

(Damn Vulnerable Web App (DVWA) :

{ Using nikto.pl }

Section 0. Background Information

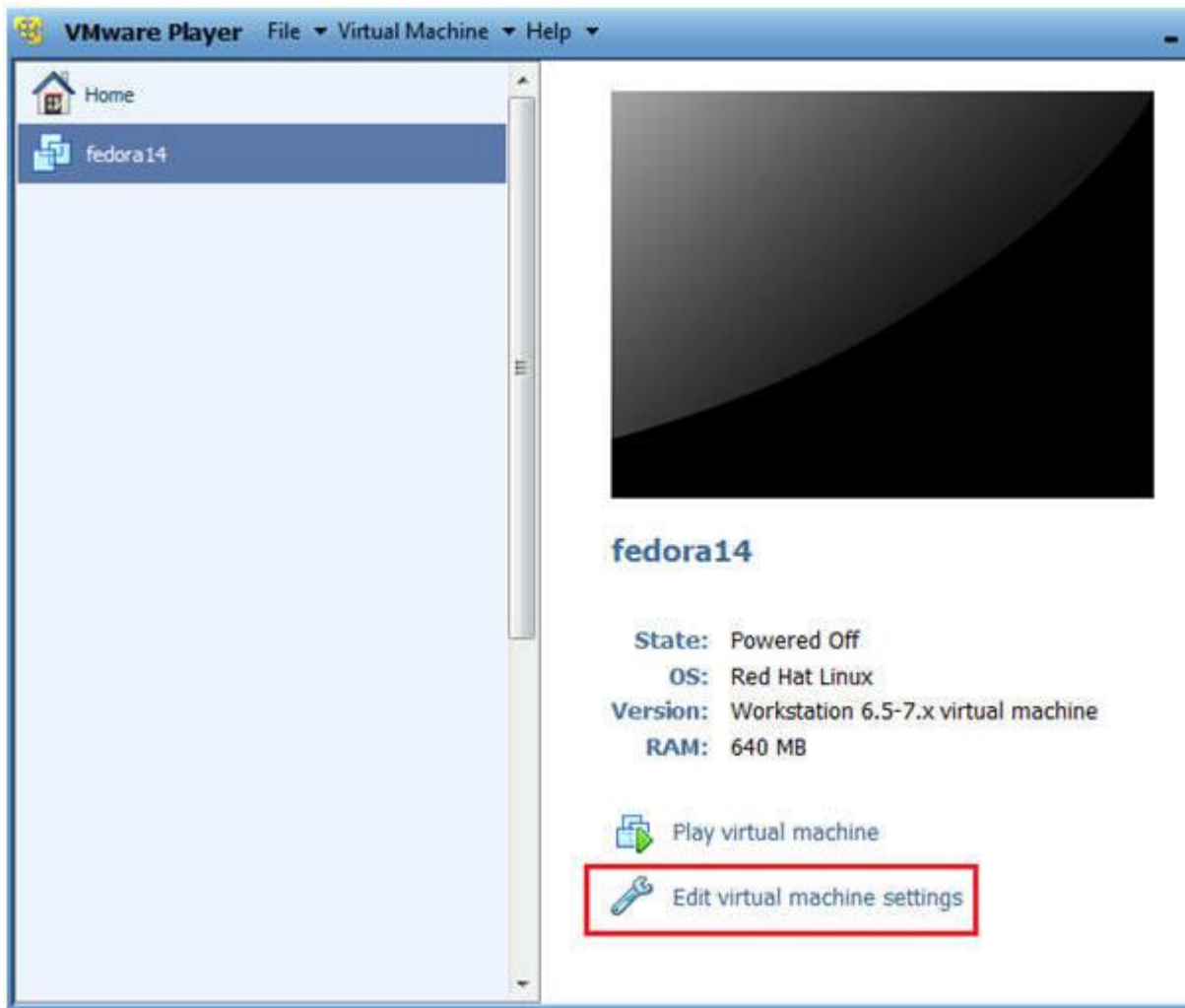
1. What is Damn Vulnerable Web App (DVWA)?
 - o Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is intentionally damn vulnerable.
 - o Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a controlled environment.
2. What is Nikto?
 - o Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 2700 common web server plugins.
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 use nikto.pl to scan DVWA for vulnerabilities.
 2. We show you how to manually grab a webserver and operating system banner.
 3. We will show you an old but still common mistake some web administrators/developers make by placing a configuration file under a web folder.
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,**

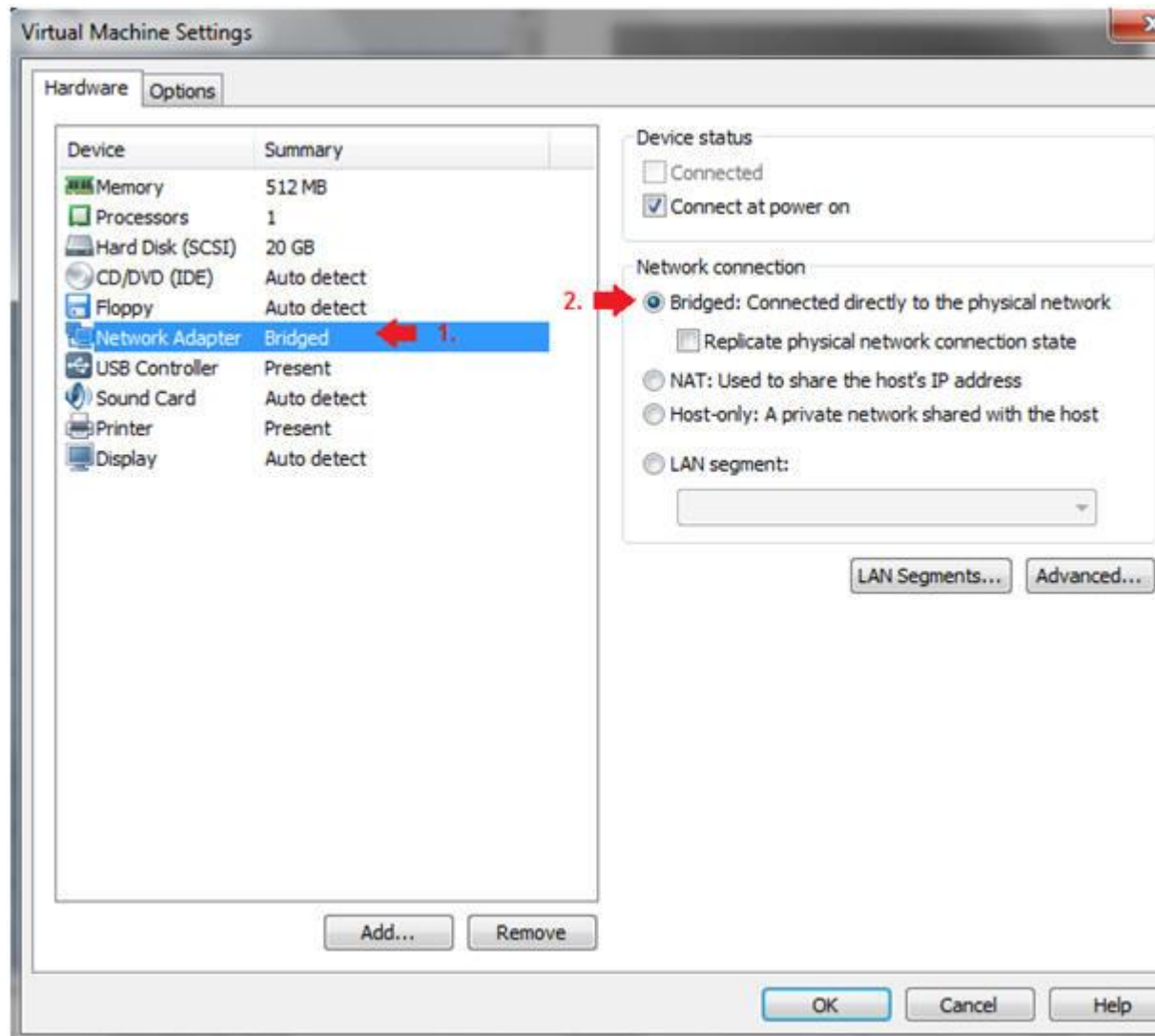
conditions, and notices.

