Module 10: Denial of Service

Objective

The objective of this lab is to help students learn to perform Denial of Service attacks and to test network for Denial of Service 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

Scenario

To be 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.

Virtual Machines

The following virtual machines are required for completion of this lab:

1. Windows 7 (10.10.10.31)
2. 2003 Server (10.10.10.61)
3. NAT
4. 2008 Server (10.10.10.1)

Exercise I: Creating a Zombie Using Poison Ivy

Lab Scenario

To be 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. You should be able to detect and neutralize attack handlers and mitigate such attacks.

Lab Objectives

The objective of this lab is to help students learn to administer networks remotely.

1. **Logon to Windows Server 2008**

Switch to Windows Server 2008 (10.10.10.1) machine from **Machines** tab in the right pane of the window.

2. **Enter Credentials**

   Go to **Machine Commands** and click **Ctrl+Alt+Del**.

   In the log on box enter the following credentials and press **Enter**.
   User Name: Administrator
   Password: Pa$$w0rd

   Once you login to Windows Server 2008 (10.10.10.1) machine server manager window will pop-up, close server manager window.

   You can use the **Machine Commands** menu to enter your user name and password.

3. **Extract Poison Ivy**

   To Extract Poison Ivy, navigate to **E:\CEHv7 Module 10 Denial of Service\Botnet\Poison Ivy**.

   Right-click on **PI2.3.2.rar** file and select **Extract Here** option from context menu.

4. **Launch Poison Ivy**

   To launch Poison Ivy, navigate to **E:\CEHv7 Module 10 Denial of Service\Botnet\Poison Ivy**.

   Double-click on **Poison Ivy 2.3.2.exe** file to launch Poison Ivy.

5. **Terms and Conditions EULA**

   In Terms and Conditions EULA window click **I Agree** button to continue

6. **Create New Server**

   To create **New Server** navigate to **File** and select **New Server**.

7. **Create a New Profile**

   To create a New Profile, click on **Create Profile** option.

8. **Profile Name**

   Provide a **Profile Name** (example: juggyboy) for the profile and click **OK**.

9. **Connection Panel**

   In the Connection panel, Click **Add** in DNS/Port number

10. **DNS/Port wizard**

    In DNS/Port wizard click on 127.0.0.1 to edit it, replace the 127.0.0.1 with the Windows Server 2008 (10.10.10.1). This IP address will be different at your network location. Click **OK**

11. **Connection Panel**

    It will again show the connection windows. Click **Next**

12. **Install Panel**

    Set the settings to default and click **Next** on **Install** panel.

13. **Advanced Panel**

    Set the settings to be default in **Advanced** panel window and click **Next**

14. **Build Panel**

    Now click **Generate** button to build a Server.

15. **Provide Server Name**

    Enter server name (example: juggyboy) and click **Save** in your desired location.

    In this lab we have saved this server in E:\CEHv7 Module 10 Denial of Server\Botnets\Poison Ivy

16. **Server Generated Message**

    After generating server, click **OK** in the Build window

17. **Create New Client**

    To create new client go to **File** and select **New Client** option from the menu bar

18. **New Client Window**

    It will open a new client window, Click **Start** button to create a client without changing any settings

19. **New Client Screen**

    The client screen will appear and will listen to the server

    Don't close the client window.

20. **Switch to Windows Server 2003**

    Switch to **Windows Server 2003** (10.10.10.61) machine from **Machines** tab in the right pane of the window.

21. **Enter Credentials**

    Go to **Machine Commands** and click **Ctrl+Alt+Del**.

    In the log on box enter the following Credentials and press **Enter**.
    User Name: **Administrator**
    Password: **Pa$$w0rd**

    You can also use the **Machine Commands** menu to enter the user name and password.

22. **Run juggyboy.exe**

    Navigate to the directory where the server '**juggyboy.exe**' is stored, In this lab, it is saved at **Z:\CEHv7 Module 10 Denial of Service\Botnet\Poison Ivy Ivy**.

    Double-click on **juggyboy.exe** to run.

    Z: drive is mapped network drive containing the CEH tools.

23. **Open File - Security Warning**

    Click on **Run** button in Open File - Security Warning window.

24. **Switch to Windows Server 2008**

    Switch to Windows Server 2008 (10.10.10.1) machine from **Machines** tab in the right pane of the window.

    You can also click on disk-arrow icon at the right-bottom corner of the window to swich to Windows Server 2008 machine.

25. **Client Records**

    The client starts **recording** the server activity.

26. **View Information**

    Double click on the **record**. It will show the information of the machine where the server is installed (Windows Server 2003 10.10.10.61)

27. **Remote Shell**

    Now select **Remote Shell** from the left pane. On the right pane, right click and select **Activate**. It will activate the command shell at Windows Server 2003 (IP address: 10.10.10.61) in client.

