

(Damn Vulnerable Web App (DVWA))

{ Burp Suite, Man-in-the-middle-attack }

Section 0. Background Information

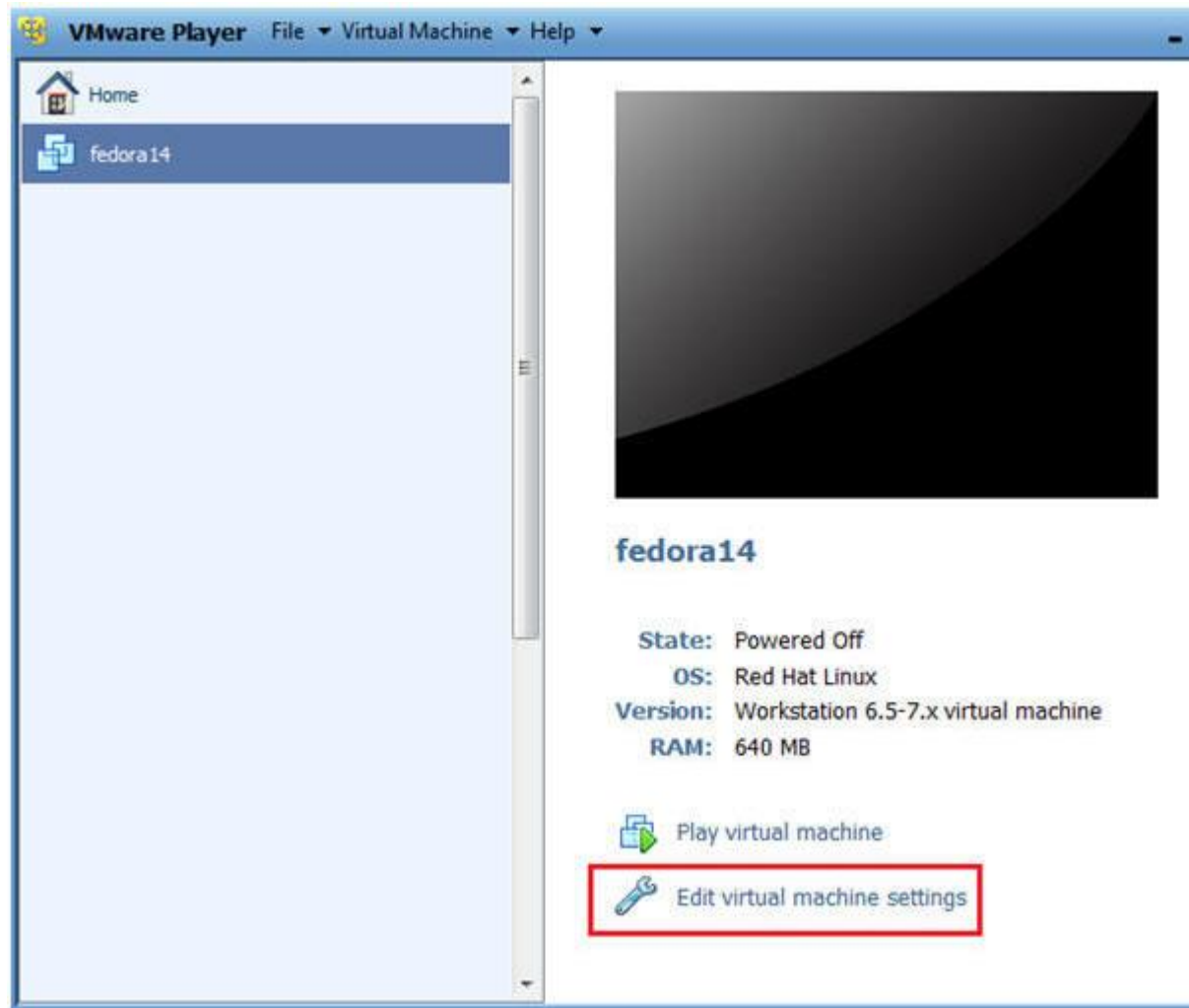
- What is Damn Vulnerable Web App (DVWA)?
 - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is intentionally damn vulnerable.
 - Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a controlled environment.
- What is Burp Suite?
 - 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.
- Pre-Requisite Labs
 - [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
 - [BackTrack: Lesson 1: Installing BackTrack 5 R1](#)
- **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 Firefox
 3. We will use Burp Suite to capture a PHPSESSID cookie.
 4. We will create a curl statement to test a man-in-the-middle attack
 5. We will use Firefox Cookies Manager+ to set up a man-in-the-middle attack
- 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 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 "no 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** illegal activities.

behavior of any kind.

- You are on notice, that continuing and/or using this lab outside of 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

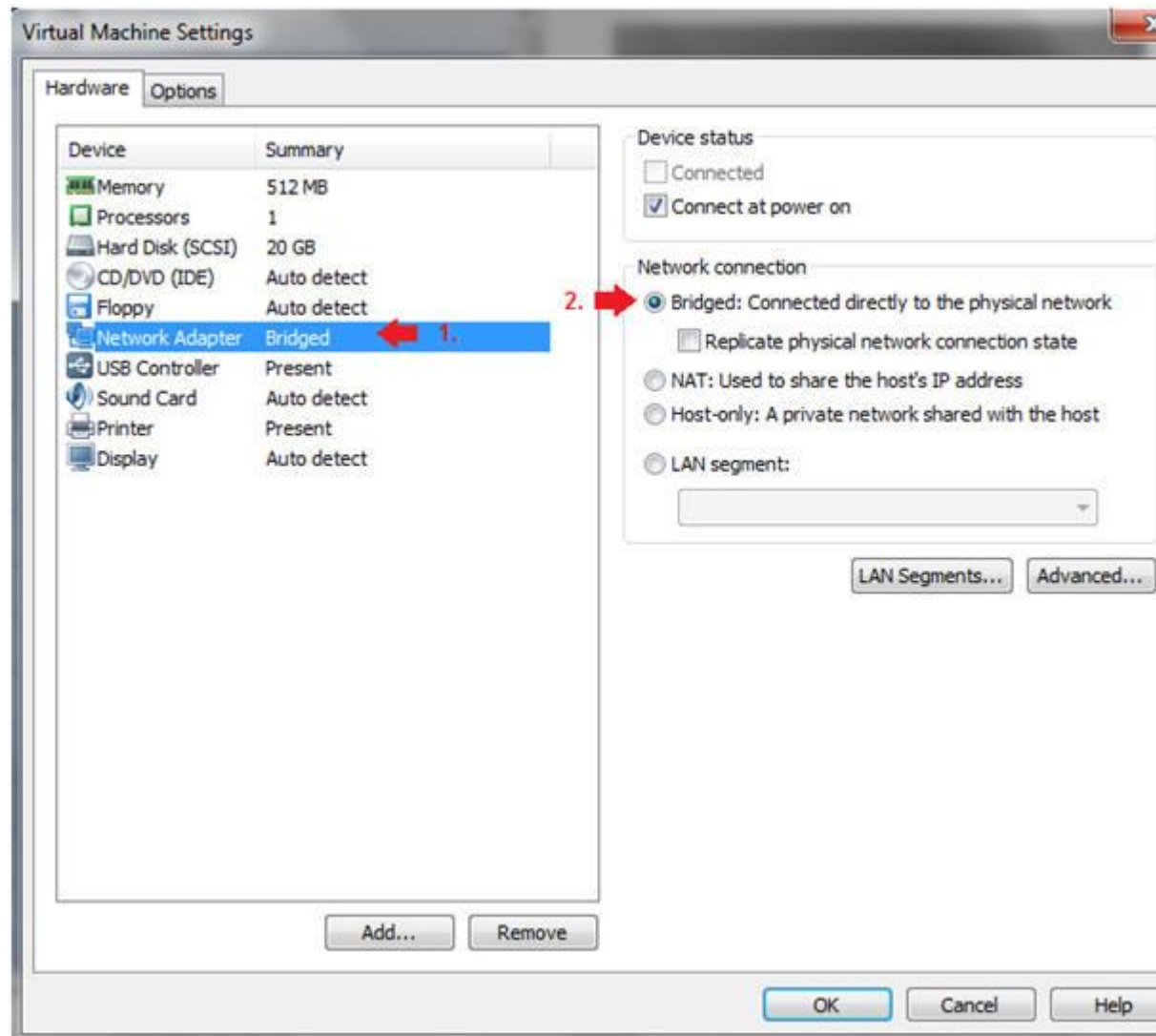
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings



3. Edit Network Adapter

- **Instructions:**

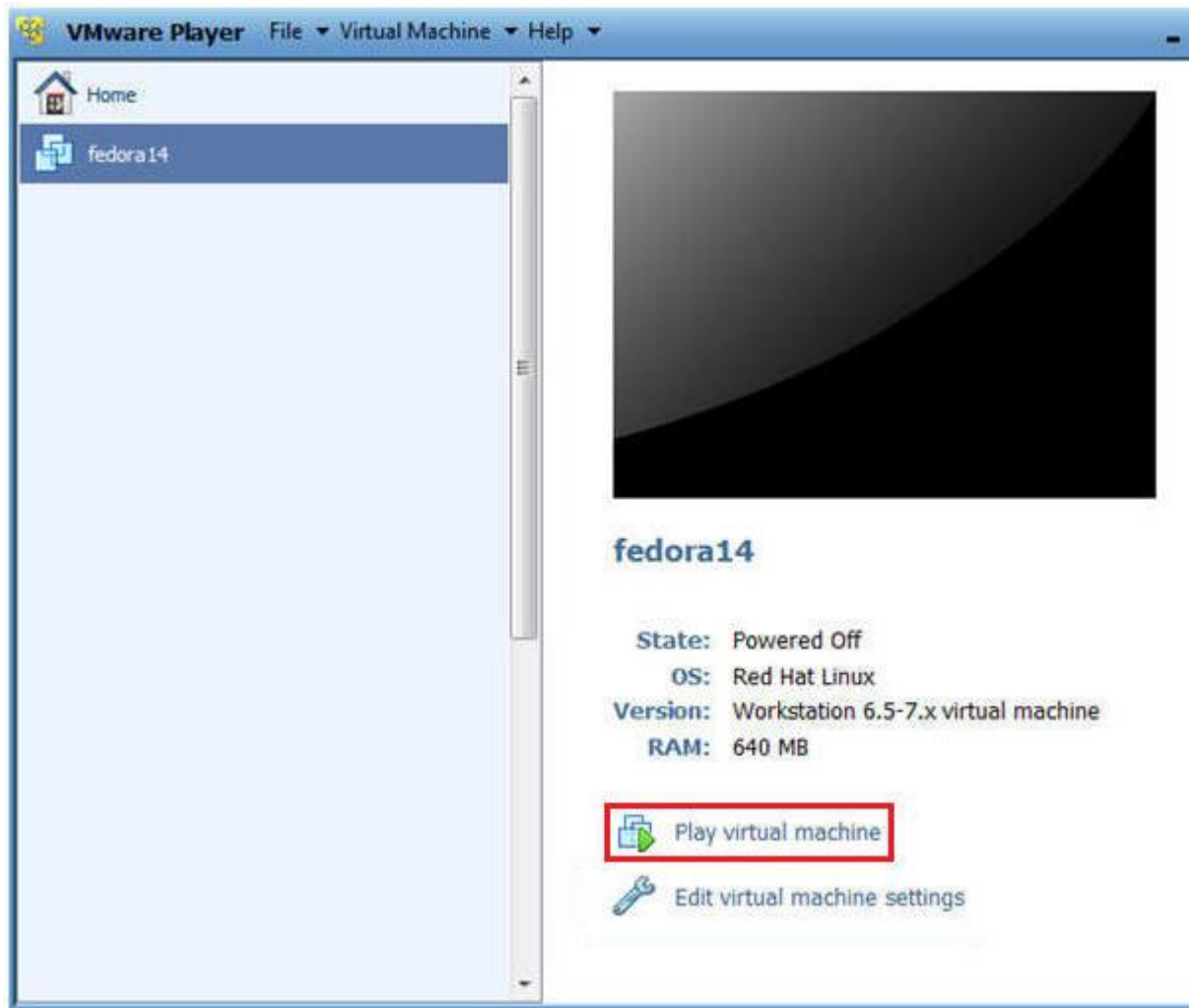
1. Highlight Network Adapter
2. Select Bridged
3. Click on the OK Button.