- 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

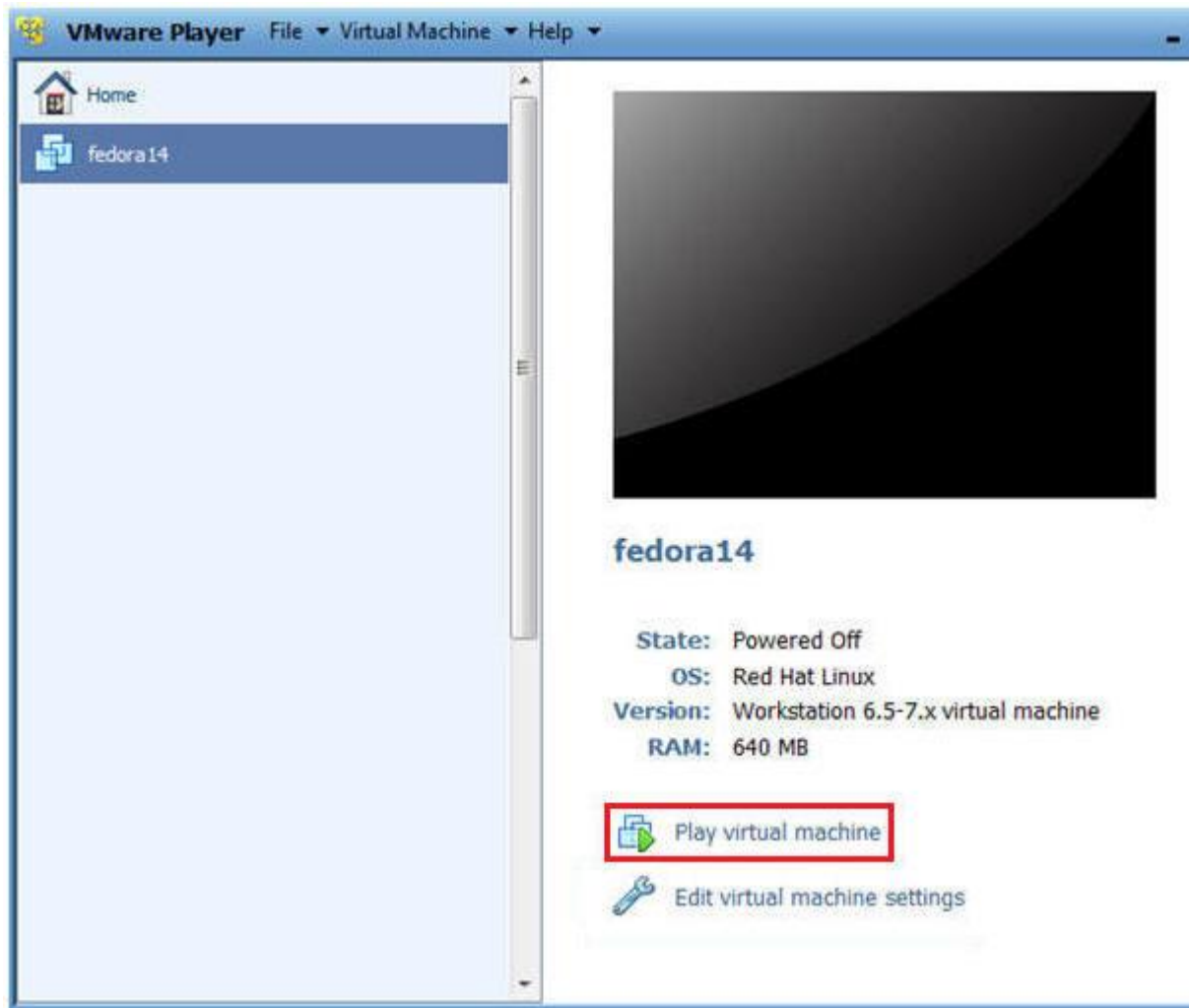
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit Fedora14 Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings
 -
3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Click on the OK Button.



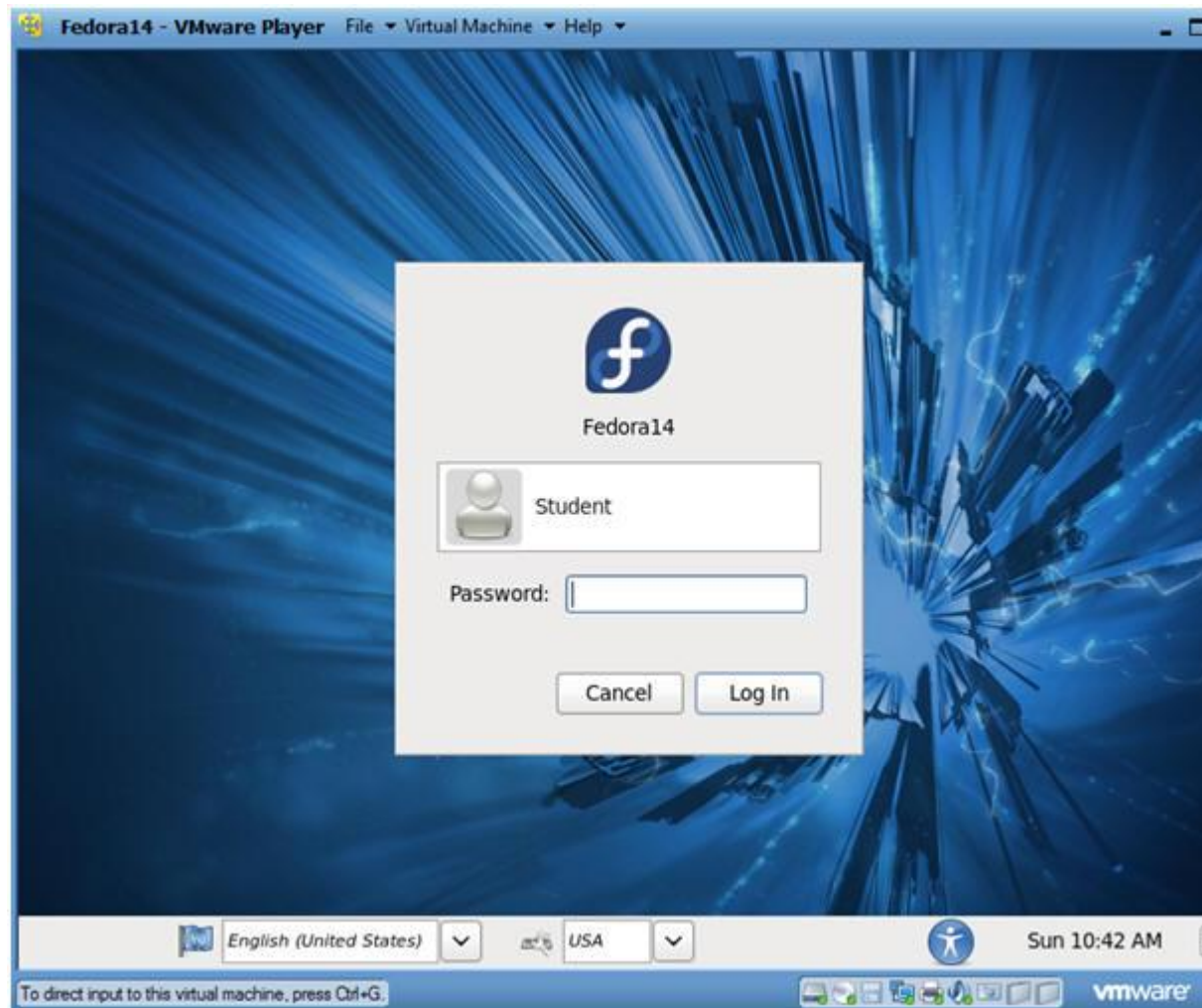


Section 2: Login to Fedora14

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>.



