ACS545 Cryptography and Network Security
Chapter 1
Network Security Basics

Instructor: Dr. Zesheng Chen

Outline

- IP Address and Network Interface
- TCP/IP Protocols
- Programming Using Scapy
- Lab Environment and Containers
- Packet Sniffing
- Packet Spoofing

IP Address: the Original Scheme

```
Class A                    |<--      Host ID     -->|
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111

Class B                             |<-- Host ID -->|
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111

Class C                                       |HostID|
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111

Class D               |<--   Address Range       -->|
224.  0.  0.  0 = 11100000.00000000.00000000.00000000
239.255.255.255 = 11101111.11111111.11111111.11111111

Class E               |<--   Address Range       -->|
240.  0.  0.  0 = 11110000.00000000.00000000.00000000
255.255.255.255 = 11111111.11111111.11111111.11111111
```

CIDR Scheme (Classless Inter-Domain Routing)

192.168.60.5/**24**

Indicate the first 24 bits are network ID

Question: What is the address range of the network **192.168.192.0/19 ?**

Special IP Addresses

- Private IP Addresses
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Loopback Address
  - 127.0.0.0/8
  - Commonly used: 127.0.0.1

List IP Address on Network Interface

```
$ ifconfig
$ ip address
```

```
$ ip -br address
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             10.0.5.5/24 fe80::bed8:53e2:5192:f265/64
docker0          DOWN           172.17.0.1/16 fe80::42:13ff:fee7:90d6/64
```

Manually Assign IP Address

```
$ sudo ip addr add 192.168.60.6/24 dev enp0s3
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
 group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_f
ast state UP group default qlen 1000
    link/ether 08:00:27:84:5e:b9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.6/24 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::3fc4:1dac:bbbb:948/64 scope link
       valid lft forever preferred lft forever
```

Automatically Assign IP Address

- DHCP: Dynamic Host Configuration Protocol

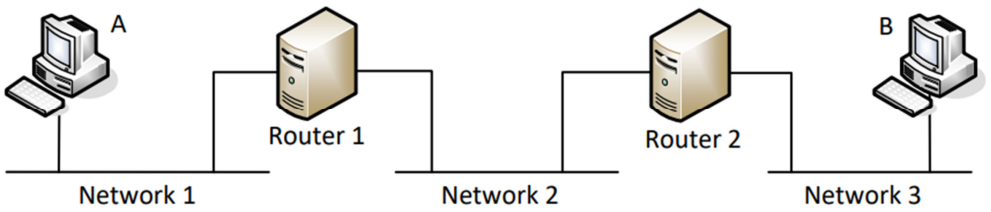
Get IP Addresses for Host Names: DNS

```
seed@VM:~$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18093
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        57405   IN      A       93.184.216.34
```

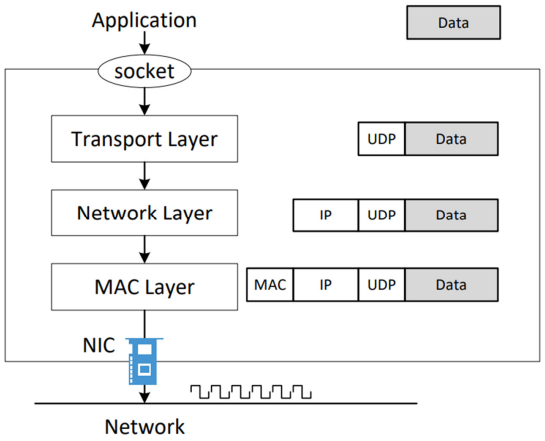
Outline

- IP Address and Network Interface
- TCP/IP Protocols
- Programming Using Scapy
- Lab Environment and Containers
- Packet Sniffing
- Packet Spoofing

