ADD COMPANY NAME

Sniffing in a Controlled Environment

Drishti Bhat(2023a7r006)
CSE(Cybersecurity)

Objectives

- To study packet sniffing and network traffic analysis as tools for identifying vulnerabilities.
- To understand the dangers of unencrypted data transmission and suggest mitigation strategies.

Packet Sniffing

Process of capturing and inspecting data packets as they travel across a network.

Network Traffic Analysis

Method of monitoring, recording, and analyzing network activity to detect anomalies or vulnerabilities.

Tools Used

- Kali Linux

  (as the attacker/sniffer machine)

- Windows 10 VM

  (as the victim/client machine)

- Vulnerable website

  http://testphp.vulnweb.com

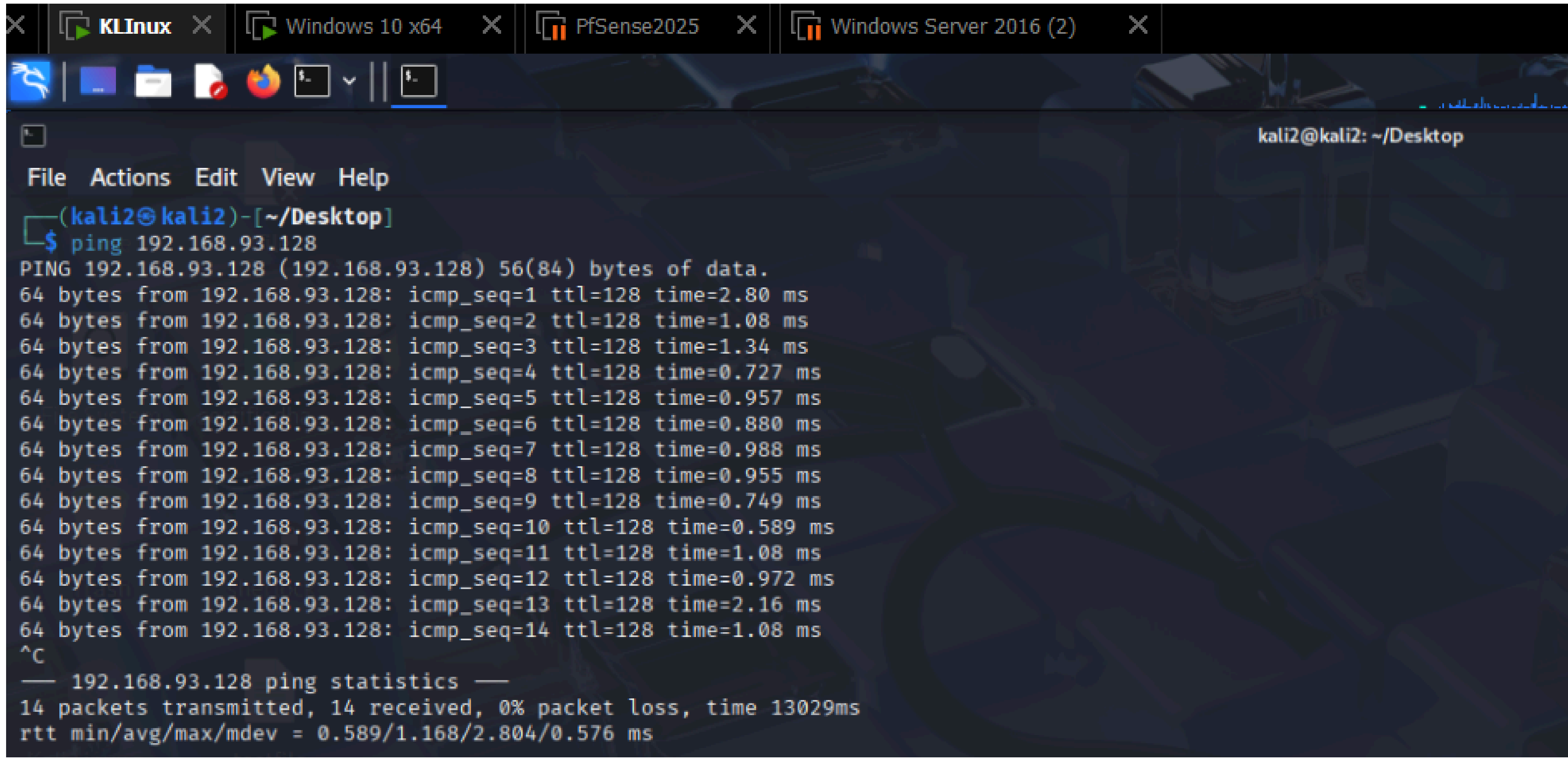
- Wireshark

  (network protocol analyzer)

