(Damn Vulnerable Web App (DVWA))

{ Burp Suite, Spider Function }

Section 0. Background Information

1. What is Damn Vulnerable Web App (DVWA)?
   - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application t
     damn vulnerable.
   - Its main goals are to be an aid for security professionals to t
     skills and tools in a legal environment, help web developers be
     understand the processes of securing web applications and aid
     teachers/students to teach/learn web application security in a
     environment.

2. What is Burp Suite?
   - Burp suite is a java application that can be used to secure or
     applications. The suite consists of different tools, like a pro
     a web spider an intruder and a so called repeater, with which r
     can be automated.

3. Pre-Requisite Labs
   - Damn Vulnerable Web App (DVWA): Lesson 1: How to Install DVWA in Fedora 14
   - BackTrack: Lesson 1: Installing BackTrack 5 R1

4. **Lab Notes**
   - 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 Firef
     3. We will use Burp Suite to spider the DVWA web application.
     4. We will conduct a very simple forensics investigation on F
        Web Server, in which the DVWA web application resides.

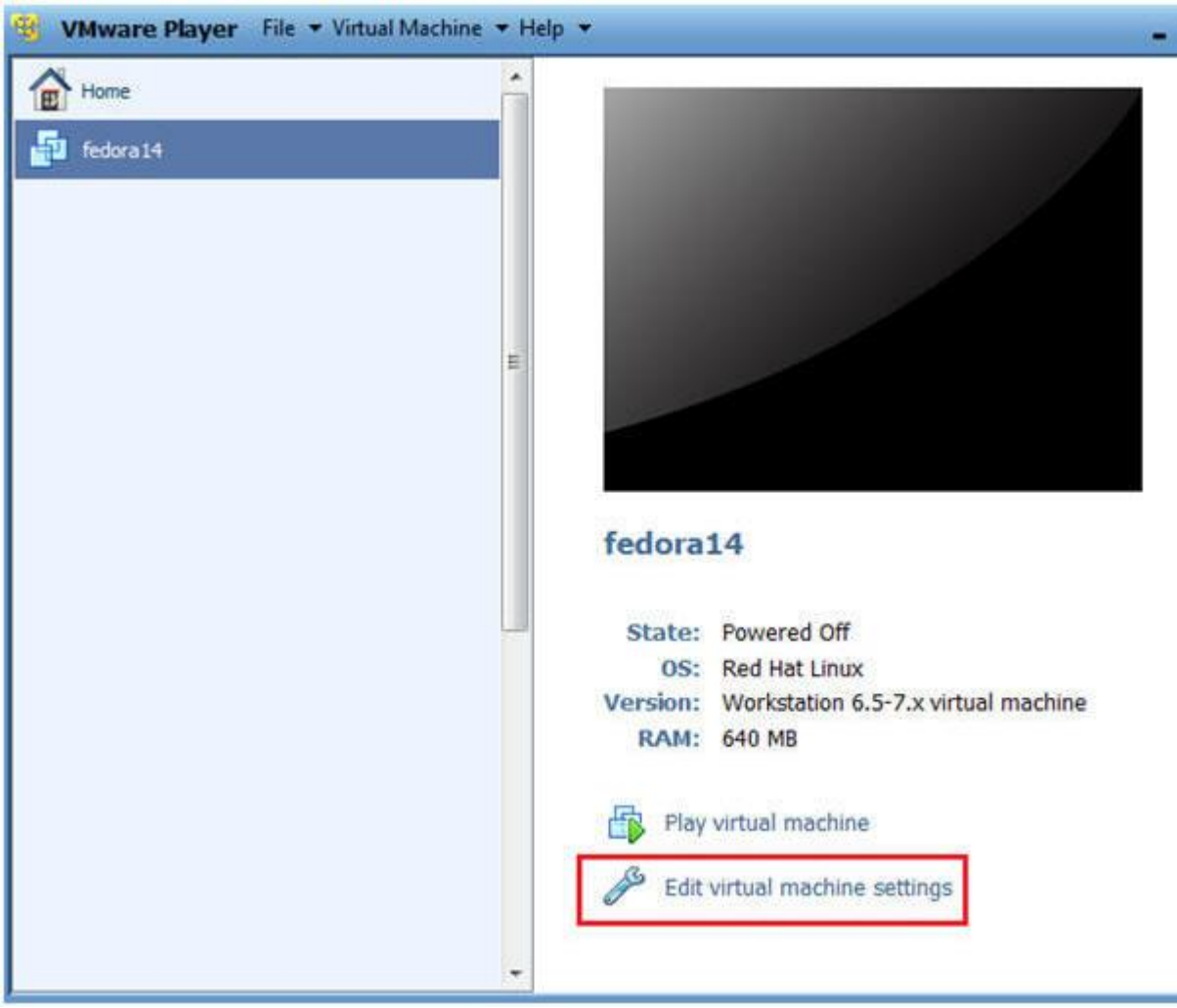
5. Legal Disclaimer
   - **As a condition of your use of this Web site, you warrant to computersecuritystudent.com that you will not use this Web site purpose that is unlawful or that is prohibited by these terms, conditions, and notices.**

- **In accordance with UCC § 2-316, this product is provided with "warranties, either expressed or implied." The information conta provided "as-is", with "no guarantee of merchantability."**
- **In addition, this is a teaching website that does not condone m behavior of any kind.**
- **Your are on notice, that continuing and/or using this lab outsi "own" test environment is considered malicious and is against t**
-

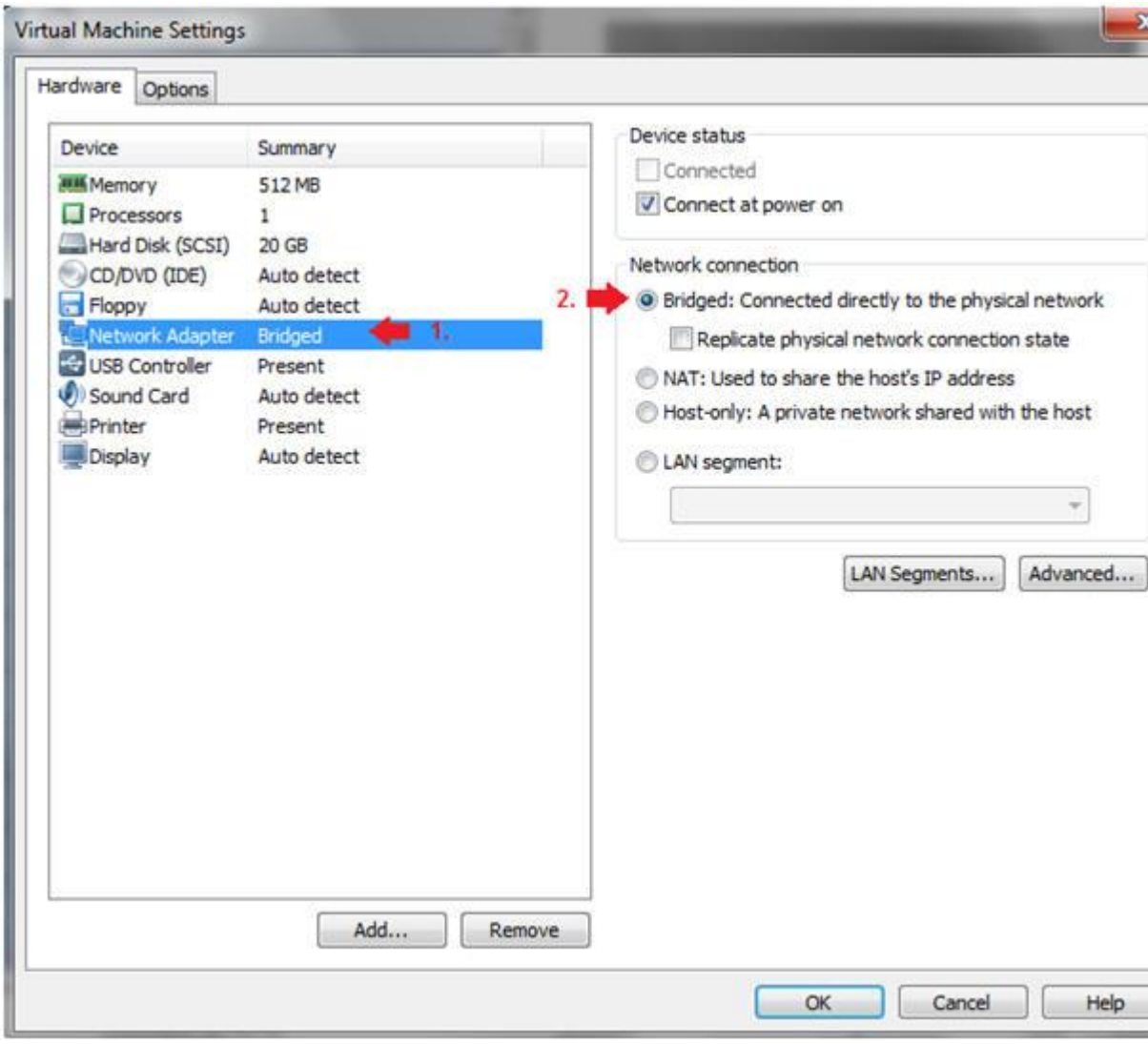
Section 1: Configure Fedora14 Virtual Machine Settings

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

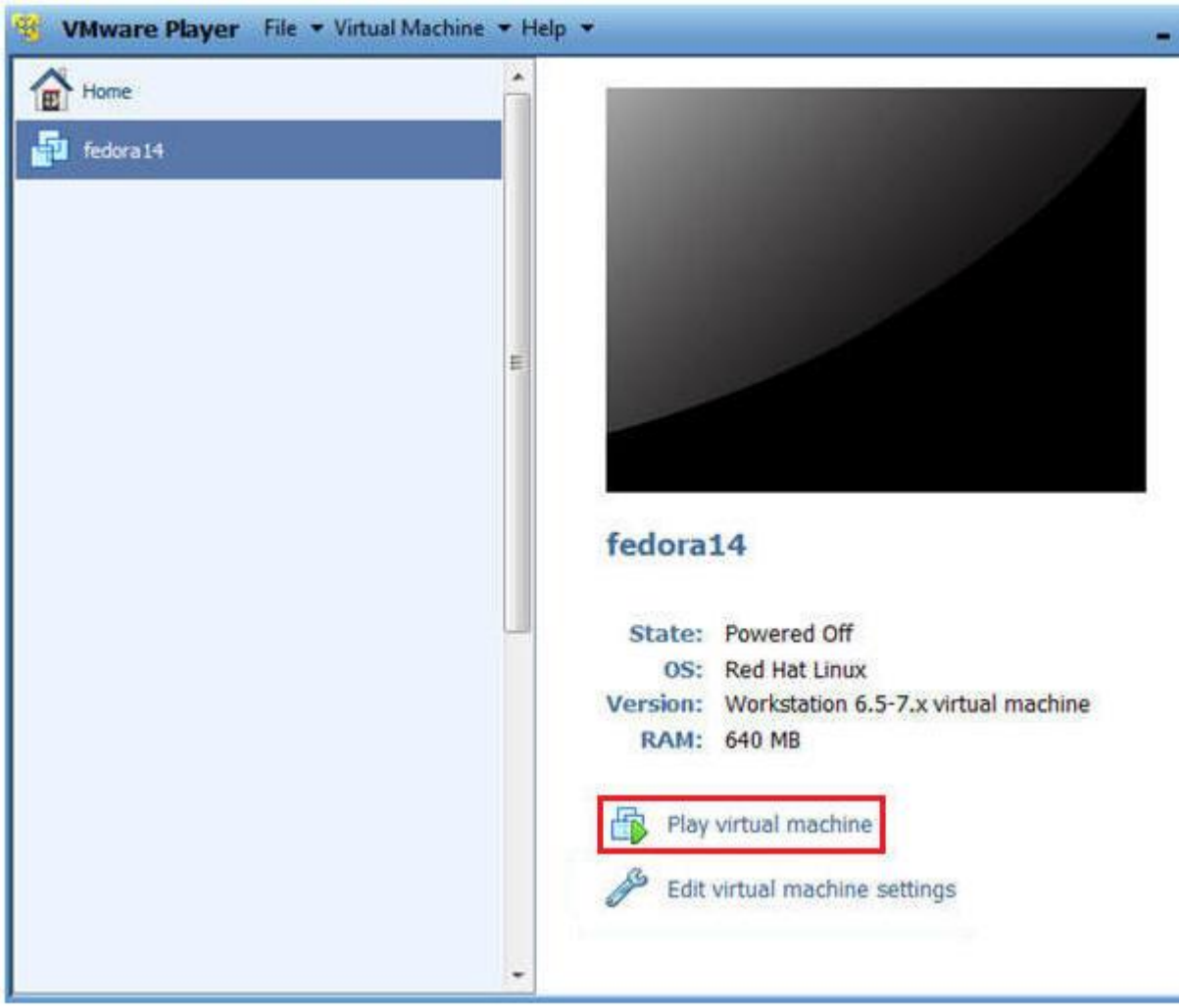
- 

3. Edit Network Adapter
    - **Instructions:**
        1. Highlight Network Adapter
        2. Select Bridged
        3. Click on the OK Button.

