

(Damn Vulnerable Web App (DVWA))

{ Burp Suite, Spider Function }

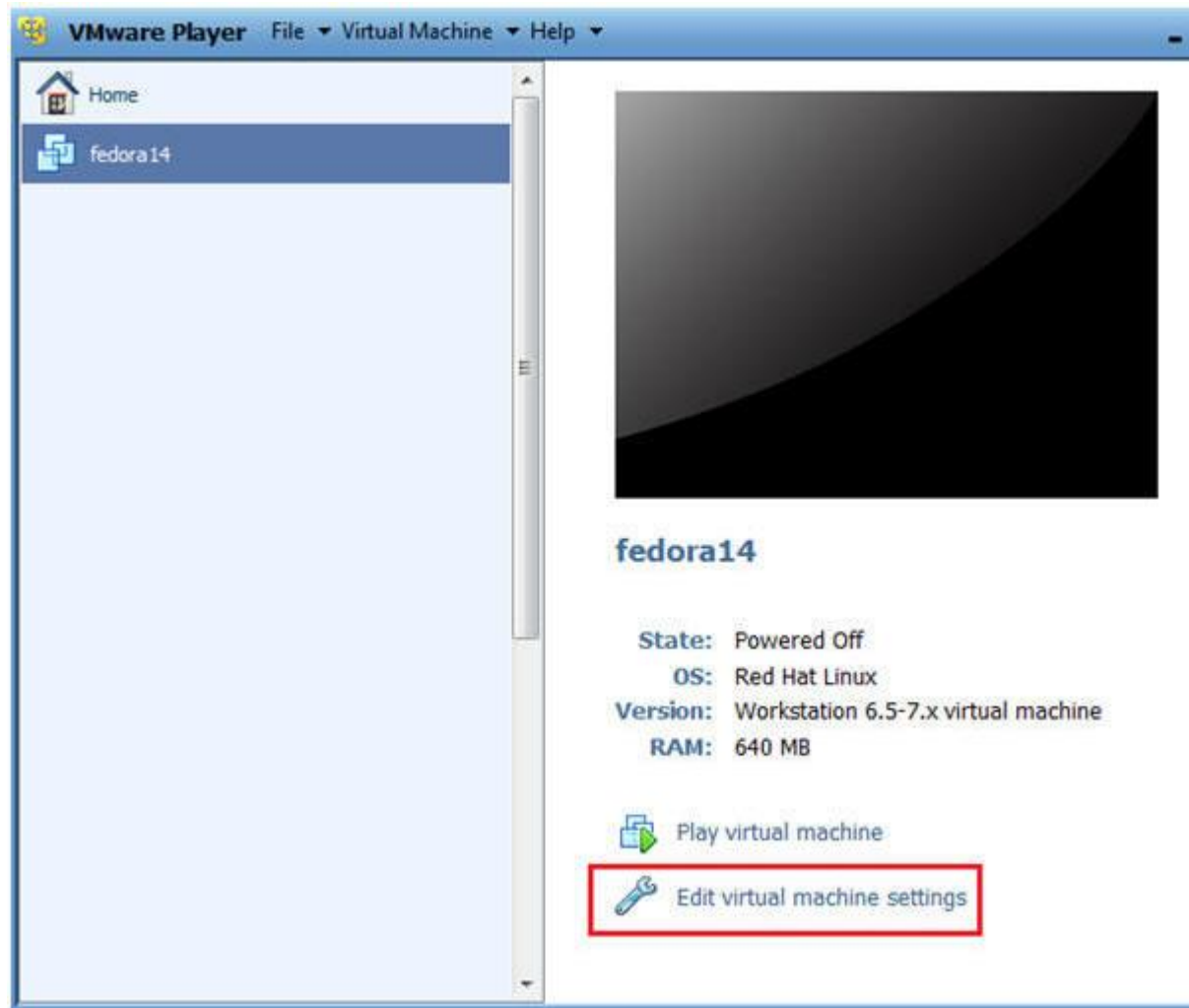
Section 0. Background Information

1. What is Damn Vulnerable Web App (DVWA)?
 - o Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is intentionally damn vulnerable.
 - o Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a controlled environment.
2. What is Burp Suite?
 - o Burp suite is a java application that can be used to secure or test web applications. The suite consists of different tools, like a proxy, a web spider, an intruder and a so called repeater, with which many tasks can be automated.
3. Pre-Requisite Labs
 - o [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
 - o [BackTrack: Lesson 1: Installing BackTrack 5 R1](#)
4. **Lab Notes**
 - o In this lab we will do the following:
 1. We will configure Firefox to use Burp Suite as its Proxy
 2. We will configure Burp Suite to accept requests from Firefox
 3. We will use Burp Suite to spider the DVWA web application.
 4. We will conduct a very simple forensics investigation on the DVWA Web Server, in which the DVWA web application resides.
5. Legal Disclaimer
 - o As a condition of your use of this Web site, you warrant to computersecuritystudent.com that you will not use this Web site for any purpose that is **unlawful or that is prohibited** by these terms, conditions, and notices.

- In accordance with UCC § 2-316, this product is provided with "warranties, either expressed or implied." The information contained herein is provided "as-is", with "no guarantee of merchantability."
- In addition, this is a teaching website that **does not condone malicious behavior** of any kind.
- You are on notice, that continuing and/or using this lab outside your "own" test environment **is considered malicious and is against the terms of use**.
- © 2012 No content replication of any kind is allowed without explicit written permission.

Section 1: Configure Fedora14 Virtual Machine Settings

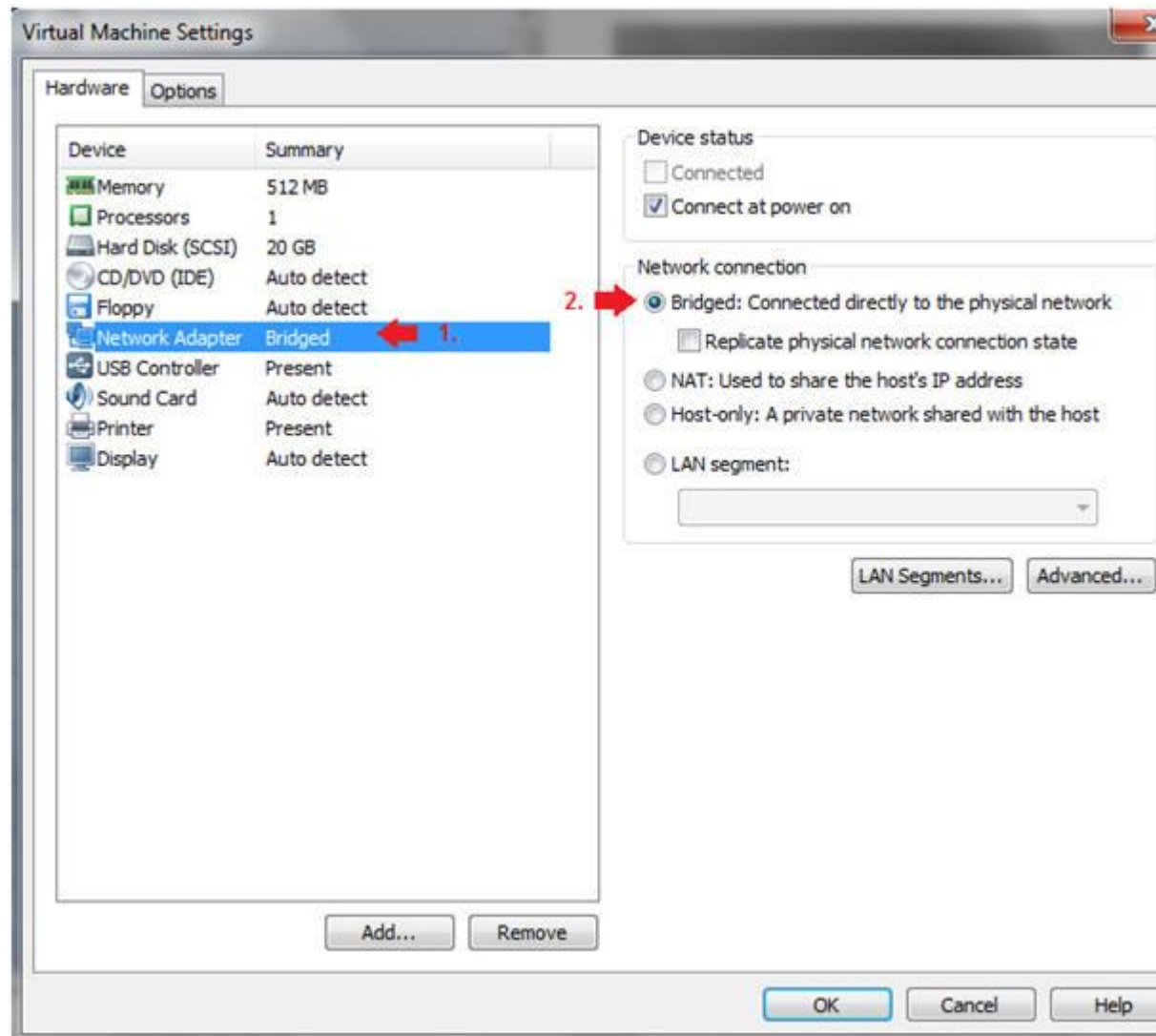
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit fedora14 Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings



3. Edit Network Adapter

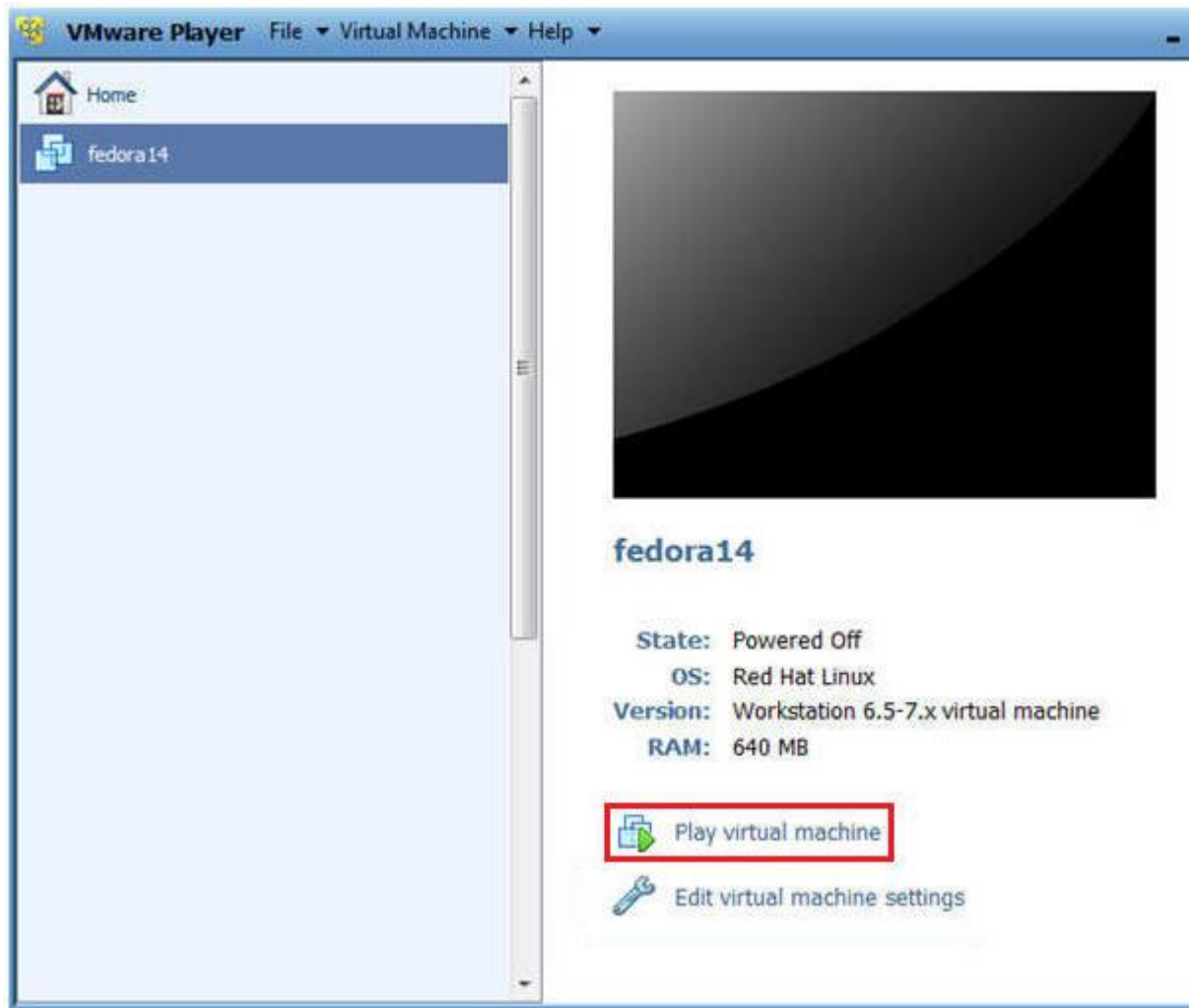
- **Instructions:**

1. Highlight Network Adapter
2. Select Bridged
3. Click on the OK Button.

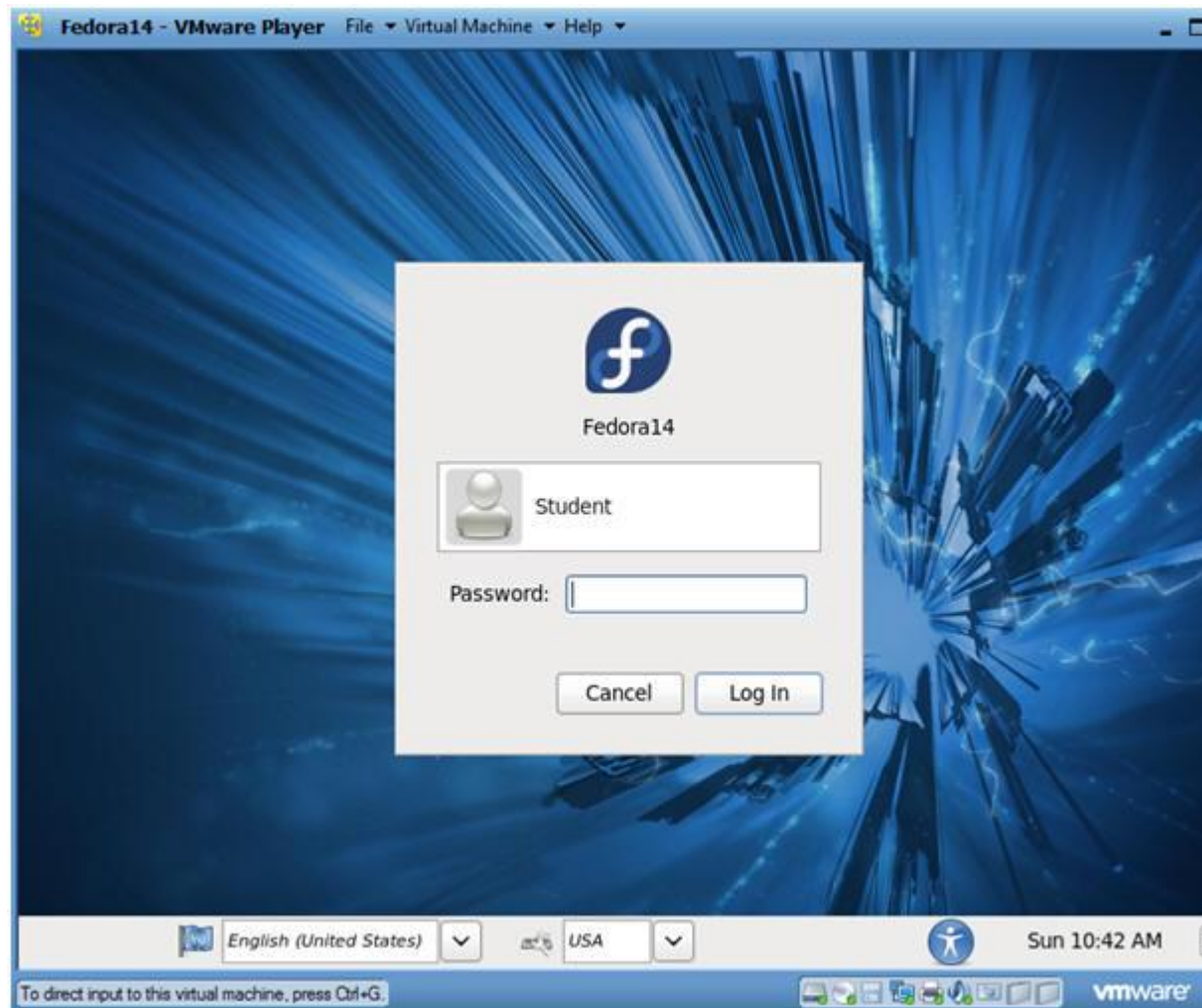


Section 2: Login to Fedora14

1. Start Fedora14 VM Instance
 - o **Instructions:**
 1. Start Up VMWare Player
 2. Select Fedora14
 3. Play virtual machine



- 2. Login to Fedora14
 - **Instructions:**
 1. Login: student
 2. Password: <whatever you set it to>.



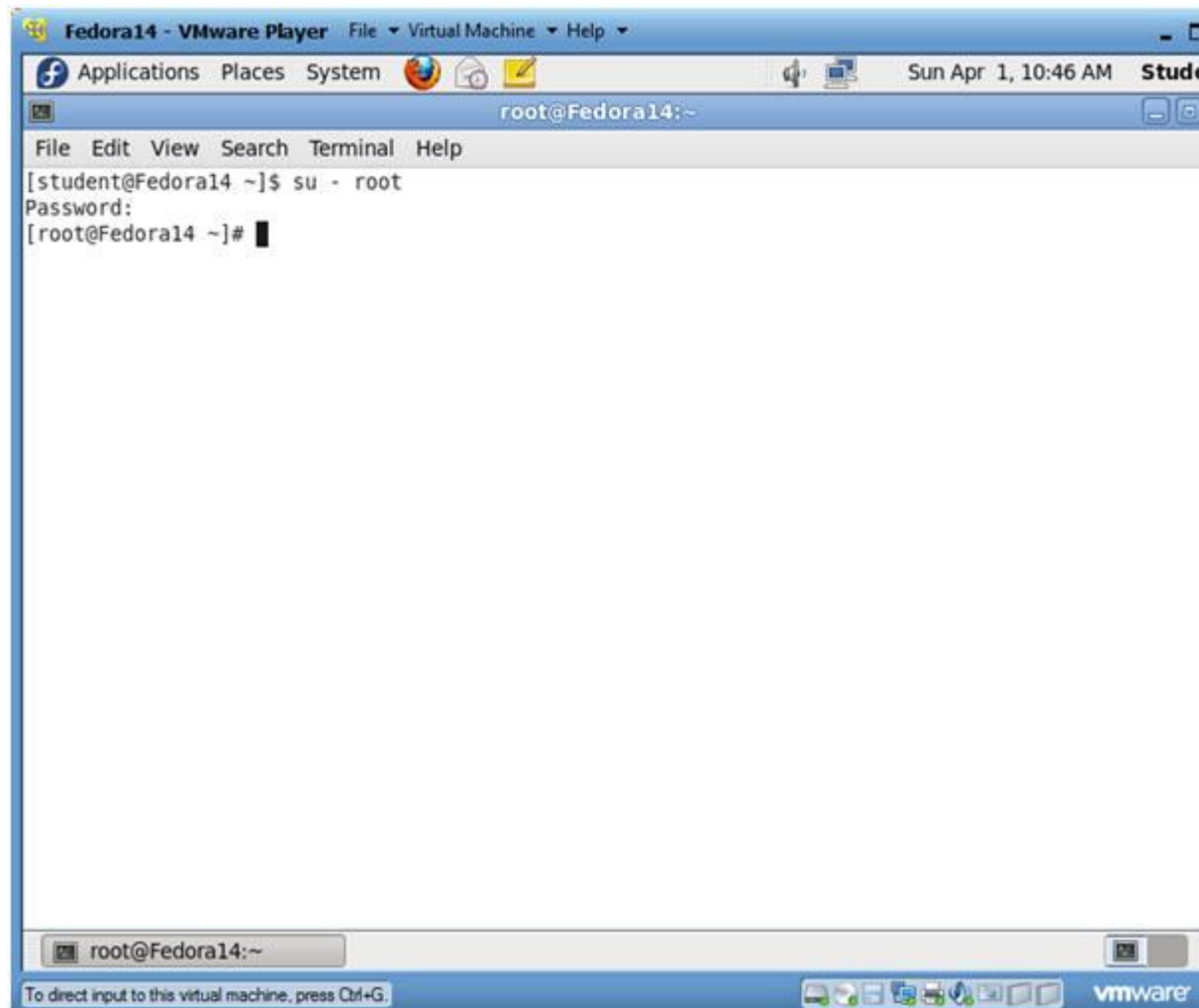
○

Section 3: Open Console Terminal and Retrieve IP Address

1. Start a Terminal Console
 - **Instructions:**
 1. Applications --> Terminal



- - 2. Switch user to root
 - **Instructions:**
 - 1. `su - root`
 - 2. <Whatever you set the root password to>



3. Get IP Address

- **Instructions:**
 1. `ifconfig -a`
- **Notes:**
 - As indicated below, my IP address is 192.168.1.106.
 - Please record your IP address.