Packet Journey at High Level

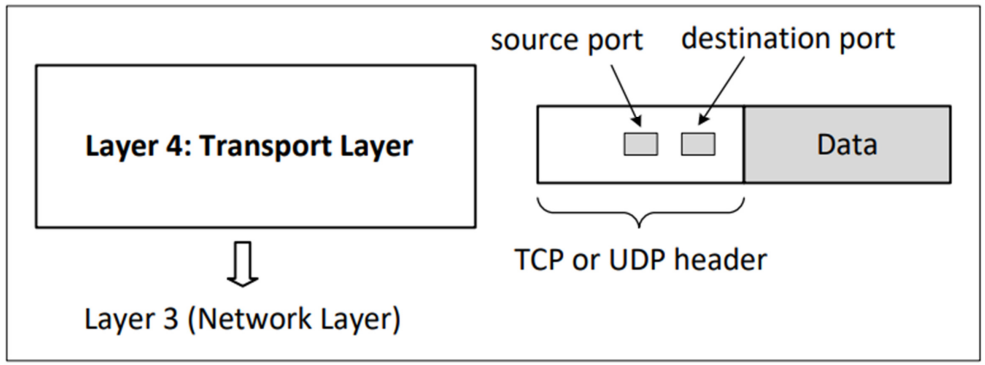


How Packets Are Constructed



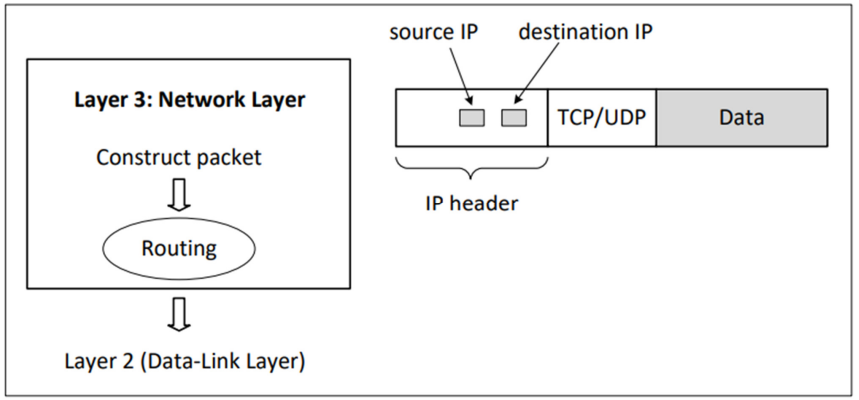
PURDUE UNIVERSITY FORT WAYNE

Layer 4: Transport Layer



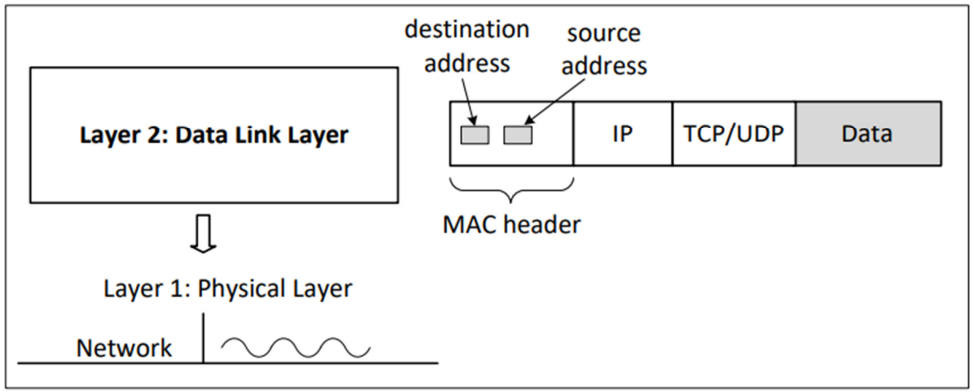
PURDUE UNIVERSITY FORT WAYNE

Layer 3: Network Layer



PURDUE UNIVERSITY FORT WAYNE

Layer 2: Data Link Layer (MAC Layer)



