

Denial of Service

Module 10

Denial of Service

Denial of Service (DoS) is an attack on a computer or network that prevents legitimate use of its resources.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

In computing, a denial-of-service attack (DoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. Denial-of-service attacks can essentially disable your computer or your network. DoS attacks can be lucrative for criminals; recent attacks have shown that DoS attacks a way for cyber criminals to profit.


As an expert ethical hacker or **security administrator** of an organization, you should have sound knowledge of how **denial-of-service** and **distributed denial-of-service** attacks are carried out, to **detect** and **neutralize** attack handlers, and to **mitigate** such attacks.

Lab Objectives

The objective of this lab is to help students learn to perform DoS attacks and to test network for DoS flaws.

In this lab, you will:

- Create and launch a denial-of-service attack to a victim
- Remotely administer clients
- Perform a DoS attack by sending a huge amount of SYN packets continuously
- Perform a DoSHTTP attack

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service**

Lab Environment

To carry out this, you need:

- A computer running Window Server 2008
- Windows XP/7 running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Denial of Service

Denial-of-service (DoS) is an attack on a computer or network that **prevents** legitimate use of its resources. In a DoS attack, attackers **flood** a victim's system with illegitimate service requests or **traffic** to **overload** its resources and prevent it from performing **intended** tasks.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in denial of service:

- SYN flooding a target host using hping3
- HTTP flooding using DoSHTTP

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.




SYN Flooding a Target Host Using hping3

hping3 is a command-line oriented TCP/IP packet assembler/analyzer.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, cause the server to send the SYN-ACK to a falsified IP address, which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

As an expert **ethical hacker** or **security administrator** of an organization, you should have sound knowledge of **denial-of-service and distributed denial-of-service** attacks and should be able to **detect** and **neutralize** attack handlers. You should use SYN cookies as a countermeasure against the SYN flood which eliminates the resources allocated on the target host.

Lab Objectives

The objective of this lab is to help students learn to perform denial-of-service attacks and test the network for DoS flaws.

In this lab, you will:

- Perform denial-of-service attacks
- Send huge amount of SYN packets continuously

Tools demonstrated in this lab are available at **D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service**

Lab Environment

To carry out the lab, you need:

- A computer running Windows 7 as victim machine
- BackTrack 5 r3 running in virtual machine as attacker machine
- **Wireshark** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

Lab Duration

Time: 10 Minutes

Overview of hping3

hping3 is a network tool able to send custom TCP/IP packets and to display target replies like a ping program does with ICMP replies. hping3 handles fragmentation, arbitrary packets body, and size and can be used in order to transfer files encapsulated under supported protocols.

Lab Tasks

TASK 1 Flood SYN Packet

1. Launch **BackTack 5 r3** on the virtual machine.
2. Launch the **hping3** utility from the BackTrack 5 r3 virtual machine. Select **BackTrack Menu → Backtrack → Information Gathering → Network Analysis → Identify Live Hosts → Hping3**.

hping3 is a command-line oriented TCP/IP packet assembler/analyzer.

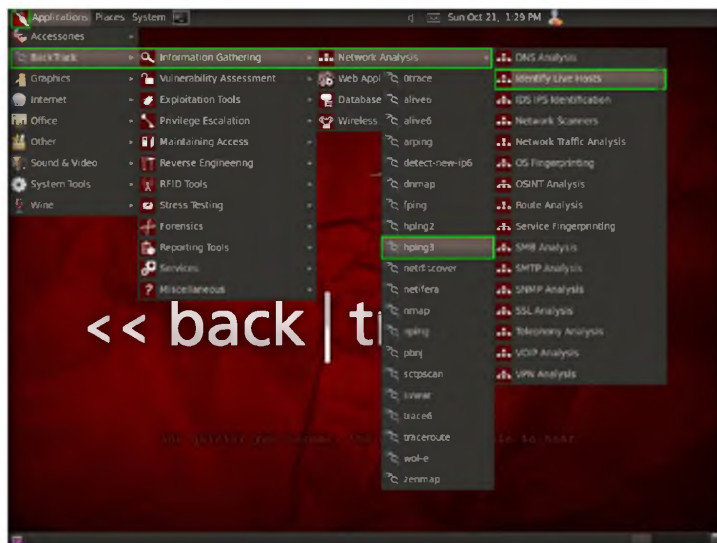
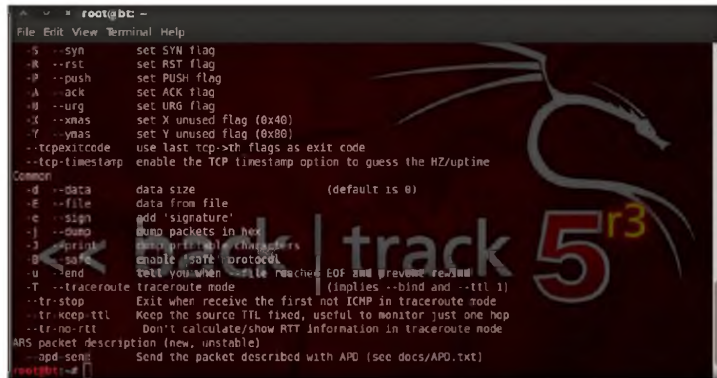


