PASSWORD SNIFFING USING ETTERCAP

Mini-Project Report submitted in partial fulfilment of the requirements of the degree of Bachelor of Engineering by

Siddhesh Vartak	72
Shakti Yadav	74
Gaurav Rawat	75

Department of Computer Engineering
St. John College of Engineering and Management
University of Mumbai

2018-2019

Abstract

Packet sniffing is technique of monitoring every packet that across the network .The security threat presented by sniffing is the ability to capture all incoming and outgoing traffic, including clear-text password and username or other sensitive material.

Introduction

What is network sniffing?

Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address. **Network sniffing is the process of intercepting data packets sent over a network.** Networking sniffing is a form of data packet analysis enabling real-time network monitoring. Network sniffing is used to diagnose network problems and analyse overall network and application activity. With packet-level insights, admins can pinpoint slowdowns, categorize and assess traffic, and identify security risks.

Network sniffers take snapshot copies of the data flowing over a network without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools work with many other network protocols and at lower levels, including Ethernet frames. This can be done by the specialized software program or hardware equipment. Sniffing can be used to:

- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files have been transmitted over a network

Ettercap

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols. Its original developers later founded Hacking Team.

Methods -

UNIFIED, this method sniffs all the packets that pass on the cable. We can choose to put or not the interface in promise mode (-p option). The packet not directed to the host running ettercap will be forwarded automatically using layer 3 routing. So we can use a MIMA attack launched from a different tool and let ettercap modify the packets and forward them for us.

BRIDGED, it uses two network interfaces and forwards the traffic from one to the other while performing sniffing and content filtering. This sniffing method is totally stealthy since there is no way to find that someone is in the middle on the cable. We can look at this method as a MIMA attack at layer 1. We will be in the middle of the cable between two entities. Don't use it on gateways or it will transform wer gateway into a bridge.

Functionality

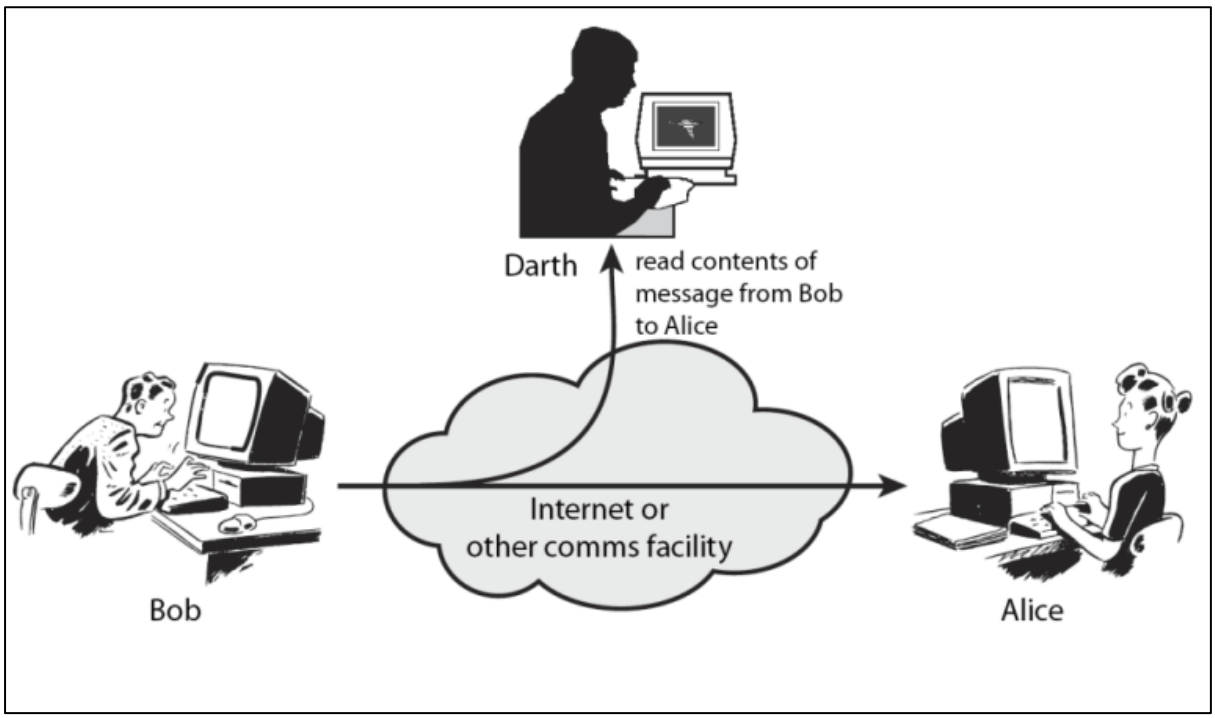
Ettercap works by putting the network interface into promiscuous mode and by ARP poisoning the target machines. Thereby it can act as a 'man in the middle' and unleash various attacks on the victims. Ettercap has plugin support so that the features can be extended by adding new plugins.

