NETWORK SECURITY LAB SERIES

Lab 5: Configuring Access Control Lists on Linux Based Firewalls

Document Version: 2015-09-28

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Introduction

This lab is a part of a series of lab exercises intended to support courseware for Network Security training. This lab includes the following tasks:

1. Setting up the Network
2. Enabling Services and Configuring Firewall Rules
3. Testing the Firewall

Key terms for this lab:

Iptables – A command line tool that allows you to create Firewall rules.

route add – This command allows you to add a default gateway on a Linux system.

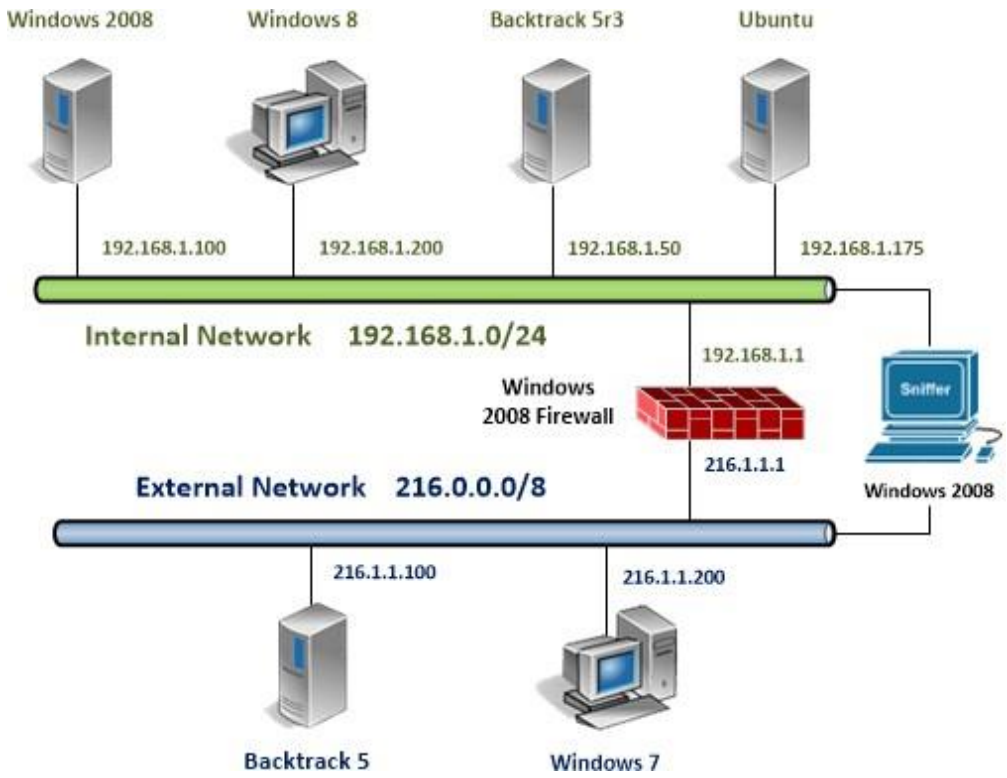
netstat – This command will allow you to view active TCP and UDP connections.

NAT – Network Address Translation will allow internal hosts to reach the external network through a single IP address. Most firewalls can be configured to perform NAT.

nmap – Nmap can be used in Linux, Mac, or Microsoft Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Nmap was used in the movie, *The Matrix.*

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Lab Topology



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
BackTrack 5 R3 Internal Machine	192.168.1.50	root	toor
Windows 7 External Machine	216.1.1.200	student	password
Windows 2008 Sniffer	n/a	administrator	sniffer

For all the tasks in this lab, you will be asked to open and return to various machines and applications within each machine. For some steps, this can get confusing.

To minimize confusion and the need to reopen machines and applications, it is suggested that you minimize, rather than close a machine before opening another.

At the end of the lab, remember to close all open windows and close the PC viewers.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

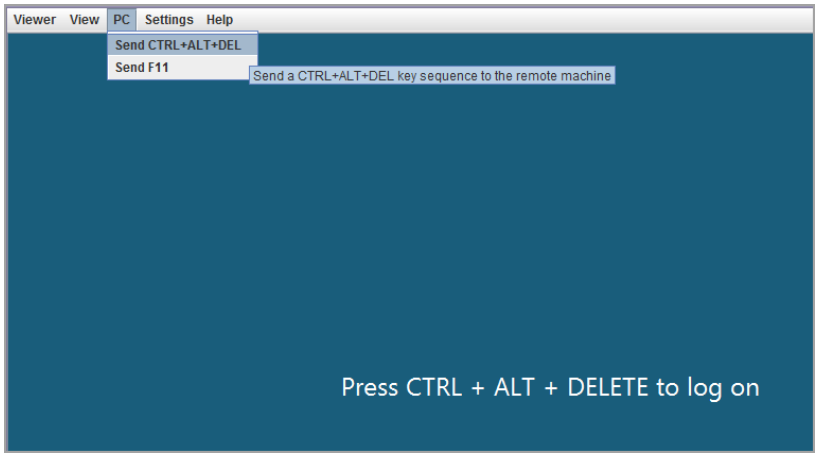
1 Setting up the Sniffer

In this section, we will reconfigure the BackTrack 5r3 Internal Machine to communicate with the Windows 2008 Sniffer Machine, running Linux. The Sniffer will be reconfigured into a Linux based firewall. In order to set up this network, we will set the IP addresses for both of the sniffer machine's (Linux OS) interfaces as well as the BackTrack 5r3 Internal Machine.

1.1 Logging on to the Sniffer

The Linux distribution BackTrack is installed on the sniffer machine. BackTrack is a distribution used by security professionals for pentration testing and forensics.

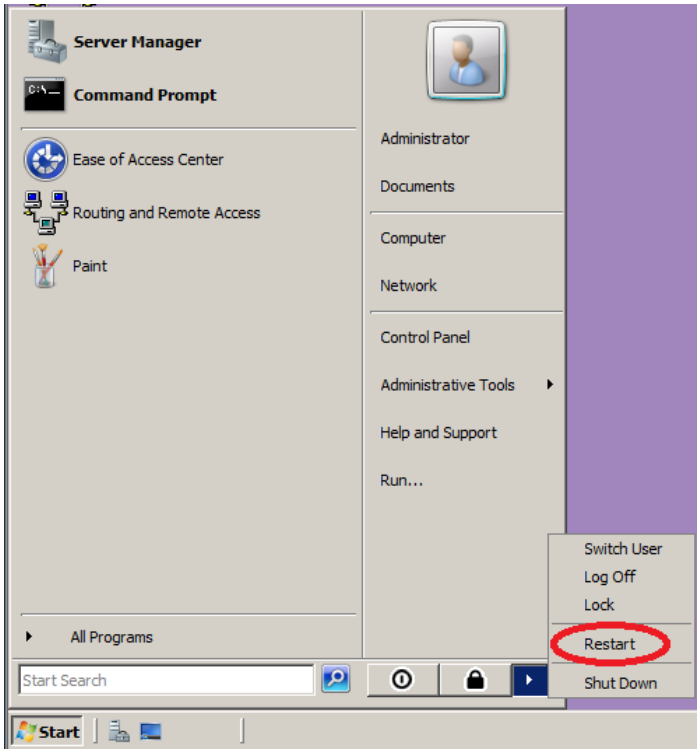
1. Log into the **Windows 2008 Server Sniffer** by clicking on the **Windows 2008 Sniffer** icon on the topology. Click **PC** in the upper-left and **Send Ctrl+Alt+Del** in order to log on to the Windows 2008 server.