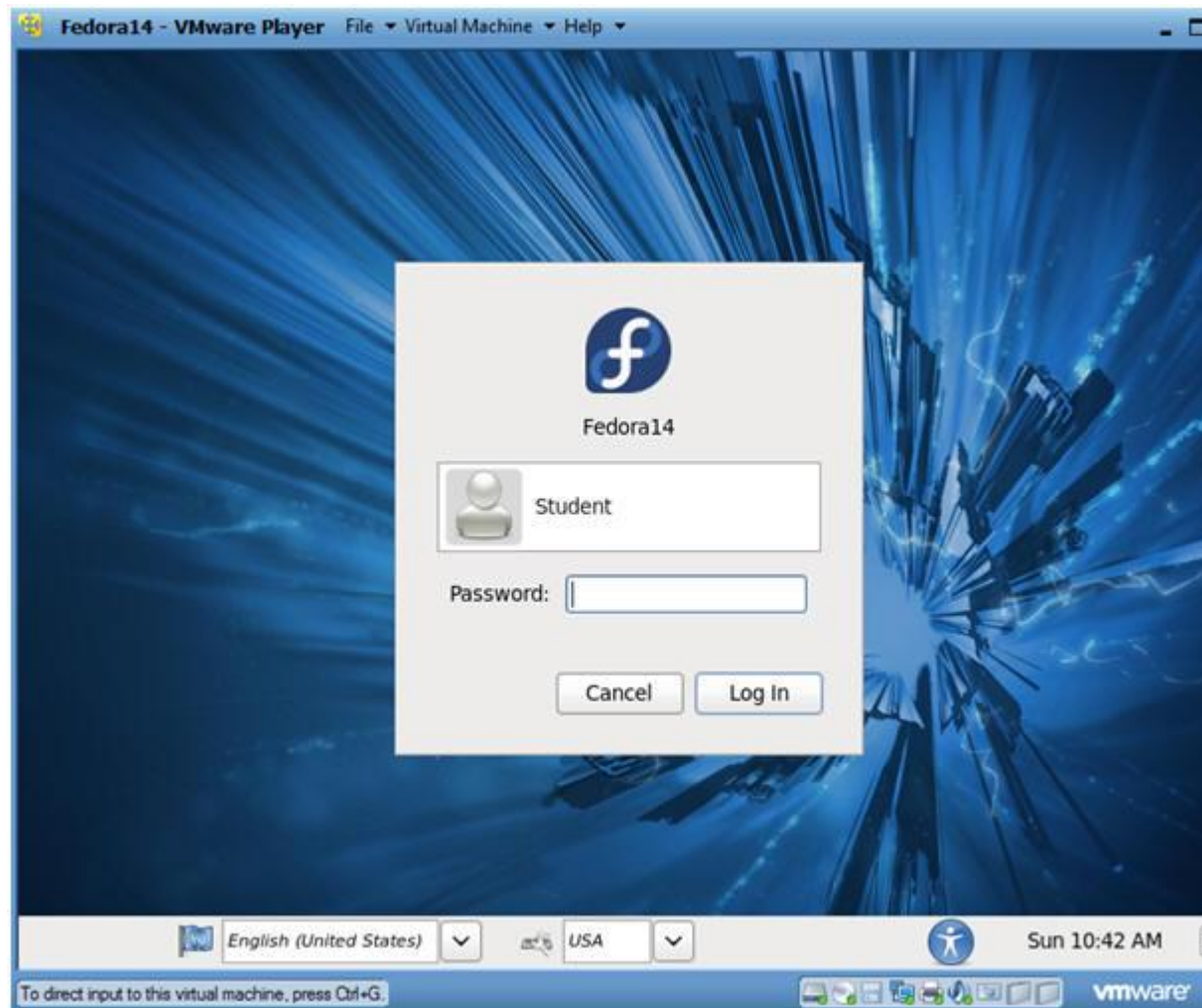
○

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



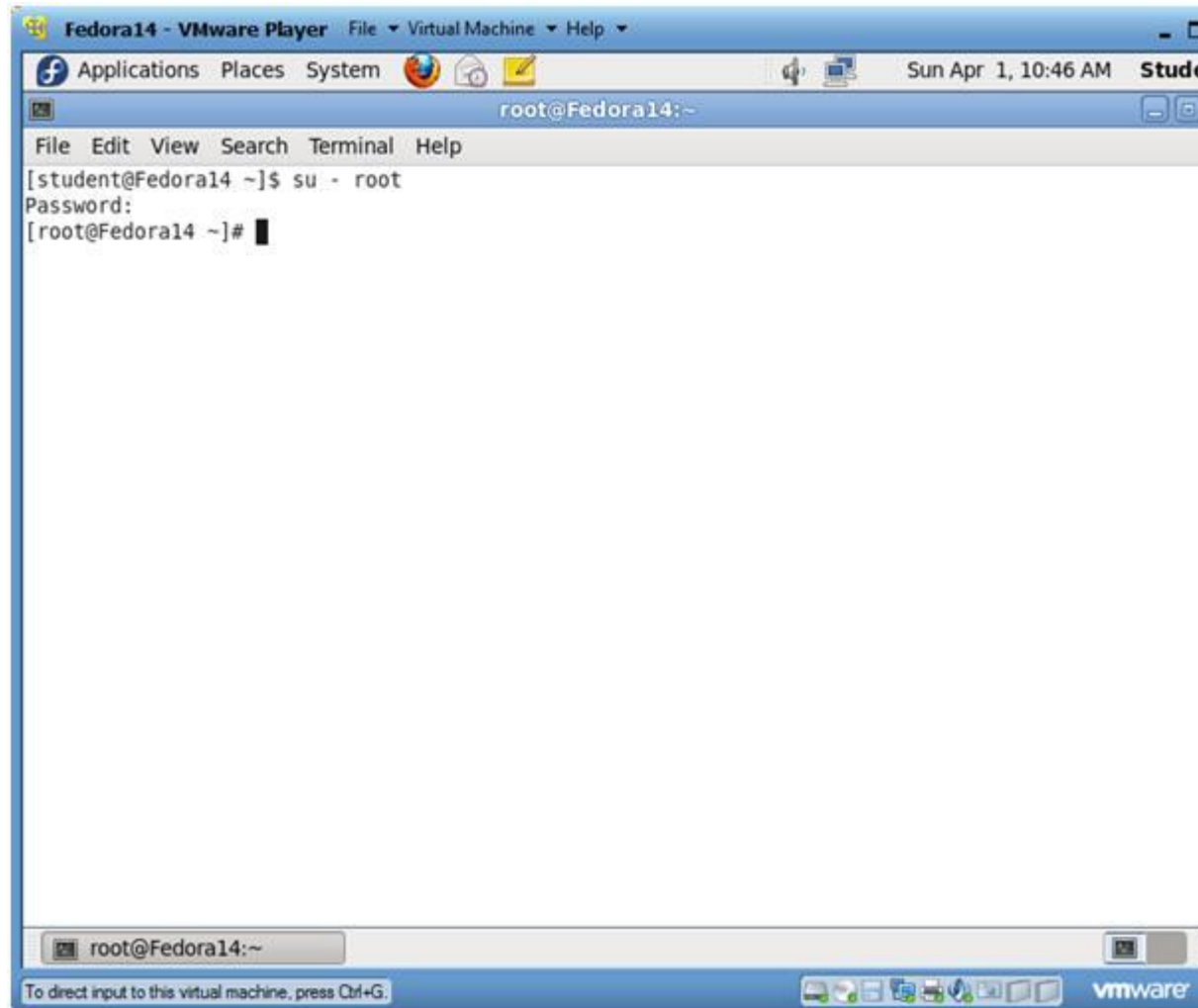
○

2. Switch user to root

○ **Instructions:**

1. `su - root`

2. <Whatever you set the root password to>

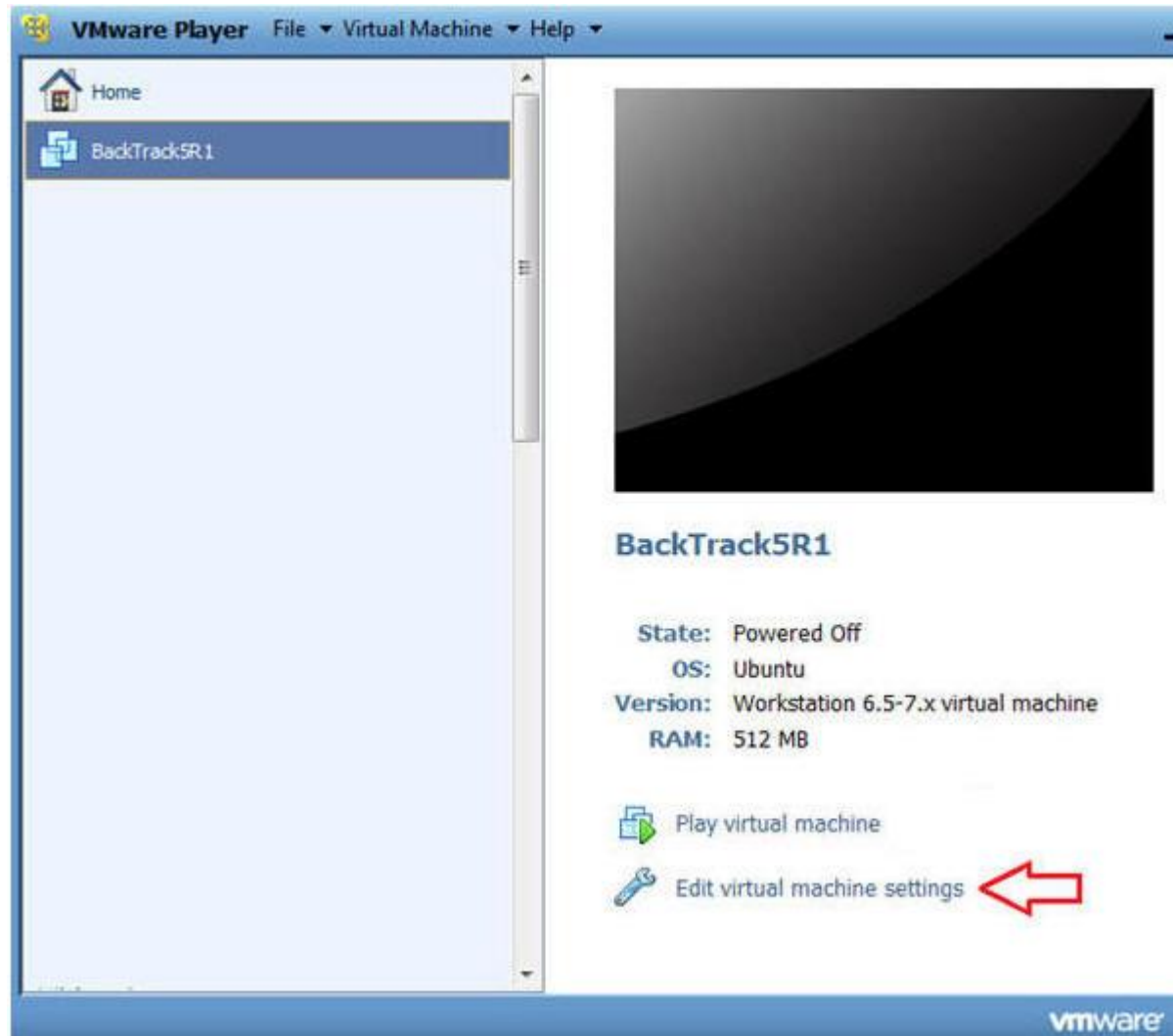


3. Get IP Address

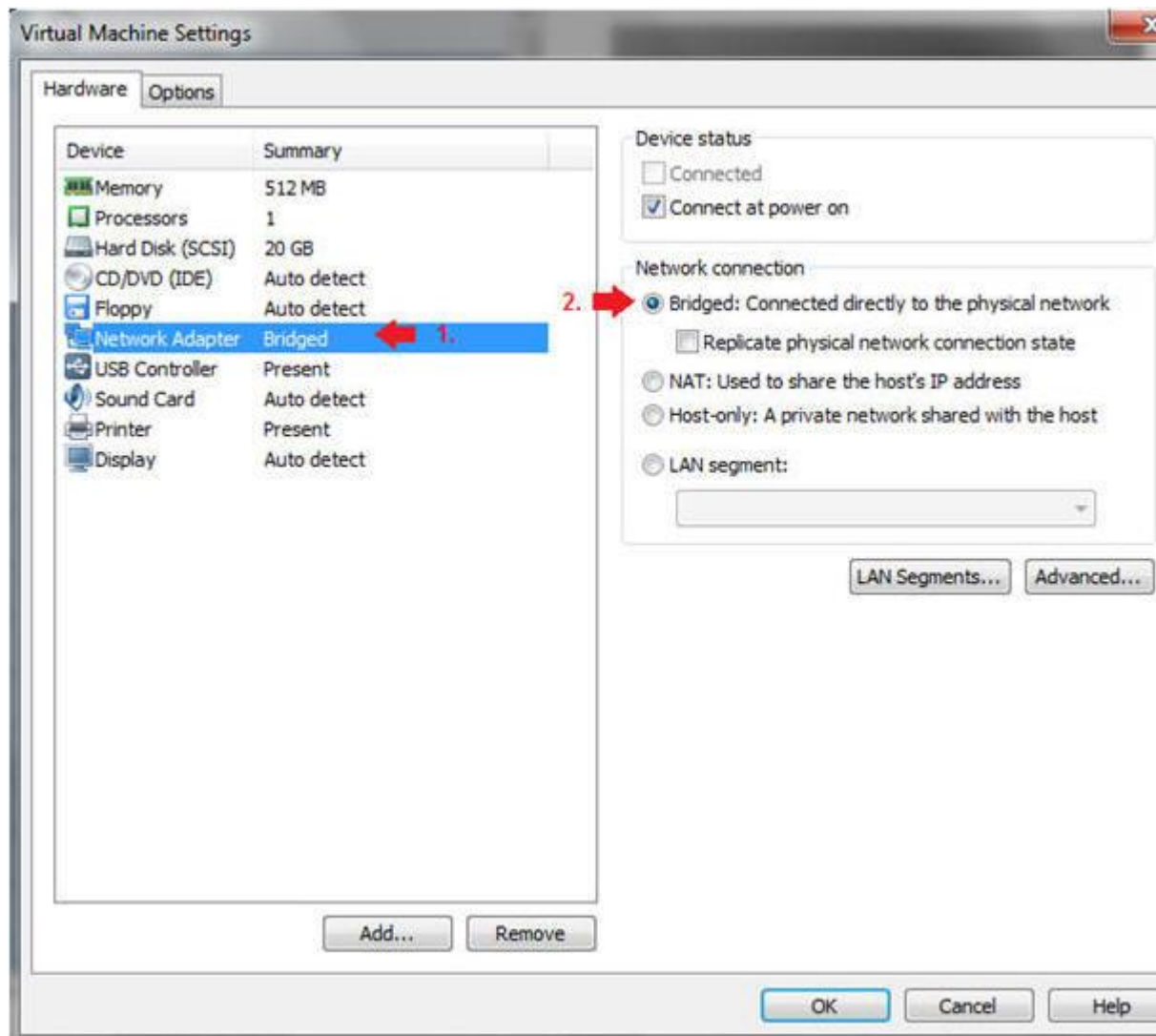
- **Instructions:**
 1. `ifconfig -a`
- **Notes:**
 - As indicated below, my IP address is 192.168.1.106.
 - Please record your IP address.

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

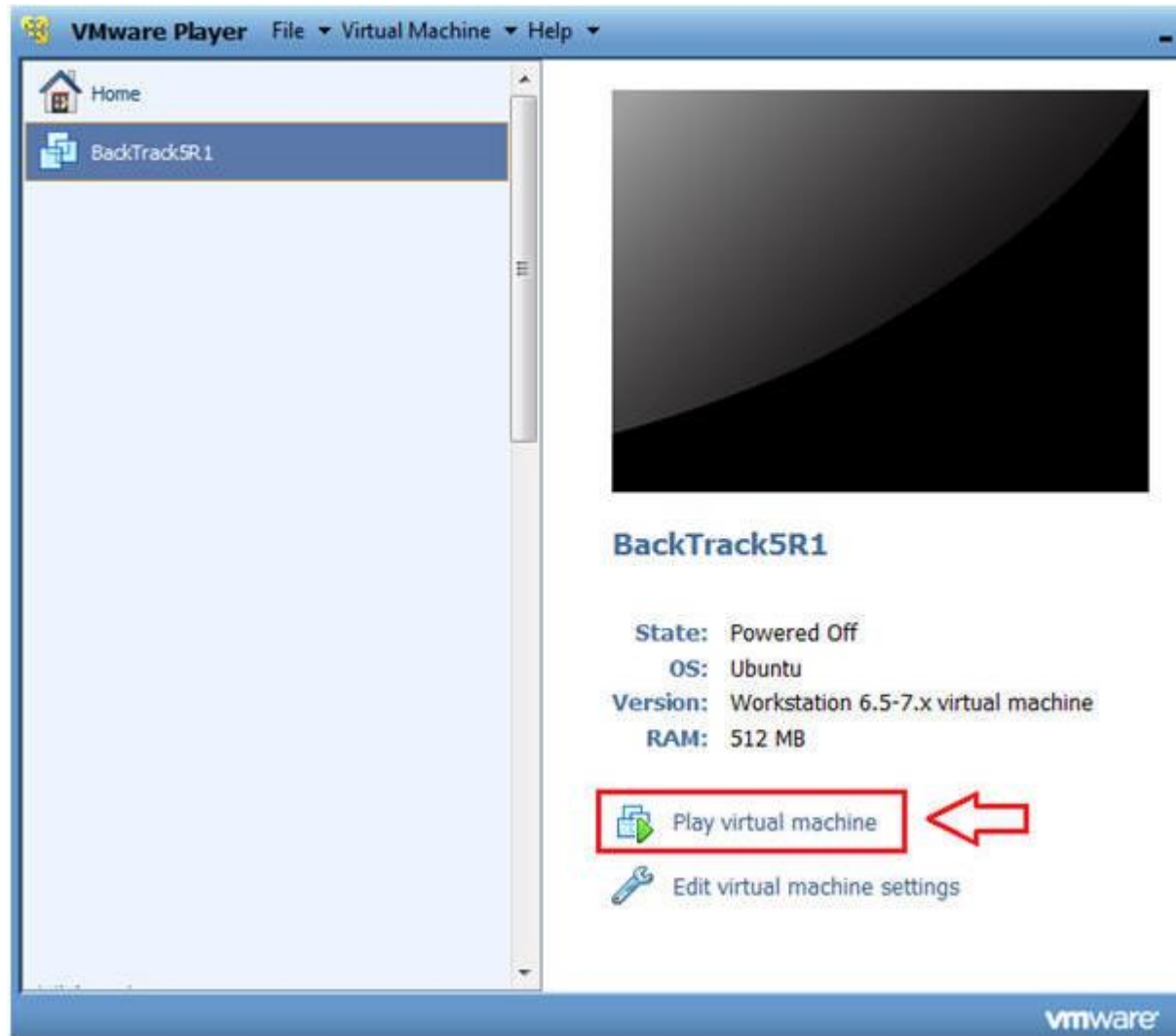


- 3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Do not Click on the OK Button.



Section 5: Login to BackTrack

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



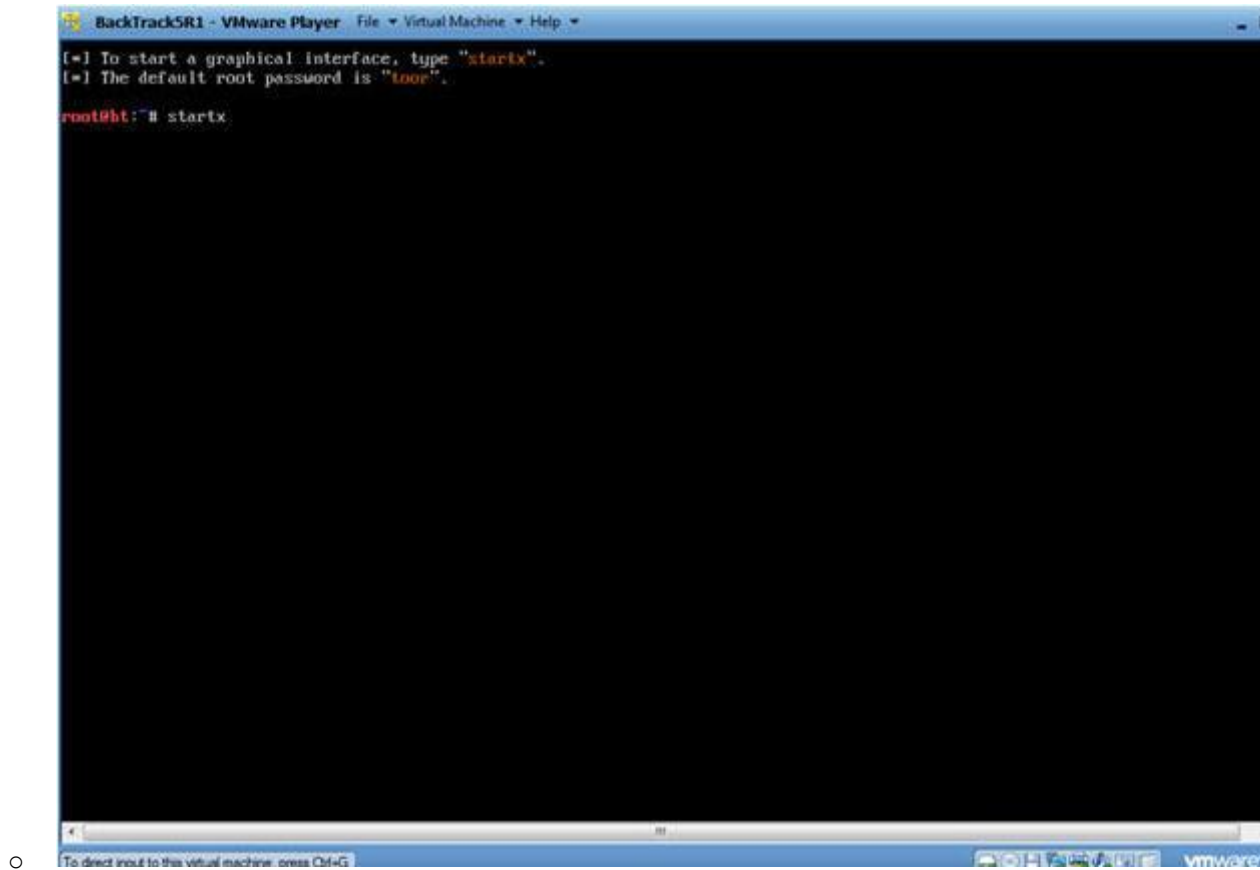
2. Login to BackTrack

- **Instructions:**

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



-



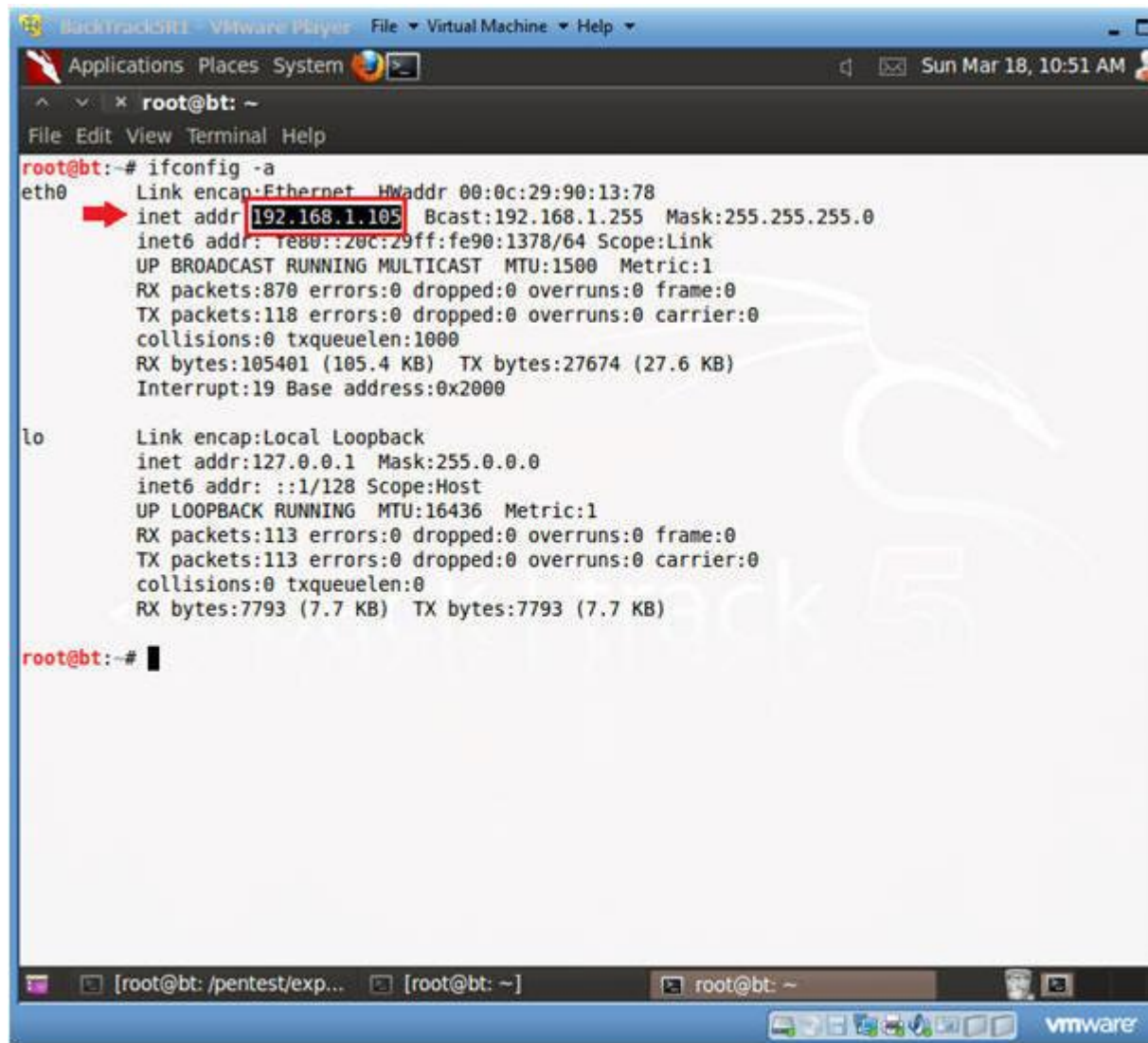
Section 6: Open Console Terminal and Retrieve IP Address

