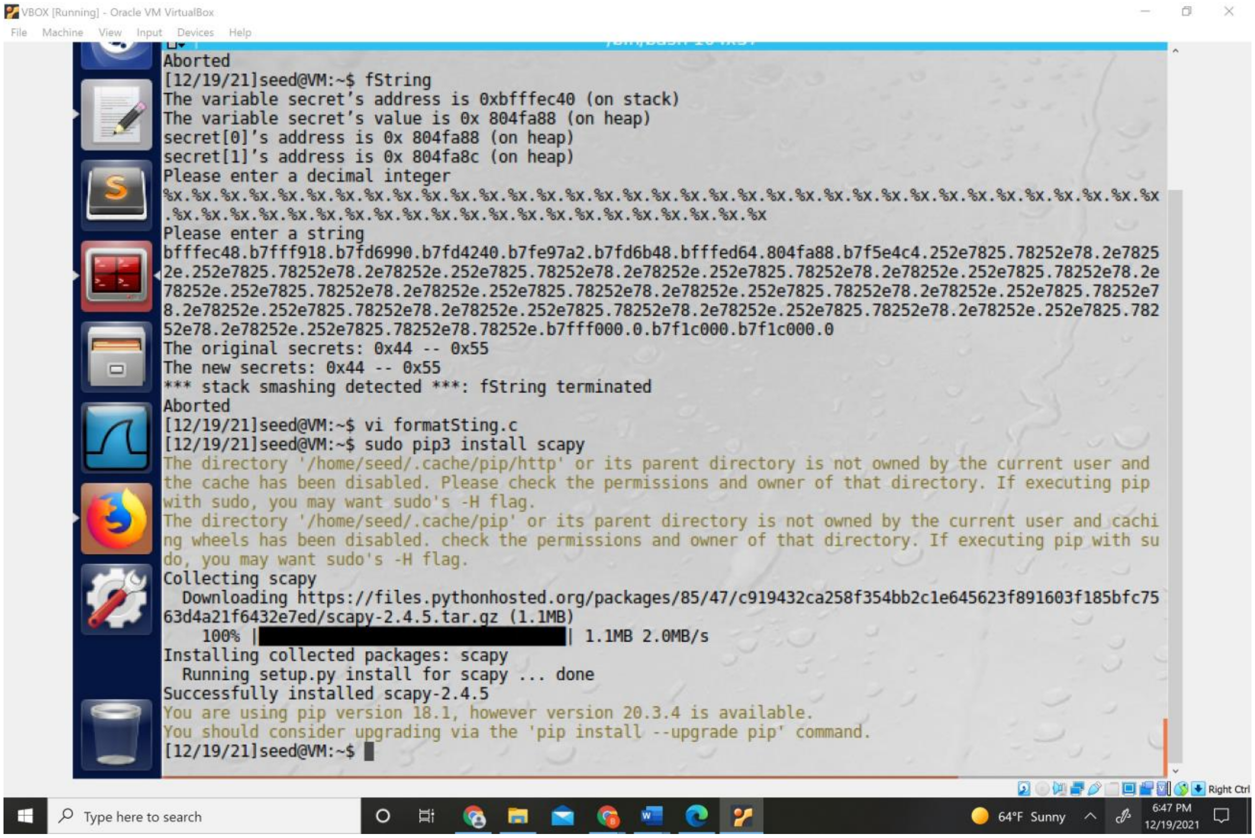
Ben Sottile

Sniffing and Spoofing

Lab Task Set 1 : Using Tools to Sniff and Spoof Packets

I downloaded scapy as requested

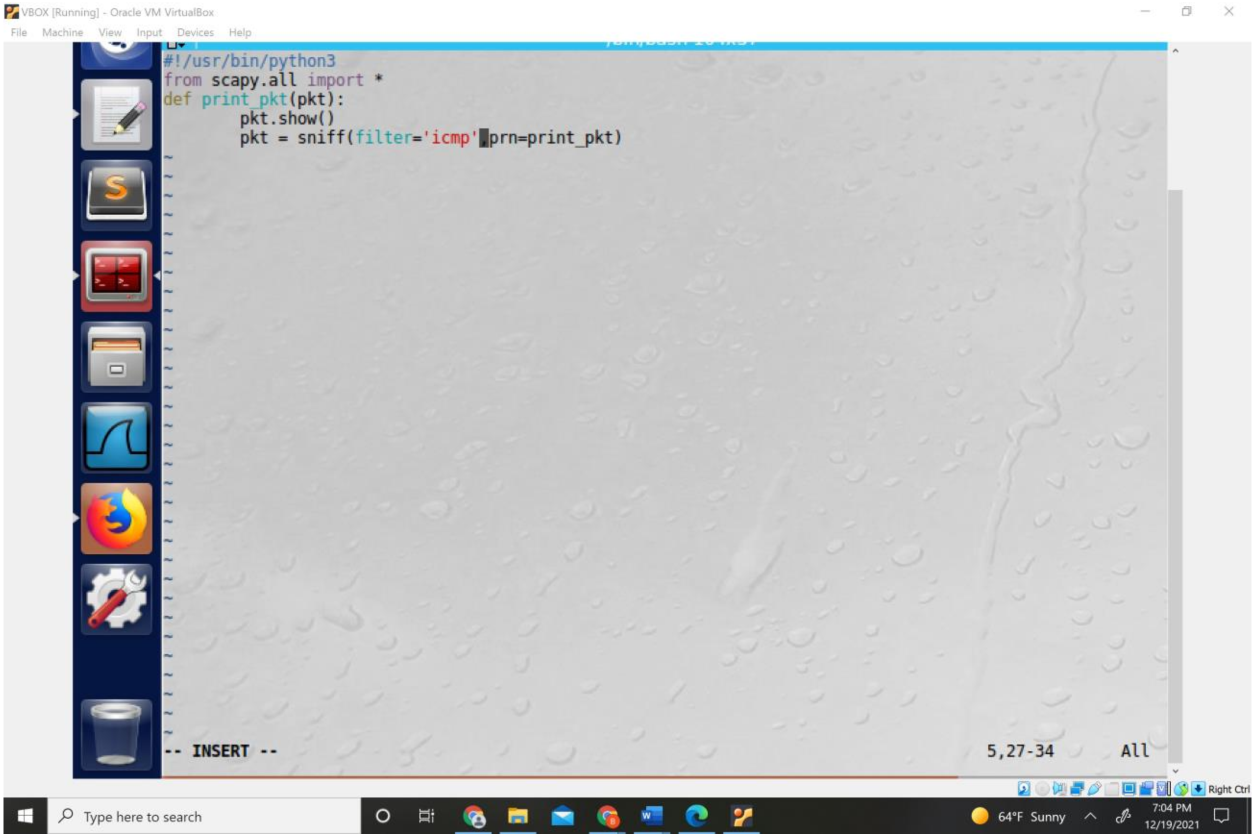


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Type here to search
64°F Sunny
6:47 PM
12/19/2021

```
Aborted
[12/19/21]seed@VM:~$ fString
The variable secret’s address is 0xbfffec40 (on stack)
The variable secret’s value is 0x 804fa88 (on heap)
secret[0]’s address is 0x 804fa88 (on heap)
secret[1]’s address is 0x 804fa8c (on heap)
Please enter a decimal integer
%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x
.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x
Please enter a string
bfffec48.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bfffed64.804fa88.b7f5e4c4.252e7825.78252e78.2e7825
2e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e
78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e7
8.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.782
52e78.2e78252e.252e7825.78252e78.78252e.b7fff000.0.b7f1c000.b7f1c000.0
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
*** stack smashing detected ***: fString terminated
Aborted