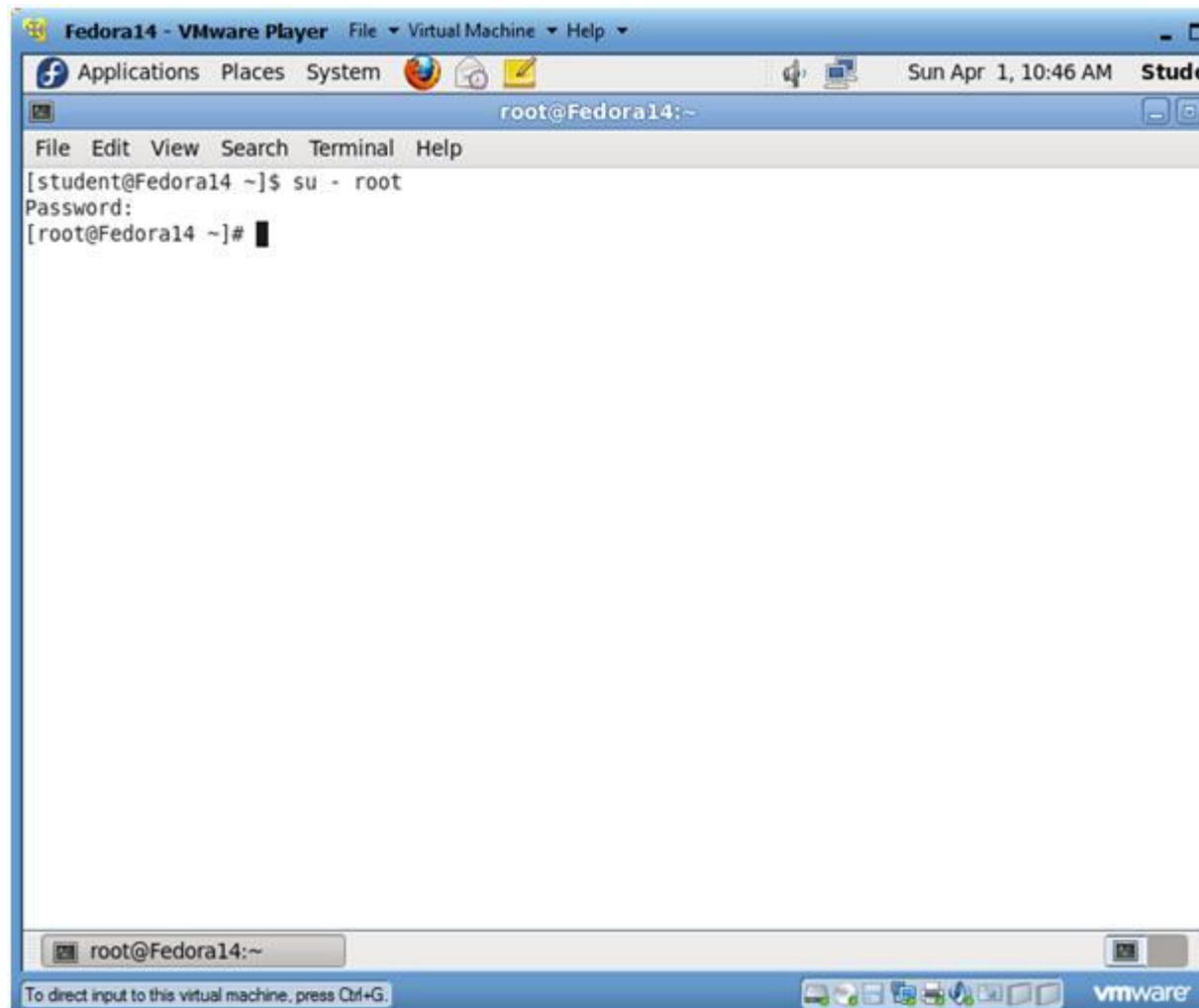
○

Section 3: Open Console Terminal and Retrieve IP Address

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

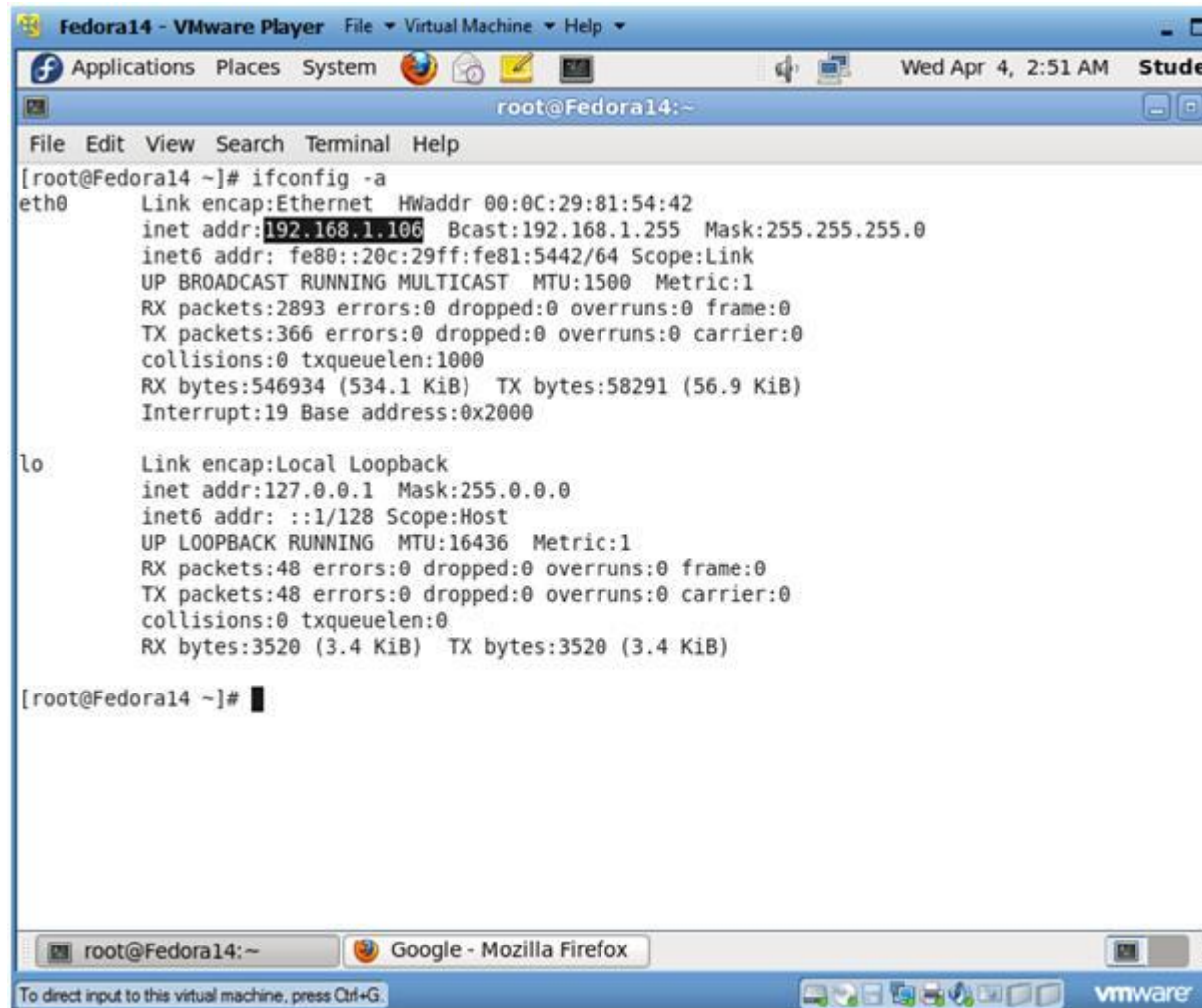


- - 2. Switch user to root
 - **Instructions:**
 - 1. `su - root`
 - 2. <Whatever you set the root password to>



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.



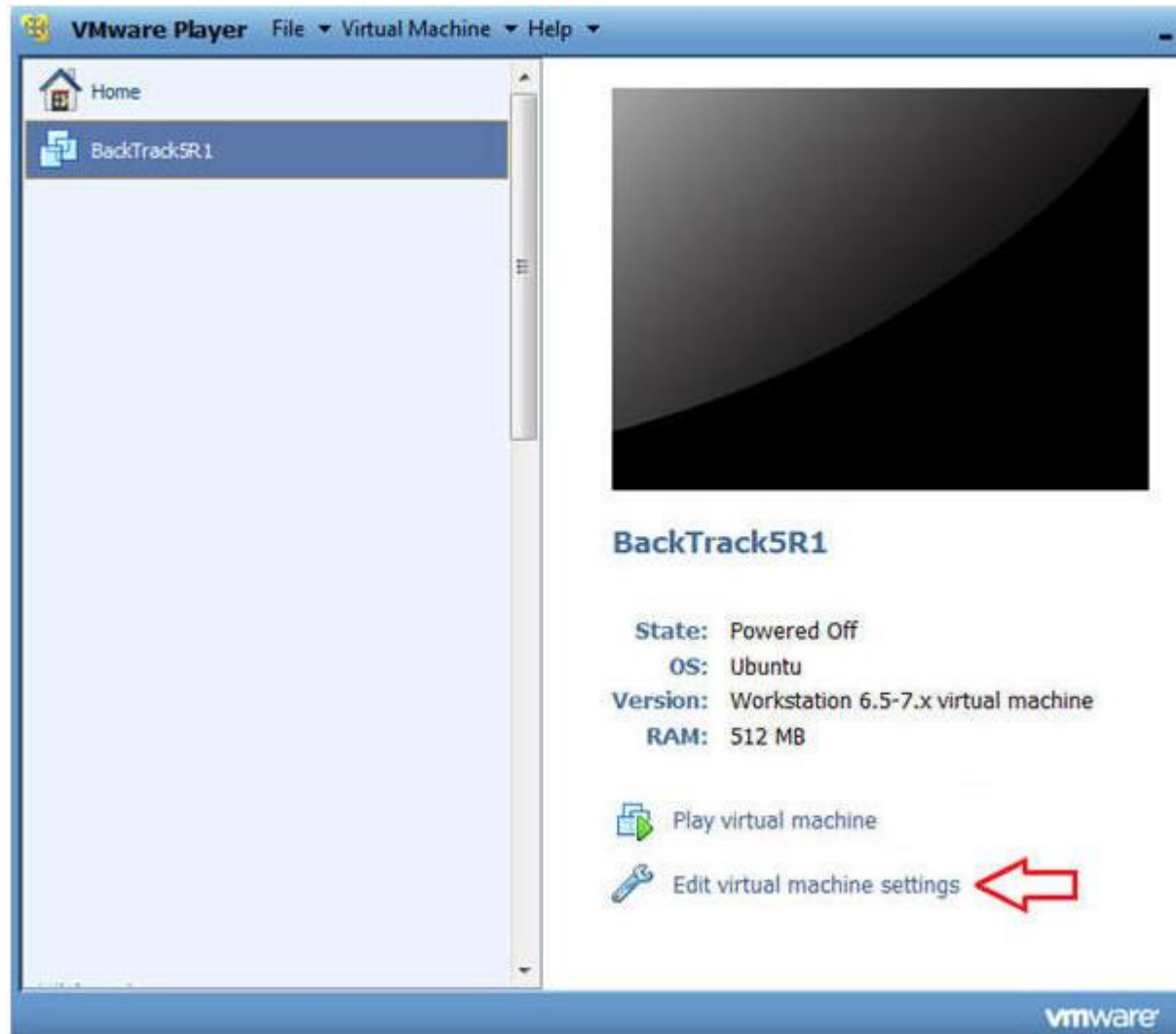
```
Fedora14 - VMware Player File Virtual Machine Help
Applications Places System Wed Apr 4, 2:51 AM
root@Fedora14:~
File Edit View Search Terminal Help
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:81:54:42
          inet addr:192.168.1.106  Bcast:192.168.1.255  Mask:255.255.255.0
          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)

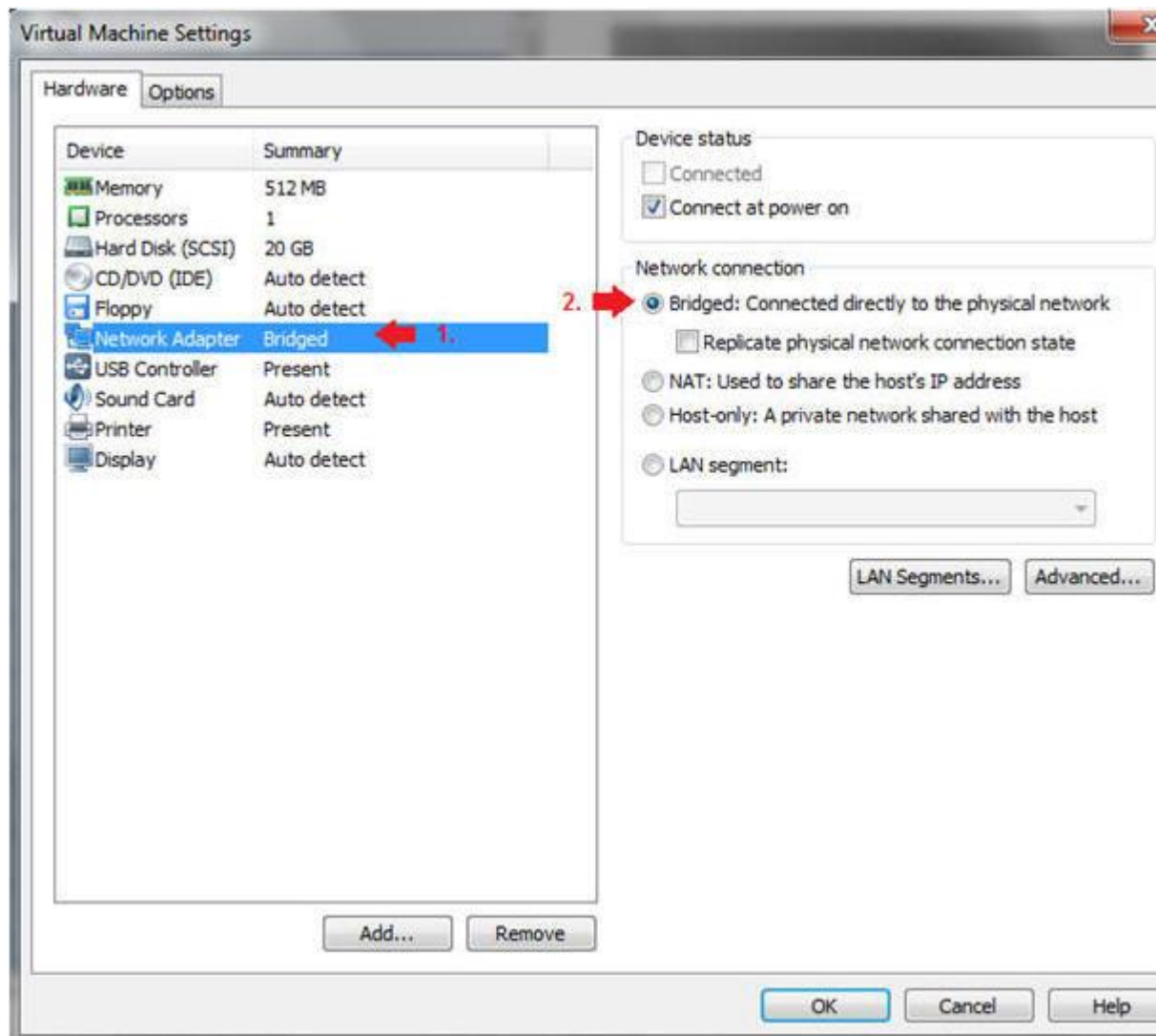
[root@Fedora14 ~]#
```

