

ECE 471 Lab 5

Packet Sniffing and Spoofing Lab / ARP Cache Poisoning Attack Lab

Mitchell Dzurick

4/15/2020

Github with all documentation - <https://www.github.com/mitchdz/ECE471>

Contents

1	Packet Sniffing and Spoofing Lab	2
1.1	Task 1.1: Sniffing Packets	2
1.1.1	Task 1.1A	2
1.1.2	Task 1.1b	2
1.2	Task 1.2: Spoofing ICMP Packets	2
1.3	Task 1.4: Sniffing and-then Spoofing (Extra Credit)	2
2	ARPCache Poisoning Attack Lab	2
2.1	Task 2.1: ARP Cache Poisoning	2

1 Packet Sniffing and Spoofing Lab

1.1 Task 1.1: Sniffing Packets

1.1.1 Task 1.1A

The program is created below:

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

def print_pkt(pkt):
    pkt.show()

pkt = sniff(filter='icmp',prn=print_pkt)
```

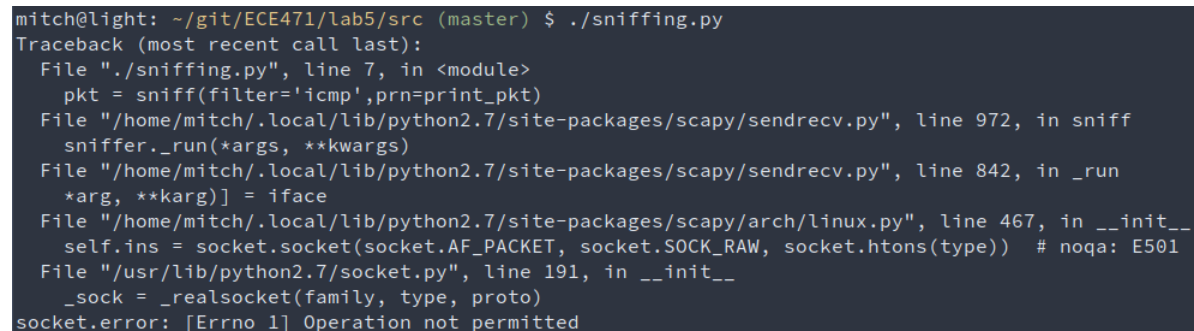
This code is placed into a file named sniffing.py and made executable with the following command

```
$ sudo chown +x sniffing.py
```

The code can then be ran with the following command

```
$ ./sniffing.py
```

The output is as follows:

A screenshot of a terminal window with a dark background. The prompt is 'mitch@light: ~/git/ECE471/lab5/src (master)'. The user has entered './sniffing.py'. The output shows a 'Traceback (most recent call last):' followed by several lines of file paths and line numbers, ending with 'socket.error: [Errno 1] Operation not permitted'.

```
mitch@light: ~/git/ECE471/lab5/src (master) $ ./sniffing.py
Traceback (most recent call last):
  File "./sniffing.py", line 7, in <module>
    pkt = sniff(filter='icmp',prn=print_pkt)
  File "/home/mitch/.local/lib/python2.7/site-packages/scapy/sendrecv.py", line 972, in sniff
    sniffer._run(*args, **kwargs)
  File "/home/mitch/.local/lib/python2.7/site-packages/scapy/sendrecv.py", line 842, in _run
    *arg, **karg)] = iface
  File "/home/mitch/.local/lib/python2.7/site-packages/scapy/arch/linux.py", line 467, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type)) # noqa: E501
  File "/usr/lib/python2.7/socket.py", line 191, in __init__
    _sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
```

Figure 1: Running the sniffing program without root

1.1.2 Task 1.1b

1.2 Task 1.2: Spoofing ICMP Packets

1.3 Task 1.4: Sniffing and-then Spoofing (Extra Credit)

2 ARPCache Poisoning Attack Lab

2.1 Task 2.1: ARP Cache Poisoning