Group no: - 8

Group Member:- **Shrut Shah – 19BCP125**

Shubham Kathiriya – 19BCP127

Vedant Patel – 19BCP138

Subject: - Cyber Security Lab

Division:-2

Lab 9:- Packet Sniffer

Introduction:-

- Packet sniffing is a technique whereby packet data flowing across the network is detected and observed.
- Network administrators use packet sniffing tools to monitor and validate network traffic, while hackers may use similar tools for nefarious purposes.

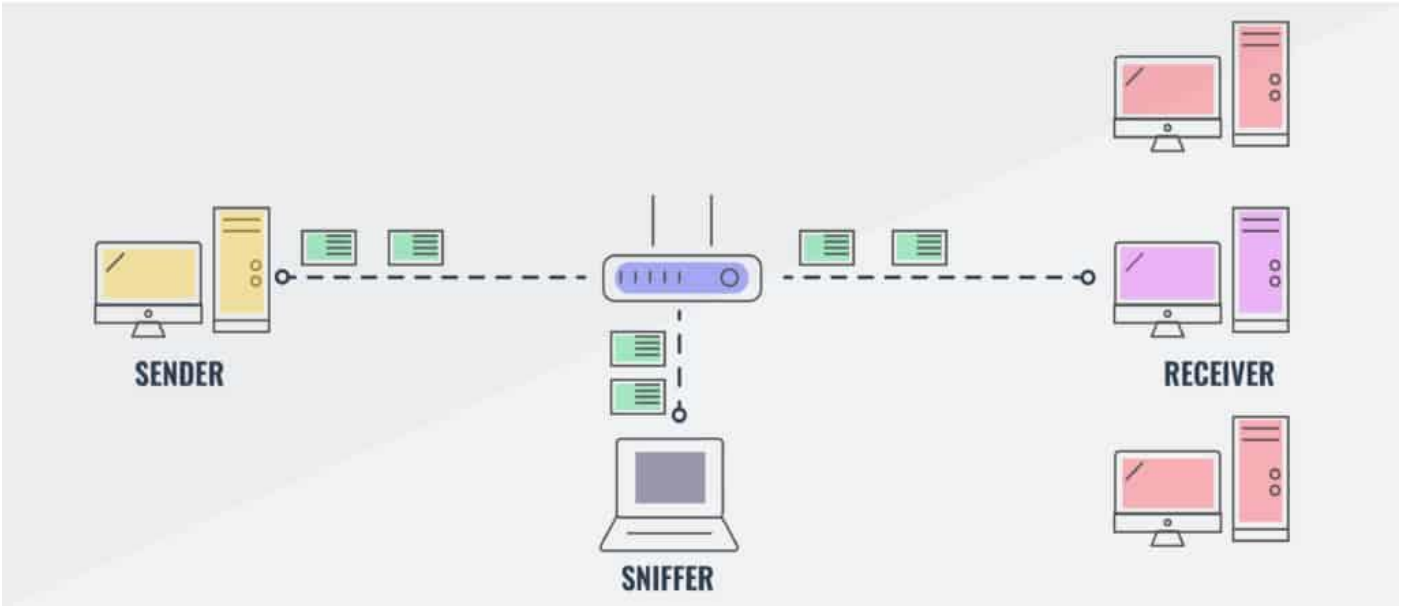
What are packet sniffers?

- Packet sniffers are applications or utilities that read data packets traversing the network within the Transmission Control Protocol/Internet Protocol (TCP/IP) layer.
- When in the hands of network administrators, these tools “sniff” internet traffic in real-time, monitoring the data, which can then be interpreted to evaluate and diagnose performance problems within servers, networks, hubs and applications.
- When packet sniffing is used by hackers to conduct unauthorized monitoring of internet activity, network administrators can use one of several methods for detecting sniffers on the network.

- Armed with this early warning, they can take steps to protect data from illicit sniffers.
- NETSCOUT's Omnis Security platform utilizes packet-based analysis for advanced threat analytics and response.

How do hackers use packet sniffing:-

- Hackers will typically use one of two different methods of sniffing to surreptitiously monitor a company's network.
- In the case of organizations with infrastructure configured using hubs that connect multiple devices together on a single network, hackers can utilize a sniffer to passively "spy" on all the traffic flowing within the system.
- Passive sniffing, such as this, is extremely difficult to uncover.
- When a much larger network is involved, utilizing numerous connected computers and network switches to direct traffic only to specific devices, passive monitoring simply won't provide access to all network traffic.
- In such a case, sniffing won't be helpful for either legitimate or illegitimate purposes.
- Hackers will be forced to bypass the constraints created by the network switches.
- This requires active sniffing, which adds further traffic to the network, and in turn makes it detectable to network security tools.