Features

Ettercap supports active and passive dissection of many protocols (including ciphered ones) and provides many features for network and host analysis. Ettercap offers four modes of operation:

- IP-based: packets are filtered based on IP source and destination.
- MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
- ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts (full-duplex).
- PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (half-duplex).

Architecture



Implementation

The best way to work on Ethernet is by installing Kali Linux. It's the most advanced and versatile penetration testing distribution ever created. It already has ettercap in its applications.

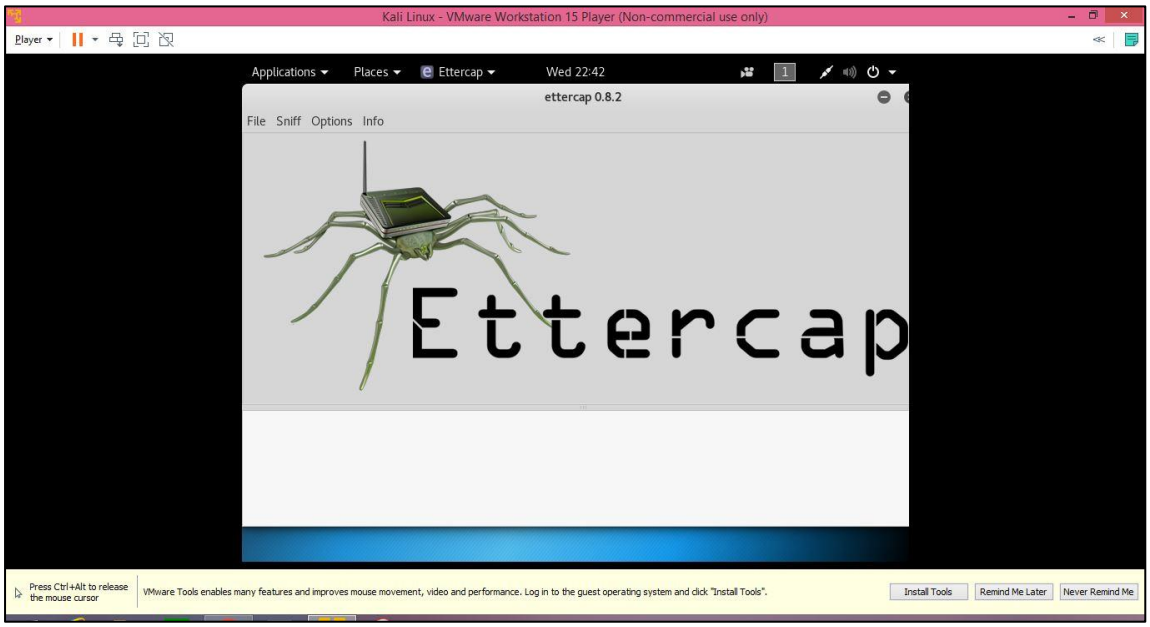
Here are some steps that will show we how to sniff passwords (they are written assuming we are using Linux):