2. Enter **sniffer** for the Administrator password to the Windows 2008 Server.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

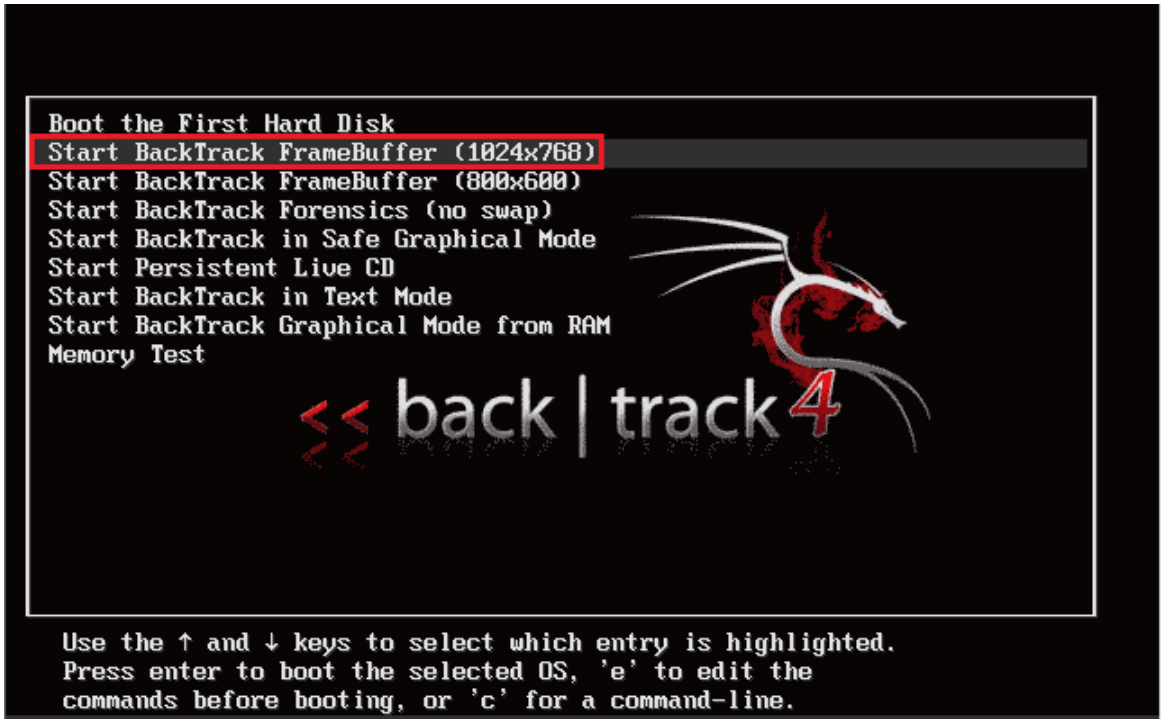
3. Click on the Start button. Click the arrow to the far-right and select **Restart**.



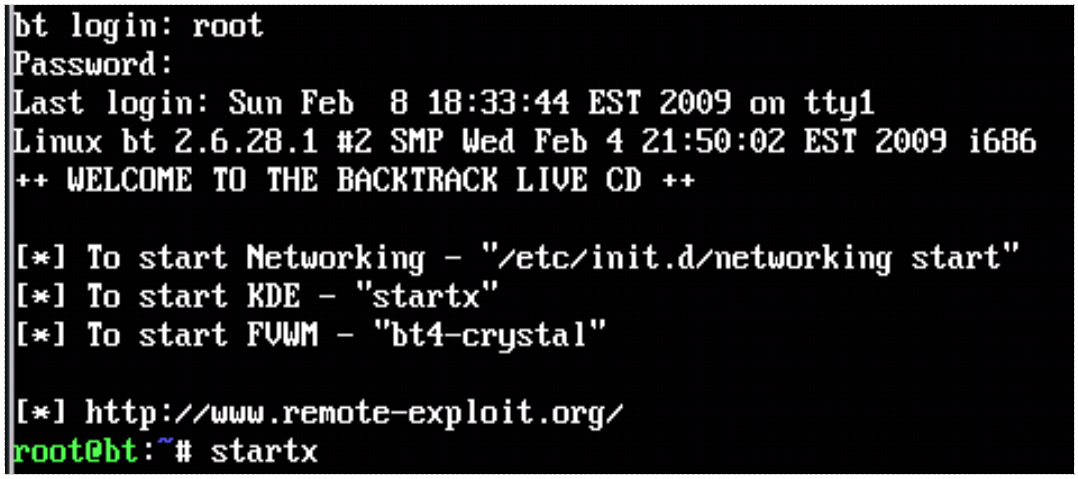
4. Select the second Option, **Hardware: Maintenance (Planned),** in the list from the drop-down box and click OK.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