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.



```
Backtrack5 VMware Player File Virtual Machine Help
Applications Places System
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:90:13:78
          inet addr:192.168.1.105  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe90:1378/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105401 (105.4 KB)  TX bytes:27674 (27.6 KB)
          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:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7793 (7.7 KB)  TX bytes:7793 (7.7 KB)

root@bt:~#
```

○

Section 7: Configure Firefox Proxy Settings

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



2. Preferences

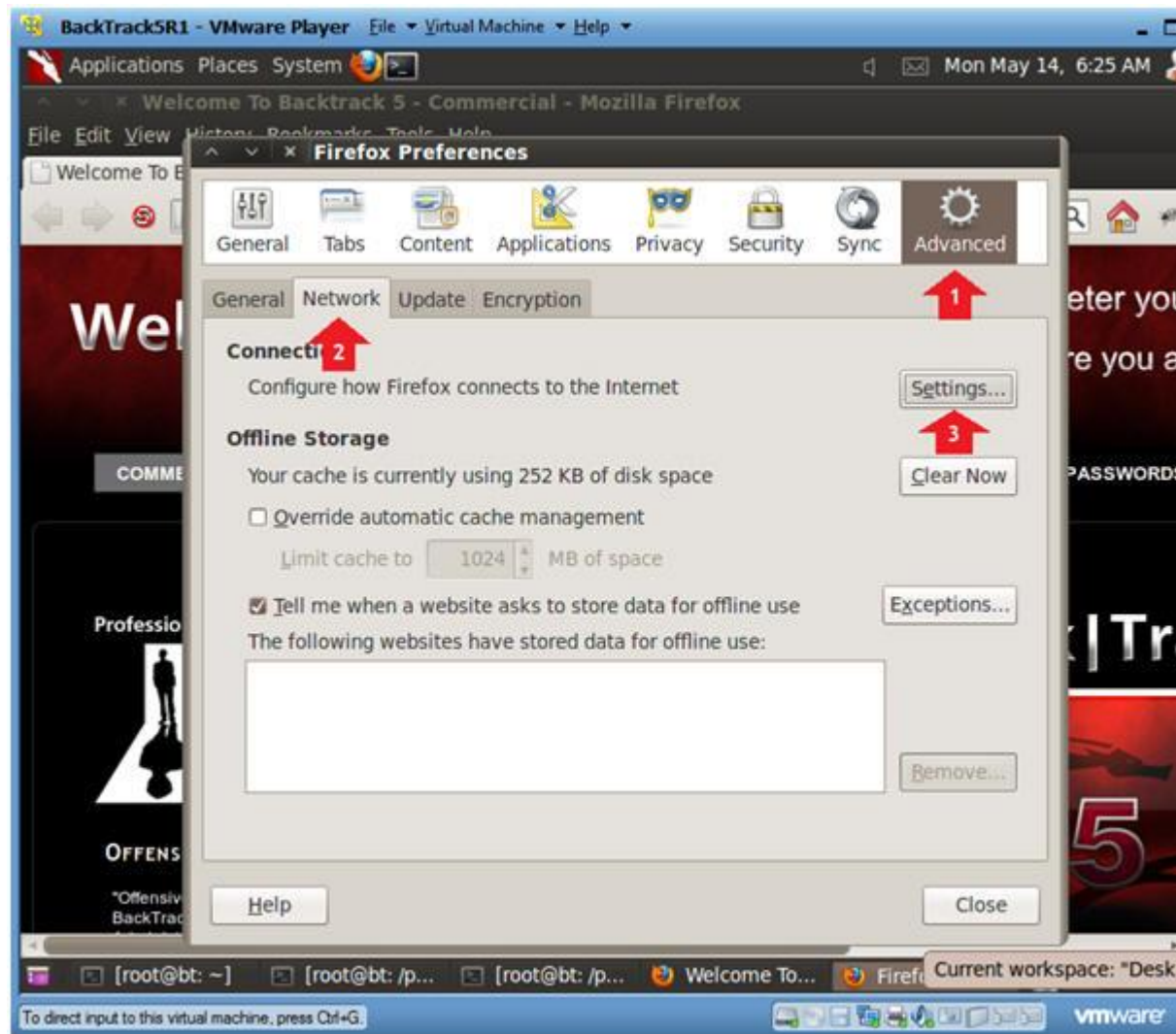
- o **Instructions:**
 1. Edit --> Preferences



3. Preferences

- **Instructions:**

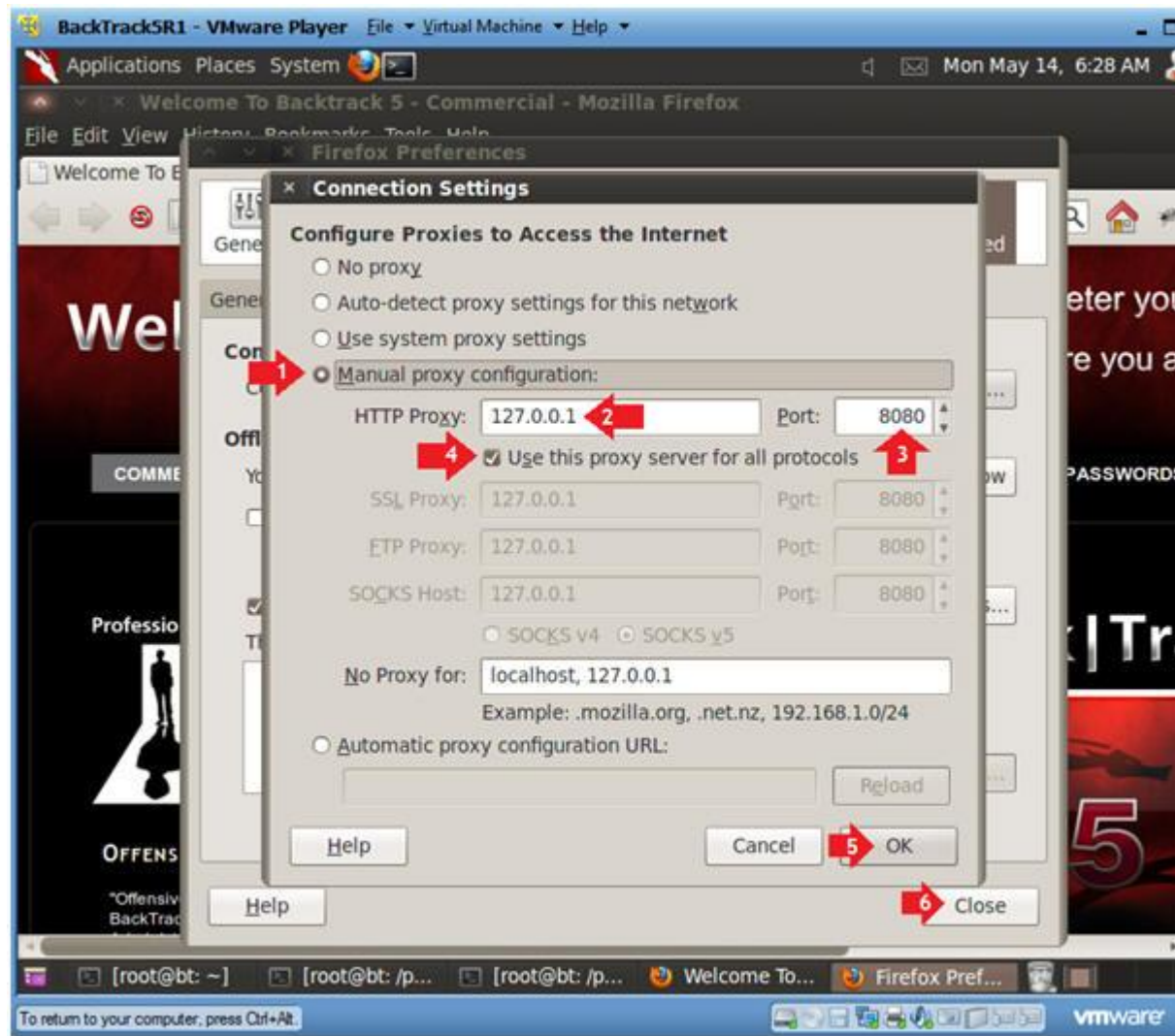
1. Click on Advanced
2. Click on the Network Tab
3. Click on the Settings Button



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:**

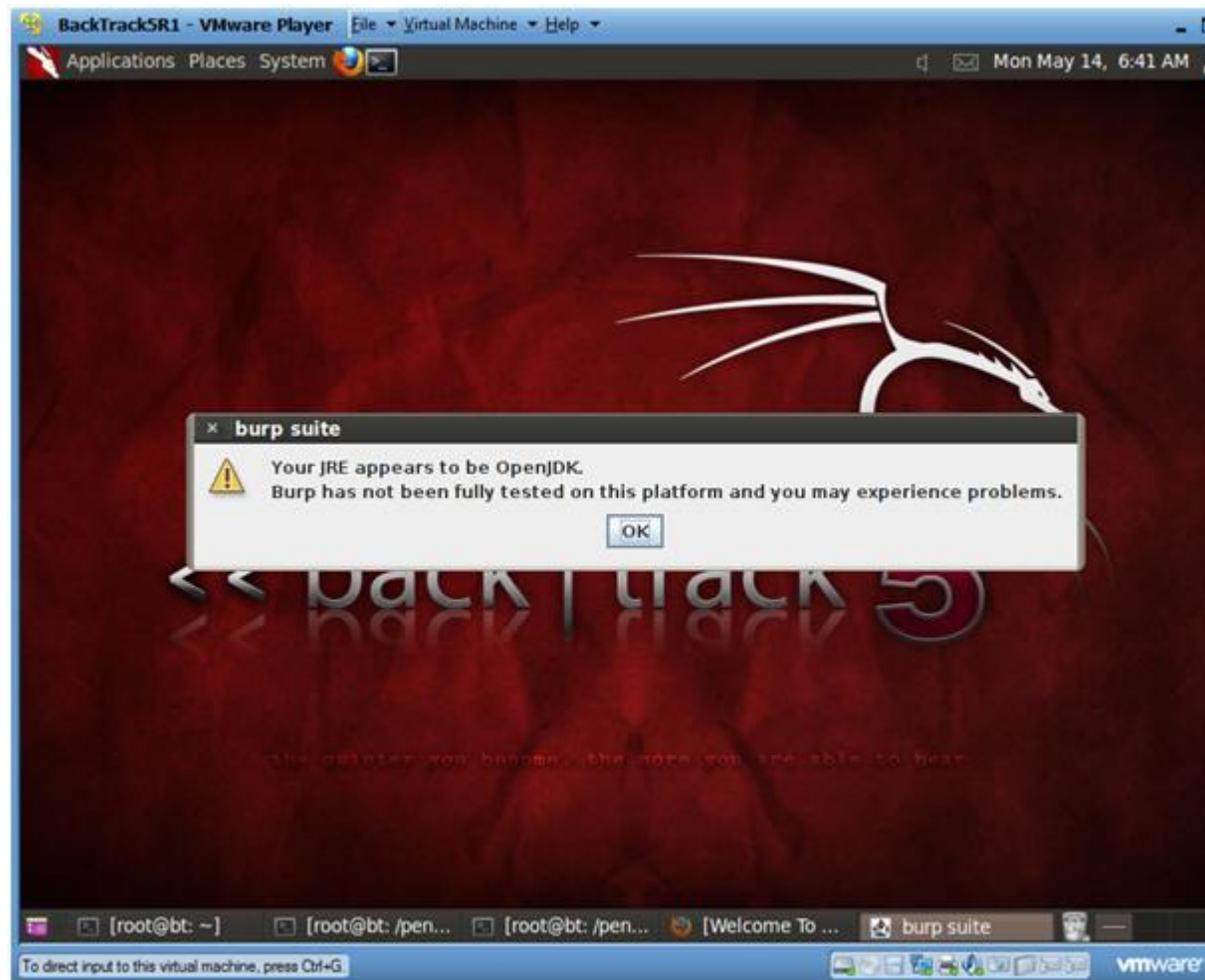
1. Applications --> BackTrack --> Vulnerability Assessment --> Application Assessment ---> Web Vulnerability Scanner -->



○

2. JRE Message

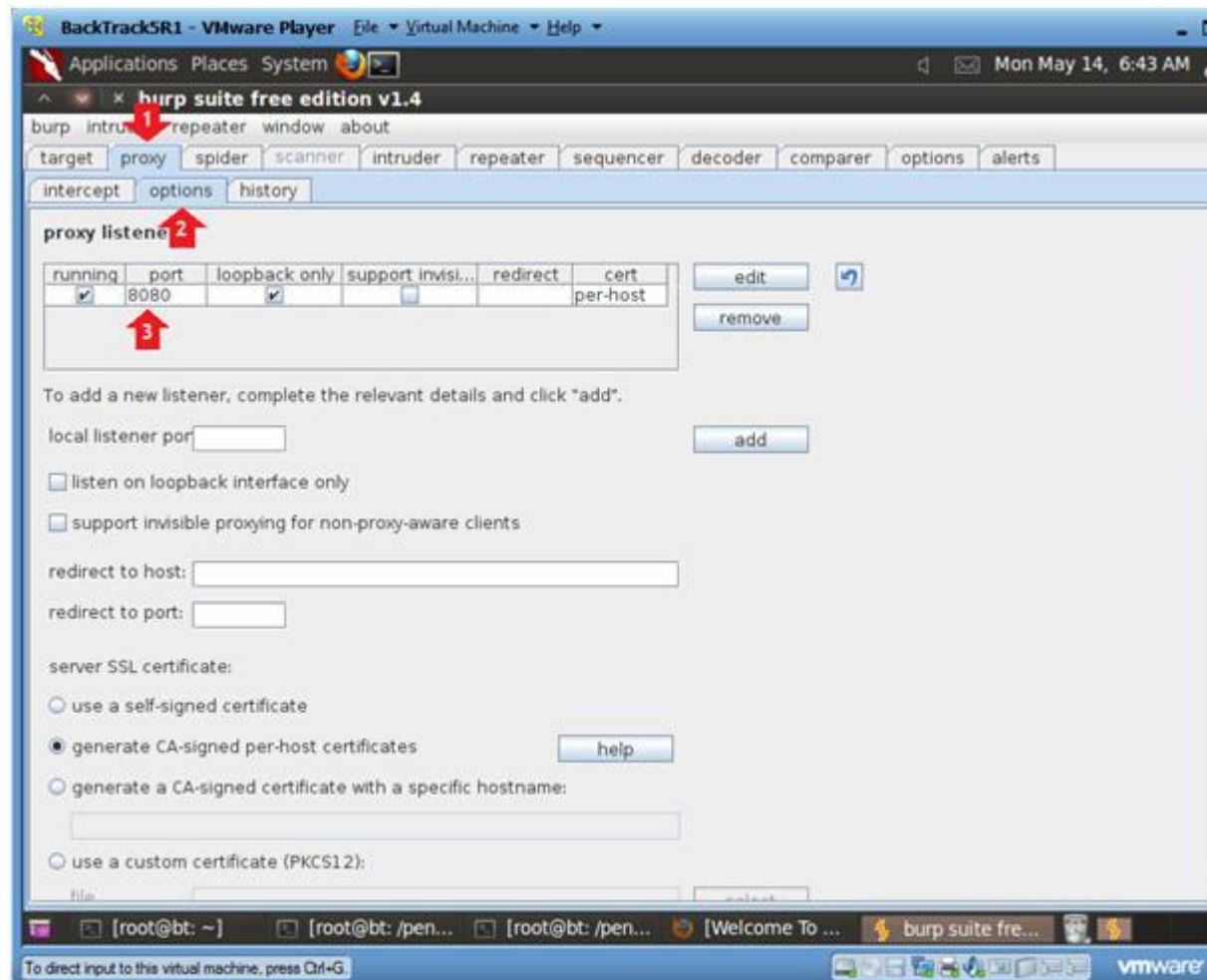
- **Instructions:**
 1. Click OK



3. Configure proxy

- **Instructions:**

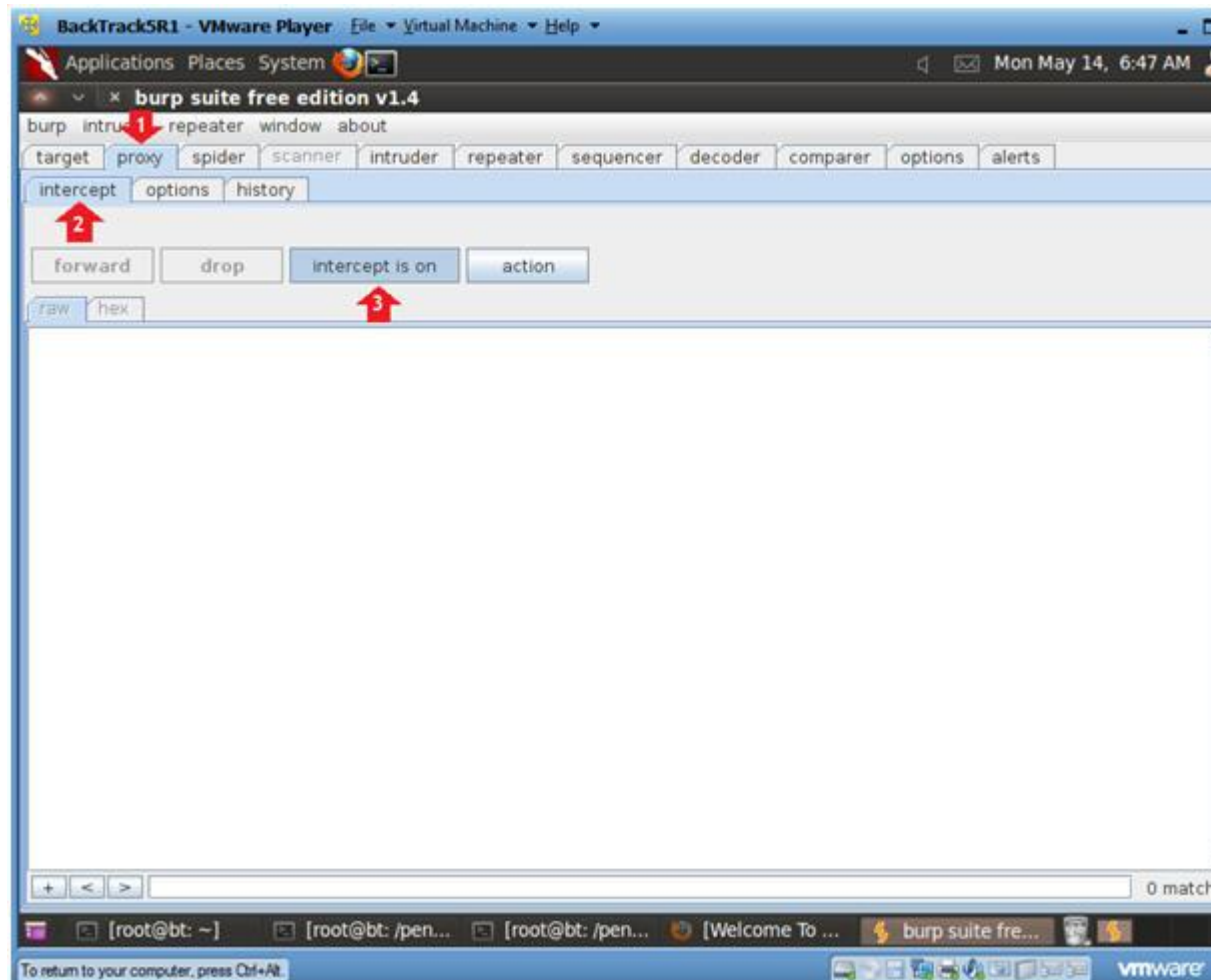
1. Click on the proxy tab
2. Click on the options tab
3. Verify the port is set to 8080