1. Open to **Ubuntu**.
2. Go to the terminal.
3. For **install ettercap** in Ubuntu.

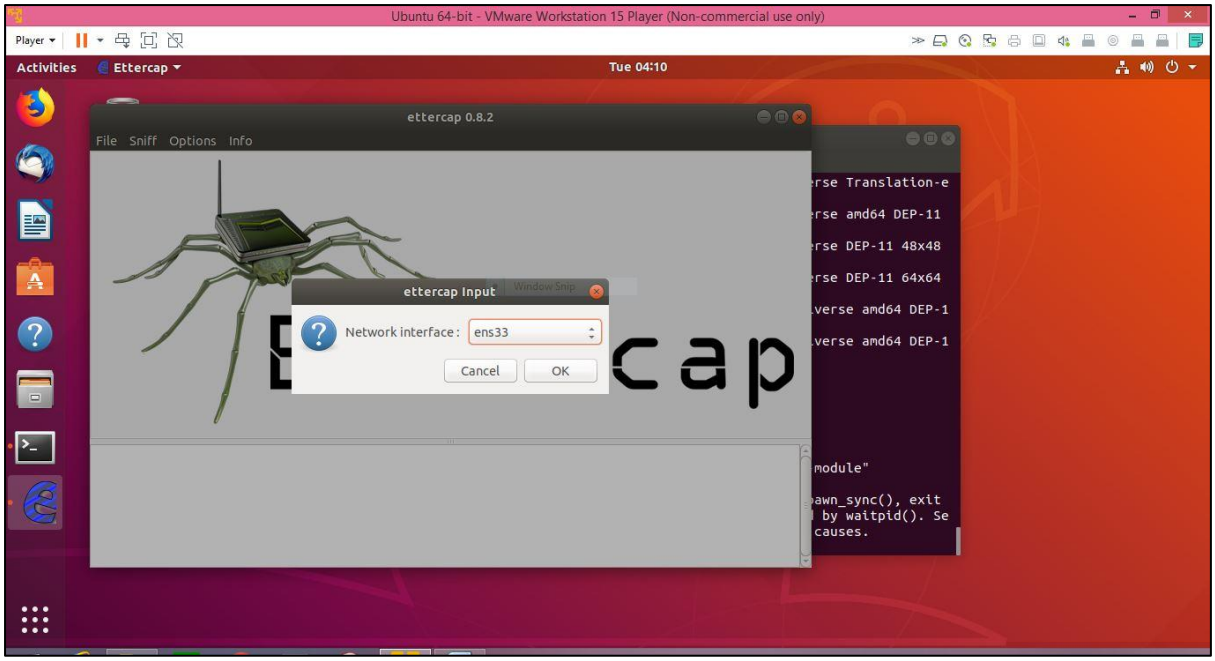
```
root@ubuntu:/home/siddhesh# apt-get install ettercap-common
root@ubuntu:/home/siddhesh# apt-get install ettercap-graphical
root@ubuntu:/home/siddhesh# apt-get install yum
```