5. Select the 2nd choice in the menu and press Enter to boot into Linux.

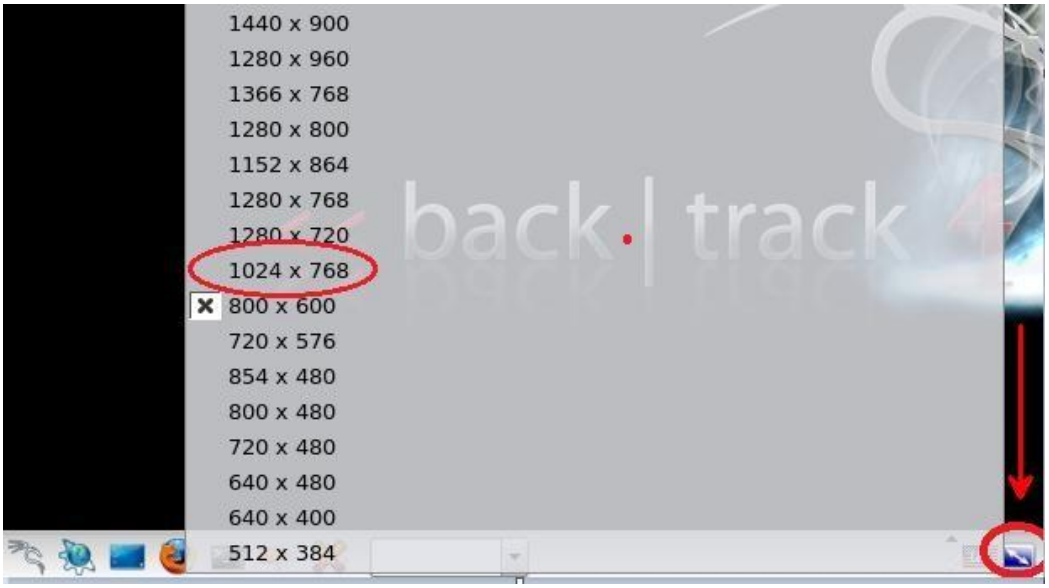


6. Type the following command to initialize the GUI (Graphical User Interface):
root@bt:~#**startx**

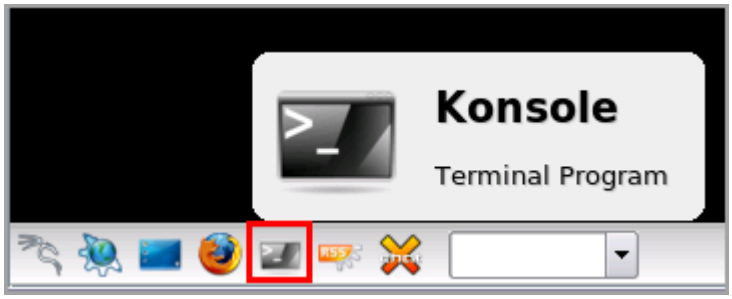


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

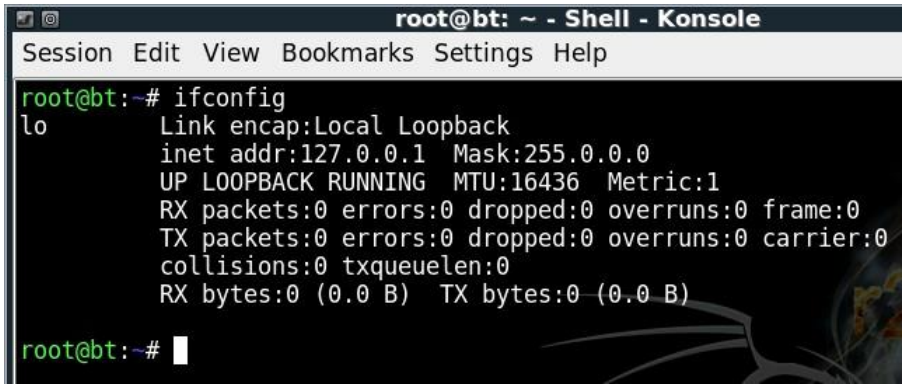
7. Click the small blue double arrow in the bottom of the screen to adjust the resolution to 1024 x 768. Click accept configuration if the desktop renders correctly.



8. Open a terminal on the Linux Sniffer system by clicking on the image to the right of Firefox in the task bar, in the bottom of the screen.

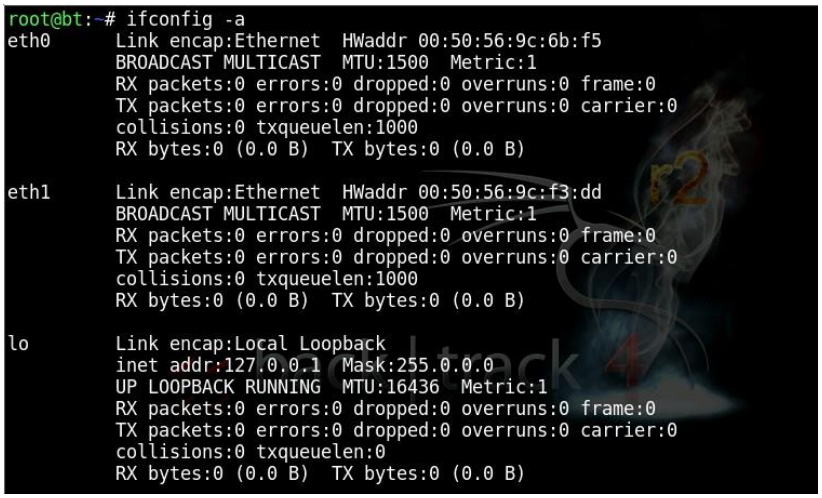


9. Type the following command to view active interfaces.
root@bt:~**#ifconfig**
Only the loopback address, 127.0.0.1, is displayed.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

10. Type the following command to view all available interfaces on the system:
root@bt:~**#ifconfig -a**



11. Type the following command to set the internal IP address of the Sniffer:
root@bt:~# **ifconfig eth0 172.16.1.1 netmask 255.255.255.0 up**

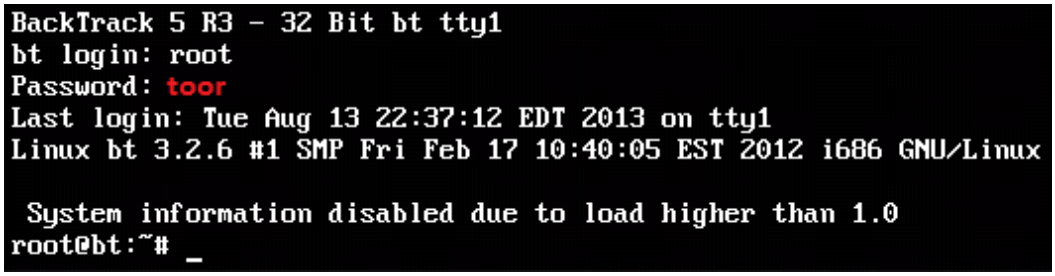
12. Type the following command to set the IP address of the Sniffer Server:
root@bt:~# **ifconfig eth1 216.80.80.80 netmask 255.0.0.0 up**

In order to configure and set up the services required, perform the following steps on the **BackTrack 5 R3 Internal Machine.**

13. Click the **Backtrack 5r3** icon to open the **BackTrack 5 R3 Internal Machine**. Type **root** for the login and **toor** *(root spelled backwards)* for the password.

Click in the window and press Enter if BackTrack is displaying a black screen.

The password of toor will not be displayed when you type it, for security purposes.

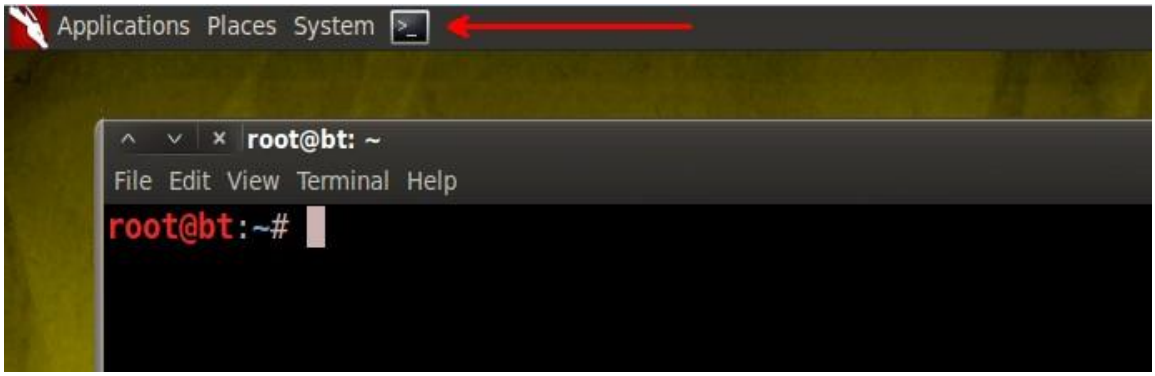


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

14. Type the following command to start the Graphical User Interface (GUI).
    root@bt:~# **startx**

```
root@bt:~# startx_
```

15. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen in BackTrack version 5 R3.



16. To set a static address on the BackTrack 5 R3 Internal Machine, type the following command:
    root@bt:~# **ifconfig eth2 172.16.1.50 netmask 255.255.255.0 up**

```
root@bt:~# ifconfig eth2 172.16.1.50 netmask 255.255.255.0 up
```

17. Type the following command to set the Gateway of the BackTrack 5 R3 Internal Machine:
    root@bt:~# **route add default gw 172.16.1.1**

```
root@bt:~# route add default gw 172.16.1.1
```

18. Type the following command to view the gateway:
    root@bt:~# **netstat -r**

```
root@bt:~# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         172.16.1.1      0.0.0.0         UG        0 0          0 eth2
172.16.1.0      *               255.255.255.0   U         0 0          0 eth2
```


