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]): -

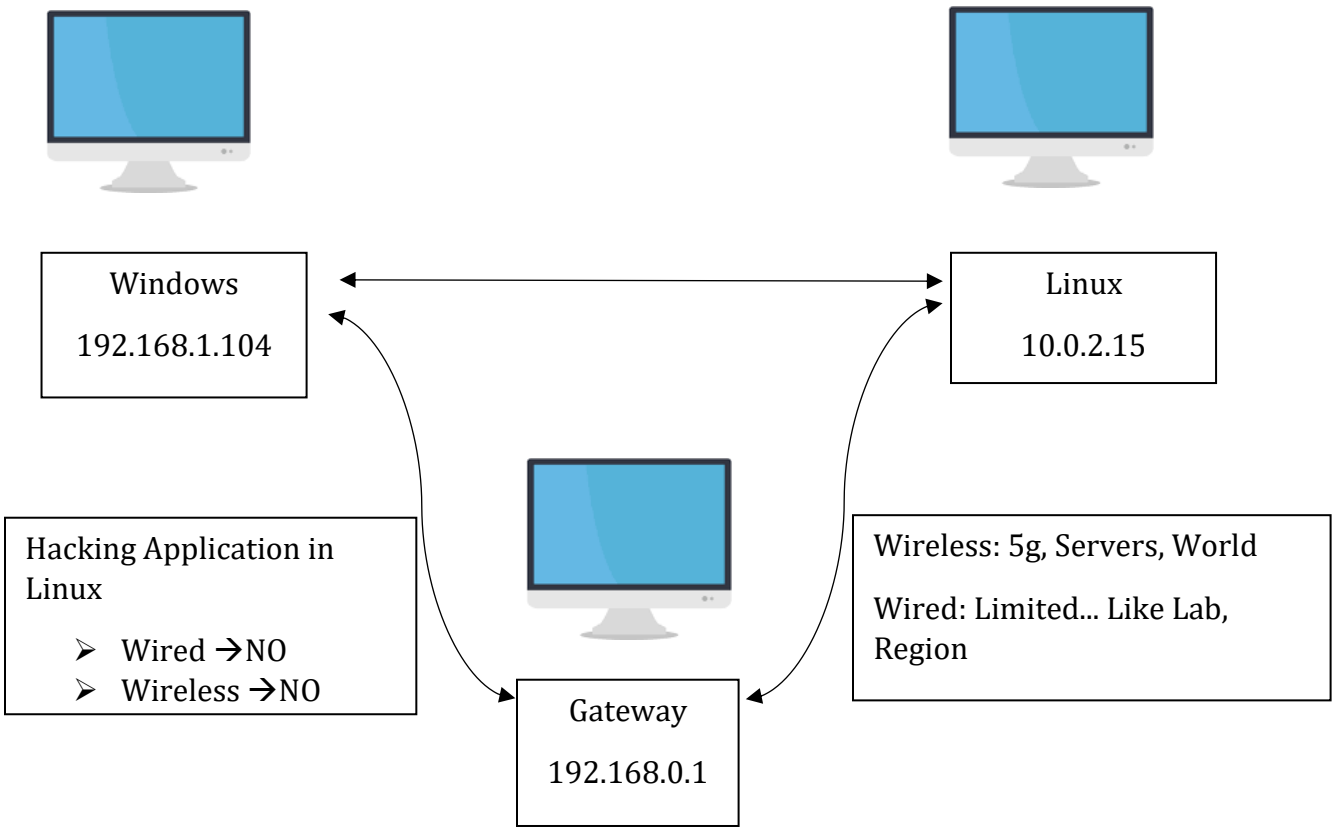
  - Case Study: -7
  - Case Study: 8

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:

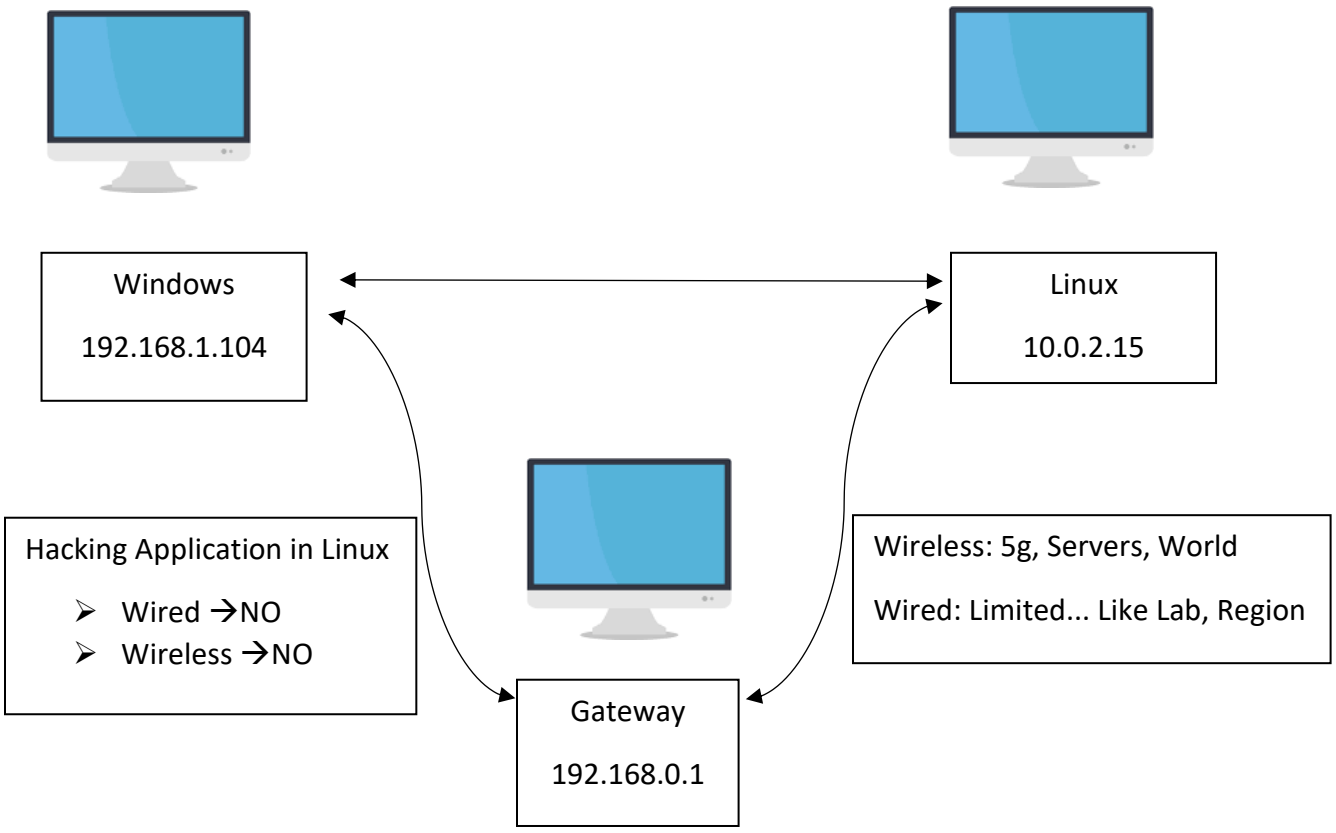
- **Windows → Wireless**
- **Linux → Wired**
- Hacking can't be performed



- **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 2:

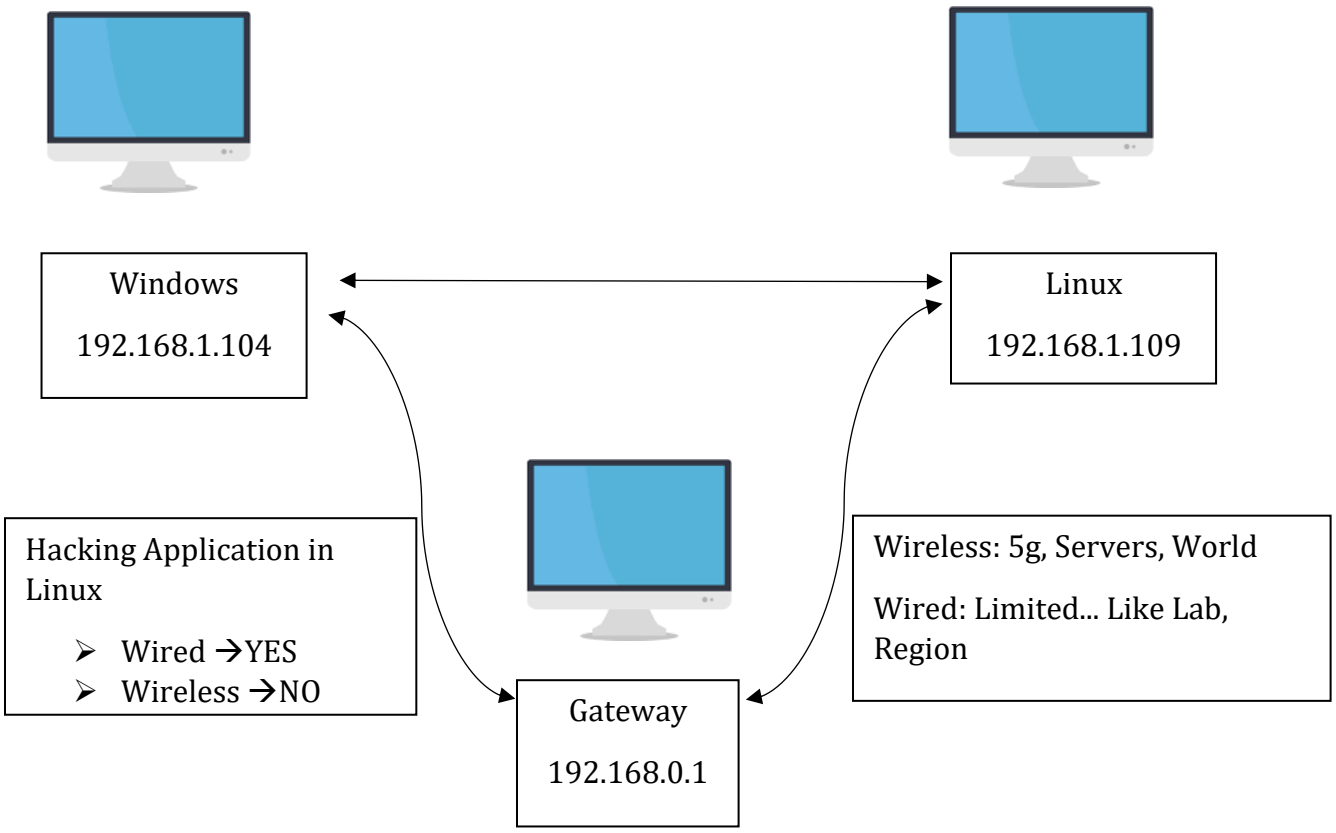
- **Windows → Wired**
- **Linux → Wired**
- Hacking can't be performed



- **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:

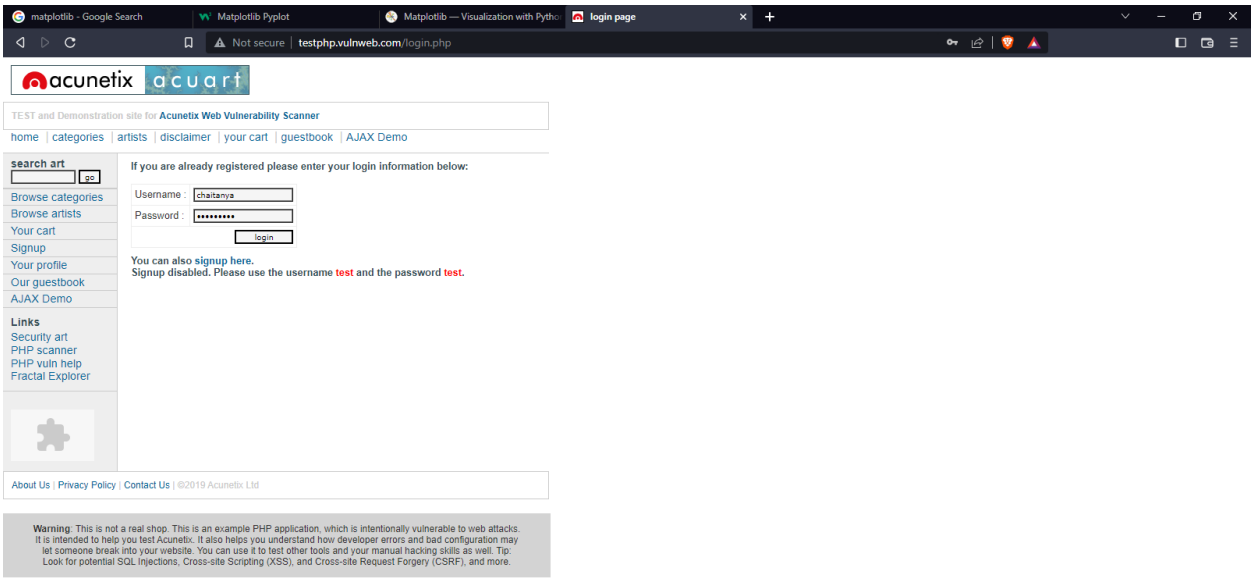
- **Windows → Wired**
- **Linux → Wired**
- With change in Configuration to Bridged
- Hacking can be performed

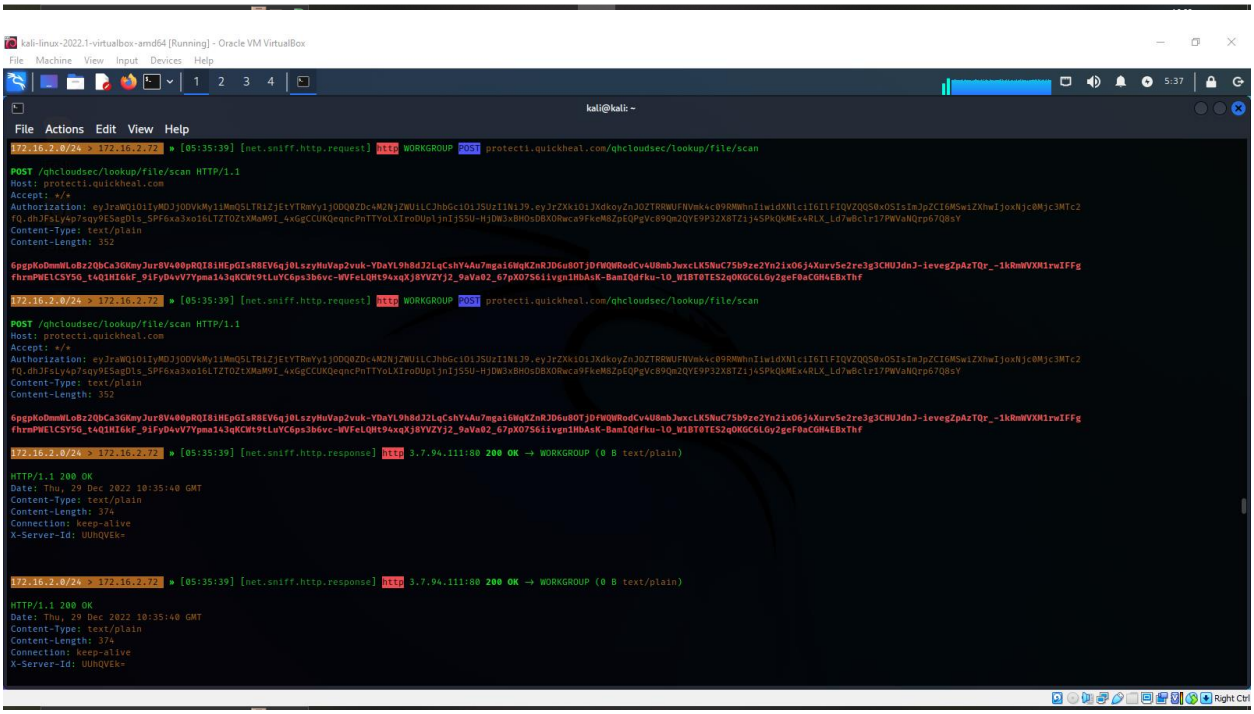


- **10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)**
- **But you can hack Linux-Linux only which is an advanced case study**

