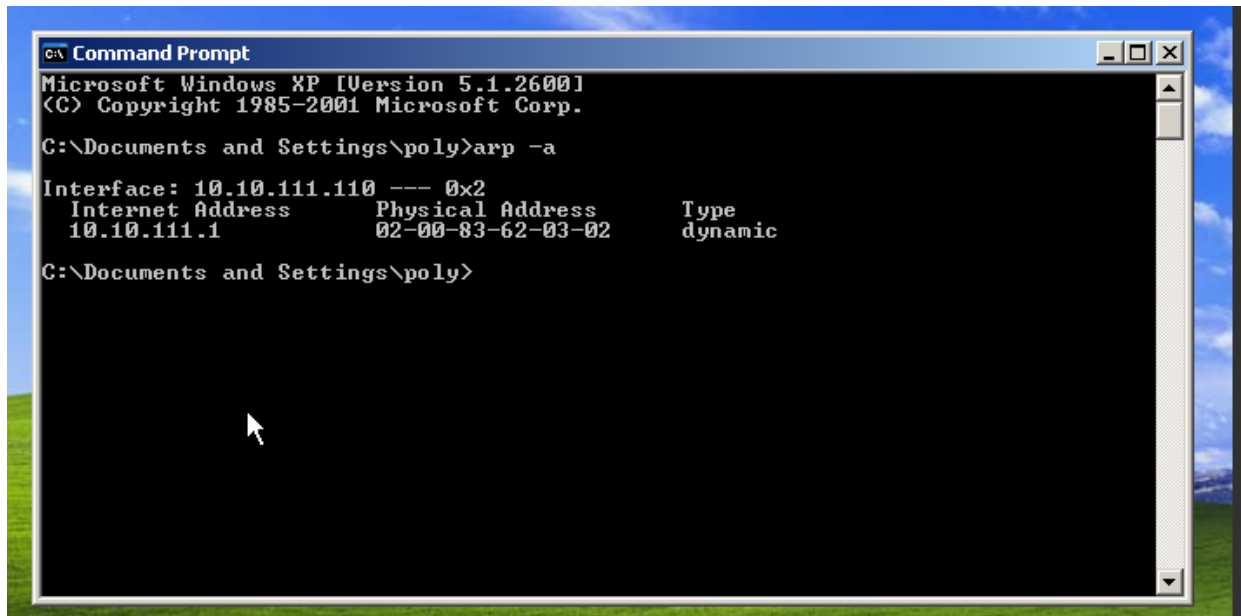


1. Snapshot of the changes in arp tables before and after arp-poisoning

Snapshot of the arp table before arp-poisoning of the victim machine is as follows:

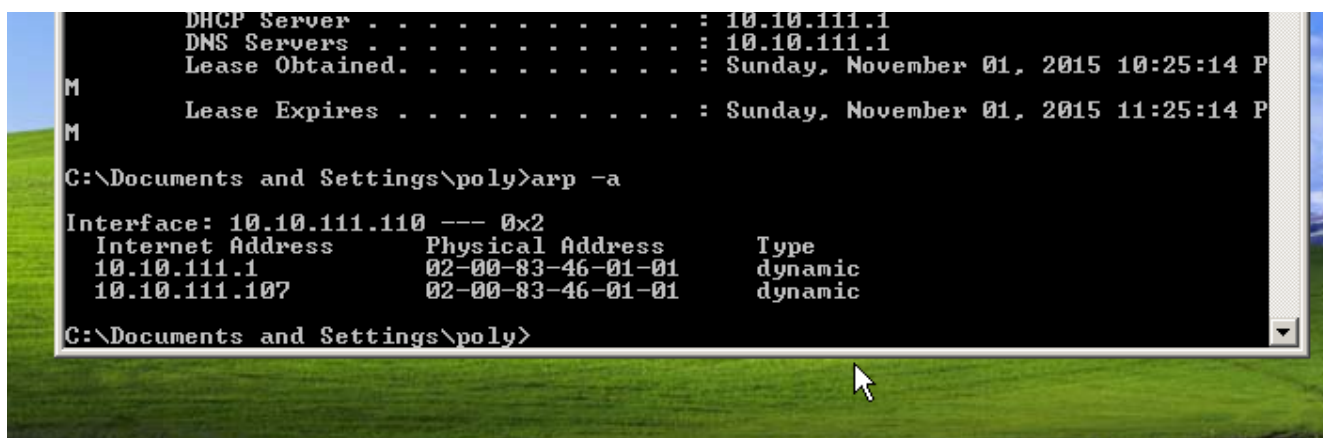


```
C:\Documents and Settings\poly>arp -a

Interface: 10.10.111.110 --- 0x2
Internet Address      Physical Address      Type
10.10.111.1           02-00-83-62-03-02     dynamic

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

Snapshot of the arp table after the scapy code was executed(of the victim machine):



```
DHCP Server . . . . . : 10.10.111.1
DNS Servers . . . . . : 10.10.111.1
Lease Obtained. . . . . : Sunday, November 01, 2015 10:25:14 P
M
Lease Expires . . . . . : Sunday, November 01, 2015 11:25:14 P
M

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

Interface: 10.10.111.110 --- 0x2
Internet Address      Physical Address      Type
10.10.111.1           02-00-83-46-01-01     dynamic
10.10.111.107         02-00-83-46-01-01     dynamic

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

We can observe that the rtr's ip address and the attacker's ip address both are linked to the attacker's MAC address.