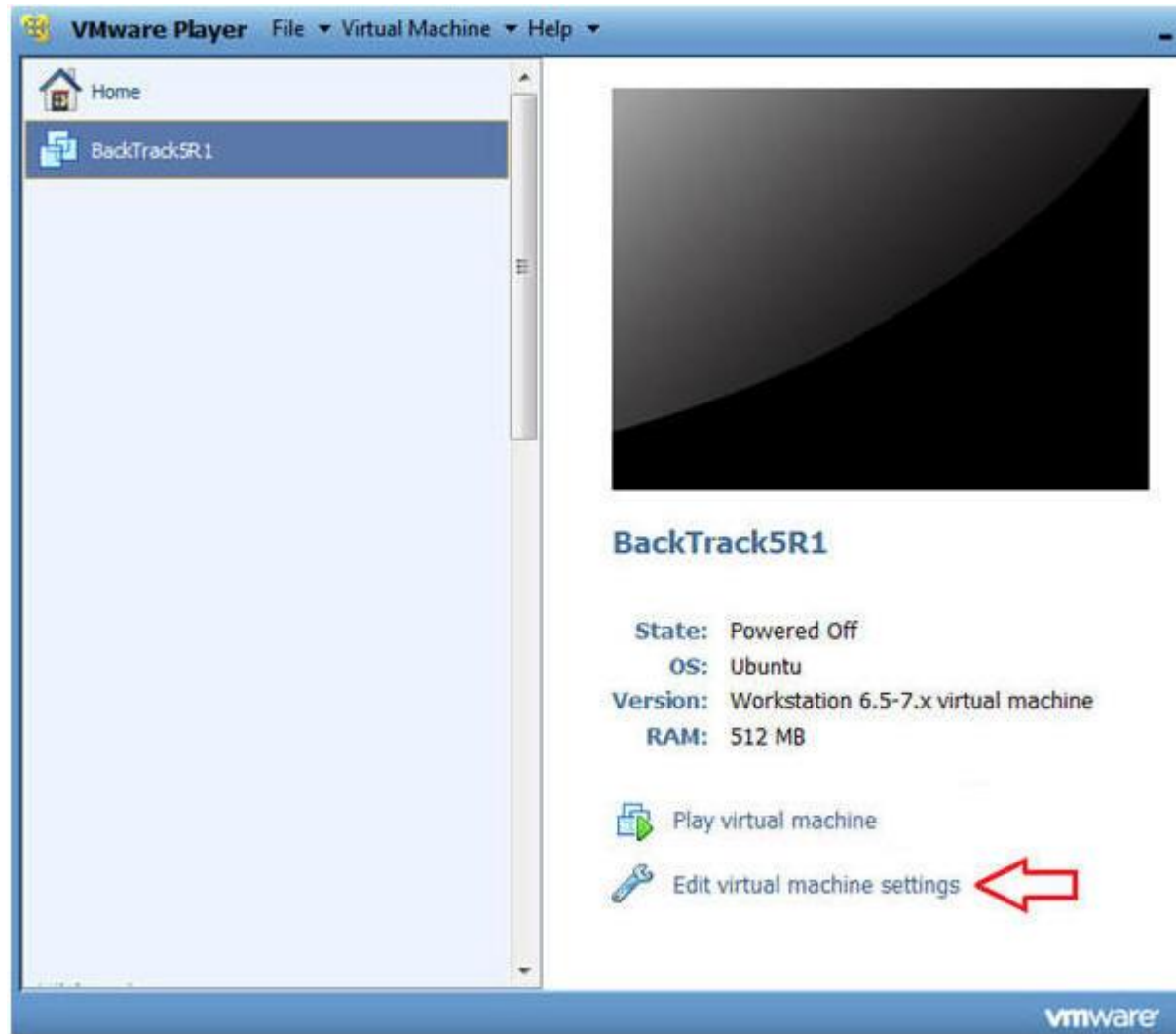

```
Fedora14 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@Fedora14:~
File  Edit  View  Search  Terminal  Help
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:81:54:42
          inet addr:192.168.1.106  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe81:5442/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2893 errors:0 dropped:0 overruns:0 frame:0
          TX packets:366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:546934 (534.1 KiB)  TX bytes:58291 (56.9 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3520 (3.4 KiB)  TX bytes:3520 (3.4 KiB)

[root@Fedora14 ~]#
```

Section 4: Configure BackTrack Virtual Machine Settings

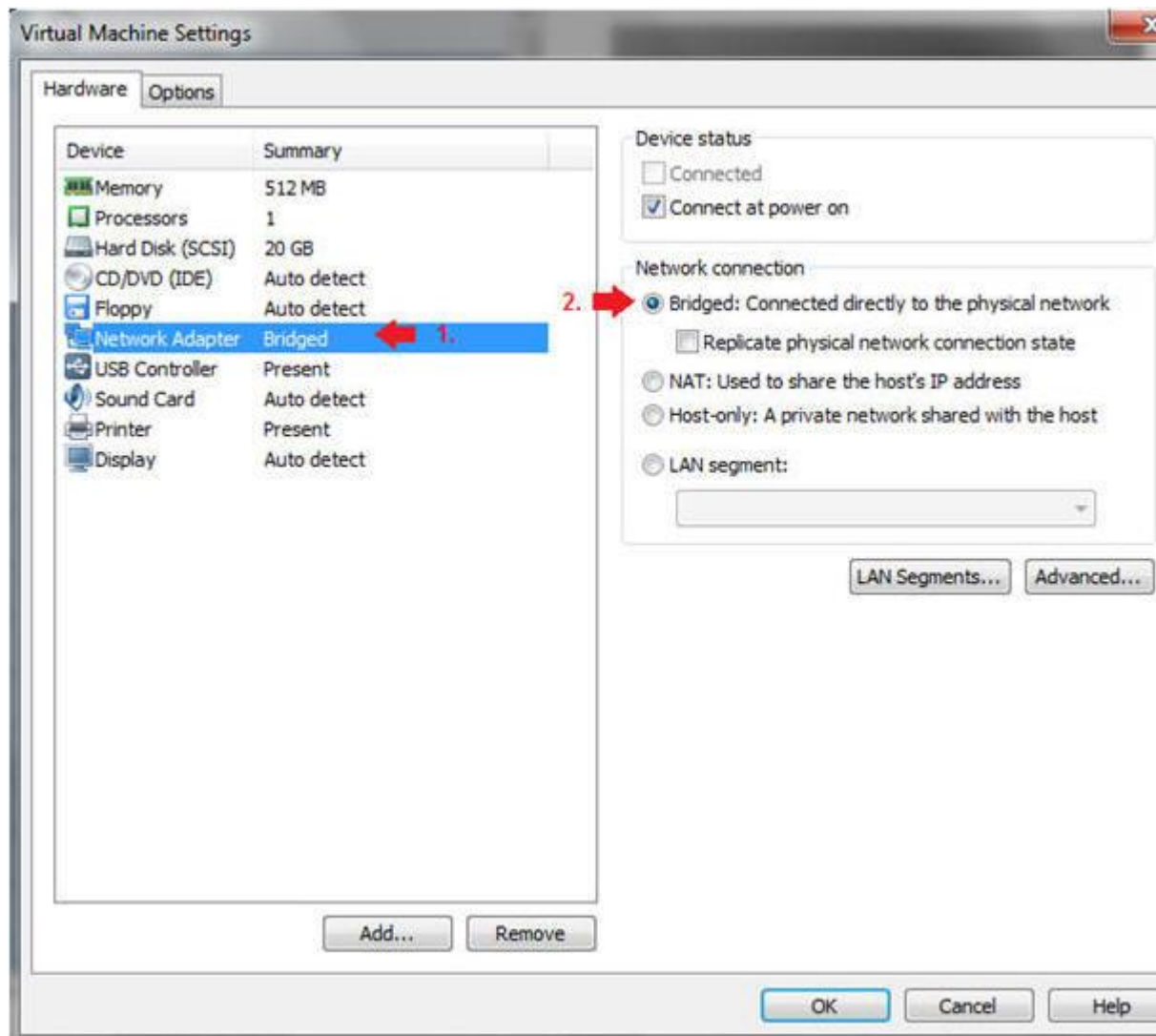
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight BackTrack5R1
 2. Click Edit virtual machine settings



3. Edit Network Adapter

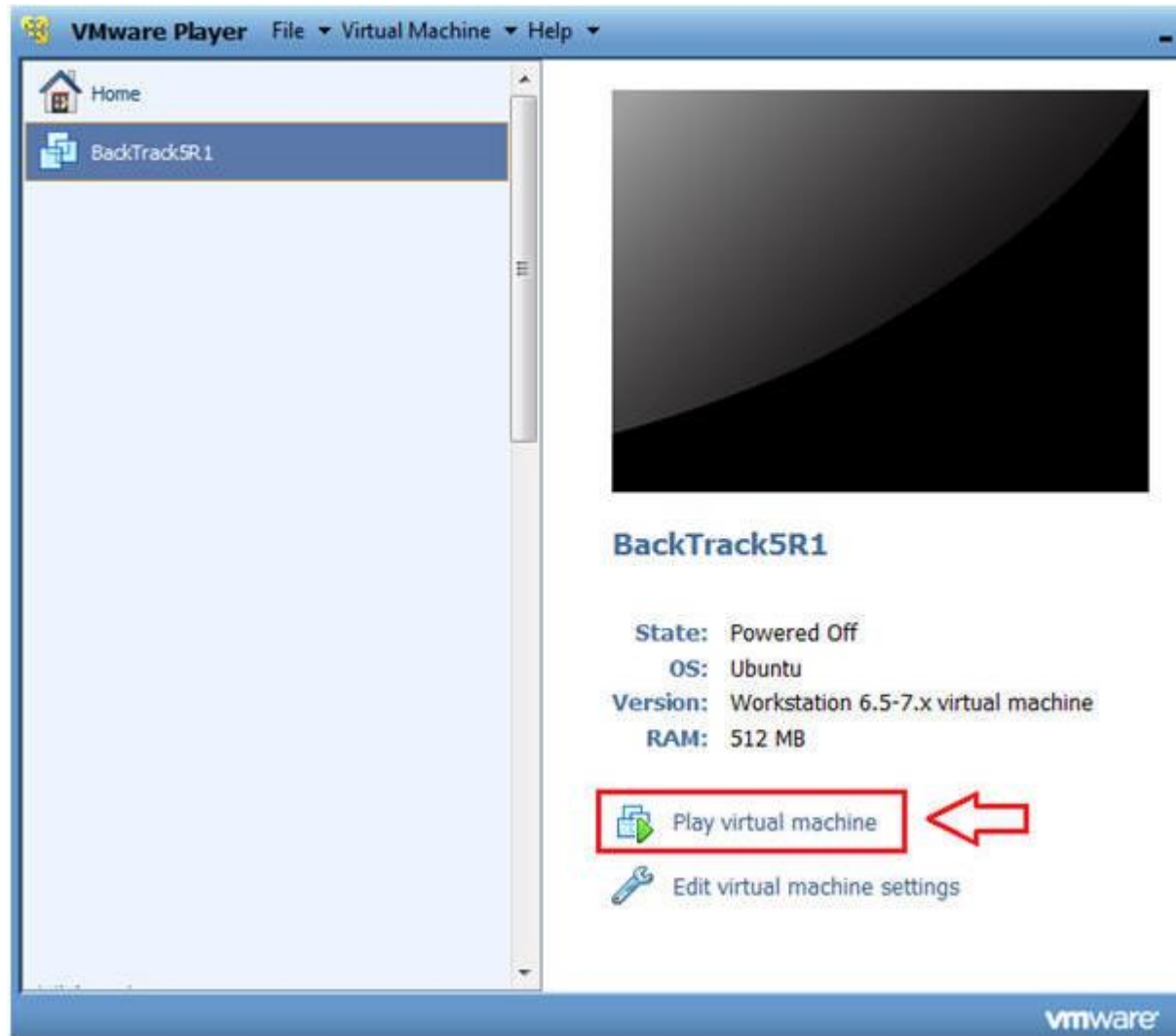
- **Instructions:**

1. Highlight Network Adapter
2. Select Bridged
3. Do not Click on the OK Button.



Section 5: Login to BackTrack

1. Start BackTrack VM Instance
 - **Instructions:**
 1. Start Up VMWare Player
 2. Select BackTrack5R1
 3. Play virtual machine