[12/19/21]seed@VM:~$ vi formatSting.c
[12/19/21]seed@VM:~$ sudo pip3 install scapy
The directory '/home/seed/.cache/pip/http' or its parent directory is not owned by the current user and
the cache has been disabled. Please check the permissions and owner of that directory. If executing pip
with sudo, you may want sudo's -H flag.
The directory '/home/seed/.cache/pip' or its parent directory is not owned by the current user and cachi
ng wheels has been disabled. check the permissions and owner of that directory. If executing pip with su
do, you may want sudo's -H flag.
Collecting scapy
  Downloading https://files.pythonhosted.org/packages/85/47/c919432ca258f354bb2c1e645623f891603f185bfc75
63d4a21f6432e7ed/scapy-2.4.5.tar.gz (1.1MB)
    100% |████████████████████████████████| 1.1MB 2.0MB/s
Installing collected packages: scapy
  Running setup.py install for scapy ... done
Successfully installed scapy-2.4.5
You are using pip version 18.1, however version 20.3.4 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
[12/19/21]seed@VM:~$ █
```

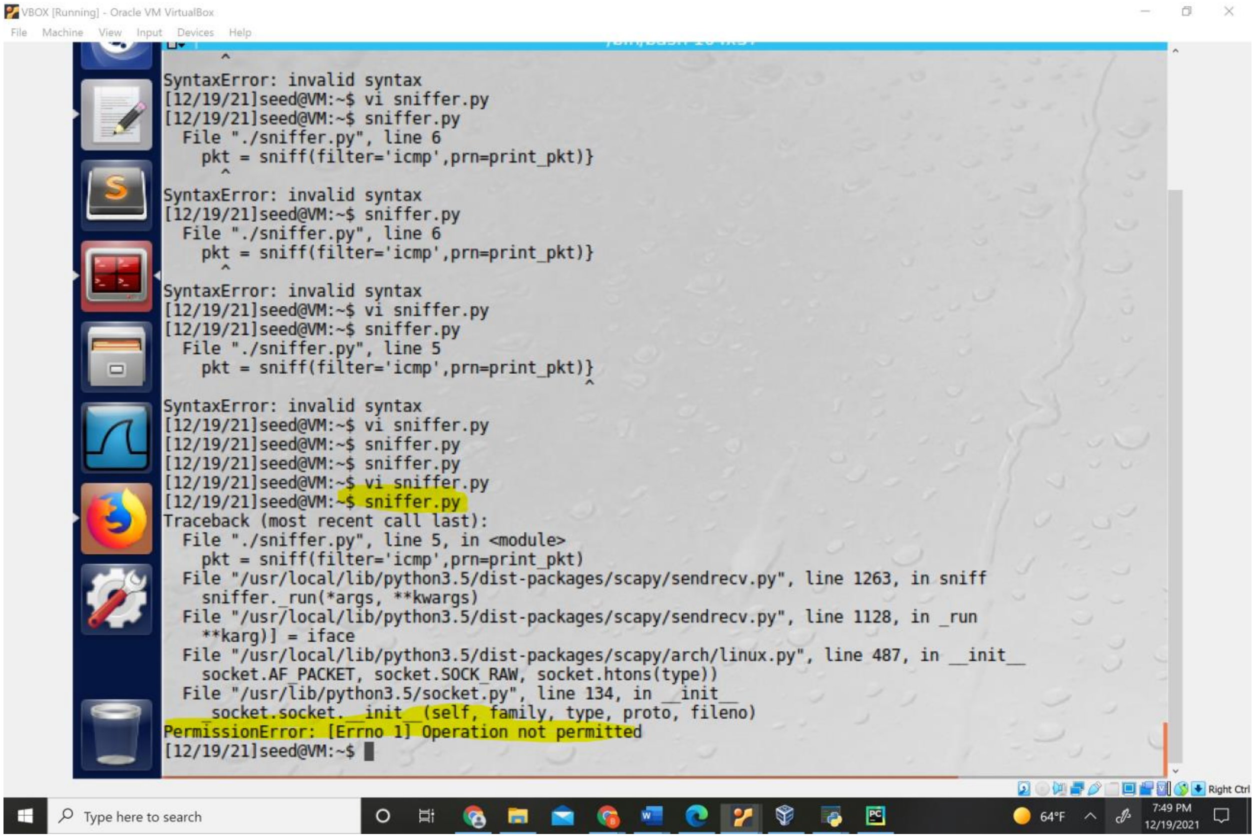
Copy pasted code from assignment into program called simpleSniffer.py