4. Turn on intercept

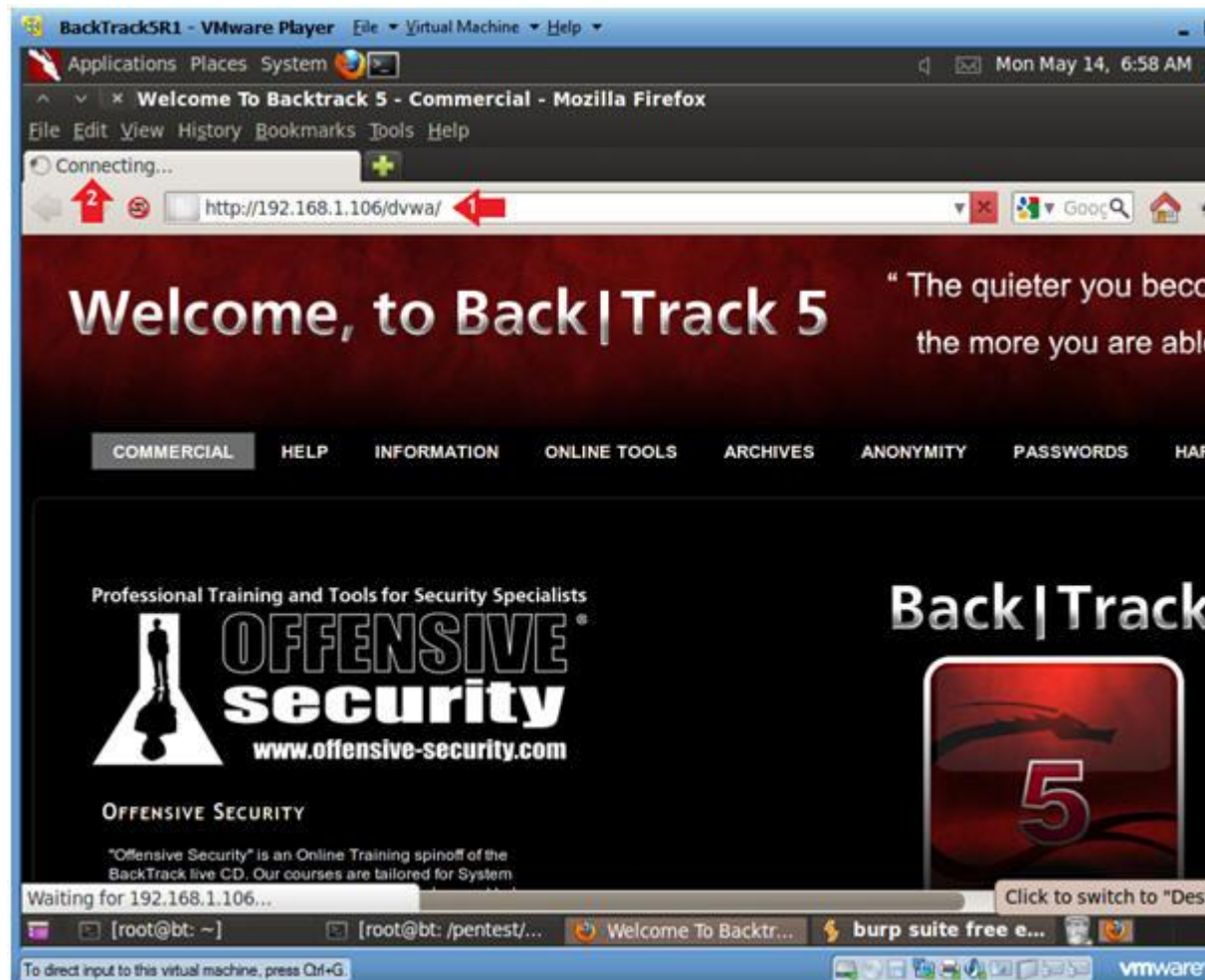
o **Instructions:**

1. Click on the proxy tab
2. Click on the intercept tab
3. Verify the intercept button shows "intercept is on"



Section 9: Intercept with Burp Suite

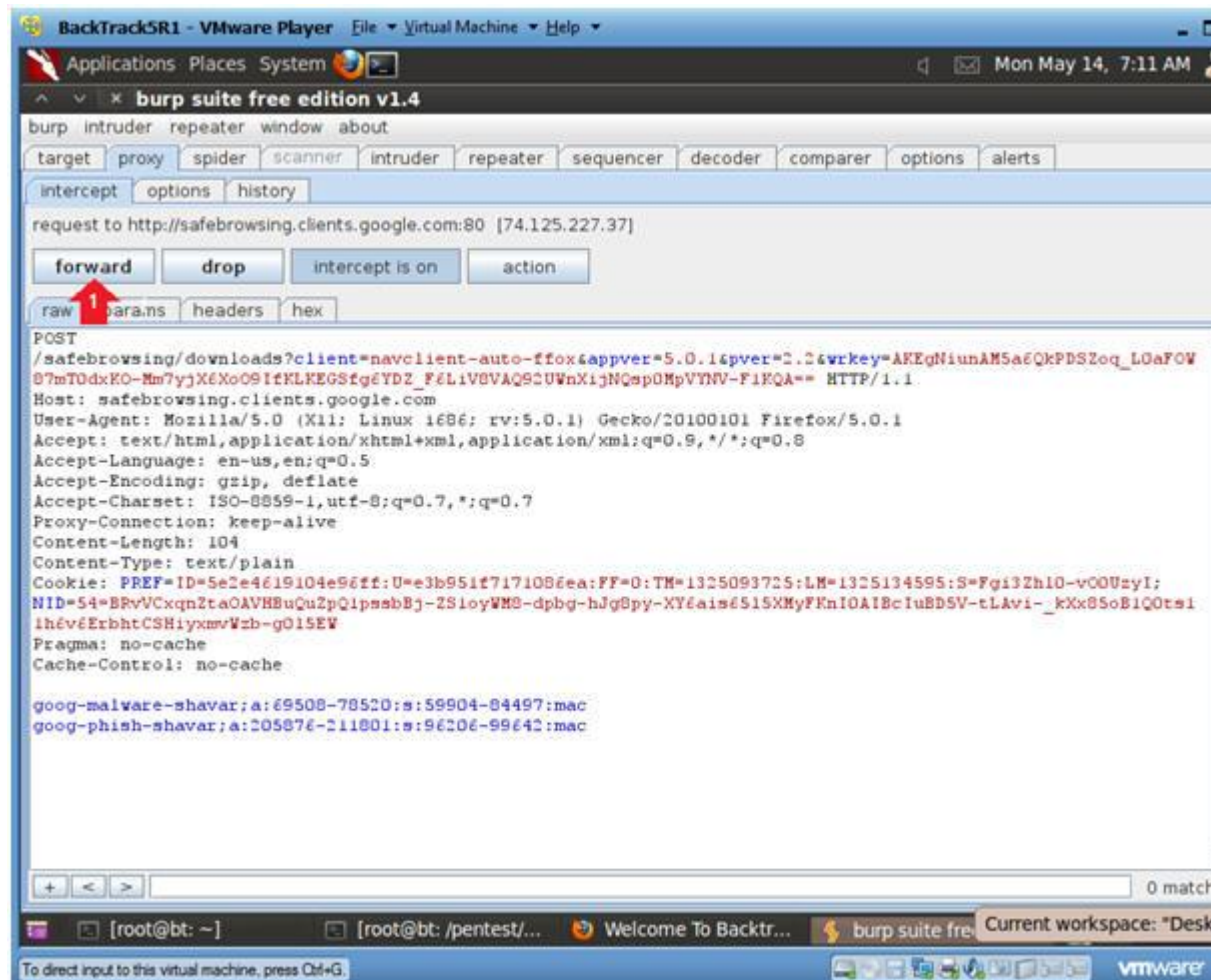
1. Browse to DVWA's homepage
 - o **Instructions:**
 1. `http://IPADDRESS/dvwa/`
 - Replace IPADDRESS with the Fedora's IP Address obtained (Section 3, Step 3).
 2. Notice that the DVWA homepage will not be displayed, but it will get a Connecting message.
 3. Continue to Next Step.



2. Forward Request

- **Instructions:**

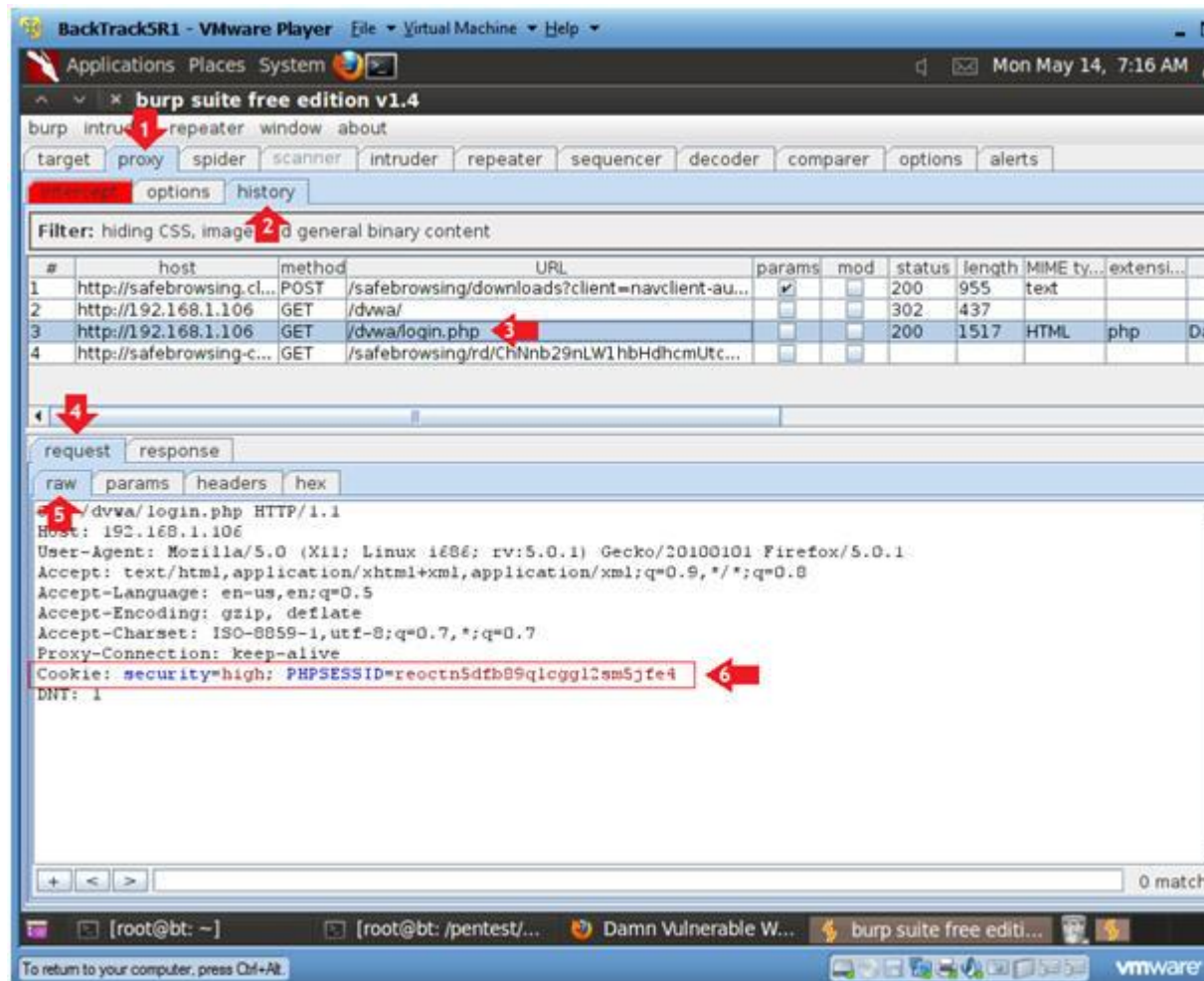
1. Click on the Forward Button 3 times.



3. View History

Instructions:

1. Click on the proxy tab
2. Click on the history tab
3. Click on /dvwa/login.php
4. Click on the request tab
5. Click on the raw tab
6. Notice that a PHP cookie session is now established, even logging to the application.



4. Login to DVWA

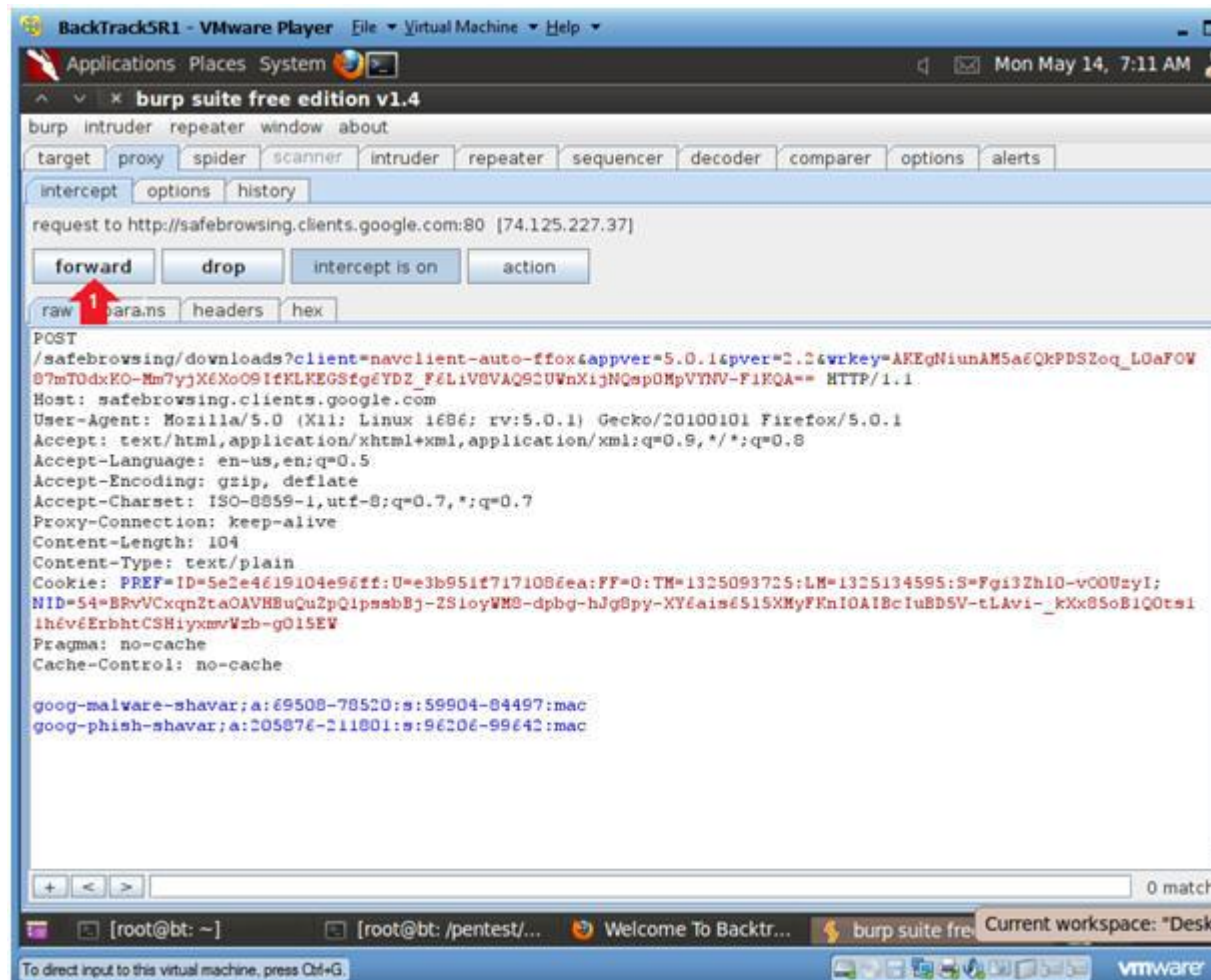
- **Instructions:**

1. Username: admin
2. Password: password
3. Click Login
4. Notice that the DVWA Navigation Menu will not be displayed instead you will get a Connecting message.
5. Continue to Next Step