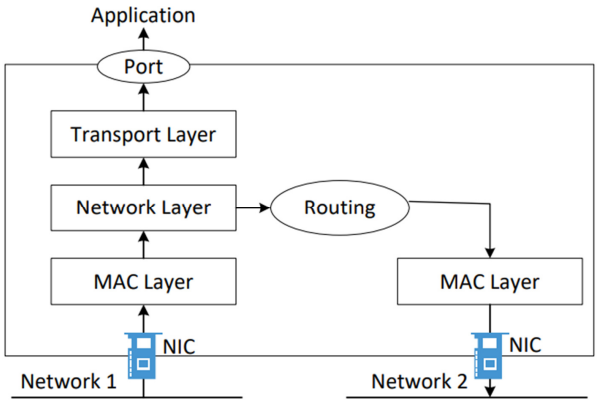
PURDUE UNIVERSITY FORT WAYNE

Two UDP Socket Examples (Python)

- udp_client.py
- udp_server.py

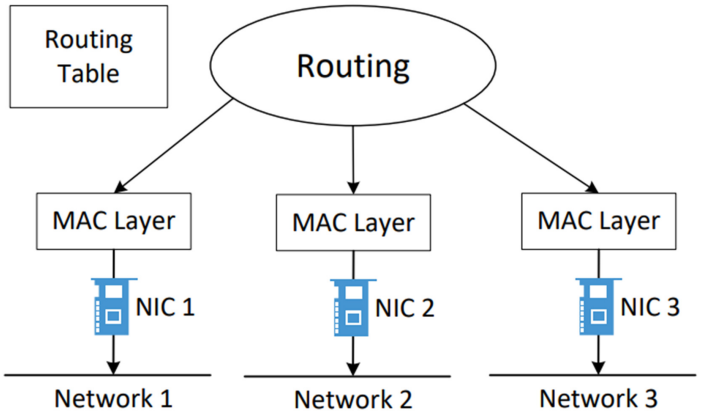
PURDUE UNIVERSITY FORT WAYNE

How Packets Are Received



PURDUE UNIVERSITY FORT WAYNE

Routing



PURDUE UNIVERSITY FORT WAYNE

The "ip route" Command

```
# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.11
192.168.60.0/24 dev eth1 proto kernel scope link src 192.168.60.11

# ip route get 10.9.0.1
10.9.0.1 dev eth0 src 10.9.0.11 uid 0

# ip route get 192.168.60.5
192.168.60.5 dev eth1 src 192.168.60.11 uid 0

# ip route get 1.2.3.4
1.2.3.4 via 10.9.0.1 dev eth0 src 10.9.0.11 uid 0
```

PURDUE UNIVERSITY FORT WAYNE

Packet Sending Tools

- Using netcat

```
$ nc <ip> <port>        ← send out TCP packet
$ nc -u <ip> <port>     ← send out UDP packet
```

- Bash: /dev/tcp or /dev/udp pseudo device

```
$ echo "data" > /dev/udp/<ip>/<port>
$ echo "data" > /dev/tcp/<ip>/<port>
```

- Others: telnet, ping, etc.

Outline

- IP Address and Network Interface
- TCP/IP Protocols
- Programming Using Scapy
- Lab Environment and Containers
- Packet Sniffing
- Packet Spoofing

Scapy

- Is a powerful interactive packet manipulation program for Python2 and Python3
- Runs natively on Linux and on most Unixes with libpcap and its python wrappers
- Used not only as a tool, but also as a building block to construct other sniffing and spoofing tools
- https://scapy.net/
- Examples

Scapy: Display Packets

- Using hexdump()

```
>>> hexdump(pkt)
0000  52 54 00 12 35 00 08
0010  00 54 F2 29 40 00 40
0020  08 08 08 00 98 01 10
0030  0C 00 08 09 0A 0B 0C
0040  16 17 18 19 1A 1B 1C
0050  26 27 28 29 2A 2B 2C
0060  36 37
```