Practical approach for Case Study: -3

- Testing a http login page for case study 3…



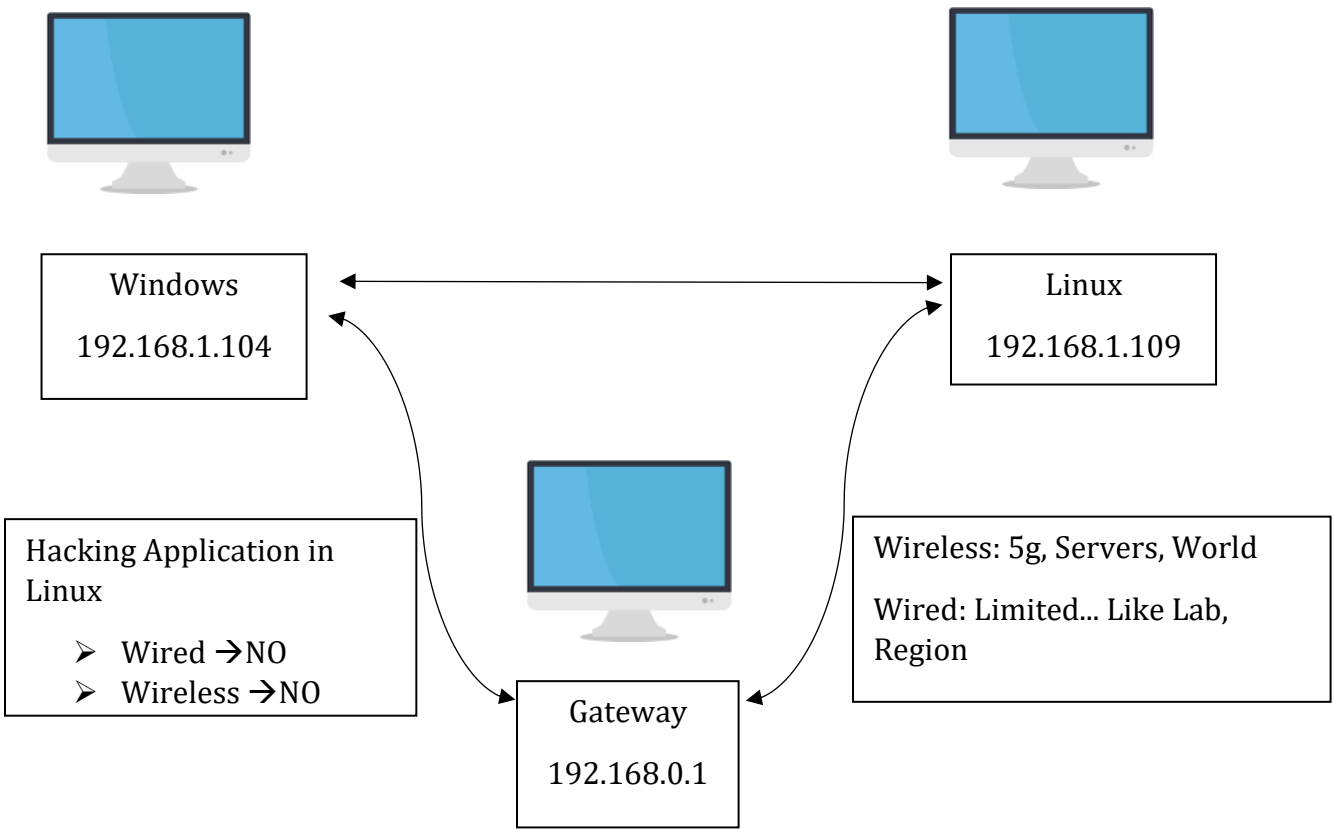


Analysis: -

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:

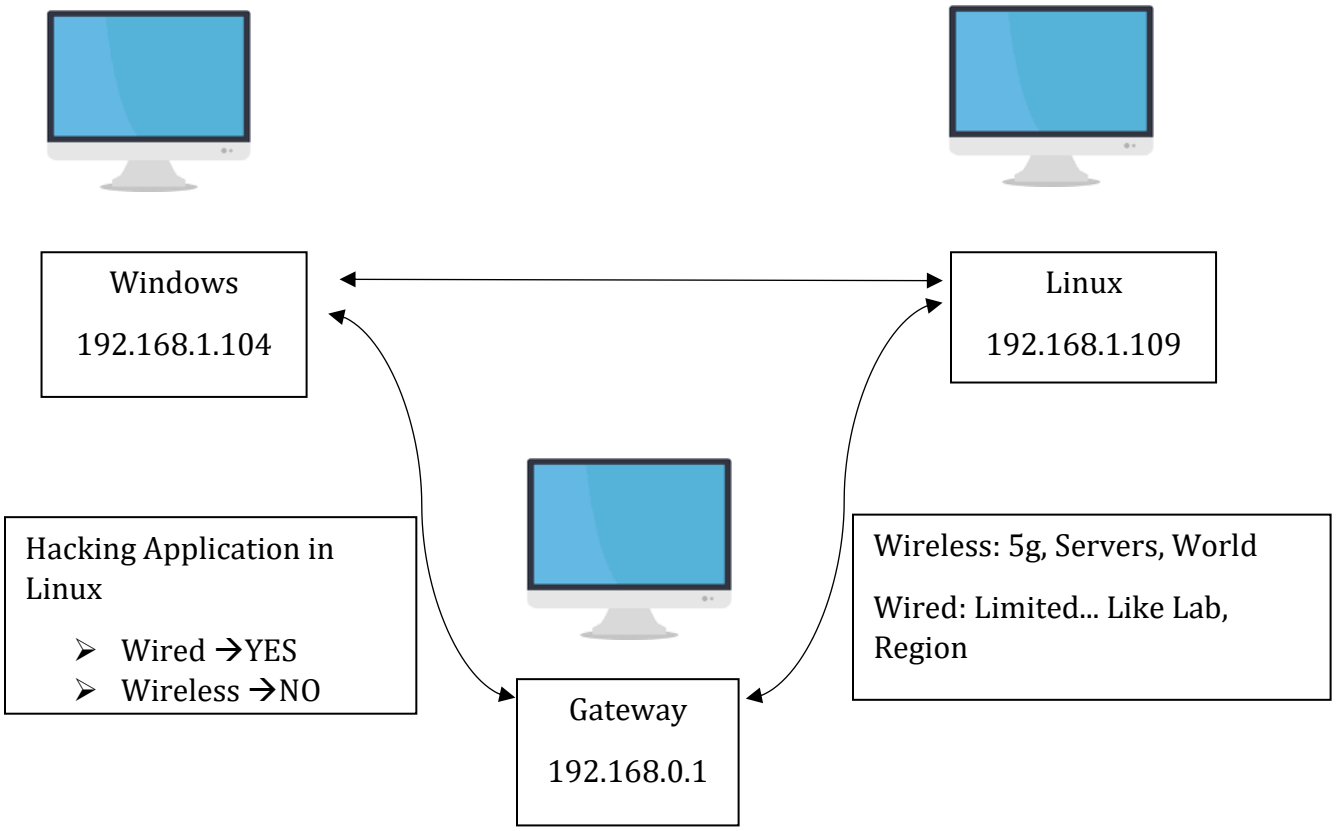
- **Windows → Wireless**
- **Linux → Wired**
  1. Using external adapter
  2. Without using an external adapter
  (Setting connection to Bridged)
- Hacking can't be performed



- **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 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

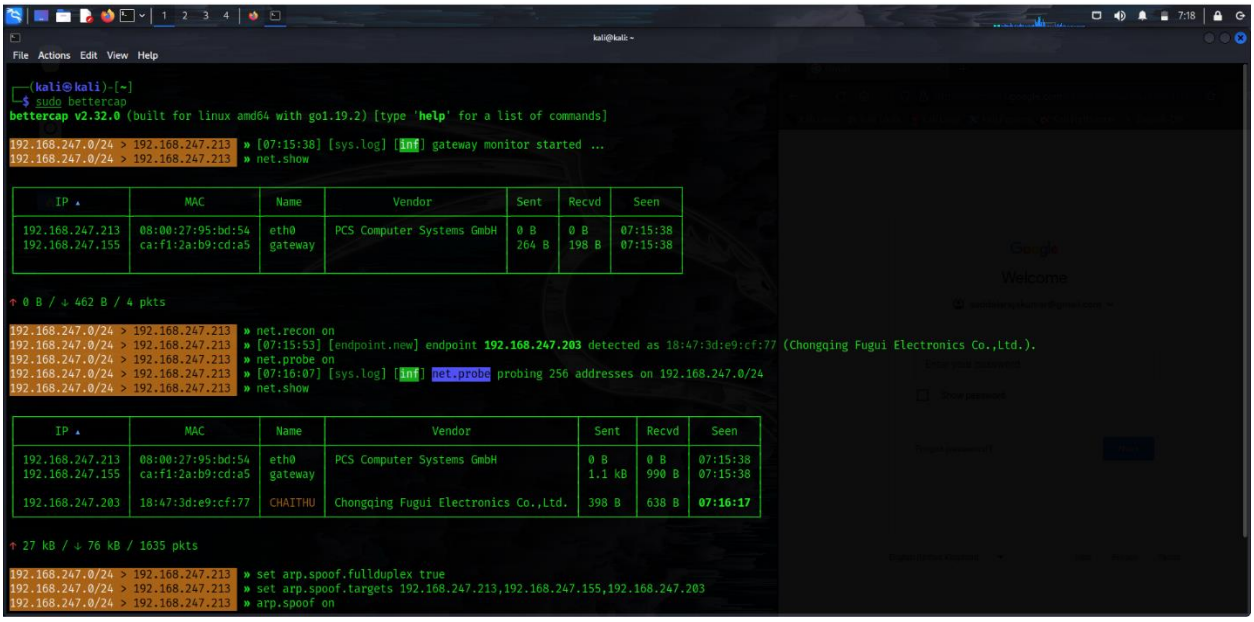


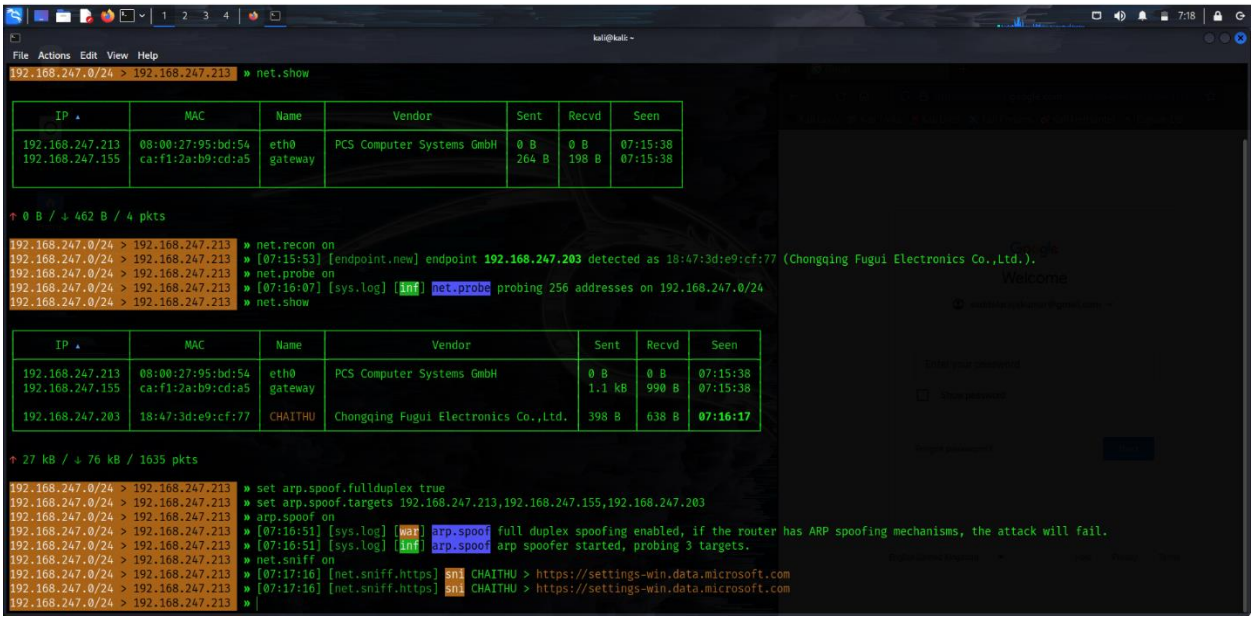
- **10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)**
- **But you can hack Linux-Linux only which is an advanced case study**

Practical Approach for Case Study 6 : -

- Here the practical approach will be on my own network

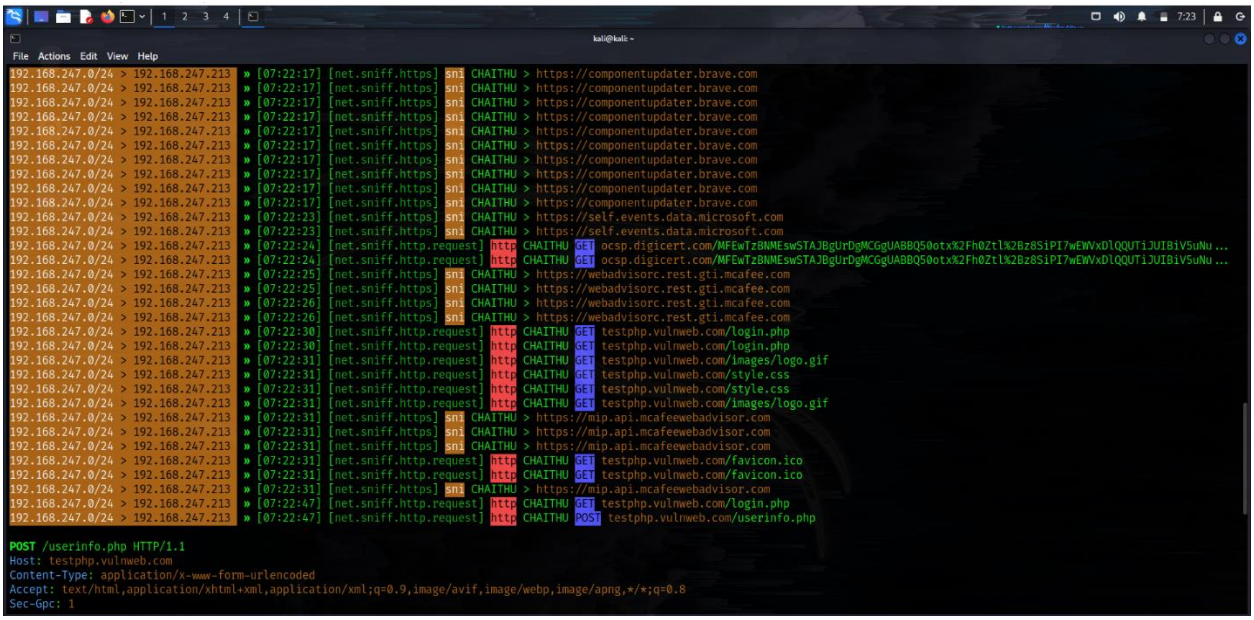
➢ Probing the network and capturing the packets…

