Lab 04 Report

Documentation

4.1 Banner Grabbing

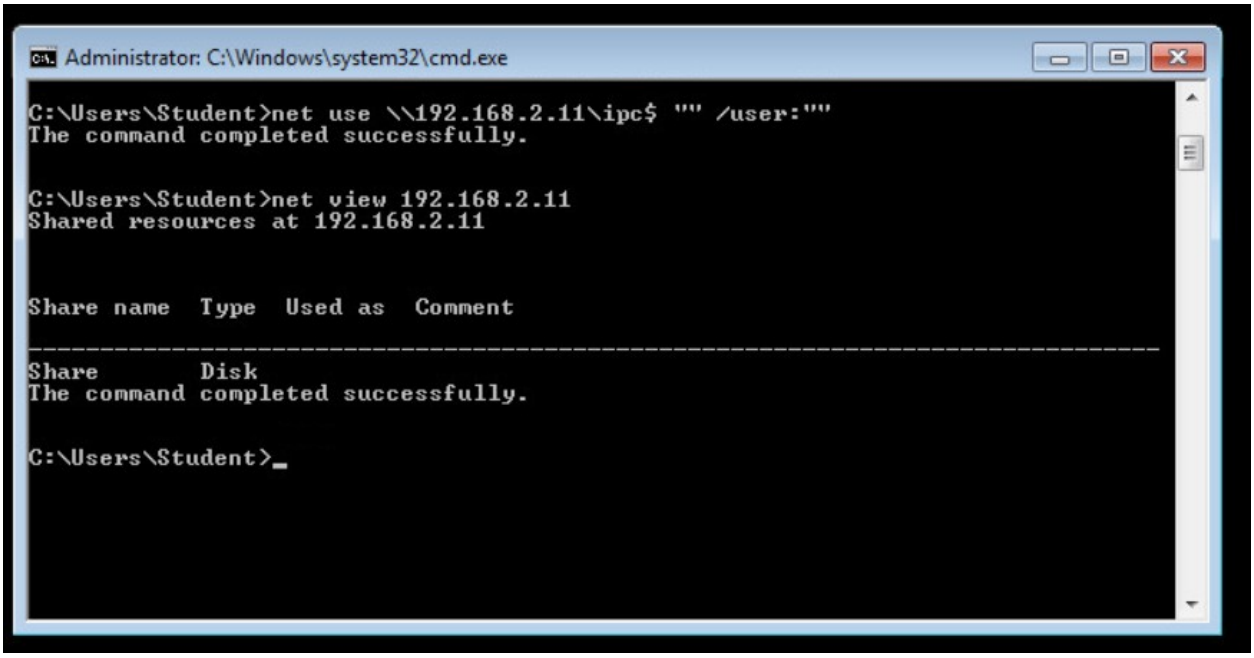
```
root@kali:~# telnet 192.168.2.11 80
Trying 192.168.2.11...
Connected to 192.168.2.11.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://192.168.2.11/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:44a"
Server: Microsoft-IIS/6.0
Date: Tue, 30 Jan 2018 15:02:58 GMT
Connection: close

<html>

<head>
<meta HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">


<title ID=titletext>Under Construction</title>
</head>

<body bgcolor=white>
<table>
<tr>
<td ID=tableProps width=70 valign=top align=center>
<img ID=pagerrorImg src="pagerror.gif" width=36 height=48>
<td ID=tablePropsWidth width=400>

<h1 ID=errortype style="font:14pt/16pt verdana; color:#4e4e4e">
<P ID=Comment1><!--Problem--><P ID="errorText">Under Construction</h1>
```