ISPs use packet sniffing to track all your activities such as:

- who is receiver of your email
- what is content of that email
- what you download
- sites you visit
- what you looked on that website
- downloads from a site
- streaming events like video, audio, etc.

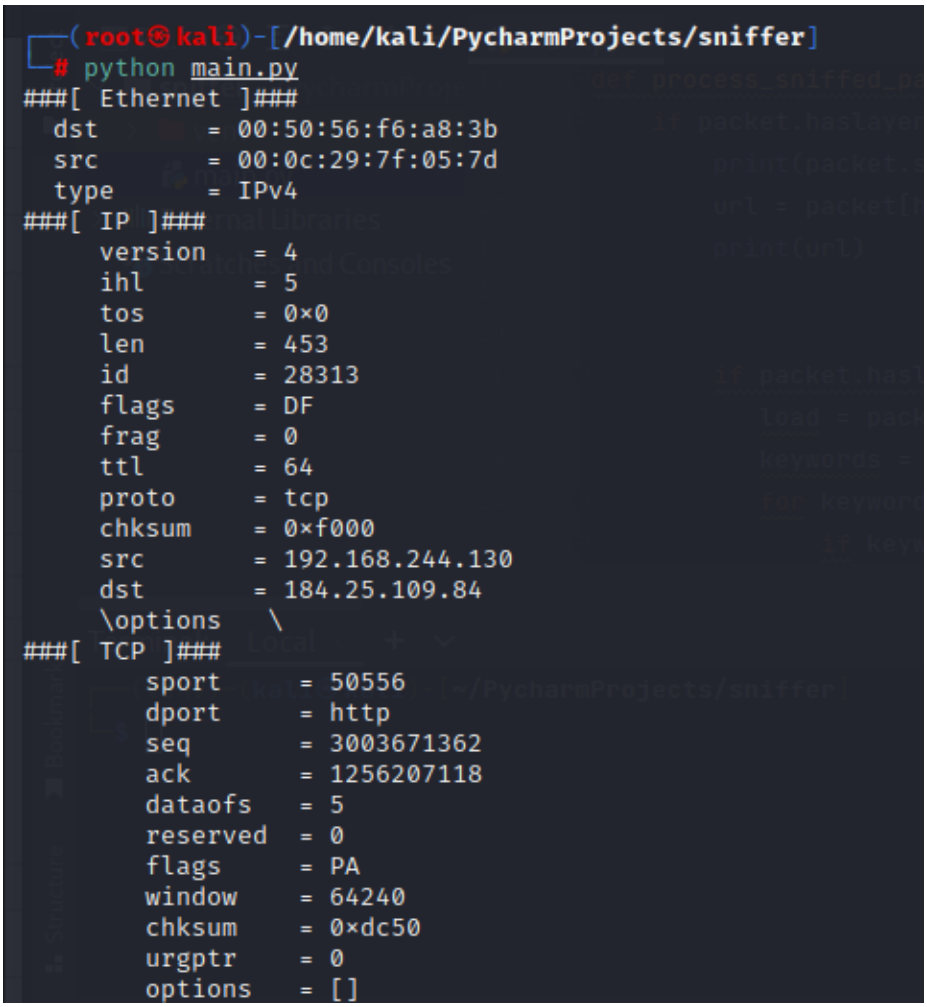
Python code: -

- **Used Library:- Scapy**
  - Scapy is a powerful and versatile packet manipulation tool written in python. Using scapy, a user will be able to send, sniff, dissect and forge network packets. Scapy also has the capability to store the sniffed packets in a pcap file.

```
#extracting urls also which target is accessing
#to see use packet.show
#http request-->path you will get image path
#host will contain domain name
#combine host and path

import scapy.all as scapy
from scapy.layers import http

def sniff(interface):
    scapy.sniff(iface=interface, store=False, prn=process_sniffed_packet)




def process_sniffed_packet(packet):

    if packet.haslayer(http.HTTPRequest):
        print(packet.show())
```

```
        url = packet[http.HTTPRequest].Host + packet[http.HTTPRequest].Path
        print(url)


        if packet.haslayer(scapy.Raw):
           load = packet[scapy.Raw].load

           keywords = ["uname", "pass", "username", "password", "login"]

           for keyword in keywords:
               if keyword in load: #username is substring
                print(load)         #it will print two times
                break                #come out if atleast one keyword is found

sniff("eth0")
```