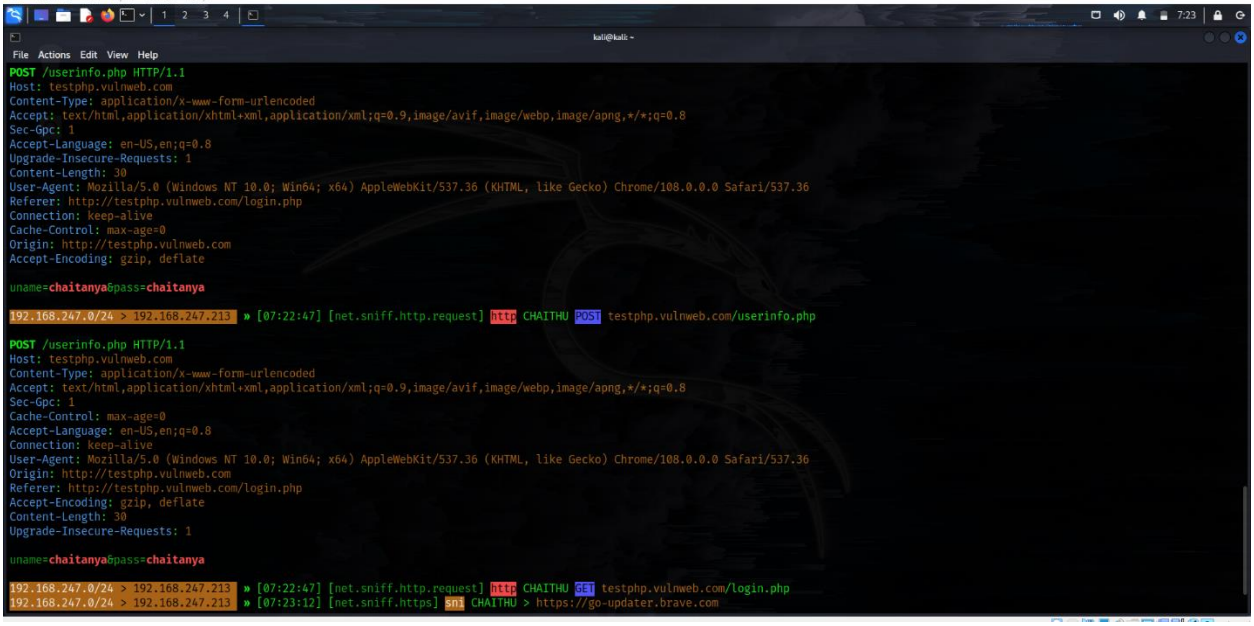




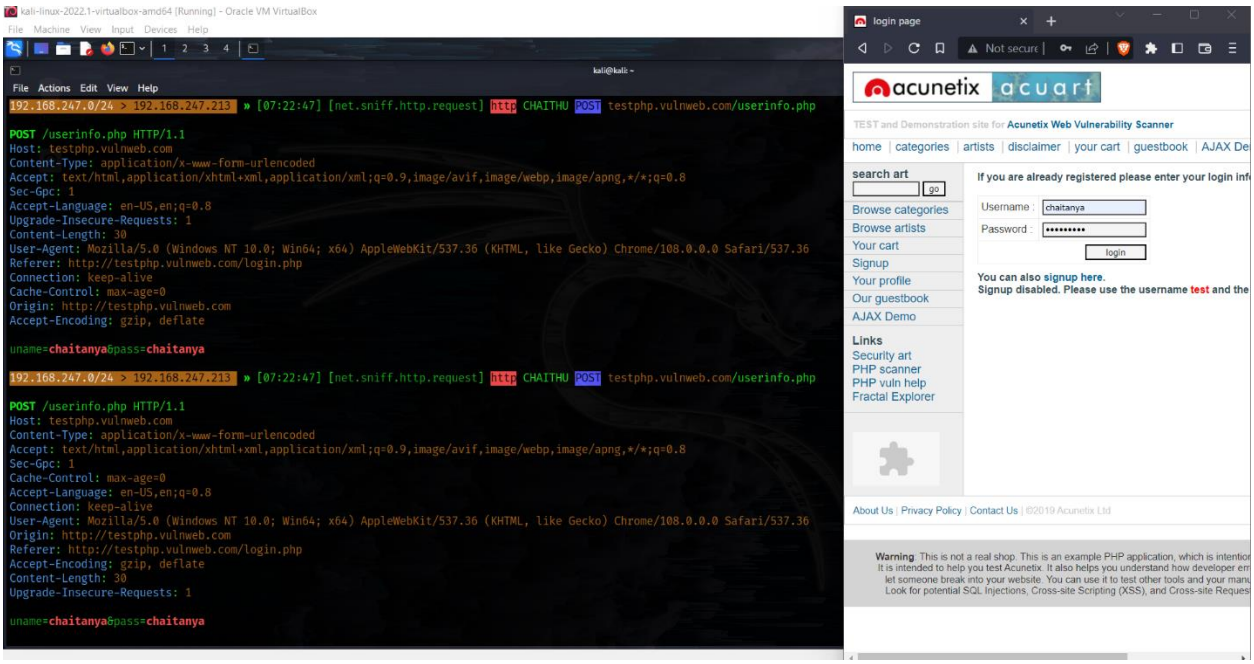
TESTING THE WEBSITES WITH HTTP

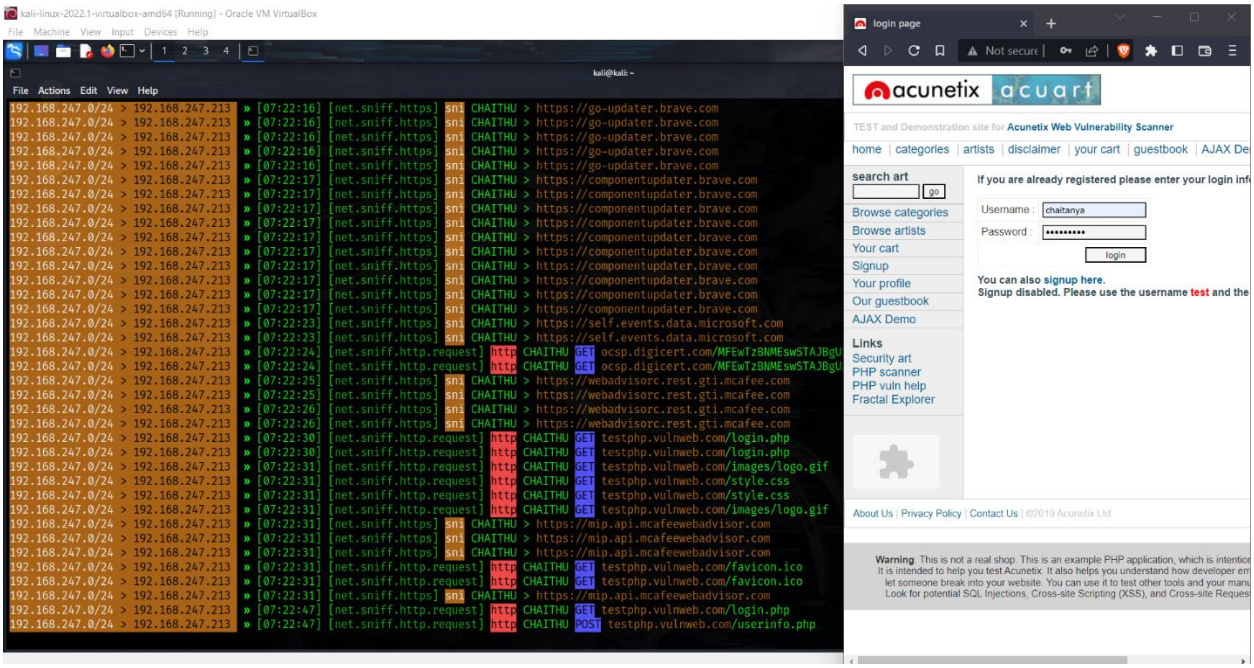
- Testing a http login site

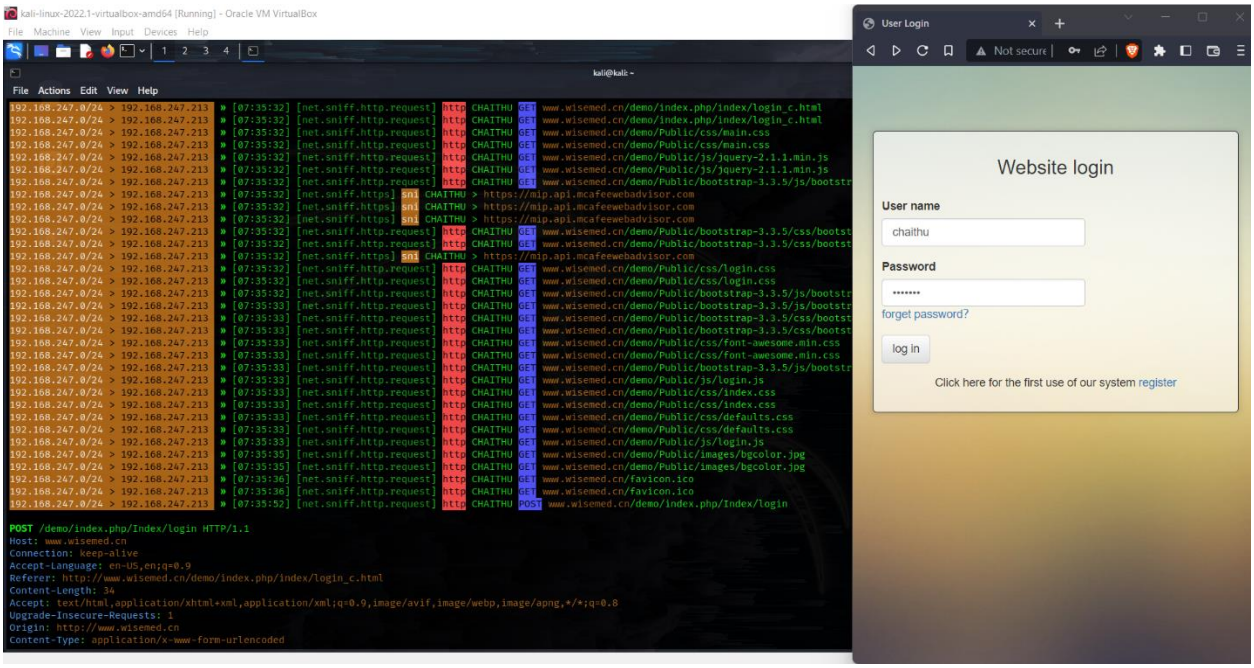


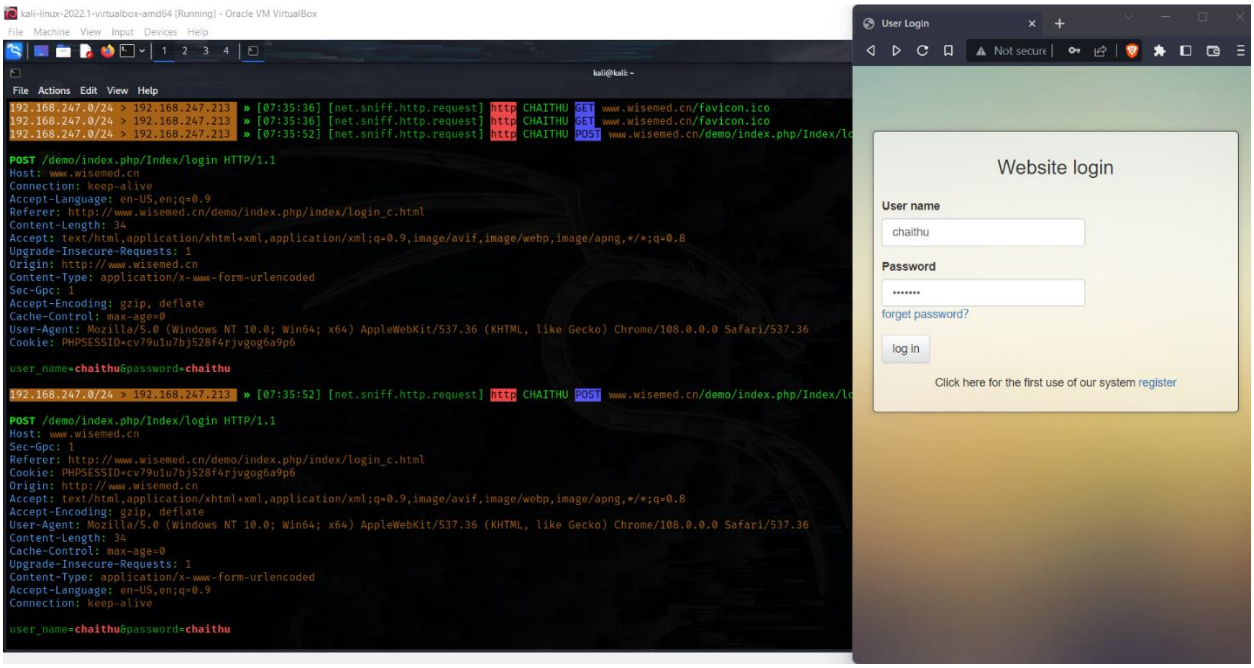


- Testing another http login page…

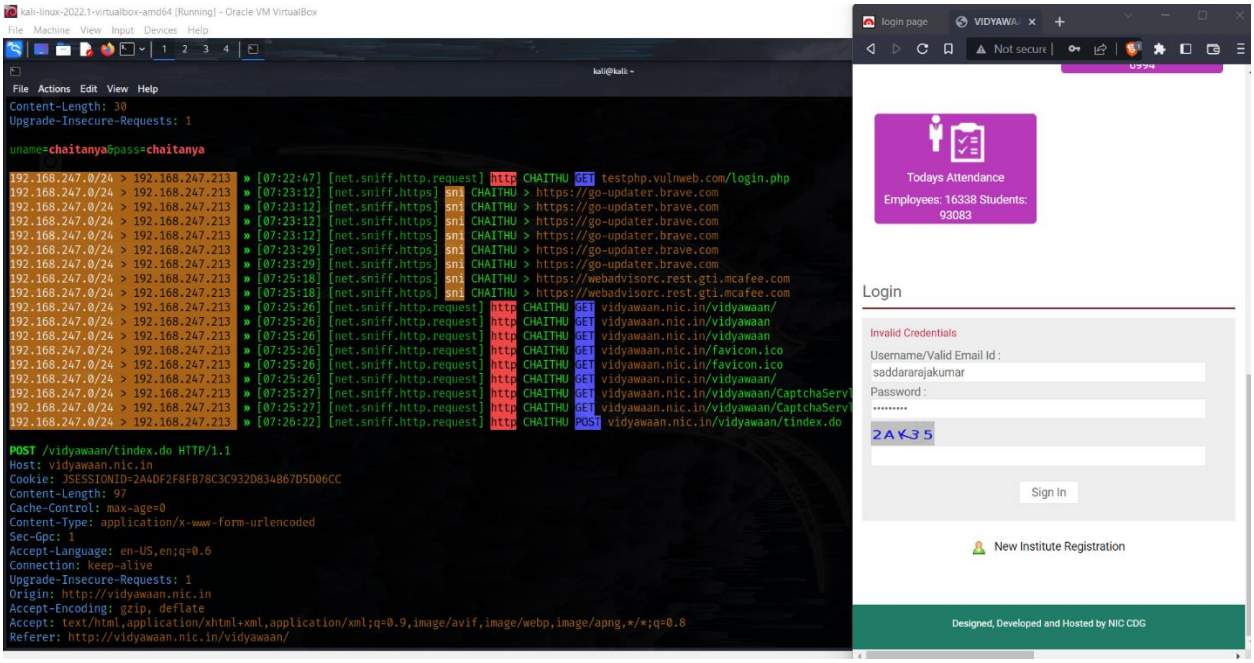


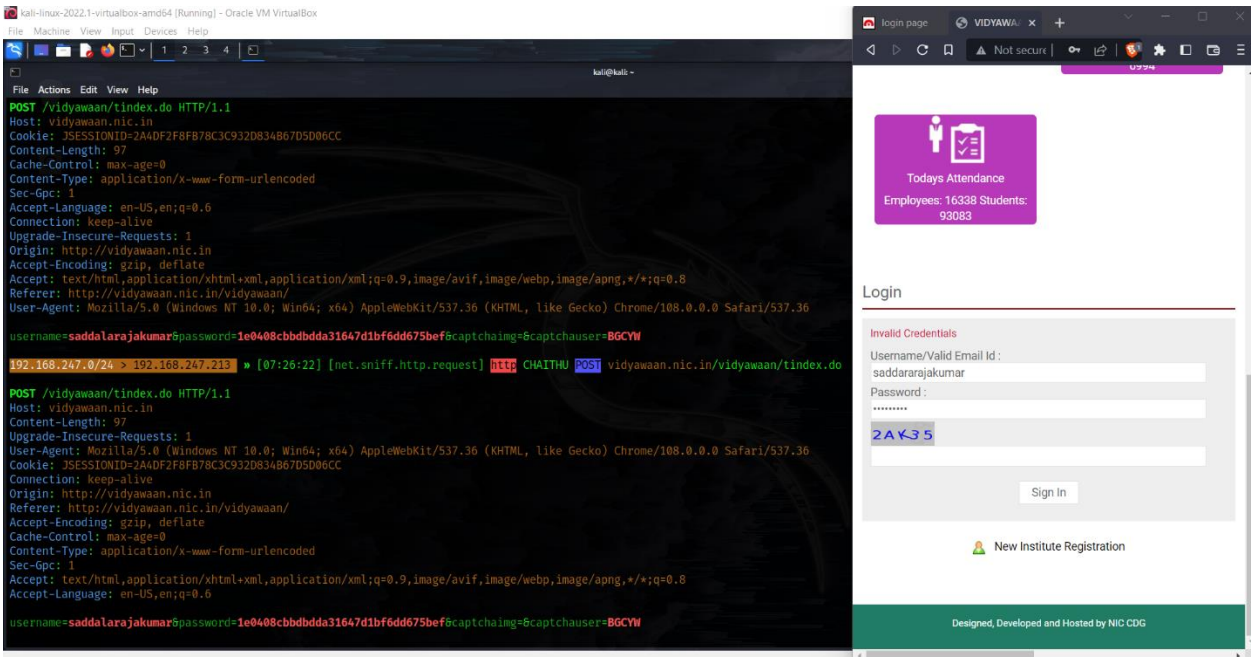



kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/index.php/index/login_c.html
192.168.247.0/24 > 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/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/bootstr
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.https] sni CHAITHU > https://mip.api.mcafeewebadvisor.com
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.https] sni CHAITHU > https://mip.api.mcafeewebadvisor.com
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.https] sni CHAITHU > https://mip.api.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/bootst
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/bootst
192.168.247.0/24 > 192.168.247.213 » [07:35:32] [net.sniff.https] sni CHAITHU > https://mip.api.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/bootstr
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/js/bootstr
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/css/bootst
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/css/bootst
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [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 » [07:35:33] [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 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/bootstrap-3.3.5/js/bootstr
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/js/login.js
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/index.css
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/index.css
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/defaults.css
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/css/defaults.css
192.168.247.0/24 > 192.168.247.213 » [07:35:33] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/js/login.js
192.168.247.0/24 > 192.168.247.213 » [07:35:35] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/images/bgcolor.jpg
192.168.247.0/24 > 192.168.247.213 » [07:35:35] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/demo/Public/images/bgcolor.jpg
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 » [07:35:52] [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-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
User Login
Not secure
Website login
User name
chaithu
Password
forget password?
log in
Click here for the first use of our system register