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

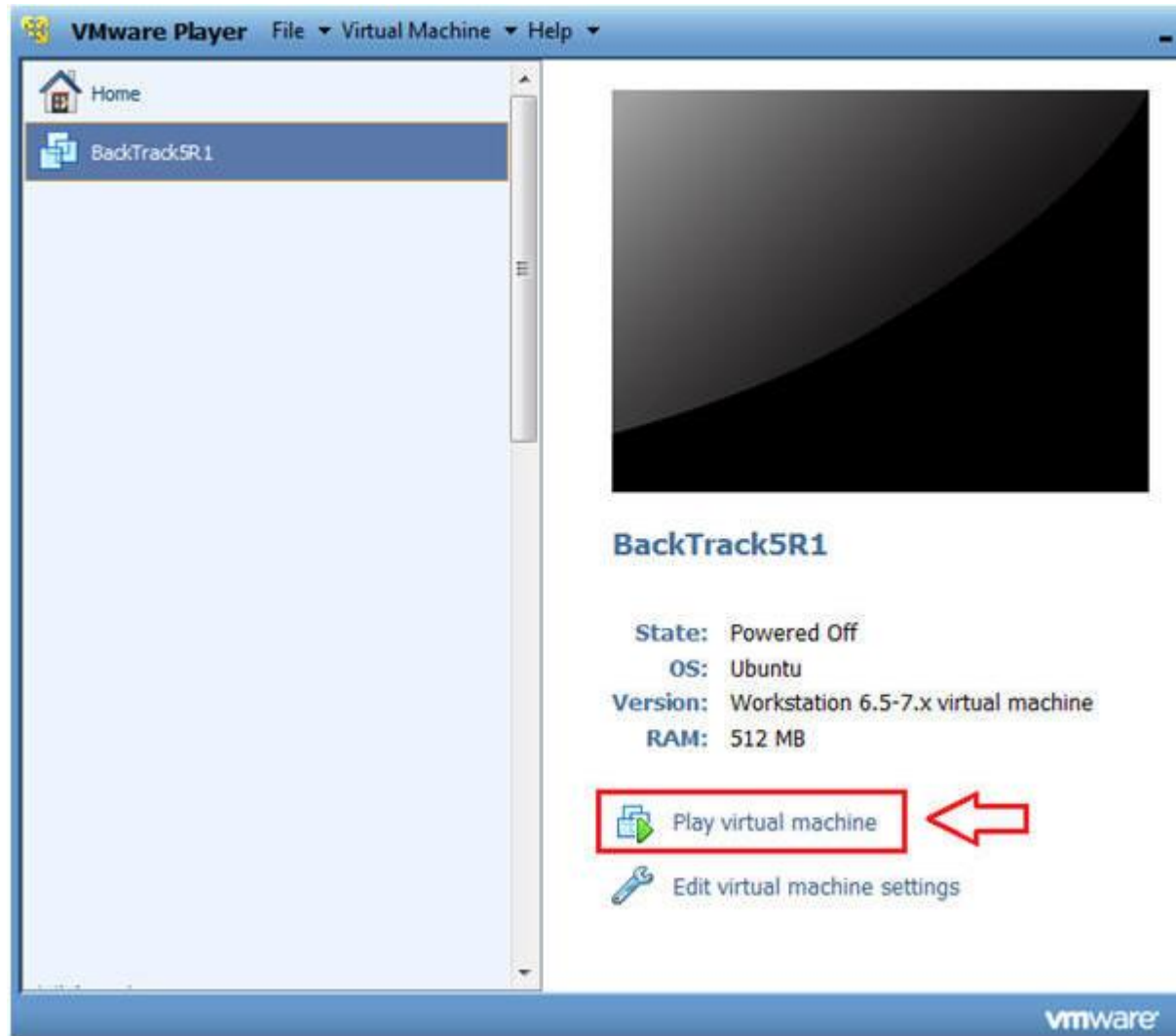


- - 3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Do not Click on the OK Button.