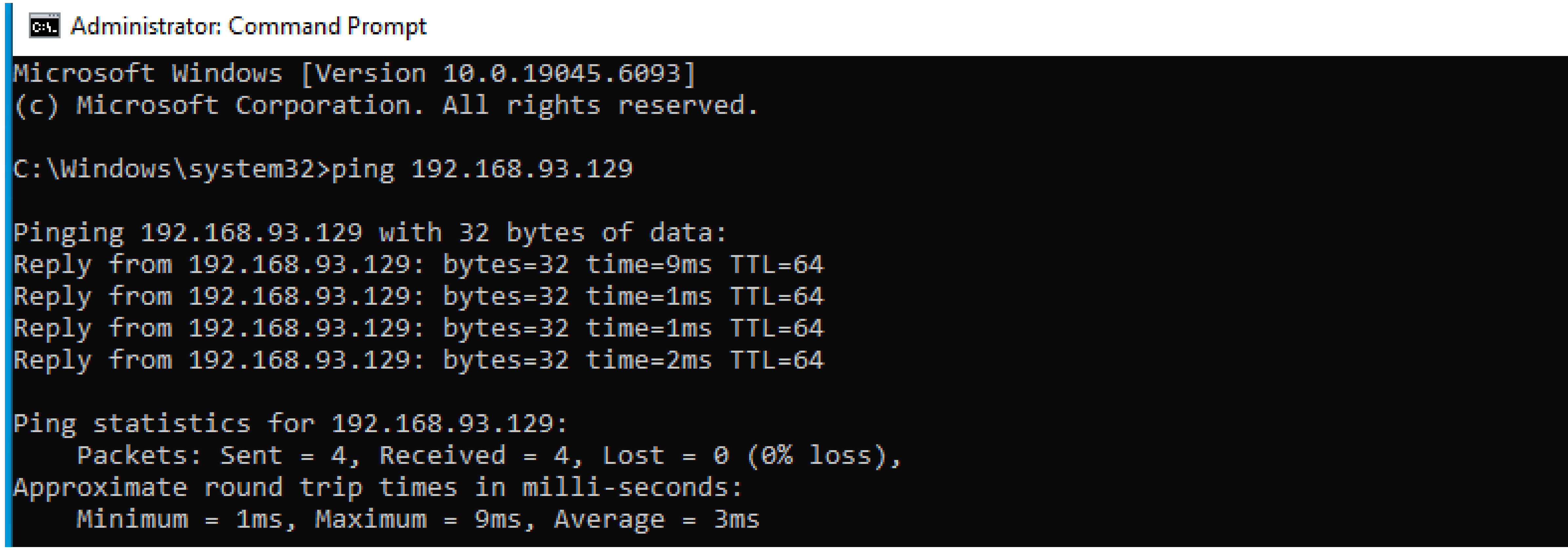
Step 1

- First we need to **ping Windows IP on Kali**

- Then,also **ping Kali on Windows**



```
┌──(kali2㉿kali2)-[~/Desktop]
└─$ ping 192.168.93.128
PING 192.168.93.128 (192.168.93.128) 56(84) bytes of data.
64 bytes from 192.168.93.128: icmp_seq=1 ttl=128 time=2.80 ms
64 bytes from 192.168.93.128: icmp_seq=2 ttl=128 time=1.08 ms
64 bytes from 192.168.93.128: icmp_seq=3 ttl=128 time=1.34 ms
64 bytes from 192.168.93.128: icmp_seq=4 ttl=128 time=0.727 ms
64 bytes from 192.168.93.128: icmp_seq=5 ttl=128 time=0.957 ms
64 bytes from 192.168.93.128: icmp_seq=6 ttl=128 time=0.880 ms
64 bytes from 192.168.93.128: icmp_seq=7 ttl=128 time=0.988 ms
64 bytes from 192.168.93.128: icmp_seq=8 ttl=128 time=0.955 ms
64 bytes from 192.168.93.128: icmp_seq=9 ttl=128 time=0.749 ms
64 bytes from 192.168.93.128: icmp_seq=10 ttl=128 time=0.589 ms