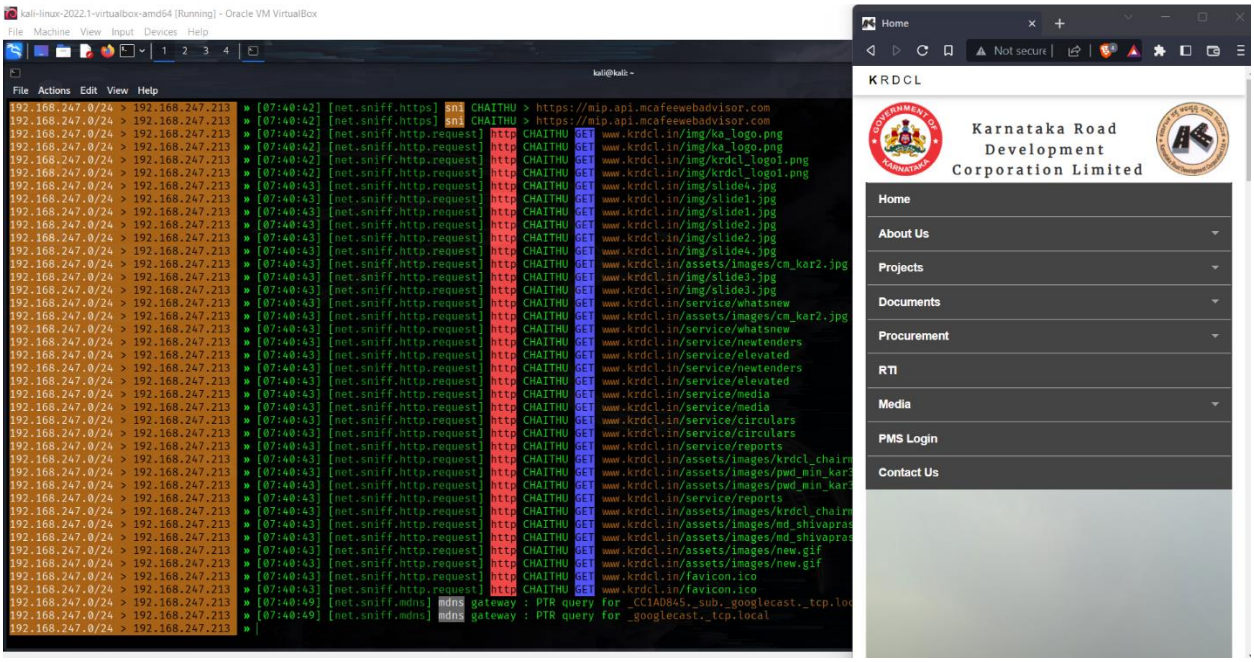

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
192.168.247.0/24 > 192.168.247.213 » [07:35:36] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/favicon.ico
192.168.247.0/24 > 192.168.247.213 » [07:35:36] [net.sniff.http.request] http CHAITHU GET www.wisemed.cn/favicon.ico
192.168.247.0/24 > 192.168.247.213 » [07:35:52] [net.sniff.http.request] http CHAITHU POST www.wisemed.cn/demo/index.php/Index/lo
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
Sec-Gpc: 1
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=cv79u1u7bj528f4rjvgog6a9p6
user_name=chaithu&password=chaithu
192.168.247.0/24 > 192.168.247.213 » [07:35:52] [net.sniff.http.request] http CHAITHU POST www.wisemed.cn/demo/index.php/Index/lo
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=cv79u1u7bj528f4rjvgog6a9p6
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

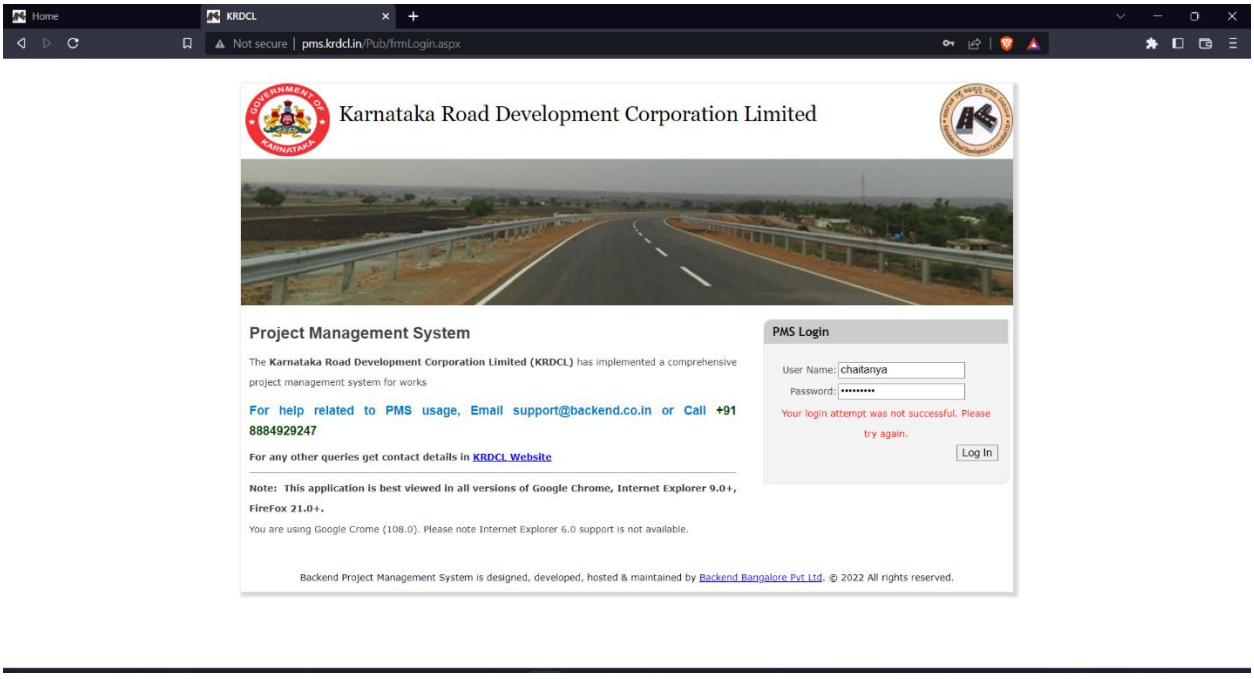
- Testing a government site called **VIDYAWAAN**...

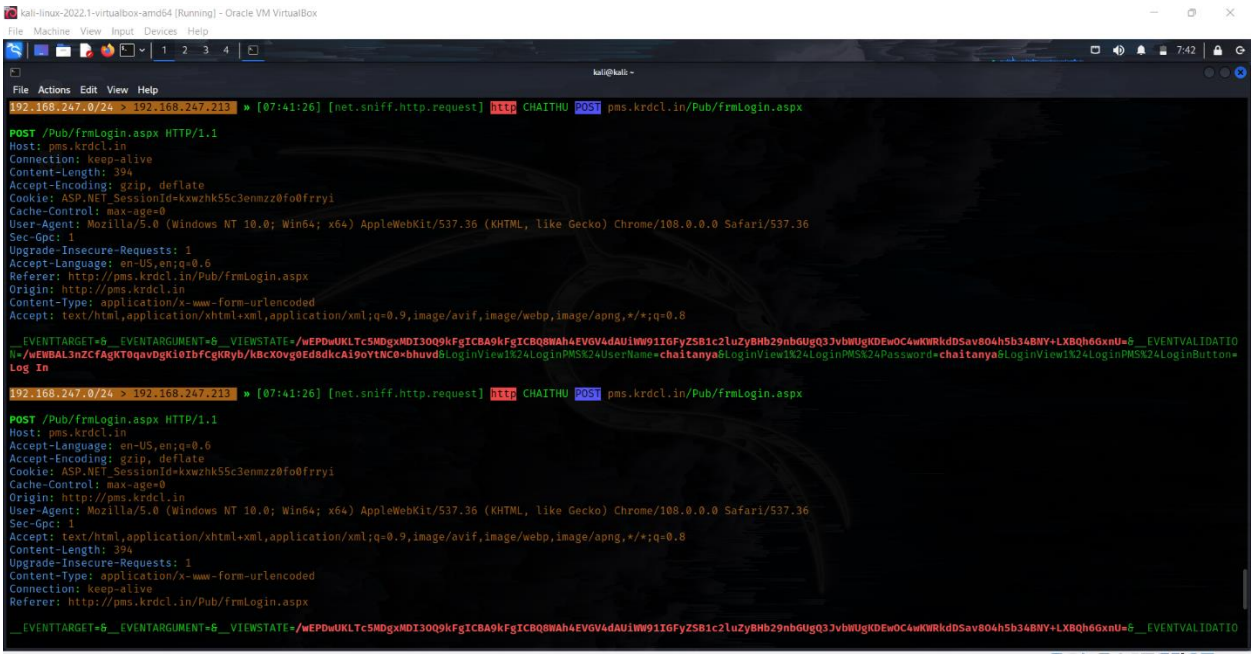




- Testing another government site called Karnataka Road Development Corporation Limited, which belongs to The Government of Karnataka…







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.

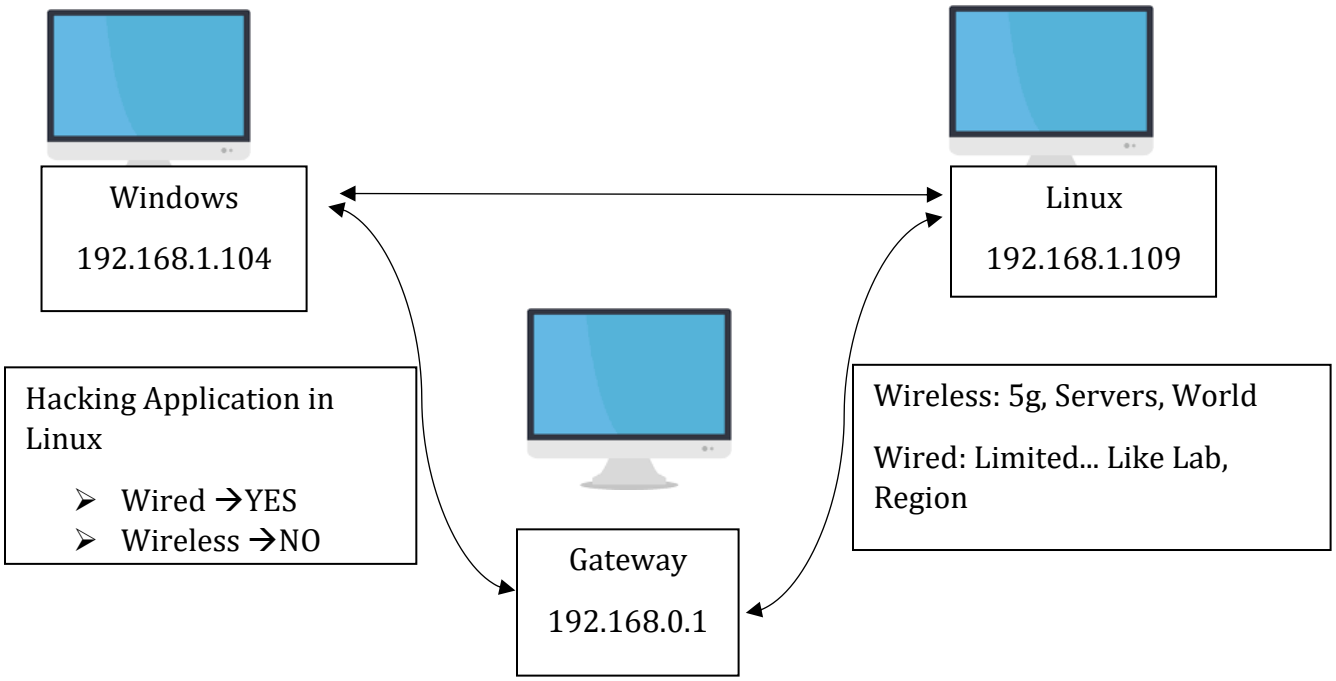
So that we can easily hack the sites which uses http instead of https…

CASE 11:

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

NOTE: -

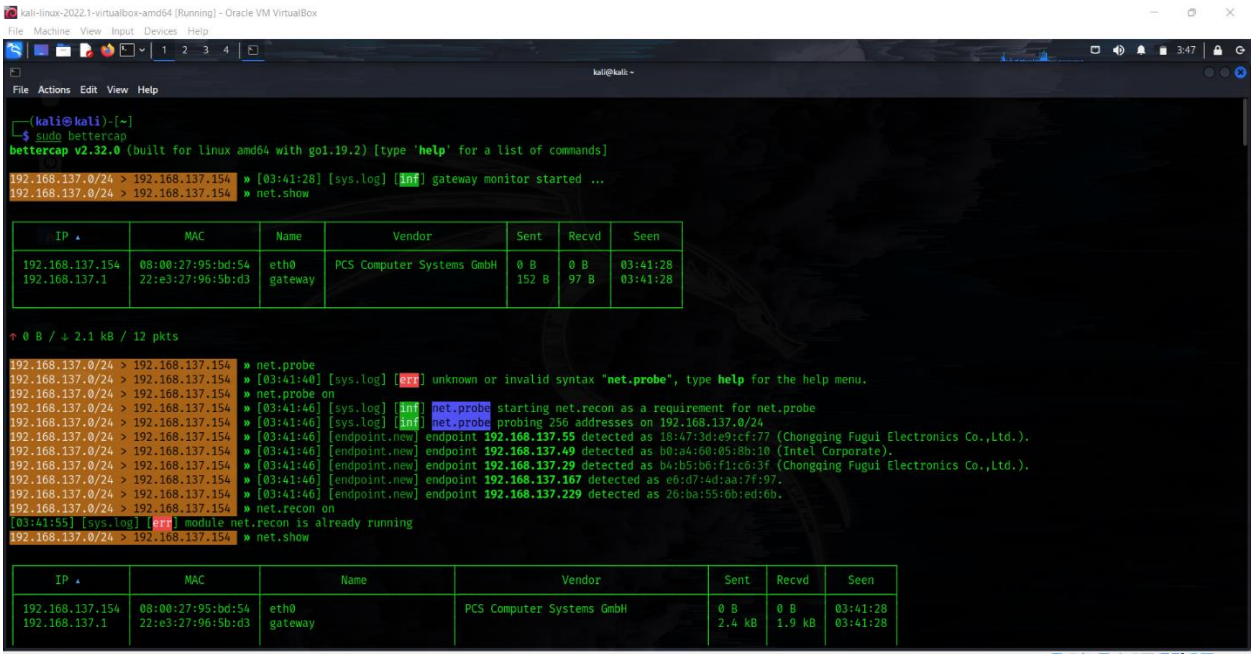
Here in this case study, we can hack windows with Linux without using External Adapter

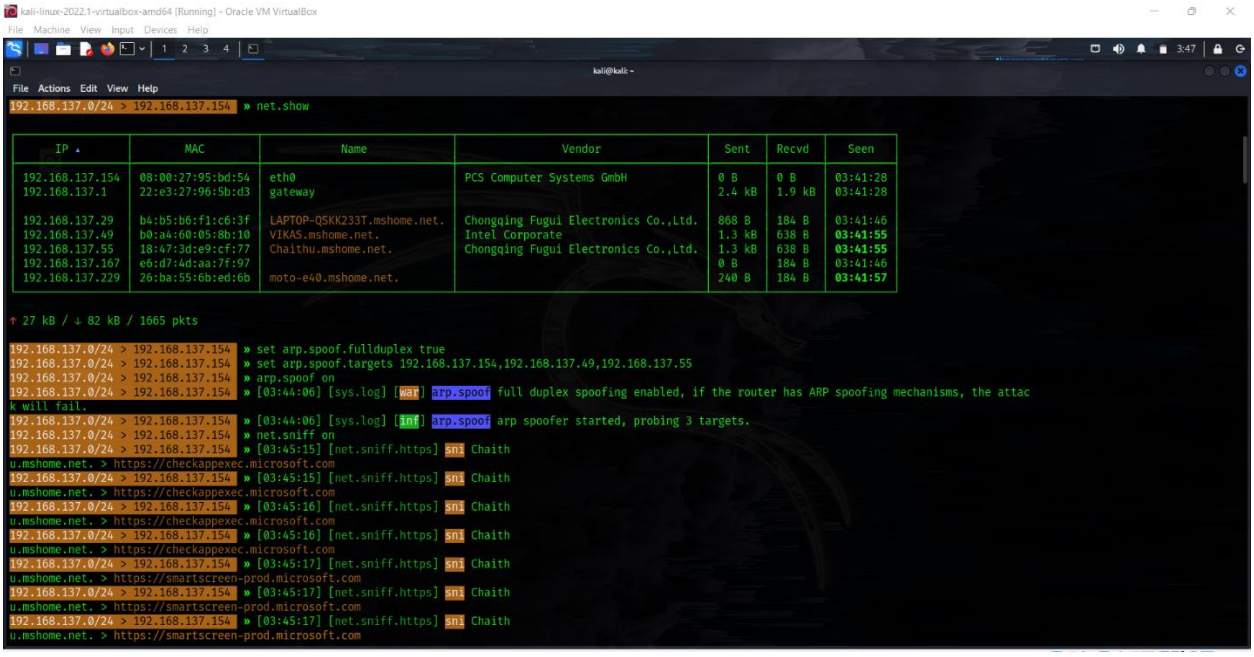


- **10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)**
- **But you can hack Linux-Linux only which is an advanced case study**