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

19. Type the following command to ping the gateway four times:
root@bt:~# ping 172.16.1.1 –c 4

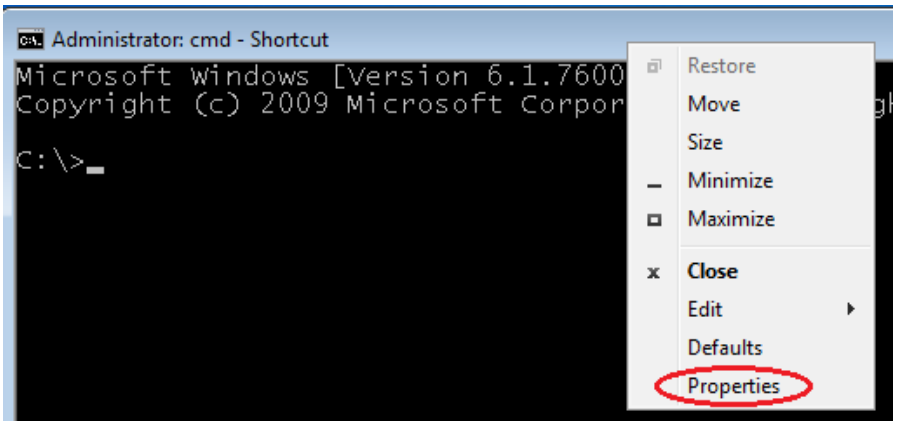
```
root@bt:~# ping 172.16.1.1 -c 4
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=18.5 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.793 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.513 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=0.674 ms

--- 172.16.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.513/5.121/18.504/7.727 ms
```

20. Log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology. If required, enter the username, **student**. Type in the password, **password,** and press **Enter** to log in.

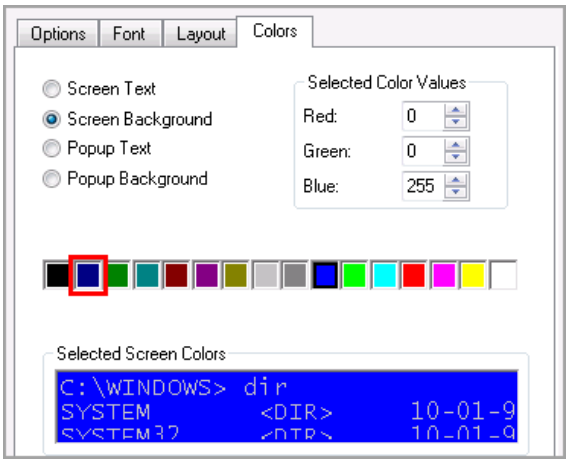
21. Open a command prompt by clicking on **cmd-shortcut** on the desktop.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

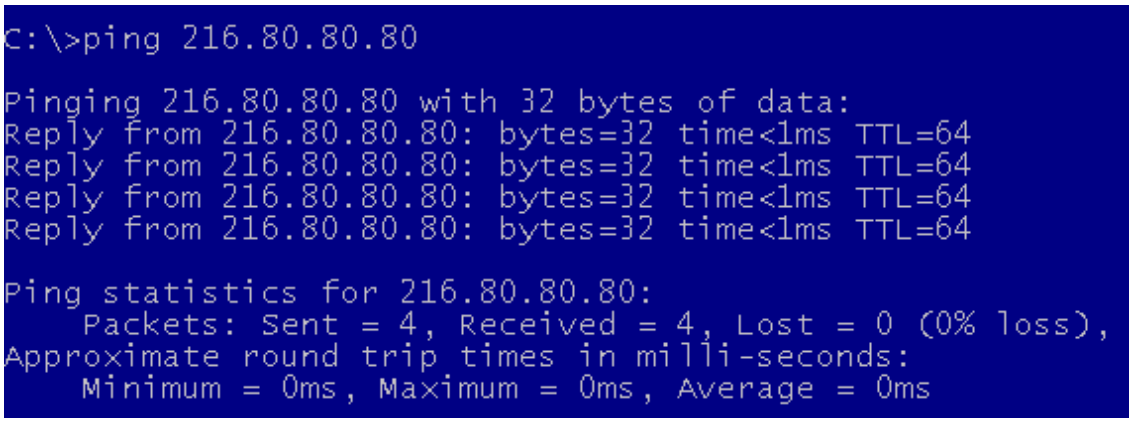
22. Right-click on the blue bar at the top of command prompt window and go to properties.



23. Click the Colors tab. Select Blue (2nd from the left) and click OK.



24. Type the following command to ping the external IP address of the sniffer:
C:\>**ping 216.80.80.80**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

1.2 Conclusion

IP addresses can be configured on the Linux operating system using the ifconfig command. Gateways can be configured by using the route add command. The netstat –r command will allow you to view the IP address of the router on a Linux box. A router itself will typically not have a gateway on the internal interface. The ping command can be used to test for connectivity between all of the IP addresses, as long as ICMP is not blocked.

1.3 Discussion Questions

1. What could prevent the ping command from working?
   Ans : NAT stands for Network address Translation . It's the process to map multiple local private address to public before transferring the information
2. What command will allow you to set a default gateway in Linux?
   Ans: The command will allow the default gateway is Linux "route add default gw [gateway IP address]" for example : route add default gw 172.161.1.3
3. What command will allow you to view all interfaces on a Linux machine?
   Ans: Command to view all interfaces on a Linux machine is "ifconfig -a" or "ip link show".
4. What switch in Linux will limit the number of pings (prevent continuous ping)?
   Ans: The switch in Linux to limit the number of pings is "-c [count]".
   For example 172.16.1.1 -c4.

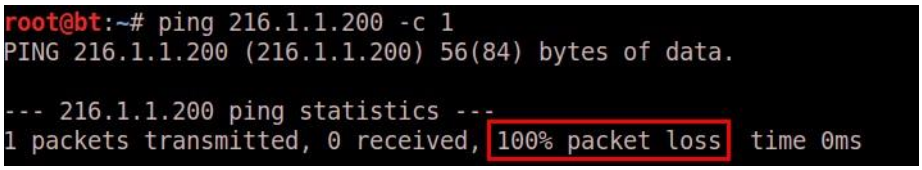
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

2 Enabling Services and Configuring Firewall Rules

Firewall Rules can be configured through the command line on a Cisco router or on a Linux operating system using iptables. We will configure NAT and allow incoming traffic using iptables.

2.1 Enabling NAT and Firewall Rules

1. Traffic is currently not being routed through the Linux sniffer machine. Navigate back to the **BackTrack 5r3 Internal Machine** and verify that this machine cannot ping the Windows 7 External Machine by typing:
   root@bt:~# ping 216.1.1.200 –c 1



We will need to type three commands in the terminal to enable NAT on the sniffer box. Switch to the **Windows 2008 Sniffer** box running the BackTrack Linux (Version 4 R 2).

2. Type the following command to set up NAT on the Linux with iptables:
   root@bt:~# **iptables --table nat --append POSTROUTING --out-interface eth1 –j MASQUERADE**

3. Type the following command to set up NAT on the Linux with iptables:
   root@bt:~# **iptables --append FORWARD --in-interface eth0 -j ACCEPT**

4. Next, type the following to enable IP forwarding on the system:
   root@bt:~# **echo 1 > /proc/sys/net/ipv4/ip_forward**

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

5. Verify that the **BackTrack 5r3 Internal Machine** can now ping the **Windows 7 External Machine** by typing:
   root@bt:~# ping 216.1.1.200 –c 4

```
root@bt:~# ping 216.1.1.200 -c 4
PING 216.1.1.200 (216.1.1.200) 56(84) bytes of data.
64 bytes from 216.1.1.200: icmp_seq=1 ttl=127 time=4.00 ms
64 bytes from 216.1.1.200: icmp_seq=2 ttl=127 time=0.350 ms
64 bytes from 216.1.1.200: icmp_seq=3 ttl=127 time=0.359 ms
64 bytes from 216.1.1.200: icmp_seq=4 ttl=127 time=0.312 ms
```

We will need to type four commands in the terminal to allow incoming traffic that will be redirected from the public IP of 216.80.80.80 to the internal IP of 172.16.1.50.