Single quotes need to be changed out



```
#!/usr/bin/python3
from scapy.all import *
def print_pkt(pkt):
        pkt.show()
        pkt = sniff(filter='icmp',prn=print_pkt)
~
~
-- INSERT --                                                  5,27-34       All
```

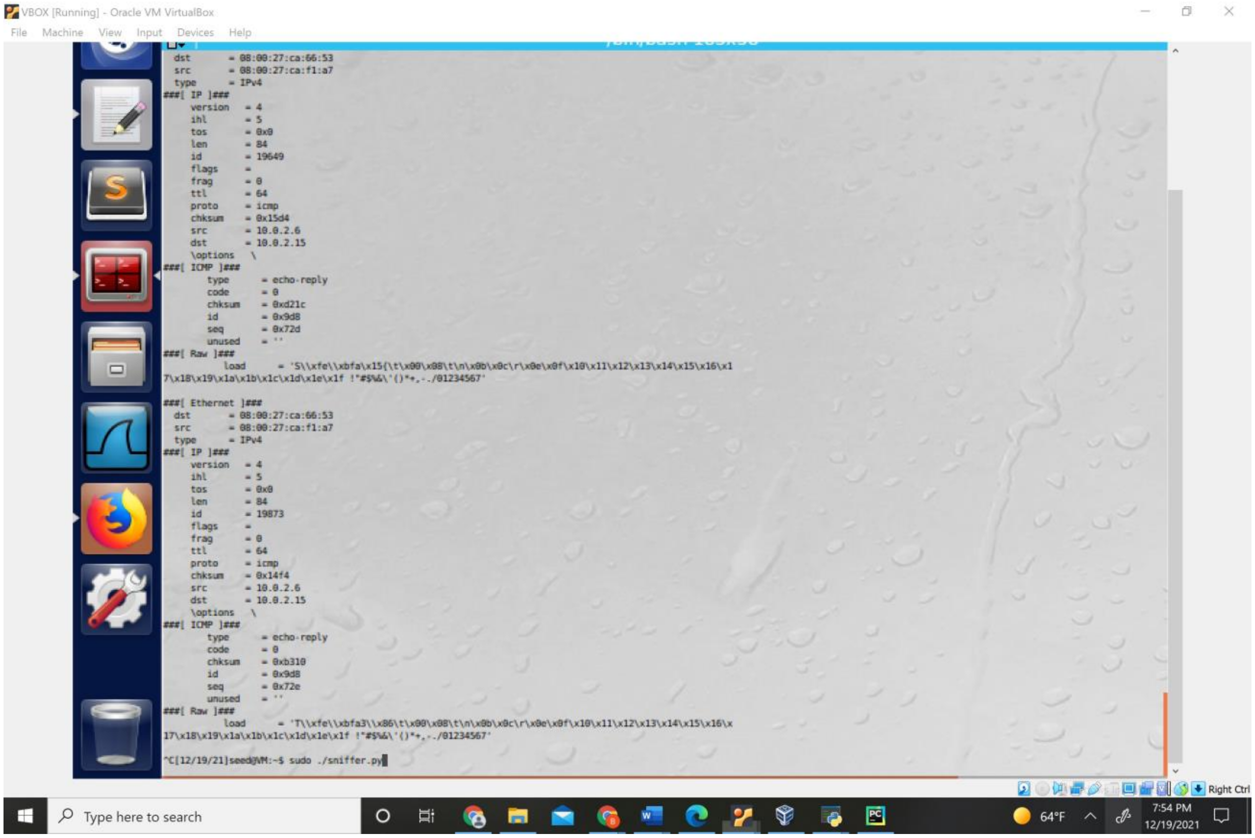
Ran without sudo



VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Type here to search
64°F
7:49 PM
12/19/2021

```
      ^
SyntaxError: invalid syntax
[12/19/21]seed@VM:~$ vi sniffer.py
[12/19/21]seed@VM:~$ sniffer.py
  File "./sniffer.py", line 6
    pkt = sniff(filter='icmp',prn=print_pkt)}
      ^
SyntaxError: invalid syntax
[12/19/21]seed@VM:~$ sniffer.py
  File "./sniffer.py", line 6
    pkt = sniff(filter='icmp',prn=print_pkt)}
      ^
SyntaxError: invalid syntax
[12/19/21]seed@VM:~$ vi sniffer.py
[12/19/21]seed@VM:~$ sniffer.py
  File "./sniffer.py", line 5
    pkt = sniff(filter='icmp',prn=print_pkt)}
                                            ^
SyntaxError: invalid syntax
[12/19/21]seed@VM:~$ vi sniffer.py
[12/19/21]seed@VM:~$ sniffer.py
[12/19/21]seed@VM:~$ sniffer.py
[12/19/21]seed@VM:~$ vi sniffer.py
[12/19/21]seed@VM:~$ sniffer.py
Traceback (most recent call last):
  File "./sniffer.py", line 5, in <module>
    pkt = sniff(filter='icmp',prn=print_pkt)
  File "/usr/local/lib/python3.5/dist-packages/scapy/sendrecv.py", line 1263, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.5/dist-packages/scapy/sendrecv.py", line 1128, in _run
    **karg)] = iface
  File "/usr/local/lib/python3.5/dist-packages/scapy/arch/linux.py", line 487, in __init__
    socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))
  File "/usr/lib/python3.5/socket.py", line 134, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[12/19/21]seed@VM:~$ 
```

Ran with sudo – Returned an IMMENSE volume of data. So much so you can't even scroll it. One of the reasons, it generated so much was because on of my other two VMs was pinging another machine.