4. For starting of ettercap application.

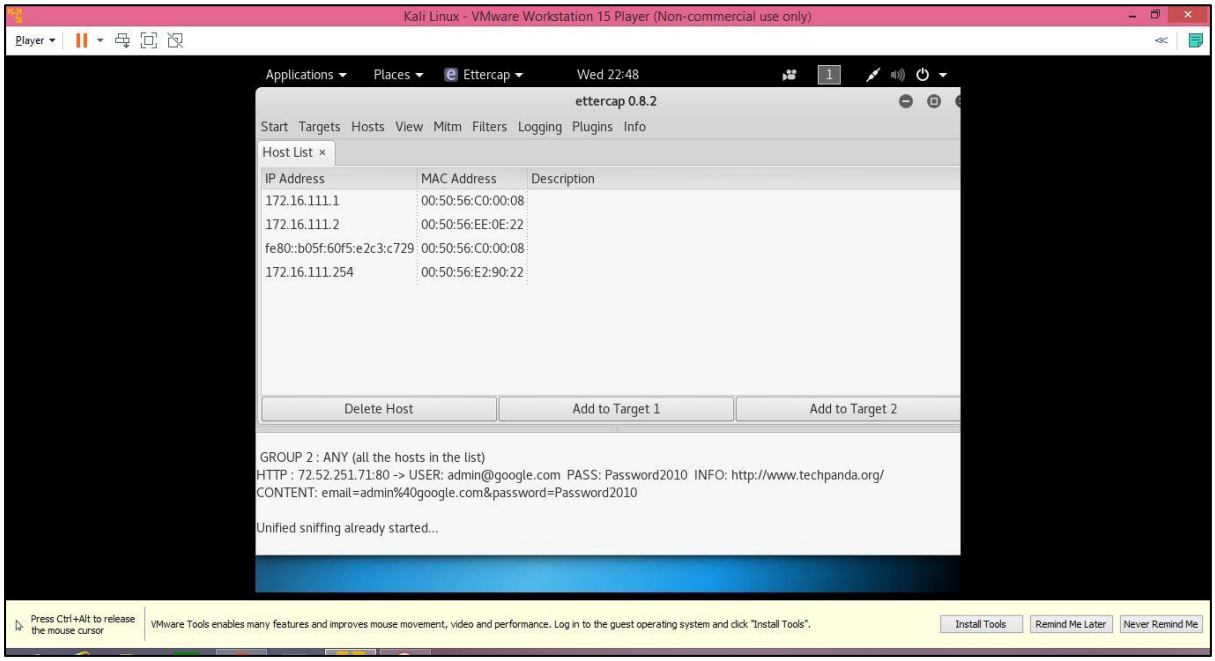
```
root@ubuntu:/home/siddhesh# sudo ettercap –G
```



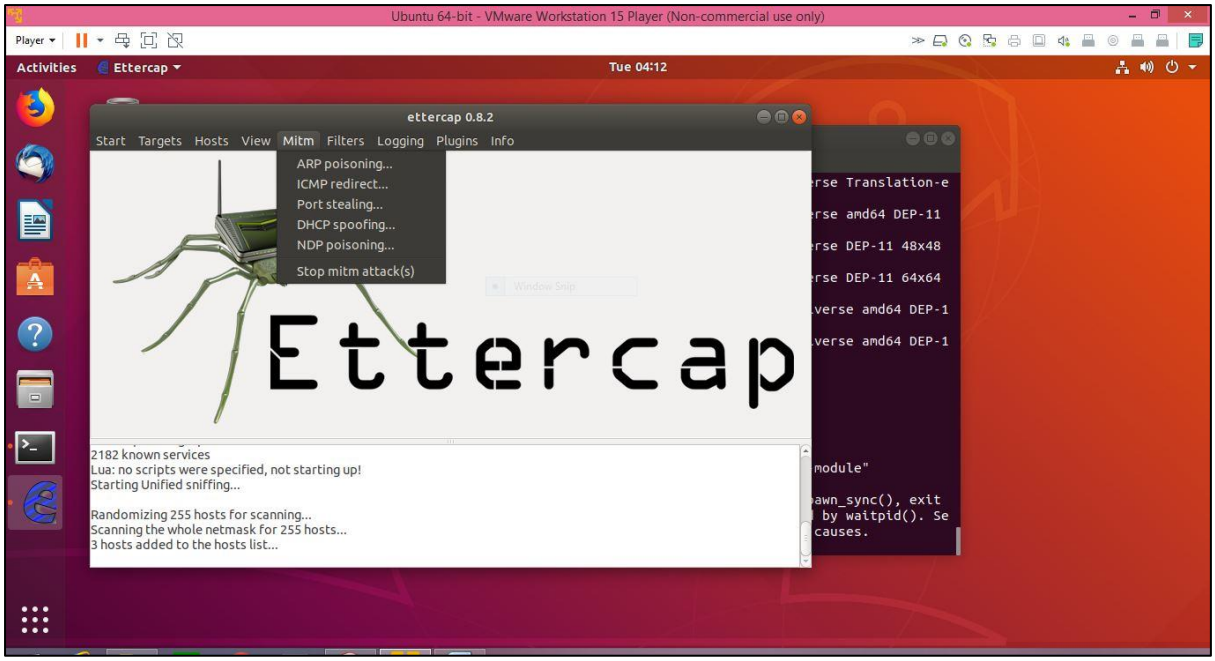
5. Click on **Sniff** and then on **Unified sniffing**.
6. Click on dropdown list symbol and **select the network interface** we are using.