64 bytes from 192.168.93.128: icmp_seq=11 ttl=128 time=1.08 ms
64 bytes from 192.168.93.128: icmp_seq=12 ttl=128 time=0.972 ms
64 bytes from 192.168.93.128: icmp_seq=13 ttl=128 time=2.16 ms
64 bytes from 192.168.93.128: icmp_seq=14 ttl=128 time=1.08 ms
^C
── 192.168.93.128 ping statistics ──
14 packets transmitted, 14 received, 0% packet loss, time 13029ms
rtt min/avg/max/mdev = 0.589/1.168/2.804/0.576 ms
```



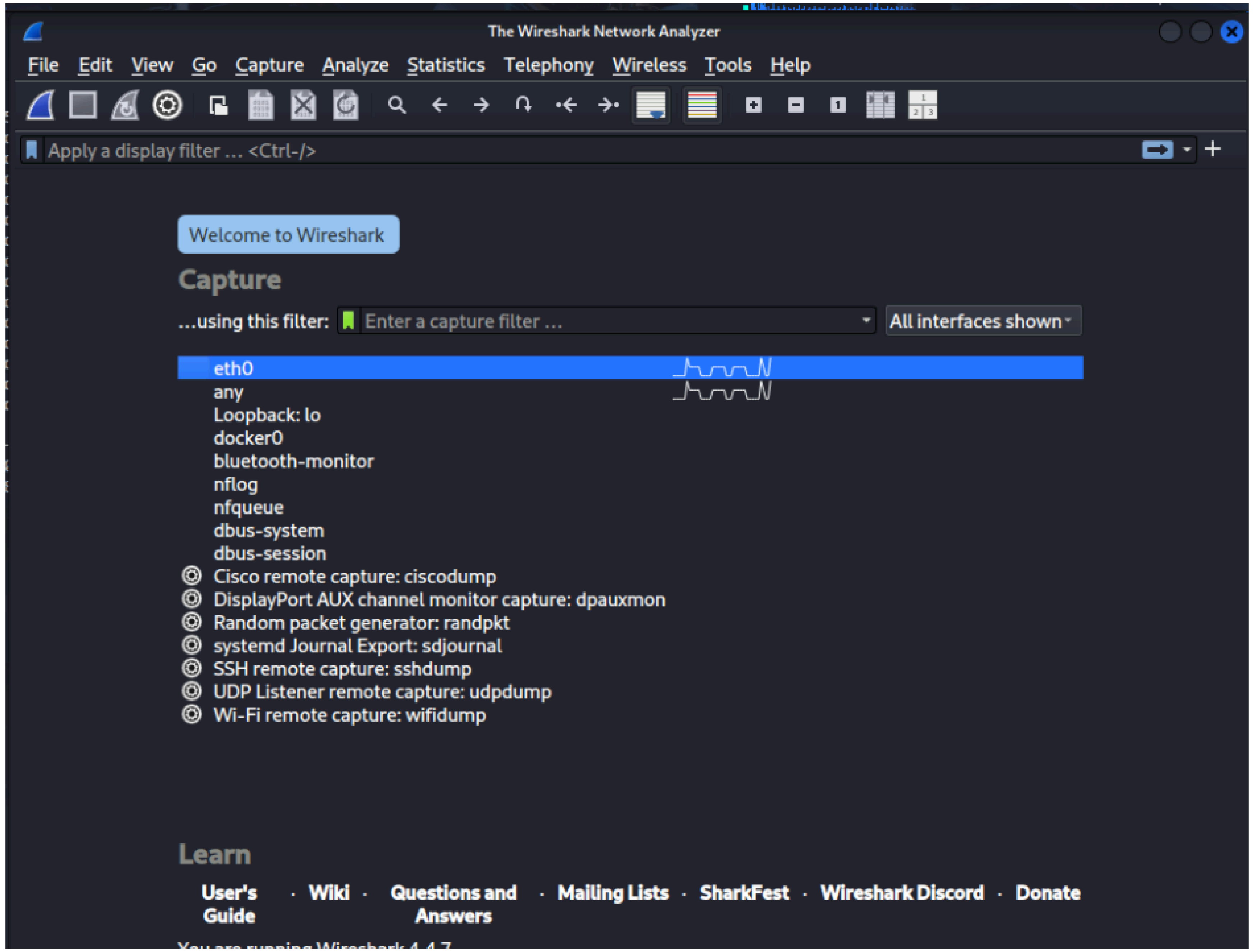
```
Microsoft Windows [Version 10.0.19045.6093]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.93.129

Pinging 192.168.93.129 with 32 bytes of data:
Reply from 192.168.93.129: bytes=32 time=9ms TTL=64
Reply from 192.168.93.129: bytes=32 time=1ms TTL=64
Reply from 192.168.93.129: bytes=32 time=1ms TTL=64
Reply from 192.168.93.129: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.93.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms
```