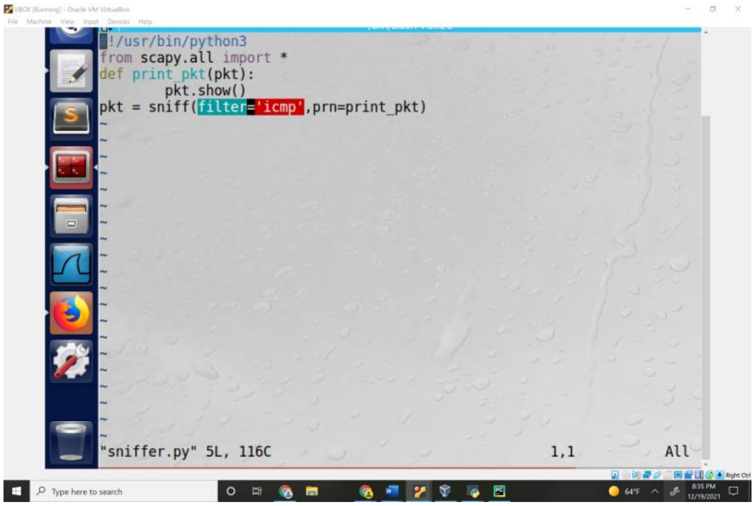
VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search
64°F
7:54 PM
12/19/2021
Right Ctrl

```
  dst       = 08:00:27:ca:66:53
  src       = 08:00:27:ca:f1:a7
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 19649
     flags     =
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x15d4
     src       = 10.0.2.6
     dst       = 10.0.2.15
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0xd21c
        id        = 0x9d8
        seq       = 0x72d
        unused    = ''
###[ Raw ]###
           load      = 'S\\xfe\\xbfa\x15{\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x1
7\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 08:00:27:ca:66:53
  src       = 08:00:27:ca:f1:a7
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 19873
     flags     =
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x14f4
     src       = 10.0.2.6
     dst       = 10.0.2.15
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0xb310
        id        = 0x9d8
        seq       = 0x72e
        unused    = ''
###[ Raw ]###
           load      = 'T\\xfe\\xbfa3\\x86\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x
17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

^C[12/19/21]seed@VM:~$ sudo ./sniffer.py
```

Capture only the ICMP packet(Default)

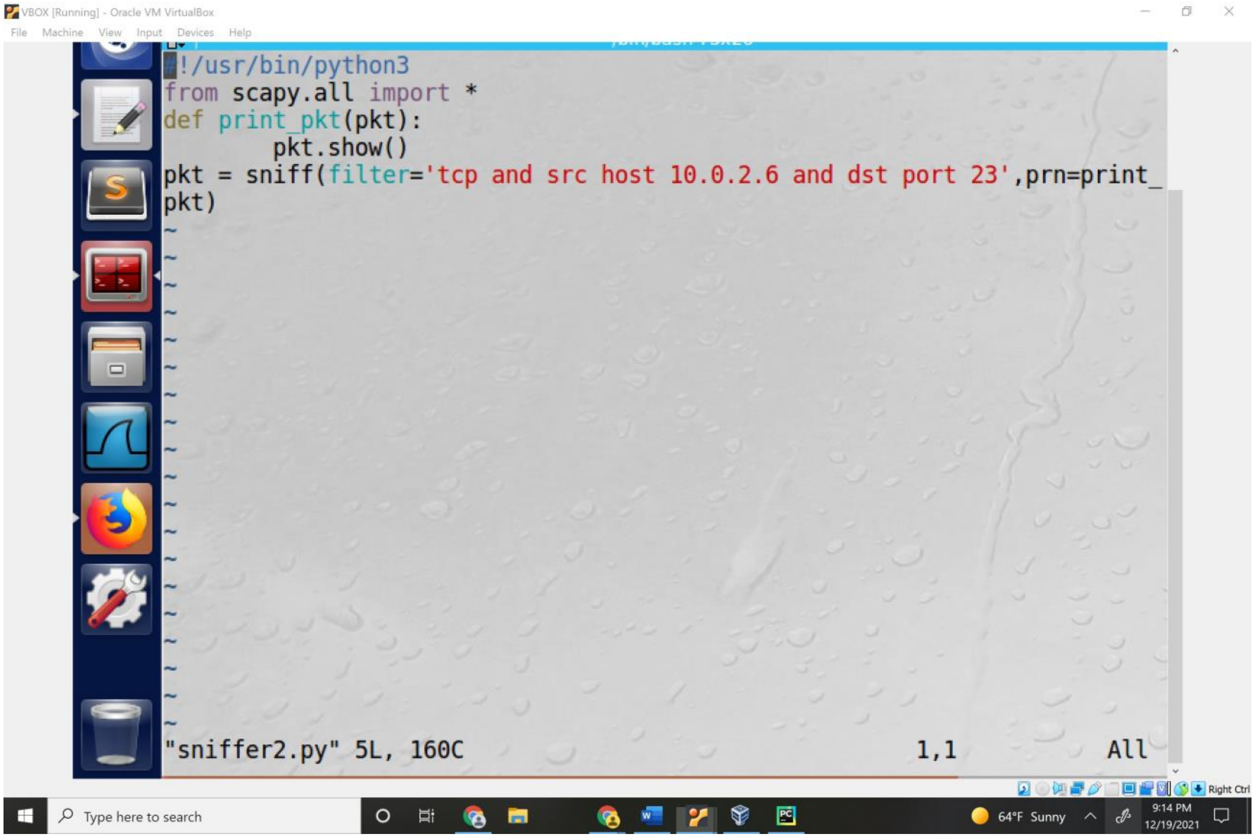


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search
64°F
8:35 PM
12/19/2021
Right Ctrl

```
#!/usr/bin/python3
from scapy.all import *
def print_pkt(pkt):
        pkt.show()
pkt = sniff(filter='icmp',prn=print_pkt)
~
"sniffer.py" 5L, 116C                                 1,1           All
```

Capture any TCP packet that comes from a particular IP and with a destination port number 23.