Figure 1.1: BackTrack 5 r3 Menu

3. The **hping3** utility starts in the command shell.

Type only **hping3** without any argument. If hping3 was compiled with Tcl scripting capabilities, you should see a prompt.


Module 10 – Denial of Service

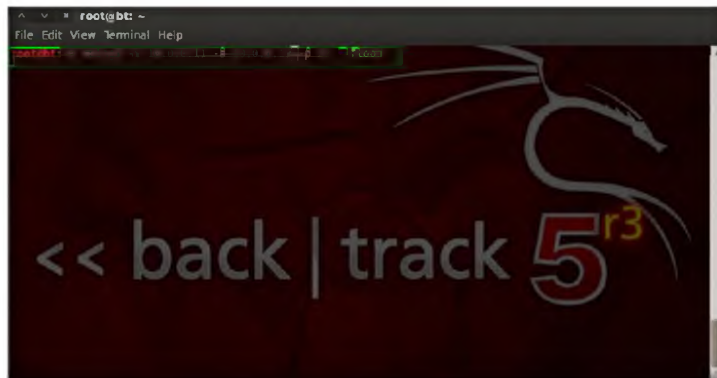


```
root@bt: ~
File Edit View Terminal Help
S --syn          set SYN flag
R --rst          set RST flag
P --push        set PUSH flag
A --ack         set ACK flag
U --urg         set URG flag
X --xmas        set X unused flag (0x40)
Y --ymas        set Y unused flag (0x80)
--tcpexitcode   use last tcp->sth flags as exit code
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data        data size (default is 0)
-e --file        data from file
-c --sig         add 'signature'
-j --dump        @dump packets in hex
-J --print       @print packet's checksums
-p --port        enable source's protocol
-u --end         tell you when message reached EOF and previous row
-T --traceroute  traceroute mode (implies --bind and --ttl 1)
--tr-stop       Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl   Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt     Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send      Send the packet described with APD (see docs/APD.txt)
root@bt: ~
```

FIGURE 1.2: BackTrack 5 r3 Command Shell with hping3

4. In the command shell, type **hping3 -S 10.0.0.11 -a 10.0.0.13 -p 22 --flood** and press **Enter**.


 First, type a simple command and see the result: #hping3.0.0-alpha-1> hping resolve www.google.com 66.102.9.104.

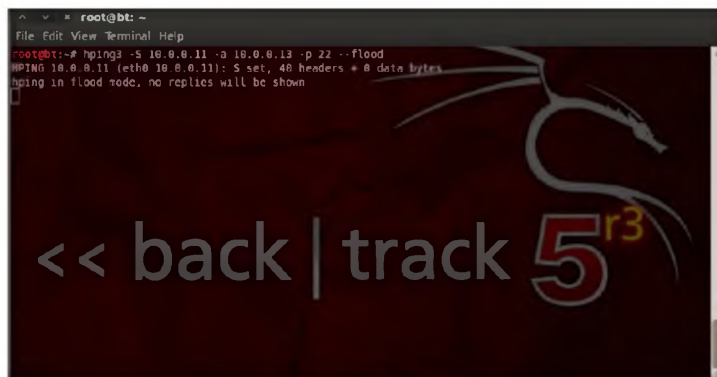


```
root@bt: ~
File Edit View Terminal Help
root@bt:~# hping3 -S 10.0.0.11 -a 10.0.0.13 -p 22 --flood
root@bt:~#
```

FIGURE 1.3: BackTrack 5 r3 hping3 command

5. In the previous command, **10.0.0.11 (Windows 7)** is the **victim's** machine IP address, and **10.0.0.13 (BackTrack 5 r3)** is the **attacker's** machine IP address.