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:**

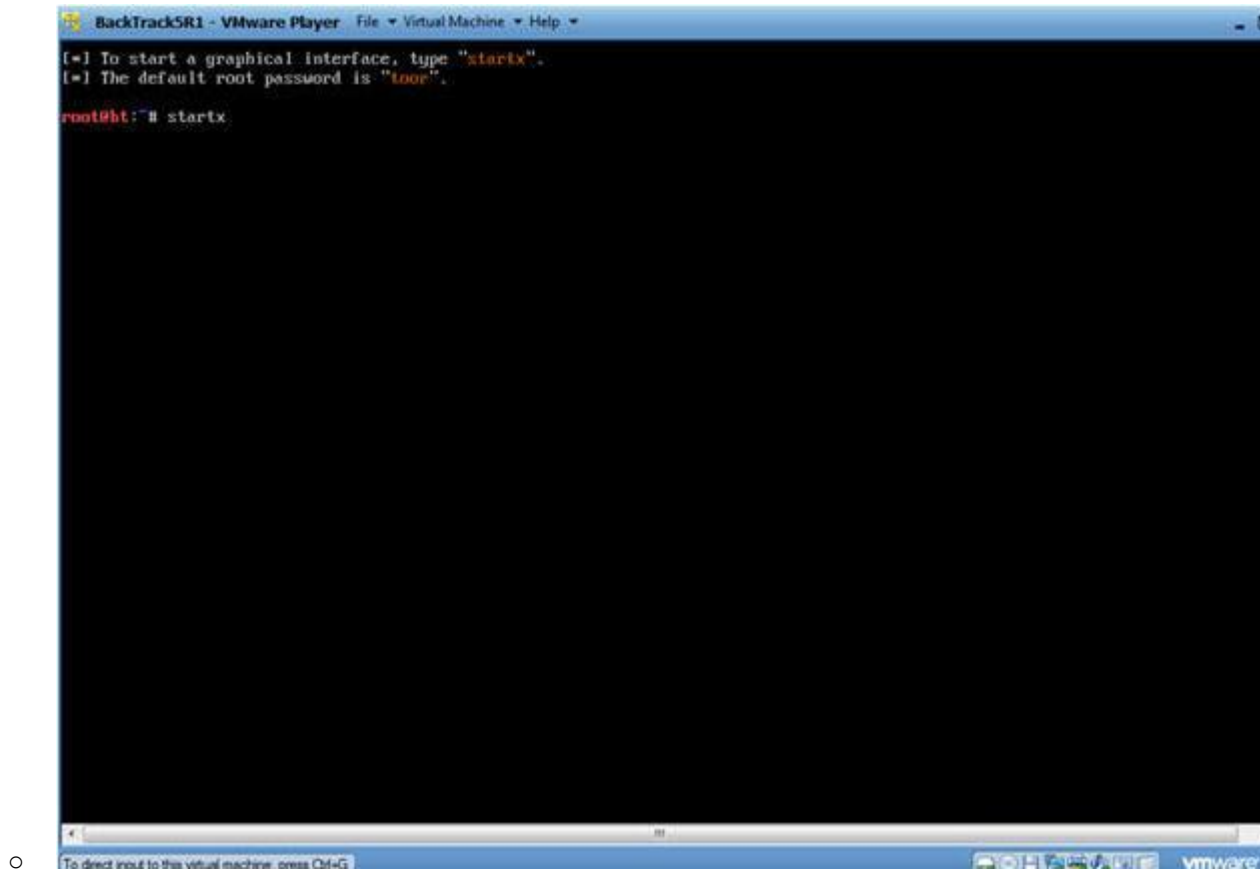
1. Login: root
2. Password: toor or <whatever you changed it to>.

```
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



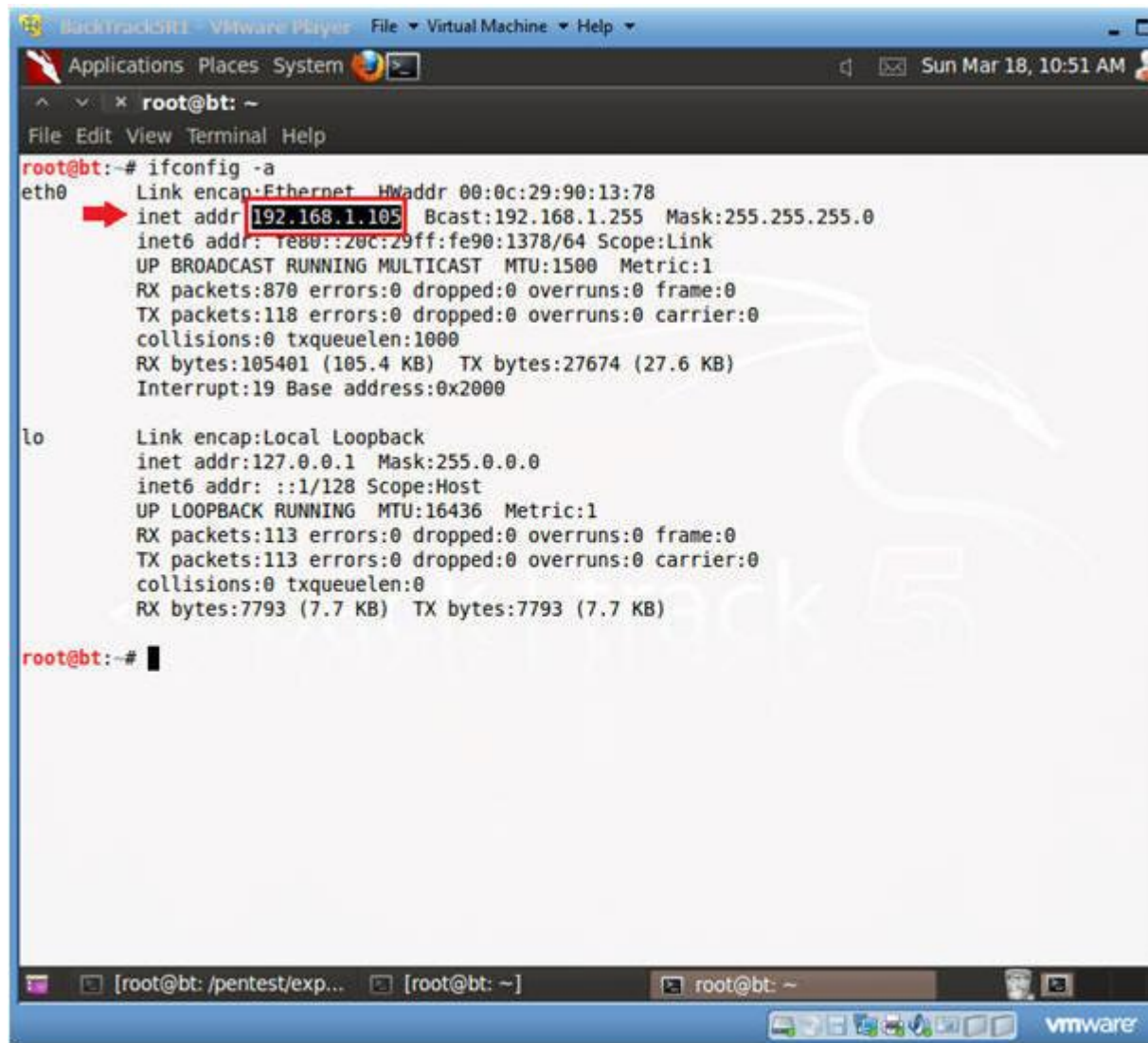
Section 6: Open Console Terminal and Retrieve IP Address

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



2. Get IP Address

- **Instructions:**
 - 1. `ifconfig -a`
- **Notes:**
 - 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: Start Nikto

1. Start nikto

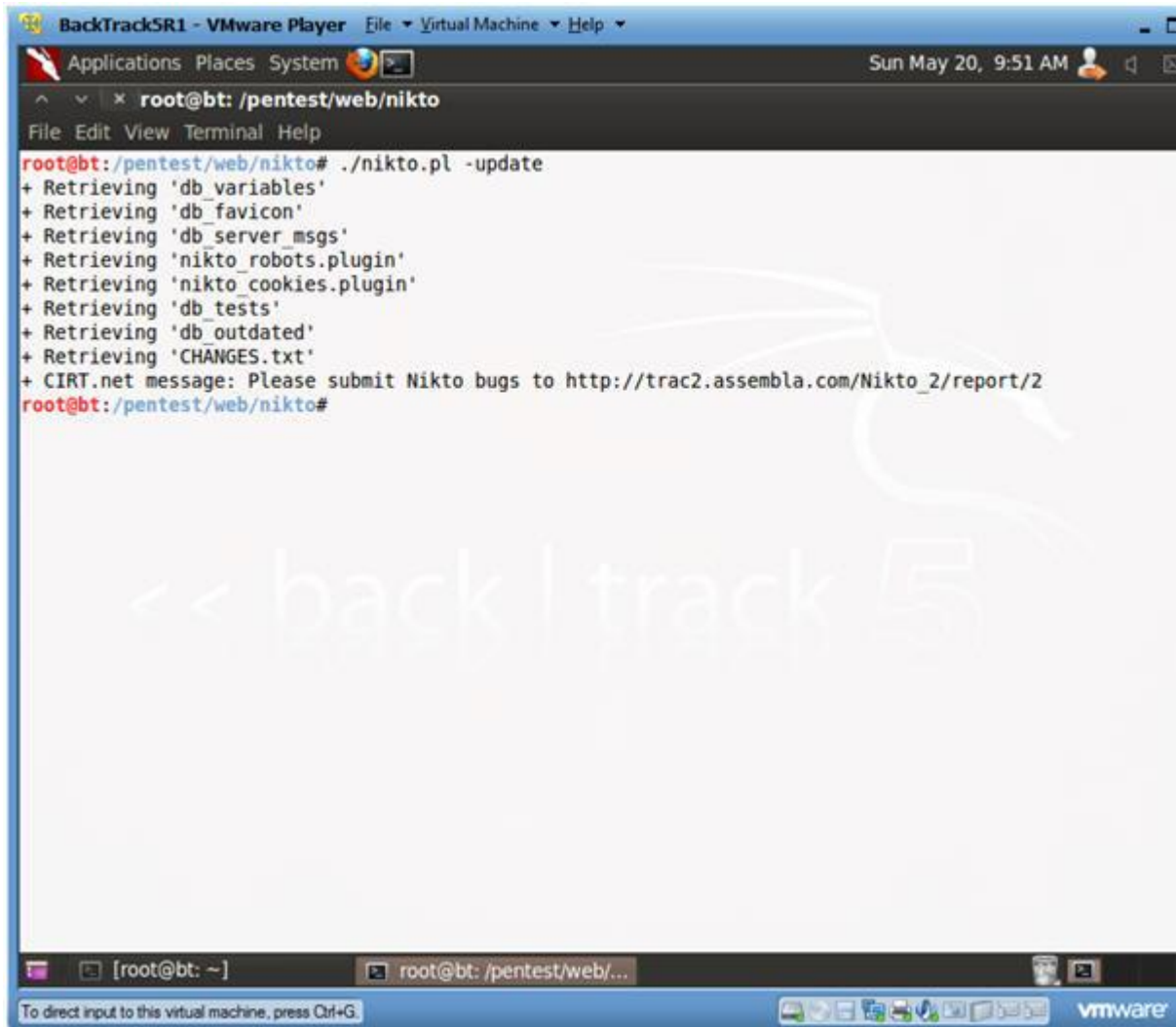
o **Instructions:**

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



○

2. Update nikto
 - **Instructions:**
 1. `./nikto.pl -update`

A screenshot of a VMware Player window titled 'BackTrackSR1 - VMware Player'. The window shows a terminal session with the user 'root' at the prompt 'root@bt: /pentest/web/nikto'. The user has executed the command './nikto.pl -update'. The terminal output shows a list of items being retrieved: 'db_variables', 'db_favicon', 'db_server_msgs', 'nikto_robots.plugin', 'nikto_cookies.plugin', 'db_tests', 'db_outdated', and 'CHANGES.txt'. A message from CIRT.net is also displayed, asking to submit bugs to a specific URL. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. The VMware window has a menu bar with 'File', 'Virtual Machine', and 'Help'. The system clock shows 'Sun May 20, 9:51 AM'. The VMware taskbar at the bottom shows the VMware logo and a status bar with the text 'To direct input to this virtual machine, press Ctrl+G.'