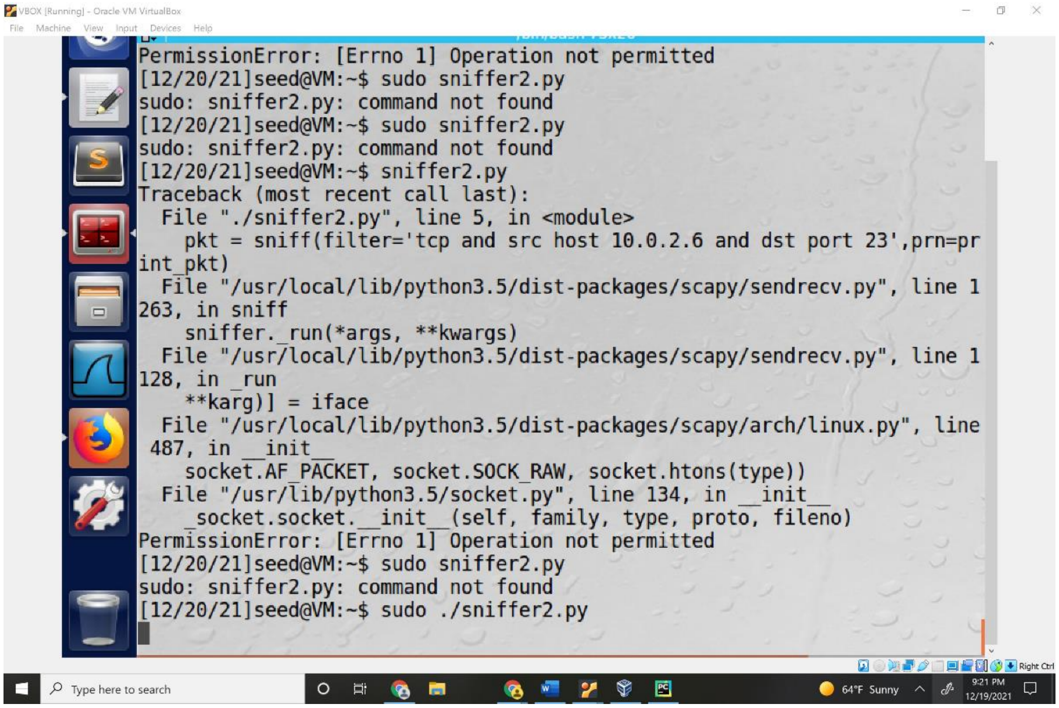
I chose 10.0.2.6/23 because it was a IP in my VM network


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search
64°F Sunny
Right Ctrl
9:14 PM
12/19/2021

```
#!/usr/bin/python3
from scapy.all import *
def print_pkt(pkt):
        pkt.show()
pkt = sniff(filter='tcp and src host 10.0.2.6 and dst port 23',prn=print_
pkt)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"sniffer2.py" 5L, 160C                                    1,1           All
```

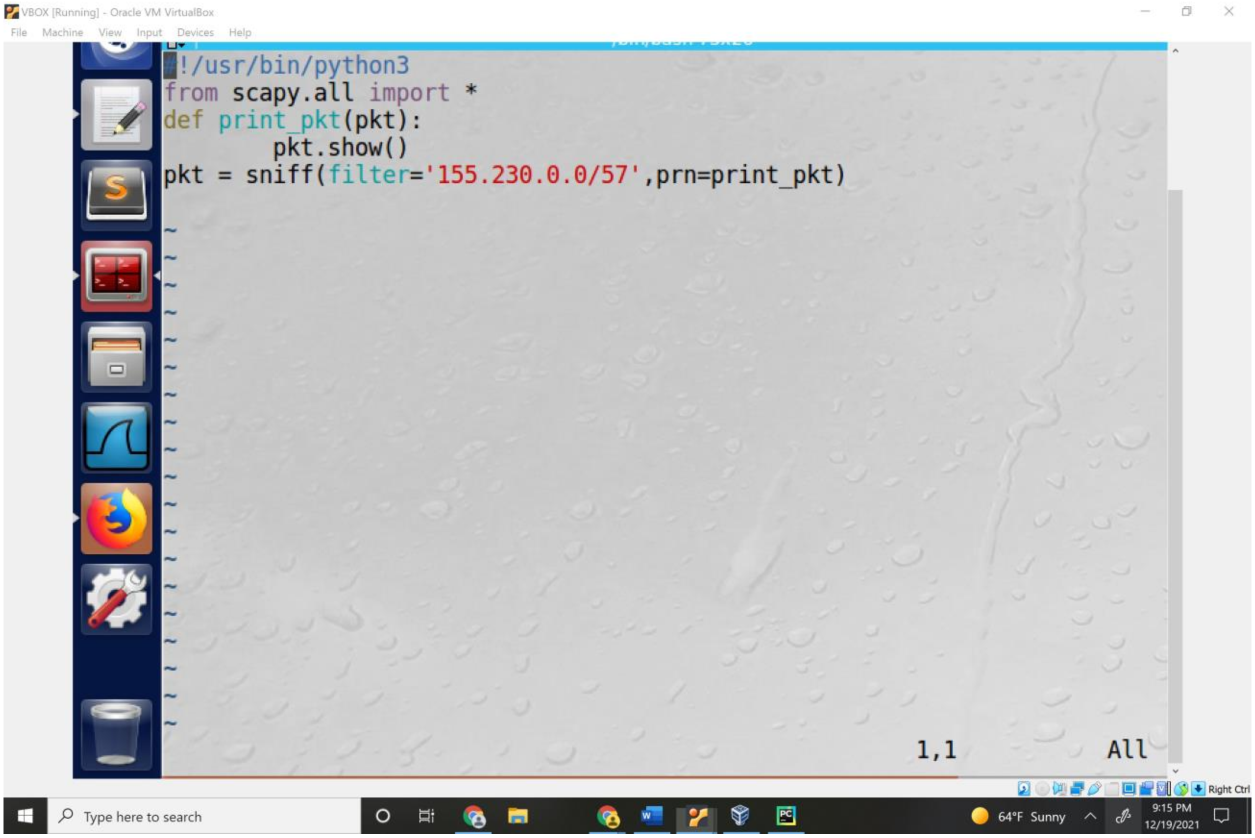
I did some research at figured a correct filter.

