

Packet Capture using scapy

Steps:

- Open scapy in kali linux
- Start writing the code give
- And run the code it starts to capture the packets
- Open one more terminal and start to ping like i used google.com and to ping my ubuntu machine ip

```

Scapy 2.5.0+git20240324.2b58b51

File Actions Edit View Help

aspr//Vasa
ayyyyyCV/////////VCa
sV////////VSpCs scpCV//pp
ayp ayyyyyySCP//pp sy//C
AYAAAYYYYYYYYY//fpe sV//s
pCCCC//p cSpa y//Y
SPPPP//a pP//AC//Y
N/A cP//C
p//Nc ac//a
V//VSpCs A//A
scccccp//pSp//p B//Y
sV/////////y caa S//P
cayCypP//Ya pP/Ya
sV/PsV//VGC ac//Yp
sc sccaCV//PCypaayCP//Yss
spCP//////////VSpCs
ccacs

using IPython 8.20.0

>>> from scapy.all import sniff

...:
...: # Callback function that will be called for every captured packet
...: def packet_callback(packet):
...:     # Print out the entire packet
...:     pprint(packet.summary())
...:
...: # Function to capture packets
...: def capture_packets(interface="eth0", count=10):
...:     # (*Starting packet capture on interface) ... *)
...:     # Sniff packets and call the packet_callback for each packet
...:     sniff(iface=interface, count=count, prn=packet_callback)
...:
...: # Main execution
...: if __name__ == "__main__":
...:     # You can change the interface and count as needed
...:     capture_packets(interface="eth0", count=10)
...:
Starting packet capture on eth0 ...
Ether / IP / UDP / DNS Qry b'google.com.'
Ether / IP / UDP / DNS Qry b'google.com.'
Ether / ARP who has 192.168.100.5 says 192.168.100.1 / Padding
Ether / ARP is at 08:00:27:bac:e1:32 says 192.168.100.5
Ether / IP / UDP / DNS Ans 142.250.189.14
Ether / fe80::3e90:6e49:1ab2:342c > ff02::2 (58) / ICMPV6ND_RS
Ether / IP / UDP / DNS Ans 2007:f8b0:a007:80e::200e
Ether / IP / ICMP 192.168.100.5 > 142.250.189.14 echo-request 0 / Raw
Ether / IP / ICMP 142.250.189.14 > 192.168.100.5 echo-reply 0 / Raw
Ether / IP / UDP / DNS Qry b'14.189.250.142.in-addr.arpa.'
>>>

```

```

ramya@kali: ~
File Actions Edit View Help

--(ramya@kali):~--
$ wireshark
** (Wireshark:65586) 00:02:58.173885 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:65586) 00:02:58.228255 [Capture MESSAGE] -- Capture started
** (Wireshark:65586) 00:02:58.228286 [Capture MESSAGE] -- File: /tmp/wireshark_eth0X3CFU2.pcapng
^C

--(ramya@kali):~--
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.5 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:feba:e132 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bac:e1:32 txqueuelen 1000 (Ethernet)
    RX packets 443 bytes 42687 (41.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 480 bytes 38445 (37.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 88 bytes 4480 (4.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 4480 (4.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

--(ramya@kali):~--
$ ping google.com
PING goog1a.com (142.250.189.14) 56(84) bytes of data:
64 bytes from 142.250.189.14: icmp_seq=1 ttl=115 time=13.0 ms
64 bytes from 142.250.189.14: icmp_seq=2 ttl=115 time=12.2 ms
64 bytes from 142.250.189.14: icmp_seq=3 ttl=115 time=16.1 ms
64 bytes from 142.250.189.14: icmp_seq=4 ttl=115 time=16.1 ms
64 bytes from 142.250.189.14: icmp_seq=5 ttl=115 time=16.9 ms
^C
-- google.com ping statistics --
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 12.235/14.873/16.943/1.888 ms

--(ramya@kali):~--
$

```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 88 bytes 4480 (4.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 4480 (4.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