- Using pkt.show()

```
>>> pkt.show()
###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:77:2e:c3
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     ...
     proto     = icmp
     chksum    = 0x3c9a
     src       = 10.0.2.8
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
```

Scapy: Iterate Through Layers

```
>>> pkt = Ether()/IP()/UDP()/"hello"
>>> pkt
<Ether type=IPv4 |<IP frag=0 proto=udp |<UDP |<Raw load='hello' |>>>>

>>> pkt.payload                              ← an IP object
<IP  frag=0 proto=udp |<UDP  |<Raw  load='hello' |>>>

>>> pkt.payload.payload                      ← a UDP object
<UDP  |<Raw  load='hello' |>>

>>> pkt.payload.payload.payload              ← a Raw object
<Raw  load='hello' |>

>>> pkt.payload.payload.payload.load         ← the actual payload
b'hello'
```

PURDUE UNIVERSITY FORT WAYNE

Accessing Layers

Get inner layers

```
>>> pkt.getlayer(UDP)
<UDP  |<Raw  load='hello' |>>
>>> pkt[UDP]
<UDP  |<Raw  load='hello' |>>

>>> pkt.getlayer(Raw)
<Raw  load='hello' |>
>>> pkt[Raw]
<Raw  load='hello' |>
```

Check layer existence

```
>>> pkt.haslayer(UDP)
True
>>> pkt.haslayer(TCP)
0
>>> pkt.haslayer(Raw)
True
```

PURDUE UNIVERSITY FORT WAYNE

Other Uses of Scapy: Send and Receive

- `send()`: Send packets at Layer 3.
- `sendp()`: Send packets at Layer 2.
- `sr()`: Sends packets at Layer 3 and receiving answers.
- `srp()`: Sends packets at Layer 2 and receiving answers.
- `sr1()`: Sends packets at Layer 3 and waits for the first answer.
- `sr1p()`: Sends packets at Layer 2 and waits for the first answer.
- `srloop()`: Send a packet at Layer 3 in a loop and print the answer each time.
- `srploop()`: Send a packet at Layer 2 in a loop and print the answer each time.

PURDUE UNIVERSITY FORT WAYNE

Example: implement ping

```
#!/usr/bin/python3
from scapy.all import *

ip = IP(dst="8.8.8.8")
icmp = ICMP()
pkt = ip/icmp
reply = sr1(pkt)
print("ICMP reply .........")
print("Source IP : ", reply[IP].src)
print("Destination IP :", reply[IP].dst)
```

PURDUE UNIVERSITY FORT WAYNE

Traceroute Code (Partial)

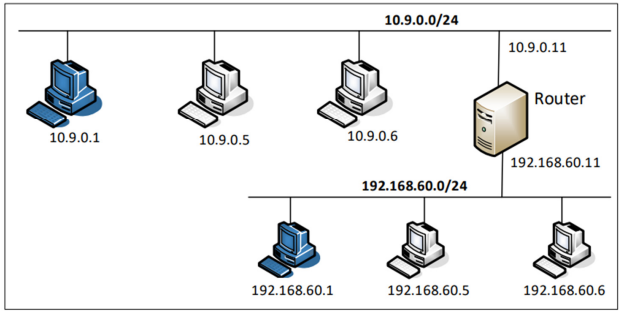
```
b = ICMP()
a = IP()
a.dst = '93.184.216.34'

TTL = 3
a.ttl = TTL
h = sr1(a/b, timeout=2, verbose=0)
if h is None:
    print("Router: *** (hops = {})".format(TTL))
else:
    print("Router: {} (hops = {})".format(h.src, TTL))
```

Outline

- IP Address and Network Interface
- TCP/IP Protocols
- Programming Using Scapy
- Lab Environment and Containers
- Packet Sniffing
- Packet Spoofing

Lab Setup and Containers

- Most labs in Internet Security use containers
  - **Lab setup files:**: Labsetup.zip
  - **Manual:**: Docker manual