```
BackTrackSR1 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/web/nikto
File Edit View Terminal Help
root@bt:/pentest/web/nikto# ./nikto.pl -update
+ Retrieving 'db_variables'
+ Retrieving 'db_favicon'
+ Retrieving 'db_server_msgs'
+ Retrieving 'nikto_robots.plugin'
+ Retrieving 'nikto_cookies.plugin'
+ Retrieving 'db_tests'
+ Retrieving 'db_outdated'
+ Retrieving 'CHANGES.txt'
+ CIRT.net message: Please submit Nikto bugs to http://trac2.assembla.com/Nikto_2/report/2
root@bt:/pentest/web/nikto#
```

3. Show Options

- **Instructions:**

1. ./nikto.pl -help

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/web/nikto
File Edit View Terminal Help
root@bt:/pentest/web/nikto# ./nikto.pl -help
Unknown option: help

-config+          Use this config file
-Cgidir+          scan these CGI dirs: 'none', 'all', or values like "/cgi/ /cgi-a/"
-dbcheck+         check database and other key files for syntax errors
-Display+         Turn on/off display outputs
-evasion+         ids evasion technique
-Format+          save file (-o) format
-host+            target host
-Help             Extended help information
-id+              Host authentication to use, format is id:pass or id:pass:realm
-list-plugins     List all available plugins
-mutate+         Guess additional file names
-mutate-options+ Provide extra information for mutations
-output+         Write output to this file
-nocache         Disables the URI cache
-nossl           Disables using SSL
-no404           Disables 404 checks
-port+           Port to use (default 80)
-Plugins+        List of plugins to run (default: ALL)
-root+           Prepend root value to all requests, format is /directory
-ssl             Force ssl mode on port
-Single          Single request mode
-timeout+        Timeout (default 2 seconds)
-Tuning+         Scan tuning
-update          Update databases and plugins from CIRT.net
-vhost+          Virtual host (for Host header)
-Version         Print plugin and database versions
+ requires a value

Note: This is the short help output. Use -H for full help.
```

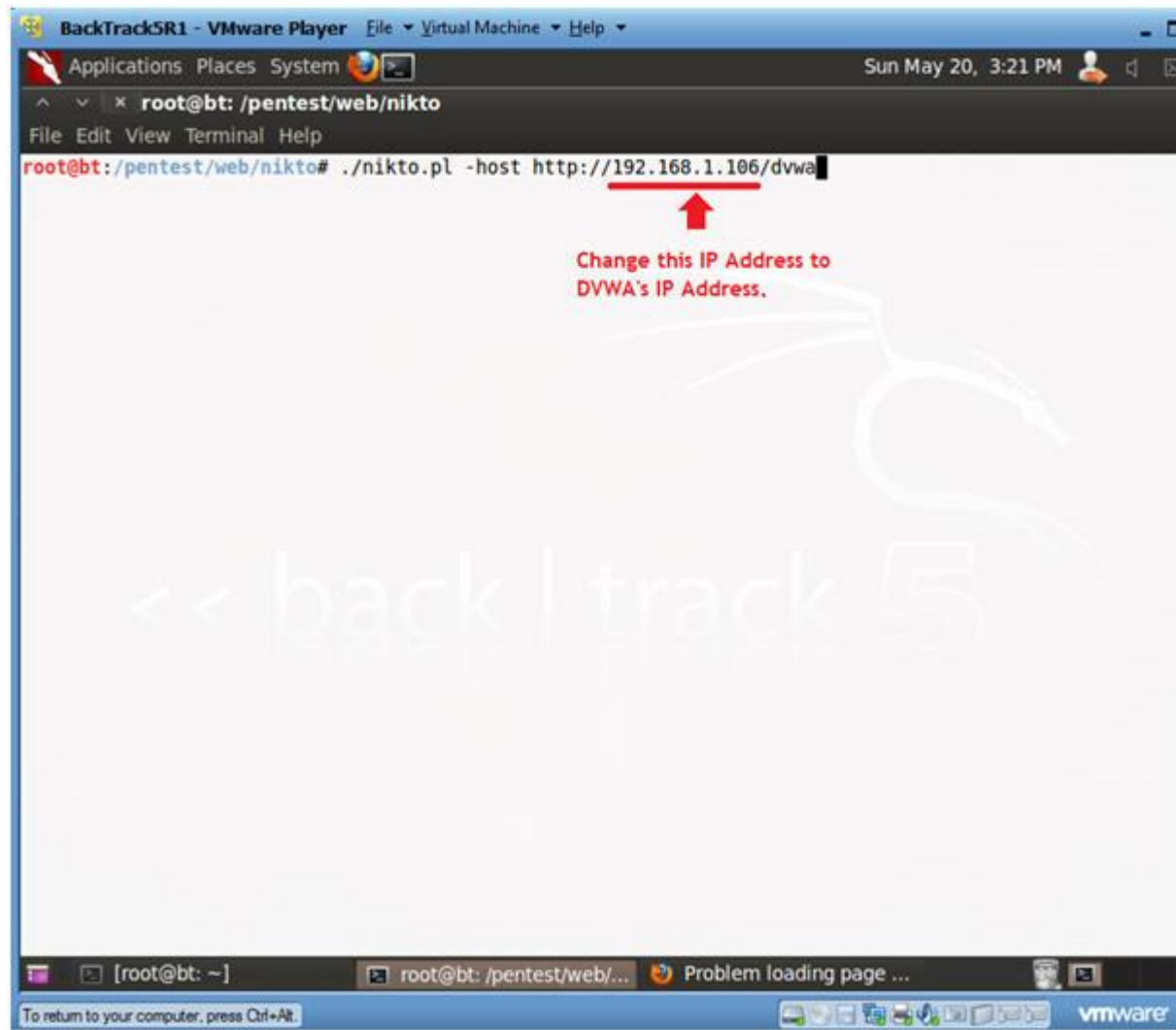
4. Scan with nikto

- o **Instructions:**

- 1. `./nikto.pl -host http://192.168.1.106/dvwa`

- o **Notes:**

- Replace 192.168.1.106 with the IP Address obtained in (Step 3)



5. View nikto Scan Results

- **Notes:**

0. Right away Nikto is not only able to identify the Apache version, but also it is outdated.
1. In addition, Nikto identifies the operating system as Fedora and the version of PHP.
2. Nikto, also displays various vulnerabilities whose explanations are found in the [Open Source Vulnerabilities Database](#).


```
BackTrack5R1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/web/nikto
File Edit View Terminal Help
root@bt:/pentest/web/nikto# ./nikto.pl -host http://192.168.1.106/dvwa
- Nikto v2.1.4

-----
+ Target IP:          192.168.1.106
+ Target Hostname:    192.168.1.106
+ Target Port:        80
+ Start Time:         2012-05-21 15:23:40
-----
+ Server: Apache/2.2.17 (Fedora)
+ Retrieved x-powered-by header: PHP/5.3.8
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 1 entry which should be manually viewed.
+ Apache/2.2.17 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ ETag header found on server, inode: 135299, size: 26, mtime: 0x481e4a83ded80
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /index.php?PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /config/: Directory indexing found.
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ /login.php: Admin login page/section found.
+ 6456 items checked: 1 error(s) and 14 item(s) reported on remote host
+ End Time:          2012-05-21 15:24:43 (63 seconds)
-----
+ 1 host(s) tested
root@bt:/pentest/web/nikto#
```

Annotations in the image:

- Red dot and line pointing to "Apache/2.2.17 (Fedora)": **Web Server**
- Red dot and line pointing to "PHP/5.3.8": **Operating System**
- Red dot and line pointing to "OSVDB-877": **Open Source Vulnerability Database**

Section 8: OSVDB-877: Use Telnet to Grab Webserver and Operating System Banner

1. Use Telnet to Grab Banner
 - **Instructions:**
 1. telnet 192.168.1.106 80
 - Replace 192.168.1.106 with DVWA's IP Address found in Step 3, Step 3).
 - Where 80 is the default Webserver Report.
 2. GET index.html
 - **Notes:**
 - Although the webserver responds back with a "400 Bad Request" error, it does provide the Webserver and Operating System Banner.
 - [OSVDB-877](#)
 - RFC compliant web servers support the TRACE HTTP method, which is a security flaw that may lead to an unauthorized information disclosure. The TRACE method is used to debug web server connections and allows the client to see what is being received at the other end of the request chain.