5. Forward Request

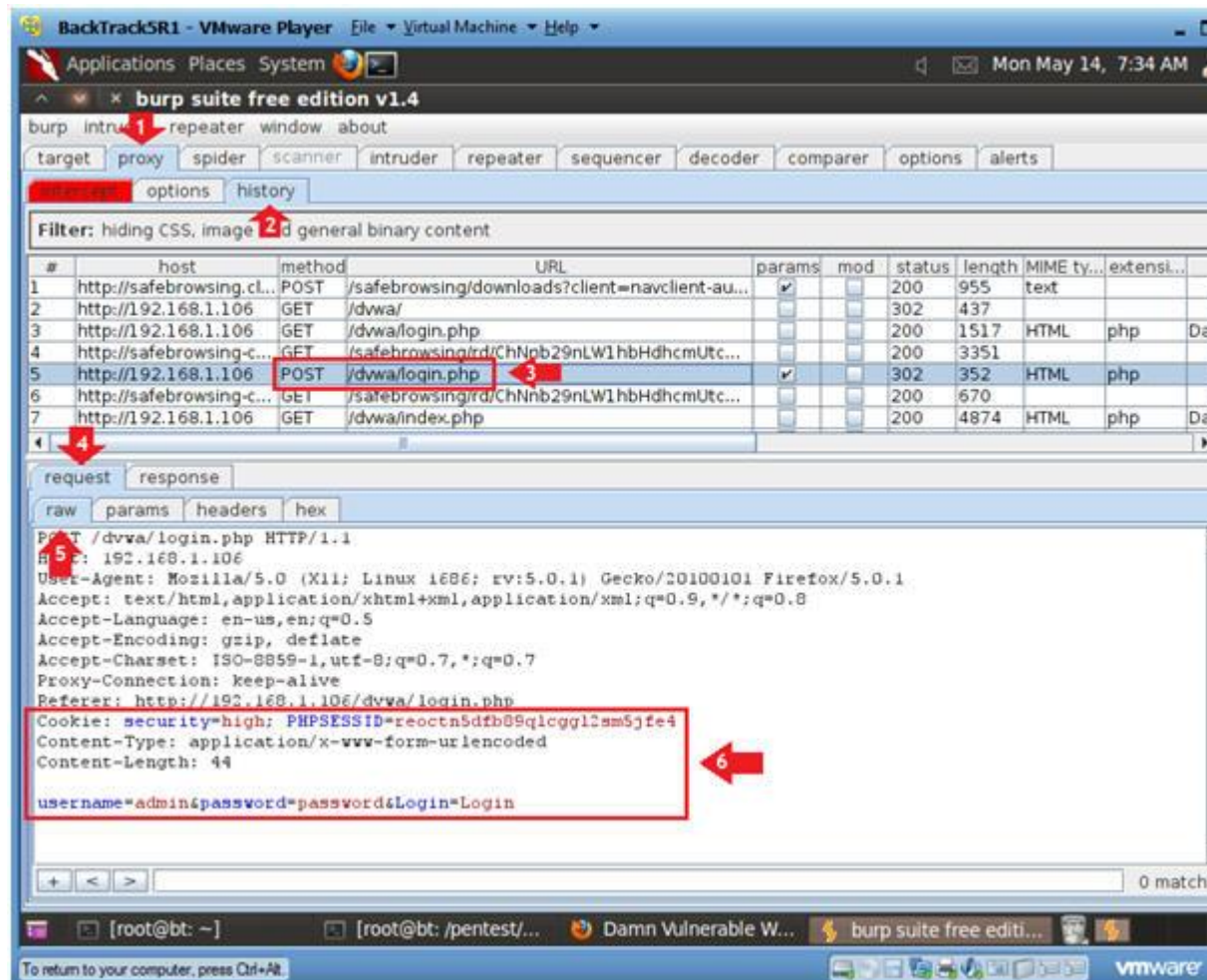
- **Instructions:**
 1. Click on the Forward Button 3 times.



6. View login.php results

○ **Instructions:**

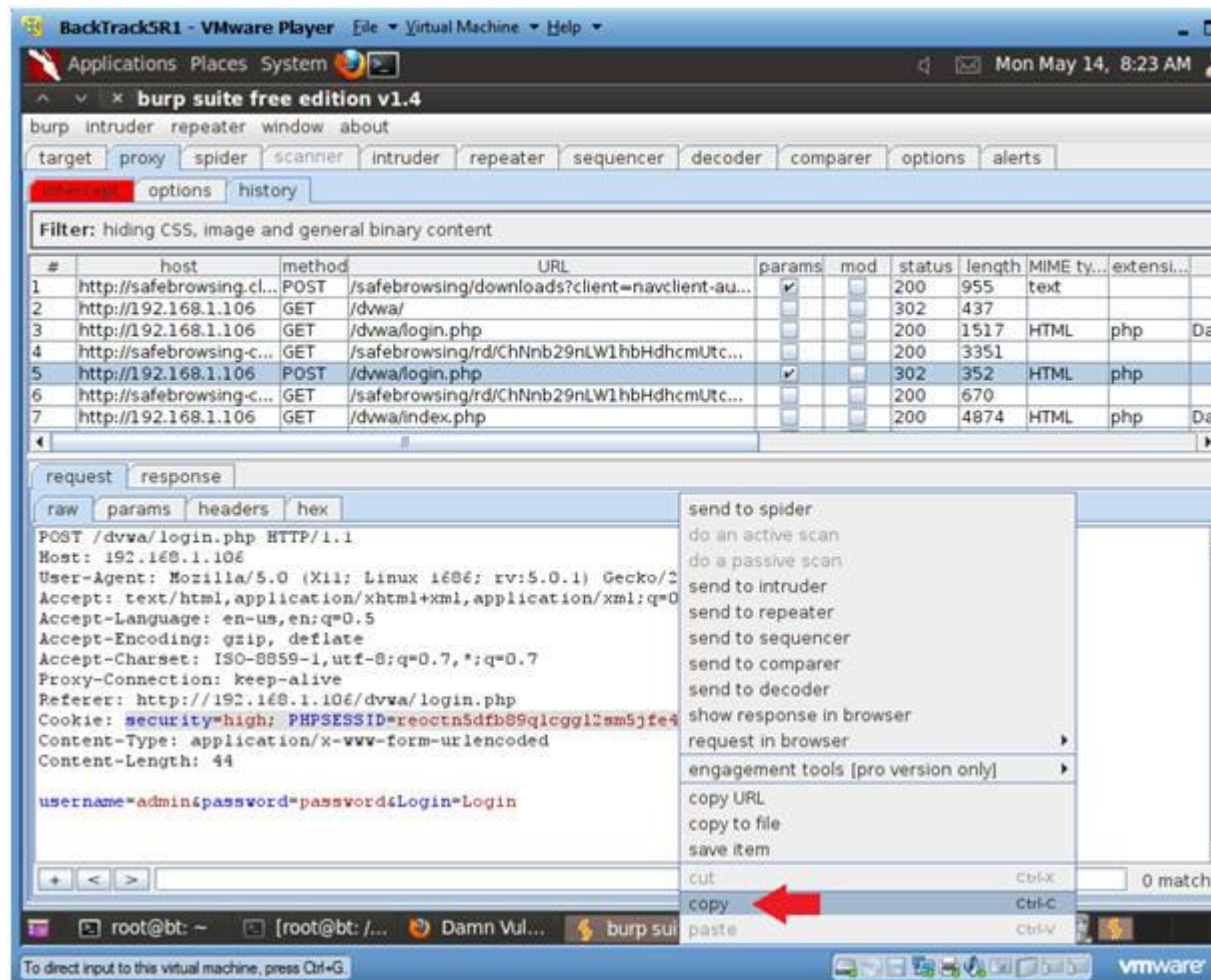
1. Click on the proxy tab
2. Click on the history tab
3. Click on /dvwa/login.php line that **contains method POST**.
4. Click on the request tab
5. Click on the raw tab
6. Notice that we now have the PHP Session ID, Username and F



7. Copy Session Information

Instructions:

1. Highlight the PHPSESSID information (See Below)
2. Right Click
3. Copy



8. Start Up Notepad

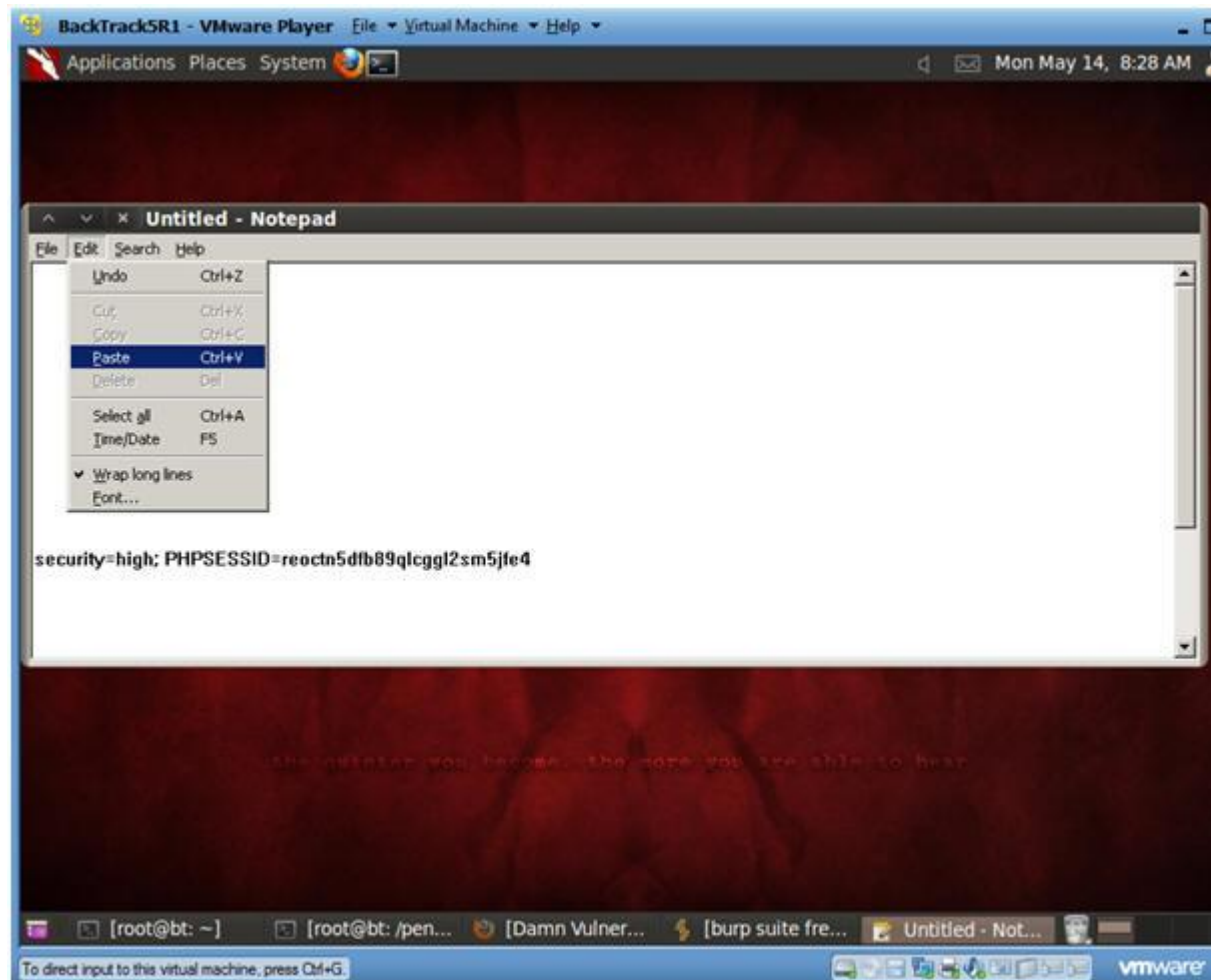
Instructions:

1. Applications --> Wine --> Programs --> Accessories --> Notepad



○

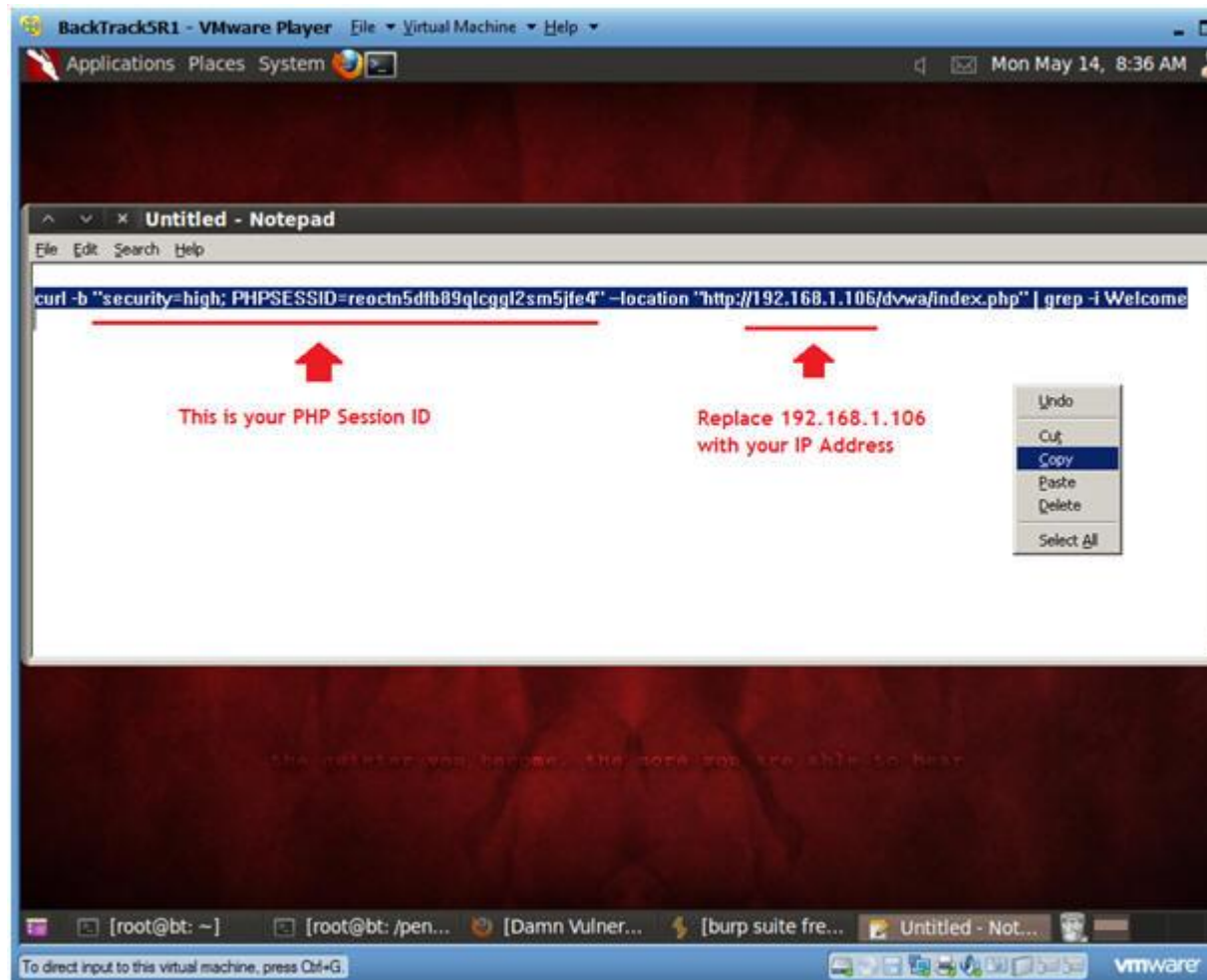
- 9. Paste URL into Notepad
 - **Instructions:**
 - 1. Edit --> Paste



10. Create a curl statement

- o **Instructions:**

1. curl -b "**security=high; PHPSESSID=reoctn5dfb89qlcgg12sm5jfe4**"
location "**http://192.168.1.106/dvwa/index.php**" | grep -i W
 - We are creating a curl statement to simulate a man-in-middle attack.
 - **PHP Session Note:** Remember to use the PHP Session info you captured in (Section 9, Step 7).
 - **IP Address Note:** Remember to use the IP Address Captured (Section 3, Step 3).
2. Highlight curl statement.
3. Right Click and Copy



○

Section 10: Curl Man-in-middle-attack

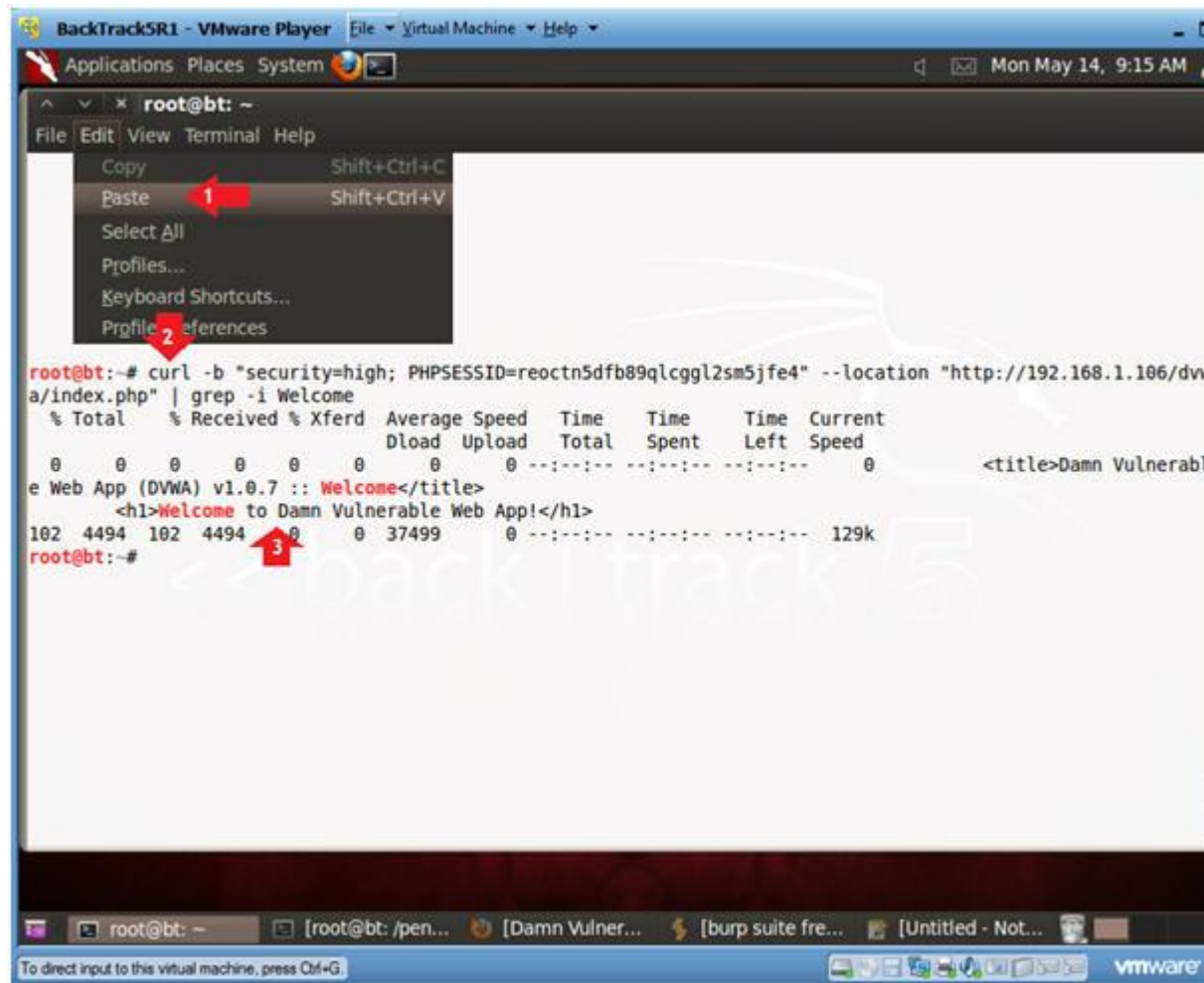
1. Open a console terminal
 - **Instructions:**
 1. Click on the console terminal