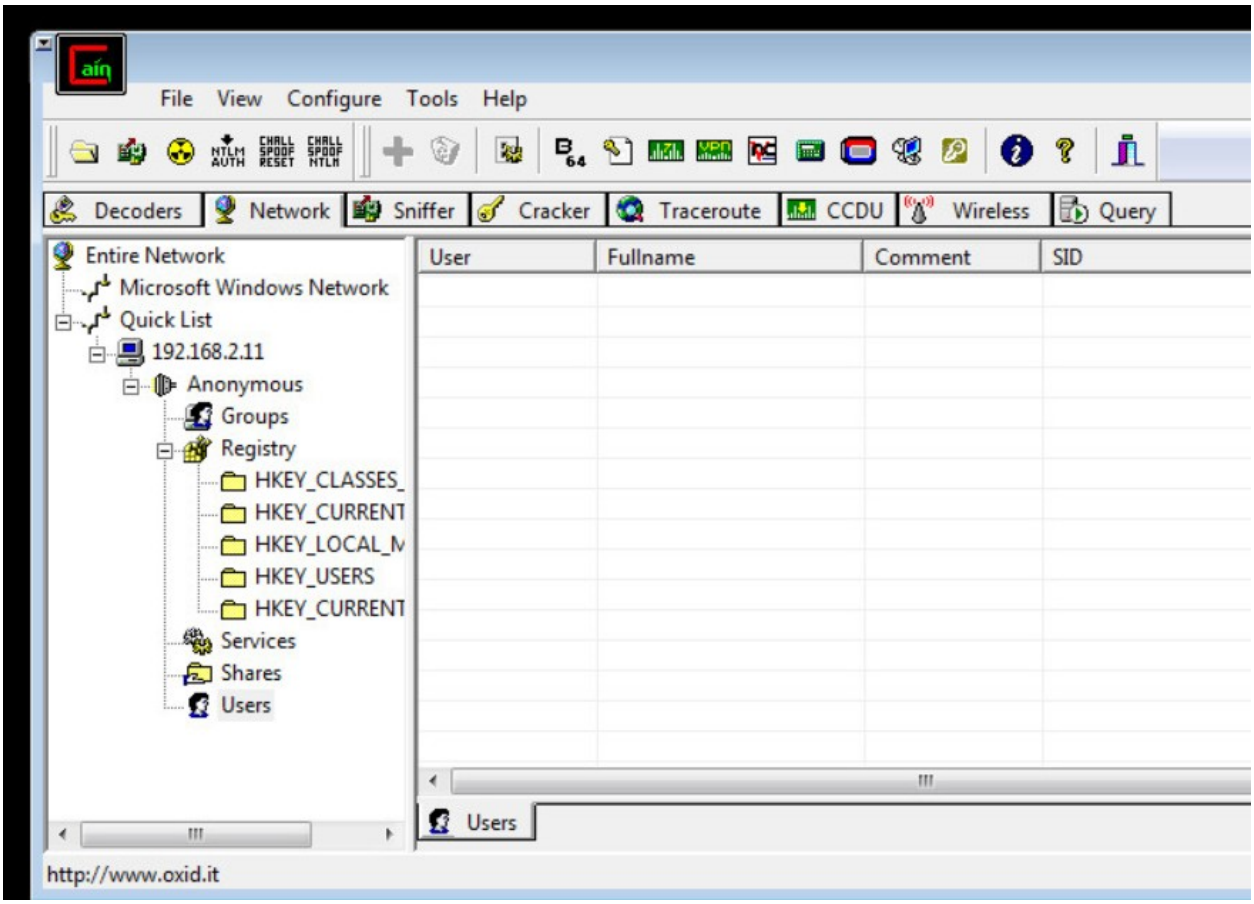
```
<P ID=Comment2><!--Probable causes:<--><P ID="errordesc"><font style="font:9pt/12pt verdana; color:black">
The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.
<P ID=term1>Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

<hr size=1 color="blue">

<P ID=message1>If you are the Web site administrator and feel you have received this message in error, please see &quot;Enabling and Disabli
ng Dynamic Content&quot; in IIS Help.

<h5 ID=head1>To access IIS Help</h5>
<ol>
<li ID=bullet1>Click <b>Start</b>, and then click <b>Run</b>.
<li ID=bullet2>In the <b>Open</b> text box, type <b>inetmgr</b>. IIS Manager appears.
<li ID=bullet3>From the <b>Help</b> menu, click <b>Help Topics</b>.
<li ID=bullet4>Click <b>Internet Information Services</b>.</ol>
</td>
</tr>
</table>

</body>
</html>
Connection closed by foreign host.
root@kali:~#
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# telnet 192.168.2.11 80
Trying 192.168.2.11...
Connected to 192.168.2.11.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://192.168.2.11/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:44a"
Server: Microsoft-IIS/6.0
Date: Tue, 30 Jan 2018 15:23:58 GMT
Connection: close

Connection closed by foreign host.
root@kali:~#
```