BackTrackSR1 - VMware Player File Virtual Machine Help

Sun May 20, 4:33 PM

root@bt: /pentest/web/nikto

File Edit View Terminal Help

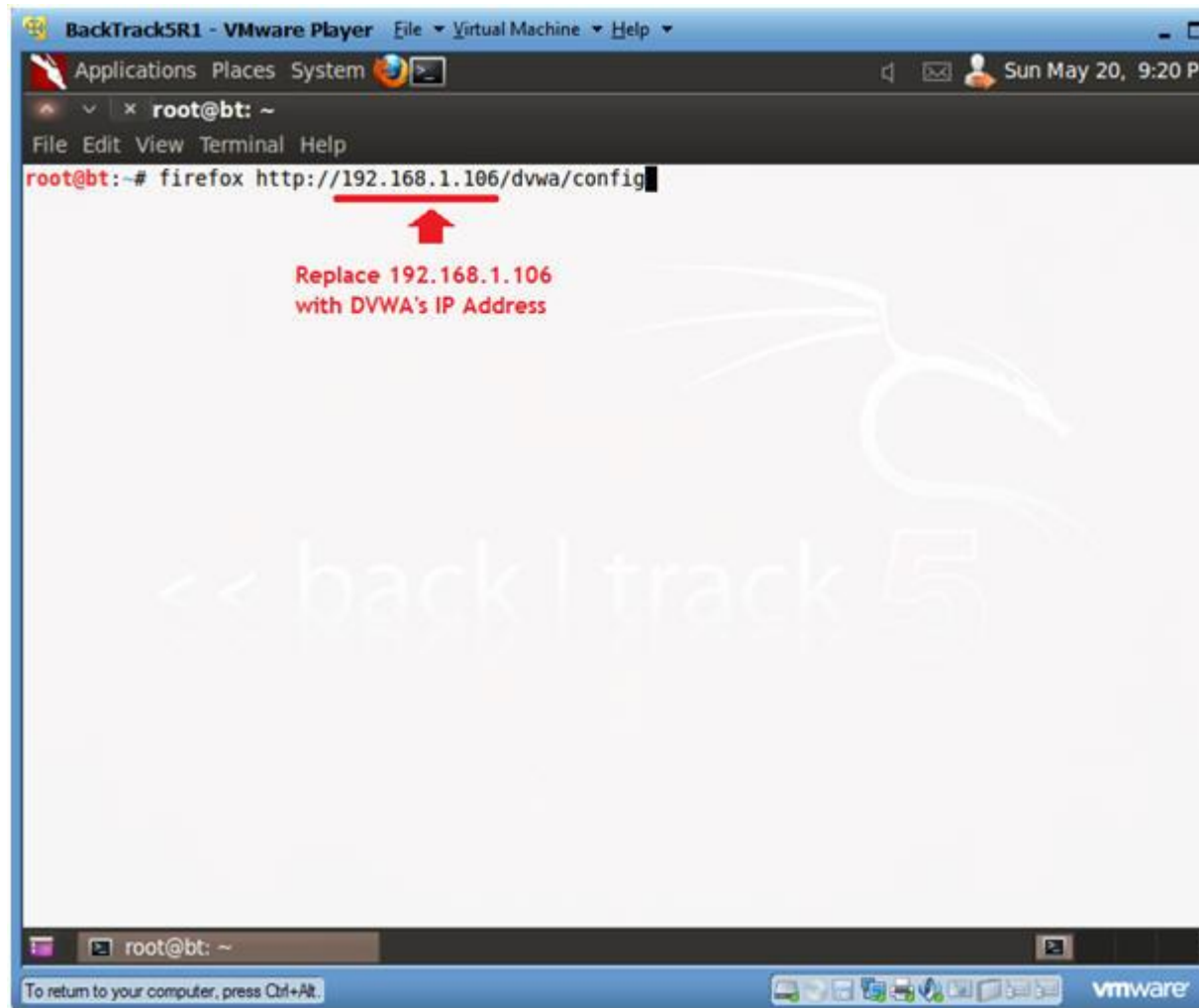
```
root@bt:/pentest/web/nikto# telnet 192.168.1.106 80
Trying 192.168.1.106...
Connected to 192.168.1.106.
Escape character is '^]'.
GET index.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.17 (Fedora) Server at ::1 Port 80</address>
</body></html>
Connection closed by foreign host.
root@bt:/pentest/web/nikto#
```

Annotations:

- 1: DVWA IP Address
- 2: Webserver Port, Default is 80
- Webserver / Operating System Banner

Section 9: OSVDB-3268: /dvwa/config/: Directory indexing found:

1. Browse /dvwa/config with Firefox
 - o **Instructions:**
 1. firefox http://192.168.1.106/dvwa/config
 - o **Notes:**
 - Replace 192.168.1.106 with the IP Address obtained in (Sec Step 3)



2. Investigate /dvwa/config

- **Instructions:**

- 0. Click on config.inc.php

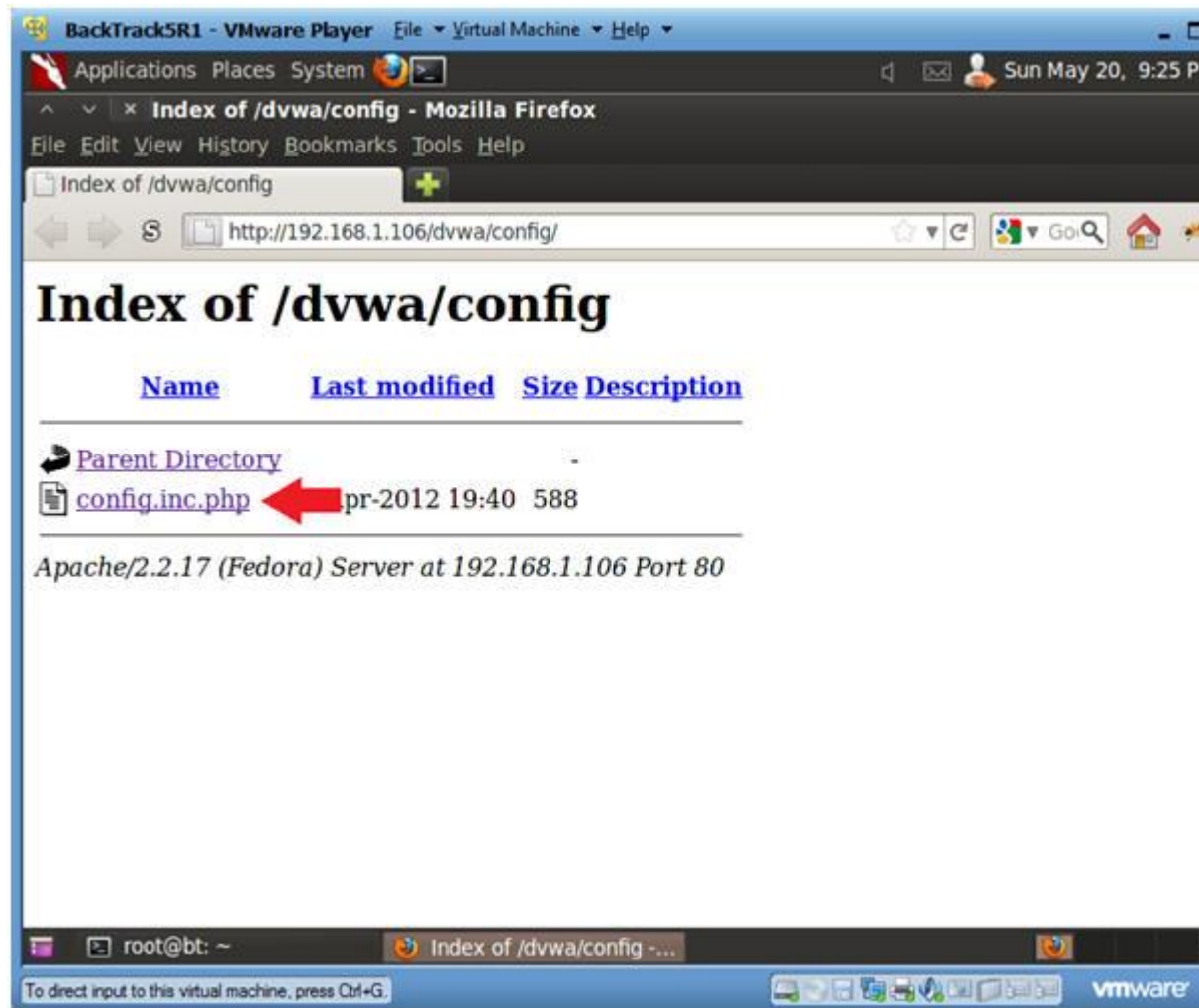
- **Notes:**

- 0. When a web directory does not contain index.html, index.php then all files in that directory will be displayed.

- 1. Note, you should never allow a configuration directory to be available to the public.

- 2. [OSVDB-3268](#)

- Directory indexing has been found to be enabled on the web server. There is no known vulnerability or exploit associated with this, but it can reveal sensitive or "hidden" files or directories to remote users in more focused attacks.