2. Issue Attack

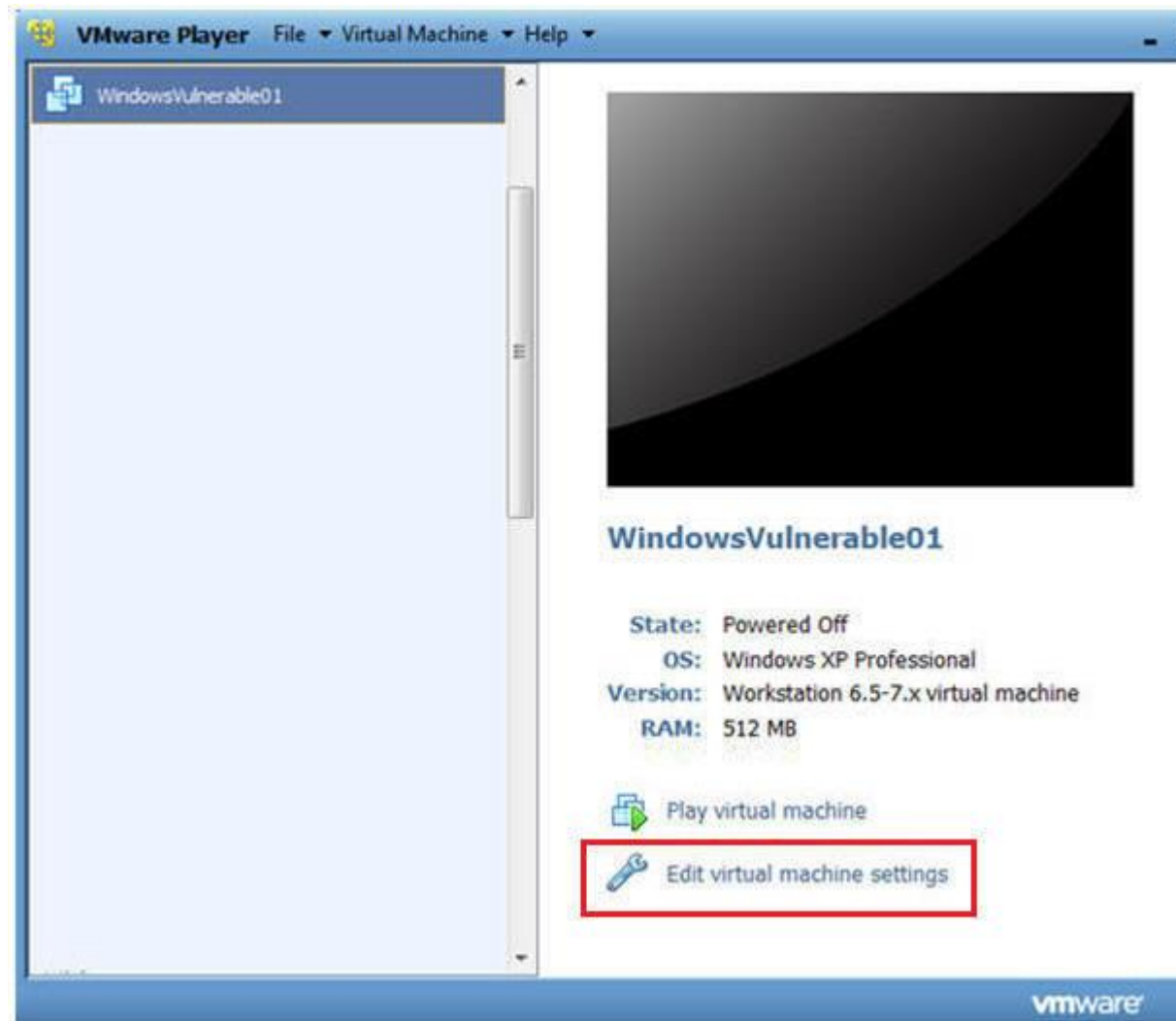
- **Instructions:**

1. Edit --> Paste
2. Press <Enter> after you verify the curl statement was correctly pasted.
3. Without supply any username and password information, notice the Welcome title displayed after logging into DVWA.



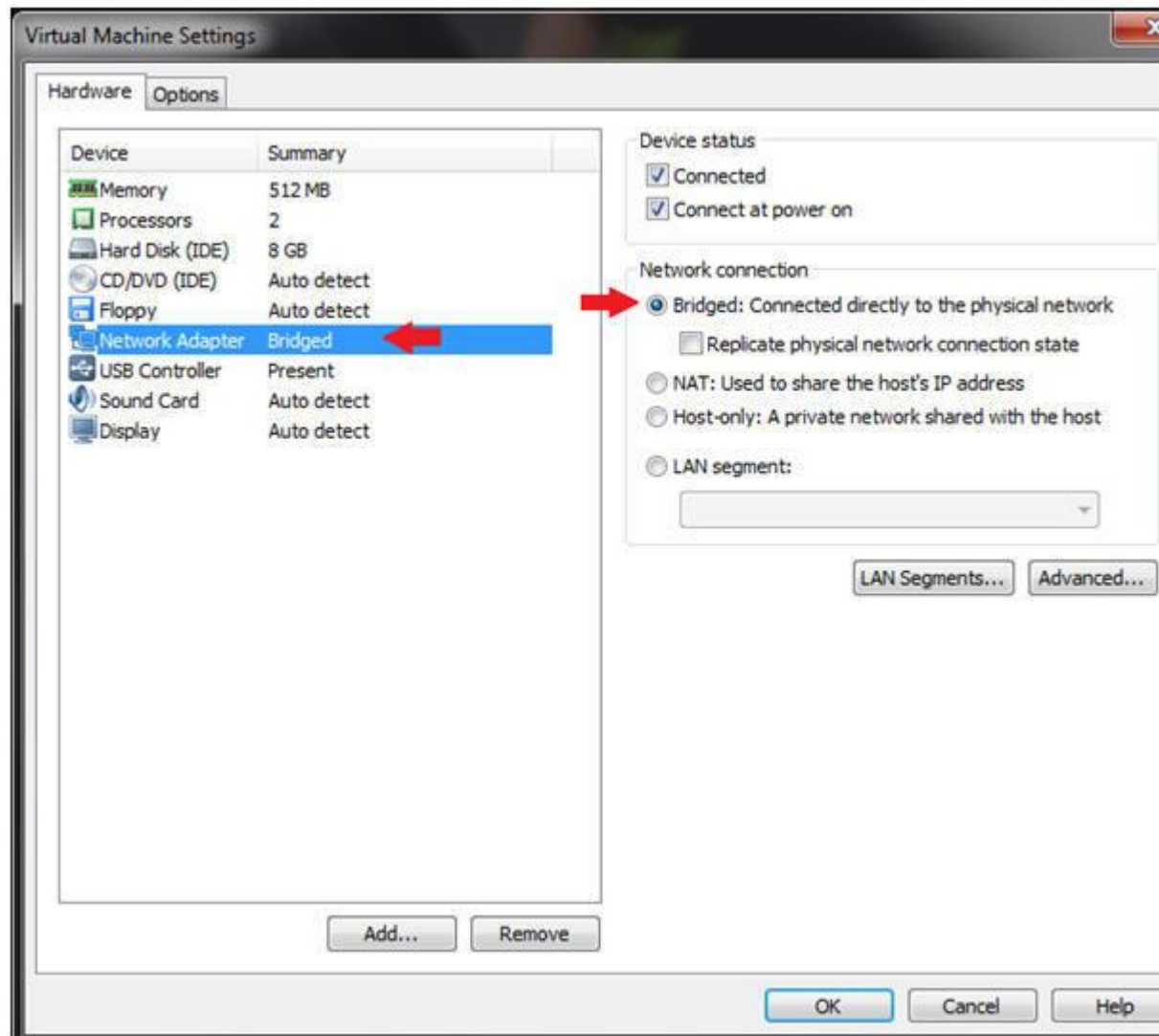
Section 11: Firefox Man-in-middle-attack

1. Booting up WindowsVulnerable01
 - o **Instructions:**
 1. Start up VMware Player
 2. Select WindowsVulnerable01
 3. Edit Virtual Machine

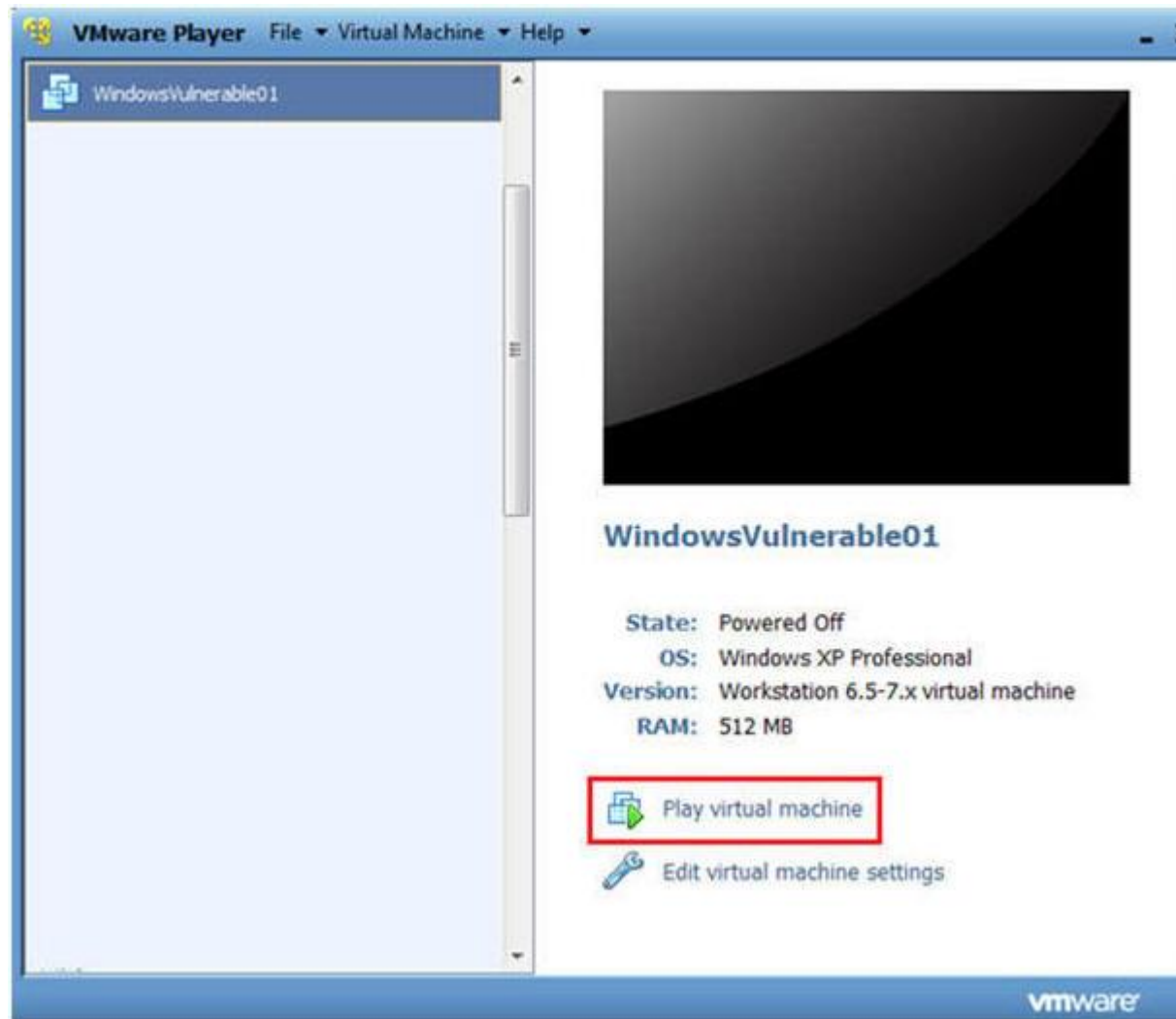


2. Configuring the Network Adapter

- **Instructions:**
 1. Select Network Adapter
 2. Select Bridged Connection
 3. Select OK

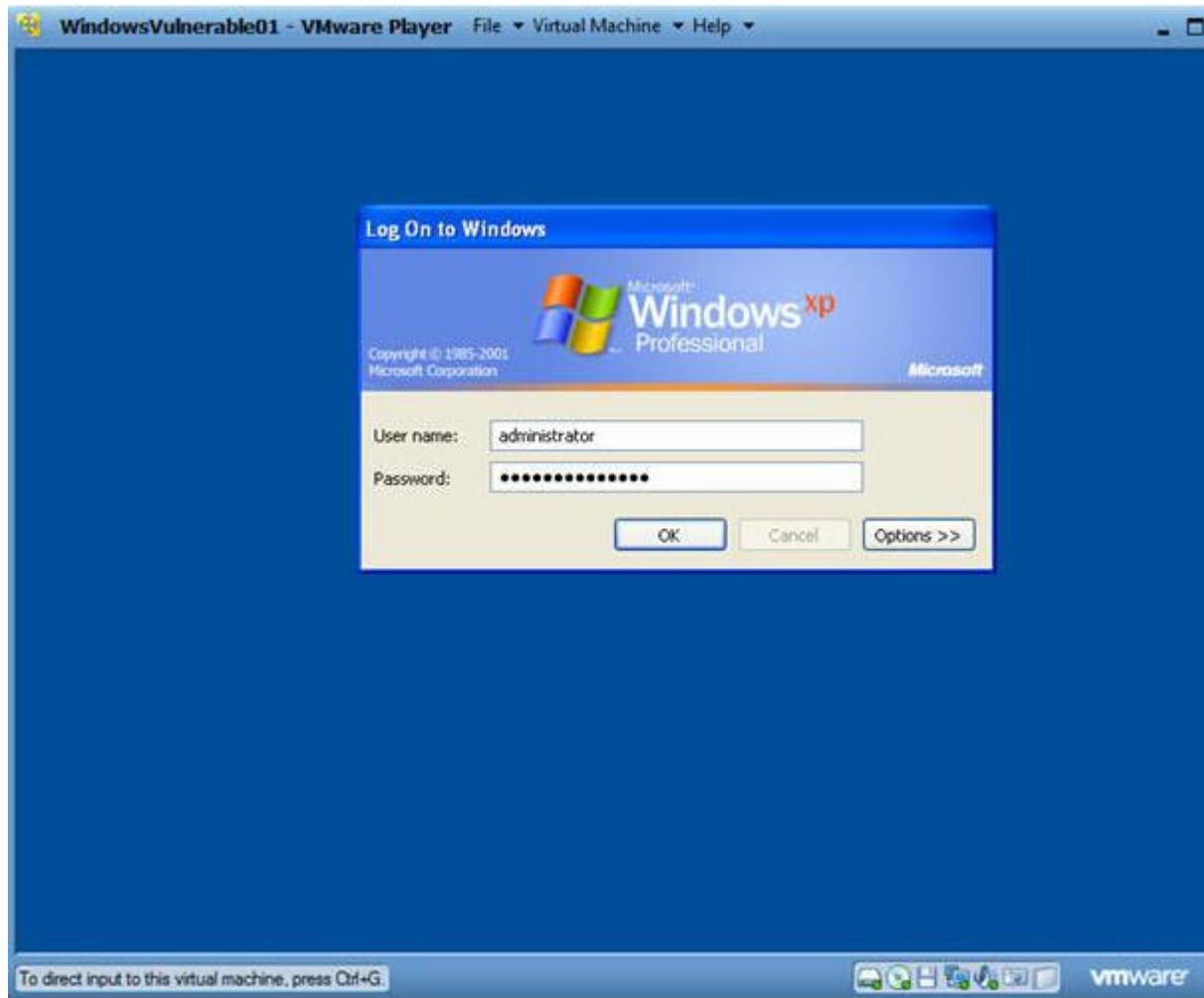


- 3. Play WindowVulnerable01
 - **Instructions:**
 1. Select Play virtual Machine



○

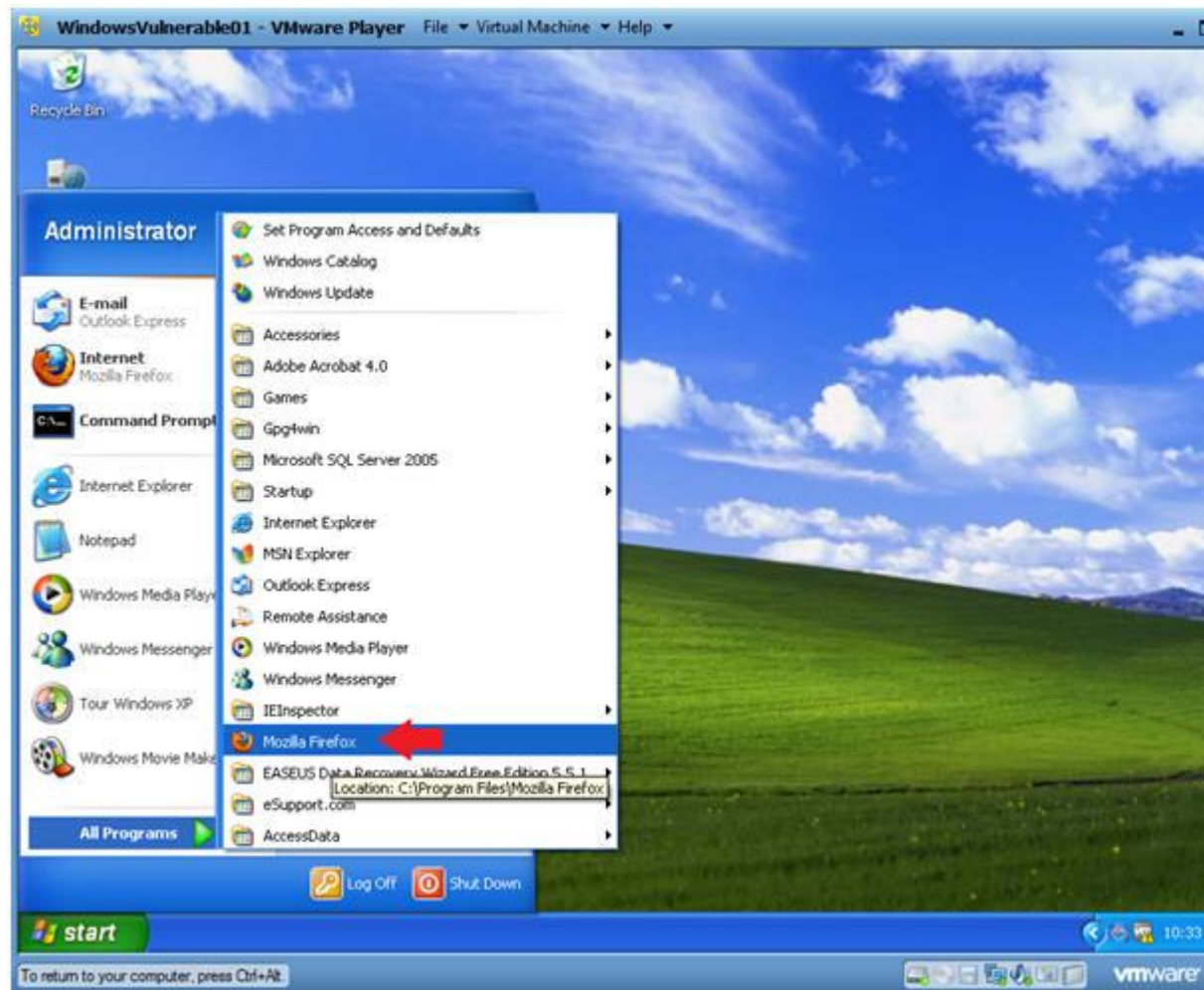
4. WindowsVulnerable01 Authentication
 - **Instructions:**
 1. Login as administrator