6. To view the current running services on the **BackTrack 5r3 Internal Machine**, type the following:
   root@bt:~# netstat -tan

```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:7337          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp6       0      0 ::1:7337                :::*                    LISTEN
```

Currently, the BackTrack system is listening on port 21 because VSFTPD has already been configured and installed on this system. Apache and SSHD also need to be running.

The netstat command is pretty much universal, and works across multiple platforms such as Linux, Microsoft Windows, UNIX, and Mac OS X. nmap also works across multiple platforms, but it is a third party utility and needs to be installed.

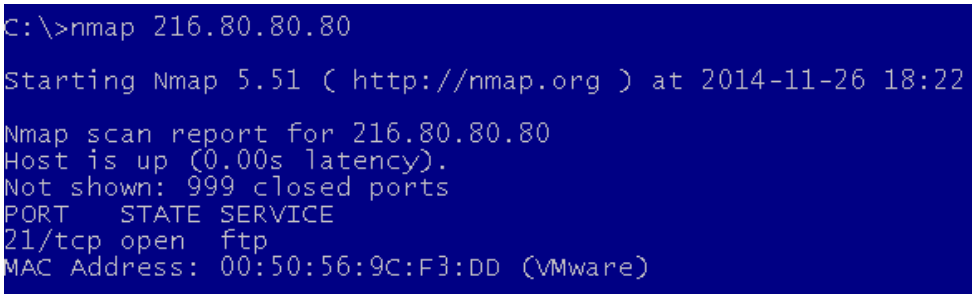
7. To view the current running services on the **BackTrack 5r3 Internal Machine**, type the following command:
   root@bt:~# nmap 127.0.0.1

```
root@bt:~# nmap 127.0.0.1

Starting Nmap 6.01 ( http://nmap.org ) at 2014-05-26 13:28 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

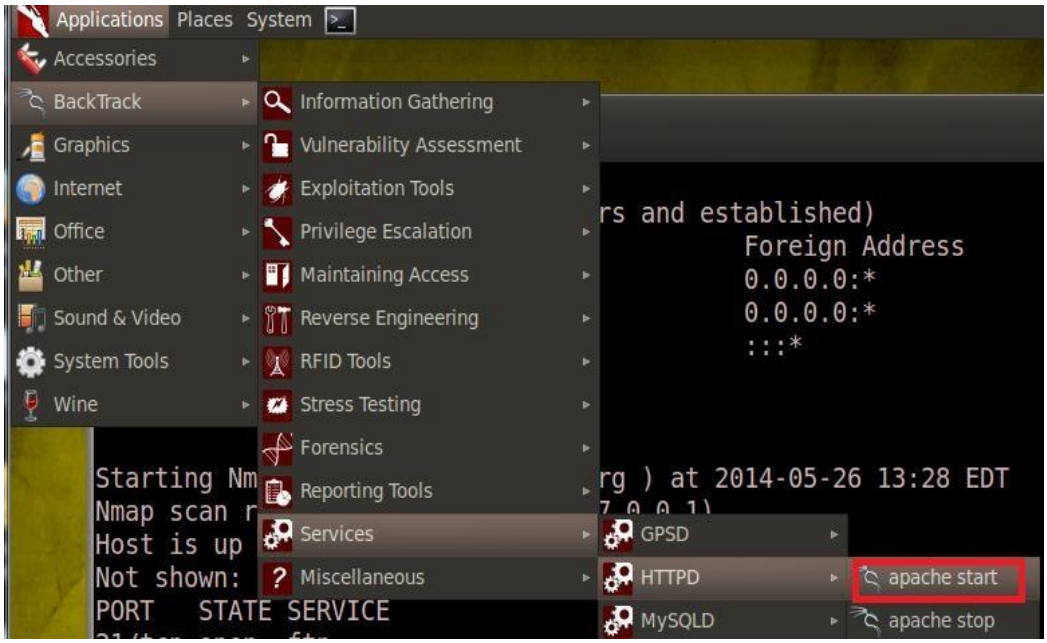

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

8. Type the following command on the **Windows 2008 Sniffer** to redirect incoming requests from the Internet to the Internal BackTrack machine running FTP Server:
   root@bt:~**# iptables -t nat -A PREROUTING -p tcp -d 216.80.80.80 --dport 21 -j DNAT --to-destination 172.16.1.50:21**

9. From the **Windows 7 External Machine**, perform an nmap scan of the Linux public IP address.
   C:\>**nmap 216.80.80.80**



10. Navigate back to the **BackTrack 5r3 Internal Machine**. Start Apache by selecting **BackTrack > Services > HTTPD > apache start.** A window will appear and then close.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

11. To view the current running services, type the following command:
    root@bt:~# netstat -tan

```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:7337          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp6       0      0 ::1:7337                :::*                    LISTEN
```

After starting Apache, the BackTrack system is now also listening on port 80.

12. Type the following command on the **Windows 2008 Sniffer** to redirect incoming requests from the Internet to the internal BackTrack machine running HTTP Server:
    root@bt:~**# iptables -t nat -A PREROUTING -p tcp -d 216.80.80.80 --dport 80 -j DNAT --to-destination 172.16.1.50:80**

```
root@bt:~# iptables -t nat -A PREROUTING -p tcp -d 216.80.80.80 --dport 80 -j DNAT --to-destination 172.16.1.50:80
```

13. From the **Windows 7 External Machine**, perform another nmap scan of the Linux Public IP address.
    C:\>**nmap 216.80.80.80**

```
C:\>nmap 216.80.80.80

Starting Nmap 5.51 ( http://nmap.org ) at 2014-11-26

Nmap scan report for 216.80.80.80
Host is up (0.00s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:50:56:9C:F3:DD (VMware)
```

When an Internet IP address is scanned, the MAC address will not be displayed. The address appears here because this is a simulated environment, not the real Internet. Before starting ssh, the ssh keys must be generated on the Internal BackTrack system.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

14. Type the following command to generate the keys for SSH on the **BackTrack 5r3 Internal Machine:**
root@bt:~#sshd-generate

```
root@bt:~# sshd-generate
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
71:49:a3:79:9a:0a:a5:88:8a:e9:e6:04:34:9f:ae:88 root@bt
The key's randomart image is:
+--[RSA1 2048]----+
|          o      |
|         + o     |
| o     . + +     |
|..o..o   *       |
|o .oo   S        |
|+..   . .        |
|+. .   .         |
|=..              |
|E+               |
+-----------------+
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
```

15. To start SSH, **select Applications > BackTrack > Services > SSHD > sshd start.** A window will appear and then close.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

16. To view the current running services, type the following command:
    root@bt:~# netstat -tan

```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:7337          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 ::1:7337                :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

After starting SSHD, the BackTrack system is now also listening on port 22.