Test


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search
64°F Sunny
Right Ctrl
9:21 PM
12/19/2021

```
PermissionError: [Errno 1] Operation not permitted
[12/20/21]seed@VM:~$ sudo sniffer2.py
sudo: sniffer2.py: command not found
[12/20/21]seed@VM:~$ sudo sniffer2.py
sudo: sniffer2.py: command not found
[12/20/21]seed@VM:~$ sniffer2.py
Traceback (most recent call last):
  File "./sniffer2.py", line 5, in <module>
    pkt = sniff(filter='tcp and src host 10.0.2.6 and dst port 23',prn=pr
int_pkt)
  File "/usr/local/lib/python3.5/dist-packages/scapy/sendrecv.py", line 1
263, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.5/dist-packages/scapy/sendrecv.py", line 1
128, in _run
    **karg)] = iface
  File "/usr/local/lib/python3.5/dist-packages/scapy/arch/linux.py", line
 487, in __init__
    socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))
  File "/usr/lib/python3.5/socket.py", line 134, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[12/20/21]seed@VM:~$ sudo sniffer2.py
sudo: sniffer2.py: command not found
[12/20/21]seed@VM:~$ sudo ./sniffer2.py
```

Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 155.230.0.0/57; you should not pick the subnet that your VM is attached to.

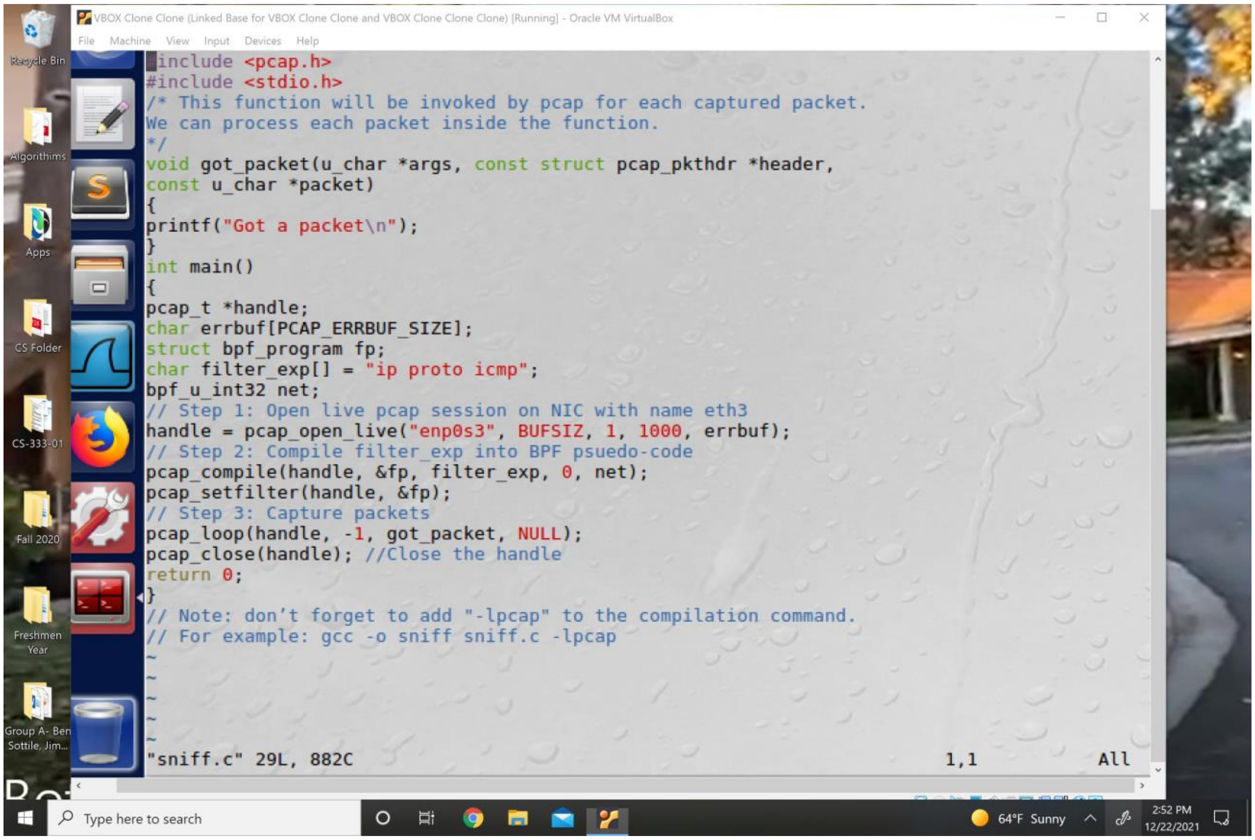


```
#!/usr/bin/python3
from scapy.all import *
def print_pkt(pkt):
        pkt.show()
pkt = sniff(filter='155.230.0.0/57',prn=print_pkt)
```

VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1,1
All
Right Ctrl
Type here to search
64°F Sunny
9:15 PM
12/19/2021