--(ramya@kali)-[~]
_
$ ping google.com
PING google.com (142.250.189.14) 56(84) bytes of data:
64 bytes from lax31s16-in-f14.1e100.net (142.250.189.14): icmp_seq=1 ttl=115 time=13.0 ms
64 bytes from lax31s16-in-f14.1e100.net (142.250.189.14): icmp_seq=2 ttl=115 time=12.2 ms
64 bytes from lax31s16-in-f14.1e100.net (142.250.189.14): icmp_seq=3 ttl=115 time=16.1 ms
64 bytes from lax31s16-in-f14.1e100.net (142.250.189.14): icmp_seq=4 ttl=115 time=16.1 ms
64 bytes from lax31s16-in-f14.1e100.net (142.250.189.14): icmp_seq=5 ttl=115 time=16.9 ms
^C
-- google.com ping statistics --
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 12.235/14.873/16.943/1.888 ms

--(ramya@kali)-[~]
_
$ ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data:
64 bytes from 192.168.100.4: icmp_seq=1 ttl=64 time=0.639 ms
64 bytes from 192.168.100.4: icmp_seq=2 ttl=64 time=0.757 ms
64 bytes from 192.168.100.4: icmp_seq=3 ttl=64 time=0.609 ms
^C
-- 192.168.100.4 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 201ms
rtt min/avg/max/mdev = 0.757/0.662/15.628/6.899 ms

--(ramya@kali)-[~]
_
$ ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data:
64 bytes from 192.168.100.4: icmp_seq=1 ttl=64 time=0.639 ms
64 bytes from 192.168.100.4: icmp_seq=2 ttl=64 time=0.691 ms
64 bytes from 192.168.100.4: icmp_seq=3 ttl=64 time=1.37 ms
64 bytes from 192.168.100.4: icmp_seq=4 ttl=64 time=0.780 ms
^C
-- 192.168.100.4 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.639/0.871/1.368/0.291 ms

--(ramya@kali)-[~]
_
$
```

```
File Actions Edit View Help

...: # Sniff packets and call the packet callback for each packet
...: sniff(iface=interface, count=count, prn=packet_callback)
...:
...: # Main execution
...: if __name__ == "__main__":
...:     # You can change the interface and count as needed
...:     capture_packets(interface="eth0", count=10)
...:
Starting packet capture on eth0...
Ether / IP / UDP / DNS Qry b'google.com.'
Ether / IP / UDP / DNS Qry b'google.com.'
Ether / ARP who has 192.168.100.5 says 192.168.100.1 / Padding
Ether / ARP is at 08:00:27:b4e1:12 says 192.168.100.5
Ether / IP / UDP / DNS Ans 142.250.189.14
Ether / fe80::3698:6a49:1ab2:342c > ff02::2 (58) / ICMPv6ND_RS
Ether / IP / UDP / DNS Ans 2607:f8b0:4007:a00::20b0
Ether / IP / ICMP 192.168.100.5 > 142.250.189.14 echo-request 0 / Raw
Ether / IP / ICMP 142.250.189.14 > 192.168.100.5 echo-reply 0 / Raw
Ether / IP / UDP / DNS Qry b'192.168.100.5 in-addr.arpa.'
>>> from scapy.all from sniff
...:
...: # Callback function that will be called for every captured packet
...: def packet_callback(packet):
...:     # Print out the entire packet
...:     print(packet.summary())
...:
...: # Function to capture packets
...: def capture_packets(interface="eth0", count=10):
...:     print(f"Starting packet capture on {interface} ...")
...:     # Sniff packets and call the packet callback for each packet
...:     sniff(iface=interface, count=count, prn=packet_callback)
...:
...: # Main execution
...: if __name__ == "__main__":
...:     # You can change the interface and count as needed
...:     capture_packets(interface="eth0", count=10)
...:
Starting packet capture on eth0...
Ether / IP / ICMP 192.168.100.5 > 192.168.100.4 echo-request 0 / Raw
Ether / IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.100.5 > 192.168.100.4 echo-request 0 / Raw
Ether / IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.100.5 > 192.168.100.4 echo-request 0 / Raw
Ether / IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Raw
Ether / IP / ICMP 192.168.100.5 > 192.168.100.4 echo-request 0 / Raw
Ether / IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Raw
Ether / ARP who has 192.168.100.4 says 192.168.100.5
Ether / ARP is at 08:00:27:ddaa:1d says 192.168.100.4 / Padding
>>>
```