Practical Approach for Case Study 11 : -

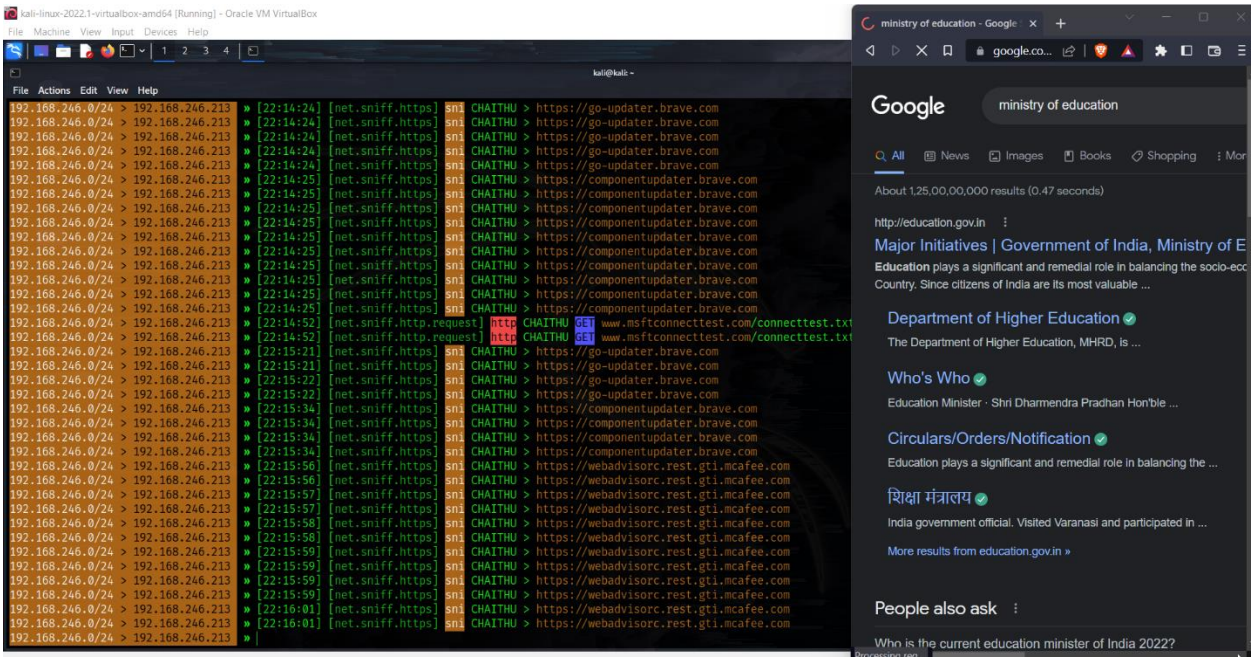
- **Probing the network and capturing the packets…**



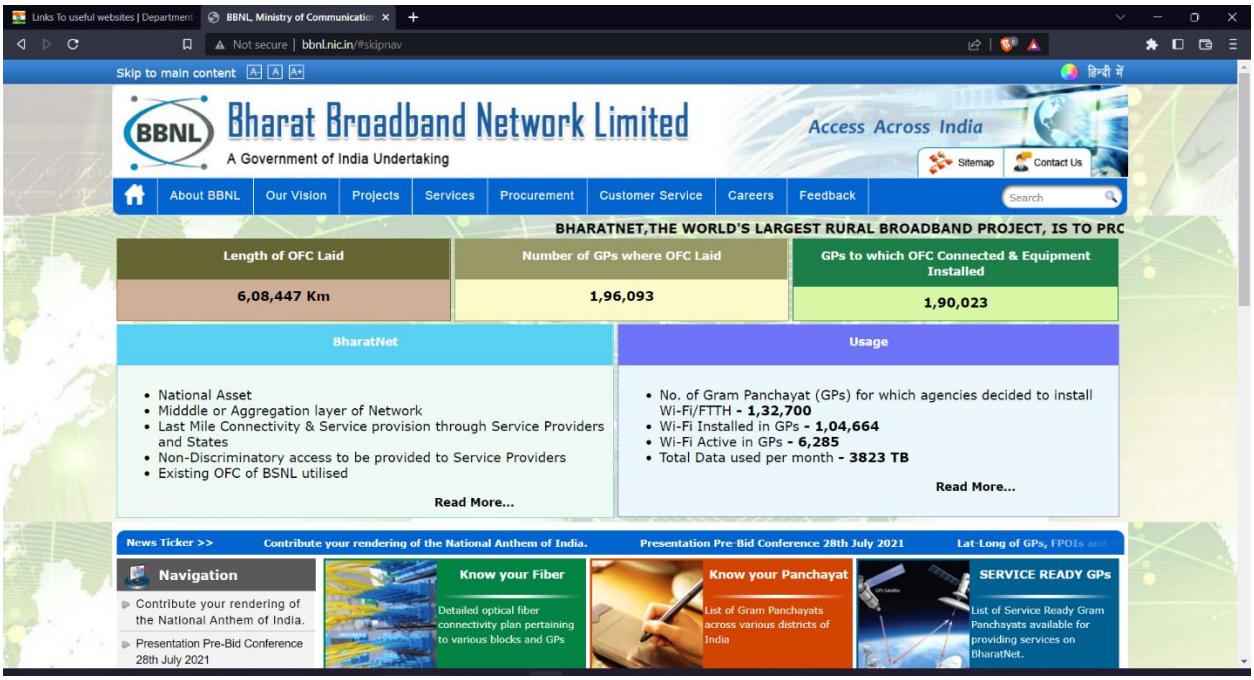


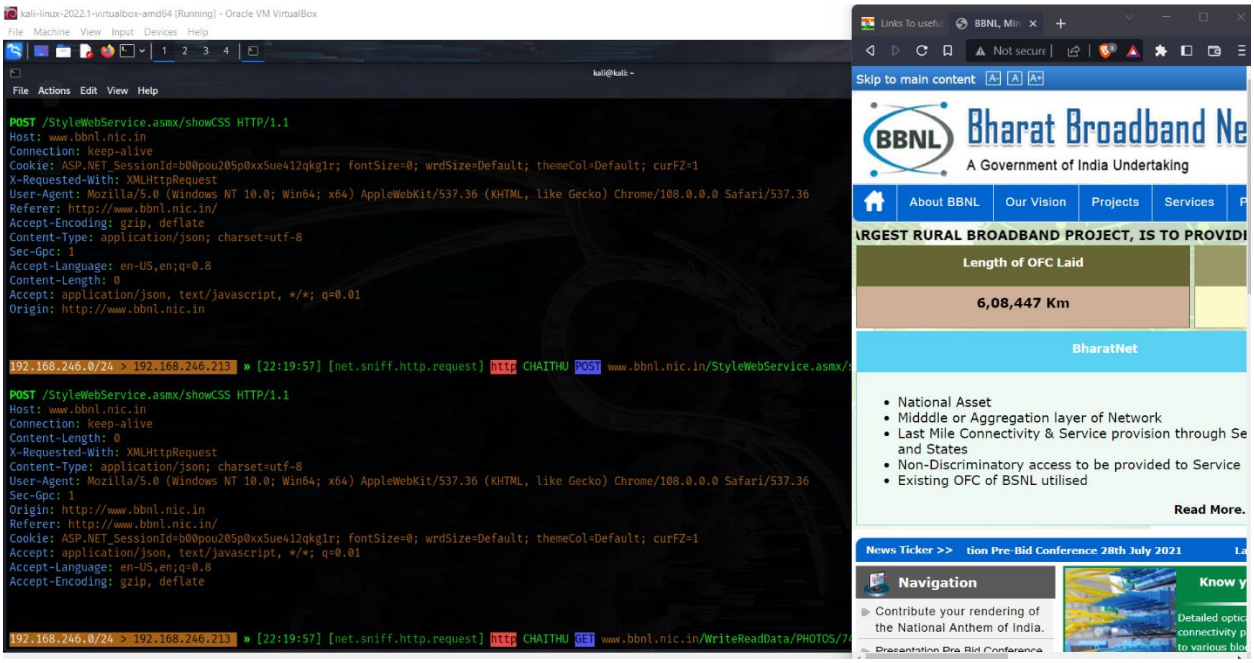
TESTING THE WEBSITES WITH HTTP

- Testing a http site which belongs to the government…



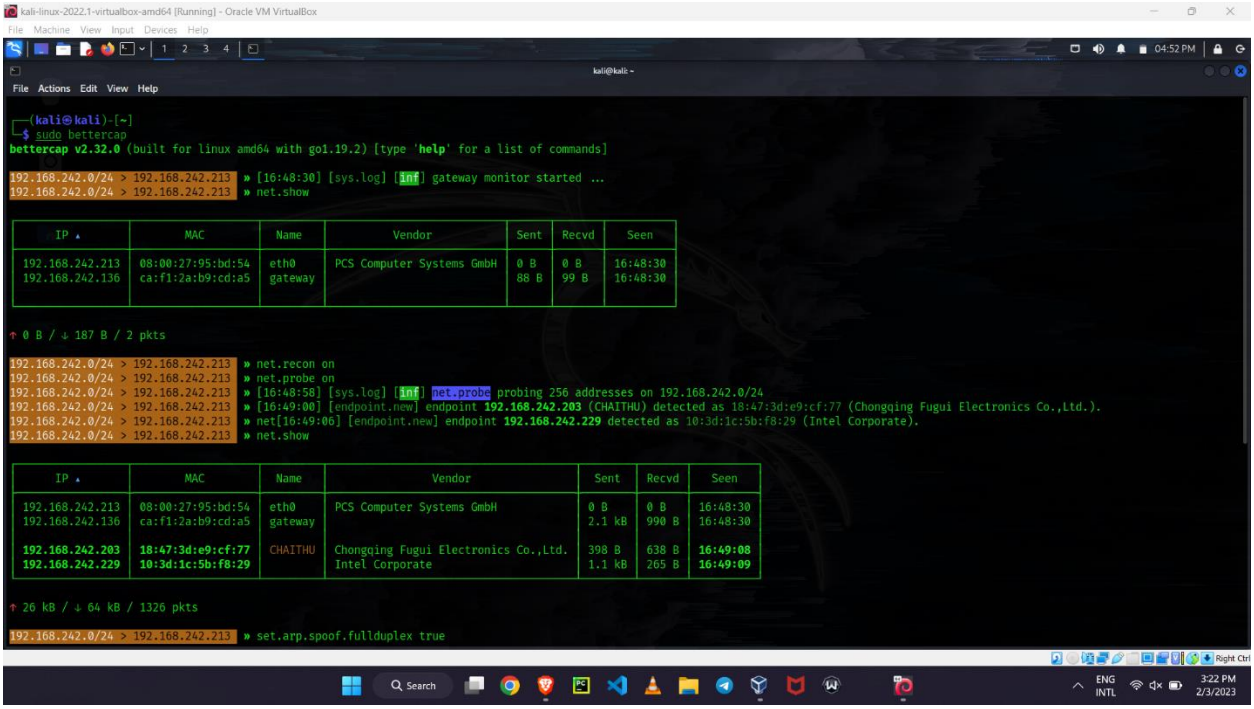
- Testing another website called BBNL(Bharat Broadband Network Limited)

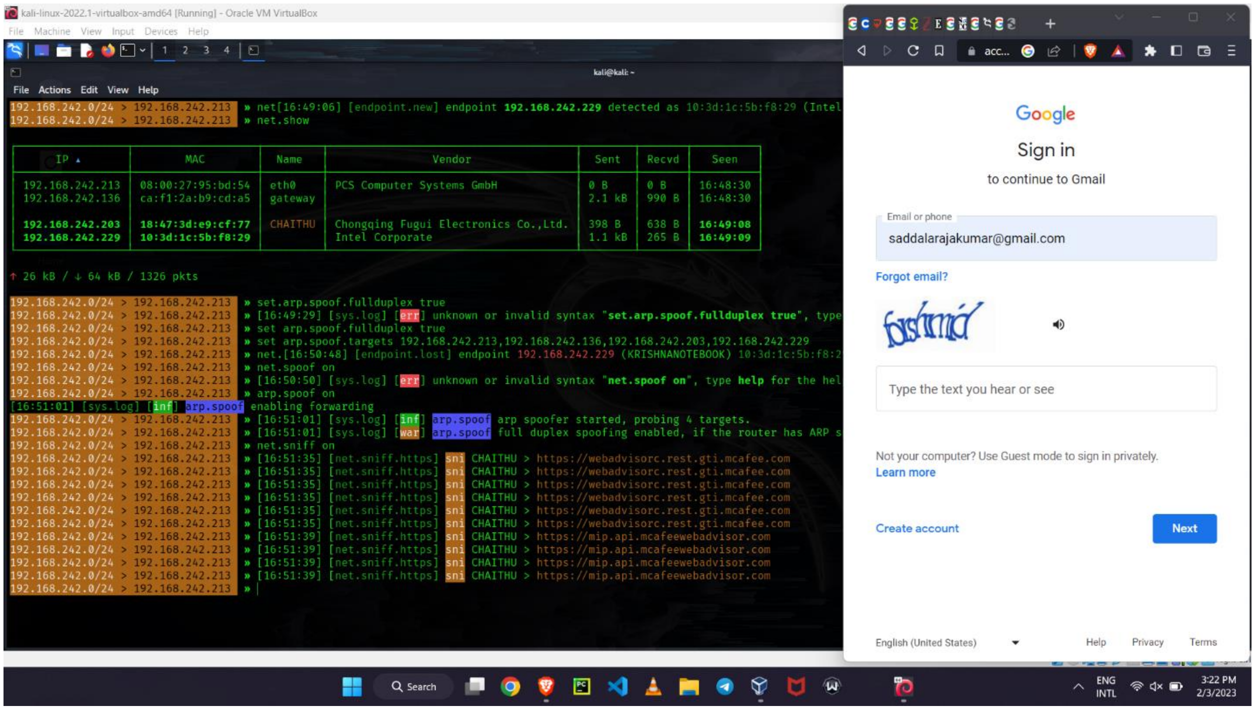




TESTING THE WEBSITES WITH HTTPS

- Testing a famous website Gmail





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.