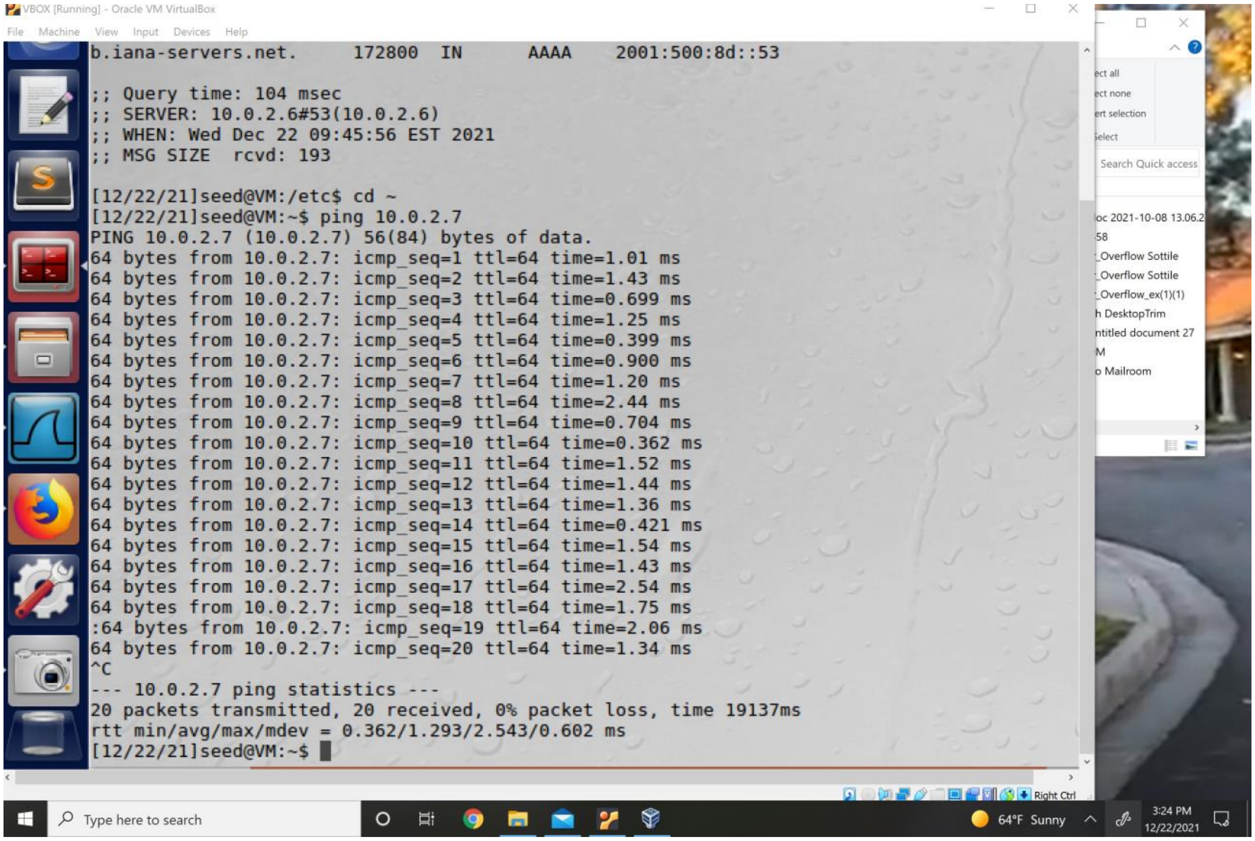
Lab Task 2

Writing a packet sniffing program



VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Algorithims
Apps
CS Folder
CS-333-01
Fall 2020
Freshmen Year
Group A- Ben Sottile, Jim...
Type here to search
64°F Sunny
2:52 PM
12/22/2021