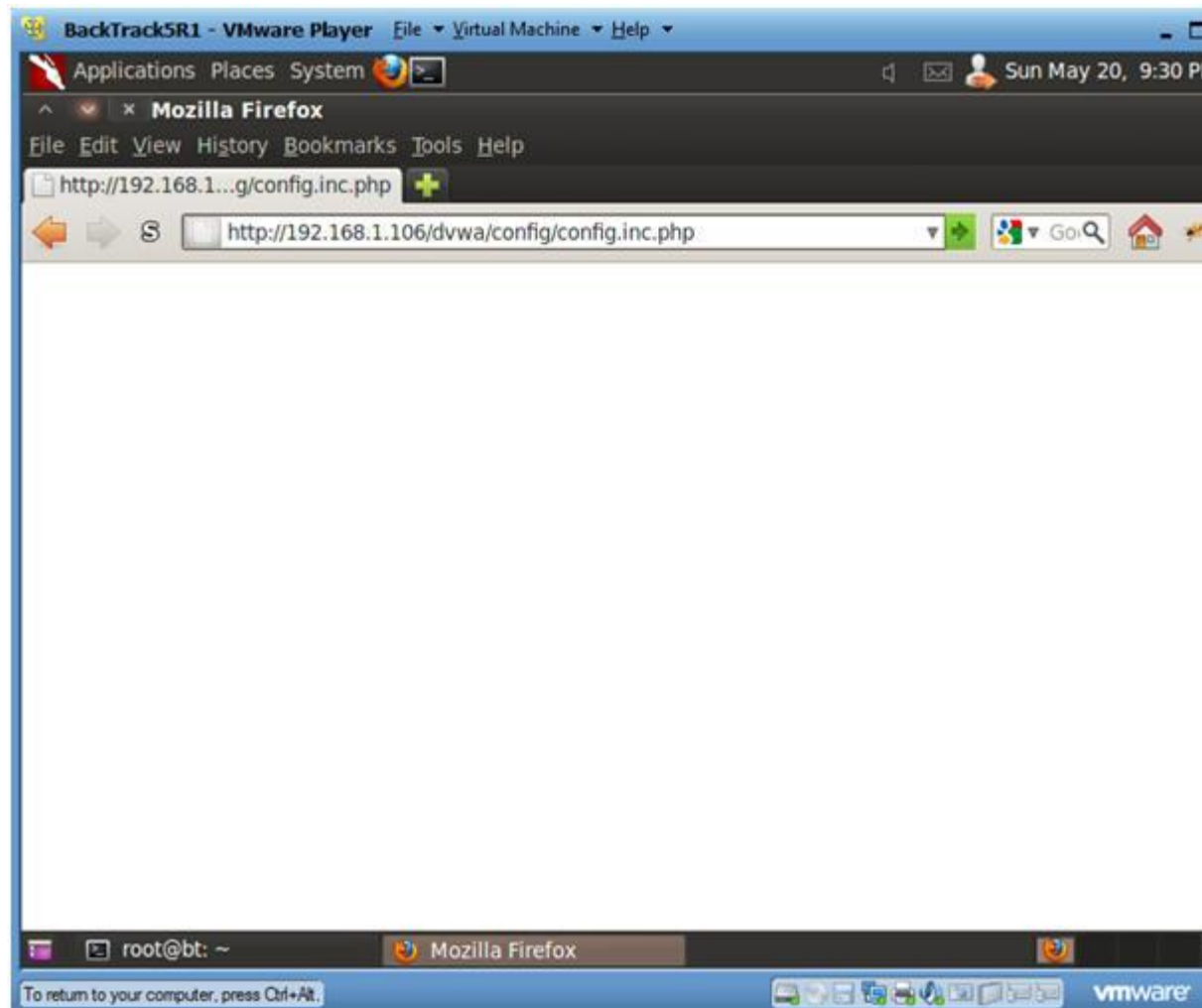


3. Nothing Happened?

- **Note:**

- 0. The config.inc.php produced nothing.

- 1. Typically php, perl, asp, etc script will execute as designed. If nothing happens, the script will not produce output.



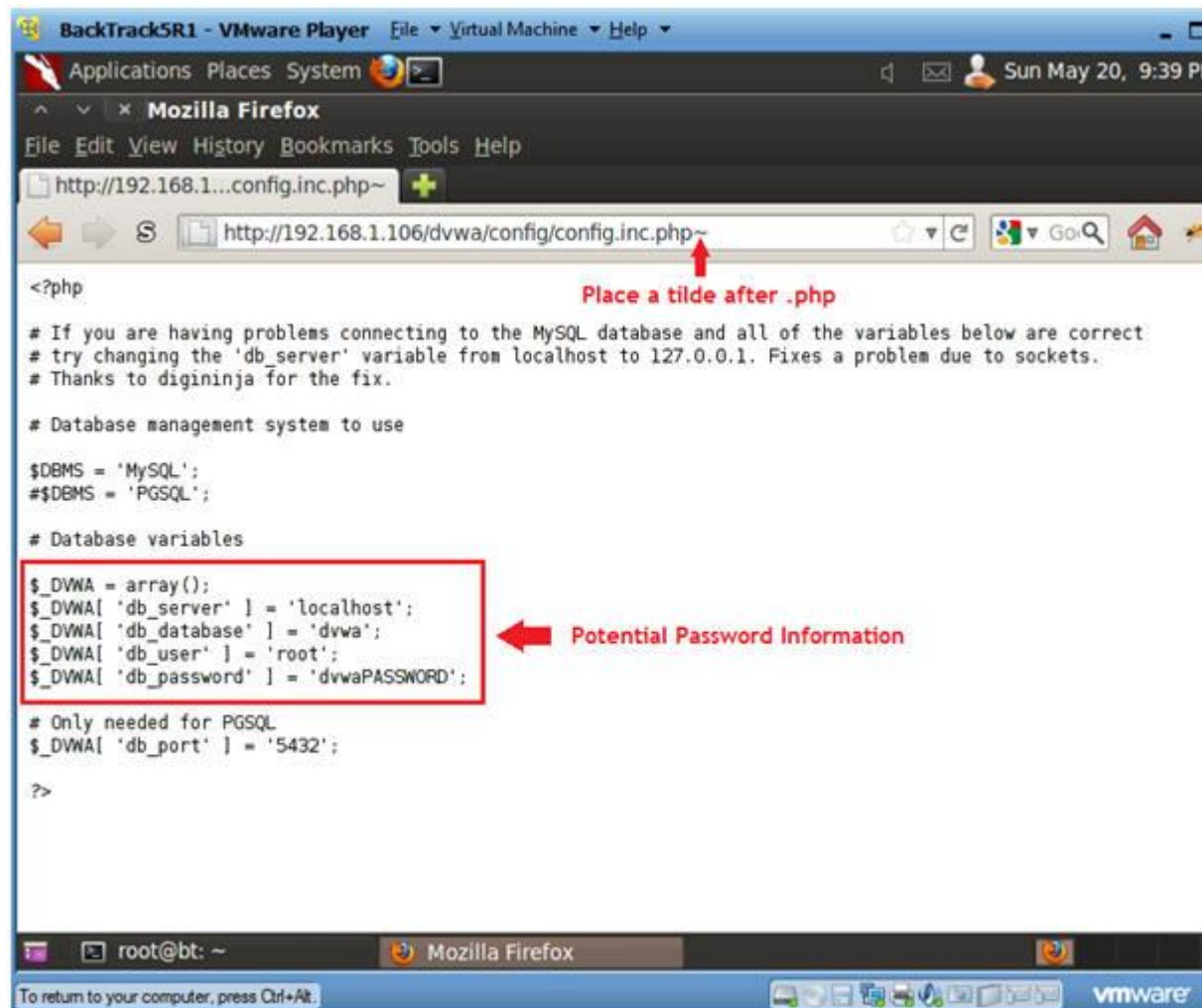
4. Let's test for a tilde

- **Instructions:**

- 0. `http://192.168.1.106/dvwa/config/config.inc.php~`
 - Place a tilde(~) after .php

- **Notes:**

- 0. Some applications create a backup file of the file you are editing with a "~" following it.
- 1. The contents of the php file are displayed to the screen, but the Web Server does not recognize a file as a php script because of the "~".



Section 10: Proof of Lab

1. Proof of Lab

o **Proof of Lab Instructions:**

1. On BackTrack, pull up a terminal window.
2. `cd /pentest/web/nikto`
3. `./nikto.pl -host http://192.168.1.106/dvwa 2>&1 > /var/tmp/`
 - Replace 192.168.1.106 with DVWA's IP Address obtained (Section 3, Step 3).
4. `ls -l /var/tmp/nikto.txt`
5. `date`
6. `echo "Your Name"`
 - Replace the string "Your Name" with your actual name.
 - e.g., `echo "John Gray"`
7. Do a <PrtScn>
8. Paste into a word document
9. Upload to Moodle

BackTrack5R1 - VMware Player File Virtual Machine Help

Applications Places System

root@bt: /pentest/web/nikto

File Edit View Terminal Help

```
root@bt:~# cd /pentest/web/nikto/
root@bt:/pentest/web/nikto#
root@bt:/pentest/web/nikto# ./nikto.pl -host http://192.168.1.106/dvwa 2>&1 > /var/tmp/nikto.txt
root@bt:/pentest/web/nikto#
root@bt:/pentest/web/nikto# ls -l /var/tmp/nikto.txt
-rw-r--r-- 1 root root 1681 2012-05-20 22:36 /var/tmp/nikto.txt
root@bt:/pentest/web/nikto#
root@bt:/pentest/web/nikto# date
Sun May 20 22:36:32 CDT 2012
root@bt:/pentest/web/nikto#
root@bt:/pentest/web/nikto# echo "Your Name"
Your Name
root@bt:/pentest/web/nikto#
```

<< back | track 5

root@bt: ~ Index of /dvwa/docs - ... root@bt: /pentest/web/nikto root@bt: /pentest/web/nikto

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

vmware