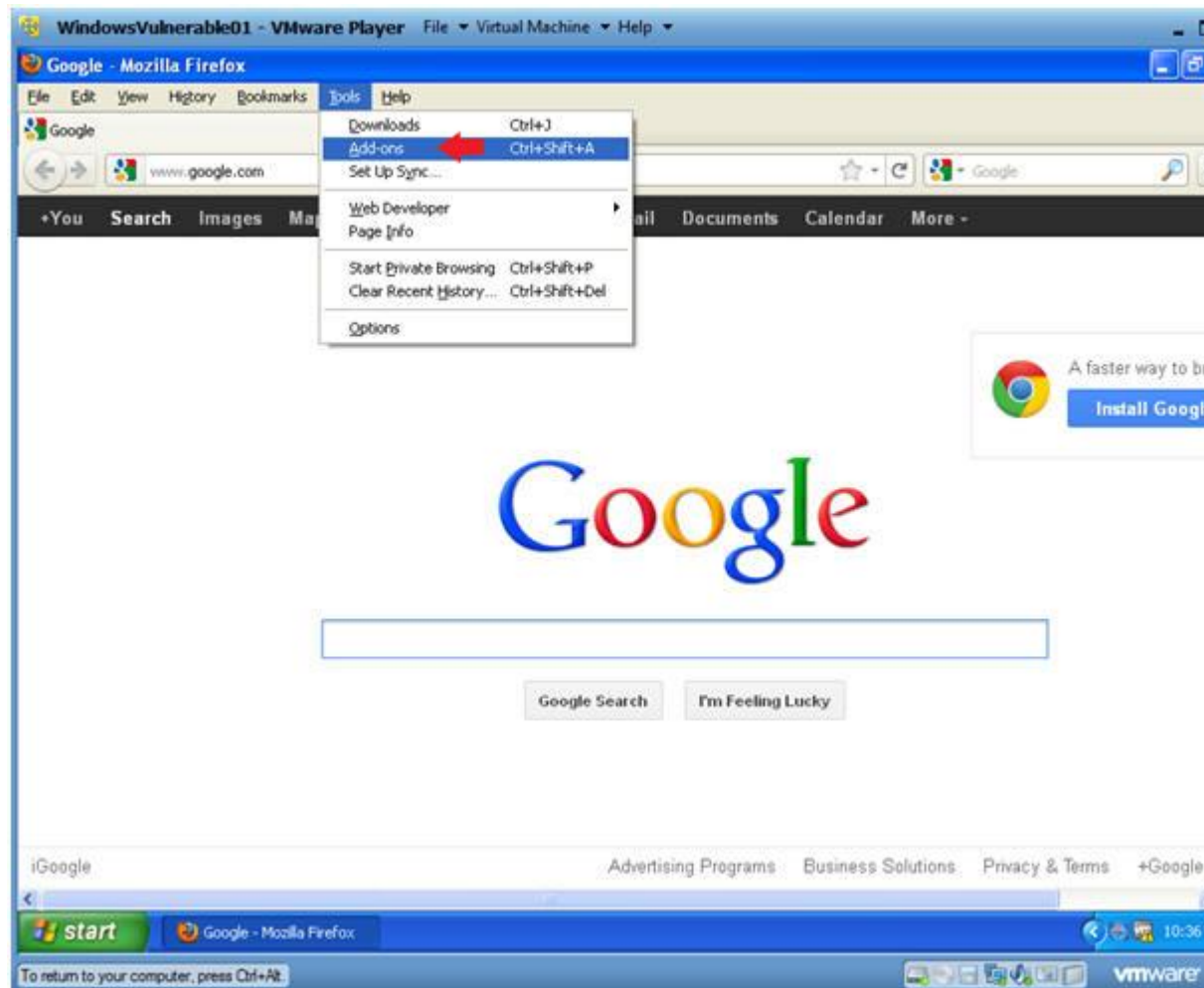
5. Start FireFox

- **Instructions:**

- 1. Start --> All Programs --> Mozilla Firefox



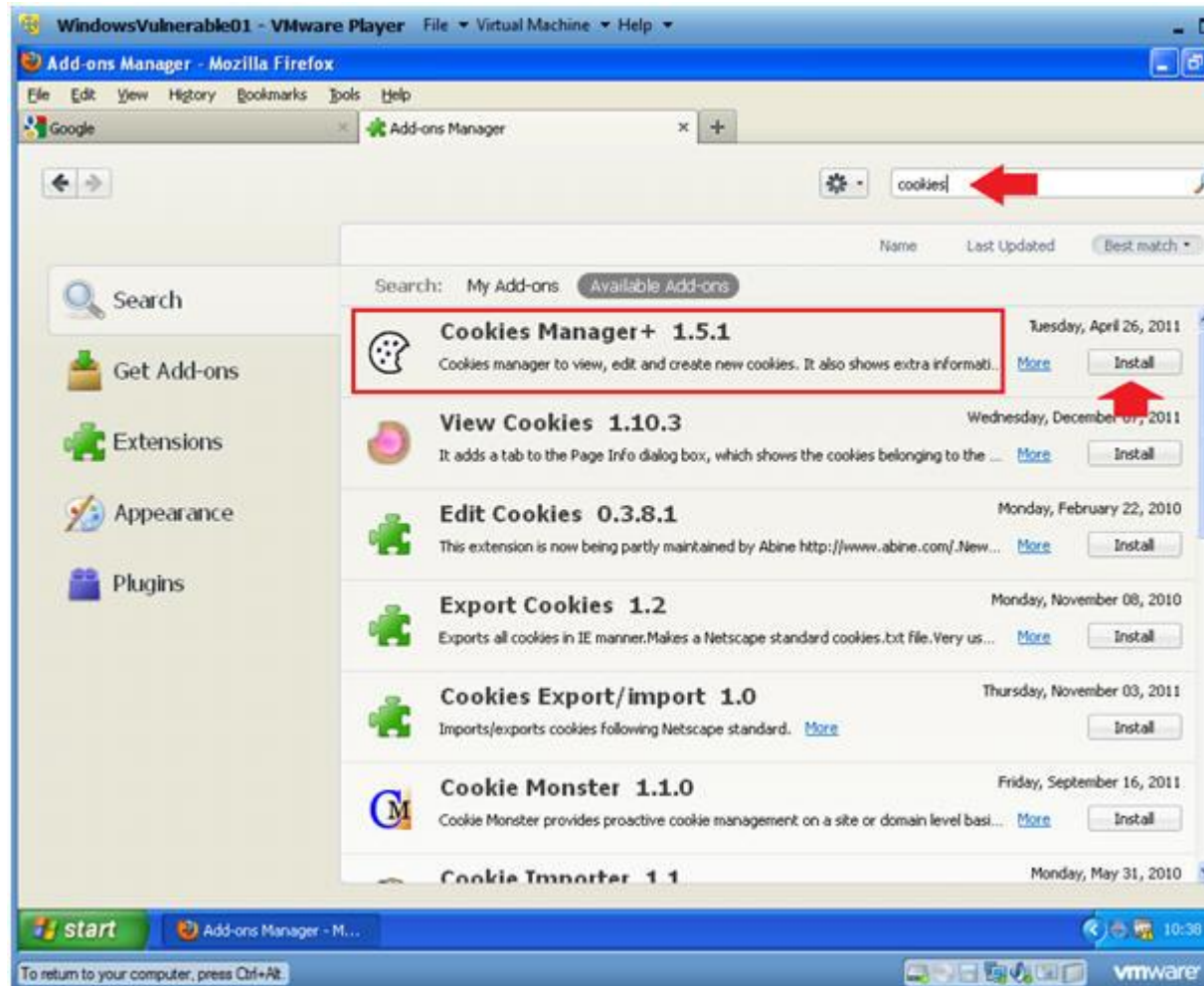
- 6. Go to Add-ons
 - 1. Tools --> Add-ons



7. Install Cookies Manager+ 1.5.1

○ **Instructions:**

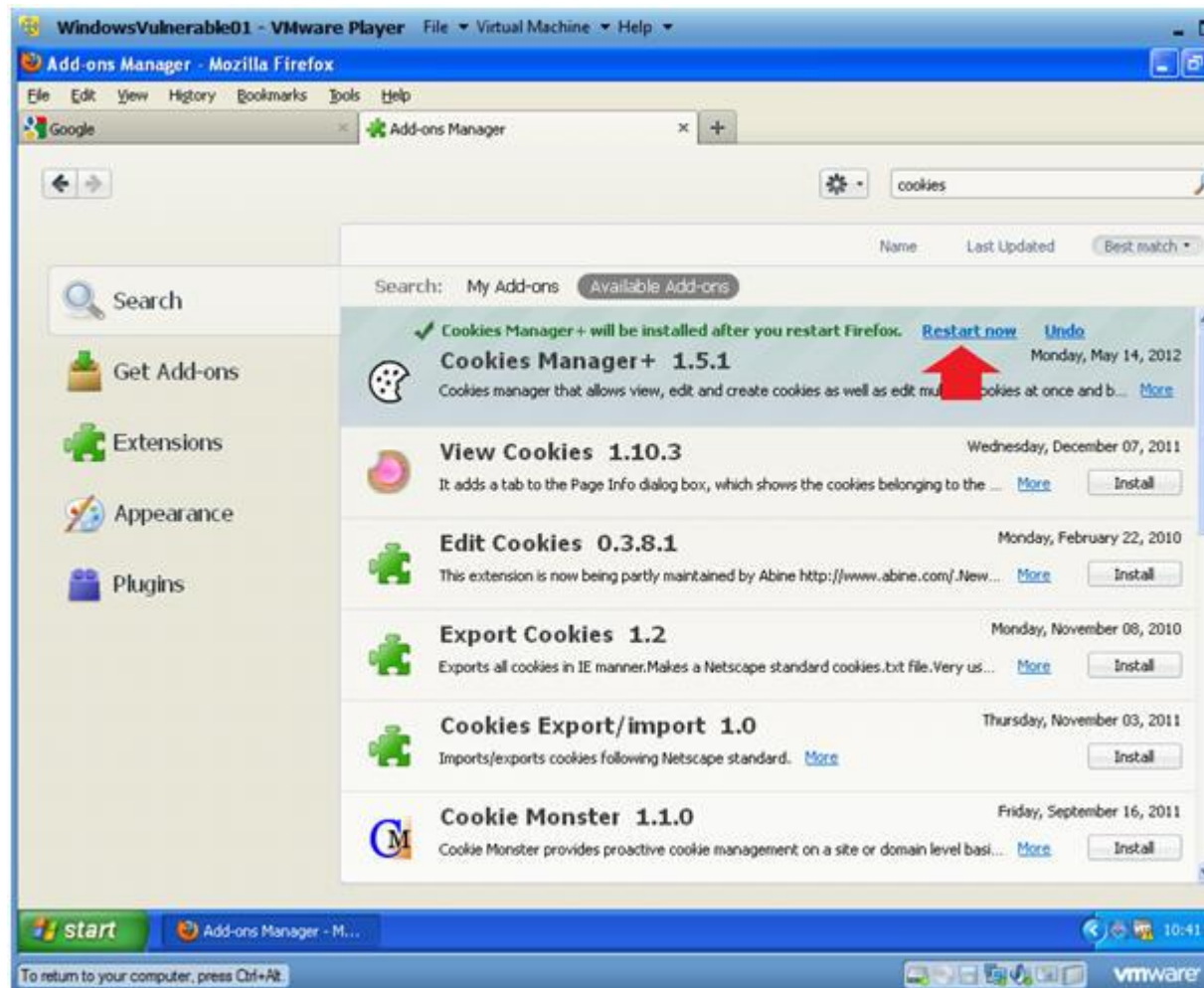
1. Search for cookies
2. Click the Install button next to Cookies Manager+ 1.5.1



8. Restart Firefox

- **Instructions:**

- 1. Click Restart now



9. Browse to DVWA's Login Page

○ **Instructions:**

1. `http://192.168.1.106/dvwa/login.php`
 - Replace 192.168.1.106 with the DVWA's address obtained (Section 3, Step 3).
2. DO NOT LOGIN!!!