Step 2

- Launch **Wireshark** (sniffing tool) with root privileges.

- The command is **sudo wireshark**

- Selected network interface **eth0** for packet capturing(as shown).



Capture

…using this filter: Enter a capture filter … All interfaces shown

eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

Learn

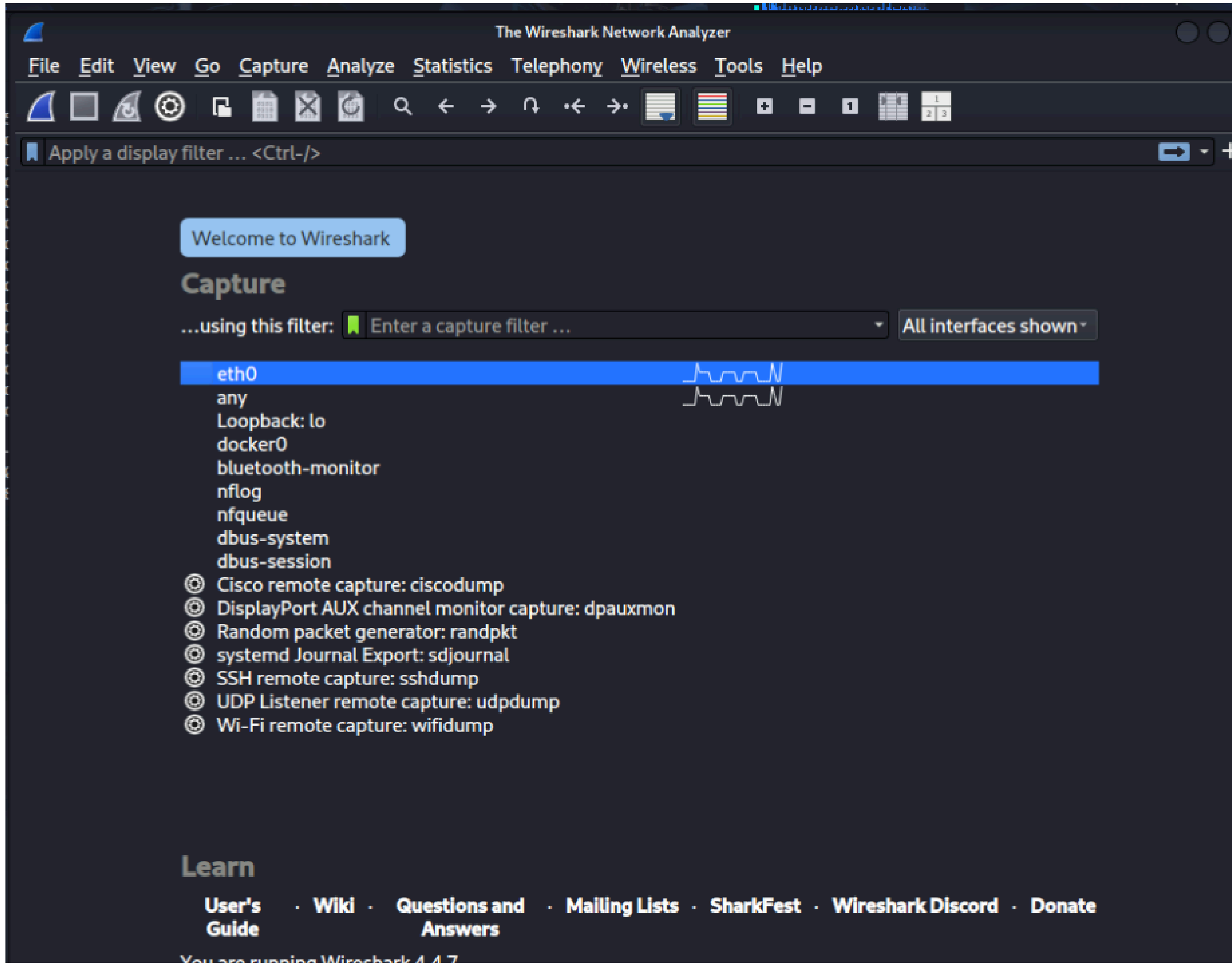
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.7

Step 3

- (1) Visited the website **http://testphp.vulnweb.com/login.php** from the Windows 10 VM