 The hping3 command should be called with a subcommand as a first argument and additional arguments according to the particular subcommand.



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# hping3 -S 10.0.0.11 -a 10.0.0.13 -p 22 --flood
HPING 10.0.0.11 (eth0 10.0.0.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

FIGURE 1.4: BackTrack4 Command Shell with hping3

6. hping3 floods the victim machine by sending bulk SYN packets and overloading victim resources.

 The hping resolve command is used to convert a hostname to an IP address.

Module 10 – Denial of Service

- Go to the **victim's machine (Windows 7)**. Install and launch Wireshark, and observe the SYN packets.

hping3 was mainly used as a security tool in the past. It can be used in many ways by people who don't care for security to test networks and hosts. A subset of the things you can do using hping3:

- Firewall testing
- Advanced port scanning
- Network testing, using various protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

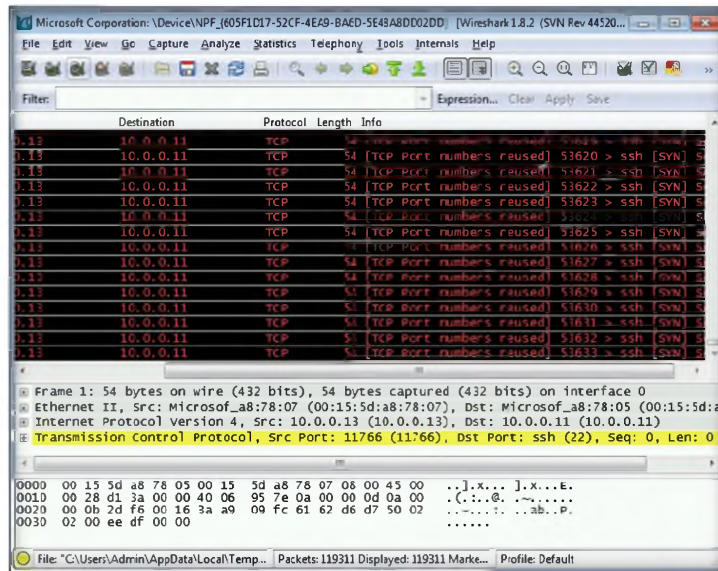


FIGURE 1.5: Wireshark with SYN Packets Traffic

- You sent huge number of SYN packets, which caused the victim's machine to crash.

Lab Analysis

Document all the results gather during the lab.

Tool/Utility	Information Collected/Objectives Achieved
hping3	SYN packets observed over flooding the resources in victim machine

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



HTTP Flooding Using DoSHTTP

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. DoSHTTP includes port designation and reporting.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

Lab Scenario

HTTP flooding is an attack that uses enormous useless packets to jam a web server. In this paper, we use hidden semi-Markov models (HSMM) to describe Web-browsing patterns and detect HTTP flooding attacks. We first use a large number of legitimate request sequences to train an HSMM model and then use this legitimate model to check each incoming request sequence. Abnormal Web traffic whose likelihood falls into unreasonable range for the legitimate model would be classified as potential attack traffic and should be controlled with special actions such as filtering or limiting the traffic. Finally we validate our approach by testing the method with real data. The result shows that our method can detect the anomaly web traffic effectively.

In the previous lab you learned about SYN flooding using `hping3` and the countermeasures that can be implemented to prevent such attacks. Another method that attackers can use to attack a server is by using the HTTP flood approach.

As an expert **ethical hacker** and **penetration tester**, you must be aware of all types of hacking attempts on a web server. For HTTP flooding attack you should implement an advanced technique known as “tarpitting,” which once established successfully will set connections window size to few bytes. According to TCP/IP protocol design, the connecting device will initially only send as much data to target as it takes to fill the window until the server responds. With tarpitting, there will be no response back to the packets for all unwanted HTTP requests, thereby protecting your web server.

Lab Objectives

The objective of this lab is to help students learn HTTP flooding denial-of-service (DoS) attack.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service

Lab Environment

To carry out this lab, you need:

- **DoSHTTP** tool located at **D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service\DDoS Attack Tools\DoS HTTP**
- You can also download the latest version of **DoSHTTP** from the link <http://www.socketsoft.net/>
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 7** running on virtual machine as attacker machine
- A web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of DoSHTTP

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. It includes URL verification, HTTP redirection, and performance monitoring. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP flood. DoSHTTP can be used simultaneously on multiple clients to emulate a distributed denial-of-service (DDoS) attack. This tool is used by IT professionals to test web server performance.