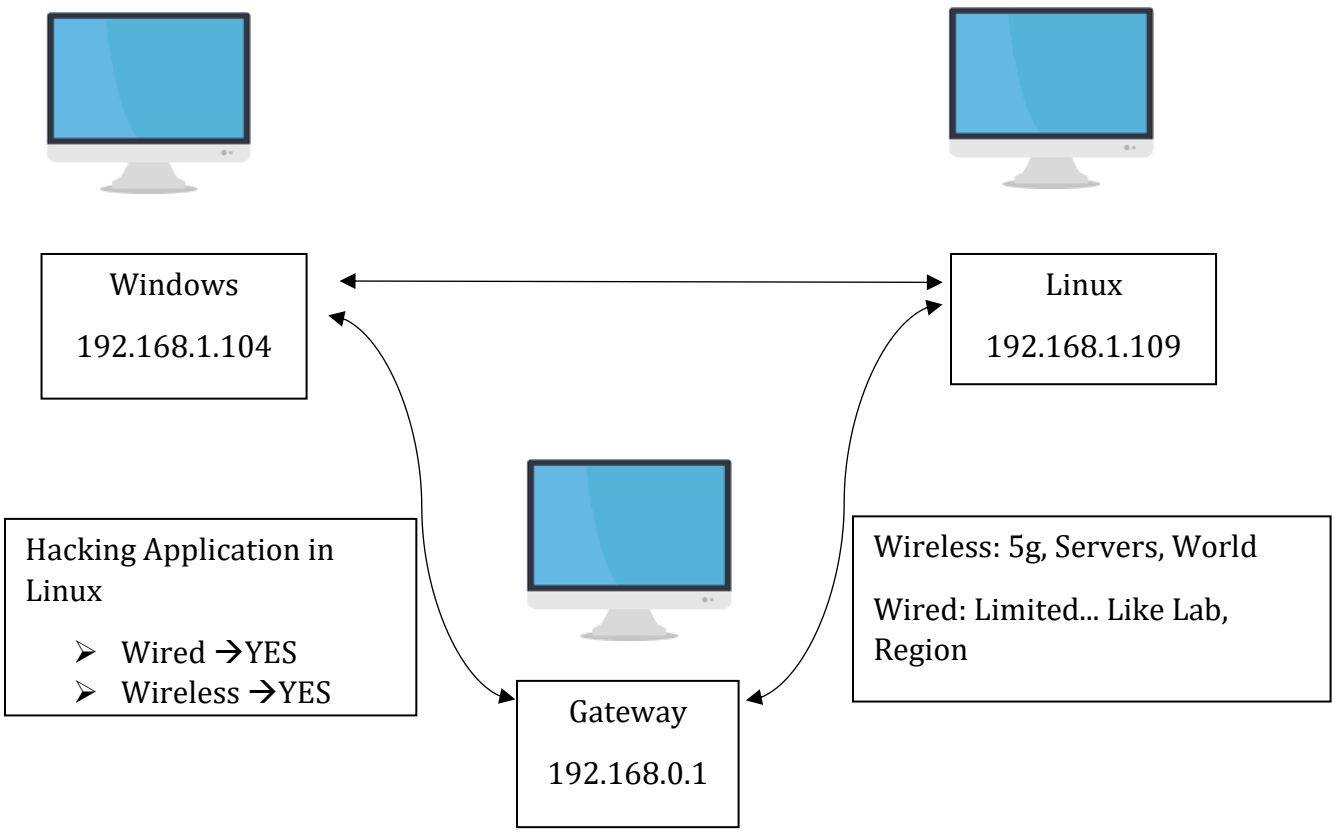
When we come to the Gmail which uses https, so the security is relatively high when compared to the sites with http. We can observe that the data is encrypted, no sensitive data is displayed even when we log into that website.

SPECIAL CASE STUDIES

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

CASE 7:

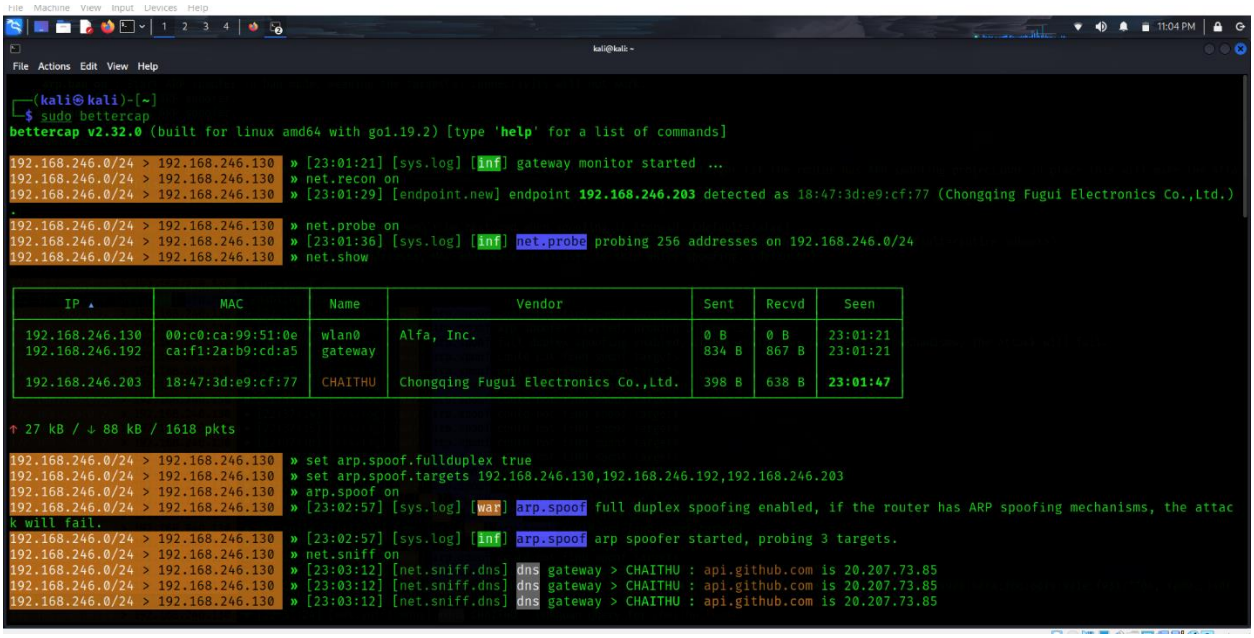
- **Windows → Wireless**
- **Linux → Wireless**
- Without change in network adapter(NAT)
- By using the Wi-fi Adapter(Alfa Adapter)
- Hacking can be performed

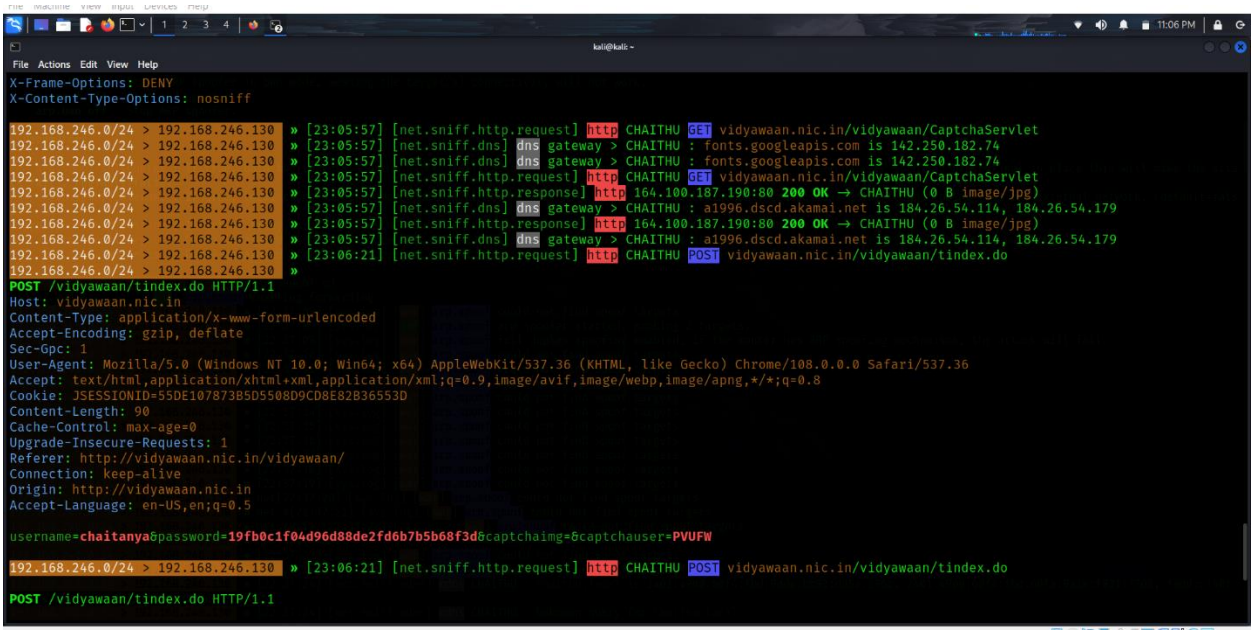


- **10.0.2.15 → No Hacking can be done outside Linux(Wired, Wireless)**
- **But you can hack Linux-Linux only which is an advanced case study**

Practical Approach for Case Study 7: -

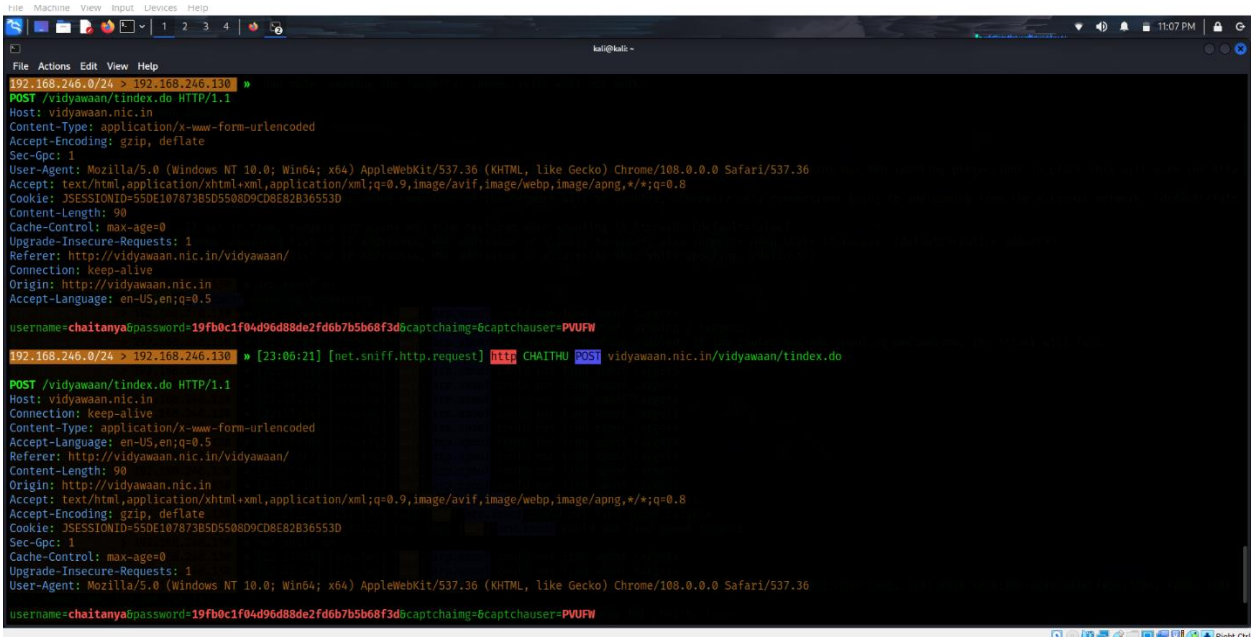
- **Probing the network and capturing the packets**



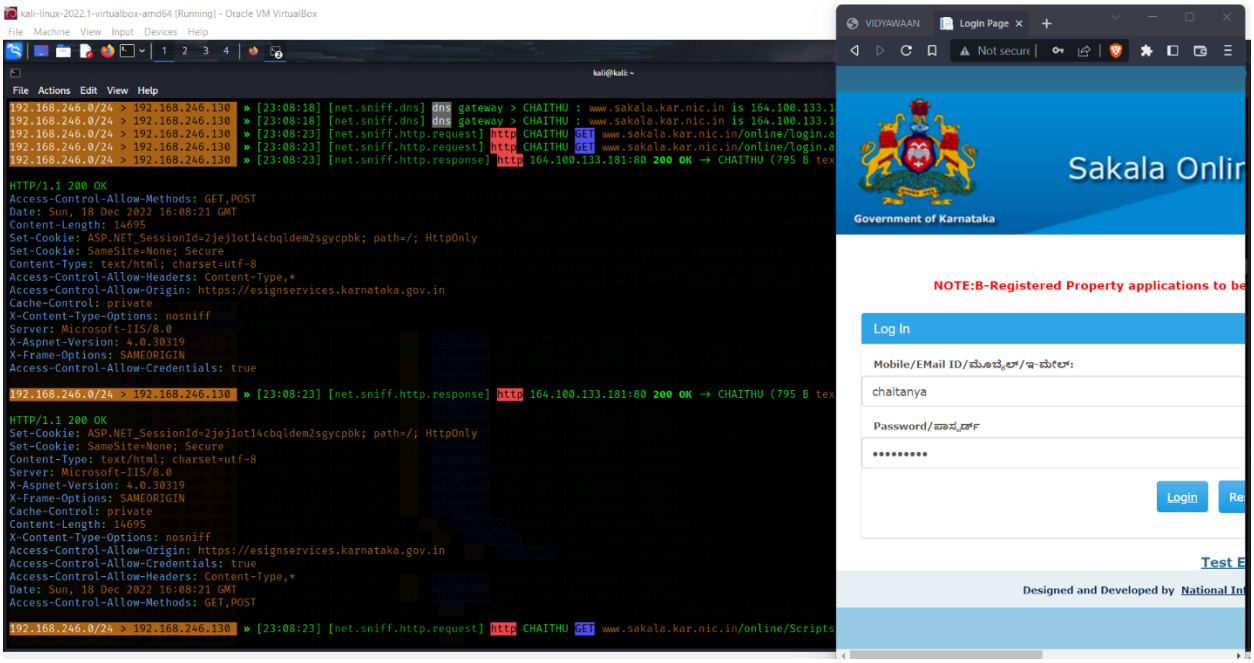


TESTING THE WEBSITES WITH HTTP

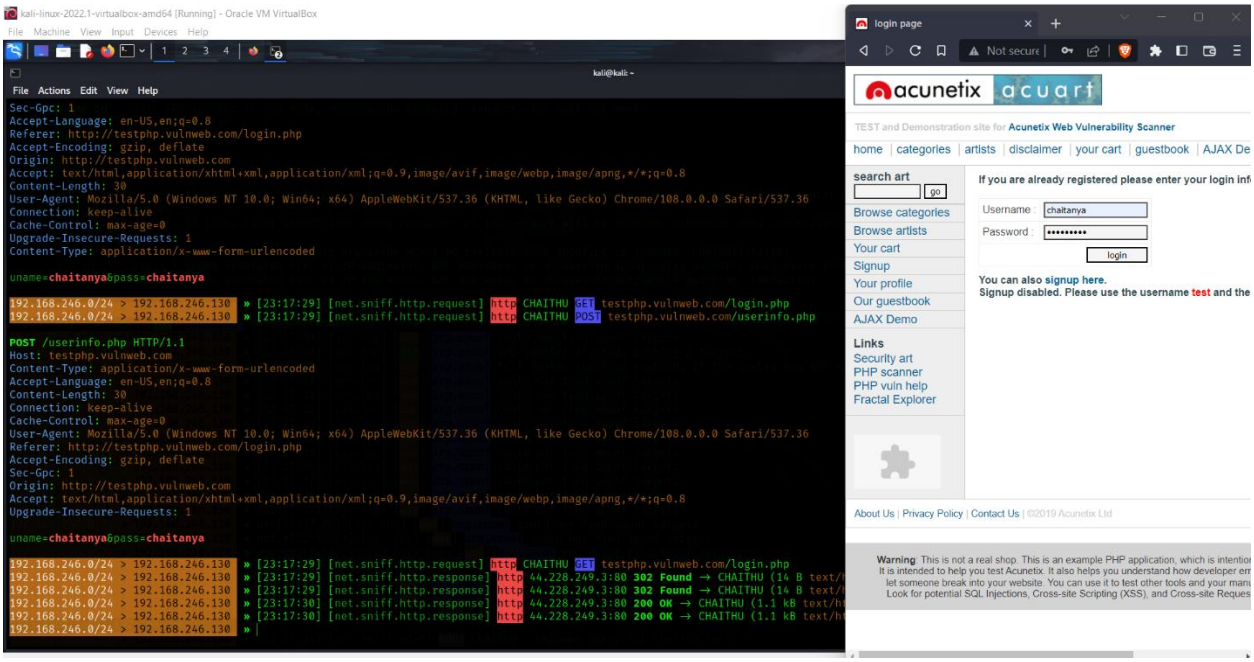
- Testing the government site called VIDYAWAAN