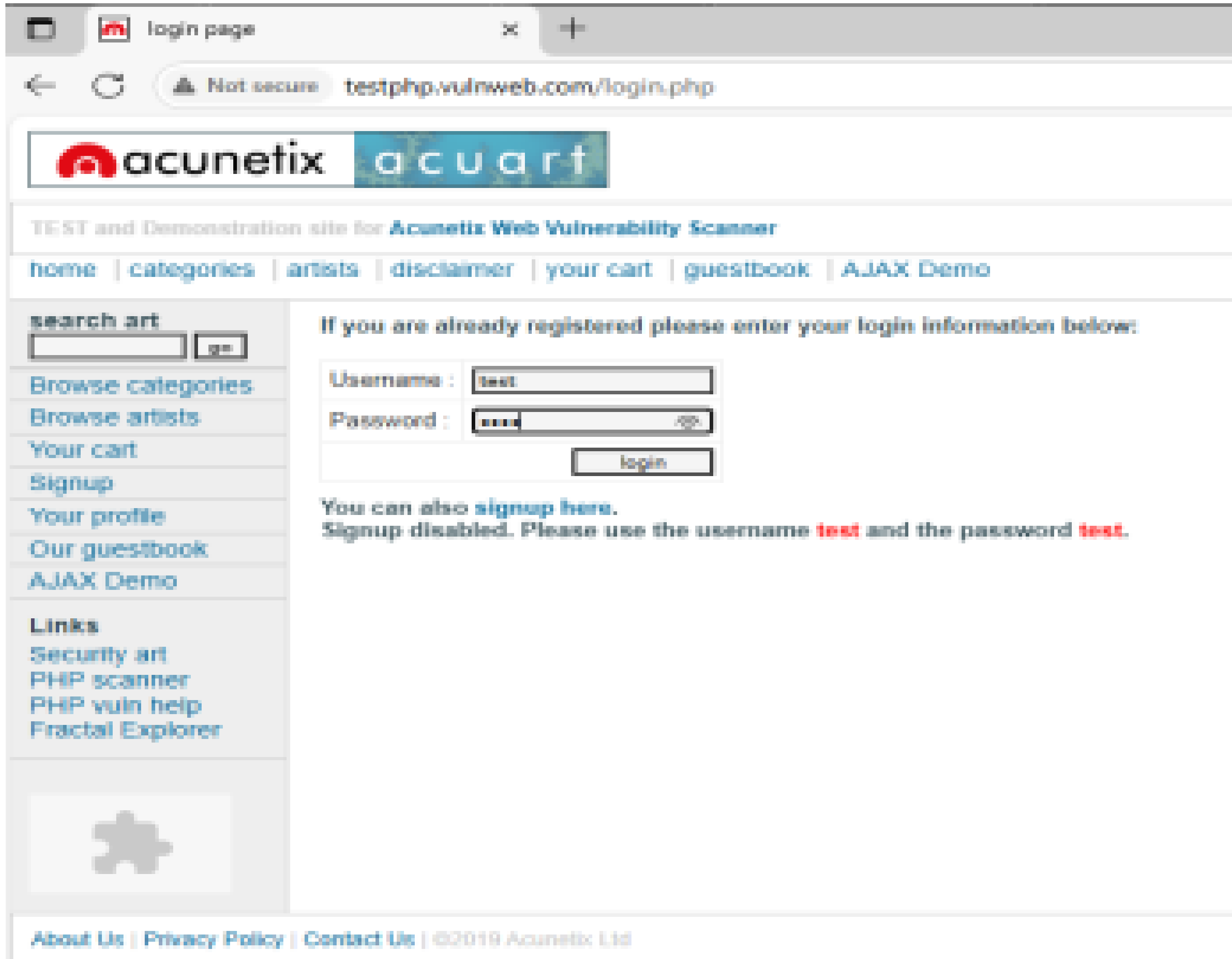
- Then entered the following credentials as: **Username**: test **Password**: test


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide
Wiki
Questions and Answers
Mailing Lists
SharkFest
Wireshark Discord
Donate
You are running Wireshark 4.4.7

Step 4

- Visited the website **http://testphp.vulnweb.com/login.php** from the Windows 10 VM

- Then entered the following credentials as: **Username**: test **Password**: test



testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

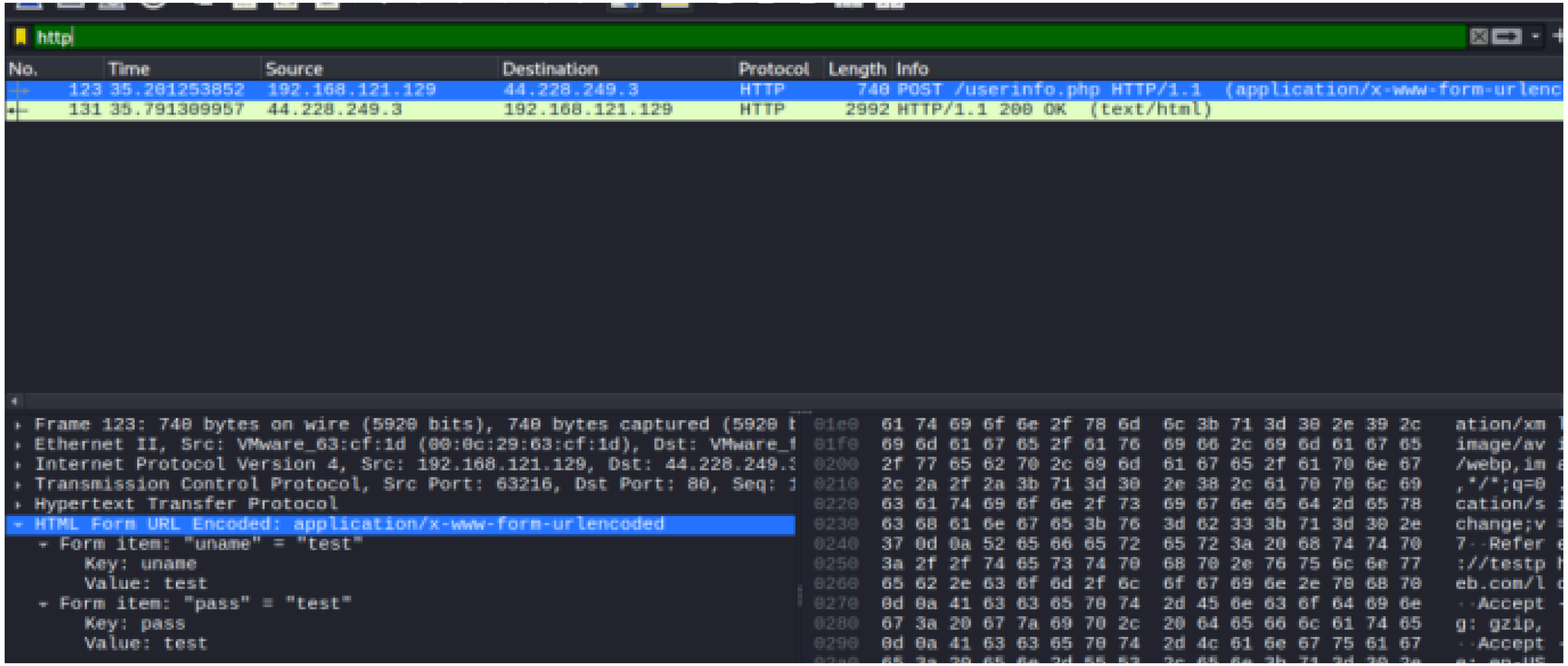
Username : test

Password : ••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 5

- During the login attempt, **Wireshark** on Kali captured the packets.
- The filter used for capturing: **http**
- The POST request has the credentials is clear as shown below



```
http
```

```
No.     Time            Source            Destination       Protocol  Length Info
    123 35.201253852    192.168.121.129   44.228.249.3      HTTP         740 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlenc
    131 35.791309957    44.228.249.3      192.168.121.129   HTTP        2992 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 123: 740 bytes on wire (5920 bits), 740 bytes captured (5920 b
▸ Ethernet II, Src: VMware_63:cf:1d (00:0c:29:63:cf:1d), Dst: VMware_f
▸ Internet Protocol Version 4, Src: 192.168.121.129, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 63216, Dst Port: 80, Seq: 1
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "uname" = "test"
      Key: uname
      Value: test
  ▾ Form item: "pass" = "test"
      Key: pass
      Value: test
```

```
01e0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l
01f0  69 6d 61 67 65 2f 61 76  69 66 2c 69 6d 61 67 65   image/av i
0200  2f 77 65 62 70 2c 69 6d  61 67 65 2f 61 70 6e 67   /webp,im a
0210  2c 2a 2f 2a 3b 71 3d 30  2e 38 2c 61 70 70 6c 69   ,*/*;q=0 .
0220  63 61 74 69 6f 6e 2f 73  69 67 6e 65 64 2d 65 78   cation/s i
0230  63 68 61 6e 67 65 3b 76  3d 62 33 3b 71 3d 30 2e   change;v =
0240  37 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   7··Refer e
0250  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp h
0260  65 62 2e 63 6f 6d 2f 6c  6f 67 69 6e 2e 70 68 70   eb.com/l o
0270  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -
0280  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,
0290  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -
```

Mitigations

- Using website (with **HTTPS**) keeps the connection private and encrypted.
- Enabling two-factor authentication(**2FA**).
- Monitoring the network should be done to catch suspicious activity early,so that attacker has no chance to extract the user's sensitive information(unethical purpose).
- Segment the network using **VLANs** and isolate sensitive systems from public devices