2. Login to BackTrack

- **Instructions:**

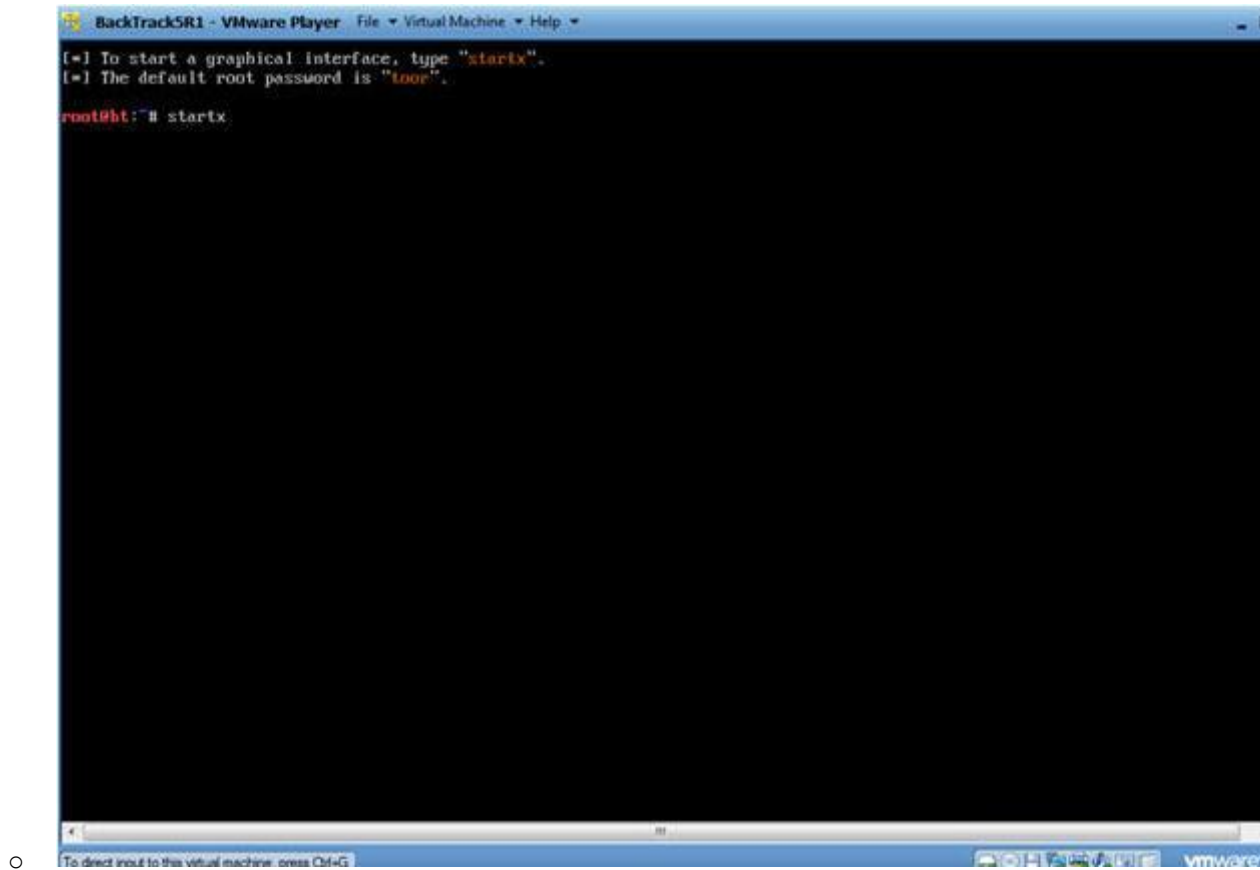
1. Login: root
2. Password: toor or <whatever you changed it to>.

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
[ 3.312567] Copyright (c) 1999-2008 LSI Corporation
[ 3.313456] FDC 0 is a post-1991 82077
[ 3.340877] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[ 3.360567] pcnet32 0000:02:01.0: PCI INT A -> GSI 19 (level, low) -> IRQ 19
[ 3.364871] agpgart-intel 0000:00:00.0: Intel 440BX Chipset
[ 3.368532] pcnet32: PCnet/PCI II 79C970A at 0x2000, 00:0c:29:90:13:78 assigned IRQ 19
[ 3.372931] agpgart-intel 0000:00:00.0: AGP aperture is 256M @ 0x0
[ 3.376916] pcnet32: eth0: registered as PCnet/PCI II 79C970A
[ 3.384739] pcnet32: 1 cards found
[ 3.404691] Fusion MPT SPI Host driver 3.04.18
[ 3.408410] mptspi 0000:00:10.0: PCI INT A -> GSI 17 (level, low) -> IRQ 17
[ 3.408733] mptbase: ioc0: Initiating bringup
[ 3.488282] ioc0: LSI53C1030 B0: Capabilities={Initiator}
[ 3.656180] scsi2 : ioc0: LSI53C1030 B0, FuRev=01032920h, Ports=1, MaxQ=128, IRQ=17
[ 3.775716] scsi 2:0:0:0: Direct-Access VMware, VMware Virtual S 1.0 PQ: 0 ANSI: 2
[ 3.779710] scsi target2:0:0: Beginning Domain Validation
[ 3.783701] scsi target2:0:0: Domain Validation skipping write tests
[ 3.783772] scsi target2:0:0: Ending Domain Validation
[ 3.787761] scsi target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
[ 3.794467] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[ 3.795671] sd 2:0:0:0: [sda] Write Protect is off
[ 3.795811] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.795881] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.800343] sd 2:0:0:0: Attached scsi generic sg1 type 0
[ 3.801376] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.803626] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.855626] sda: sda1 sda2 < sda5 >
[ 3.883776] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.887505] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.887577] sd 2:0:0:0: [sda] Attached SCSI disk

BackTrack 5 R1 - Code Name Revolution 32 bitbt tty1
bt login: root
Password:

To direct input to this virtual machine, press Ctrl+G.
```

- 3. Bring up the GNOME
 - o **Instructions:**
 - 1. Type startx



Section 6: Open Console Terminal and Retrieve IP Address

1. Open a console terminal
 - **Instructions:**
 1. Click on the console terminal



2. Get IP Address

- **Instructions:**
 - 1. `ifconfig -a`
- **Notes:**
 - As indicated below, my IP address is 192.168.1.105.
 - Please record your IP address.



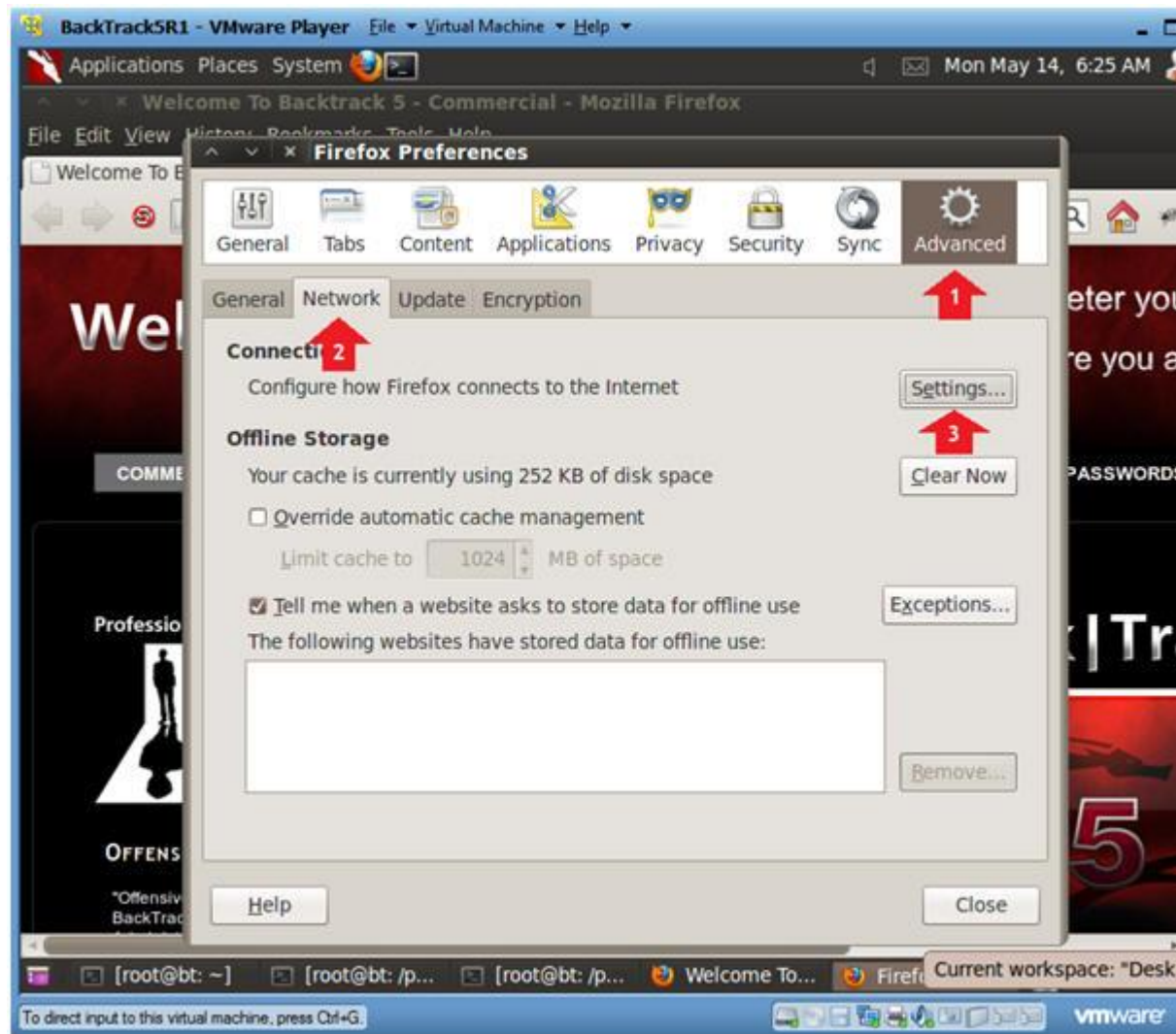
- - 2. Preferences
 - **Instructions:**
 - 1. Edit --> Preferences



3. Preferences

- **Instructions:**

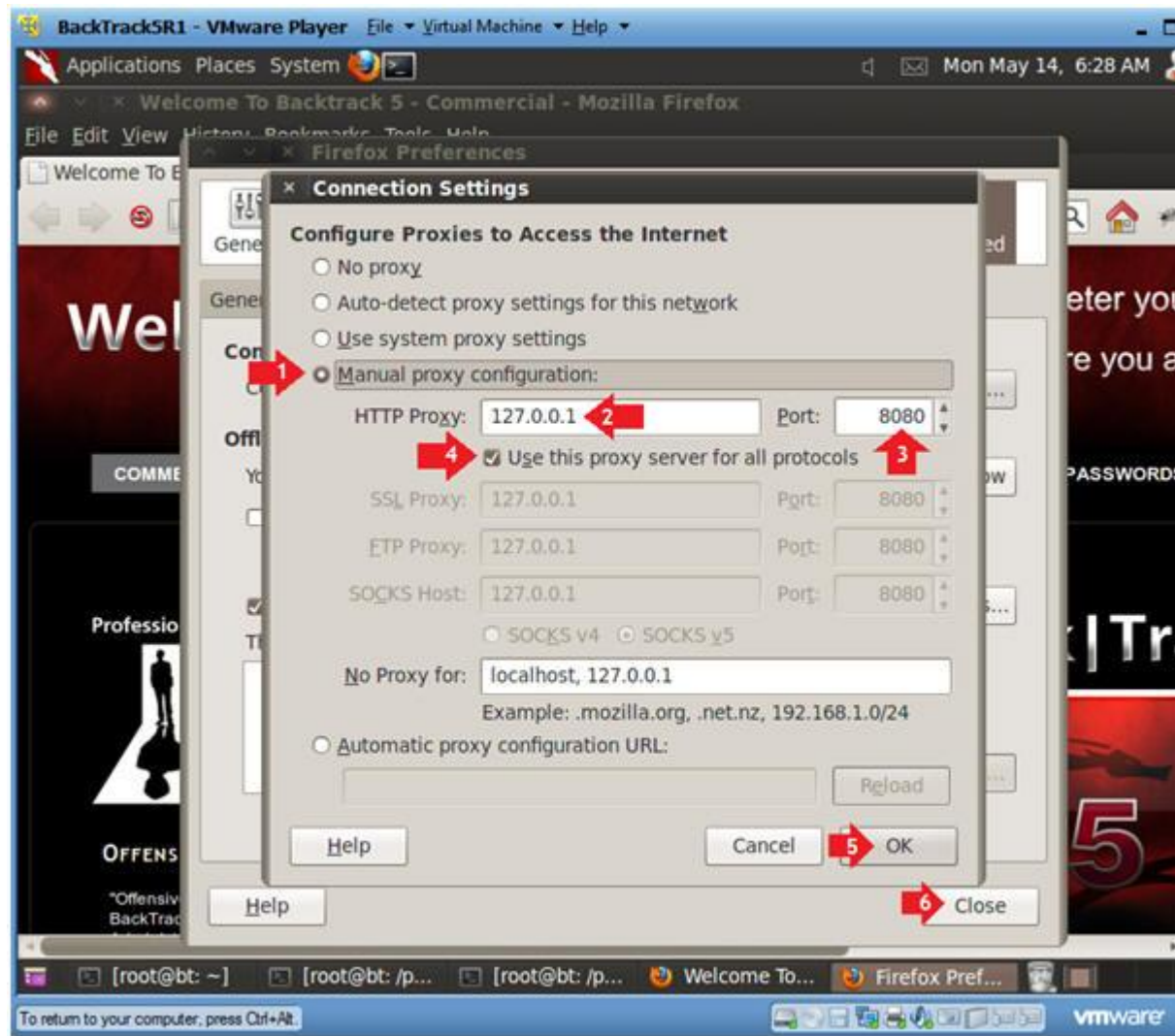
1. Click on Advanced
2. Click on the Network Tab
3. Click on the Settings Button



4. Preferences

- **Instructions:**

1. Click on Manual proxy configurations
2. Type "127.0.0.1" in the HTTP Proxy Text Box
3. Type "8080" in the Port Text Box
4. Check Use the proxy server for all protocols
5. Click OK
6. Click Close



Section 8: Configure Burp Suite

1. Start Burp Suite

o **Instructions:**

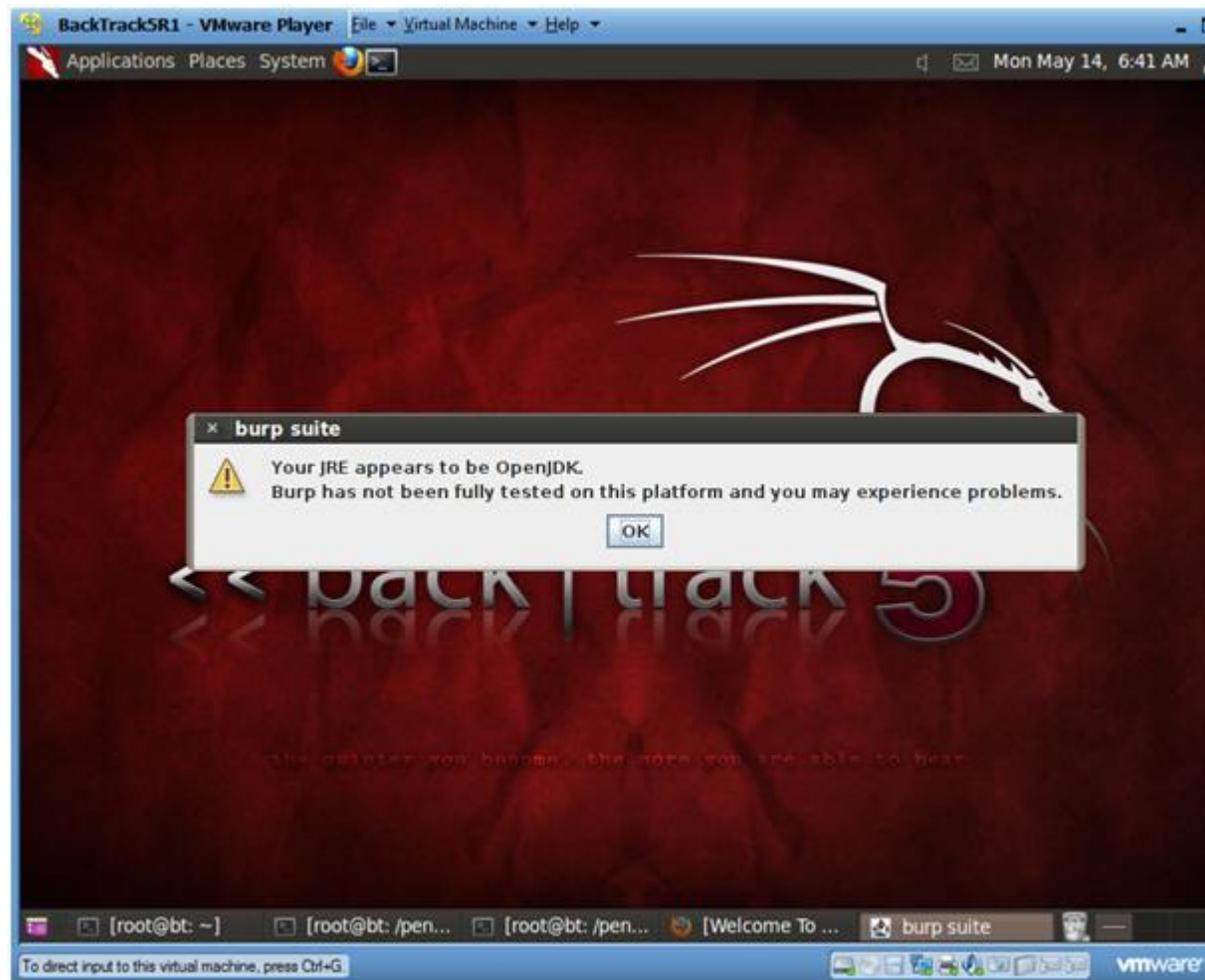
1. Applications --> Vulnerability Assessment --> Web Application Assessment ---> Web Vulnerability Scanner --> burpsuite



○

2. JRE Message

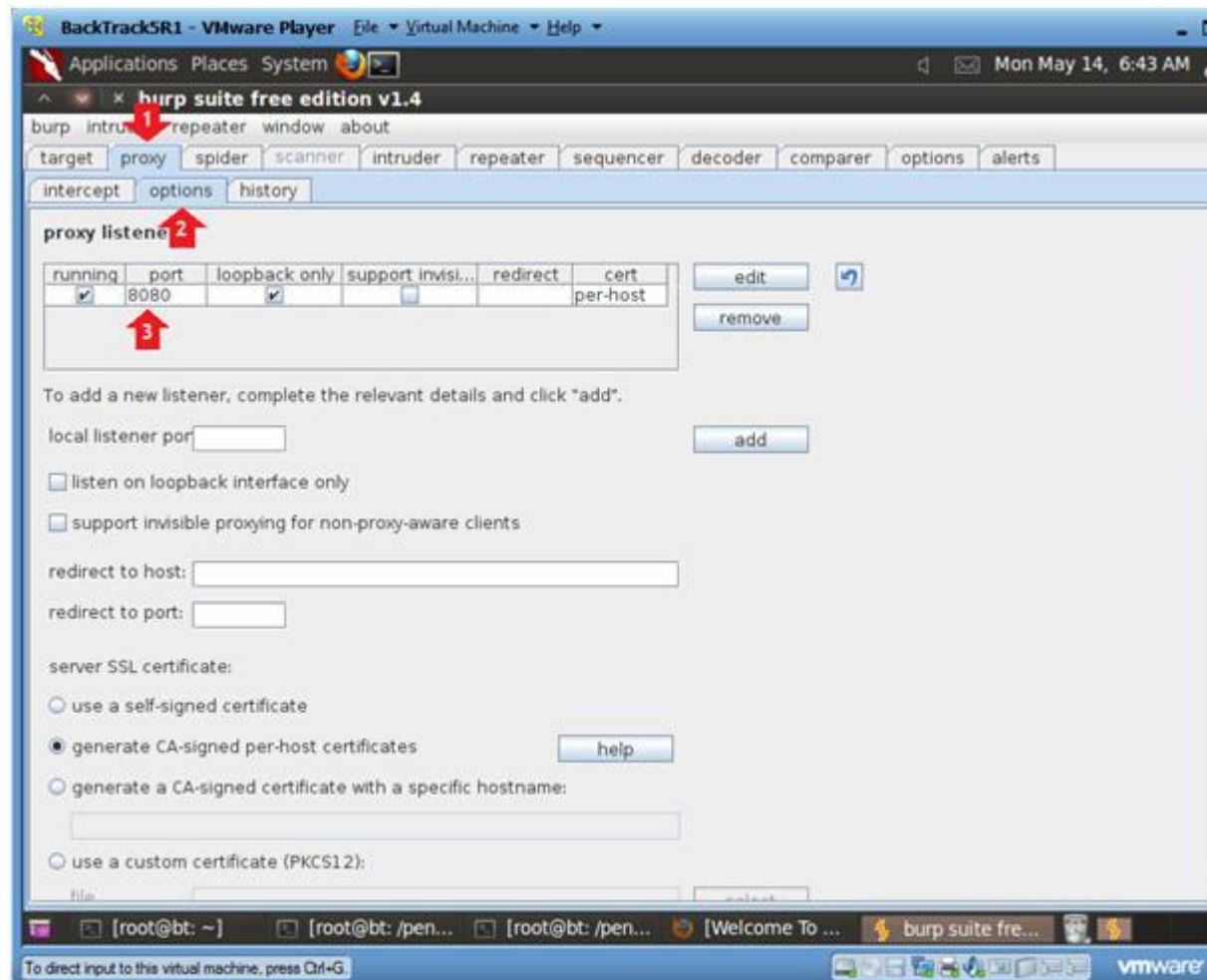
- **Instructions:**
 1. Click OK



3. Configure proxy

- **Instructions:**

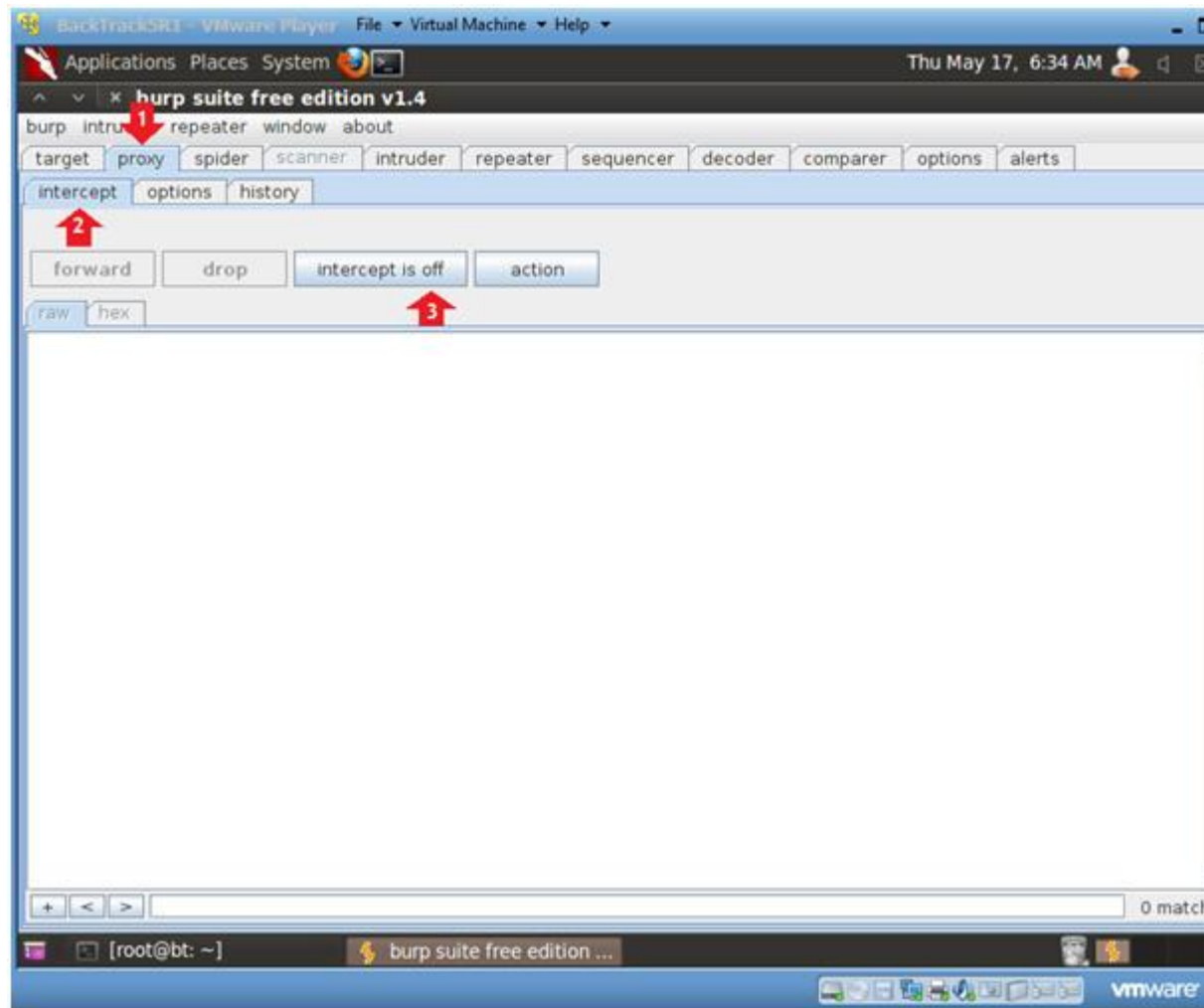
1. Click on the proxy tab
2. Click on the options tab
3. Verify the port is set to 8080



4. Turn on intercept

o **Instructions:**

1. Click on the proxy tab
2. Click on the intercept tab
3. Click on the "intercept is on" button to change it to "int
off"



Section 9: Spider with Burp Suite

1. Browse to DVWA's homepage
 - o **Instructions:**
 1. `http://IPADDRESS/dvwa/`
 - Replace IPADDRESS with the Fedora's IP Address obtained in Section 3, Step 3).
 2. Press <Enter>
 3. Continue to Next Step.