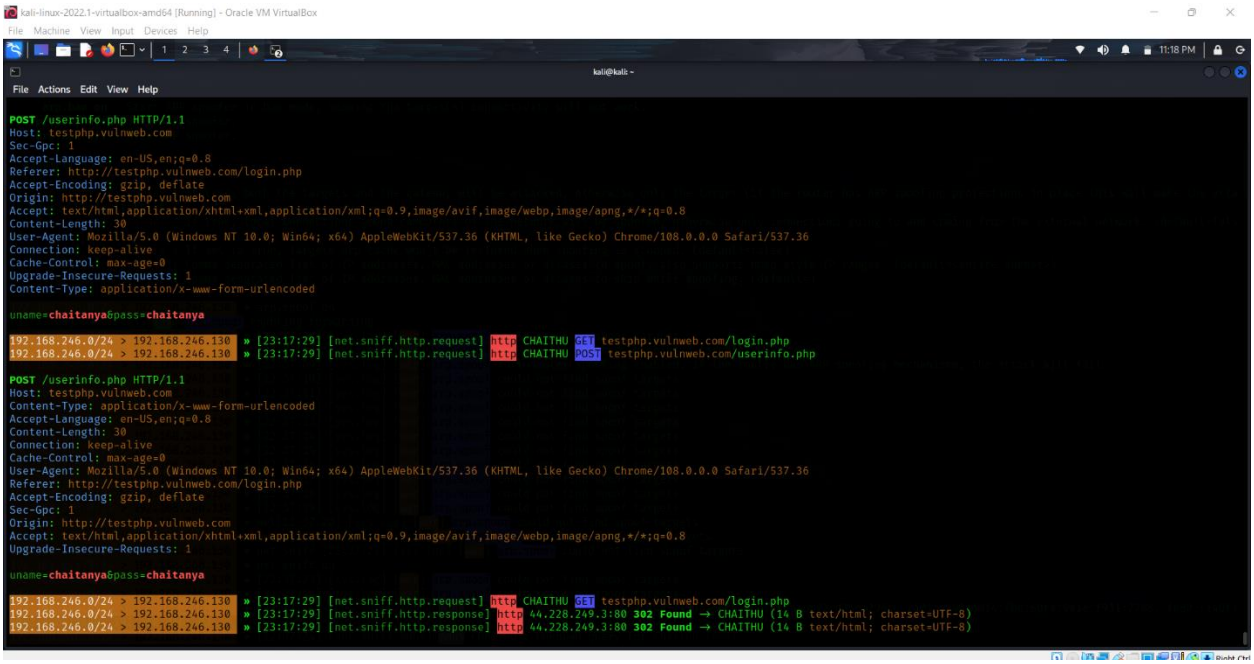


- Testing a website belongs to the government of **KARNATAKA**



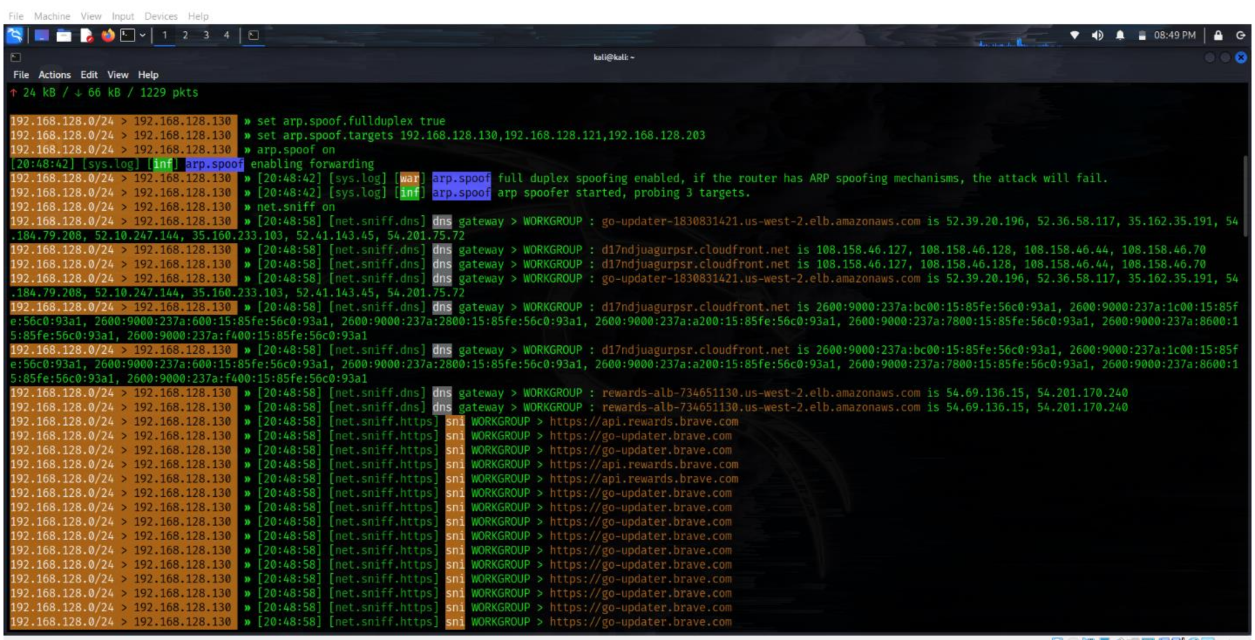
- Testing another http login page

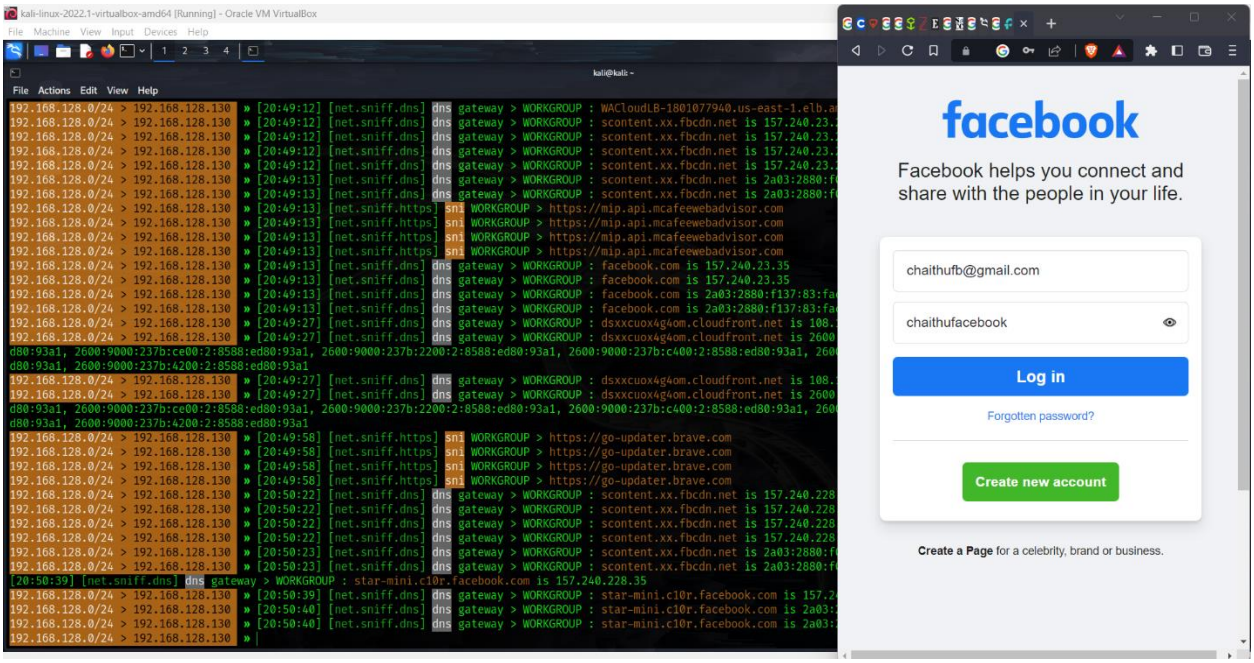


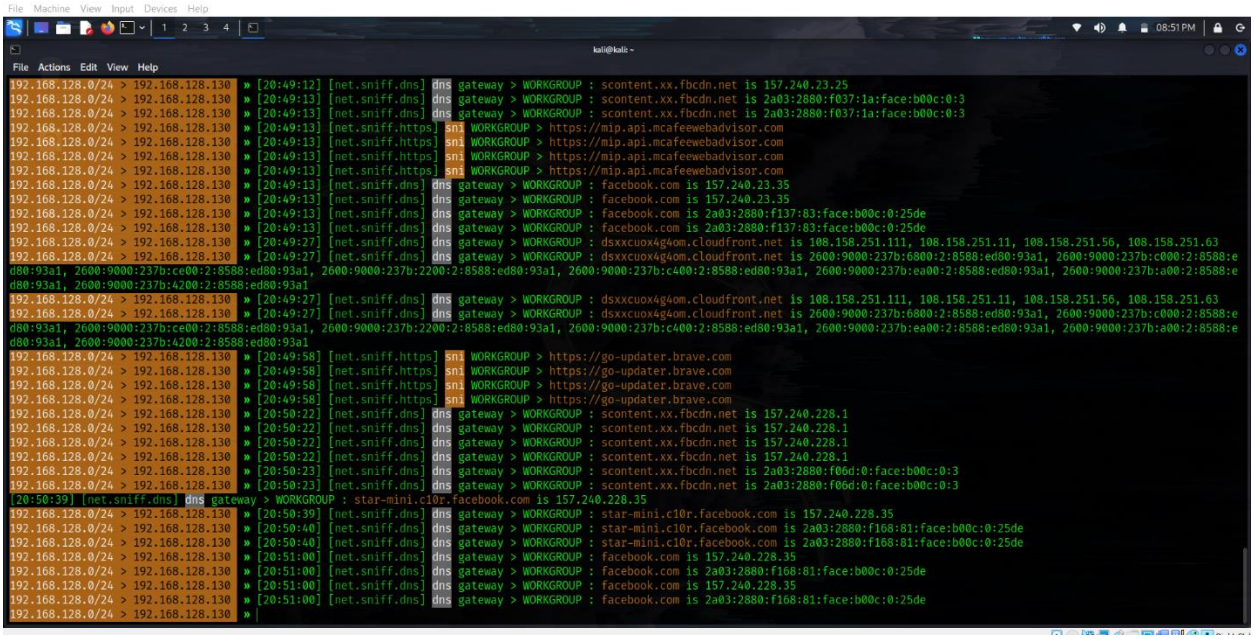


TESTING THE WEBSITE WITH HTTPS

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







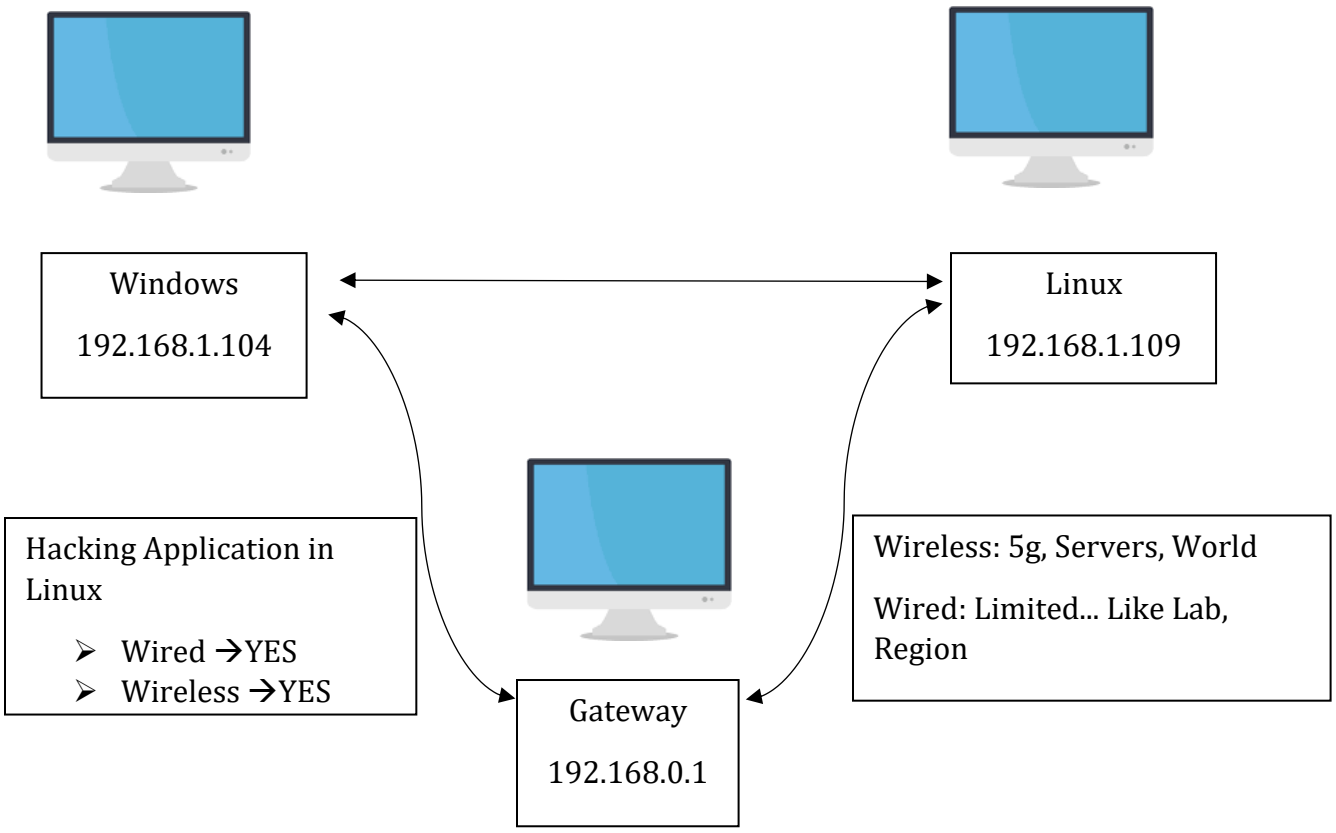
Analysis: -

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.

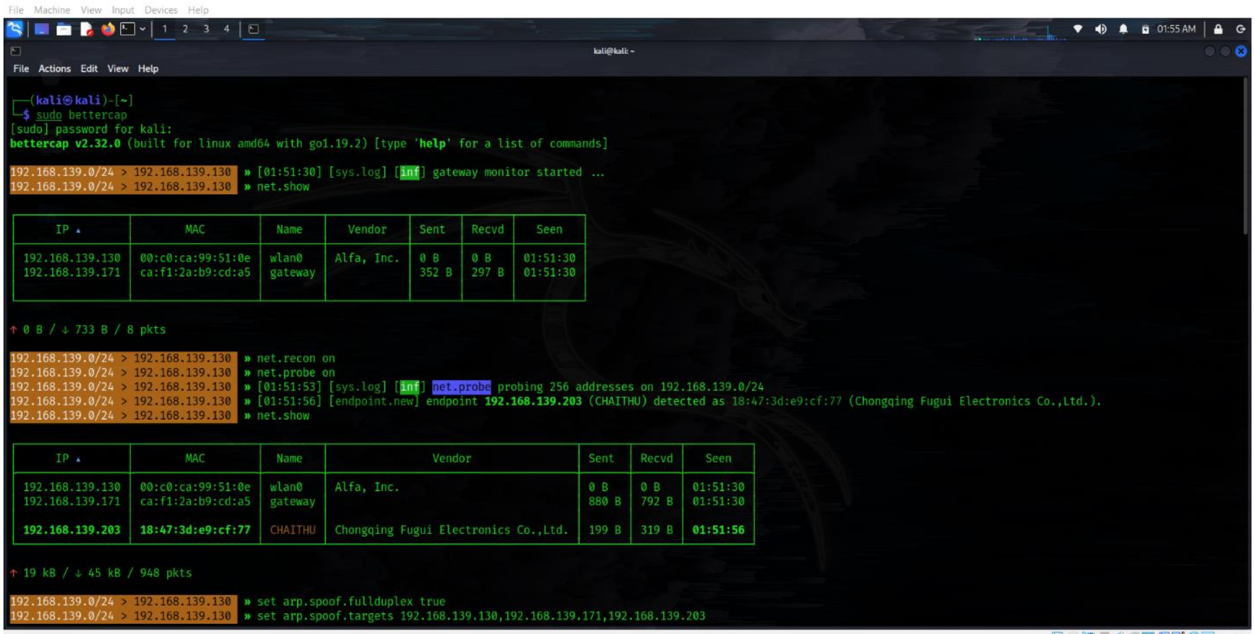
CASE 8:

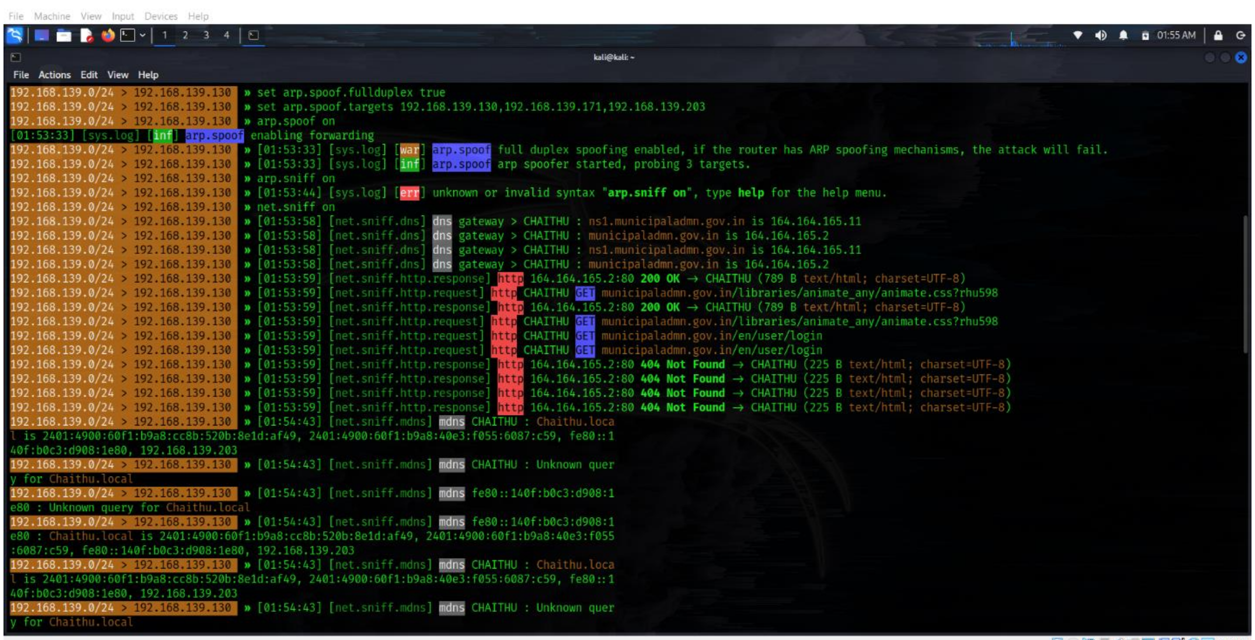
- **Windows → Wireless**
- **Linux → Wireless**
- With change in Configuration to Bridged
- By using the Wi-fi Adapter(Alfa Adapter)
- Hacking can be performed