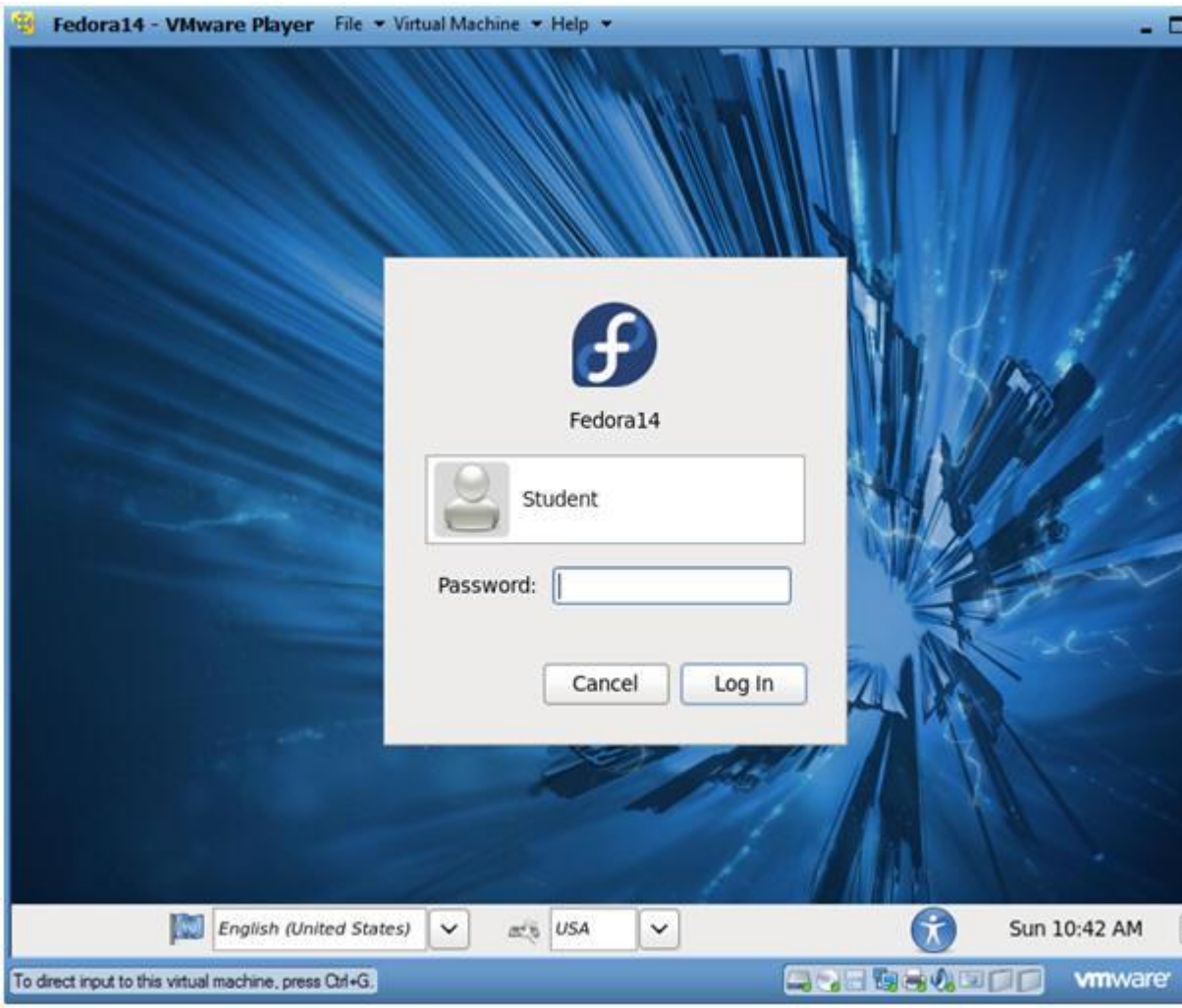


Section 2: Login to Fedora14

1. Start Fedora14 VM Instance
    - **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>.

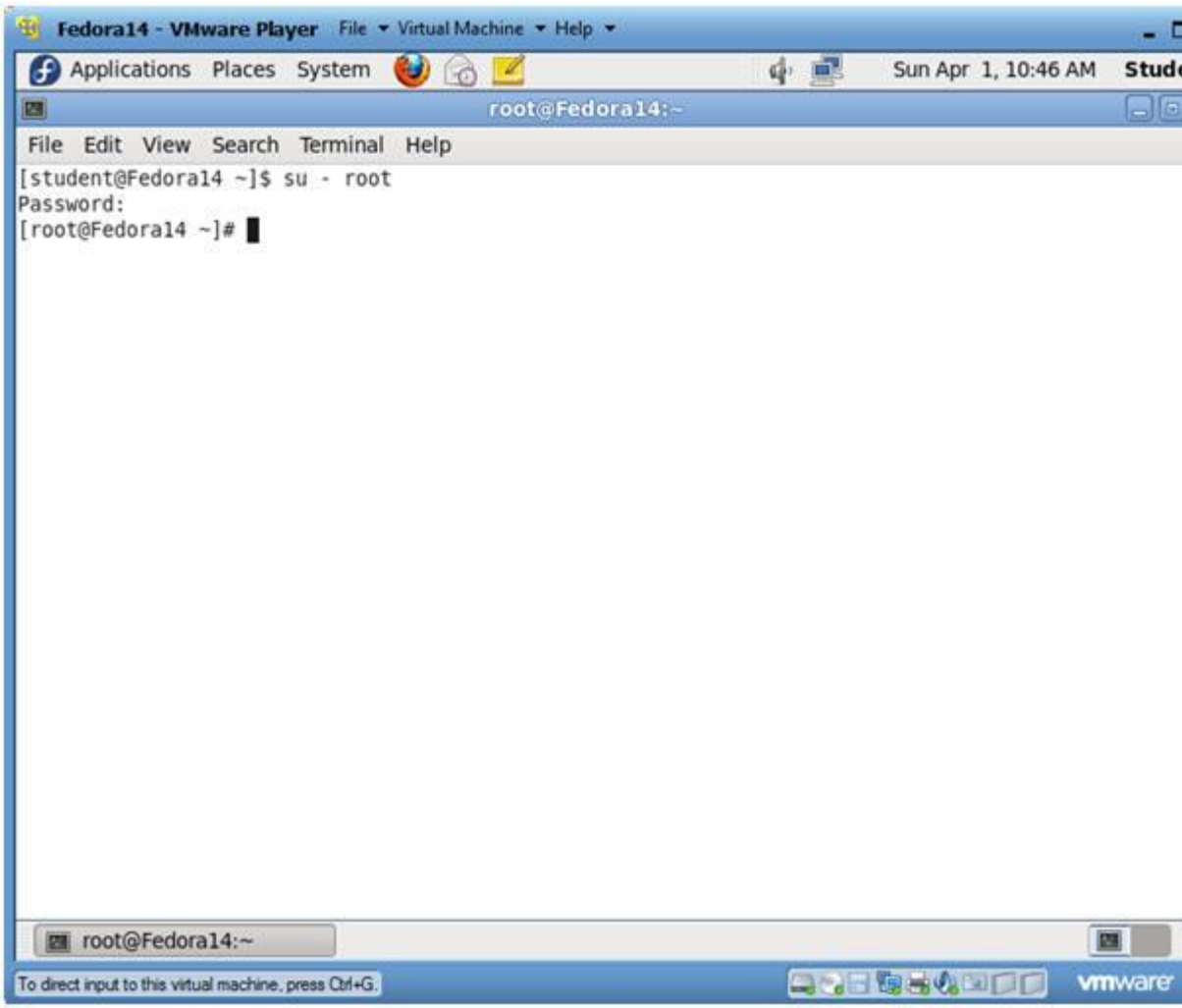
- 

Section 3: Open Console Terminal and Retrieve IP Address

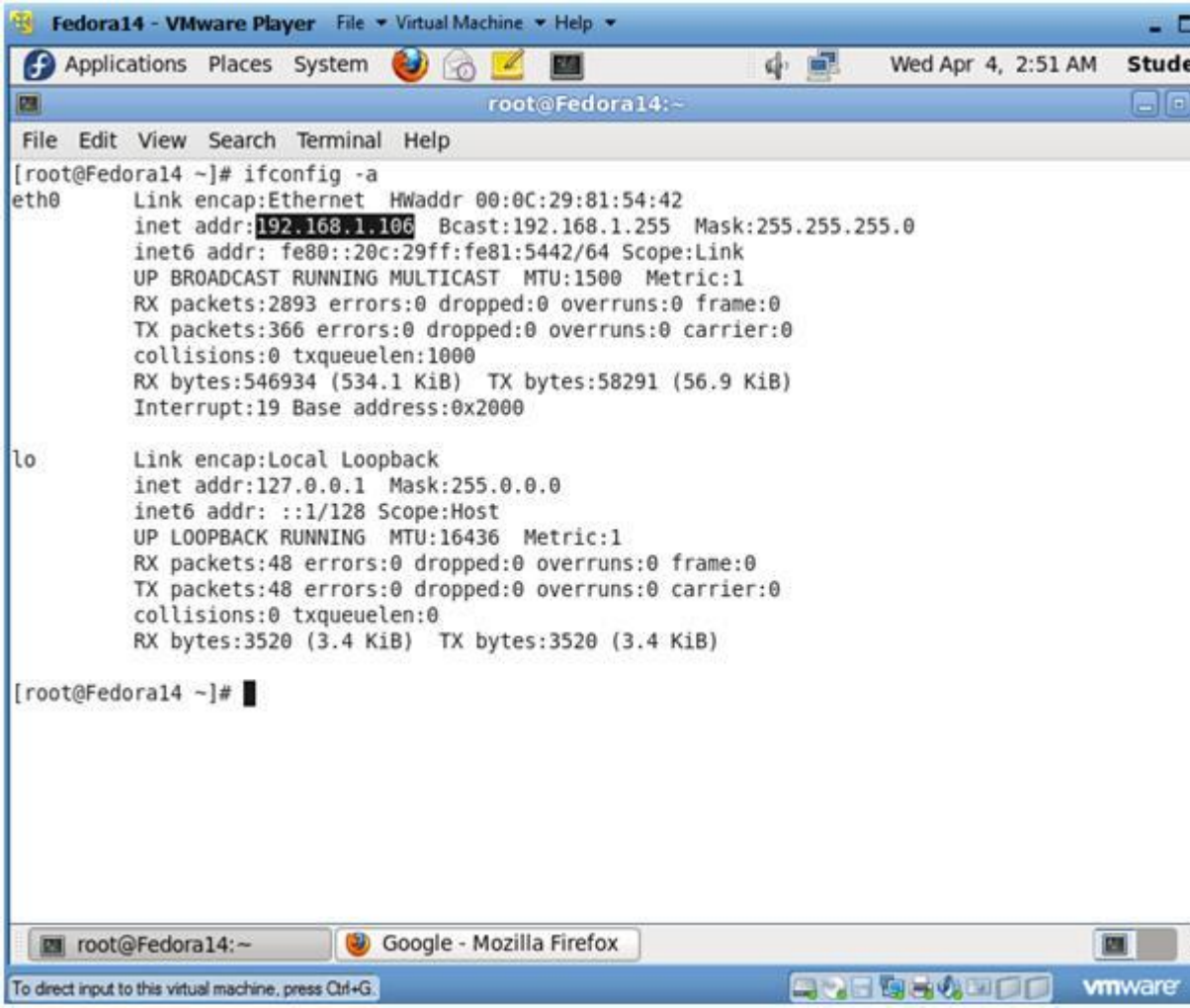
1. Start a Terminal Console
    - **Instructions:**
        1. Applications --> Terminal

- 

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

- 

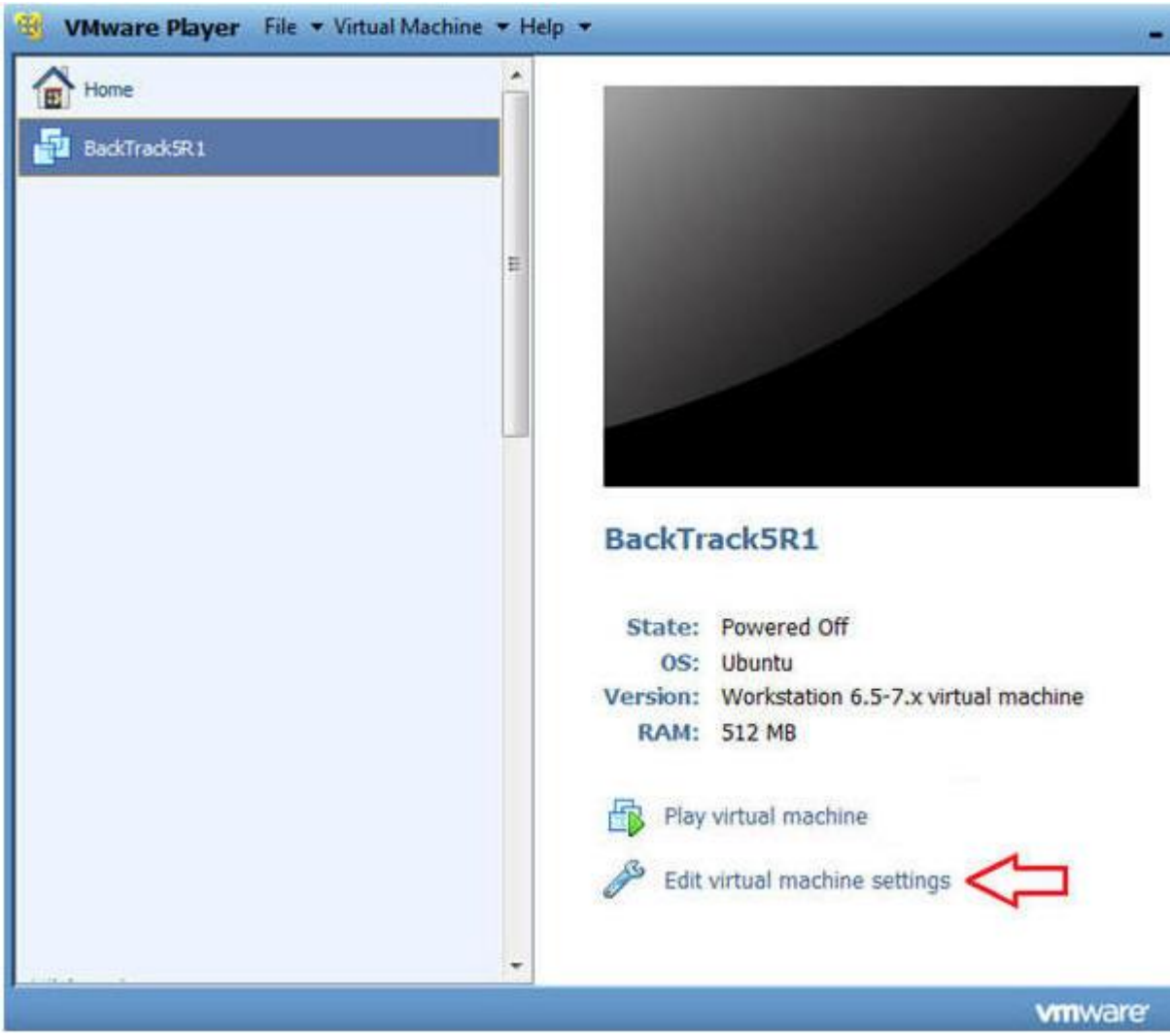
3. Get IP Address
   - **Instructions:**
     1. ifconfig -a
   - **Notes:**
     - As indicated below, my IP address is 192.168.1.106.
     - Please record your IP address.