Output Screenshot :-



```
###[ HTTP 1 ]###
###[ HTTP Request ]###
          Method    = 'POST'
          Path      = '/'
          Http_Version= 'HTTP/1.1'
          A_IM      = None
          Accept    = '*/*'
          Accept_Charset= None
          Accept_Datetime= None
          Accept_Encoding= 'gzip, deflate'
          Accept_Language= 'en-US,en;q=0.5'
          Access_Control_Request_Headers= None
          Access_Control_Request_Method= None
          Authorization= None
          Cache_Control= 'no-cache'
          Connection= 'keep-alive'
          Content_Length= '85'
          Content_MD5= None
          Content_Type= 'application/ocsp-request'
          Cookie    = None
          DNT       = None
          Date      = None
          Expect    = None
          Forwarded = None
          From      = None
          Front_End_Https= None
          HTTP2_Settings= None
          Host      = 'r3.o.lencr.org'
          If_Match  = None
          If_Modified_Since= None
          If_None_Match= None
          If_Range  = None
          If_Unmodified_Since= None
          Keep_Alive= None
          Max_Forwards= None
          Origin    = None
          Permanent = None
          Pragma    = 'no-cache'
          Proxy_Authorization= None
          Proxy_Connection= None
          Range     = None
          Referer   = None
          Save_Data = None
          TE        = None
          Upgrade   = None
          Upgrade_Insecure_Requests= None
          Upgrade_Insecure_Requests= None
          User_Agent= 'Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0'
          Via       = None
          Warning   = None
```

```
          Pragma    = 'no-cache'
          Proxy_Authorization= None
          Proxy_Connection= None
          Range     = None
          Referer   = None
          Save_Data = None
          TE        = None
          Upgrade   = None
          Upgrade_Insecure_Requests= None
          Upgrade_Insecure_Requests= None
          User_Agent= 'Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0'
          Via       = None
          Warning   = None
          X_ATT_DeviceId= None
          X_Correlation_ID= None
          X_Csrf_Token= None
          X_Forwarded_For= None
          X_Forwarded_Host= None
          X_Forwarded_Proto= None
          X_Http_Method_Override= None
          X_Request_ID= None
          X_Requested_With= None
          X_UIDH    = None
          X_Wap_Profile= None
          Unknown_Headers= None
###[ Raw ]###
             load      = '0S0Q0O0M0K0\t\x06\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14H\xda\xc9\xa0\xfb+\xd3-O\xf0\xdeh\xd2\xf5g\xb75\xf9\xb3\xc4\x04\x14\x14.\xb
3\x17\xb7XV\xcb\xaeP\t@\xe6\x1f\xaf\x9d\x8b\x14\xc2\xc6\x02\x12\x03\xca3Q\xb1I\xcd4\xe9\x96\x0f\xf1\xf8\x9f\xc2\xae\xd2\xfb'
```

Advertising agencies or internet advertising agencies are paid according to:

- Number of ads shown by them.
- Number of clicks on their ads also called PPC (pay per click).

To achieve this target, these agencies use packet sniffing to inject advertisements into the flowing packets. Most of the time these ads contain malware.

Government agencies use packet sniffing to:

- Ensure security of data over the network.
- Track an organisation's unencrypted data.

How to protect networks from illicit sniffers

There are several steps organizations can take to protect their networks from illicit sniffing activities. The following defenses can reduce the risk of exposure to hackers:

1) **Do not use public Wi-Fi networks:** Wi-Fi networks found in public spaces typically lack security protocols to fully protect users. Hackers can easily sniff the entire network, gaining access to sensitive data. Avoiding such networks is a wise security choice unless the user is accessing an encrypted VPN.

2) **Rely on a trusted VPN connection:** When accessing the internet remotely, always use a trusted Virtual Private Network that encrypts the connection and masks all data from sniffers. Any sniffer attempting to monitor traffic over a VPN will only see data that has been scrambled, making it useless to the hacker.

3) **Always deploy robust antivirus software:** By installing effective antivirus software, organizations can prevent malware from infiltrating the network and system. Robust antivirus tools will also uncover sniffers present in the system and offer to delete them.

4) **Look for secure HTTPS protocols before surfing the web:** Before surfing the internet, look for the "HTTPS" in the address bar of a website. Some sites only indicate "HTTP." The additional "S" at the end is an indication that the site adheres to more robust security protocols that encrypt communications and will prevent sniffers used by hackers from seeing the data.

5) **Don't fall prey to social engineering tricks and traps:** Hackers and cyber attackers will often employ phishing emails and spoofed website to trick people into unwittingly downloading sniffers. Being aware and cautious when browsing can prevent users from falling prey to nefarious tactics.

Conclusion: -

Packet sniffing is a sophisticated subject that wears two hats. It can be used for either good or evil depending on the intentions of the person using the program. It can help with analysing network problems and detect misuses in the network for good purposes. Meanwhile, it can also help hackers and other cyber-criminals steal data from insecure networks and commit crimes, as in the case of Dave & Buster's. The best way to protect data from being "sniffed" is to encrypt it. Necessary policies and training also help with the protection. As technology evolves, there will be more and more ways to commit cybercrime. Extremely sensitive and valuable data such as credit card information should be well-protected, from the perspectives of both organizations and individuals. In order to protect this information, users should be aware of the benefits of packet sniffers but also protect against the threat of their misuse.