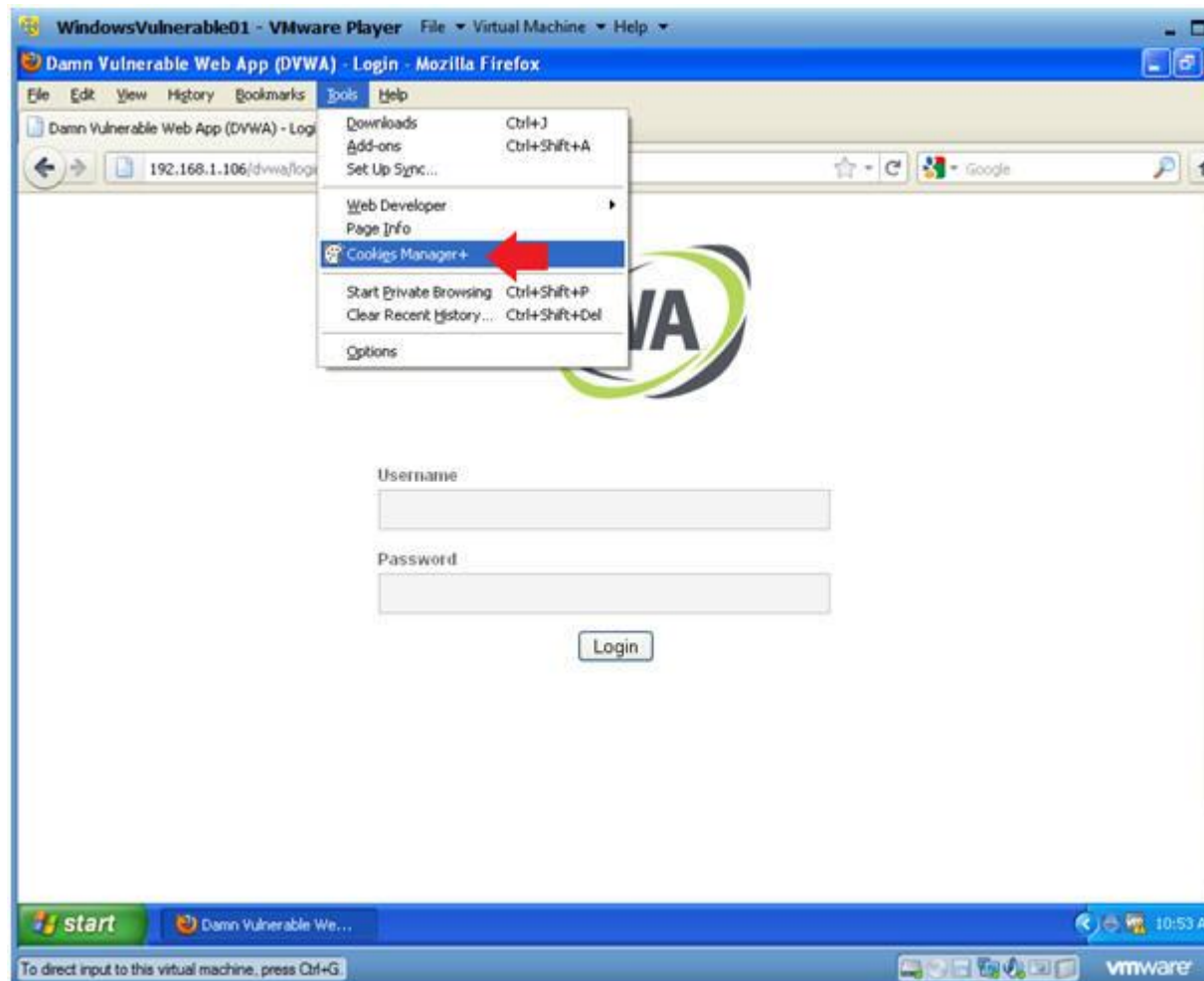


○

10. Start Cookies Manager+

○ **Instructions:**

1. Tools --> Cookies Manager+

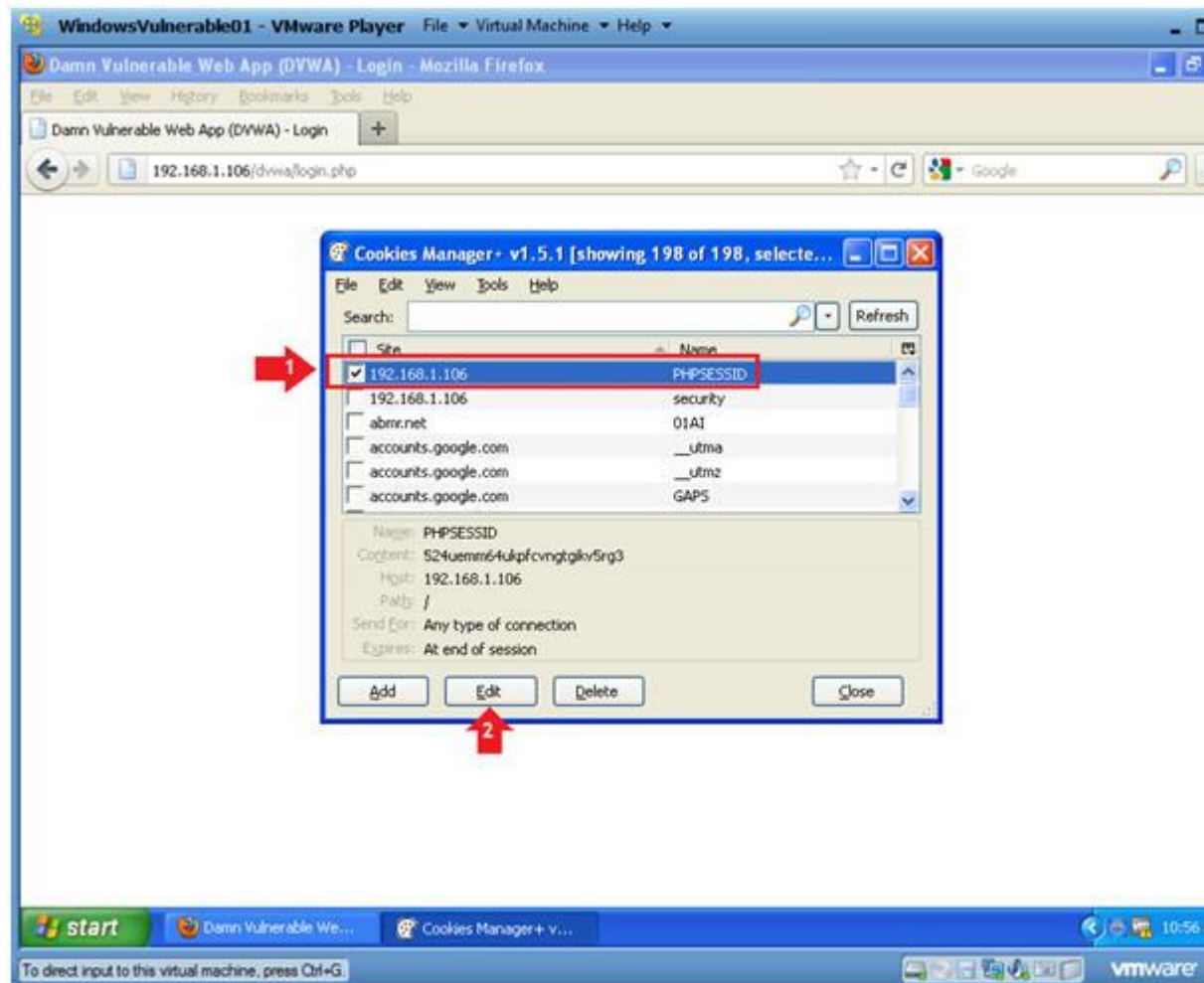


○

11. Edit PHPSESSID Cookie

○ **Instructions:**

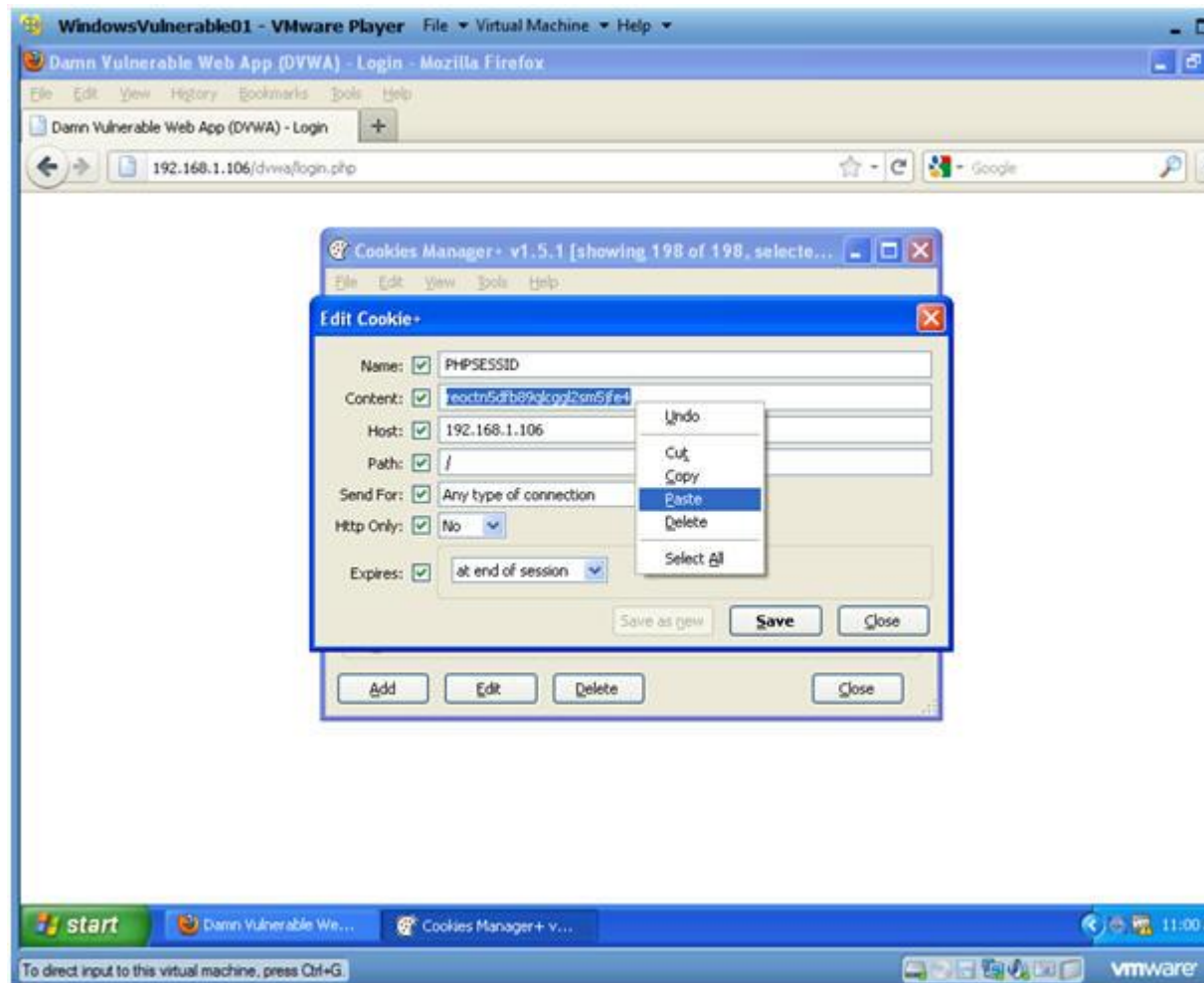
1. Select the PHPSESSID cookie that was just created
2. Click on the edit button



12. Replace PHPSESSID Cookie

Instructions:

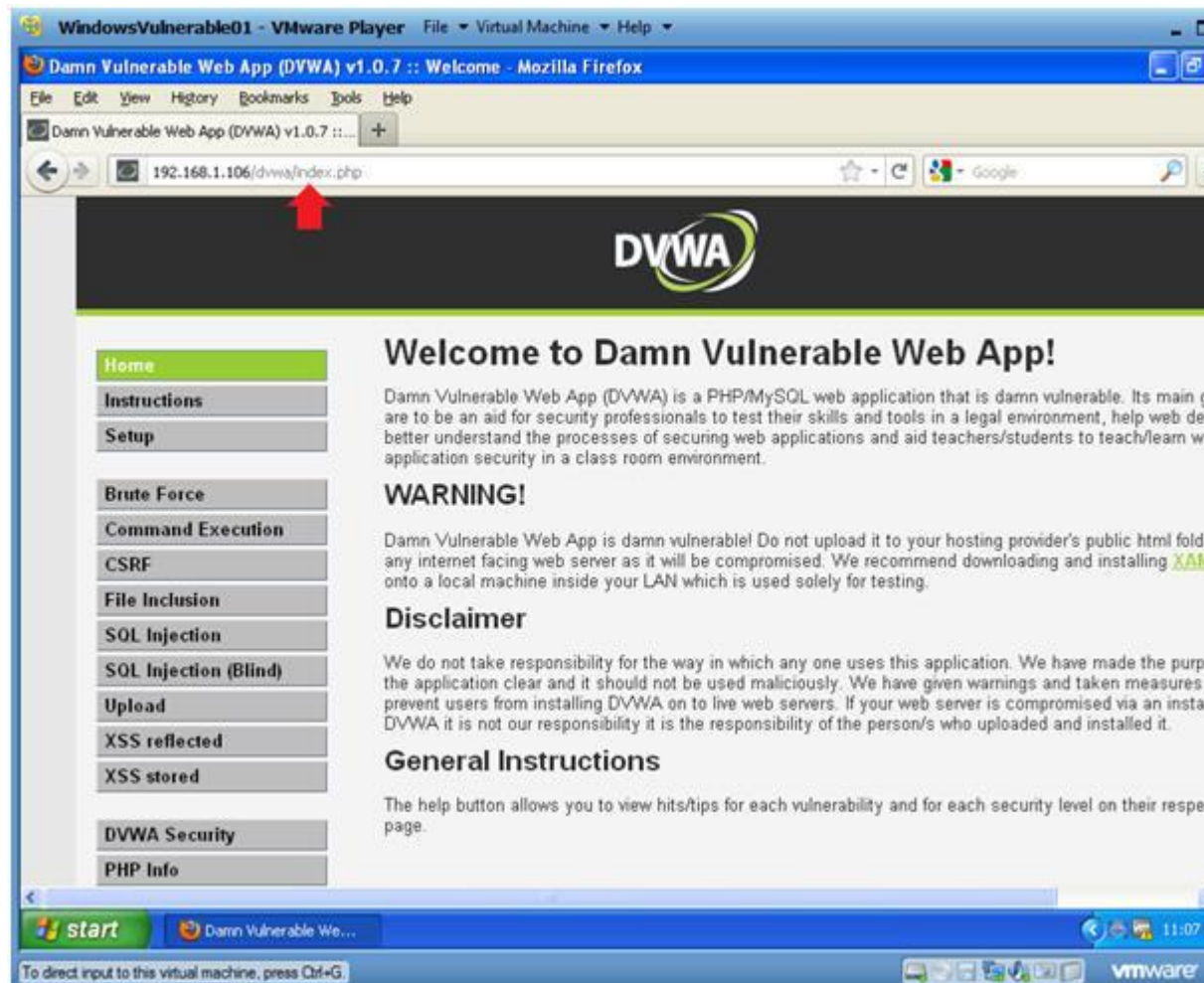
1. Delete the PHPSESSID in the Content textbox.
2. In the Content textbox, Paste the PHPSESSID obtained from 9, Step 7).
3. Click Save
4. Click the Close Button



13. Launch Man-in-middle-attack

- o **Instructions:**

1. Replace login.php with index.php. Your URL should look similar to the following:
 - `http://192.168.1.106/dvwa/index.php`
 - Remember to replace 192.168.1.106 with DVWA's IP address obtained in (Section 3, Step 3).
2. Press <Enter>
3. Notice you just by-passed the login screen and successfully executed a man-in-the-middle attack.



Section 12: Clean Up Notes

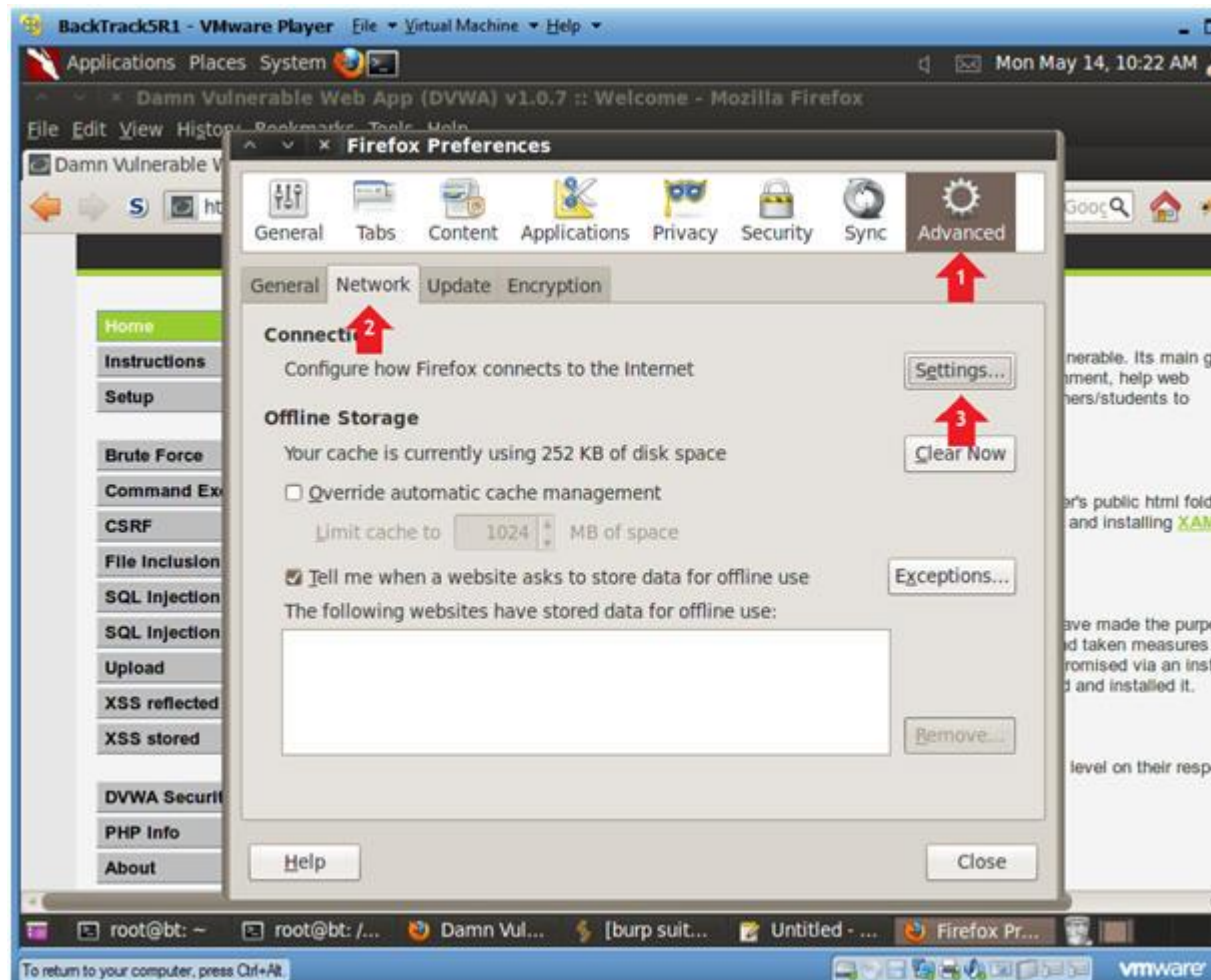
1. On BackTrack's Firefox
 - **Instructions:**
 1. Edit --> Preferences



2. Edit Network Settings

o **Instructions:**

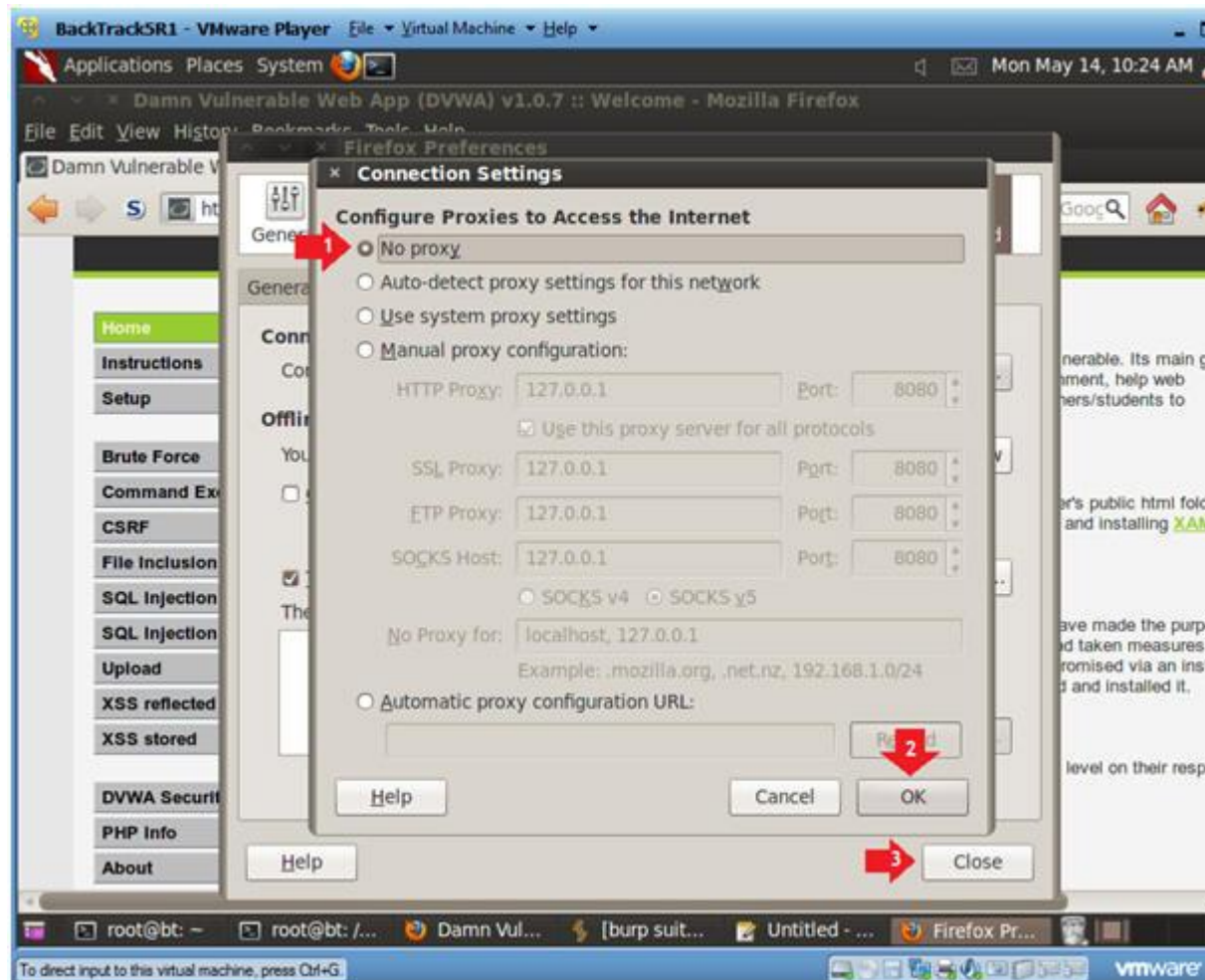
1. Click on Advanced
2. Click on Network Tab.
3. Click on Settings Button.



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 13: Proof of Lab

1. Proof of Lab

o **Proof of Lab Instructions:**

1. Pull up your BackTrack Terminal Window
2. `history | grep curl | grep Welcome | grep -v history | tail`
3. `date`
4. `echo "Your Name"`
 - Replace the string "Your Name" with your actual name.
 - e.g., `echo "John Gray"`
5. Do a <PrtScn>
6. Paste into a word document
7. Upload to Moodle