17. To view the current running services, type the following command:
    root@bt:~# nmap 127.0.0.1

```
root@bt:~# nmap 127.0.0.1

Starting Nmap 6.01 ( http://nmap.org ) at 2014-05-26 13:55 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

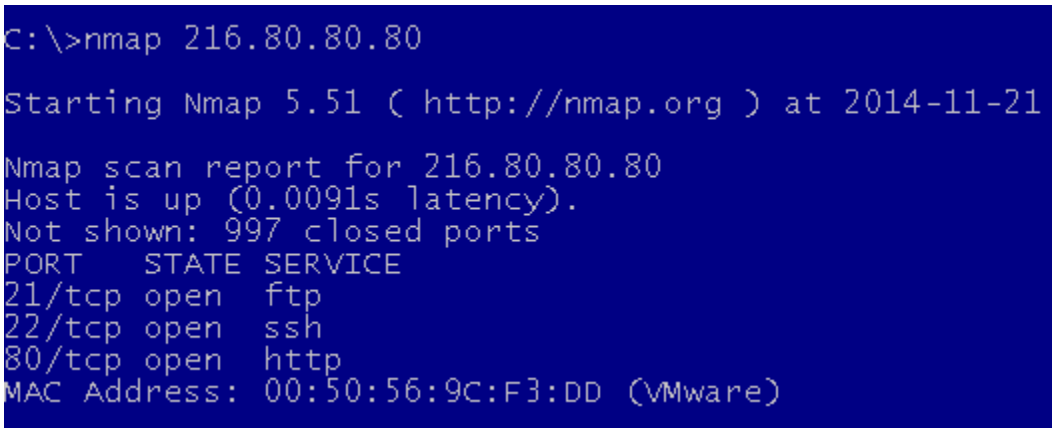

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Next, we will need to remove the hidden file in root's home directory, which will automatically set the IP address to 192.168.1.50 when the root account logs in.

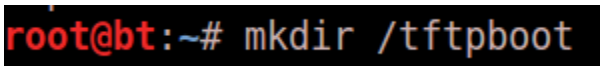
18. Type the following on the **BackTrack 5r3 Internal Machine** to remove the .bash_profile file.
    root@bt:~# rm –rf /root/.bash_profile

19. Return to the **Windows 2008 Sniffer** and type the following command to redirect incoming requests from the Internet to the Backtrack 5r3 Internal machine running SSH:
    root@bt:~# **iptables -t nat -A PREROUTING -p tcp -d 216.80.80.80 –dport 22 -j DNAT --to-destination 172.16.1.50:22**

20. From the **Windows 7 External Machine**, perform an nmap scan of the Linux public IP address.
    C:\>**nmap 216.80.80.80**



21. On the **BackTrack 5r3 Internal Machine**, make a directory called tftpboot by typing the following command:
    root@bt:~# mkdir /tftpboot



22. Start the tftp server on the BackTrack 5r3 Internal Machine by typing the following command:
    root@bt:~# atftpd --daemon /tftpboot

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

23. Type the following command to verify that TFTP is listening on UDP port 69:
    root@bt:~# netstat -uan

```
root@bt:~# netstat -uan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:69              0.0.0.0:*
udp6       0      0 ::1:38973               ::1:38973               ESTABLISHED
```

24. Type the following command to verify that TFTP is listening on UDP port 69:
    root@bt:~# nmap –sU 127.0.0.1 | grep 69

```
root@bt:~# nmap -sU 127.0.0.1 | grep 69
69/udp open|filtered tftp
```

25. Copy fgdump to the web-root of the BackTrack 5r3 Internal Machine by typing the following:
    root@bt:~# cp /pentest/windows-binaries/passwd-attack/fgdump.exe /tftpboot/

```
root@bt:~# cp /pentest/windows-binaries/passwd-attack/fgdump.exe  /tftpboot/
```

26. Verify that the malicious file is present in the tftpboot directory by typing:
    root@bt:~# ls /tftpboot/

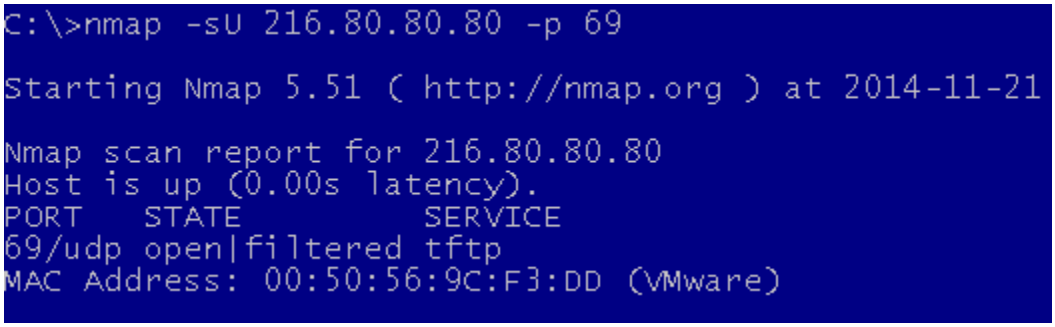
```
root@bt:~# ls  /tftpboot/
fgdump.exe
```

27. Type the following command on the **Windows 2008 Sniffer** to redirect incoming requests from the Internet to the internal BackTrack machine running TFTP Server:
    root@bt:~# **iptables -t nat -A PREROUTING -p udp -d 216.80.80.80 --dport 69 -j DNAT --to-destination 172.16.1.50:69**