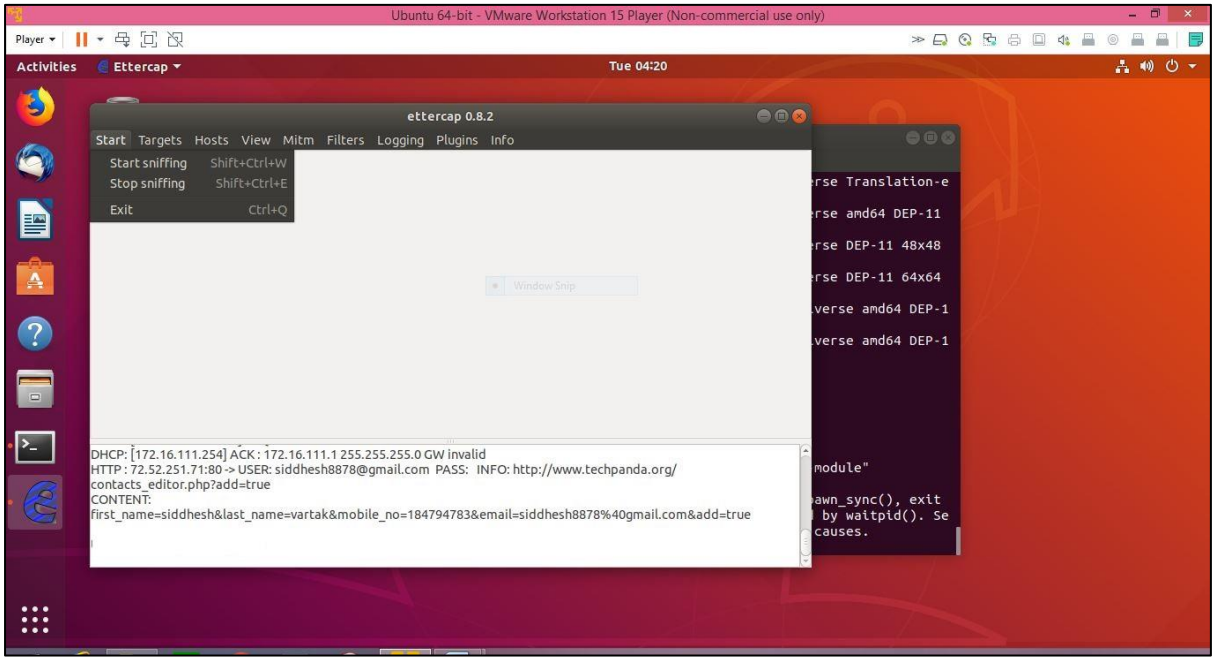
7. Click on **Hosts** and then on **Scan for hosts**.