- 

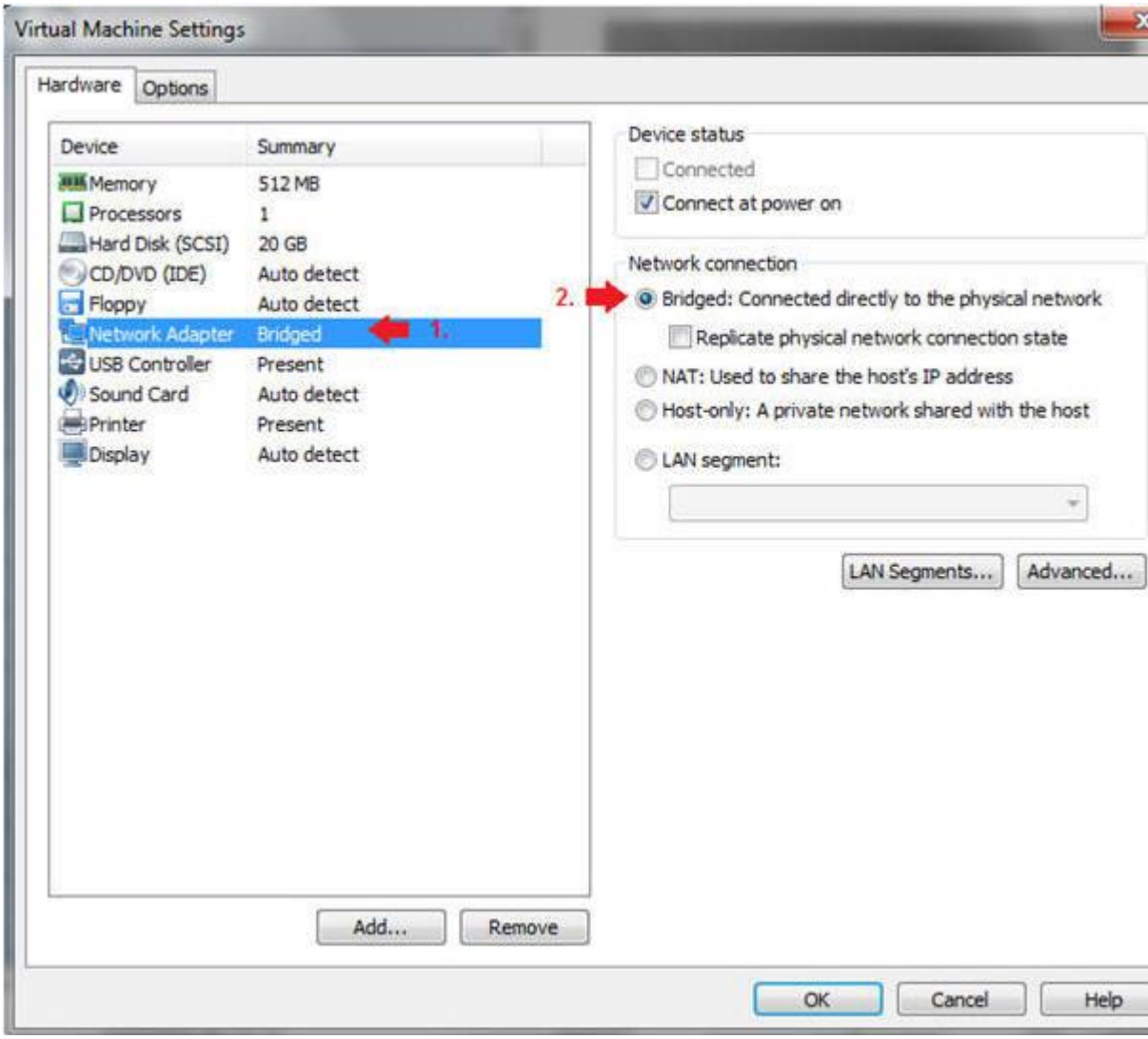
Section 4: Configure BackTrack Virtual Machine Settings

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

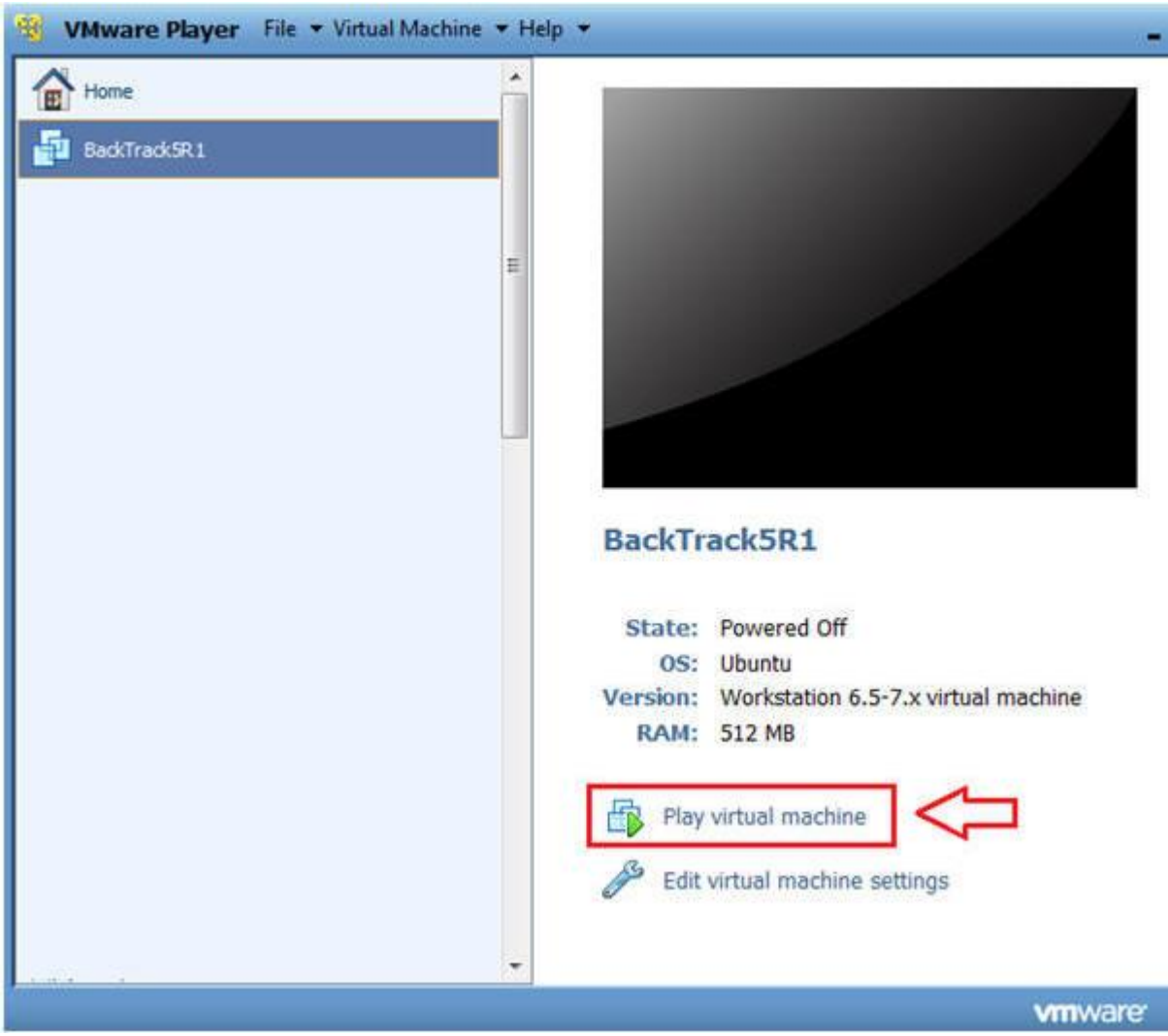
- 

3. Edit Network Adapter
    - **Instructions:**
        1. Highlight Network Adapter
        2. Select Bridged
        3. Do not Click on the OK Button.