```
root@bt:~# iptables -t nat -A PREROUTING -p udp -d 216.80.80.80 --dport 69 -j DNAT --to-destination 172.16.1.50:69
```


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

28. From the **Windows 7 External Machine**, perform another nmap scan of the Linux public IP address.
    C:\>**nmap –sU 216.80.80.80 –p 69**



2.2 Conclusion

In order for external users on the WAN (Internet) to use services on a machine on the internal network, the firewall must be configured to allow requests to be re-directed to an internal machine. Commands like nmap and netstat can be utilized by the network administrator in order to determine if services are listening and ports are open.

2.3 Discussion Questions

1. What does NAT stand for?
   Ans: NAT stands for Network Address Translation.
2. What command is used to set up NAT rules on a Linux machine?
   Ans: IP table is used to setup NAT rules on Linux machine. The command used to set up NAT rules on a Linux machine is "iptables".
3. Why would an administrator run the Nmap scan on 127.0.0.1?
   Ans: Nmap scan is one scan security vulnerability and security services.
4. What command is used to create SSH keys on a Linux machine?
   Ans: Command used to create SSH keys on a Linux machine is "ssh-keygen".

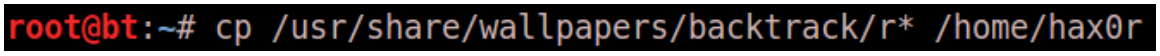
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

3 Using Internal Services from an External Machine

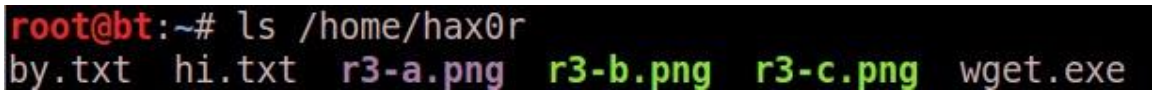
Even though we have used nmap to verify that the correct ports are open, a good network administrator will also test each of the services to verify that they are working correctly. In this scenario, we will test the FTP, SSH, and HTTP services of the firewall.

3.1 Testing the iptables Firewall

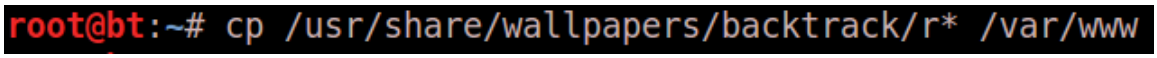
1. On the **BackTrack 5r3 Internal Machine**, type the following to copy picture files to the FTP root:
   root@bt:~# **cp /usr/share/wallpapers/backtrack/r* /home/hax0r**



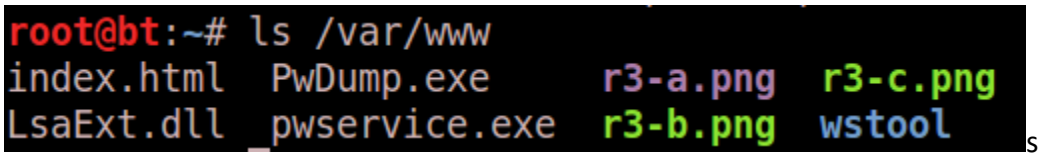
2. Type the following to list the files within FTP root:
   root@bt:~# **ls /home/hax0r**



3. Type the following to copy picture files to the HTTP root:
   root@bt:~# **cp /usr/share/wallpapers/backtrack/r* /var/www**



4. Type the following command to list the files within FTP root:
   root@bt:~# **ls /var/www**

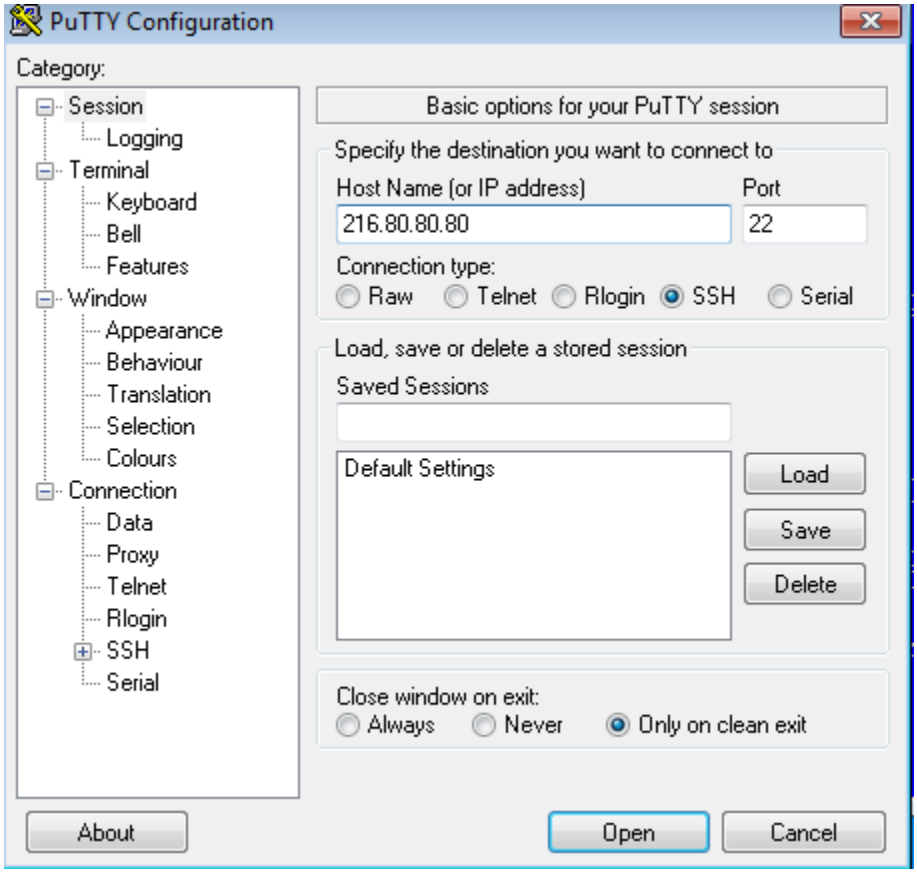


s

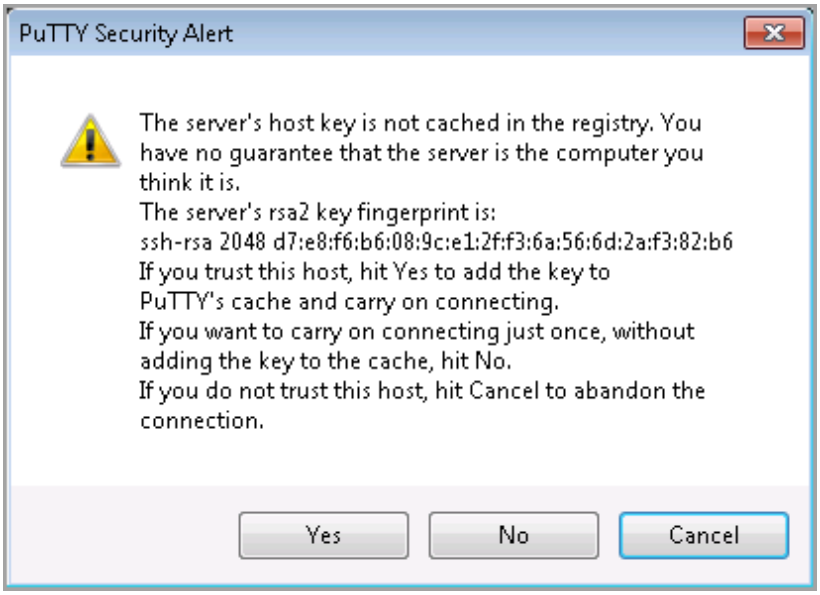
5. From the **Windows 7 External Machine**, open **putty.exe** on the desktop.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

6. Type 216.80.80.80 in the Host Name box and click Open.

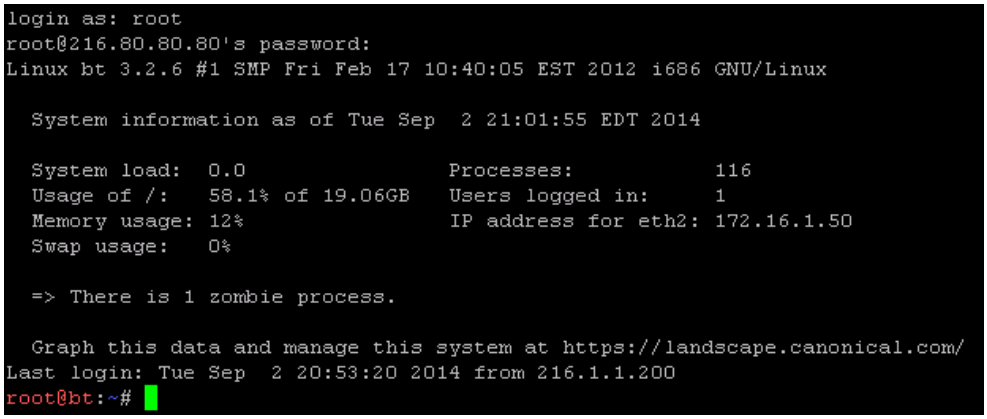


7. Click **Yes** to add the host key to cache.

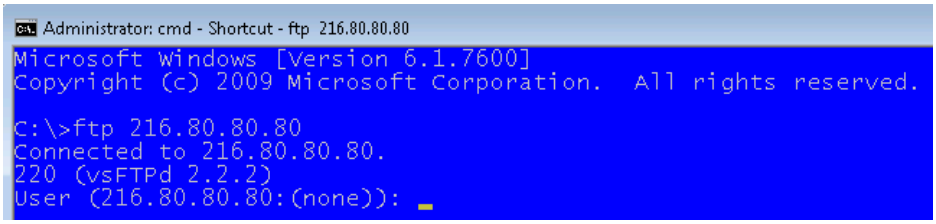


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

8. Log in as **root** with the password of **toor**. Close the SSH session by typing **exit**.

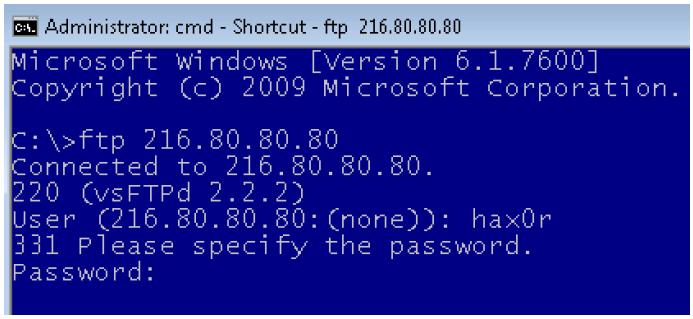


9. From the **Windows 7 External Machine** command prompt, type the following command to connect to the VSFTPD server:
C:\>**ftp 216.80.80.80**



10. For the username, type **hax0r.**

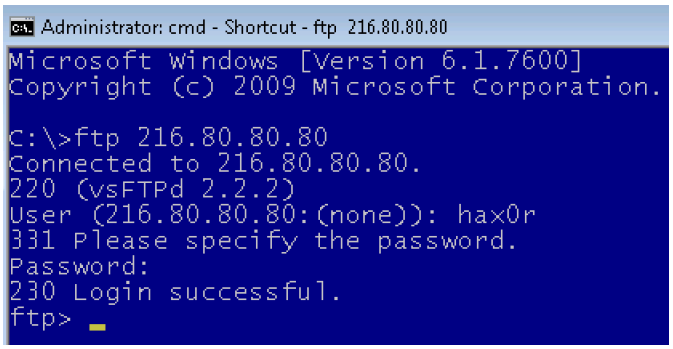
The username hax0r uses a zero, not the letter 0.



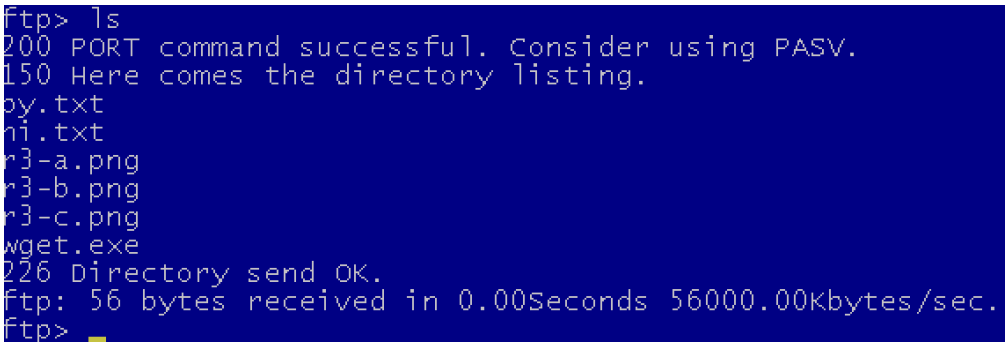
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

11. Type **hacker** for the password. You should receive the login successful message.

The FTP password will not be displayed when you type it, for security purposes.

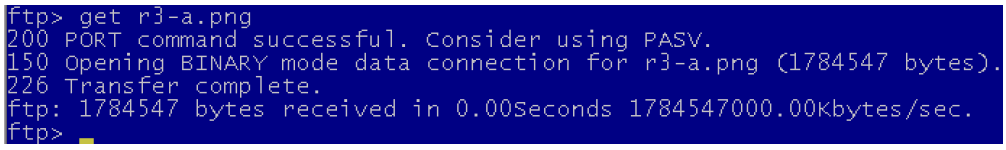


12. Type the following to list the files on the VSFTPD server:
ftp>**ls**



13. Type the following command to switch to binary mode:
ftp>**bin**

14. Type the following to download the PNG file from the FTP Site (After typing the command, you should receive the message, *transfer complete*) :
ftp>**get r3-a.png**



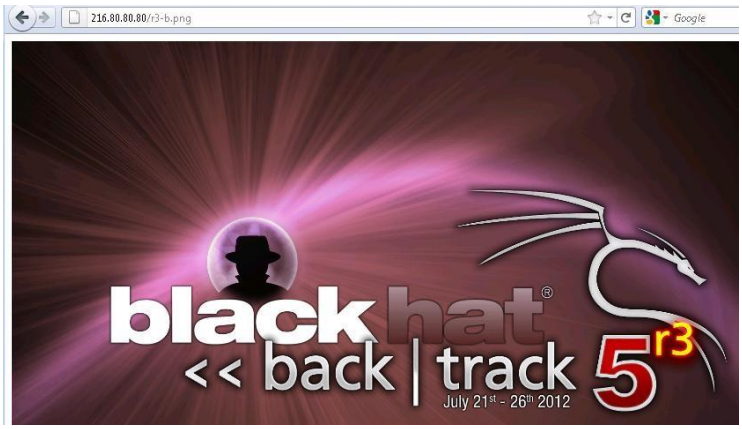
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

15. Type the following to leave the FTP session:
    ftp>**bye**

16. Now type the following to view the downloaded PNG file:
    C:\>**mspaint r3-a.png**

17. From the Windows 7 desktop, click the shortcut to go to Firefox:

18. In the URL bar, type http://216.80.80.80/r3-b.png to access the Public Website.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

19. From the Windows 7 command prompt, type the following to download the fgdump.exe file:
    C:\>**tftp -i 216.80.80.80 get fgdump.exe**