Snapshot of arp table of rtr before arp-poisoning:

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
router:~# arp -a
? (10.10.111.107) at 02:00:83:46:01:01 [ether] on eth1
? (10.12.1.1) at 00:30:48:be:c8:31 [ether] on eth0
? (10.12.1.10) at 02:00:0b:a4:3e:02 [ether] on eth0
? (10.10.111.110) at 02:00:83:7e:05:01 [ether] on eth1
router:~# _
```

Snapshot of the arp table of the rtr after the code was executed:

```
router:~# arp -a
? (10.12.1.1) at 00:30:48:be:c8:31 [ether] on eth0
? (10.10.111.110) at 02:00:83:46:01:01 [ether] on eth1
router:~# _
```

We can observe that the MAC address linked with the victim change's to that of the attacker's.

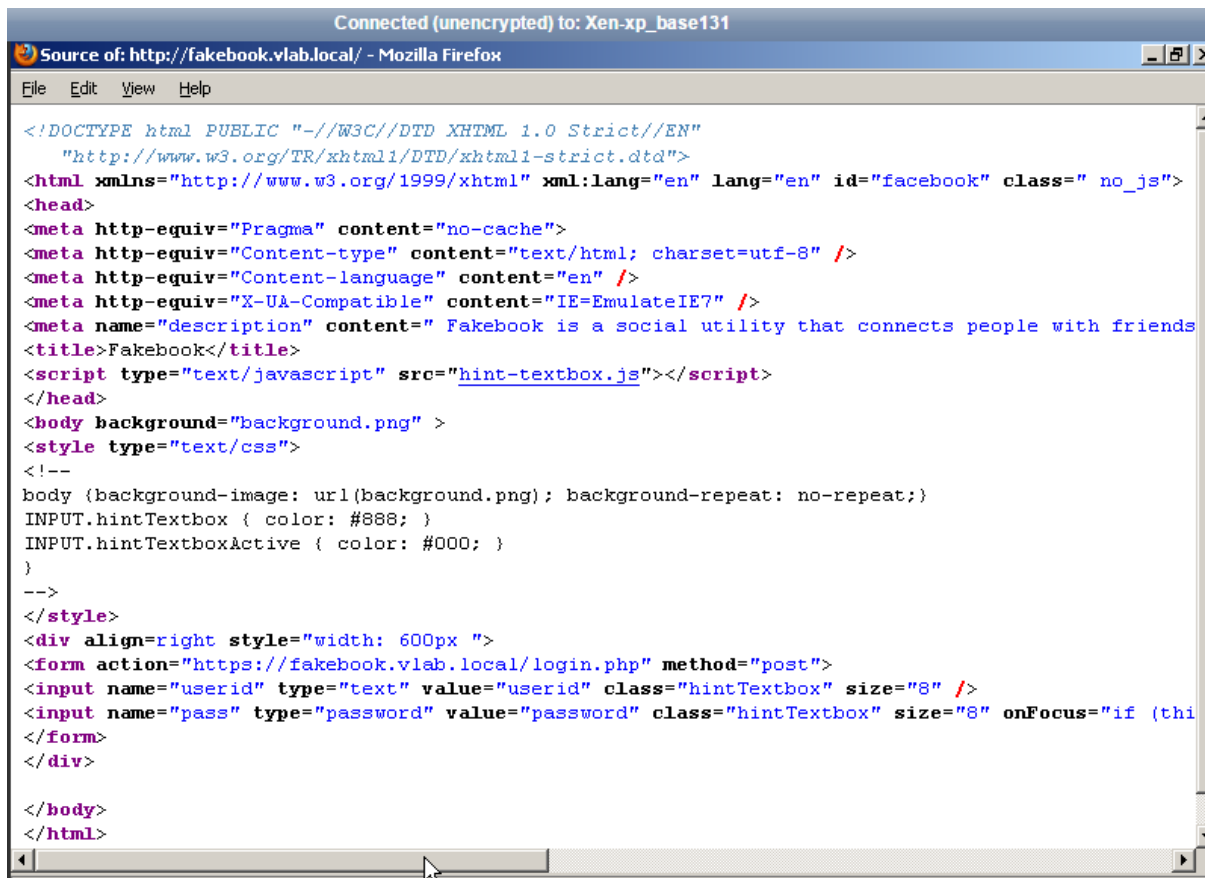
2. Sslstrip performed:

Following is the screenshot of the Sslstrip being performed simultaneously with the scapy code.

[illegible]

3. Screenshot of the Page source:

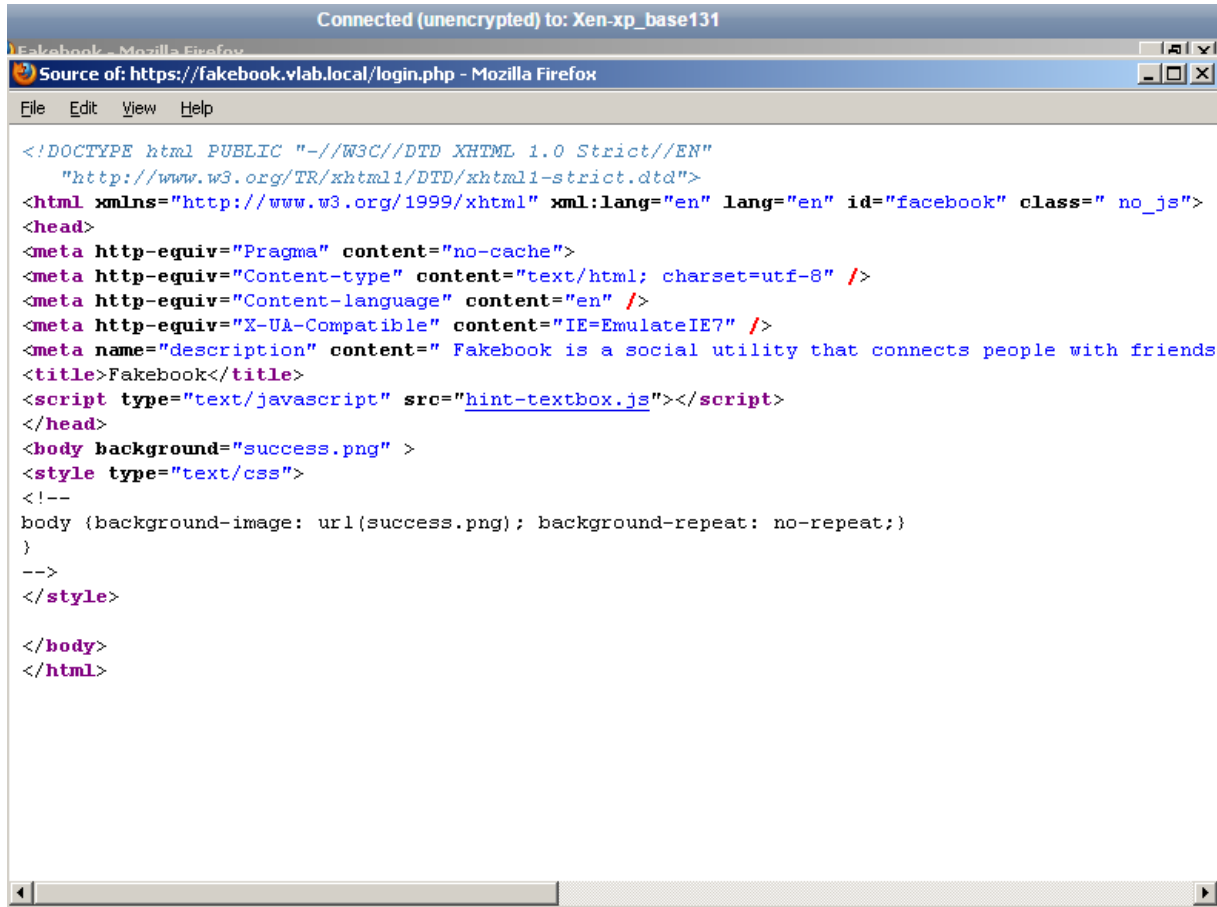
Following is the snapshot of the page source before the code was executed:



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" id="facebook" class="no_js">
<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 with friends
<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="if (thi
</form>
</div>

</body>
</html>
```

Screenshot of the page source after the code was executed:



```
Connected (unencrypted) to: Xen-xp_base131
Fakebook - Mozilla Firefox
Source of: https://fakebook.vlab.local/login.php - Mozilla Firefox
File Edit View Help
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" id="facebook" class="no_js">
<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 with friends
<title>Fakebook</title>
<script type="text/javascript" src="hint-textbox.js"></script>
</head>
<body background="success.png" >
<style type="text/css">
<!--
body {background-image: url(success.png); background-repeat: no-repeat;}
}
-->
</style>

</body>
</html>
```

The difference between the two forms is mainly the change of the site clearly changing from a secured site to an unsecured one. Before the sslstrip was run the form action says “https” whereas after the execution it changes to “http”, observing which we can clearly say that the attack has been successful and the fakebook page was opened not via the rtr but via the attacker’s machine. The change in the header gives us enough information about the SSL certification hinting us the successful implementation of the attack.