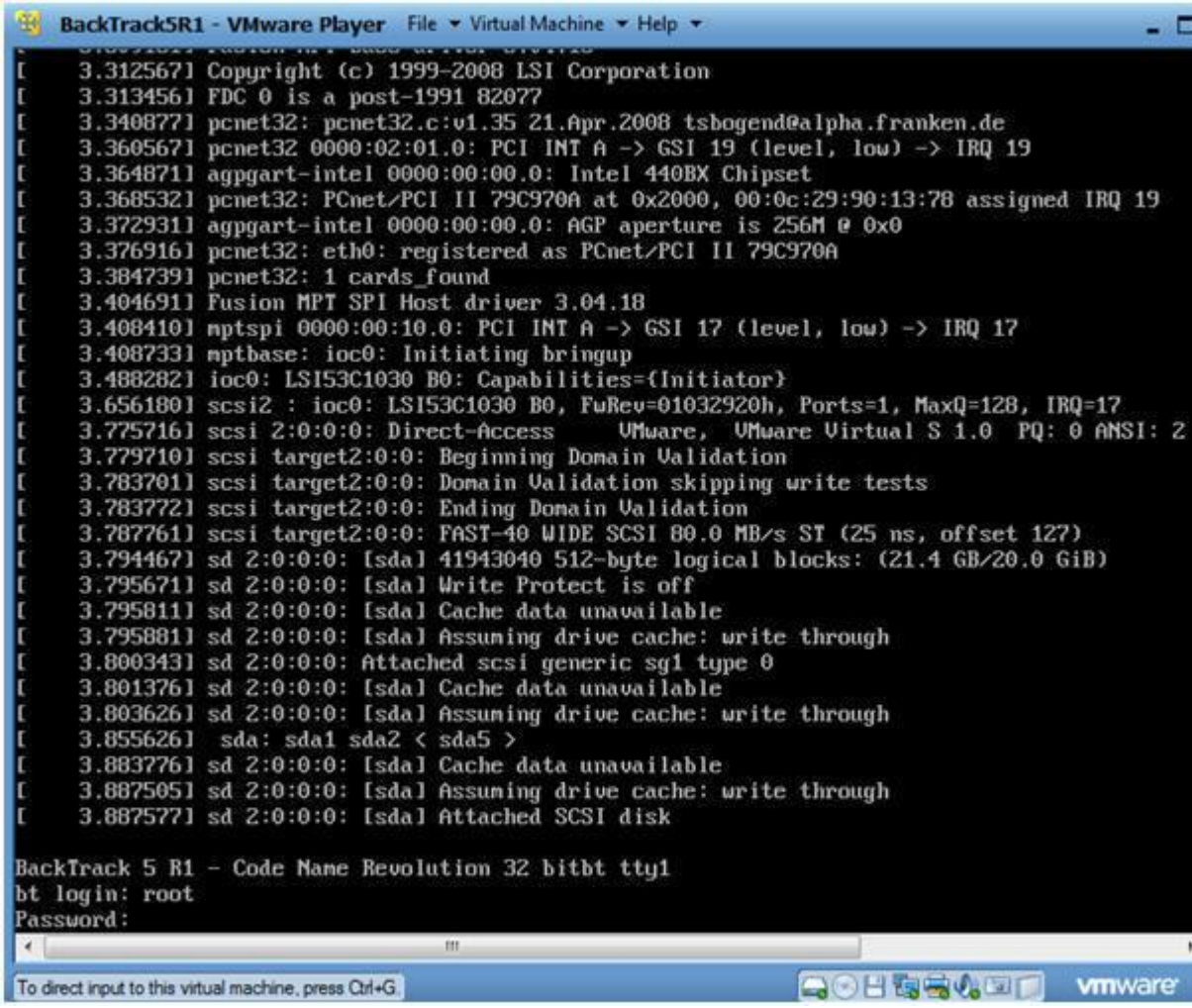
- 

Section 5: Login to BackTrack

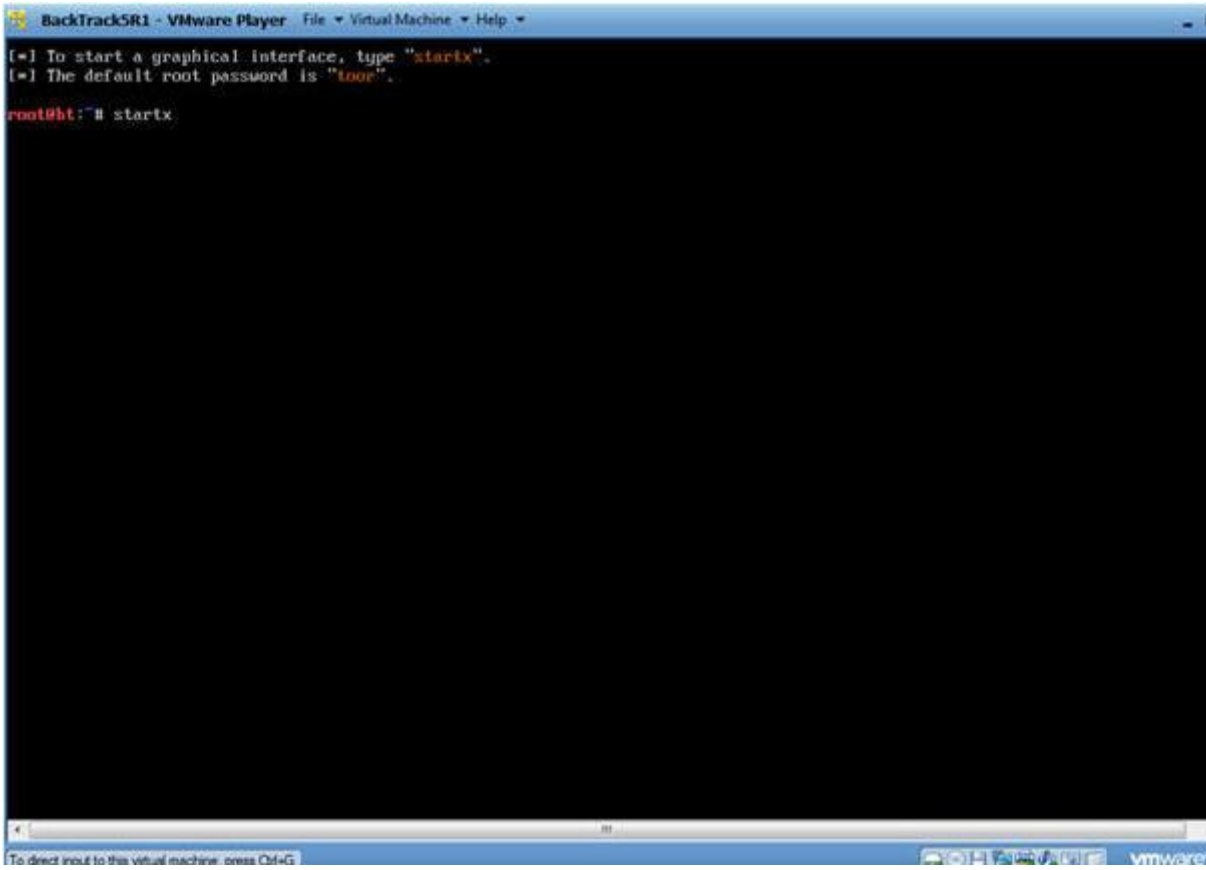
1. Start BackTrack VM Instance
    - **Instructions:**
        1. Start Up VMWare Player
        2. Select BackTrack5R1
        3. Play virtual machine

- 

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

- 

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

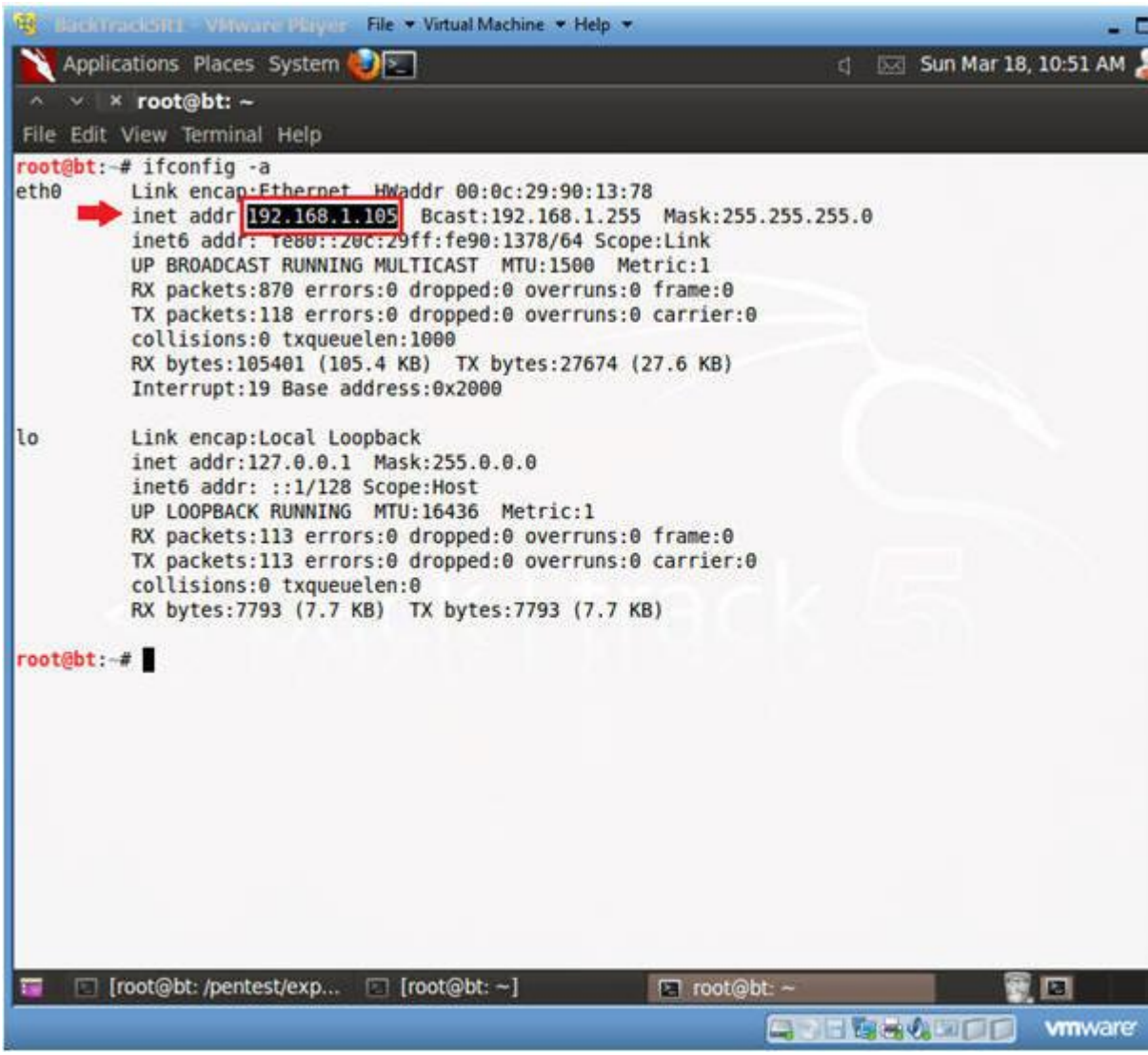
- 

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.

- 

Section 7: Configure Firefox Proxy Settings

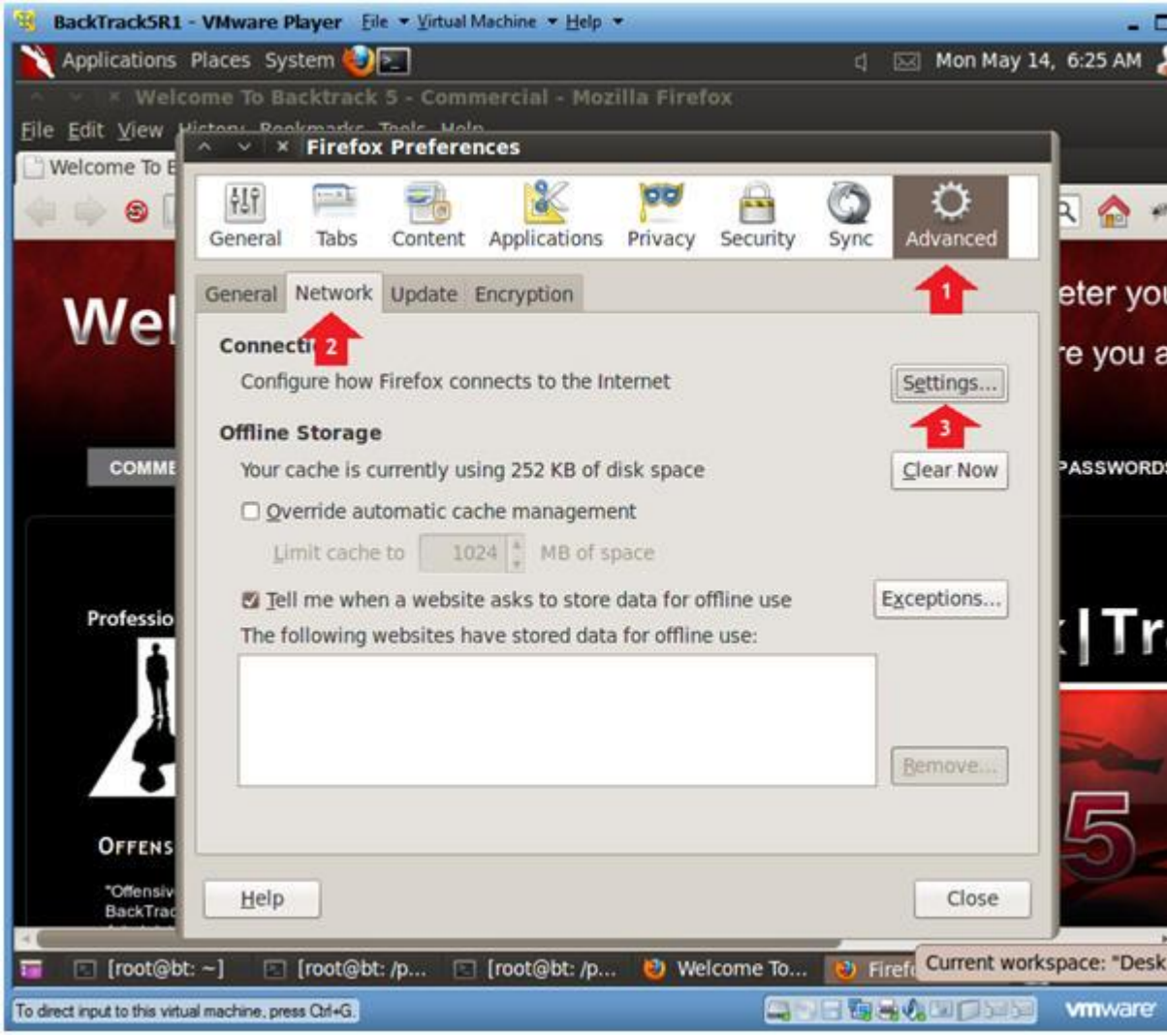
1. Start Firefox
   - **Instructions:**
     1. Click on Firefox