```
C:\>tftp -i 216.80.80.80 get fgdump.exe
Transfer successful: 974848 bytes in 1 second(s), 974848 bytes/s
```

20. Type fgdump. Press **Ctrl + C** if the program takes longer than a few minutes.
    C:\>**fgdump.exe**

```
C:\>fgdump
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

No parameters specified, doing a local dump. Specify -? if you are looking for
elp.
--- Session ID: 2015-09-26-19-10-45 ---
Starting dump on 127.0.0.1

** Beginning local dump **
OS (127.0.0.1): Microsoft Windows Unknown Professional (Build 7600)
Passwords dumped successfully
Cache dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
127.0.0.1

Total failed: 0
Total successful: 1

C:\>_
```

21. Type the following command to dump the password hashes:
    C:\>**type 127.0.0.1.pwdump**

```
C:\>type 127.0.0.1.pwdump
Administrator:500:NO PASSWORD*********************:NO PASSWORD*****************
***:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HomeGroupUser$:1006:NO PASSWORD*********************:1FA16353A1B2AC6654E760092D
61452:::
student:1000:NO PASSWORD*********************:8846F7EAEE8FB117AD06BDD830B7586C:
:

C:\>
```

22. Close all open windows and PC viewers. End the reservation.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

3.2 Conclusion

While using nmap is an effective way to verify ports are open, it will not be as effective as testing each service. In this section of the lab, we tested the SSH, FTP, HTTP, and TFTP services. The successful logins and file transfers proved that the services were operating properly. These quality assurance checks are essential for production environments.

3.3 Discussion Questions

1. What is the command to download a file with tftp?
   Ans: The command to download a file is
   tftp -i 216.80.80.80 get fgdump.exe 2.
2. What does the program fgdump.exe do?
   Ans: It extracts the passwords hashes .
3. What command needs to be typed in ftp to switch to binary mode?
   Ans: ftp > bin command
4. Where is the default web root directory located in BackTrack Linux?
   Ans: In BackTrack Linux, the default web root directory is located at "/var/www/". This is the directory where Apache web server serves the web pages from.

References

1. IPTABLES:
   http://en.wikipedia.org/wiki/Iptables

2. IPTABLES Port Redirection:
   http://blog.softlayer.com/2011/iptables-tips-and-tricks-port-redirection

3. IPTABLES NAT:
   http://www.howtoforge.com/nat_iptables

4. nat:
   http://en.wikipedia.org/wiki/Network_address_translation

5. fgdump:
   http://foofus.net/goons/fizzgig/fgdump/

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.