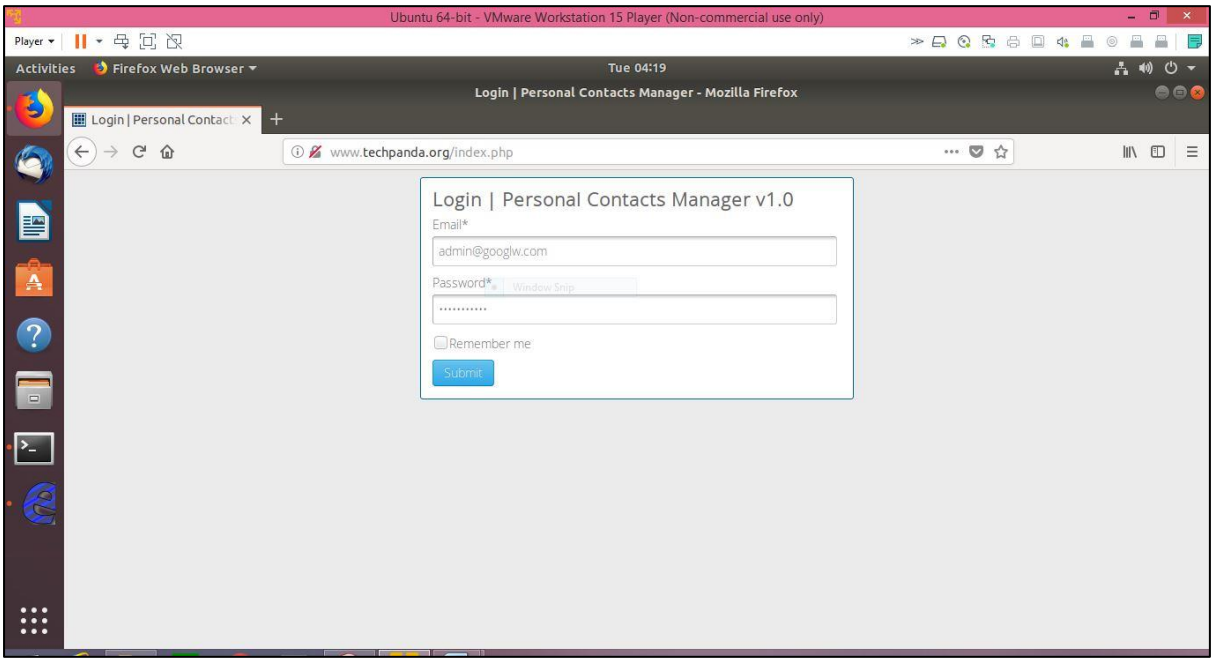
8. Go to **MIMA** and then on **Arp poisoning**.