Docker Compose

- Setup file: docker-compose.yml

```
version: "3"

services:
    HostA1:
        ...
    HostA2:
        ...
    ...
networks:
    net-192.168.60.0:
        ...
    net-10.9.0.0:
        ...
```

Docker Manual:
https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/SEEDManual-Container.md

Set Up Networks

```
networks:
    net-10.9.0.0:
        name: net-10.9.0.0
        ipam:
            config:
                - subnet: 10.9.0.0/24

    net-192.168.60.0:
        name: net-192.168.60.0
        ipam:
            config:
                - subnet: 192.168.60.0/24
```

Find out interface name

```
$ ifconfig
br-03bc5aebc4c4: flags=4163<UP,
        inet 10.9.0.1  netmask
```

```
$ docker network ls
NETWORK ID          NAME
c616fa7f4f46        bridge
b3581338a28d        host
03bc5aebc4c4        net-10.9.0.0
e0afdc1c0e70        net-192.168.60.0
```

Set Up Hosts

```
HostA1:
    image: handsonsecurity/seed-ubuntu:large
    container_name: host-10.9.0.5
    tty: true
    cap_add:
            - ALL
    privileged: true
    volumes:
            - ./volumes:/volumes
    networks:
        net-10.9.0.0:
            ipv4_address: 10.9.0.5
    command: bash -c "
                  ip route add 192.168.60.0/24 via 10.9.0.11 &&
                  tail -f /dev/null
             "
```

Sniffing Inside Containers

- Limitation
  - Can only sniff its own traffic
  - Due to how the virtual network is implemented

Sniffing Inside Containers

- Overcome the limitation
  - Use the “host” mode
  - `network_mode: host`

Start/Stop Containers

Alias created in the SEED VM

```
docker-compose build
docker-compose up
docker-compose down
```

```
dcbuild
dcup
dcdown
```

Get Into A Container

```
$ docker ps
CONTAINER ID        NAMES       ...
bcff498d0b1f     host-10.9.0.6  ...
1e122cd314c7     host-10.9.0.5  ...
31bd91496f62     host-10.9.0.7  ...

$ docker exec -it 1e /bin/bash
root@1e122cd314c7:/#
```

Alias created in the SEED VM

```
$ dockps
bcff498d0b1f  host-10.9.0.6
1e122cd314c7  host-10.9.0.5
31bd91496f62  host-10.9.0.7

$ docksh 31
root@31bd91496f62:/#
```

Copy Files Between Host and Container

Get container ID

```
$ docker ps
CONTAINER ID        NAMES
bcff498d0b1f     host-10.9.0.6
1e122cd314c7     host-10.9.0.5
31bd91496f62     host-10.9.0.7
```

```
// From host to container
$ docker cp  file.txt  bcff:/tmp/
$ docker cp  folder  bcff:/tmp

// From container to host
$ docker cp  bcff:/tmp/file.txt .
$ docker cp  bcff:/tmp/folder  .
```

Outline

- IP Address and Network Interface
- TCP/IP Protocols
- Programming Using Scapy
- Lab Environment and Containers
- Packet Sniffing
- Packet Spoofing

How Packets Are Received

- NIC (Network Interface Card) is a physical or logical link between a machine and a network
- Each NIC has a MAC address
- Every NIC on the network will hear all the frames on the wire
- NIC checks the destination address for every packet, if the address matches the cards MAC address, it is further copied into a buffer in the kernel

PURDUE UNIVERSITY FORT WAYNE

Promiscuous Mode

- The frames that are not destined to a given NIC are discarded
- When operating in promiscuous mode, NIC passes every frame received from the network to the kernel
  - Elevated or root privileges are required
- If a sniffer program is registered with the kernel, it will be able to see all the packets
- In Wi-Fi, it is called Monitor Mode
  - Miss info on the same network but different channels