- 

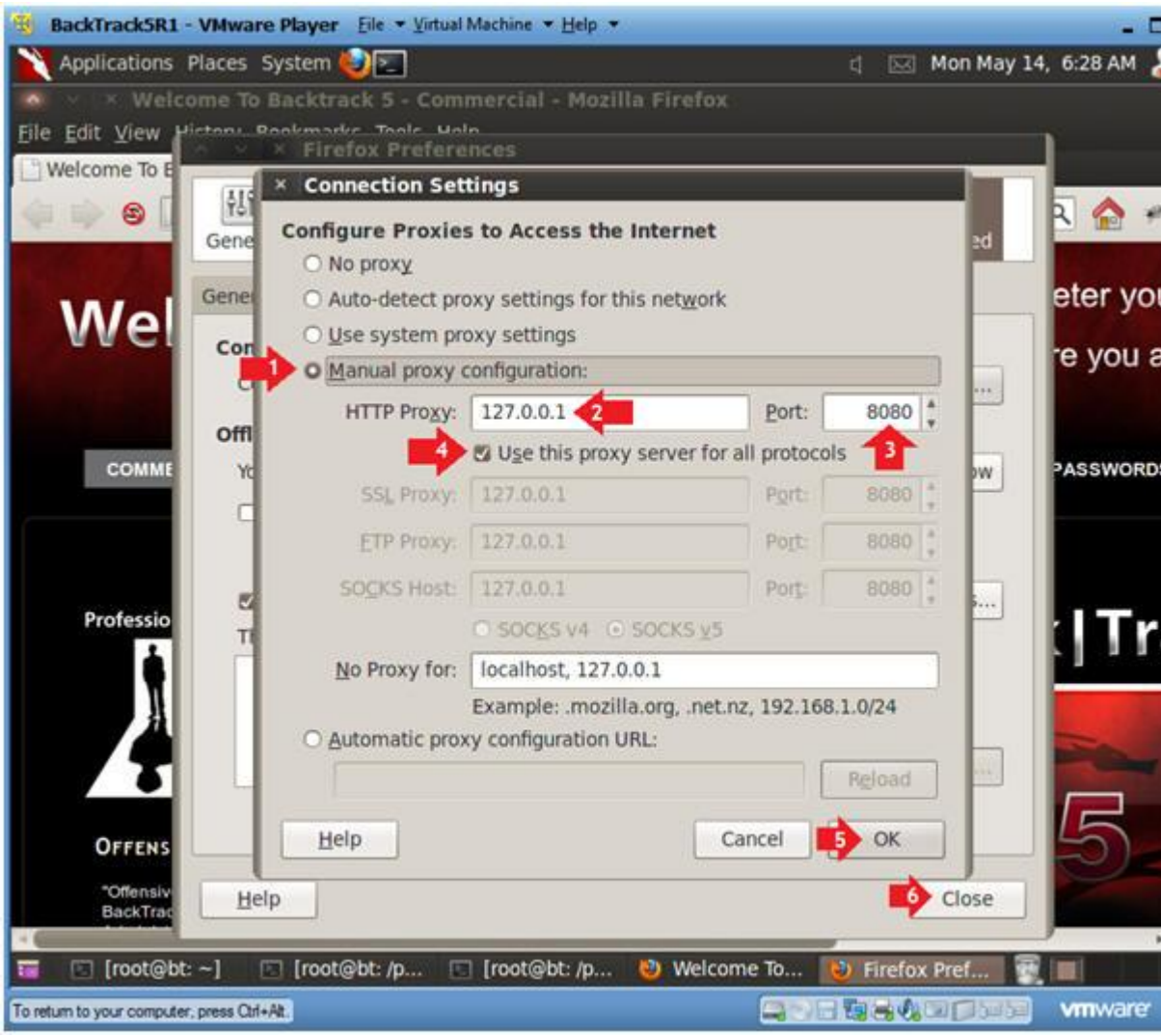
2. Preferences
    - **Instructions:**
        1. Edit --> Preferences

- 

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

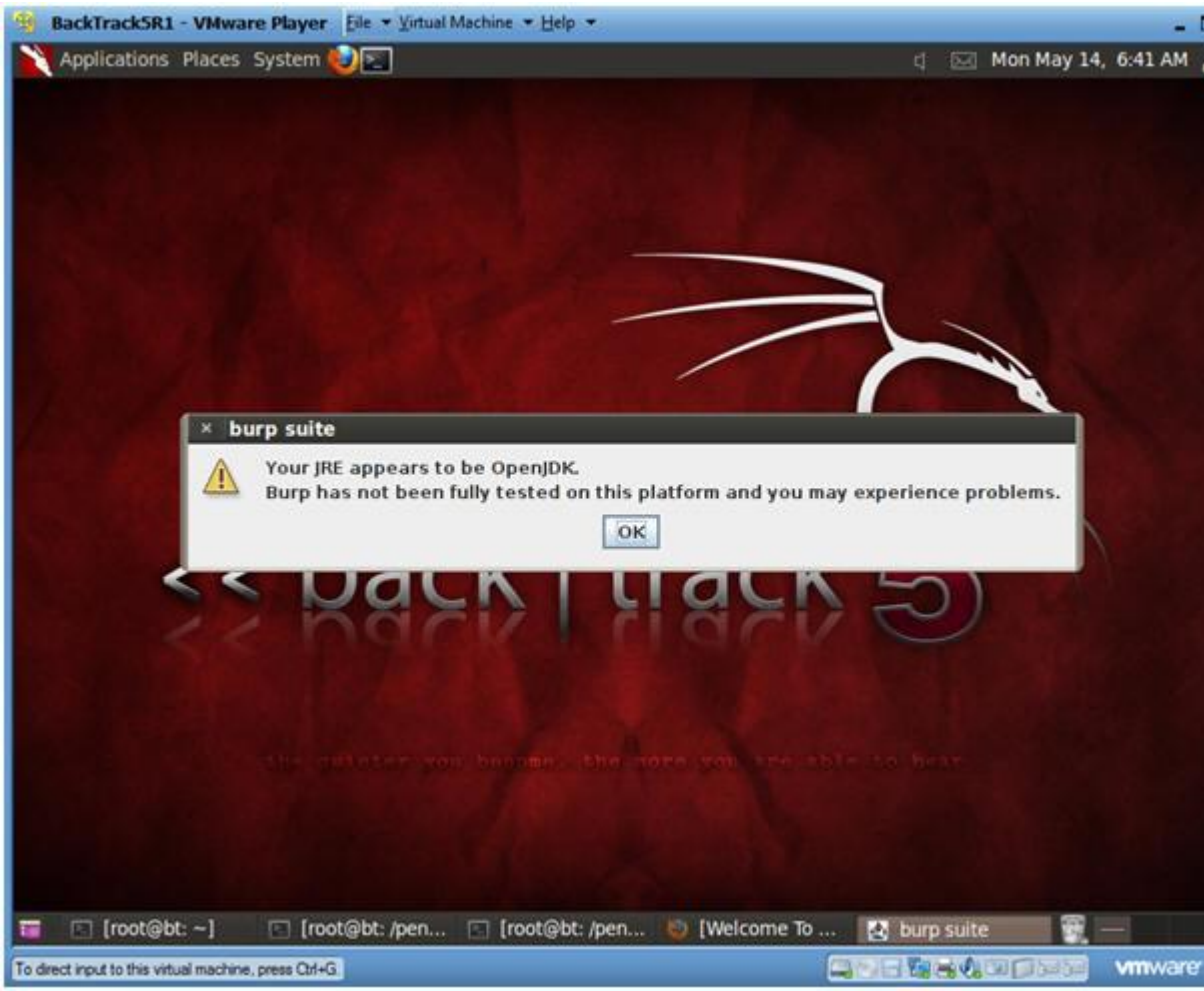
- 

Section 8: Configure Burp Suite

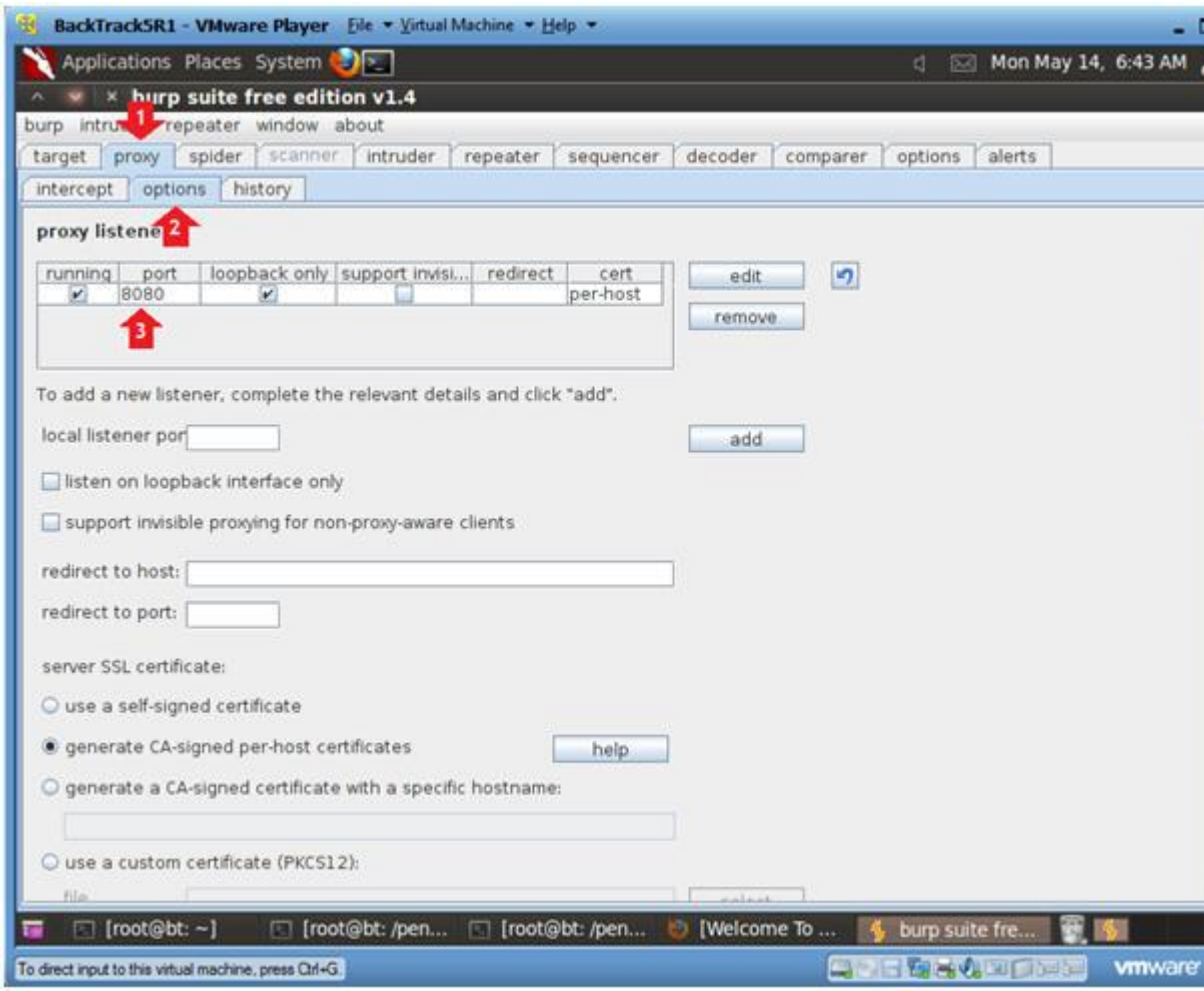
1. Start Burp Suite
   - **Instructions:**
     1. Applications --> Vulnerability Assessment --> Web Applicat
        Assessment ---> Web Vulnerability Scanner --> burpsuite

- 

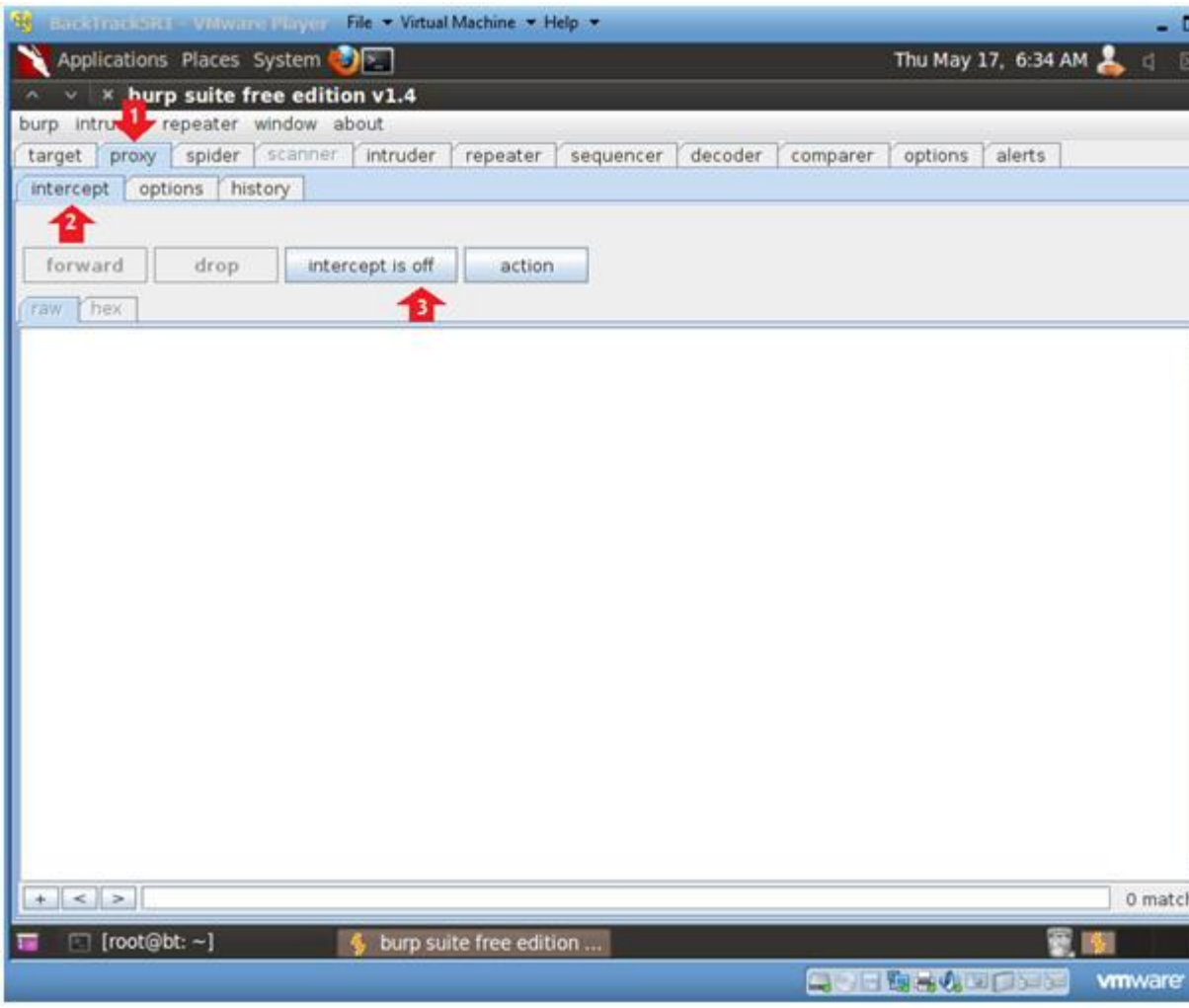
2. JRE Message
    - **Instructions:**
        1. Click OK