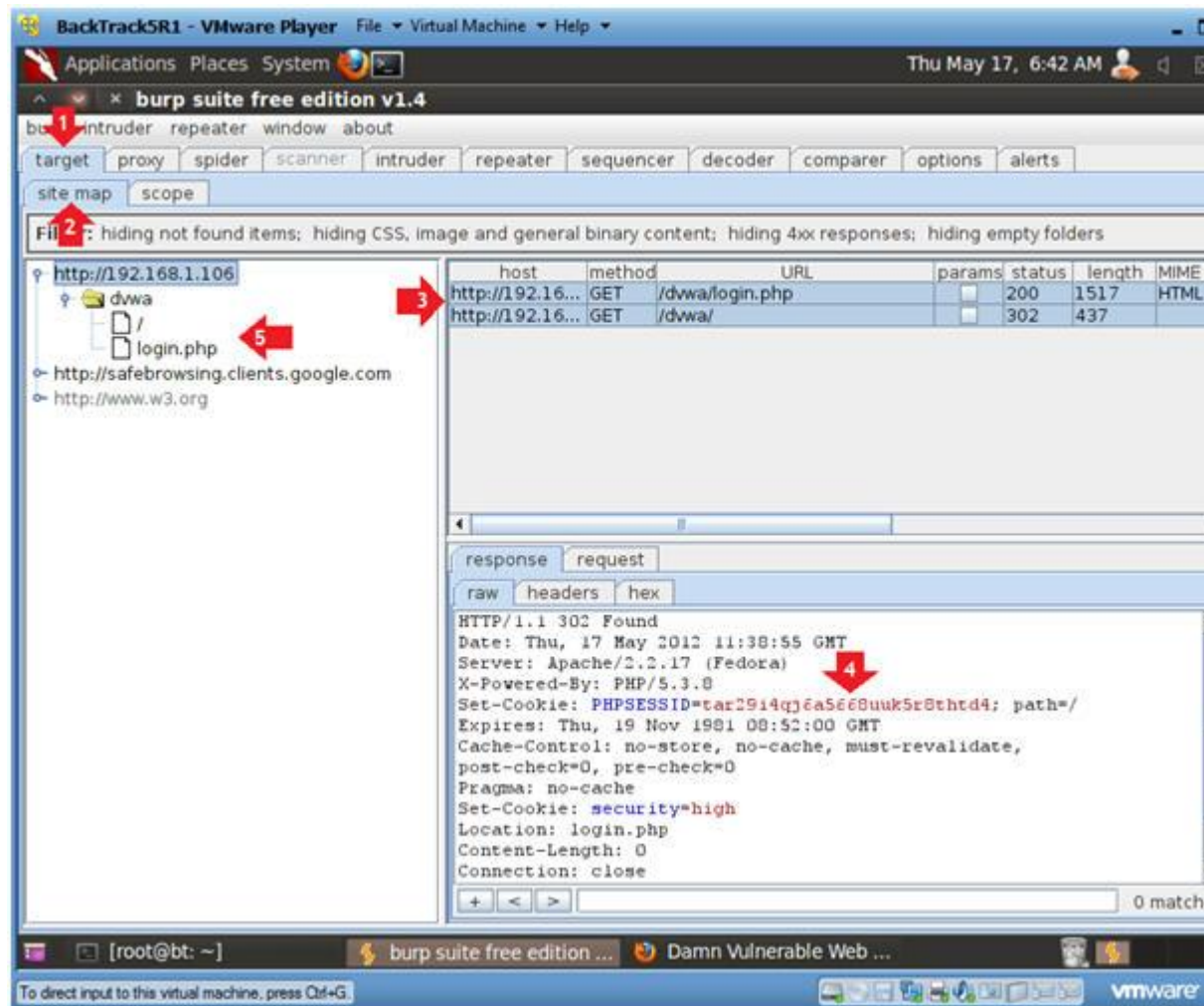
2. Target Host

- **Instructions:**

1. Click on the target tab
2. Click on the site map tab

- **Notes (FYI) :**

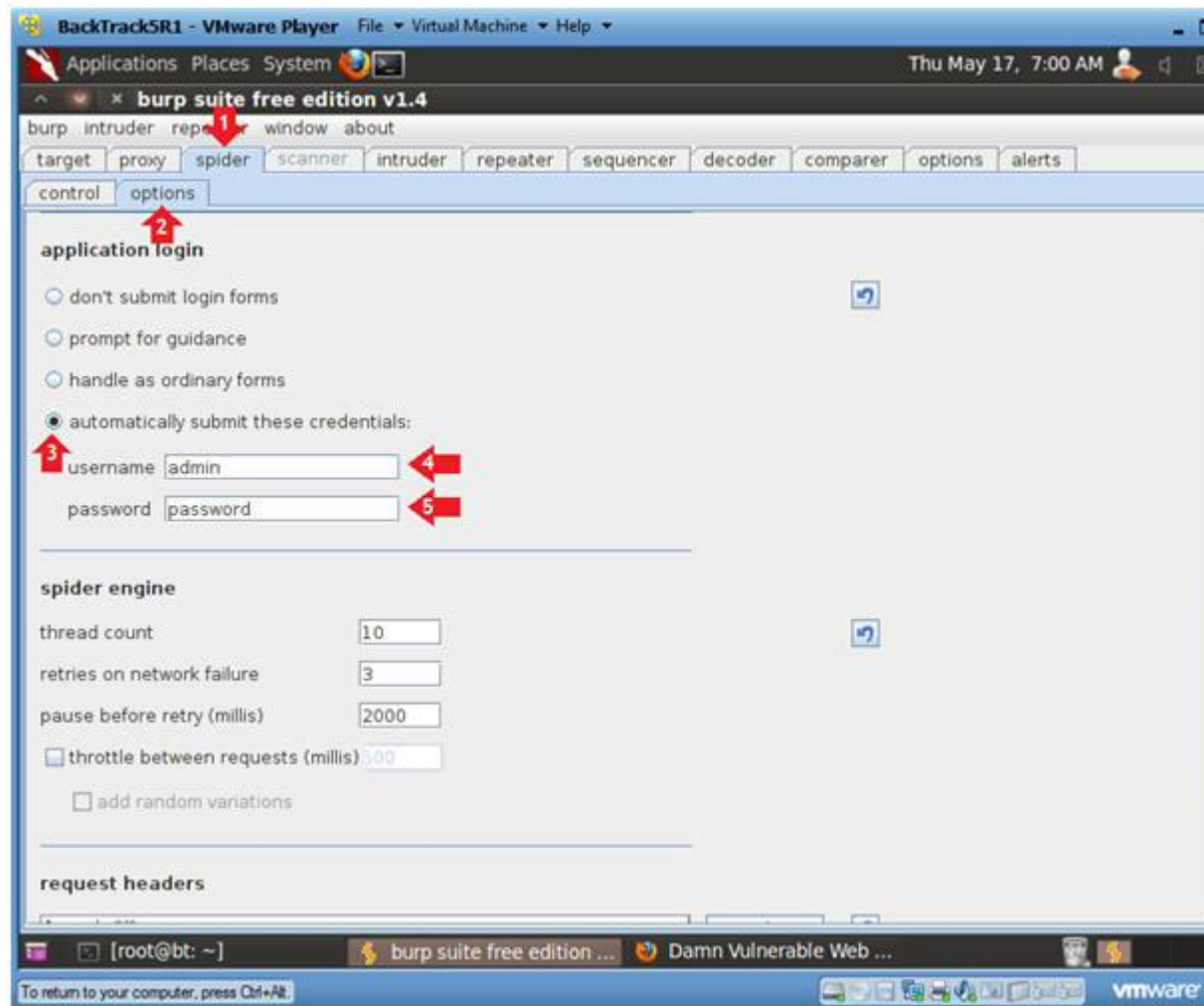
3. Although the intercept is turned off you are still able to see the contents of the requests.
4. In addition, you are able to see the contents of the get request including the PHPSESSID for /dvwa/login.php.
5. Notice, how a directory structure of the DVWA has been created for the login page.
6. Continue to Next Step.



3. Spider Configuration

o **Instructions:**

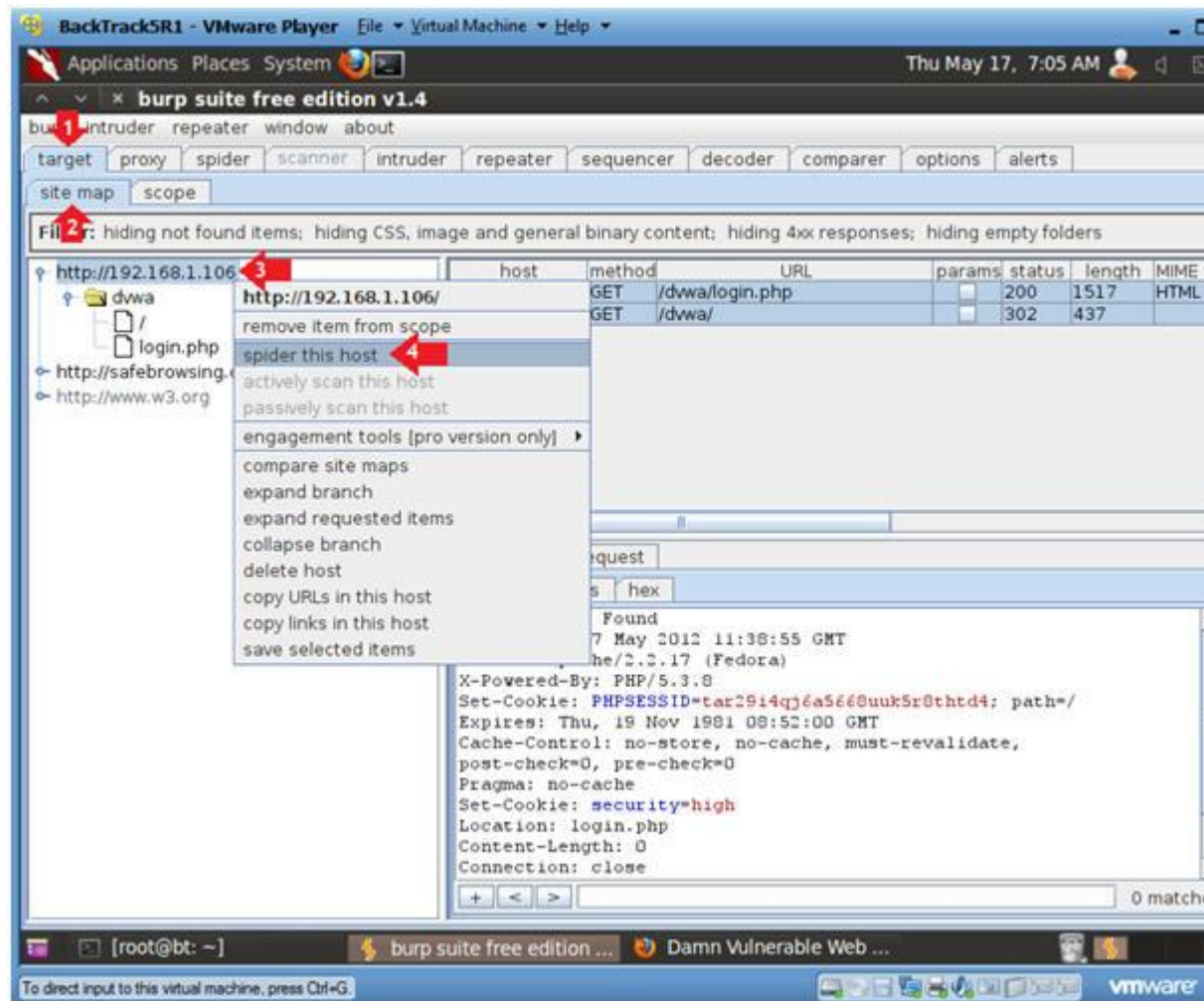
3. Click on the spider tab
4. Click on the options tab
5. Click on radio button "automatically submit these credentials"
6. Click on the request tab
7. username: admin
8. password: password



4. Spider Host

- **Instructions:**

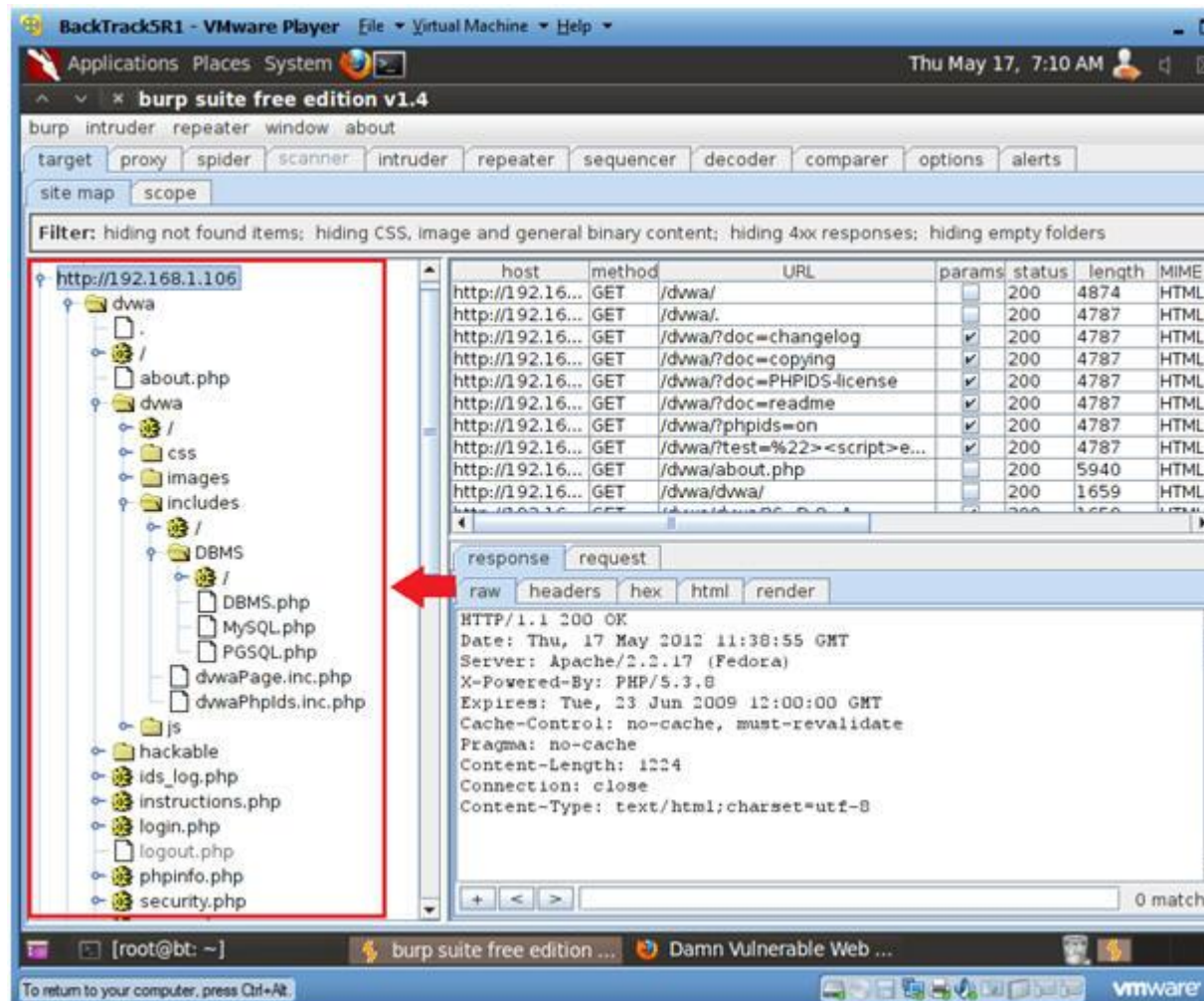
0. Click on the target tab
1. Click on the site map tab
2. Click on the DVWA IP Address, then Right Click to display utility menu.
3. Click on spider this host.
4. Continue to Next Step



5. Spider Directory True Results

Notes:

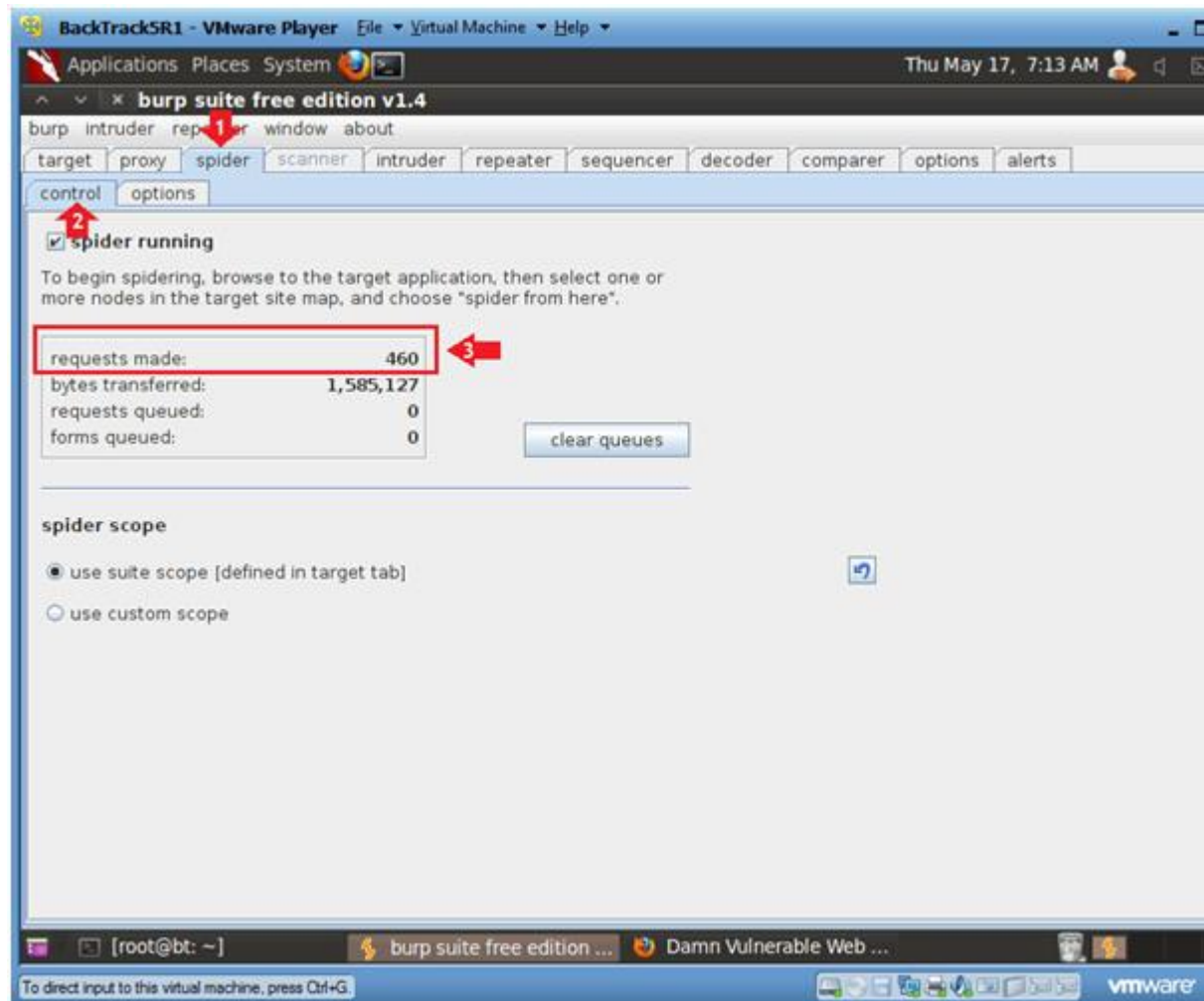
0. Notice that you now have a pretty accurate map of the DVWA
1. Continue to next step.



6. Spider Directory True Results

o **Instructions:**

0. Click on the spider tab
1. Click on the control tab
2. Notice that 460+/- requests were made to the DVWA website.
3. Continue to Next Step



Section 10: View Scan Results on Fedora DVWA web server

1. Viewing Apache's Access Log

o **Instructions:**

1. Go to the Fedora14 VM
2. Bring up a Terminal Windows
3. `su - root`
4. `cd /var/log/httpd`
5. `tail -400 access_log | more`
 - `tail -400`, means display the last 400 lines of the `access_log`. (I choose 400, because there 460 requests DVWA during the spider action)
 - `more`, means give it to me one screenful at a time.

```
Fedora14 - VMware Player File Virtual Machine Help
Applications Places System Thu May 17, 7:25 AM
root@Fedora14:/var/log/httpd
File Edit View Search Terminal Help
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]#
[root@Fedora14 ~]# cd /var/log/httpd/
[root@Fedora14 httpd]#
[root@Fedora14 httpd]# tail -400 access_log | more
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /dvwa/dvwa/images/?C=M;O=D HTTP/1.1" 200 2161 "http://192.168.1.106/dvwa/dvwa/images/?C=M;O=A" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /dvwa/vulnerabilities/xss_s/. HTTP/1.1" 200 5007 "http://192.168.1.106/dvwa/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /dvwa/vulnerabilities/xss_s/ HTTP/1.1" 200 5007 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/a.gif HTTP/1.1" 200 246 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/?C=N;O=D HTTP/1.1" 200 68393 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/a.png HTTP/1.1" 200 306 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/alert.black.png HTTP/1.1" 200 293 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/alert.black.gif HTTP/1.1" 200 242 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/?C=S;O=A HTTP/1.1" 200 68393 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/?C=M;O=A HTTP/1.1" 200 68393 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/alert.red.png HTTP/1.1" 200 314 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/alert.red.gif HTTP/1.1" 200 247 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/?C=D;O=A HTTP/1.1" 200 68393 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
192.168.1.105 - - [17/May/2012:07:09:44 -0500] "GET /icons/apache_pb.png HTTP/1.1" 200 68393 "http://192.168.1.106/icons/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)"
Click to switch to "Workspace"
root@Fedora14:/var/lo... root@Fedora14:/var/lo...
To direct input to this virtual machine, press Ctrl+G
```

2. Viewing Apache's Error Log

Instructions:

1. `cd /var/log/httpd`
2. `grep `date '+%a %b %d'` error_log | head`
 - `grep`, search and print lines matching a certain pattern.
 - ``date '+%a %b %d'``, display today's date where `%a` is the abbreviated weekday name, `%b` is the abbreviated month name, and `%d` is the abbreviated day name.
 - `error_log`, is apache's error_log. Events go in this log when (1) people/spiders are searching for something that doesn't exist or (2) people/spiders are sending passive/malicious instructions to a form.
 - `head`, show me the first 10 lines.
3. Notice how the burpsuite spider is searching for files that don't exist.

```
Fedora14 - VMware Player File Virtual Machine Help
Applications Places System Thu May 17, 7:36 AM
root@Fedora14:/var/log/httpd
File Edit View Search Terminal Help
[root@Fedora14 httpd]# grep 'date '+%a %b %d'' error_log | head
grep: May: No such file or directory
grep: 17: No such file or directory
error_log:[Thu May 17 06:27:05 2012] [notice] SELinux policy enabled; httpd running as context system_u:sys
em_r:httpd t:s0
error_log:[Thu May 17 06:27:05 2012] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
error_log:[Thu May 17 06:27:05 2012] [notice] Digest: generating secret for digest authentication ...
error_log:[Thu May 17 06:27:05 2012] [notice] Digest: done
error_log:[Thu May 17 06:27:06 2012] [warn] ./mod_dnssd.c: No services found to register
error_log:[Thu May 17 06:27:06 2012] [notice] Apache/2.2.17 (Unix) DAV/2 PHP/5.3.8 configured -- resuming n
ormal operations
error_log:[Thu May 17 06:38:56 2012] [error] [client 192.168.1.105] File does not exist: /var/www/html/favi
on.ico
error_log:[Thu May 17 06:38:56 2012] [error] [client 192.168.1.105] File does not exist: /var/www/html/favi
on.ico
error_log:[Thu May 17 07:09:41 2012] [error] [client 192.168.1.105] File does not exist: /var/www/html/robo
s.txt
error_log:[Thu May 17 07:09:41 2012] [error] [client 192.168.1.105] Directory index forbidden by Options di
rective: /var/www/html/
[root@Fedora14 httpd]#
```

Section 11: Clean Up Notes

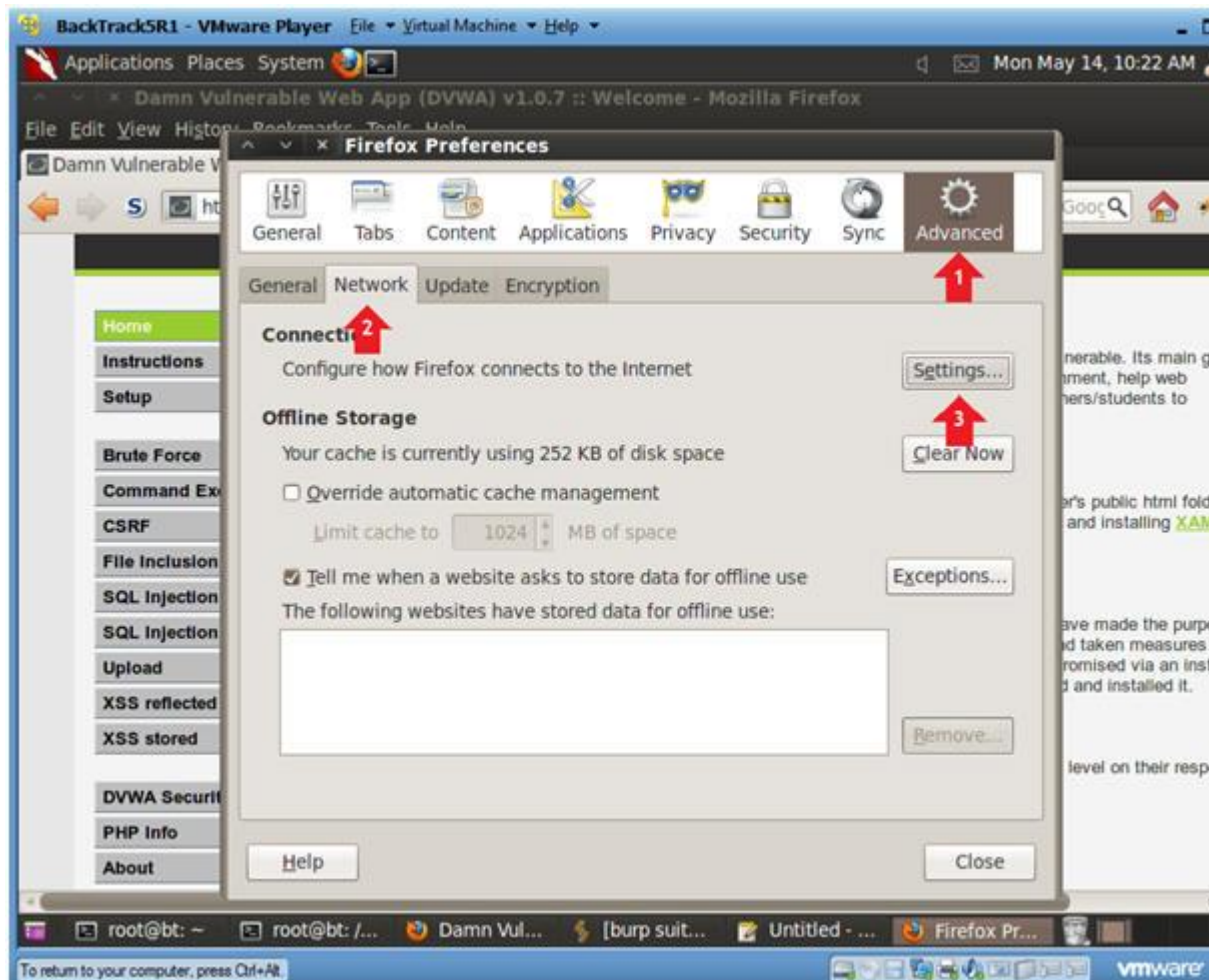
1. On BackTrack's Firefox
 - **Instructions:**
 1. Edit --> Preferences



2. Edit Network Settings

o **Instructions:**

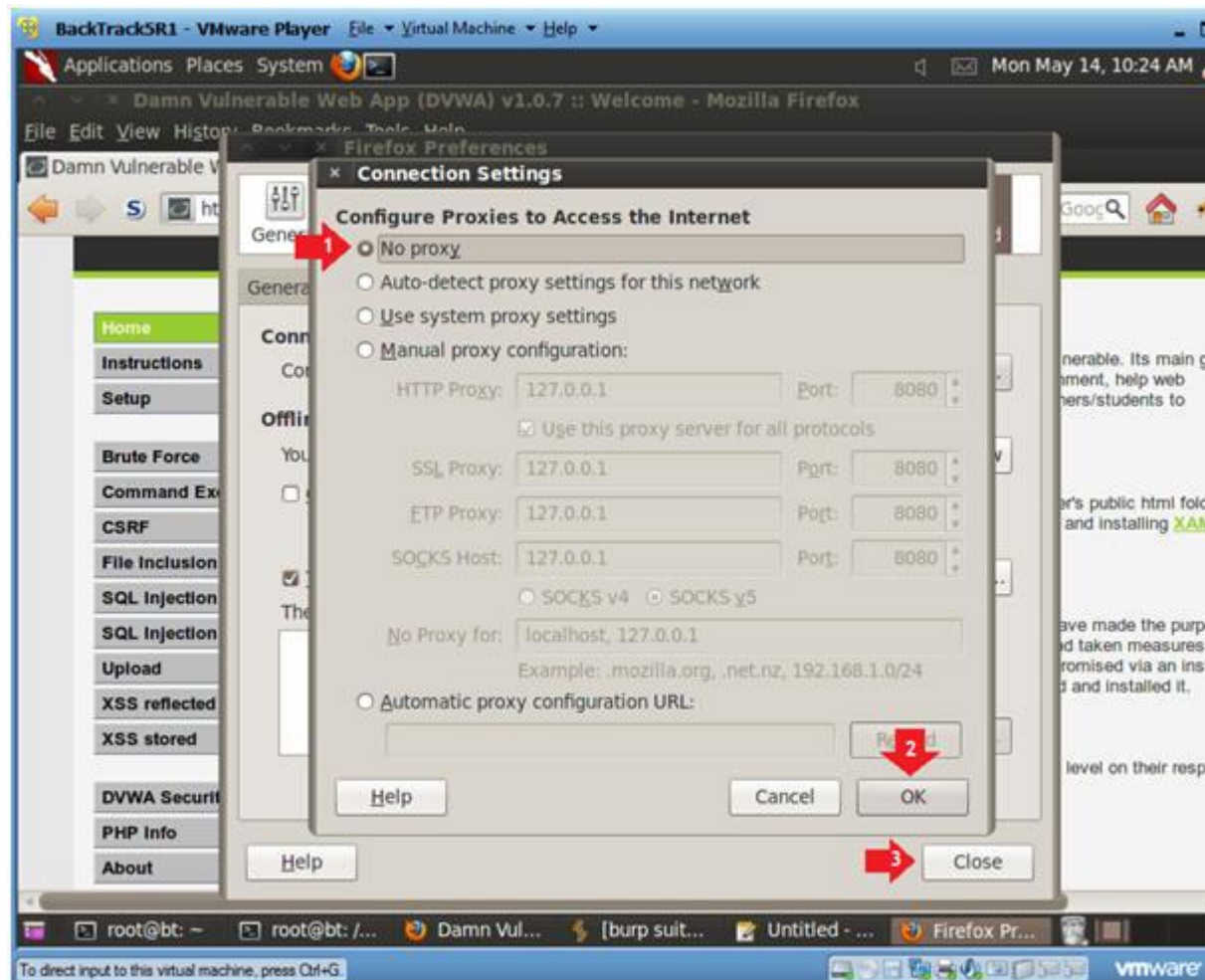
1. Click on Advanced
2. Click on Network Tab.
3. Click on Settings Button.



3. Configure Connection Settings

- **Instructions:**

1. Click on No proxy radio button
2. Click on the OK Button
3. Click on the Close button



Section 12: Proof of Lab

1. Proof of Lab

o **Proof of Lab Instructions:**

1. On Fedora, pull up a terminal window.
2. `cd /var/log/httpd`
3. `grep `date '+%d/%b/%Y'` access_log | wc -l`
 - `wc -l`, count how many lines grep found for today's data in `access_log`.
4. `date`
5. `echo "Your Name"`
 - Replace the string "Your Name" with your actual name.
 - e.g., `echo "John Gray"`
6. Do a <PrtScn>
7. Paste into a word document
8. Upload to Moodle

Fedora14 - VMware Player File Virtual Machine Help

Applications Places System Thu May 17, 7:48 AM

root@Fedora14:/var/log/httpd

File Edit View Search Terminal Help

```
[root@Fedora14 ~]# cd /var/log/httpd/
[root@Fedora14 httpd]#
[root@Fedora14 httpd]# grep 'date '+%d/%b/%Y' access_log | wc -l
468
[root@Fedora14 httpd]# date
Thu May 17 07:48:43 CDT 2012
[root@Fedora14 httpd]#
[root@Fedora14 httpd]# echo "Your Name"
Your Name
[root@Fedora14 httpd]#
```

root@Fedora14:/var/lo... root@Fedora14:/var/lo...

To direct input to this virtual machine, press Ctrl+G.

vmware