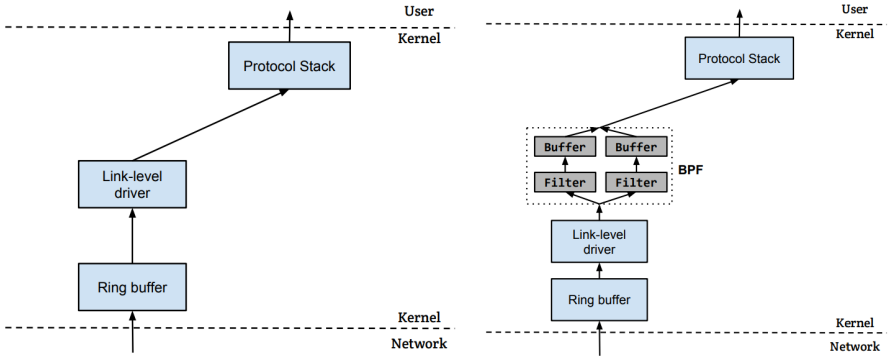
PURDUE UNIVERSITY FORT WAYNE

BSD Packet Filter (BPF)

- It is very inefficient to discard packets at the application level, so we try to filter packets as early as possible and hence use BSD Packet Filter (BPF)
- BPF allows a user-program to attach a filter to the socket, which tells the kernel to discard unwanted packets
- The filter is often written in human readable format using Boolean operators and is compiled into a pseudo-code and passed to the BPF driver

PURDUE UNIVERSITY FORT WAYNE

Packet Flow With/Without Filters



(a) Packet flow (b) Packet flow with filter

PURDUE UNIVERSITY FORT WAYNE

Packet Sniffing

Packet sniffing describes the process of capturing live data as they flow across a network.

Packet Sniffing Tools

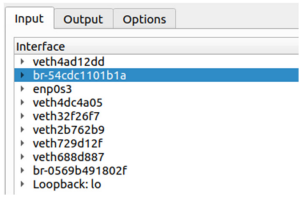
- Tcpdump
  - Command line
  - Good choice for containers (in the lab setup)
- Wireshark
  - GUI
  - Good choices for the environment supporting GUI (not containers)
- Scapy
  - Implement your own sniffing tools

Tcpdump Examples

- `tcpdump -n -i eth0`
  - **-n**: do not resolve the IP address to host name
  - **-i**: sniffing on this interface
- `tcpdump -n -i eth0 -vvv “tcp port 179”`
  - **-vvv**: asks the program to produce more verbose output.
- `tcpdump -i eth0 -w /tmp/packets.pcap`
  - saves the captured packets to a PCAP file
  - use Wireshark to display them

Wireshark and Containers

Find the correct interface




```
seed@VM:~$ docker network ls
NETWORK ID          NAME                DRIVER              SCOPE
d10f14b6b6f9        bridge              bridge              local
b3581338a28d        host                host                local
54cdc1101b1a        net-10.9.0.0        bridge              local
0569b491802f        net-192.168.60.0    bridge              local
77acecccbe26        none                null                local
seed@VM:~$ ip -br address
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             10.0.5.5/24 fe80::bed8:53e2:5192:f265/64
docker0          DOWN           172.17.0.1/16 fe80::42:13ff:fee7:90d6/64
br-54cdc1101b1a  UP             10.9.0.1/24 fe80::42:1cff:fe17:f3e6/64
br-0569b491802f  UP             192.168.60.1/24 fe80::42:b5ff:fe9b:6b49/64
```

Packet Sniffing Using Scapy

```
#!/usr/bin/python3
from scapy.all import *

print("SNIFFING PACKETS.........")

def print_pkt(pkt):
   print("Source IP:", pkt[IP].src)
   print("Destination IP:", pkt[IP].dst)
   print("Protocol:", pkt[IP].proto)
   print("\n")

pkt = sniff(iface='br-b0cdc058d2ea', filter='icmp', prn=print_pkt)
```