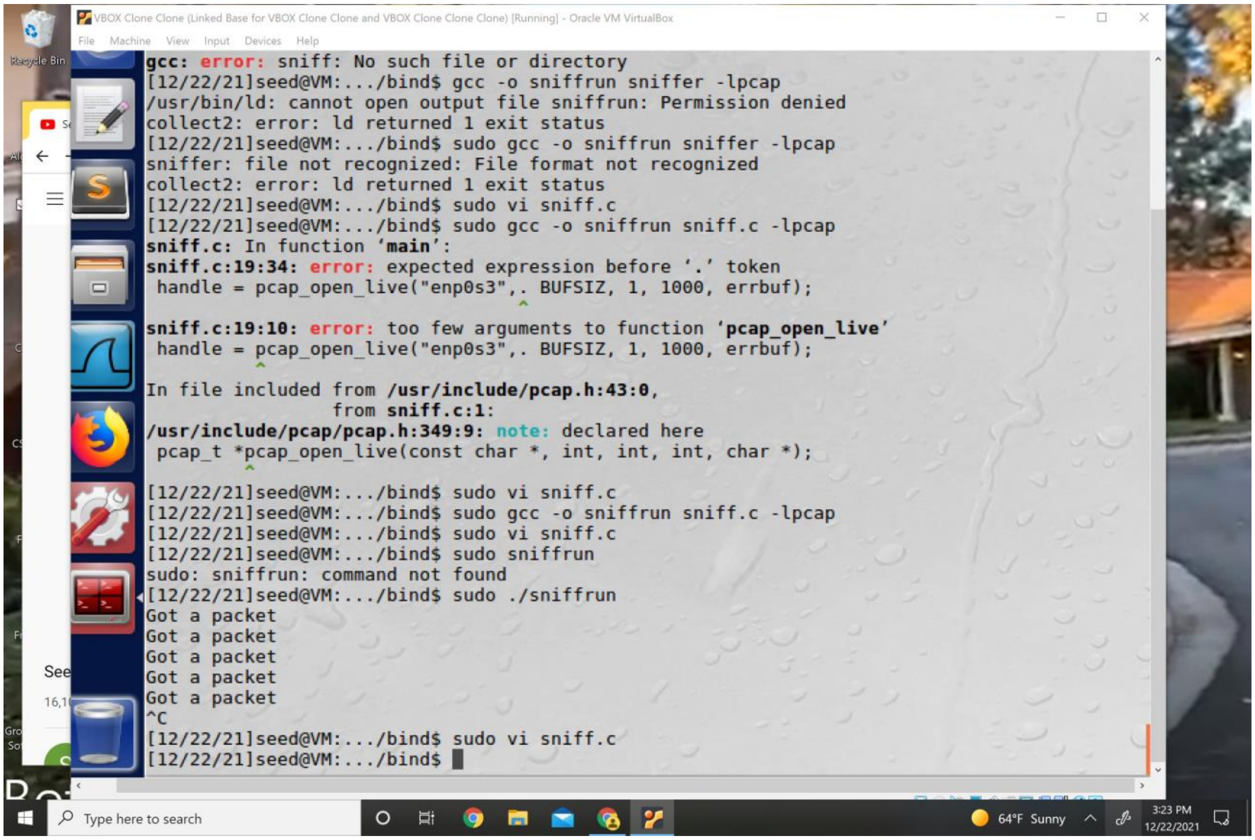
```
#include <pcap.h>
#include <stdio.h>
/* This function will be invoked by pcap for each captured packet.
We can process each packet inside the function.
*/
void got_packet(u_char *args, const struct pcap_pkthdr *header,
const u_char *packet)
{
printf("Got a packet\n");
}
int main()
{
pcap_t *handle;
char errbuf[PCAP_ERRBUF_SIZE];
struct bpf_program fp;
char filter_exp[] = "ip proto icmp";
bpf_u_int32 net;
// Step 1: Open live pcap session on NIC with name eth3
handle = pcap_open_live("enp0s3", BUFSIZ, 1, 1000, errbuf);
// Step 2: Compile filter_exp into BPF psuedo-code
pcap_compile(handle, &fp, filter_exp, 0, net);
pcap_setfilter(handle, &fp);
// Step 3: Capture packets
pcap_loop(handle, -1, got_packet, NULL);
pcap_close(handle); //Close the handle
return 0;
}
// Note: don't forget to add "-lpcap" to the compilation command.
// For example: gcc -o sniff sniff.c -lpcap
~
~
~
~
~
"sniff.c" 29L, 882C                                        1,1           All
```



```
b.iana-servers.net.     172800  IN      AAAA    2001:500:8d::53

;; Query time: 104 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Dec 22 09:45:56 EST 2021
;; MSG SIZE  rcvd: 193

[12/22/21]seed@VM:/etc$ cd ~
[12/22/21]seed@VM:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 10.0.2.7: icmp_seq=3 ttl=64 time=0.699 ms
64 bytes from 10.0.2.7: icmp_seq=4 ttl=64 time=1.25 ms
64 bytes from 10.0.2.7: icmp_seq=5 ttl=64 time=0.399 ms
64 bytes from 10.0.2.7: icmp_seq=6 ttl=64 time=0.900 ms
64 bytes from 10.0.2.7: icmp_seq=7 ttl=64 time=1.20 ms
64 bytes from 10.0.2.7: icmp_seq=8 ttl=64 time=2.44 ms
64 bytes from 10.0.2.7: icmp_seq=9 ttl=64 time=0.704 ms
64 bytes from 10.0.2.7: icmp_seq=10 ttl=64 time=0.362 ms
64 bytes from 10.0.2.7: icmp_seq=11 ttl=64 time=1.52 ms
64 bytes from 10.0.2.7: icmp_seq=12 ttl=64 time=1.44 ms
64 bytes from 10.0.2.7: icmp_seq=13 ttl=64 time=1.36 ms
64 bytes from 10.0.2.7: icmp_seq=14 ttl=64 time=0.421 ms
64 bytes from 10.0.2.7: icmp_seq=15 ttl=64 time=1.54 ms
64 bytes from 10.0.2.7: icmp_seq=16 ttl=64 time=1.43 ms
64 bytes from 10.0.2.7: icmp_seq=17 ttl=64 time=2.54 ms
64 bytes from 10.0.2.7: icmp_seq=18 ttl=64 time=1.75 ms
:64 bytes from 10.0.2.7: icmp_seq=19 ttl=64 time=2.06 ms
64 bytes from 10.0.2.7: icmp_seq=20 ttl=64 time=1.34 ms
^C
--- 10.0.2.7 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19137ms
rtt min/avg/max/mdev = 0.362/1.293/2.543/0.602 ms
[12/22/21]seed@VM:~$ 
```


VBOX Clone Clone (Linked Base for VBOX Clone Clone and VBOX Clone Clone Clone) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Recycle Bin
Type here to search
64°F Sunny
3:23 PM
12/22/2021

```
gcc: error: sniff: No such file or directory
[12/22/21]seed@VM:.../bind$ gcc -o sniffrun sniffer -lpcap
/usr/bin/ld: cannot open output file sniffrun: Permission denied
collect2: error: ld returned 1 exit status
[12/22/21]seed@VM:.../bind$ sudo gcc -o sniffrun sniffer -lpcap
sniffer: file not recognized: File format not recognized
collect2: error: ld returned 1 exit status
[12/22/21]seed@VM:.../bind$ sudo vi sniff.c
[12/22/21]seed@VM:.../bind$ sudo gcc -o sniffrun sniff.c -lpcap
sniff.c: In function ‘main’:
sniff.c:19:34: error: expected expression before ‘.’ token
 handle = pcap_open_live("enp0s3",. BUFSIZ, 1, 1000, errbuf);
                                  ^

sniff.c:19:10: error: too few arguments to function ‘pcap_open_live’
 handle = pcap_open_live("enp0s3",. BUFSIZ, 1, 1000, errbuf);
          ^

In file included from /usr/include/pcap.h:43:0,
                 from sniff.c:1:
/usr/include/pcap/pcap.h:349:9: note: declared here
 pcap_t *pcap_open_live(const char *, int, int, int, char *);
         ^

[12/22/21]seed@VM:.../bind$ sudo vi sniff.c
[12/22/21]seed@VM:.../bind$ sudo gcc -o sniffrun sniff.c -lpcap
[12/22/21]seed@VM:.../bind$ sudo vi sniff.c
[12/22/21]seed@VM:.../bind$ sudo sniffrun
sudo: sniffrun: command not found
[12/22/21]seed@VM:.../bind$ sudo ./sniffrun
Got a packet
Got a packet
Got a packet
Got a packet
Got a packet
^C
[12/22/21]seed@VM:.../bind$ sudo vi sniff.c
[12/22/21]seed@VM:.../bind$ 
```