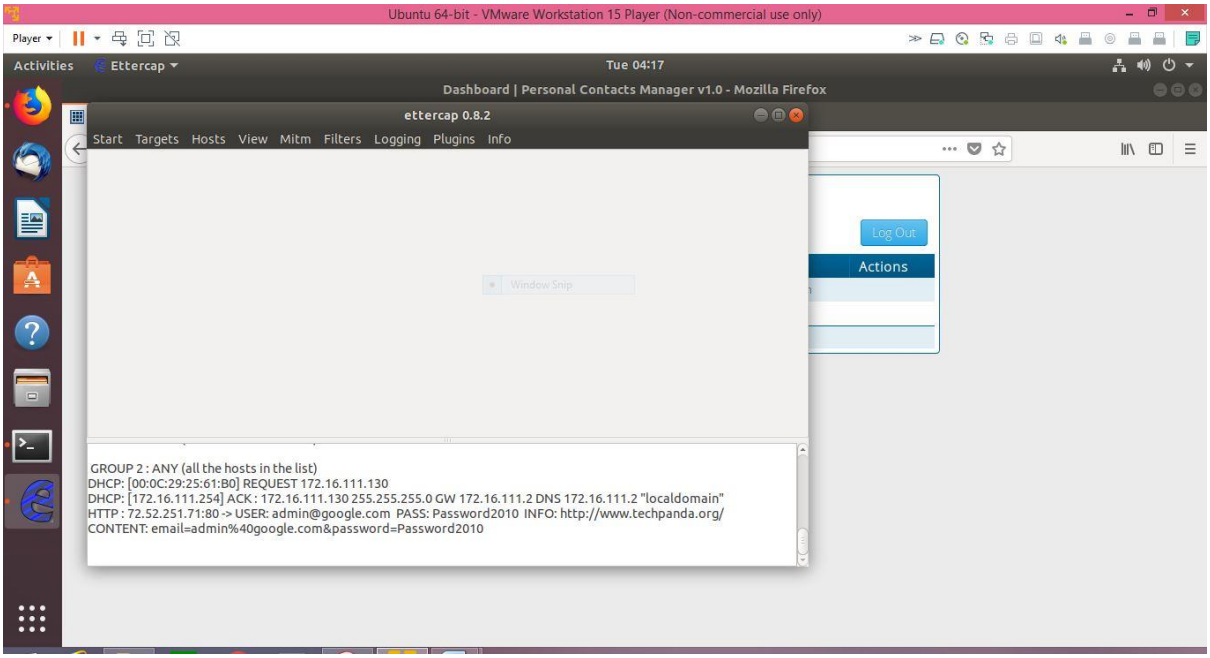


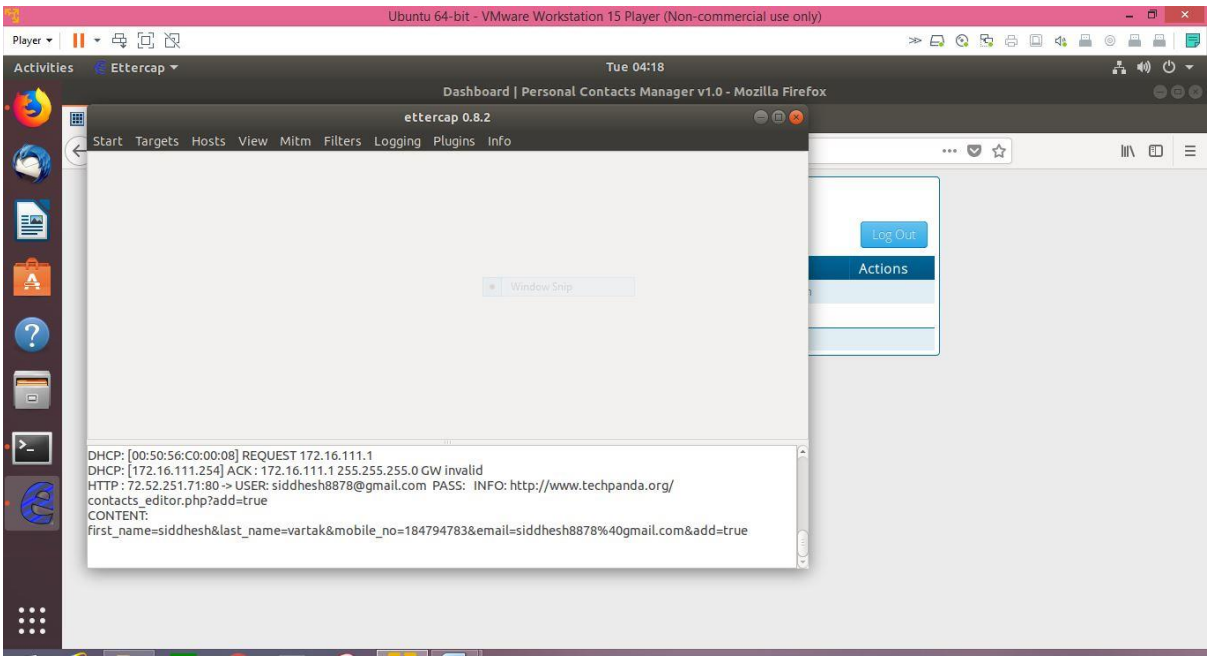
9. A dialog box will appear.
10. Select **Sniff remora connections** and then on **OK**.
11. Go to **Start** and then on **Start Sniffing**.