- 

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
   - **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"

- 

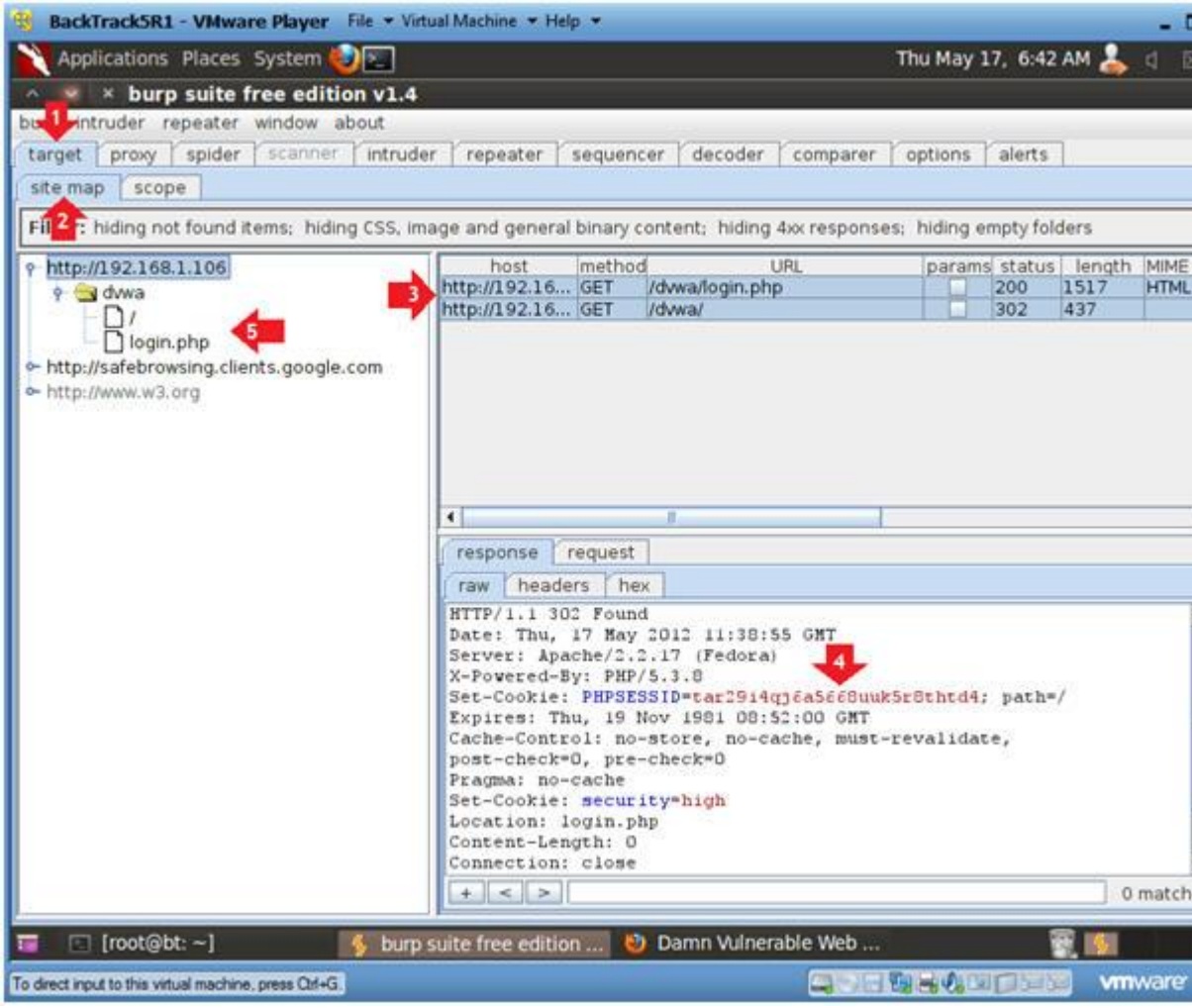
Section 9: Spider with Burp Suite

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

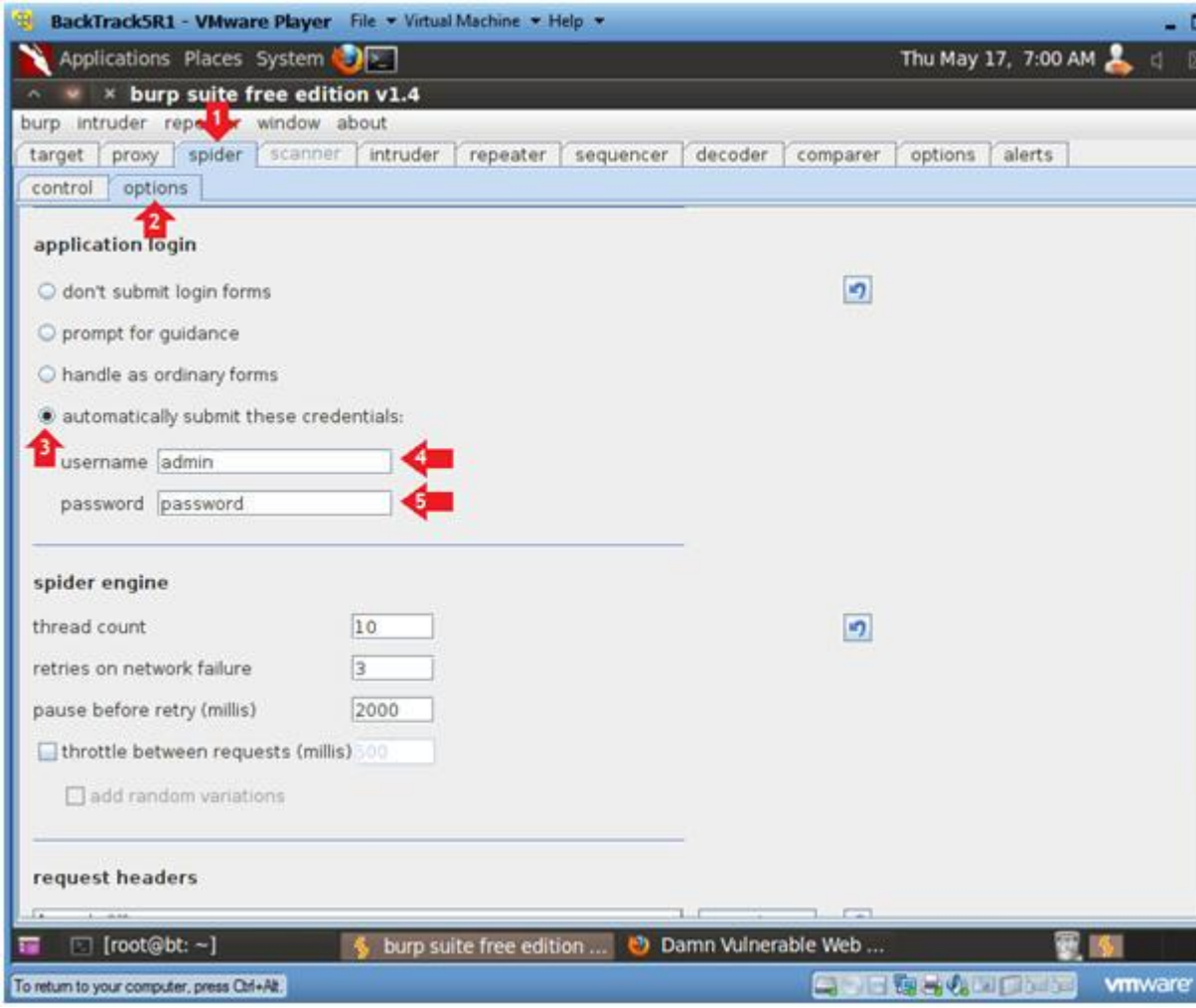
- 

2. Target Host
   - **Instructions:**
     1. Click on the target tab
     2. Click on the site map tab
   - **Notes(FYI):**

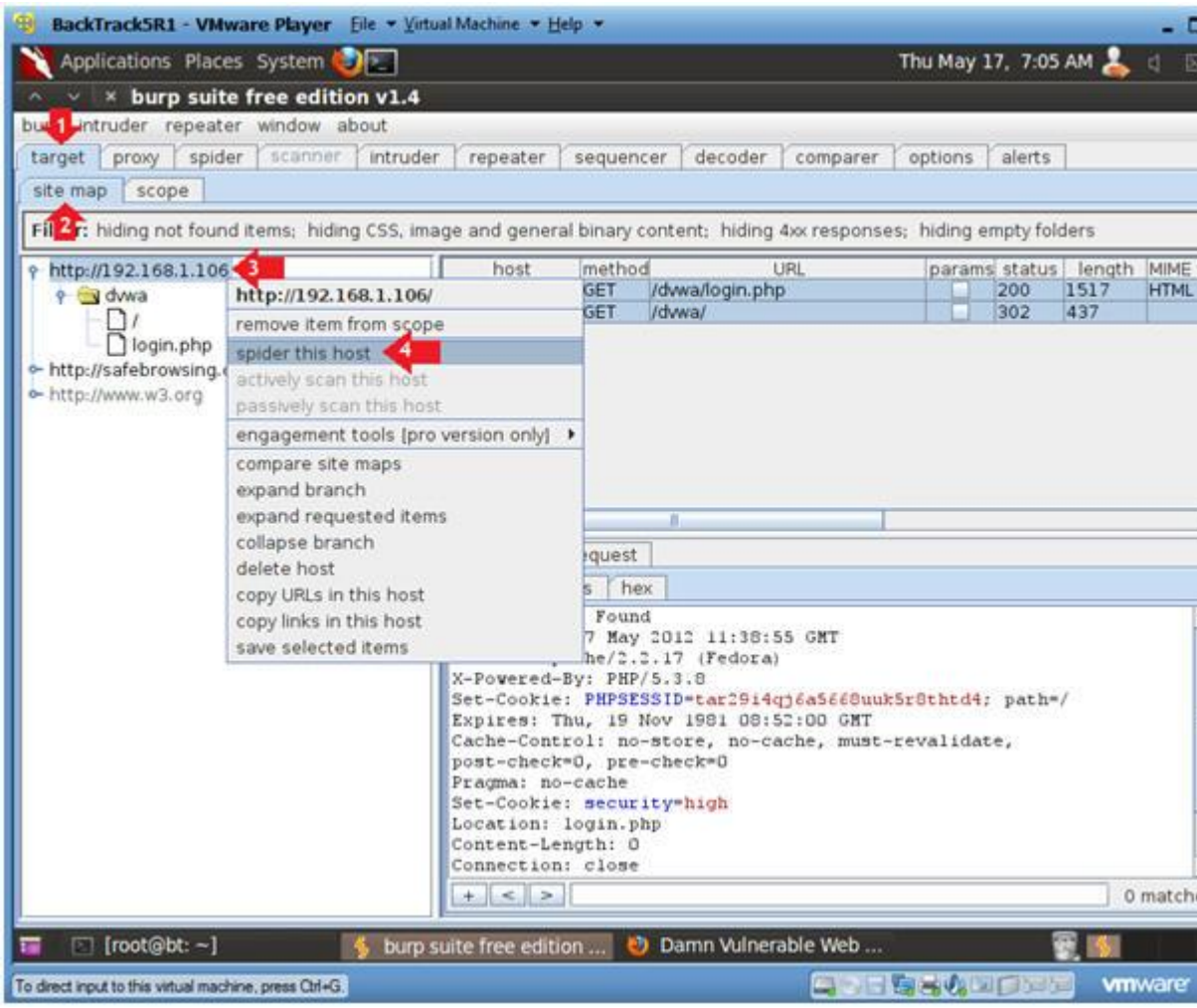
     3. Although the intercept is turned off you are still able to
        requests.
     4. In addition, you are able to see the contents of the get r
        including the PHPSESSID for /dvwa/login.php.
     5. Notice, how a directory structure of the DVWA has been cre
        the login page.
     6. Continue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