Lab 04 Report

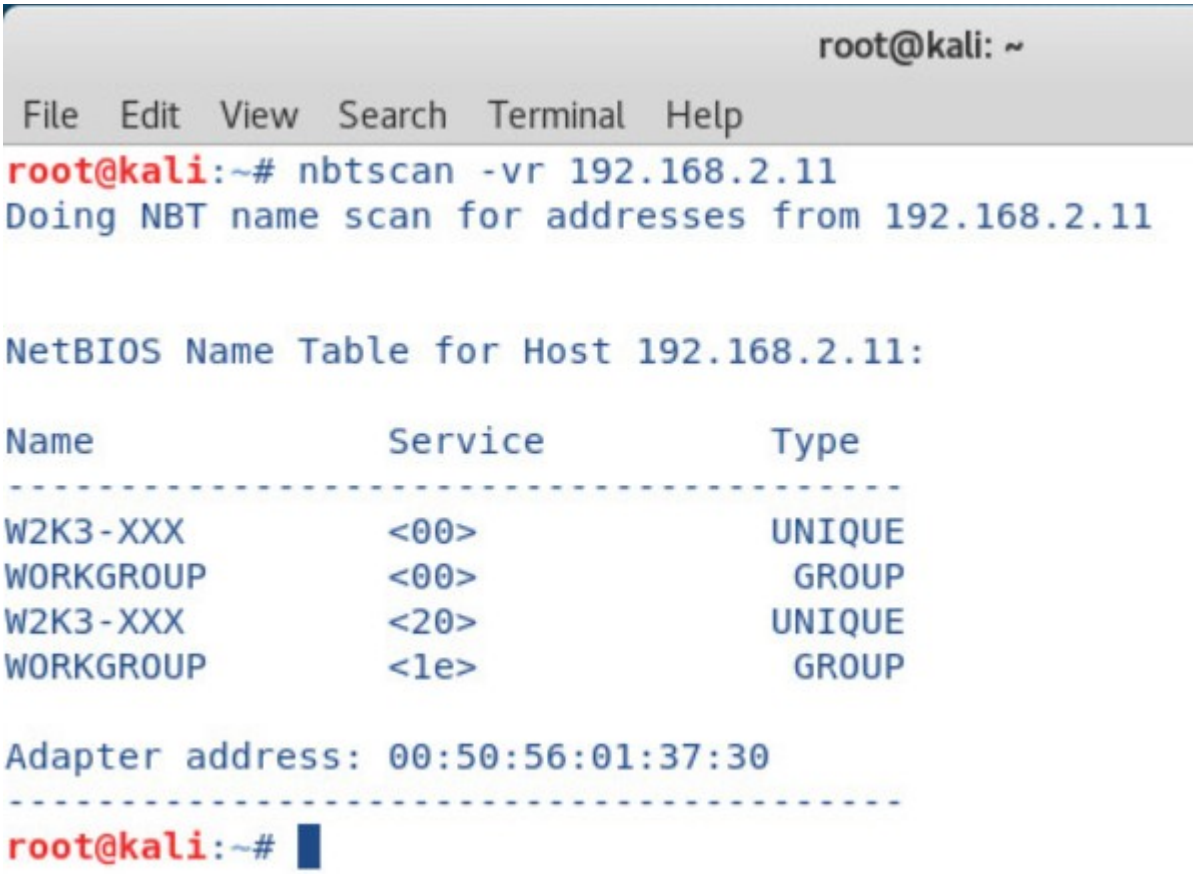
4.2 Null Sessions





When I clicked on Users. It gave me the following prompt: "Users enumeration error: Access is denied"

4.3 NetBIOS Enumeration



4.4 SMTP Enumeration

Vulnerabilities

No vulnerabilities discovered in this lab.