BPF Rules

- Examples of pcap filters

```
dst host 10.0.2.5: only capture the packets going to 10.0.2.5.
src host 10.0.2.6: only capture the packets coming from 10.0.2.6.
host 10.0.2.6 and src port 9090: only capture the packets coming
        from or going to 10.0.2.6 with the source port being 9090.
tcp: only capture TCP packets.
```

- Refer to:

  http://biot.com/capstats/bpf.html

A Sniffer Example

```
def process_packet(pkt):
    if pkt.haslayer(IP):
       ip =  pkt[IP]
       print("IP: {} --> {}".format(ip.src, ip.dst))

    if pkt.haslayer(TCP):
       tcp = pkt[TCP]
       print("    TCP  port: {} --> {}".format(tcp.sport, tcp.dport))

    elif pkt.haslayer(UDP):
       udp = pkt[UDP]
       print("    UDP  port: {} --> {}".format(udp.sport, udp.dport))

    elif pkt.haslayer(ICMP):
       icmp = pkt[ICMP]
       print("    ICMP type: {}".format(icmp.type))

    else:
       print("    Other protocol")


sniff(iface='enp0s3', filter='ip', prn=process_packet)
```

Outline

- IP Address and Network Interface
- TCP/IP Protocols
- Programming Using Scapy
- Lab Environment and Containers
- Packet Sniffing
- Packet Spoofing

Packet Spoofing

- When some critical information in the packet is forged, we refer to it as packet spoofing.
- Many network attacks rely on packet spoofing.

Packet Spoofing

- In normal packet construction
  - Only some selected header fields can be set by users
  - OS set the other fields
- Packet spoofing
  - Set arbitrary header fields
  - Using tools
  - Using Scapy

Spoofing ICMP Using Scapy

```
#!/usr/bin/python3
from scapy.all import *

print("SENDING SPOOFED ICMP PACKET.........")
ip = IP(src="1.2.3.4", dst="93.184.216.34")
icmp = ICMP()
pkt = ip/icmp
pkt.show()
send(pkt,verbose=0)
```


Spoofing UDP Using Scapy

```
#!/usr/bin/python3
from scapy.all import *

print("SENDING SPOOFED UDP PACKET.........")
ip = IP(src="1.2.3.4", dst="10.0.2.69") # IP Layer
udp = UDP(sport=8888, dport=9090)       # UDP Layer
data = "Hello UDP!\n"                   # Payload
pkt = ip/udp/data
pkt.show()
send(pkt,verbose=0)
```


Sniff Request and Spoof Reply

- In many situations, attackers need to capture packets first, and then spoof a response based on the captured packets.
- Procedure (using scapy)
  - Use sniff to capture the packets of interests
  - Construct a spoofed packet based on the captured packet
  - Send out the spoofed reply

Sniffing and Then Spoofing Using Scapy

```
#!/usr/bin/python3
from scapy.all import *

def spoof_pkt(pkt):
  if UDP in pkt:
     print("Original Packet.........")
     print("Source IP : ", pkt[IP].src)
     print("Destination IP :", pkt[IP].dst)

     ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl, ttl=50)
     udp = UDP(sport=pkt[UDP].dport, dport=pkt[UDP].sport)
     data = "This is a spoofed reply!\n"

     newpkt = ip/udp/data

     print("Spoofed Packet.........")
     print("Source IP : ", newpkt[IP].src)
     print("Destination IP :", newpkt[IP].dst)

     send(newpkt,verbose=0)

pkt = sniff(iface='br-b0cdc058d2ea', filter='udp and src host 10.9.0.5',prn=spoof_pkt)
```


Sniffing/Spoofing Using C

- C is much faster
  - Author's experiment: 40 times faster
- Speed is important for some attacks
  - SYN flooding
  - DNS remote attack
- Covered in Chapter 4

Summary

- Understand high-level picture on how packets are constructed, sent, and received over the Internet.
- Become familiar with Scapy.
- Become familiar with Docker containers.
- Understand how packets can be sniffed and spoofed.