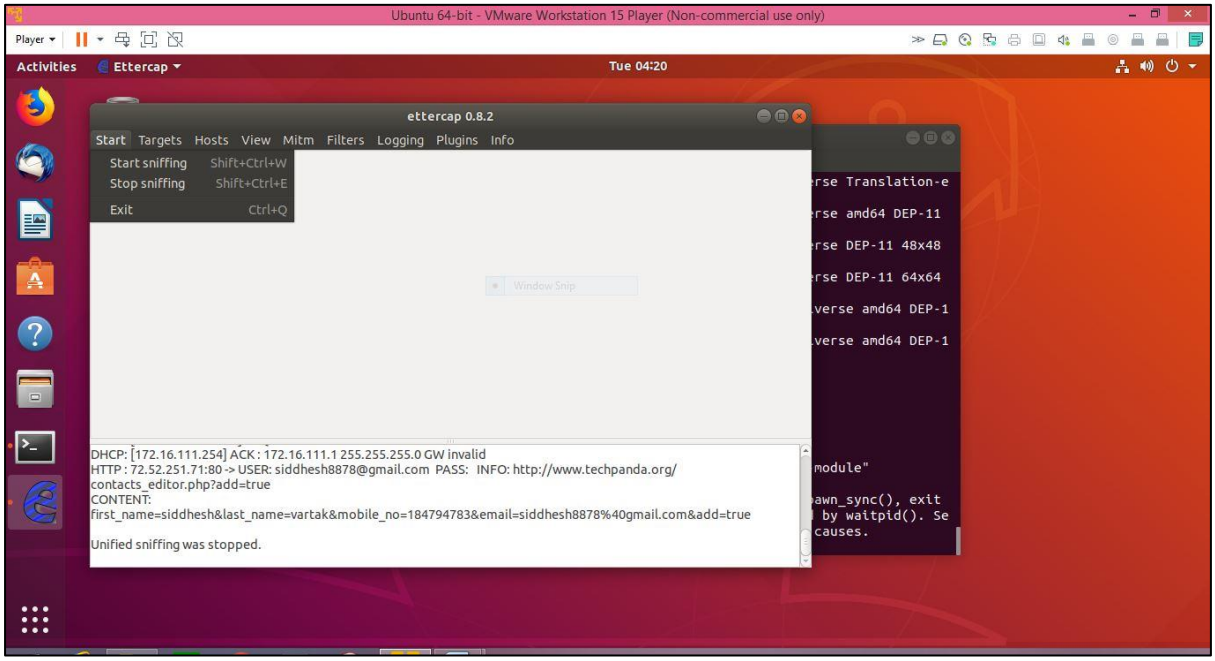
12. Wait for the person to type his ID and password on a site and we will get ID and password in decrypted mode.
13. Even register form detail is also get sniffing.


Ubuntu 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Tue 04:19
Login | Personal Contacts Manager - Mozilla Firefox
Login | Personal Contact
www.techpanda.org/index.php
Login | Personal Contacts Manager v1.0
Email*
admin@googlw.com
Password*
Remember me
Submit


Ubuntu 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player
Activities
Ettercap
Tue 04:17
Dashboard | Personal Contacts Manager v1.0 - Mozilla Firefox
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Log Out
Actions
GROUP 2 : ANY (all the hosts in the list)
DHCP: [00:0C:29:25:61:B0] REQUEST 172.16.111.130
DHCP: [172.16.111.254] ACK : 172.16.111.130 255.255.255.0 GW 172.16.111.2 DNS 172.16.111.2 "localdomain"
HTTP : 72.52.251.71:80 -> USER: admin@google.com PASS: Password2010 INFO: http://www.techpanda.org/
CONTENT: email=admin%40google.com&password=Password2010



14.For stop the sniffing go to start and stop sniffing



Conclusion:

Thus, we have implemented password sniffing using ettercap. We can sniff an ID and password also the user data from unsecure website whenever user login to any unsecure website.

References

[1] "*Network sniffer tool with network performance monitor*", solar winds, Feb 2013. Accessed on: December 2, 2018. [Online]Available: https://www.solarwinds.com/network-performance-monitor/use-cases/network-sniffer-tool#:~:text=Networking%20sniffing%20is%20a%20form,traffic%2C%20and%20identify%20security%20risks.

[2] "*What is network sniffer*", Lifewire, Feb 2013. Accessed on: December 2, 2018. [Online]Available: https://www.lifewire.com/definition-of-sniffer-817996

[3] "*Ettercap and middle-attacks tutorial*", PenTest magazine, Feb 2010. Accessed on: December 2, 2018. [Online]Available: https://pentestmag.com/ettercap-tutorial-for-windows/

[4] "*Ettercap (software)*", Wikipedia. Accessed on: December 2, 2018. [Online]Available: https://en.wikipedia.org/wiki/Ettercap_(software)