Lab Tasks

TASK 1

DoSHTTP Flooding

1. Install and launch DoSHTTP in **Windows Server 2012**.
2. To launch DoSHTTP, move your mouse cursor to lower left corner of the desktop and click **Start**.

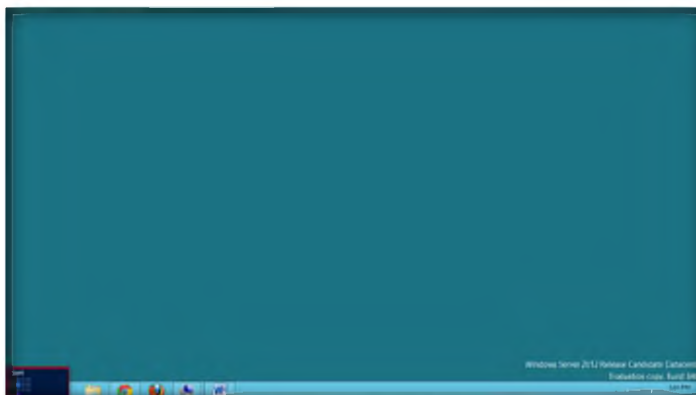


FIGURE 2.1: Windows Server 2012 Desktop view

Module 10 – Denial of Service

3. Click the **DoSHttp 2.5** app from the **Start** menu apps to launch the program.

 DoSHTTP is an easy to use and powerful HTTP Flood Denial of Service (DoS) Testing Tool for Windows. DoSHTTP includes URL Verification, HTTP Redirection, Port Designation, Performance Monitoring and Enhanced Reporting.

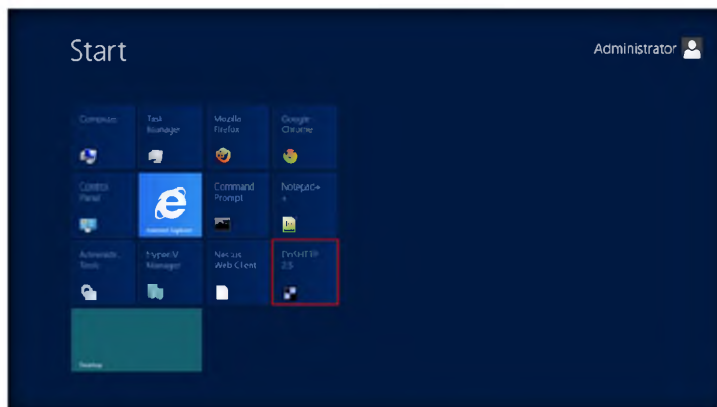



FIGURE 2.2: Windows Server 2012 Start Menu Apps

4. The **DoSHTTP** main screen appears as shown in the following figure; in this lab we have demonstrated trial version. Click **Try** to continue.

 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service**

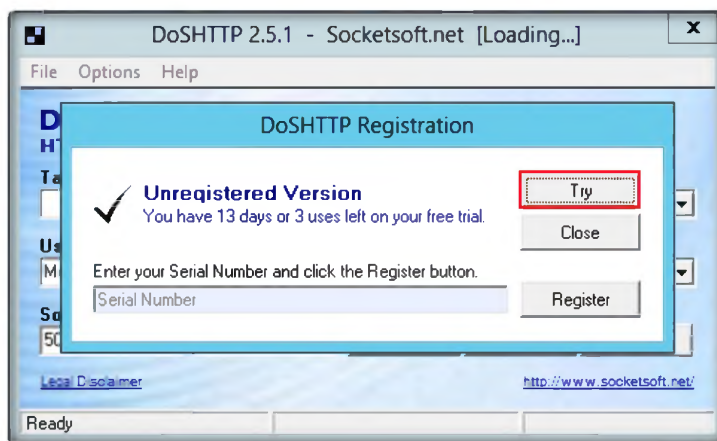


FIGURE 2.3: DoSHTTP main window

5. Enter the URL or IP address in the **Target URL** field.
6. Select a **User Agent**, number of **Sockets** to send, and the type of **Requests** to send. Click **Start**.
7. In this lab, we are using Windows 7 IP (10.0.0.7) to flood.