- 

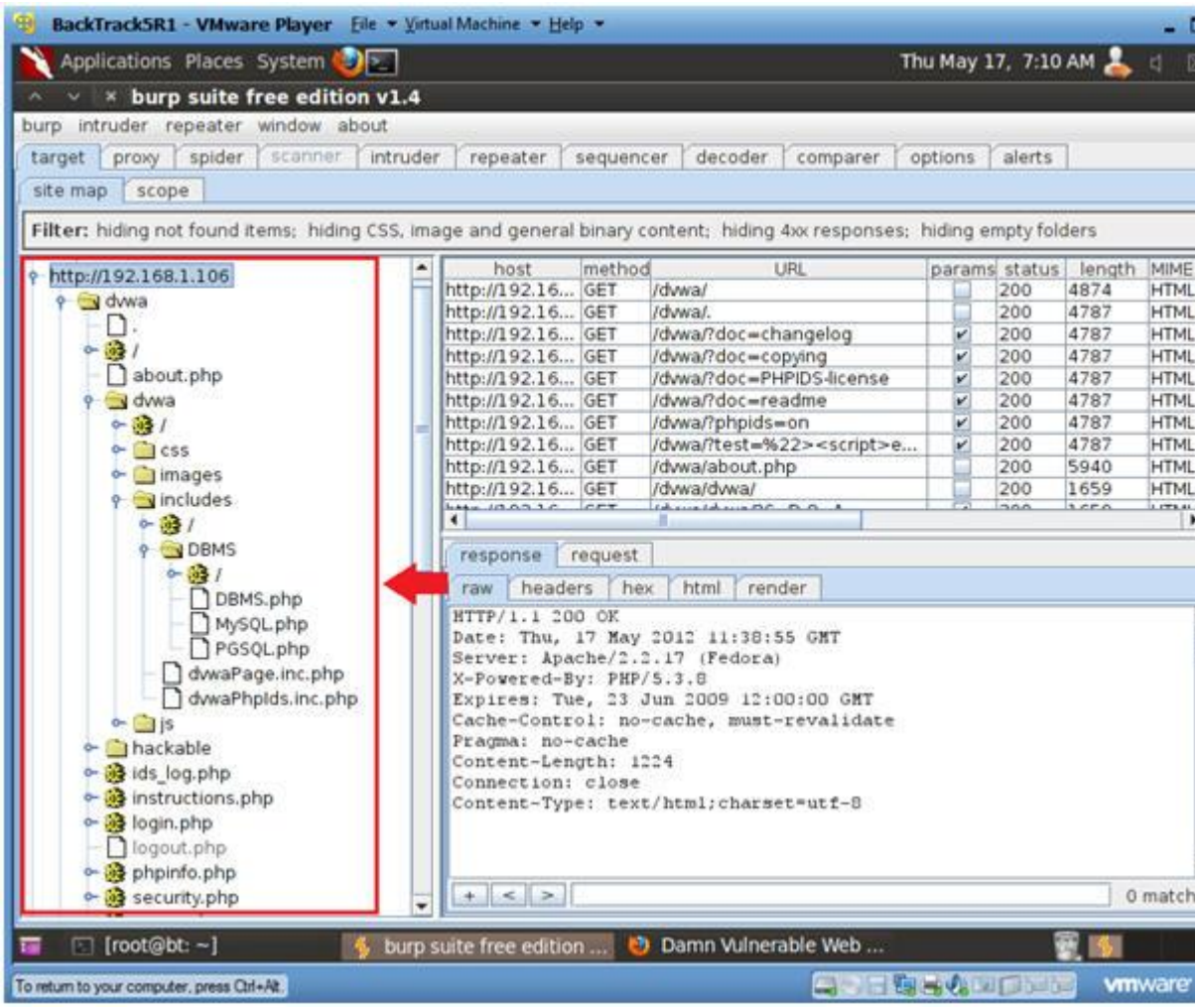
3. Spider Configuration
    - **Instructions:**
        3. Click on the spider tab
        4. Click on the options tab
        5. Click on radio button "automatically submit these credenti
        6. Click on the request tab
        7. username: admin
        8. password: password

- 

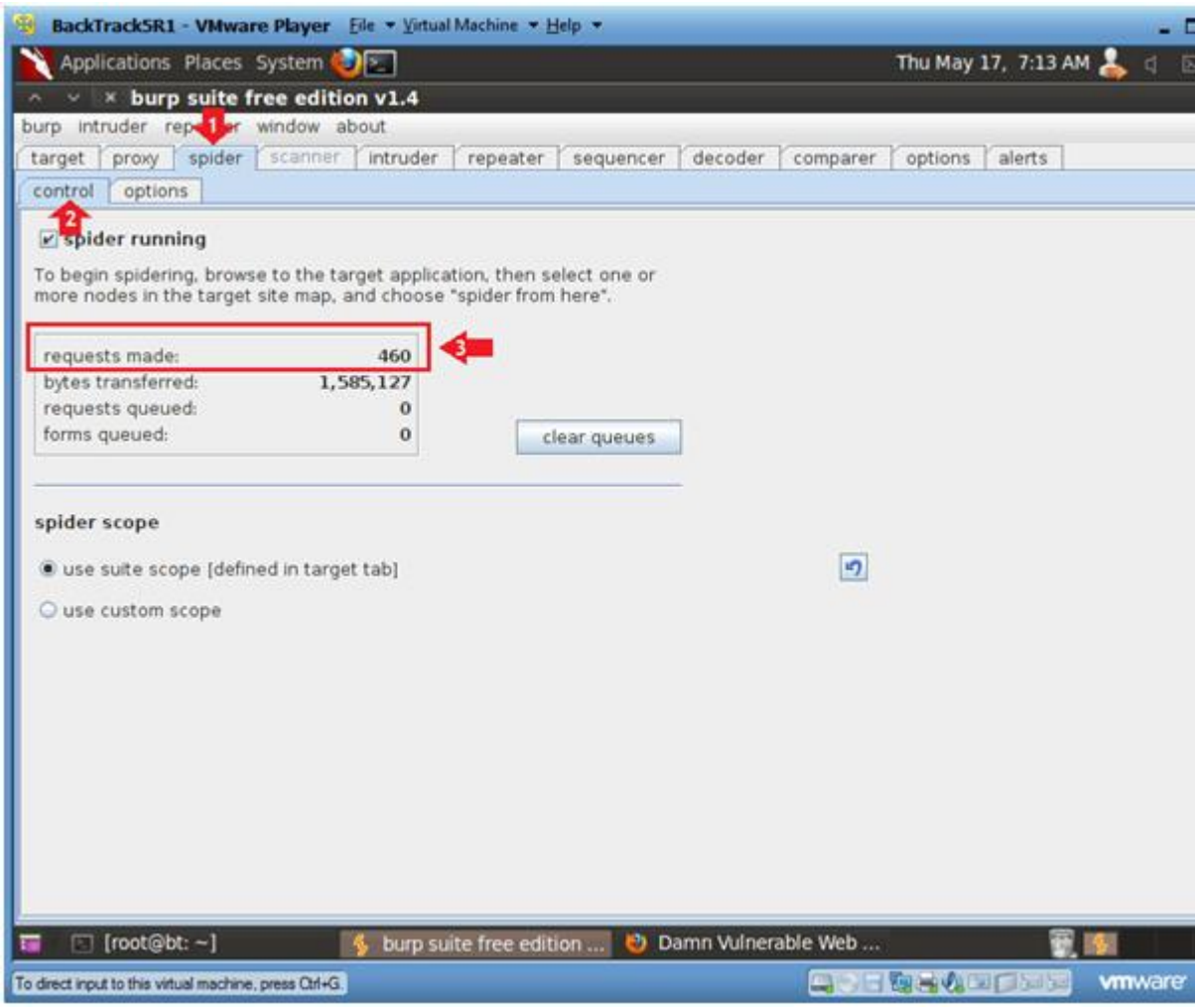
4. Spider Host
    - **Instructions:**
        0. Click on the target tab
        1. Click on the site map tab
        2. Click on the DVWA IP Address, then Right Click to display utility menu.
        3. Click on spider this host.
        4. Continue to Next Step

- 

5. Spider Directory True Results
    - **Notes:**
        0. Notice that you now have a pretty accurate map of the DVWA
        1. Continue to next step.

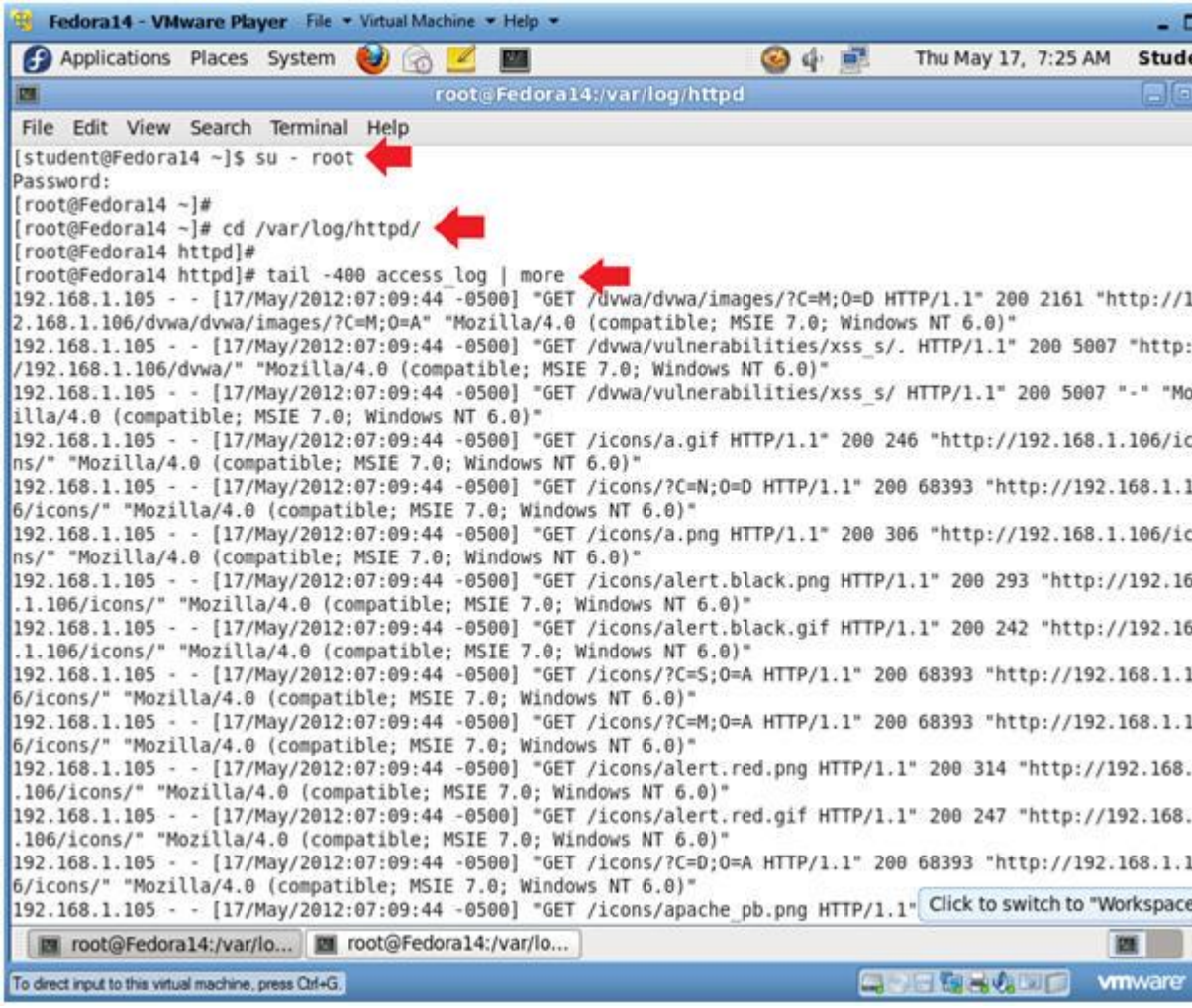
- 

6. Spider Directory True Results
    - **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

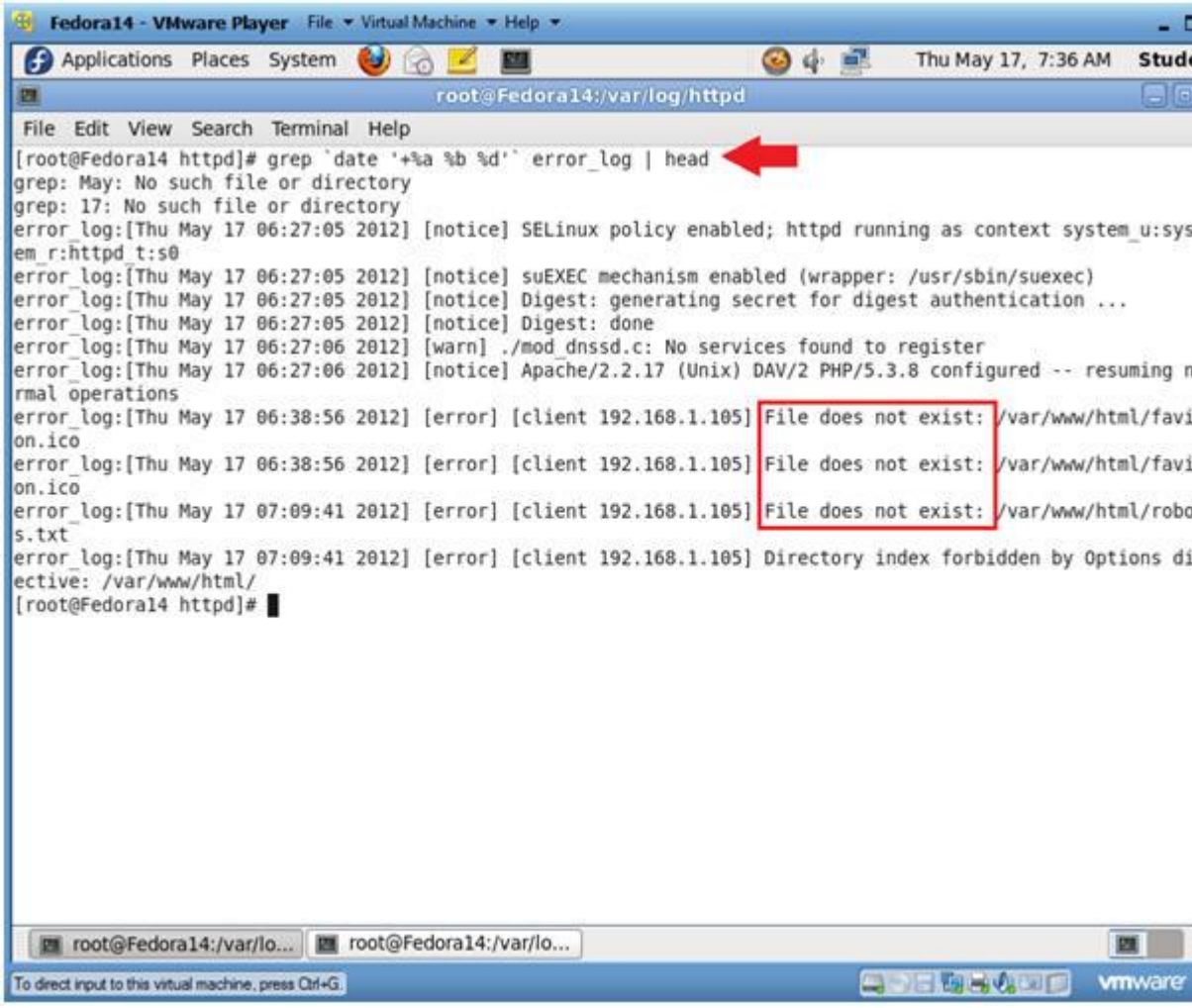
- 

Section 10: View Scan Results on Fedora DVWA web server

1. Viewing Apache's Access Log
    - **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 ap 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.

- 

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 patte
            - **`date '+%a %b %d'`**, display today's date where %a is abbreviated weekday name, %b is the abbreviated month %d is the abbreviated month name.
            - error_log, is apache's error_log. Events go in this (1) people/spiders are searching for something that m exists or (2) people/spiders are sending passive/mali instructions to a form.
            - head, show me the first 10 lines.
        3. Notice how the burpsuite spider is searching for fires tha exist.

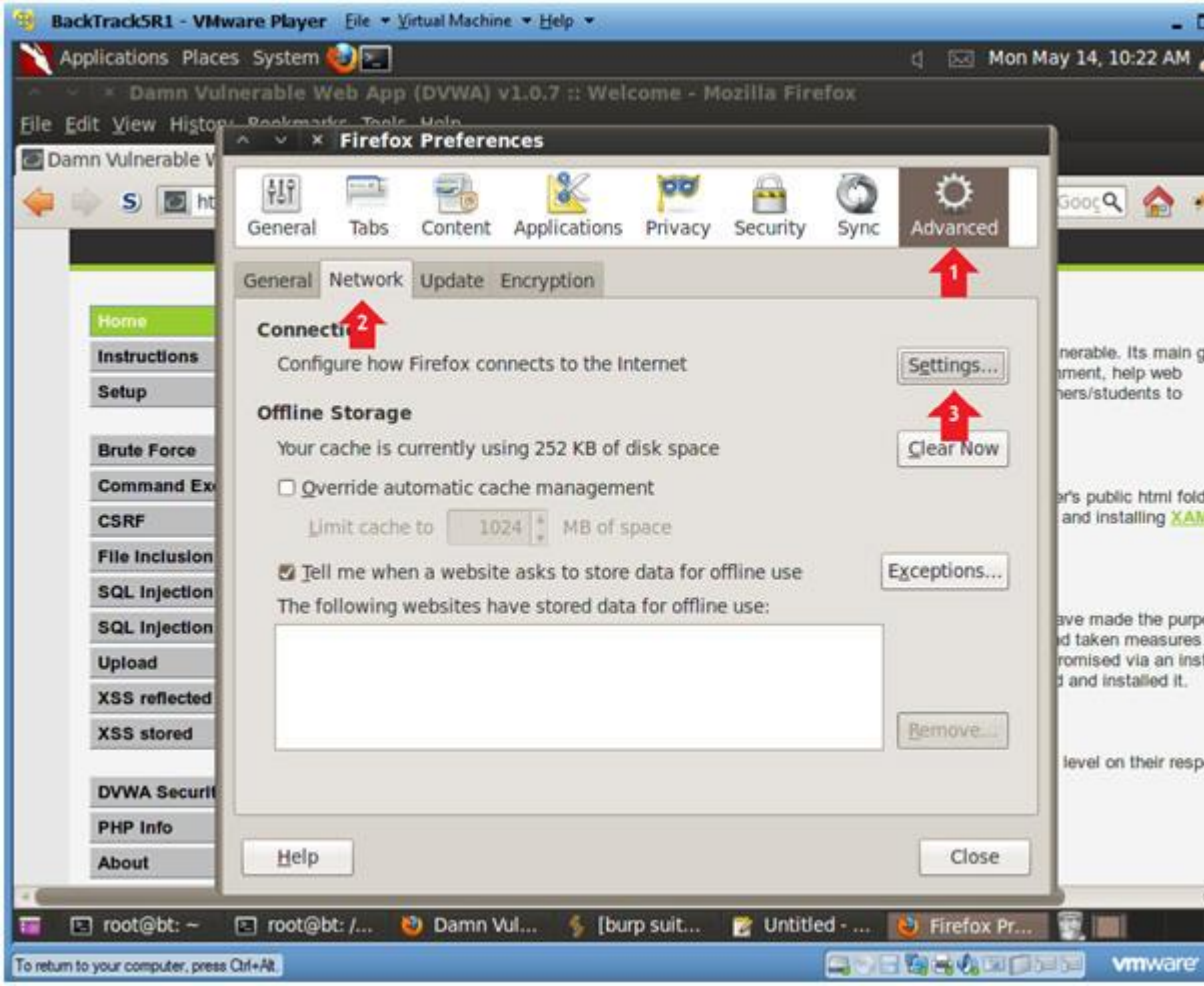
- 

Section 11: Clean Up Notes

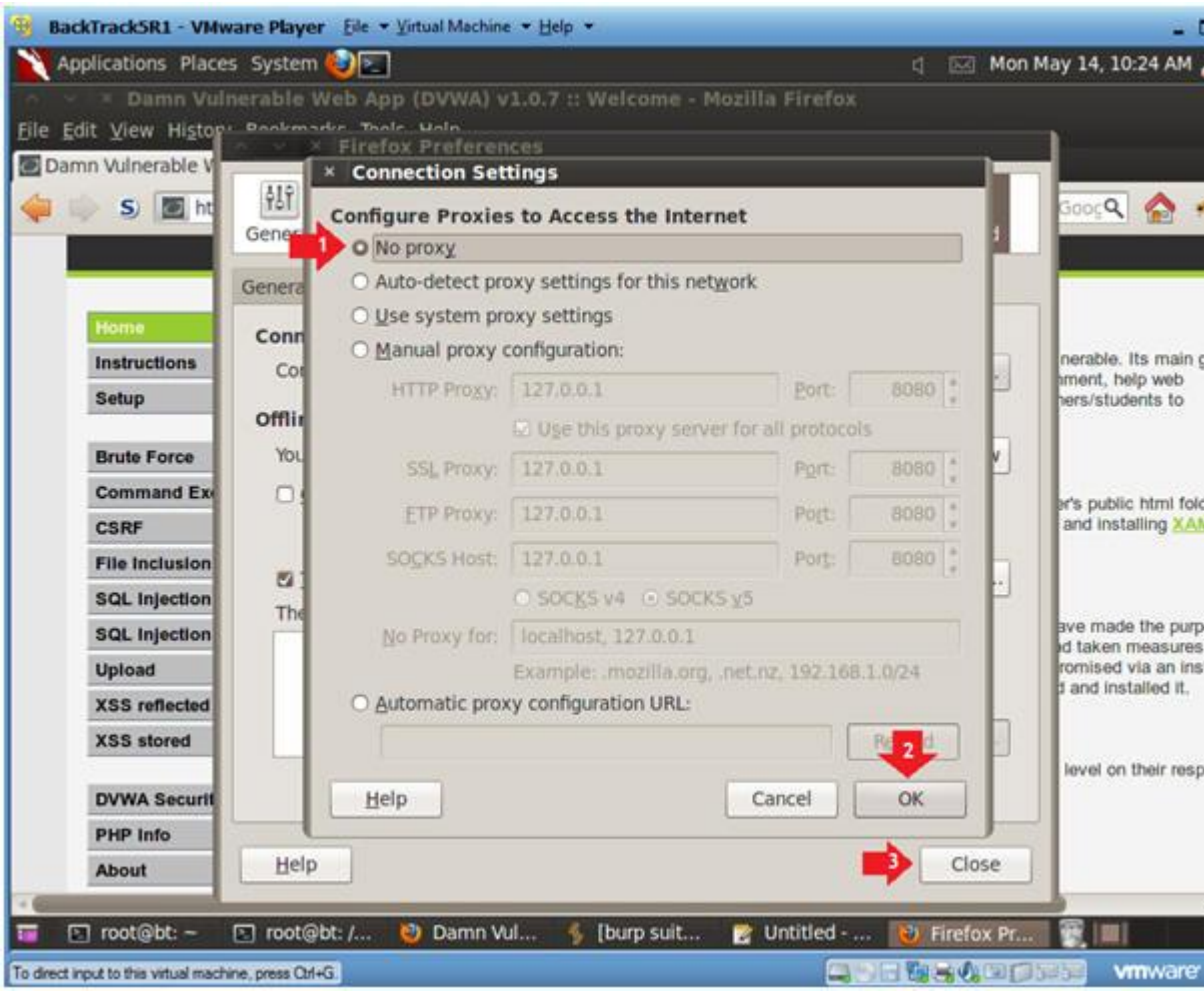
1. On BackTrack's Firefox
    - **Instructions:**
        1. Edit --> Preferences

- 

2. Edit Network Settings
    - **Instructions:**
        1. Click on Advanced
        2. Click on Network Tab.
        3. Click on Settings Button.

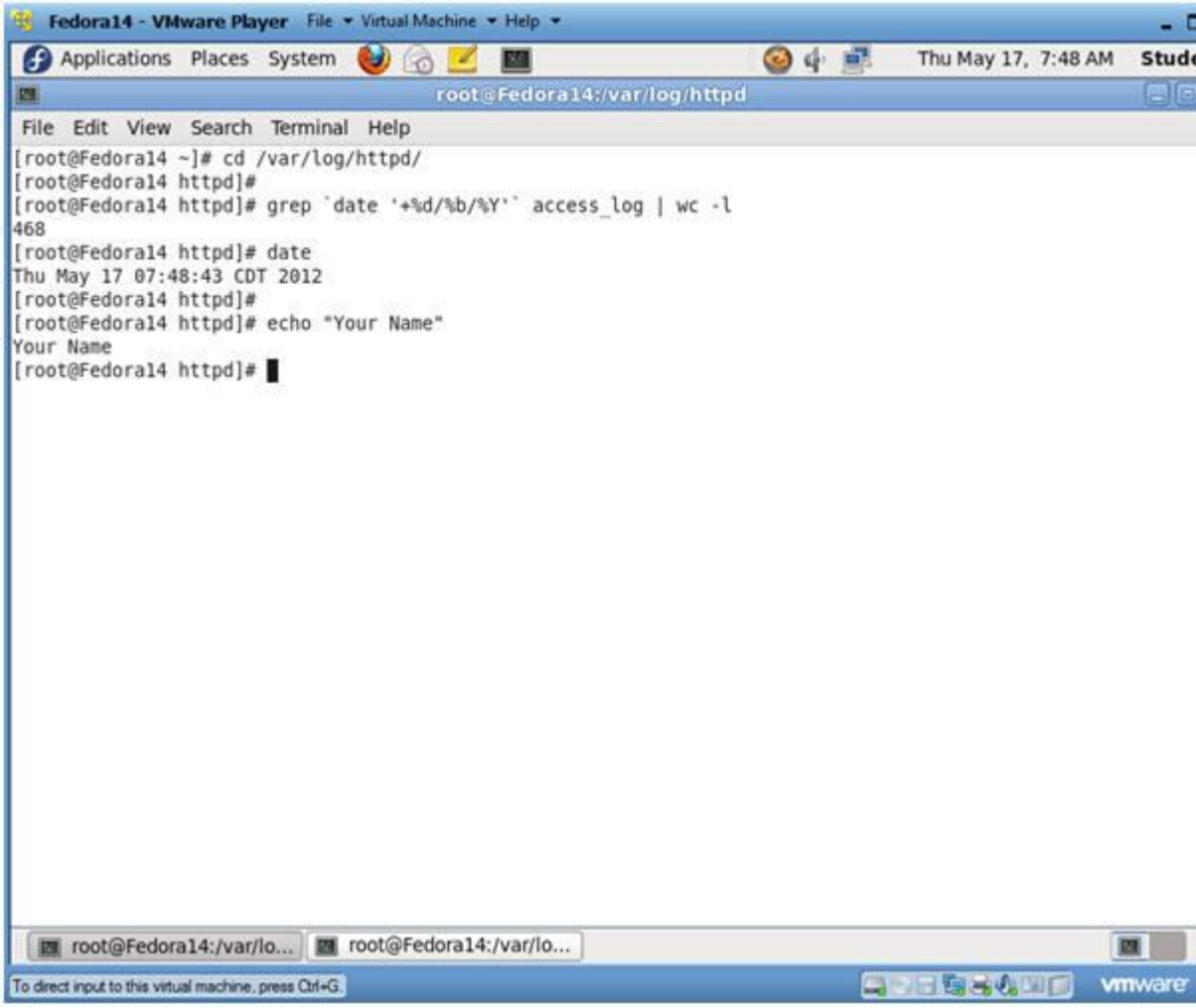
- 

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
   - **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 man lines grep found for today's dat 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