- **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**

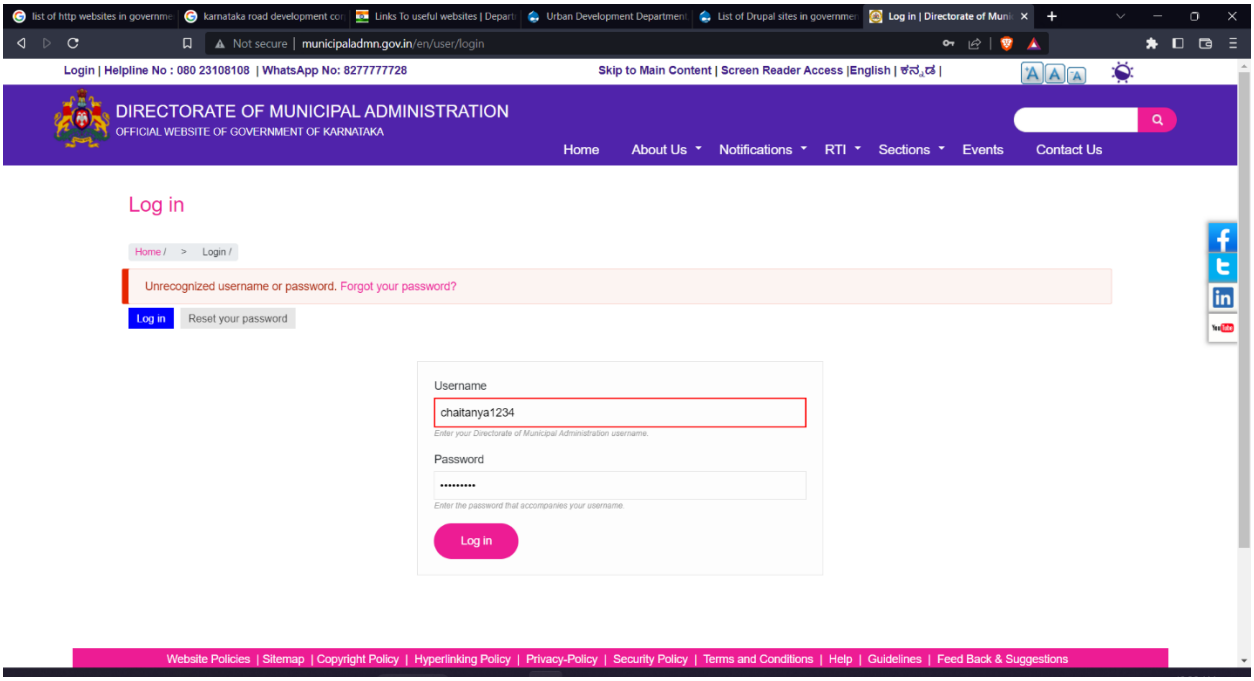
➢ **Probing the network and capturing the packets**

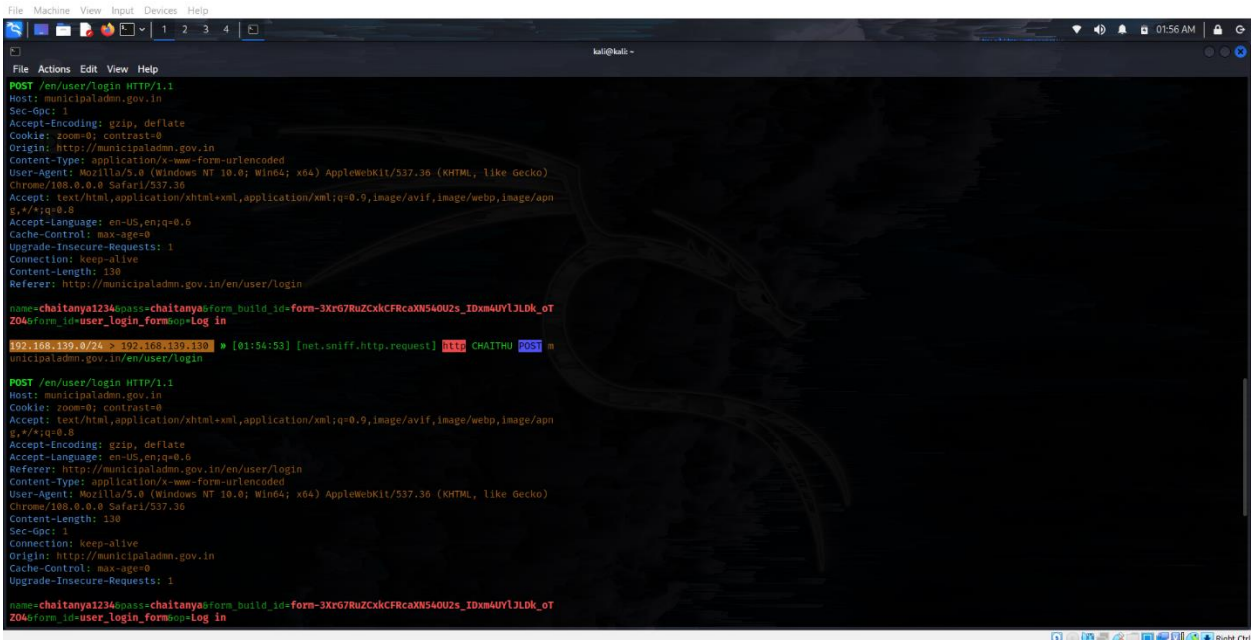


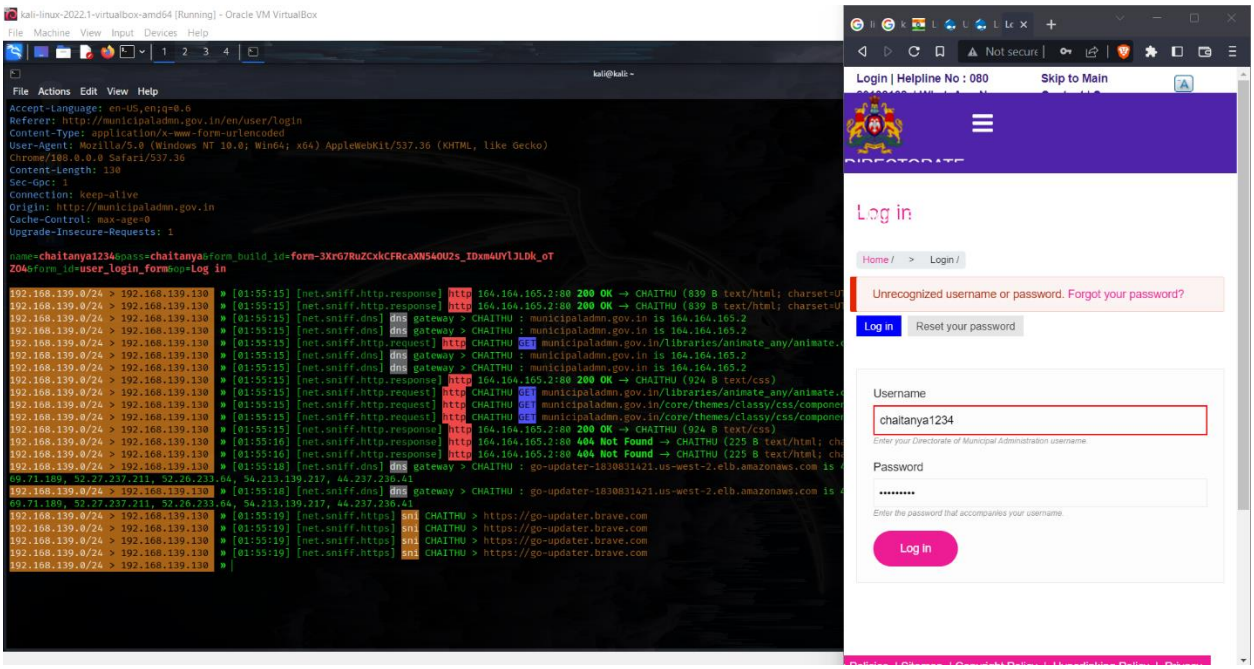


TESTING THE WEBSITES WITH HTTP

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

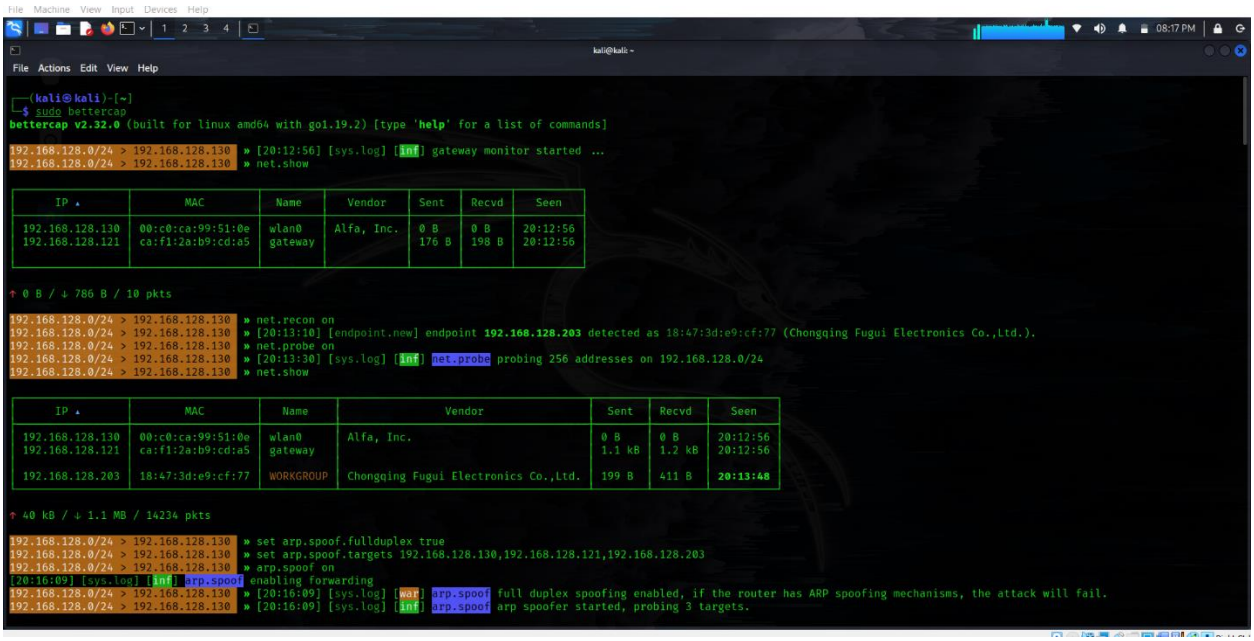


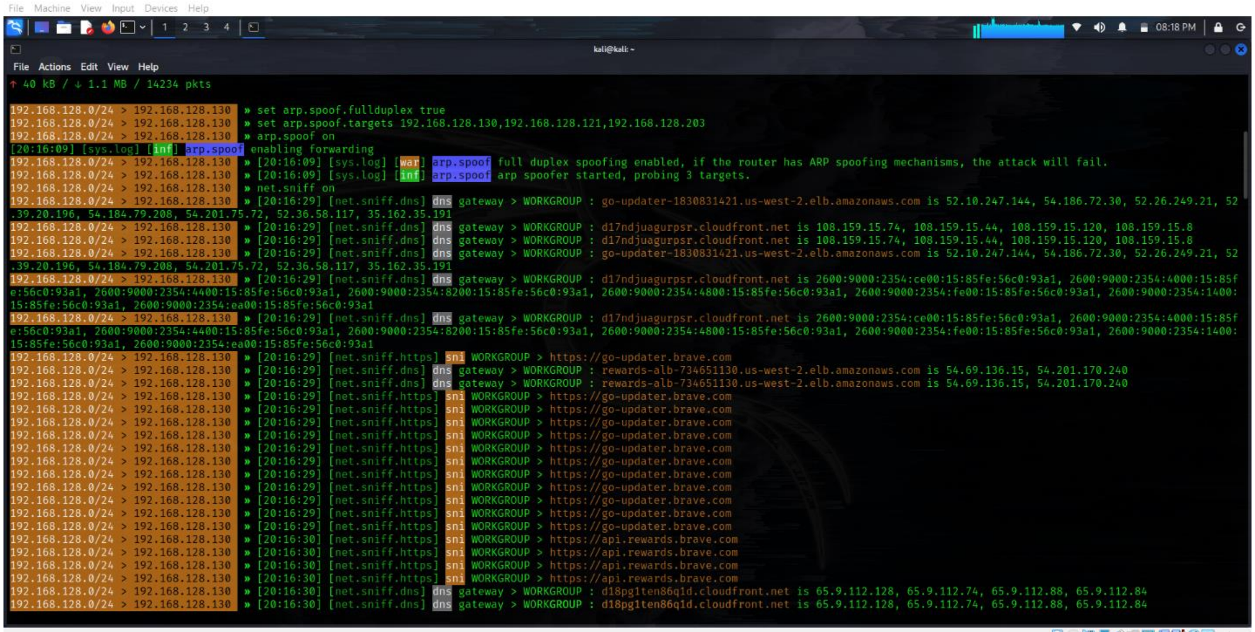


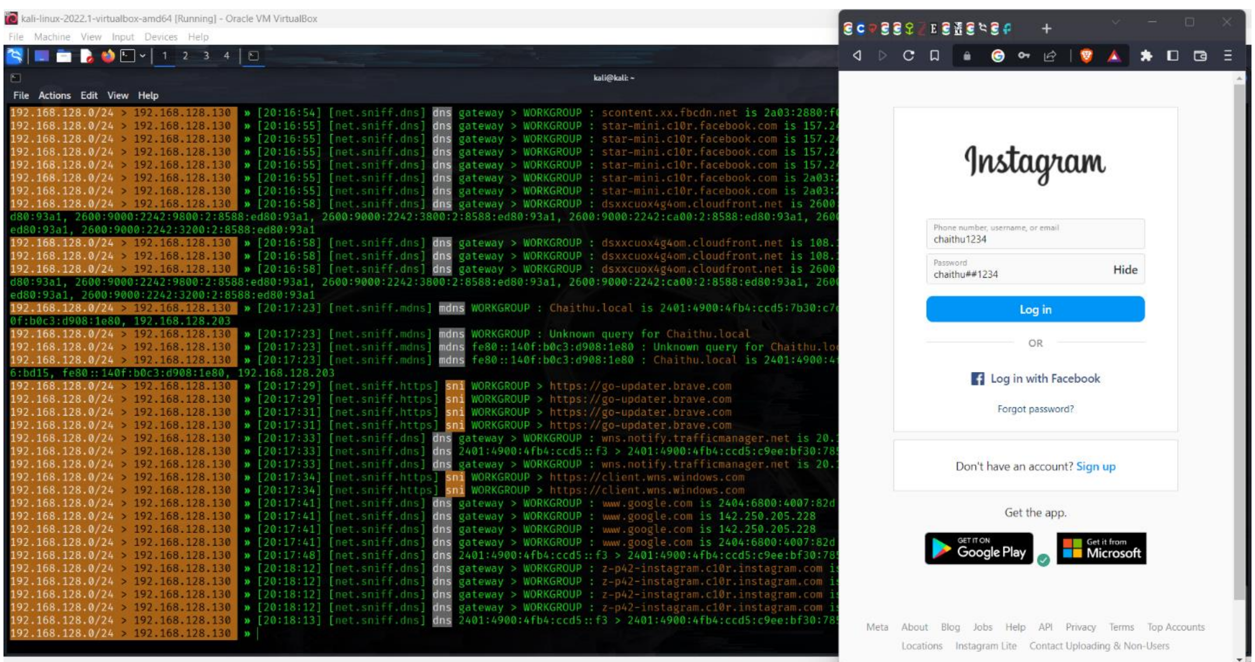


TESTING THE WEBSITES WITH HTTPS

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







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.