28. **IP Config**

    Type **ipconfig** in the command prompt of **Poison Ivy** client, it will show the IP of Windows Server 2003 (IP address: 10.10.10.61).

Lab Analysis

In this lab you have administered the networks remotely.

Exercise II: HTTP Flooding using DoSHTTP

Lab Scenario

*To be an expert Ethical Hacker and Penetration Tester, you must have sound knowledge of how to carry out **Denial of Service** and **Distributed Denial of Service attacks**, **HTTP Flood Denial of Service** (DoS) attacks. You must be able to **detect** and **neutralize attack handlers** and mitigate such attacks.*

Lab Objectives

*The objective of this lab is to help students learn **HTTP Flooding** Denial of Service (DoS) attack.*

1. **Switch to Windows Server 2003 Machine**

   Switch to **Windows Server 2003** (10.10.10.61) machine from **Machines** tab in the right pane of the window.

2. **Enter Credentials**

   Go to **Machine Commands** and click **Ctrl+Alt+Del**.

   In the log on box enter the following credentials and press **Enter**.
   User Name: **Administrator**
   Password: **Pa$$w0rd**

You can also use the **Machine Commands** menu to enter your user name and password.

3. **Install DoSHTTP**

   To install DoSHTTP, navigate to **Z:\CEHv7 Module 10 Denial of Service\DoS Attack Tools\DoSHTTP**

   Double-click on **doshttp_setup.exe** to install DoSHTTP.

   Follow the wizard driven installation steps to install DoSHTTP.

   Z:\ drive is mapped network drive containing the CEH tools.

4. **CRC32 Error**

   While installation in process CRC32 Error pop-up appears, click **OK** to continue.

5. **Application Error**

   Application Error pop-up appears click **OK** to continue.

6. **Switch to Windows Server 2008 Machine**

   Switch to **Windows Server 2008** (10.10.10.1) machine from **Machines** tab in the right pane of the window.

7. **Enter Credentials**

   Go to **Machine Commands** and click **Ctrl+Alt+Del**.

   In the log on box enter the following credentials and press **Enter**.
   User Name: **Administrator**
   Password: **Pa$$w0rd**

   Once you login to Windows Server 2008 (10.10.10.1) machine, **Server Manager** window will pop-up. Close the **Server Manager** window.

   You can also use the **Machine Commands** menu to enter the user name and password.

8. **Install Wireshark**

   To install Wireshark, navigate to **E:\CEH-Tools\CEHv7 Module 08 Sniffers\Sniffing Tools\Wireshark**.

   Double-click on **wireshark.exe** to install Wireshark.

Follow the wizard driven installation steps.

9. **Launch Wireshark**

   Launch the Wireshark network protocol analyzer in the **Windows Server 2008** (IP address: 10.10.10.1) and start its interface.

   To launch Wireshark, navigate to **Start** -> **All Programs** -> **Wireshark** -> **Wireshark**.

10. **Wireshark pop-up**

    As you launch Wireshark, Wireshark pop-up appears as shown in the following figure, Click **OK** to continue.

11. **Start Interface**

    To start the interface, navigate to **Capture** --> **Interface**.

12. **Wireshark Capture Interfaces**

    Select the **ethernet adapter** and click on **Start** button.

    Leave the Wireshark running in the Windows Server 2008.

13. **Switch to Windows Server 2003**

    Switch back to **Windows Server 2003** machine from the **Machines** tab.

14. **Launch DoSHTTP**

    To launch DoSHTTP, navigate to **Start** -> **All Programs** -> **Socketsoft** -> **DoSHTTP 2.5**.

15. **Step 1 of 2**

    Click on **I Accept** button in the **License Agreement** wizard.

16. **Step 2 of 2**

    Click on **I Accept** in the **Legal Disclaimer** wizard.

17. **DoSHTTP pop-up**

    DoSHTTP pop-up appears click **OK** to continue.

18. **DoSHTTP Flooding**

The DoSHTTP window appears. In the **Target URL field**, input the **IP address** of the Windows Server 2008 machine (victim machine).

Select a **User Agent**, **number of Sockets to send**, and the **type of Requests to send**.

After selecting all the fields, click **Start Flood**.

19. **Switch Back to Windows Server 2008 Machine**

    Switch back to **Windows Server 2008** machine from the **Machines** tab.

20. **Check with Wireshark**

    DoSHTTP sends asynchronous sockets and performs **HTTP flooding** of the target network.

    Go to the **Windows Server 2008** machine, open **Wireshark** and observe that a lot of packet traffic is captured by Wireshark.

Lab Analysis

In this lab you have performed HTTP Flooding Denial of Service (DoS) attack.