Module 10 – Denial of Service

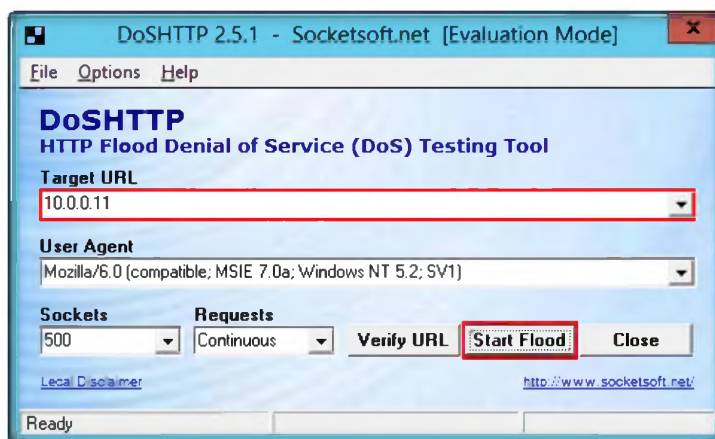


FIGURE 2.4: DoSHTTP Flooding

Note: These IP addresses may differ in your lab environment.

8. Click **OK** in the DoSHTTP evaluation pop-up.

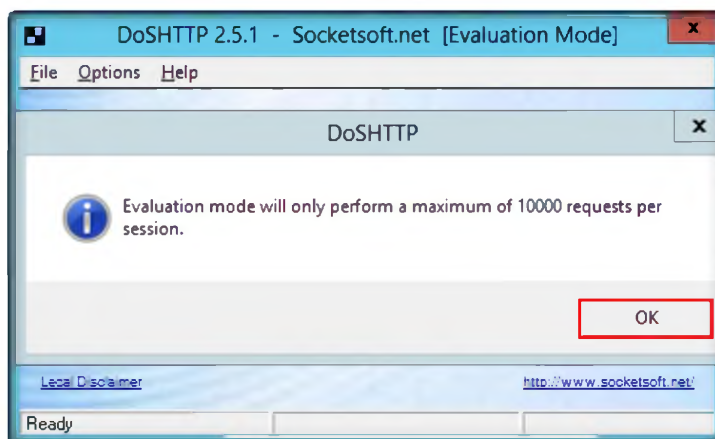


FIGURE 2.5: DoSHTTP Evaluation mode pop-up

9. Launch the **Wireshark** network protocol analyzer in the **Windows 7 virtual machine** and start its interface.
10. DoSHTTP sends **asynchronous** sockets and performs **HTTP flooding** of the target network.
11. Go to **Virtual machine**, open **Wireshark**, and observe that a lot of packet traffic is captured by Wireshark.

 DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP Flood. DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

 DoSHTTP can help IT Professionals test web server performance and evaluate web server protection software. DoSHTTP was developed by certified IT Security and Software Development professionals

Module 10 – Denial of Service

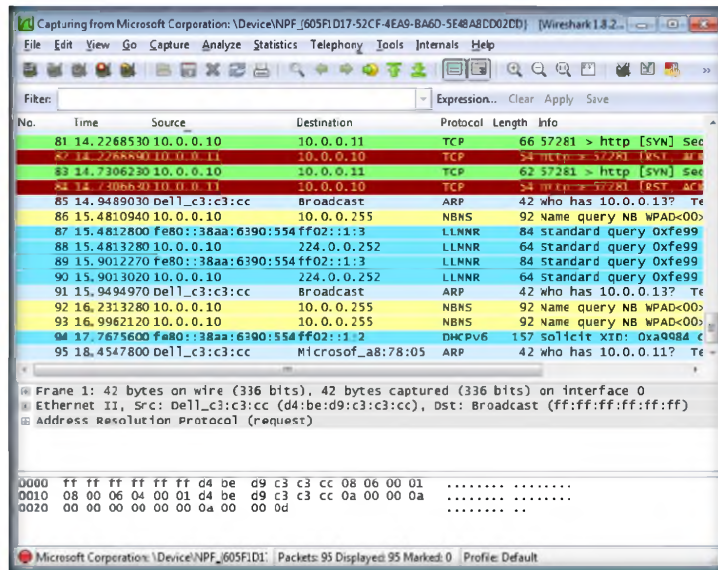


FIGURE 2.6: Wireshark window

DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

12. You see a lot of HTTP packets are flooded to the host machine.
13. DoSHTTP uses multiple asynchronous sockets to perform an HTTP flood against the entered network.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
DoSHTTP	HTTP packets observed flooding the host machine

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate how DoSHTTP can be used simultaneously on multiple clients and perform DDoS attacks.

Module 10 – Denial of Service

2. Determine how you can prevent DoS/HTTP attacks on a network.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs