RTR IP and MAC addresses

```
Connected (unencrypted) to: Xen-rtr_new_base135
          TX packets:417 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7661 (7.4 KiB)  TX bytes:33553 (32.7 KiB)
          Interrupt:32 Base address:0xe000

eth1      Link encap:Ethernet  HWaddr 02:00:87:62:07:02
          inet addr:10.10.111.1  Bcast:10.10.111.255  Mask:255.255.255.0
          inet6 addr: fe80::87ff:fe62:702/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10645 (10.3 KiB)  TX bytes:2332 (2.2 KiB)
          Interrupt:36 Base address:0x100
```

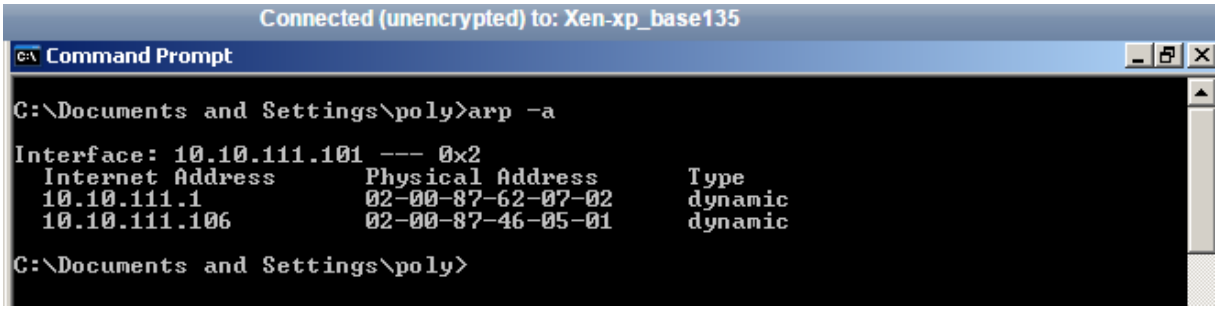
RTR ARP table

```
Connected (unencrypted) to: Xen-rtr_new_base135
router:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.10.111.101            ether   02:00:87:7e:09:01   C                     eth1
10.12.1.1                ether   00:30:48:be:c8:31   C                     eth0
10.10.111.106            ether   02:00:87:46:05:01   C                     eth1
router:~# _
```

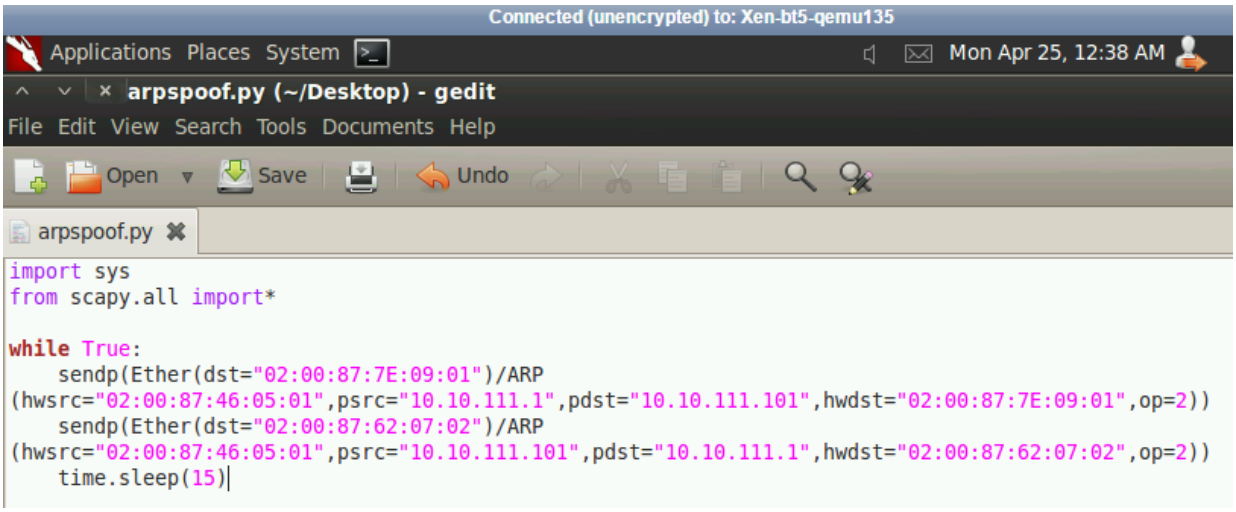
XP IP and MAC addresses

```
Connected (unencrypted) to: Xen-xp_base135
Command Prompt

Windows IP Configuration

        Host Name . . . . . . . . . . . . : victim1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : vlab.local
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 02-00-87-7E-09-01
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.10.111.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.10.111.1
        DHCP Server . . . . . . . . . . . : 10.10.111.1
        DNS Servers . . . . . . . . . . . : 10.10.111.1
        Lease Obtained. . . . . . . . . . : Monday, April 25, 2016 4:31:14 AM
        Lease Expires . . . . . . . . . . : Monday, April 25, 2016 5:31:14 AM

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

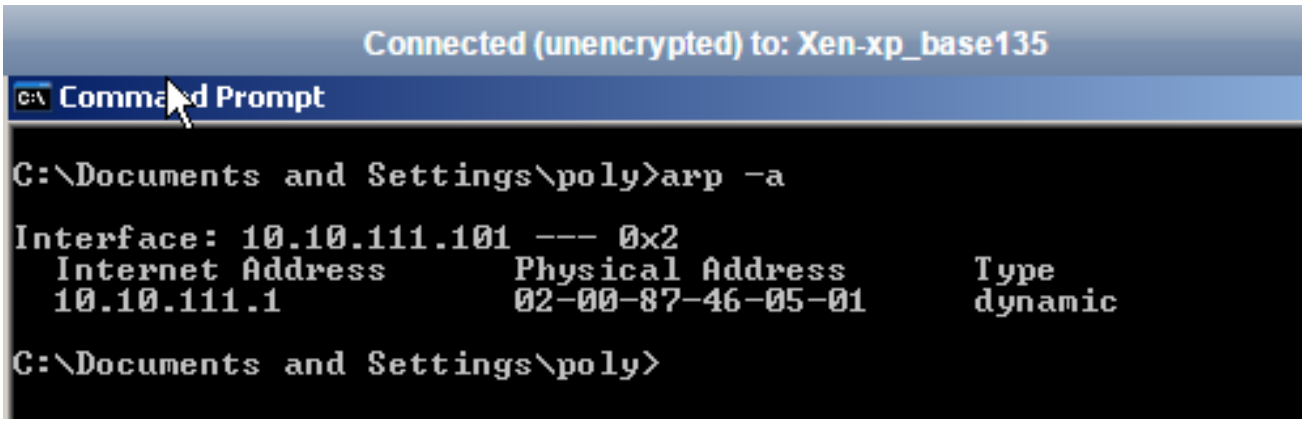
XP ARP table



1. Write a SCAPY program on BT5 that sends gratuitous ARPs to XP and rtr so that BT5 is in the middle of the communication between rtr and XP.



2. Show the results of successful ARP spoofing by taking screenshots showing the output of the arp command.
   After running the script above from BT5, the ARP entries in XP machines looks like:



RTR machine ARP looks like:

```
Connected (unencrypted) to: Xen-rtr_new_base135
router:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.10.111.101            ether   02:00:87:46:05:01   C                     eth1
10.12.1.1                ether   00:30:48:be:c8:31   C                     eth0
10.10.111.106            ether   02:00:87:46:05:01   C                     eth1
10.12.1.10               ether   02:00:0b:a4:3e:02   C                     eth0
router:~# _
```

This causes ARP poisoning.

3. Perform sslstrip attack on the client accessing Fakebook.

```
Connected (unencrypted) to: Xen-bt5-qemu135
System >_                                   Mon Apr 25, 12:47 AM
root@bt: /pentest/web/sslstrip
File Edit View Terminal Help

sslstrip 0.8 by Moxie Marlinspike
Usage: sslstrip <options>

Options:
-w <filename>, --write=<filename> Specify file to log to (optional).
-p , --post                       Log only SSL POSTs. (default)
-s , --ssl                        Log all SSL traffic to and from server.
-a , --all                        Log all SSL and HTTP traffic to and from serve
r.
-l <port>, --listen=<port>        Port to listen on (default 10000).
-f , --favicon                    Substitute a lock favicon on secure requests.
-k , --killsessions               Kill sessions in progress.
-h                                Print this help message.

root@bt:/pentest/web/sslstrip# python sslstrip.py -l 8080

sslstrip 0.8 by Moxie Marlinspike running...
```

4. Record the new FORM post method and explain what is different.
   Before running SSL strip the page source looks like:

Connected (unencrypted) to: Xen-bt5-qemu135

Applications Places System

Fakebook - Mozilla Firefox

Source of: http://fakebook.vlab.local/ - Mozilla Firefox

File Edit View Help

```
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta http-equiv="Content-language" content="en" />
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
<meta name="description" content=" Fakebook is a social utility that connects people wit
<title>Fakebook</title>
<script type="text/javascript" src="hint-textbox.js"></script>
</head>
<body background="background.png" >
<style type="text/css">
<!--
body {background-image: url(background.png); background-repeat: no-repeat;}
INPUT.hintTextbox { color: #888; }
INPUT.hintTextboxActive { color: #000; }
}
-->
</style>
<div align=right style="width: 600px ">
<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" size="8" onFocus
</form>
</div>

</body>
</html>
```

After running SSLstrip, it looks as:

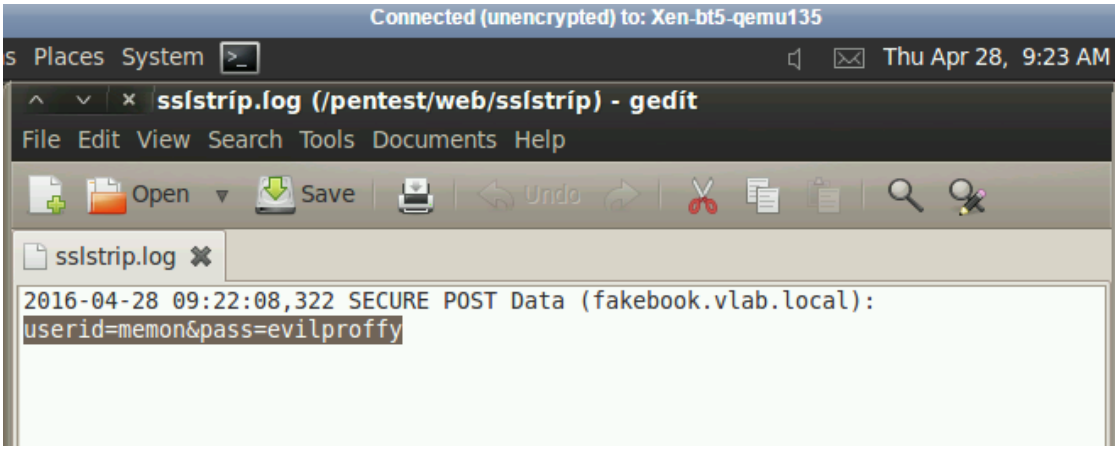
Connected (unencrypted) to: Xen-xp_base135

Source of: http://fakebook.vlab.local/ - Mozilla Firefox

File Edit View Help

```
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
<meta name="description" content=" Fakebook is a social utility that connect
<title>Fakebook</title>
<script type="text/javascript" src="hint-textbox.js"></script>
</head>
<body background="background.png" >
<style type="text/css">
<!--
body {background-image: url(background.png); background-repeat: no-repeat;}
INPUT.hintTextbox { color: #888; }
INPUT.hintTextboxActive { color: #000; }
}
-->
</style>
<div align=right style="width: 600px ">
<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
</form>
</div>

</body>
</html>
```

5. Open this log file in your favorite text editor and find and record the captured login and passwords.



6. Fully explain in a paragraph or two how sslstrip works.
First, arpspoof convinces a host that our MAC address is the router's MAC address, and the target begins to send us all its network traffic. The kernel forwards everything along except for traffic destined to port 80, which it redirects to 8080.
Any request through XP machine to RTR is sent via BT5 which changes the connection between XP and BT5 to http instead of https and from BT5 to RTR as a normal connection i.e., https.
The SSLstrip is running which is listening at port 8080 and logs down in SSLstrip.log .