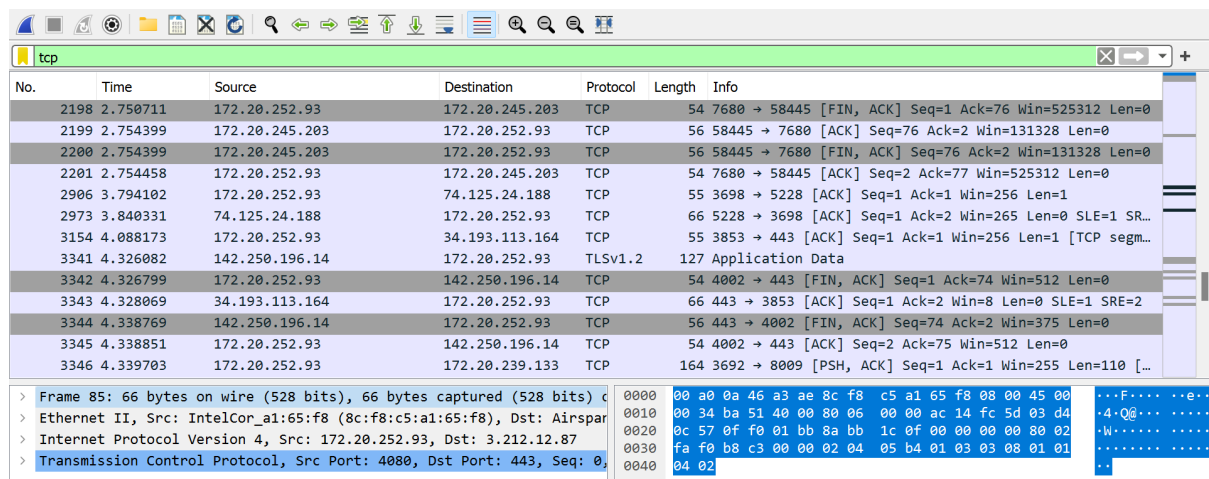
UDP



No.	Time	Source	Destination	Protocol	Length	Info
14	12.289042	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	98	443 -> 64499 Len=36
15	12.289474	2401:4900:4bbf:213d:65a7:...	2404:6800:4007:...	UDP	98	64499 -> 443 Len=36
16	12.336806	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	98	443 -> 64499 Len=36
17	12.337221	2401:4900:4bbf:213d:65a7:...	2404:6800:4007:...	UDP	100	64499 -> 443 Len=38
18	13.965854	2401:4900:4bbf:213d:65a7:...	2404:6800:4007:...	UDP	705	64499 -> 443 Len=643
19	14.051566	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	90	443 -> 64499 Len=28
20	14.076362	2401:4900:4bbf:213d:65a7:...	2404:6800:4007:...	UDP	95	64499 -> 443 Len=33
21	14.438349	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	634	443 -> 64499 Len=572
22	14.438349	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	158	443 -> 64499 Len=96
23	14.438349	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	97	443 -> 64499 Len=35
24	14.438349	2404:6800:4007:82a::200e	2401:4900:4bbf:...	UDP	146	443 -> 64499 Len=84
25	14.439697	2401:4900:4bbf:213d:65a7:...	2404:6800:4007:...	UDP	98	64499 -> 443 Len=36
26	14.469863	2401:4900:4bbf:213d:65a7:...	2404:6800:4007:...	UDP	95	64499 -> 443 Len=33

Since it doesn't have a sequence number and acknowledgment number, therefore, UDP is not secured.

TCP



No.	Time	Source	Destination	Protocol	Length	Info
2198	2.750711	172.20.252.93	172.20.245.203	TCP	54	7680 -> 58445 [FIN, ACK] Seq=1 Ack=76 Win=525312 Len=0
2199	2.754399	172.20.245.203	172.20.252.93	TCP	56	58445 -> 7680 [ACK] Seq=76 Ack=2 Win=131328 Len=0
2200	2.754399	172.20.245.203	172.20.252.93	TCP	56	58445 -> 7680 [FIN, ACK] Seq=76 Ack=2 Win=131328 Len=0
2201	2.754458	172.20.252.93	172.20.245.203	TCP	54	7680 -> 58445 [ACK] Seq=2 Ack=77 Win=525312 Len=0
2906	3.794102	172.20.252.93	74.125.24.188	TCP	55	3698 -> 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
2973	3.840331	74.125.24.188	172.20.252.93	TCP	66	5228 -> 3698 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SR...
3154	4.088173	172.20.252.93	34.193.113.164	TCP	55	3853 -> 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segm...
3341	4.326082	142.250.196.14	172.20.252.93	TLSv1.2	127	Application Data
3342	4.326799	172.20.252.93	142.250.196.14	TCP	54	4002 -> 443 [FIN, ACK] Seq=1 Ack=74 Win=512 Len=0
3343	4.328069	34.193.113.164	172.20.252.93	TCP	66	443 -> 3853 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2
3344	4.338769	142.250.196.14	172.20.252.93	TCP	56	443 -> 4002 [FIN, ACK] Seq=74 Ack=2 Win=375 Len=0
3345	4.338851	172.20.252.93	142.250.196.14	TCP	54	4002 -> 443 [ACK] Seq=2 Ack=75 Win=512 Len=0
3346	4.339703	172.20.252.93	172.20.239.133	TCP	164	3692 -> 8009 [PSH, ACK] Seq=1 Ack=1 Win=255 Len=110 [...]

Frame 85: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0	0000	00 a0 0a 46 a3 ae 8c f8 c5 a1 65 f8 08 00 45 00	...
Ethernet II, Src: IntelCor_al:65:f8 (8c:f8:c5:a1:65:f8), Dst: Airtel:80:00:00:00:00:00	0010	00 34 ba 51 40 00 80 06 00 00 ac 14 fc 5d 03 d4	...4..Q@...
Internet Protocol Version 4, Src: 172.20.252.93, Dst: 3.212.12.87	0020	0c 57 0f f0 01 bb 8a bb 1c 0f 00 00 00 00 80 02	...W.....
Transmission Control Protocol, Src Port: 4080, Dst Port: 443, Seq: 0,	0030	fa f0 b8 c3 00 00 02 04 05 b4 01 03 03 08 01 01
	0040	04 02	...

Since TCP's packets have sequence numbers and acknowledgment numbers therefore TCP is secured.

